Guide de l’utilisateur

Agent de sécurité AWS

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Agent de sécurité AWS: Guide de l’utilisateur

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Les marques et la présentation commerciale d’Amazon ne peuvent pas être utilisées en relation avec un produit ou un service qui n’appartient pas à Amazon, de toute manière susceptible de créer une confusion chez les clients ou de toute manière dénigrant ou discréditant Amazon. Toutes les autres marques commerciales qui ne sont pas la propriété d’Amazon appartiennent à leurs propriétaires respectifs, qui peuvent ou non être affiliés ou connectés à Amazon, ou sponsorisés par Amazon.

Table of Contents

Introduction 1
Qu'est-ce qu'AWS Security Agent ? 1
Capacités clés 1
Avantages 3
Fonctionnalités d'AWS Security Agent 4
Comment fonctionne l'agent de sécurité AWS 5
Présentation de 5
Comprendre la hiérarchie et le cycle de vie des ressources 9
Ce qui est partagé au sein de votre organisation 10
Ce qui est défini par agent Space 10
Comment les GitHub référentiels s'insèrent dans la hiérarchie 12
Principales différences entre les capacités de sécurité 13
Comprendre les relations entre les ressources 15
Prise en main 16
Inscrivez-vous pour AWS 16
Choisissez votre voie 16
Démarrage rapide : exécutez un test de pénétration 17
Conditions préalables 18
Étape 1 : configurer l'agent de sécurité AWS dans la console AWS 18
Étape 2 : Activez les tests de pénétration et vérifiez votre domaine 19
Étape 3 : Connecter le code source (facultatif) 20
Étape 4 : Création et exécution d'un test de pénétration 20
Étape 5 : Examiner les résultats des tests de pénétration 21
Démarrage rapide : Exécuter une révision du code 22
Conditions préalables 18
Étape 1 : configurer l'agent de sécurité AWS dans la console AWS 18
Étape 2 : activer et configurer la révision du code 23
Étape 3 : créer et exécuter une révision de code 25
Étape 4 : Examiner les résultats de la révision du code 25
Démarrage rapide : exécuter un modèle de menace 26
Étape 1 : configurer l'agent de sécurité AWS dans la console AWS 18
Étape 2 : Connecter le code source 27
Étape 3 : créer et exécuter un modèle de menace 28
Étape 4 : Examiner les menaces 29

Pour les administrateurs (console) 30
Exemple de configuration 30
Configuration et création d'espaces d'agents 30
Configuration de l'agent de sécurité AWS 30
Création d'un espace d'agent 36
Intégrations Connect 38
Comment fonctionnent les intégrations avec Agent Spaces 38
Connect AWS Security Agent aux GitHub référentiels 41
Supprimer une GitHub intégration 47
Connect AWS Security Agent aux GitLab référentiels 49
Connectez l'agent de sécurité AWS à GitLab Self-Managed 53
Supprimer une GitLab intégration 56
Connect AWS Security Agent au serveur GitHub d'entreprise 57
Supprimer une intégration de serveur d' GitHub entreprise 61
Trouvez votre identifiant d'installation Atlassian 62
Connect AWS Security Agent aux référentiels Bitbucket 63
Supprimer une intégration Bitbucket 67
Connectez l'agent de sécurité AWS à Confluence 68
Supprimer une intégration Confluence 72
Connectez-vous au contrôle de source hébergé en privé 73
Connect l'agent aux ressources VPC privées 78
Configurer les fonctionnalités 82
Activer le test de pénétration 82
Activer la révision du code de pull request pour les GitHub référentiels 88
Activer la révision du code 89
Activez la modélisation des menaces 96
Permettre aux utilisateurs de commencer à corriger les résultats des tests d'intrusion et de la révision du code 100
Fournir des ressources aux agents à partir d'un compartiment S3 101
Activer un domaine d'application pour les tests de pénétration 102
Domaines cibles gérés utilisés pour les tests de pénétration 105
Gérer les exigences de sécurité 106
Gérer les exigences de sécurité 106
Packs gérés par AWS 113
Générez des exigences de sécurité à partir de documents 115
Préparer les documents pour la génération d'exigences 117

Gérer les utilisateurs et les accès 118
Autoriser les utilisateurs à accéder à l'application Web AWS Security Agent 119
Création d'un rôle IAM pour AWS Security Agent 121
Clés gérées par le client 127
Résolution des problèmes 152
Accès refusé : type de GitHub compte sélectionné incorrect ou nom d'organisation incorrect spécifié 152
Accès refusé : autorisations insuffisantes pour installer GitHub l'application dans l'organisation 153
L'agent ne peut pas se connecter au terminal pendant un test d'intrusion 153
Aide supplémentaire 154
Pour les utilisateurs et les développeurs (application Web et IDE) 155
Connectez-vous à l'application Web AWS Security Agent 155
Modes d'accès 155
Connectez-vous avec IAM Identity Center (SSO) 156
Connectez-vous avec un accès administrateur (IAM) 157
Création d'une revue de conception 158
Conditions préalables 18
Étape 1 : Commencez à créer une révision de conception 158
Étape 2 : Donnez un nom à votre critique de conception 159
Étape 3 : Téléchargez les fichiers de conception 159
Étape 4 : Lancer la révision de la conception 160
Étapes suivantes 35
Examiner les résultats d'une revue de conception 161
Création d'un modèle de menace 165
Conditions préalables 18
Comment l'agent de sécurité AWS exécute un modèle de menace 166
Accédez à la page des modèles de menaces 167
Création d'un modèle de menace 167
Exécutez un modèle de menace 170
Surveiller l'exécution d'un modèle de menace 170
Modifier un modèle de menace 171
Supprimer un modèle de menace 172
Étapes suivantes 35
Analyser les menaces à partir d'un modèle de menace 172
Passez en revue les résultats de sécurité du code dans les pull requests 178

Comment fonctionne la révision du code dans les pull requests 179
Comprendre les résultats de la révision du code 179
Réagir aux constatations relatives à la sécurité 180
Résultats de l'examen du code de filtrage 181
Étapes suivantes 35
Création d'une révision de code 183
Conditions préalables 18
Accédez à la page de révision du code 184
Création d'une révision de code 184
Exécuter une révision du code 190
Surveiller l'exécution d'une révision de code 190
Étapes suivantes 35
Examiner les résultats d'une révision de code 192
Corriger les résultats de la révision du code 199
Exécuter un scan de code différentiel avec S3 202
Comment fonctionnent les scans différentiels 202
Conditions préalables 18
Étape 1 : générer un fichier diff 204
Étape 2 : télécharger le diff sur S3 204
Étape 3 : démarrer une tâche de révision du code différentiel 204
Étape 4 : Surveiller le scan 205
Étape 5 : Examiner les résultats 206
Quotas et limites 206
Étapes suivantes 35
Exécutez des analyses de sécurité du code à partir de votre IDE 207
Comment fonctionne l'intégration IDE 207
Conditions préalables 18
Installation du serveur MCP 209
First-time configuration 210
Exécuter une analyse de sécurité complète 211
Exécuter un scan différentiel 211
Exécuter un examen du modèle de menace 212
Examen des résultats 213
Appliquer des correctifs automatisés 213
Suggestions de numérisation automatique (Kiro) 214
Types de scan disponibles 214

Variables d'environnement 215
Résolution des problèmes 215
Quotas et limites 206
Étapes suivantes 35
Créez un test de pénétration 216
Conditions préalables 18
Commencez à créer un test de pénétration 217
Donnez un nom à votre test de pénétration 217
Configuration de la portée du test de pénétration 218
Configurer le rôle IAM 221
Correction automatique du code 200
Configurer les ressources VPC (facultatif) 222
Configurer les informations d'authentification (facultatif) 223
Joindre des ressources supplémentaires (facultatif) 226
Créez le test de pénétration 229
Examiner les résultats d'un test de pénétration 230
Fournir des informations d'authentification pour les tests de pénétration 242
Corriger les résultats d'un test d'intrusion 248
Sécurité et référence 250
Sécurité 250
Considérations de sécurité 250
Politiques gérées par AWS 259
Protection des données 262
Gestion des identités et des accès 265
Intervention en cas d'incidents 283
Validation de conformité 284
Résilience 285
Sécurité de l'infrastructure 286
Points de terminaison de VPC d'Interface 287
Analyse de la configuration et des vulnérabilités 292
Cross-service prévention confuse des adjoints 292
Bonnes pratiques de sécurité 293
Migration des actions et des ressources IAM 297
Se connecter avec CloudTrail 301
Service Quotas 304
Quotas d'opérations 304

Quotas de configuration 304
Historique du document 305
..... cccix

Introduction

Découvrez ce que fait l'agent de sécurité AWS, comment il fonctionne et comment ses ressources s'articulent.

Qu'est-ce qu'AWS Security Agent ?

AWS Security Agent est un agent novateur qui sécurise de manière proactive vos applications tout au long du cycle de développement. Il réalise des examens de sécurité automatisés adaptés aux besoins de votre organisation, élabore des modèles de menace pour identifier la manière dont vos applications pourraient être attaquées et fournit des tests de pénétration contextuels à la demande. En validant en permanence la sécurité de la conception au déploiement, AWS Security Agent aide à prévenir les vulnérabilités à un stade précoce dans tous vos environnements.

Les équipes de sécurité définissent les exigences de sécurité de l'organisation une fois dans la console AWS : bibliothèques d'autorisations approuvées, normes de journalisation et politiques d'accès aux données. AWS Security Agent applique automatiquement ces exigences de sécurité tout au long du développement, en évaluant les documents architecturaux et le code par rapport à vos normes et en fournissant des conseils spécifiques lorsqu'il détecte des violations. Cela permet une application cohérente de la sécurité pour la conception et la révision du code au sein de toutes les équipes.

Pour la validation du déploiement, AWS Security Agent transforme les tests d'intrusion d'un goulot d'étranglement périodique en une fonctionnalité à la demande. Les équipes de sécurité fournissent les URL cibles, les informations d'authentification, le code source et la documentation des applications. AWS Security Agent développe une compréhension approfondie des applications et exécute des chaînes d'attaque sophistiquées pour découvrir et valider les vulnérabilités, ce qui permet aux équipes de procéder à des tests chaque fois que cela est nécessaire.

Capacités clés

AWS Security Agent fournit des fonctionnalités de sécurité complètes couvrant l'ensemble du cycle de développement.

Examen de la sécurité de la conception

AWS Security Agent déplace la sécurité vers la gauche en fournissant des commentaires de sécurité en temps réel sur les documents de conception et en évaluant la conformité aux exigences

de sécurité de l'organisation avant l'écriture du code. Les équipes de sécurité téléchargent des documents via l'application Web et reçoivent des conseils de correction pour hiérarchiser les résultats, accélérant ainsi les révisions manuelles fastidieuses vers des analyses ciblées. En intégrant de manière proactive vos normes de sécurité à chaque révision de conception, vous réduisez les retouches architecturales à un stade avancé et vous suivez le rythme de plusieurs équipes de développement.

Modélisation des menaces

AWS Security Agent crée des modèles de menace pour vos applications afin d'identifier la manière dont elles pourraient être attaquées. Fournissez des documents de conception technique (documents de portée) pour définir les domaines sur lesquels l'agent se concentre, le code source comme contexte permettant à l'agent de comprendre votre système existant, ou les deux. AWS Security Agent génère une vue d'ensemble du système décrivant l'architecture, les composants, les limites de confiance, les flux de données et le niveau de sécurité de votre application, ainsi qu'un ensemble de menaces classées par catégorie STRIDE (usurpation, falsification, répudiation, divulgation d'informations, déni de service, élévation de privilèges) avec des niveaux de gravité et des recommandations exploitables. Les modèles de menace sont des configurations réutilisables que vous pouvez réexécuter au fur et à mesure de l'évolution de votre code et de votre conception, ce qui permet une évaluation itérative de la sécurité tout au long du cycle de développement.

Révision de la sécurité du code

AWS Security Agent sécurise les applications de manière proactive grâce à deux approches complémentaires. Tout d'abord, vous pouvez créer des révisions de code dans l'application Web afin d'effectuer des analyses complètes de votre code source complet à partir de GitHub référentiels Bitbucket ou GitHub Enterprise Server ou de compartiments S3, d'identifier les failles de sécurité et de valider la conformité avec les exigences de votre organisation sur l'ensemble de votre base de code. GitLab Ensuite, vous pouvez activer l'analyse automatique des demandes d'extraction pour les référentiels connectés, où AWS Security Agent examine les modifications de code et publie les résultats de sécurité directement sous forme de commentaires sur les demandes d'extraction ou de fusion. Dans les deux cas, les développeurs reçoivent des conseils de correction, et AWS Security Agent peut générer automatiquement des pull requests ou des demandes de fusion avec des correctifs de code pour les vulnérabilités identifiées. Cela permet d'intégrer l'expertise en matière de sécurité dans tous les référentiels, de réduire les délais liés à la sécurité dans le pipeline de développement et d'étendre l'évaluation à toutes les bases de code.

Tests de pénétration

AWS Security Agent propose des tests de pénétration à la demande en déployant des agents d'intelligence artificielle spécialisés pour découvrir, valider, signaler et corriger les vulnérabilités de sécurité grâce à des scénarios d'attaque personnalisés en plusieurs étapes. L'agent comprend le contexte de votre application en analysant le code source et la documentation afin d'identifier et d'exploiter les vulnérabilités que les outils d'analyse de sécurité automatisés ne peuvent pas détecter. Il documente les résultats à l'aide d'une analyse d'impact, de chemins d'attaque reproductibles et crée des pull requests avec des correctifs de code prêts à implémenter, transformant les évaluations périodiques en une validation continue qui s'adapte à toutes les applications au lieu de se limiter aux seules applications critiques.

Avantages

On-demand accessibilité

AWS Security Agent fournit un accès immédiat à l'expertise en matière de sécurité. Les équipes de développement peuvent effectuer des révisions de conception, des modèles de menaces, des analyses de code et des tests de pénétration à la demande chaque fois que cela est nécessaire, en suivant le rythme des cycles de développement modernes et en garantissant une sécurité proactive à chaque étape.

Validez automatiquement les exigences organisationnelles

Définissez les exigences de sécurité de votre organisation une fois dans la console AWS. AWS Security Agent valide automatiquement ces exigences pour toutes les applications lors de chaque révision de la conception et de la sécurité du code, garantissant ainsi que les équipes répondent à vos exigences spécifiques plutôt qu'à des listes de contrôle génériques.

Développer l'expertise en matière de sécurité

AWS Security Agent adapte les évaluations de sécurité à la vitesse de développement en automatisant l'application des exigences de sécurité de l'organisation. Configurez les exigences de manière centralisée, effectuez des examens complets avec analyse des résultats et gérez les étendues des tests d'intrusion au sein de votre organisation via la console AWS.

Correctifs exploitables pour les vulnérabilités confirmées

AWS Security Agent valide les résultats de sécurité découverts lors des tests d'intrusion grâce à une exploitation basée sur des preuves, en fournissant des chemins d'exploitation reproductibles,

une analyse d'impact complète et crée des pull requests contenant des correctifs prêts à être mis en œuvre dans un langage convivial pour les développeurs. Cela permet aux équipes de se concentrer sur les risques de sécurité légitimes à fort impact sans perdre de temps sur des faux positifs.

Support pour le cloud hybride et multiple

AWS Security Agent fonctionne dans les environnements AWS, sur site, hybrides, multicloud et SaaS, garantissant ainsi des conseils et des tests de sécurité cohérents, quels que soient vos choix en matière d'infrastructure ou de plateforme.

Fonctionnalités d'AWS Security Agent

AWS Security Agent fournit quatre fonctionnalités de sécurité de base tout au long de votre cycle de développement :

- Examen de la sécurité de la conception : examine les documents de conception et d'architecture pour identifier les risques de sécurité. Téléchargez des documents via l'application Web et le service les analyse par rapport aux exigences de sécurité de votre organisation. AWS Security Agent évalue la conformité aux exigences de sécurité que vous avez définies, telles que les bibliothèques d'autorisations approuvées, les normes de journalisation et les politiques d'accès aux données. Cela vous permet de détecter les conceptions peu sûres et les violations des politiques dès le début du processus de développement.
- Modélisation des menaces : crée un modèle de menace pour votre application afin d'identifier la manière dont elle pourrait être attaquée. Fournissez des documents de conception sous forme de documents de portée pour définir l'objectif de l'analyse, du code source comme contexte permettant à l'agent de comprendre votre système existant, ou les deux. AWS Security Agent génère une vue d'ensemble du système qui décrit l'architecture, les composants, les limites de confiance, les flux de données et le niveau de sécurité de votre application, ainsi qu'un ensemble de menaces classées par catégorie STRIDE (usurpation, falsification, répudiation, divulgation d'informations, déni de service, élévation de privilèges) avec des niveaux de gravité et des recommandations exploitables. Chaque menace renvoie à des preuves contenues dans votre code source.
- Examen de la sécurité du code : analyse le code de vos référentiels et de vos sources S3 afin d'identifier les failles de sécurité et les violations des exigences de sécurité de l'organisation dans tous les langages, frameworks et architectures. Créez des révisions de code dans l'application Web pour effectuer des analyses complètes de votre code source complet, ou activez les commentaires de type pull request pour examiner automatiquement les modifications apportées au

code GitHub. AWS Security Agent fournit des conseils de correction spécifiques et peut générer automatiquement des pull requests avec des correctifs de code pour les vulnérabilités identifiées. Cela garantit l'application cohérente de vos politiques de sécurité dans toutes les équipes de développement.

- On-demand tests de pénétration : découvre, valide, signale et corrige les vulnérabilités de sécurité dans les applications Web et les API en ligne grâce à des scénarios d'attaque personnalisés en plusieurs étapes. Configurez le service pour créer un pentest via l'application Web en spécifiant l'étendue du test, les détails de l'authentification et les ressources. AWS Security Agent développe le contexte des applications à partir du code source et de la documentation fournis et exécute des chaînes d'attaque sophistiquées afin d'identifier les vulnérabilités exploitables que l'analyse statique et les outils classiques oublient. Il fournit également des correctifs de code prêts à être implémentés et crée des pull requests directement dans votre référentiel de code, ce qui vous permet de résoudre les vulnérabilités encore plus rapidement.

Comment fonctionne l'agent de sécurité AWS

AWS Security Agent fonctionne sur trois interfaces afin de garantir une sécurité proactive des applications tout au long du cycle de développement. Les configurations de sécurité sont gérées dans l'AWS Management Console, les examens de sécurité sont effectués dans l'application Web Security Agent, et la correction automatique du code et des résultats de sécurité s'effectue directement sur des plateformes de référentiel de code telles que GitHub.

Présentation de

AWS Security Agent se compose de trois composants principaux :

- AWS Management Console : configurez les espaces d'agent, définissez les exigences de sécurité, configurez les tests de pénétration, connectez les référentiels de code et gérez l'accès des utilisateurs
- Application Web Security Agent : effectuez des révisions de conception, créez et exécutez des modèles de menaces, exécutez des tests de pénétration, créez et exécutez des révisions de code et passez en revue les résultats de sécurité dans les espaces d'agent qui vous sont assignés
- Intégration au référentiel de code : recevez des révisions de code automatisées sur les pull requests et les pull requests de correction des tests d'intrusion. Actuellement, AWS Security Agent prend en charge la connexion à GitHub.

Vous travaillez avec AWS Security Agent dans l'un des trois rôles suivants, que vous pouvez identifier en fonction de l'interface que vous utilisez :

Role	Où travaillez-vous et ce que vous faites
Administrateur	Fonctionne dans la console de gestion AWS : configure les espaces d'agent, définit les exigences de sécurité, configure les fonctionnalités et gère l'accès des utilisateurs.
Utilisateur	Fonctionne dans l'application Web Security Agent : exécute des révisions de conception, des modèles de menaces, des tests de pénétration et des révisions de code, puis examine les résultats obtenus.
Développeur	Fonctionne dans un IDE GitHub ou un IDE (tel que Kiro ou Claude Code) : reçoit des résultats de sécurité automatisés sur les pull requests et exécute des analyses de code sans quitter l'environnement de développement.

Nous utilisons ces noms de rôles partout pour indiquer qui exécute chaque tâche. Une même personne peut occuper plusieurs rôles.

Configuration de la console

Les administrateurs configurent AWS Security Agent via l'AWS Management Console.

Espaces d'agent : lorsque vous créez votre premier espace d'agent dans l'AWS Management Console, AWS Security Agent crée l'application Web pour votre compte. Chaque espace agent que vous créez représente une application ou un projet distinct que vous souhaitez sécuriser. Dans l'application Web, les utilisateurs sélectionnent l'espace agent dans lequel ils souhaitent travailler lors des évaluations de sécurité.

Exigences de sécurité : définissez les exigences de sécurité qu'AWS Security Agent évalue lors de la conception et de la révision du code, organisées dans des packs d'exigences de sécurité. Activez des AWS-managed packs basés sur les normes du secteur, créez des packs personnalisés pour les politiques de votre entreprise ou générez des exigences en téléchargeant votre documentation de sécurité. Les exigences s'appliquent à tous les espaces d'agent.

Configuration des tests d'intrusion : configurez les fonctionnalités des tests d'intrusion pour chaque espace d'agent en :

- Vérification des domaines cibles pour les tests par le biais de la vérification DNS ou HTTP
- Configuration de l'accès VPC pour tester des applications privées
- Configuration de la CloudWatch journalisation pour les tests d'intrusion
- Configuration des fonctions AWS Secrets Manager ou Lambda pour les informations d'identification de test
- Spécification de compartiments S3 pour un contexte d'application supplémentaire

Configuration de la révision du code : configurez les fonctionnalités de révision du code pour chaque espace agent en :

- Connexion de GitHub référentiels ou de compartiments S3 contenant du code source
- Sélection des paramètres de révision du code (vulnérabilités de sécurité, exigences personnalisées, ou les deux)
- Activation des commentaires par pull request pour un examen automatique des modifications de code dans GitHub
- Configuration de la CloudWatch journalisation pour les exécutions de révision du code

Configuration de la modélisation des menaces : configurez les fonctionnalités de modélisation des menaces pour chaque espace agent en :

- Connexion de référentiels de code source ou de compartiments S3 contenant du code source
- Ajout de documents de portée (documents de conception de fonctionnalités) pour concentrer l'analyse sur une fonctionnalité spécifique
- Configuration de la CloudWatch journalisation pour les exécutions de modèles de menace
- Configuration d'un rôle de service pour l'accès aux ressources AWS

Intégrations - Connectez des GitHub référentiels à chaque agent Space pour activer les fonctionnalités clés :

- Fournir un contexte applicatif pour des tests de pénétration plus précis
- Activez la révision du code pour les analyses complètes du référentiel et l'analyse des pull requests
- Activez la correction automatique du code par le biais de pull requests pour la révision du code et les résultats des tests d'intrusion

Accès utilisateur : gérez la manière dont les utilisateurs accèdent à l'application Web Security Agent. Si vous avez activé IAM Identity Center (SSO), attribuez des utilisateurs dans la console AWS Security Agent pour fournir un accès SSO direct à l'application Web. Si vous utilisez l' IAM-only accès, les utilisateurs ayant accès à la console AWS peuvent lancer l'application Web via le lien d'accès administrateur dans la console pour n'importe quel espace d'agent.

Activités liées aux applications Web

Les utilisateurs accèdent à l'application Web Security Agent pour effectuer des évaluations de sécurité dans les espaces d'agent qui leur sont assignés.

Sélectionnez l'espace agent : lorsqu'ils se connectent à l'application Web, les utilisateurs sélectionnent l'espace agent dans lequel ils souhaitent travailler. Les utilisateurs peuvent uniquement voir et accéder aux espaces d'agent auxquels ils ont été affectés.

Révisions de conception - Téléchargez les documents de conception et les spécifications d'architecture à des fins d'analyse par rapport aux exigences de sécurité de l'organisation. Passez en revue les résultats avec des conseils de remédiation.

Modèles de menace - Créez et exécutez des modèles de menace en fournissant du code source, des documents de conception technique (documents de portée), ou les deux. Les documents Scope définissent sur quoi l'agent concentre son analyse ; le code source fournit le contexte de votre système existant. Chaque exécution produit une vue d'ensemble du système décrivant l'architecture, les limites de confiance, les flux de données et le niveau de sécurité de votre application, ainsi qu'un ensemble de menaces classées par catégorie STRIDE avec des niveaux de gravité et des recommandations exploitables.

Révisions de code : créez et exécutez des révisions de code qui effectuent une analyse statique complète de l'ensemble de votre code source. Sélectionnez GitHub des référentiels ou des sources S3, configurez les paramètres de scan et passez en revue les résultats de sécurité détaillés avec des conseils de correction. AWS Security Agent identifie les failles de sécurité et valide la conformité aux exigences de sécurité personnalisées de votre organisation sur l'ensemble de votre base de code.

Tests de pénétration : configurez et exécutez des tests de pénétration en fournissant des URL cibles, des informations d'authentification et de la documentation. AWS Security Agent effectue des tests autonomes pour découvrir les vulnérabilités exploitables grâce à des scénarios d'attaque en plusieurs étapes.

Résultats de l'examen : examinez les résultats de sécurité détaillés issus des revues de conception, des modèles de menaces, des révisions du code et des tests de pénétration, y compris les analyses d'impact, les chemins d'attaque reproductibles et les conseils de correction.

Valider les correctifs : évaluations Re-run de sécurité après la mise en œuvre des correctifs pour vérifier que les vulnérabilités ont été corrigées.

GitHub intégration

AWS Security Agent s'intègre directement à AWS GitHub pour fournir des informations de sécurité automatisées dans les flux de travail des développeurs.

Commentaires sur les demandes d'extraction : une fois que les administrateurs ont installé GitHub l'application AWS Security Agent et activé la révision du code avec des commentaires de révision de code pour un espace d'agent, AWS Security Agent analyse automatiquement les demandes d'extraction dans les référentiels connectés. Les développeurs reçoivent des résultats de sécurité et des conseils de correction directement dans les commentaires des pull requests, validant les modifications de code par rapport aux exigences de sécurité de l'organisation et aux vulnérabilités courantes.

Correction automatique : lorsque les utilisateurs activent la correction automatique du code pour une révision de code, AWS Security Agent génère des correctifs pour les vulnérabilités identifiées et envoie des pull requests aux référentiels associés GitHub .

Correction des tests d'intrusion : lorsque les administrateurs activent la recherche de mesures correctives dans la console, les utilisateurs peuvent demander une correction automatique des résultats des tests d'intrusion depuis l'application Web. AWS Security Agent ouvre une pull request vers le GitHub référentiel associé avec des correctifs de code pour corriger la vulnérabilité.

Comprendre la hiérarchie et le cycle de vie des ressources

AWS Security Agent organise les ressources de test de sécurité dans une structure hiérarchique qui détermine ce qui est partagé au sein de votre organisation et ce qui est délimité par application. La compréhension de cette structure vous permet de configurer AWS Security Agent de manière efficace et de savoir où trouver et gérer les différentes ressources.

Ce qui est partagé au sein de votre organisation

Certaines ressources d'AWS Security Agent sont configurées une seule fois au niveau de l'organisation et s'appliquent à toutes vos applications et à tous vos espaces d'agent. Ces ressources au niveau du locataire assurent la cohérence et réduisent les tâches de configuration dupliquées.

Ressource	Description	Pourquoi c'est partagé
Exigences en matière de sécurité	Normes de sécurité organisationnelles qui définissent ce que l'agent de sécurité AWS valide lors de la conception et de la révision du code	Vos politiques de sécurité s'appliquent à toutes les applications. Définissez-les une seule fois et AWS Security Agent les applique partout.
GitHub intégrations	GitHub Organisations enregistrées ou comptes d'utilisateurs autorisés à se connecter à AWS Security Agent	Enregistrez votre GitHub organisation une seule fois, puis connectez des référentiels spécifiques à n'importe quel espace agent selon vos besoins.
Configurations du centre d'identité IAM	Paramètres SSO qui contrôlent la manière dont les utilisateurs accèdent à AWS Security Agent	La gestion centralisée des identités s'applique à tous les agents Spaces de votre organisation.

> **Important**
>
> Les modifications apportées aux exigences de sécurité concernent toutes les futures révisions de conception et de code dans tous les Agent Spaces. Les avis existants ne sont pas affectés.

Ce qui est défini par agent Space

Chaque espace agent représente une application ou un projet distinct que vous souhaitez sécuriser. Les ressources au niveau de l'espace agent sont limitées à cette application spécifique, ce qui permet aux différentes équipes de travailler indépendamment avec leurs propres configurations et évaluations.

Ressource	Description	Pourquoi le champ d'application est-il limité par application
Configurations des tests de pénétration	Testez les configurations pour des fonctionnalités, des points de terminaison d'API ou des fonctionn alités spécifiques au sein de votre application	Chaque application possède des cibles, des méthodes d'authent ification et des limites de portée uniques qui lui sont propres.
Revues de design	Évaluations individuelles de la sécurité architecturale des documents de conception	Chaque application possède sa propre architecture et ses propres documents de conception qui sont évalués indépendamment.
Modèles de menaces	Évaluations de modélisation des menaces qui fournissent une vue d'ensemble du système et identifient les menaces à partir du code source, des documents de conception, ou des deux	Chaque application possède son propre code et son propre design, et les menaces sont modélisées indépendamment. Les modèles de menace sont des configura tions réutilisables que vous pouvez réexécuter au fur et à mesure de l'évolution de votre code et de votre conception.
Intégrations	Fournisseurs de sources et de documentation (GitHub GitLab,, Bitbucket, GitHub Enterprise Server et Confluence) connectés à cet agent Space	Les différentes applications s'appuien t sur des sources et des documenta tions différentes. En les connectan t au niveau de l'espace agent, les limites des applications restent claires.
Paramètres de révision du code	Configuration des fonctionnalités de révision du code, y compris les sources connectées, les paramètre s de numérisation et l'activation des commentaires PR	Chaque application possède ses propres référentiels et ses besoins en matière de révision de sécurité sont configurés indépendamment.

Ressource	Description	Pourquoi le champ d'application est-il limité par application
Paramètres de correction des tests d'intrusion	Configuration des référentiels connectés pouvant recevoir des demandes de correction automatisées pour les résultats des tests d'intrusion	Les équipes contrôlent les endroits où AWS Security Agent peut soumettre des modifications de code en fonction du flux de travail de leur application.
Attributions d'utilisateurs	Utilisateurs ayant accès à cet espace d'agent spécifique	Les équipes ne voient que les évaluations de sécurité pour les applications dont elles sont responsables, ce qui permet d'organiser et de cibler le travail.

> **Tip**
>
> Nous vous recommandons de créer un espace agent par application ou projet afin de maintenir des limites claires entre les équipes et d'organiser efficacement les évaluations de sécurité.

Comment les GitHub référentiels s'insèrent dans la hiérarchie

GitHub les référentiels sont intégrés par le biais d'un processus en plusieurs étapes qui connecte les ressources de l'organisation à des applications spécifiques :

1. Inscrivez-vous au niveau du locataire : autorisez une seule fois GitHub l'application AWS Security Agent pour votre GitHub organisation ou votre compte utilisateur
2. Connexion au niveau de l'espace agent : sélectionnez des référentiels spécifiques pour vous connecter à chaque espace agent
3. Configurer l'utilisation par référentiel - Activez des fonctionnalités spécifiques pour chaque référentiel connecté :
   - Révision du code : analyse complète du code source et analyse automatique des pull requests
   - Contexte des tests d'intrusion - Compréhension de l'application à partir du code source lors des tests d'intrusion

- Correction automatique du code : requêtes d'extraction automatisées avec correctifs de vulnérabilité pour la révision du code et les résultats des tests d'intrusion

Un référentiel unique peut être connecté à plusieurs espaces d'agent avec différentes fonctionnalités activées dans chacun d'eux.

Principales différences entre les capacités de sécurité

Chaque fonctionnalité de sécurité d'AWS Security Agent suit un modèle de flux de travail différent en fonction de la façon dont les équipes de sécurité l'utilisent.

Tests de pénétration : configurations réutilisables avec exécutions indépendantes

Les tests d'intrusion utilisent un modèle de configuration et d'exécution qui prend en charge les tests de sécurité itératifs :

- Créez une fois, exécutez plusieurs fois : définissez une configuration pour une cible spécifique (point de terminaison d'API, zone de fonctionnalités) avec les limites du champ d'application, l'authentification et les paramètres de test
- Exécutions indépendantes : exécutez plusieurs fois la même configuration pour améliorer la sécurité. Chaque exécution est indépendante et génère de nouvelles découvertes

Ce modèle prend en charge la validation continue de la sécurité au fur et à mesure que vous développez et déployez des améliorations.

Revues de conception : One-off évaluations avec clonage

Les révisions de conception sont des évaluations indépendantes qui ne suivent pas un modèle de configuration réutilisable :

- Évaluation unique : chaque revue de conception analyse les documents téléchargés une seule fois par rapport aux exigences de sécurité de votre organisation
- Impossible de réexécuter : les révisions de conception ne sont pas réutilisables. Vous ne pouvez pas réexécuter le même avis
- Cloner pour les mises à jour : clonez une révision de conception existante pour créer une nouvelle révision avec les documents originaux préchargés, ce qui vous permet de mettre à jour les documents et d'exécuter une nouvelle analyse

Ce modèle prend en charge les évaluations ponctuelles de la sécurité architecturale.

Révisions du code : configurations réutilisables avec analyses à la demande et analyse automatique des relations publiques

Les révisions de code proposent deux modes de fonctionnement pour sécuriser votre code source :

- Révisions complètes du code (application Web) : créez des configurations de révision de code qui sélectionnent GitHub des référentiels ou des sources S3, puis exécutez des analyses complètes à la demande. Chaque exécution effectue une analyse statique de l'ensemble de votre code source et génère des résultats accompagnés de conseils de correction. Vous pouvez réexécuter la même configuration de révision de code au fur et à mesure que votre code évolue.
- Pull request comments (GitHub) - Activez l'analyse automatique pour les GitHub référentiels connectés. AWS Security Agent examine automatiquement les pull requests lorsqu'elles sont marquées comme étant prêtes à être examinées et publie les résultats de sécurité sous forme de commentaires directement dans les commentaires GitHub.

Les deux modes utilisent les paramètres de révision du code que vous avez configurés (vulnérabilités de sécurité, exigences personnalisées, ou les deux) et prennent en charge la correction automatique du code par le biais de pull requests.

Modèles de menace : configurations réutilisables avec exécutions à la demande

Les modèles de menace utilisent un modèle de configuration et d'exécution qui prend en charge l'évaluation itérative de votre architecture :

- Créez une fois, exécutez plusieurs fois : définissez un modèle de menace en sélectionnant le code source comme source, en téléchargeant des documents de conception sous forme de documents de portée, ou les deux. Exécutez-le à la demande et réexécutez-le au fur et à mesure de l'évolution de votre code et de votre conception.
- Entrées flexibles : exécutez un modèle de menace uniquement sur le code source, sur les documents de conception uniquement, ou sur les deux. Les documents Scope définissent sur quoi l'agent concentre son analyse ; le code source fournit le contexte de votre système existant.
- Vue d'ensemble du système et menaces : chaque exécution produit une vue d'ensemble du système décrivant l'architecture, les limites de confiance, les flux de données et le niveau de sécurité de votre application, ainsi qu'un ensemble de menaces classées par catégorie STRIDE avec leur gravité, des preuves et des recommandations exploitables.

Comprendre les relations entre les ressources

La hiérarchie détermine l'endroit où vous configurez et accédez aux différentes ressources :

Dans la console de gestion AWS :

- Configuration des ressources au niveau du locataire (exigences de sécurité, GitHub intégrations, IAM Identity Center)
- Création et gestion d'espaces d'agents
- Configuration des paramètres de l'espace agent (référentiels connectés, activation de la révision du code, correction des tests d'intrusion)

Dans l'application Web Security Agent :

- Créez et gérez des configurations de tests d'intrusion et des exécutions de tests
- Création et gestion de révisions de conception
- Créez, gérez et exécutez des révisions de code par rapport à des référentiels connectés et à des sources S3
- Créez, gérez et exécutez des modèles de menaces par rapport au code source, aux documents de portée, ou aux deux
- Consultez les résultats des tests d'intrusion, des révisions de code, des révisions de conception et des modèles de menace

Dans GitHub :

- Afficher les résultats de l'examen du code de pull request sous forme de commentaires
- Recevez des pull requests de correction automatisés pour la révision du code et les résultats des tests d'intrusion (lorsque cette option est activée dans l'espace des agents)

> **Note**
>
> Les résultats de la révision du code Pull Request apparaissent dans GitHub. Les résultats complets de l'examen du code, des tests d'intrusion et de la révision de la conception apparaissent dans l'application Web Security Agent.

Prise en main

Inscrivez-vous, trouvez le bon point de départ pour atteindre votre objectif et lancez votre première évaluation avec un démarrage rapide.

Inscrivez-vous pour un AWS compte

Pour commencer AWS, vous avez besoin d'un AWS compte. Pour plus d'informations sur la création d'un AWS compte, voir Commencer à utiliser un AWS compte dans le Guide de référence sur la gestion des AWS comptes.

Choisissez votre voie

Trouvez le bon point de départ pour ce que vous souhaitez faire avec AWS Security Agent. Utilisez le tableau ci-dessous pour associer votre objectif à une tâche, puis accédez directement à cette page. Si vous utilisez AWS Security Agent pour la première fois, lisez d'the section called “Qu'est-ce qu'AWS Security Agent ?”abord pour une présentation rapide.

Je veux...	Qui	Commencez ici
Découvrez ce que fait AWS Security Agent avant de le configurer	Tout le monde	the section called “Qu'est-ce qu'AWS Security Agent ?”
Configuration du service et création d'un espace d'agent	Admin	the section called “Configuration de l'agent de sécurité AWS”
Tester mon application en ligne ou déployée pour détecter les vulnérabilités exploitables	Utilisateur	the section called “Démarrage rapide : exécutez un test de pénétration”
Scannez mon code source pour détecter les vulnérabilités et les violations des politiques	Utilisateur	the section called “Démarrage rapide : Exécuter une révision du code”
Modéliser la façon dont mon application pourrait être attaquée (STRIDE)	Utilisateur	the section called “Démarrage rapide : exécuter un modèle de menace”

Je veux...	Qui	Commencez ici
Obtenez des informations sur la sécurité d'un design avant que j'écrive du code	Utilisateur	the section called “Création d'une revue de conception”
Scannez le code sans quitter mon IDE (Kiro ou Claude Code)	Developer	the section called “Exécutez des analyses de sécurité du code à partir de votre IDE”
Scannez uniquement mes lignes modifiées avant de les fusionner	Developer	the section called “Exécuter un scan de code différentiel avec S3”
Obtenez des commentaires de sécurité automatiques sur les pull requests et les demandes de fusion	Admin	the section called “Activer la révision du code”
Passez en revue les résultats et décidez de ce qu'il faut corriger en premier	Utilisateur	Test de pénétration, revue du code, modèle de menace, revue de conception

> **Note**
>
> AWS Security Agent utilise trois rôles, que vous pouvez identifier en fonction de l'interface dans laquelle vous travaillez : l'administrateur travaille dans l'AWS Management Console (installation et configuration), l'utilisateur travaille dans l'application Web (exécution des évaluations et examen des résultats) et le développeur travaille dans GitHub un IDE tel que Kiro ou Claude Code. Une même personne peut occuper plusieurs rôles. Pour les définitions complètes, voirthe section called “Comment fonctionne l'agent de sécurité AWS”.

Démarrage rapide : exécutez un test de pénétration

Ce guide de démarrage rapide vous explique comment exécuter votre premier test d'intrusion (pentest) avec AWS Security Agent. Un test d'intrusion teste votre application déployée par rapport à un domaine cible vérifié et fournit des résultats de sécurité, chacun assorti d'une note de gravité et de

preuves à l'appui. Il couvre une application accessible au public ; pour en tester une hébergée dans un VPC privé, voir. the section called "Activer le test de pénétration"

> **Note**
>
> Vous devez accéder à la console de gestion AWS pour configurer AWS Security Agent et définir la portée du test, ainsi que l'accès à l'application Web pour créer et exécuter des tests d'intrusion.

Conditions préalables

Avant de commencer, assurez-vous d'avoir :

- Accès à la console de gestion AWS avec les autorisations nécessaires pour configurer AWS Security Agent.
- Domaine cible actif hébergeant l'application que vous souhaitez tester.
- Possibilité d'ajouter un enregistrement DNS pour ce domaine ou une zone hébergée Route 53 dans le même compte AWS, afin que vous puissiez en vérifier la propriété.
- (Facultatif) Un référentiel de code source (GitHub, GitLab, ou Bitbucket) pour votre application, afin de donner plus de contexte à l'agent.

Étape 1 : configurer l'agent de sécurité AWS dans la console AWS

Si vous n'avez pas encore configuré AWS Security Agent, effectuez la configuration initiale :

1. Accédez à AWS Security Agent dans l'AWS Management Console.
2. Sélectionnez Configurer l'agent de sécurité AWS.
3. Créez un espace d'agent. Un espace agent peut être utilisé par plusieurs utilisateurs et doit être spécifique à chaque application que vous souhaitez tester. Entrez un nom et une description. Le nom doit identifier l'application que vous souhaitez tester d'intrusion.
4. Sélectionnez IAM-only l'accès sous Configuration de l'accès utilisateur.
   - Ce guide de démarrage rapide ne couvre pas l'activation de l'authentification unique (SSO) avec IAM Identity Center, qui permet aux utilisateurs d'accéder à l'application Web directement depuis la console AWS.

- Pour permettre aux utilisateurs n'ayant pas accès à l'AWS Management Console de démarrer des tests d'intrusion, activez l'intégration IAM Identity Center. Pour en savoir plus, consultez the section called "Autoriser les utilisateurs à accéder à l'application Web AWS Security Agent".

5. Choisissez Configurer l'agent de sécurité AWS.

> **Note**
>
> Lorsque vous choisissez Configurer, AWS Security Agent crée votre espace d'agent et établit une application Web dans laquelle les utilisateurs peuvent exécuter des tests de pénétration, des révisions de code, des modèles de menaces et des révisions de conception.

Étape 2 : Activez les tests de pénétration et vérifiez votre domaine

> **Note**
>
> Dans la console AWS, vous définissez l'étendue de ce qui peut être testé. Les utilisateurs exécutent ensuite des tests de pénétration spécifiques dans ce cadre à partir de l'application Web.

1. Dans la barre latérale gauche, sélectionnez Agent Spaces, puis sélectionnez l'Agent Space que vous avez créé à l'étape 1.
2. Sélectionnez l'onglet Test de pénétration, puis sélectionnez Configurer le test de pénétration pour ouvrir l'assistant.
3. Configurer le domaine : entrez le domaine cible que vous souhaitez tester et sélectionnez une méthode de vérification, un enregistrement TXT DNS ou une route HTTP. Le domaine doit être actif et héberger l'application que vous souhaitez tester. Choisissez Suivant.
4. Vérifier les domaines : vérifiez la propriété de chaque domaine dans le tableau des domaines cibles. AWS Security Agent exécute des tests uniquement sur des domaines vérifiés. Pour connaître les étapes détaillées et les valeurs exactes à copier, consultezthe section called "Activer un domaine d'application pour les tests de pénétration".
   - Route 53 domaines dans le même compte AWS : sélectionnez le domaine et choisissez la One-click vérification. L'agent de sécurité AWS crée l'enregistrement DNS et effectue la vérification pour vous.

- Enregistrement DNS TXT (autres fournisseurs DNS) : dans le tableau des domaines cibles, copiez le nom de l'enregistrement et la valeur de l'enregistrement, ajoutez-les sous forme d'enregistrement TXT auprès de votre fournisseur DNS, puis sélectionnez le domaine et choisissez Vérifier. Les modifications du DNS peuvent prendre du temps à se propager, de sorte que la vérification risque de ne pas être terminée immédiatement.
- Route HTTP : créez un fichier `.well-known/aws/securityagent-domain-verification.json` sur votre serveur Web, ajoutez le jeton de vérification au format`{"tokens": ["<token>"]}`, puis sélectionnez le domaine et choisissez Vérifier.

5. (Facultatif) Configurez des fonctionnalités supplémentaires : ajoutez des ressources facultatives telles que des groupes de CloudWatch journaux et des informations d'identification. La section Accès aux services est préconfigurée : AWS Security Agent crée un rôle de service avec les autorisations requises, sauf si vous choisissez un rôle IAM existant.

Étape 3 : Connecter le code source (facultatif)

La connexion à un fournisseur de code source fournit à AWS Security Agent le contexte de votre application et améliore la couverture des tests d'intrusion. Cette étape est facultative.

1. Dans l'onglet Test de pénétration, choisissez Ajouter sur la bannière Connecter un fournisseur de code source pour les tests de pénétration en haut de la page.
2. Enregistrez et connectez votre fournisseur, puis sélectionnez les référentiels à mettre à disposition pour les tests d'intrusion.

Pour le flux d'intégration complet, consultez Connect AWS Security Agent aux GitHub référentiels ou la rubrique Connect de votre fournisseur.

Étape 4 : Création et exécution d'un test de pénétration

> **Note**
>
> Vous créez et exécutez des tests de pénétration dans l'application Web AWS Security Agent. Nous vous recommandons d'effectuer des tests dans un environnement de test qui reflète étroitement la production.

1. Lancez l'application Web : sélectionnez l'onglet Application Web, puis Accès administrateur.

2. Dans la barre latérale gauche, choisissez Tests de pénétration, puis Créer un test de pénétration.
3. Détails du test d'intrusion - Configurez l'étendue du test et la source du journal :
   a. Entrez un nom Pentest.
   b. Sous URL cibles, sélectionnez ou entrez un domaine vérifié à tester (par exemple,`https://example.com`). Seuls les domaines vérifiés peuvent être testés, et les sous-domaines sont couverts automatiquement.
   c. (Facultatif) Sous URL accessibles, ajoutez des domaines que l'agent doit atteindre pour se connecter et naviguer mais ne doit pas attaquer, tels que des fournisseurs d'identité, des CDN ou des API en dehors de votre domaine cible. AWS Security Agent peut accéder à ces domaines mais ne les teste pas ; seuls vos domaines cibles sont attaqués.
   d. Passez en revue les règles de configuration réseau pour vérifier quels points de terminaison peuvent et ne peuvent pas recevoir du trafic pendant le test.
   e. Sous Autorisations, sélectionnez un rôle de service et, éventuellement, un groupe de CloudWatch journaux. Choisissez Suivant.
4. Ressources VPC (facultatif) - Configurez un VPC si votre cible se trouve sur un réseau privé non accessible au public. Consultez the section called “Activer le test de pénétration”.
5. (Facultatif) Ressources d'authentification - Fournissez des informations d'identification afin que l'agent puisse accéder à des chemins authentifiés et non publics. Nous vous recommandons de les ajouter afin d'élargir la couverture et de détecter les vulnérabilités liées à une connexion.
6. (Facultatif) Configuration supplémentaire : ajoutez un contexte d'application tel que des fichiers, GitHub des référentiels ou des sources S3 pour améliorer la qualité de la recherche. Vous pouvez également activer la correction automatique du code et définir d'autres options d'exécution ici.
7. Choisissez Créer et exécuter pour démarrer le test maintenant, ou Créer un pentest pour l'enregistrer et l'exécuter ultérieurement.

Étape 5 : Examiner les résultats des tests de pénétration

1. Un test de pénétration peut prendre plusieurs heures. La plupart sont achevés dans un délai de 16 heures, selon la taille et la complexité de votre demande.
2. L'exécution commence par une phase de pré-vol qui valide la configuration avant le début des tests : elle configure l'infrastructure de journalisation, vérifie que vos points de terminaison cibles sont accessibles et prépare l'environnement de test. Si une vérification avant le vol échoue (par exemple, un domaine cible ne peut pas être résolu), l'exécution s'arrête avant le début des tests.

Ouvrez l'onglet Preflight pour voir quelle vérification a échoué, la résoudre et recommencer une nouvelle exécution.

3. Une fois l'exécution terminée, ouvrez-la et consultez les onglets Vue d'ensemble de l'exécution, Journaux et Résultats.
4. Dans l'onglet Constatations, sélectionnez une constatation pour en afficher la description, la gravité, le type de risque et les preuves à l'appui.

Pour de plus amples informations, veuillez consulter the section called "Créez un test de pénétration" et the section called "Examiner les résultats d'un test de pénétration".

Démarrage rapide : Exécuter une révision du code

Ce guide de démarrage rapide vous explique comment effectuer votre première révision de code avec AWS Security Agent. AWS Security Agent analyse vos référentiels de code source à la recherche de failles de sécurité et de conformité aux exigences de sécurité de votre organisation.

> **Note**
>
> Vous devez accéder à la console de gestion AWS pour configurer AWS Security Agent et accéder à l'application Web pour créer et exécuter des révisions de code.

Conditions préalables

Avant de commencer, assurez-vous d'avoir :

- Accès à la console de gestion AWS avec les autorisations nécessaires pour configurer AWS Security Agent.
- Un référentiel de code source (GitHub GitLab,, ou Bitbucket) ou une source Amazon S3 contenant le code que vous souhaitez consulter.

Étape 1 : configurer l'agent de sécurité AWS dans la console AWS

Si vous n'avez pas encore configuré AWS Security Agent, effectuez la configuration initiale :

1. Accédez à AWS Security Agent dans l'AWS Management Console.

2. Sélectionnez Configurer l'agent de sécurité AWS.
3. Créez un espace d'agent. Un espace agent peut être utilisé par plusieurs utilisateurs et doit être spécifique à chaque application que vous souhaitez tester. Entrez le nom et la description de votre premier espace d'agent. Ce nom apparaît aux utilisateurs dans l'application Web. Le nom doit identifier l'application dont vous souhaitez vérifier le code.
4. Sélectionnez IAM-only l'accès sous Configuration de l'accès utilisateur.
   - Ce guide de démarrage rapide ne couvre pas l'activation de l'authentification unique (SSO) avec IAM Identity Center. Cela permet aux utilisateurs d'accéder directement à l'application Web AWS Security Agent depuis la console AWS.
   - Pour permettre aux utilisateurs n'ayant pas accès à l'AWS Management Console d'exécuter des révisions de code, activez l'intégration IAM Identity Center. Pour en savoir plus, consultez the section called “Autoriser les utilisateurs à accéder à l'application Web AWS Security Agent”.
5. Choisissez Configurer l'agent de sécurité AWS.

> **Note**
>
> Lorsque vous choisissez Configurer, AWS Security Agent crée votre espace d'agent et établit une application Web dans laquelle les utilisateurs peuvent exécuter des tests d'intrusion, des révisions de code, des modèles de menaces et des révisions de conception.

Étape 2 : activer et configurer la révision du code

> **Note**
>
> Si GitHub des référentiels ou des compartiments S3 sont déjà connectés à votre espace agent (par exemple, par le biais de la configuration de tests d'intrusion), la révision du code est déjà activée. Vous pouvez ignorer cette étape et accéder directement à l'application Web.

Ouvrez l'assistant de configuration de la révision du code

1. Dans la barre latérale gauche, sélectionnez Agent Spaces, puis sélectionnez votre Agent Space.
2. Sélectionnez Activer la révision du code dans l'en-tête ou dans l'onglet Révision du code.

Connect les intégrations, les référentiels et les buckets

1. (Si vous n'avez pas encore d' GitHub intégration) Créez une GitHub inscription. Si vous en avez déjà un, passez à l'étape suivante.
   a. Dans la section Intégrations connectées, choisissez Ajouter, puis Créer un nouvel enregistrement.
   b. Sélectionnez GitHubet choisissez Next.
   c. Choisissez Installer et autoriser, puis terminez l'installation dans GitHub :
      i. Sélectionnez l' GitHub utilisateur ou l'organisation propriétaire du référentiel que vous souhaitez consulter.
      ii. Sélectionnez Tous les référentiels ou Sélectionnez uniquement les référentiels.
      iii. Choisissez Installer et autoriser et terminez GitHub l'authentification.
   d. De retour dans la console de gestion AWS, entrez un nom d'enregistrement et vérifiez que le type de compte correspond à l'endroit où vous avez installé l' GitHub application.
   e. Choisissez Connect pour enregistrer l'enregistrement.

   Pour le flux GitHub d'intégration complet, consultez Connect AWS Security Agent aux GitHub référentiels.
2. Connectez les GitHub référentiels. Dans la section Intégrations connectées, choisissez Ajouter, puis sélectionnez votre GitHub enregistrement. L' GitHubassistant Connect en deux étapes s'ouvre :
   a. Sur les GitHub référentiels Connect, sélectionnez les référentiels à inclure et choisissez Next.
   b. Dans Gérer les fonctionnalités, activez les options suivantes par référentiel :
      - Commentaires relatifs à la révision du code : laissez l'agent de sécurité AWS publier les résultats de sécurité sous forme de commentaires sur les pull requests dans le référentiel.
      - Correction automatique : permettez aux utilisateurs de l'application Web AWS Security Agent de demander des pull requests qui corrigent les résultats.
   c. Choisissez Enregistrer pour revenir à l'assistant de configuration.
3. (Facultatif) Connectez les sources S3. Dans la section compartiments S3, choisissez Ajouter une ressource S3 et entrez l'URI S3 d'un compartiment contenant du code source, ou choisissez Browse pour en choisir un.
4. Sélectionnez les paramètres de révision de votre code. Par défaut, Security requirements and vulnerability findings, analyse le code pour vérifier sa conformité aux exigences de sécurité que vous avez activées et les vulnérabilités courantes.

5. Choisissez Suivant.

Configurations facultatives

1. Configurez les groupes de CloudWatch journaux facultatifs et l'accès aux services. Le rôle de service par défaut est préconfiguré avec les autorisations requises.
2. Choisissez Enregistrer.

Étape 3 : créer et exécuter une révision de code

> **Note**
>
> Vous créez et exécutez des révisions de code uniquement dans l'application Web AWS Security Agent.

1. Sélectionnez l'onglet Application Web, puis Accès administrateur pour lancer l'application Web AWS Security Agent.
2. Dans la barre latérale gauche, choisissez Code reviews.
3. Choisissez Créer une révision de code.
4. Configurez la révision du code :
   a. Entrez un titre identifiant l'étendue de cet examen (par exemple, « billing-service-security-review »).
   b. Sous Sources, sélectionnez les GitHub référentiels que vous avez connectés à votre espace agent à l'étape 2, ou entrez les sources S3 que vous souhaitez analyser.
   c. Sélectionnez le rôle de service parmi les rôles que vous avez configurés.
   d. (Facultatif) Sélectionnez Activer la correction automatique du code pour qu'AWS Security Agent envoie automatiquement des pull requests contenant des correctifs pour tous les résultats.
5. Choisissez Créer une révision de code.
6. Sur la page détaillée de la révision du code, choisissez Commencer la révision.

Étape 4 : Examiner les résultats de la révision du code

1. La révision du code prend généralement de 30 à 60 minutes, selon la taille de votre base de code.

2. L'exécution commence par une phase de pré-vol qui valide la configuration avant le début de l'analyse : elle confirme qu'AWS Security Agent peut extraire votre code source de votre référentiel ou de votre source S3 et configure l'environnement d'analyse. Si une vérification avant vol échoue (par exemple, si elle ne peut pas accéder à votre source), l'exécution s'arrête avant l'analyse statique. Ouvrez l'onglet Preflight pour voir quelle vérification a échoué, la résoudre et recommencer une nouvelle exécution.
3. Une fois terminé, accédez à l'exécution terminée et sélectionnez l'onglet Résultats.
4. Passez en revue les résultats dans la vue détaillée de la liste :
   a. Sélectionnez un résultat dans le panneau de gauche pour en afficher les détails.
   b. Consultez les sections Description, Emplacement du code, Preuves et Correctifs suggérés.
   c. Utilisez le code de correction pour générer une pull request avec un correctif, ou passez en revue les PR de correction automatique si vous avez activé cette option.

Pour de plus amples informations, veuillez consulter the section called “Création d'une révision de code” et the section called “Examiner les résultats d'une révision de code”.

Démarrage rapide : exécuter un modèle de menace

Ce guide de démarrage rapide vous explique comment exécuter votre premier modèle de menace avec AWS Security Agent. Un modèle de menace analyse l'architecture de votre application et produit une vue d'ensemble du système (comment AWS Security Agent comprend votre système) et un ensemble de menaces (la manière dont il pourrait être attaqué, chacune avec un niveau de gravité, une classification STRIDE et des recommandations). Vous pouvez exécuter un modèle de menace sur les documents de conception (documents de portée) pour définir l'objectif, le code source (sources) pour fournir le contexte de votre système existant, ou les deux.

> **Note**
>
> Vous devez accéder à la console de gestion AWS pour configurer AWS Security Agent et accéder à l'application Web pour créer et exécuter des modèles de menace.

Étape 1 : configurer l'agent de sécurité AWS dans la console AWS

Si vous n'avez pas encore configuré AWS Security Agent, effectuez la configuration initiale :

1. Accédez à AWS Security Agent dans l'AWS Management Console.
2. Sélectionnez Configurer l'agent de sécurité AWS.
3. Créez un espace d'agent. Un espace d'agent peut être utilisé par plusieurs utilisateurs et doit être spécifique à chaque application que vous souhaitez sécuriser. Entrez le nom et la description de votre premier espace d'agent. Le nom doit identifier l'application que vous souhaitez modéliser comme menace.
4. Sélectionnez IAM-only l'accès sous Configuration de l'accès utilisateur.
   - Ce guide de démarrage rapide ne couvre pas l'activation de l'authentification unique (SSO) avec IAM Identity Center. Cela permet aux utilisateurs d'accéder directement à l'application Web AWS Security Agent depuis la console AWS.
   - Si vous souhaitez permettre aux utilisateurs n'ayant pas accès à l'AWS Management Console d'effectuer des tâches telles que le démarrage d'un modèle de menace, vous devez activer l'intégration IAM Identity Center.
5. Choisissez Configurer l'agent de sécurité AWS.

> **Note**
>
> Lorsque vous choisissez Configurer, AWS Security Agent crée votre espace d'agent et établit une application Web dans laquelle les utilisateurs peuvent exécuter des tests de pénétration, des révisions de code, des modèles de menaces et des révisions de conception.

Étape 2 : Connecter le code source

> **Note**
>
> Si des référentiels ou des compartiments S3 sont déjà connectés à votre espace agent (par exemple, par le biais de la révision du code ou de la configuration de tests d'intrusion), vous pouvez ignorer cette étape et accéder directement à l'application Web. Vous pouvez toujours exécuter un modèle de menace sur les documents de scope téléchargés sans connecter de code source.

Connectez des référentiels ou des compartiments S3 contenant le code source que vous souhaitez que l'agent utilise comme contexte pour comprendre votre système existant :

1. Dans la barre latérale gauche, sélectionnez Agent Spaces, puis sélectionnez votre Agent Space.
2. Accédez à la section Intégrations pour connecter votre fournisseur de code source.
3. Vous pouvez également connecter des compartiments S3 contenant votre code source.

Pour le flux d'intégration complet, consultez Connect AWS Security Agent aux GitHub référentiels.

Étape 3 : créer et exécuter un modèle de menace

> **Note**
>
> Vous créez et exécutez des modèles de menace dans l'application Web AWS Security Agent.

1. Lancez l'application Web depuis l'onglet Application Web de l'AWS Management Console. Sinon, si vous avez configuré IAM Identity Center, connectez-vous directement.
2. Dans la barre latérale gauche, choisissez Threat models.
3. Choisissez Créer un modèle de menace.
4. Configurez le modèle de menace :
   a. Entrez un titre identifiant l'étendue de ce modèle de menace (par exemple, « billing-service » ou « checkout-api »).
   b. Fournissez au moins une entrée :
      - Sous Scope docs, téléchargez des documents de conception (DOC, DOCX, JPEG, MD, PDF, PNG ou TXT), entrez des URI S3 ou sélectionnez des pages Confluence.
      - Sous Sources, sélectionnez des référentiels parmi vos intégrations connectées ou saisissez des URI S3 contenant du code source.

      > **Tip**
      >
      > Fournissez à la fois des sources et des documents de portée pour étendre le modèle de menace à une conception spécifique (par exemple, un document de conception des fonctionnalités) tout en fournissant à l'agent votre code source comme contexte pour comprendre votre système existant.

   c. Sélectionnez le rôle de service parmi les rôles que vous avez configurés.
   d. (Facultatif) Sélectionnez un groupe de CloudWatch journaux pour les journaux.

5. Choisissez Créer un modèle de menace.
6. Sur la page détaillée du modèle de menace, choisissez Démarrer l'exécution.

Étape 4 : Examiner les menaces

1. L'exécution progresse au fil de ses tâches d'analyse. Vous pouvez suivre la progression dans l'onglet Preflight et consulter les détails des tâches dans l'onglet Logs.
2. Une fois l'exécution terminée, le statut d'exécution passe à Terminé.
3. Sélectionnez l'onglet Vue d'ensemble pour consulter la vue d'ensemble du système et la distribution de gravité.
4. Sélectionnez l'onglet Menaces pour passer en revue les menaces identifiées :
   a. Sélectionnez une menace dans la liste pour en afficher les détails dans le panneau latéral.
   b. Passez en revue les champs Déclaration, Gravité, Catégories STRIDE, Recommandation, Preuve et autres.
   c. Mettez à jour le statut de la menace sur Résolu ou Rejeté au fur et à mesure que vous traitez ou triez chaque menace.

Pour de plus amples informations, veuillez consulter the section called “Création d'un modèle de menace” et the section called “Analyser les menaces à partir d'un modèle de menace”.

Pour les administrateurs (console)

En tant qu'administrateur, vous configurez AWS Security Agent dans l'AWS Management Console et configurez les espaces d'agent auxquels les utilisateurs accèdent via l'application Web AWS Security Agent. Chaque espace d'agent représente un environnement distinct avec des autorisations et des ressources spécifiques.

Nous vous recommandons de créer un espace agent unique pour chaque application que vous souhaitez tester. Par exemple, si vous avez deux projets internes (une application de facturation et une application de suivi des tâches), vous devez créer deux espaces d'agent distincts.

Exemple de configuration

Imaginons qu'un administrateur configure un espace agent pour évaluer la sécurité d'une application de facturation interne. L'administrateur doit :

- Vérifiez le domaine (par exemple`beta.billing.example.com`)
- Connectez-vous GitHub et activez la révision du code
- Configurez l'accès au réseau en attribuant un VPC, un sous-réseau et un groupe de sécurité appropriés pour les tests de pénétration

Lorsque les utilisateurs lancent un test d'intrusion ou une révision de conception, ils peuvent choisir parmi ces ressources préconfigurées, en respectant les garde-fous que vous avez définis tout en conservant la flexibilité nécessaire pour répondre à leurs besoins d'évaluation spécifiques.

Configuration et création d'espaces d'agents

Configurez AWS Security Agent pour votre organisation et créez les espaces d'agent qui définissent les ressources et les évaluations de chaque application.

Configuration de l'agent de sécurité AWS

Configurez AWS Security Agent pour votre organisation en créant votre premier espace d'agent et en définissant le mode d'accès des utilisateurs à l'application Web.

Cette configuration initiale permet aux administrateurs de configurer les fonctionnalités de sécurité dans la console AWS et permet aux utilisateurs d'accéder à la révision de la conception et aux tests

de pénétration via l'application Web Security Agent. Après cette configuration unique, vous pouvez créer des espaces d'agent supplémentaires grâce à un processus simplifié.

Présentation de

Comprendre les espaces réservés aux agents

Un espace d'agent est un espace de travail dédié à la sécurisation d'une application ou d'un projet spécifique. Il contient tous les examens de sécurité, les GitHub référentiels éventuellement connectés, les configurations des tests d'intrusion, les résultats et les conclusions relatifs à cette application.

Les espaces d'agent vous aident à organiser le travail de sécurité en séparant les évaluations de sécurité de chaque application, ce qui permet aux équipes de se concentrer sur leur application spécifique. Nous vous recommandons de créer un espace agent par application ou projet afin de maintenir des limites claires.

Les exigences de sécurité sont définies au niveau de l'organisation et s'appliquent à tous les espaces d'agents, chaque espace d'agent gérant ses propres documents de conception, référentiels de code, configurations de tests d'intrusion, résultats de tests de pénétration et résultats de sécurité.

Ce qui est inclus dans un espace d'agents

Chaque espace d'agent contient :

- GitHub Référentiels éventuellement connectés associés à l'application ou au projet
- Révisions de conception précédentes de l'application
- Configurations et limites des tests d'intrusion spécifiques à l'application
- Résultats des tests de pénétration et résultats de sécurité

Ce que vous allez configurer lors de l'installation

Lors de cette première configuration, vous prendrez des décisions organisationnelles qui s'appliquent à tous les agents Spaces :

- Méthode d'accès : choisissez le mode d'accès des utilisateurs à l'application Web Security Agent (IAM Identity Center SSO ou IAM-only accès via la console AWS)
- Autorisations : configurez le rôle IAM utilisé par l'application Web pour accéder aux services AWS
- Premier espace d'agent - Créez votre espace d'agent initial avec un nom et une description

> **Note**
>
> Une fois cette configuration terminée, la création d'espaces d'agent supplémentaires est plus simple : il suffit de fournir un nom et une description. Consultez the section called "Création d'un espace d'agent" pour plus de détails sur la création des espaces d'agent suivants.

Conditions préalables

Avant de commencer, assurez-vous de disposer des éléments suivants :

- Autorisations pour créer et gérer les ressources d'AWS Security Agent
- Compréhension des exigences de gestion des identités de votre organisation
- (Facultatif) Compte AWS autorisé à créer des rôles IAM et à configurer IAM Identity Center (si vous utilisez un accès SSO)
- (Facultatif) Rôle IAM existant si vous souhaitez utiliser une configuration d'autorisations personnalisée

Étape 1 : Créez votre premier espace d'agent

Définissez les propriétés de base de votre premier espace agent qui sera affiché aux utilisateurs dans l'application Web.

1. Sur la page de la console AWS Security Agent, sélectionnez Configurer l'agent de sécurité.
2. Dans le champ Nom de l'espace agent, entrez le nom de votre espace agent.

   > **Note**
   >
   > Le nom de l'espace agent est affiché aux utilisateurs dans l'application Web et permet d'identifier l'application ou le projet que cet espace représente.

3. (Facultatif) Dans le champ Description, fournissez une description qui aide à distinguer l'objectif de l'espace agent.

   > **Tip**
   >
   > La description permet de distinguer l'objectif de l'espace agent. Nous vous recommandons de décrire l'application ou le projet spécifique que cet espace d'agent sécurisera,

par exemple « application Web du portail client », « microservices de traitement des paiements » ou « plateforme d'analyse interne ».

Étape 2 : Choisissez votre méthode d'accès

Sélectionnez le mode d'accès des utilisateurs à l'application Web Security Agent. Vous avez le choix entre activer l'accès SSO via IAM Identity Center ou fournir un accès via la console AWS.

> **Note**
>
> Si vous choisissez IAM-only l'accès et que vous souhaitez utiliser ultérieurement IAM Identity Center, vous devrez supprimer la configuration de votre agent de sécurité AWS et recommencer le processus de configuration.

1. Dans la section Méthode d'accès, sélectionnez l'une des options suivantes :
   - IAM Identity Center (SSO) - Activez l'accès SSO pour votre équipe via IAM Identity Center. Cette option est recommandée pour les équipes qui ont besoin d'une gestion centralisée des utilisateurs et qui souhaitent que les utilisateurs accèdent directement à l'application Web sans passer par la console AWS.
   - IAM-only accès - Fournissez un accès via un lien d'accès administrateur dans la console AWS. Cette option est plus simple à configurer et convient aux équipes qui préfèrent un accès par console ou qui n'ont pas besoin de fonctionnalités d'authentification unique.
2. Si vous avez sélectionné IAM Identity Center (SSO), passez à l'étape 2a ci-dessous.
3. Si vous avez sélectionné IAM-only l'accès, passez à l'étape 3.

Étape 2a : Configuration du centre d'identité IAM (accès SSO uniquement)

Effectuez ces étapes uniquement si vous avez sélectionné IAM Identity Center (SSO) comme méthode d'accès.

1. Dans la section Connect to IAM Identity Center, passez en revue la région AWS.

> **Important**
>
> Votre application doit être configurée dans la même région que celle dans laquelle vous activez IAM Identity Center. La région affichée est l'endroit où votre espace d'agent sera créé. Le centre d'identité IAM doit être activé dans la même région que celle où vous créez votre espace d'agent.

2. Dans la section IAM Identity Center, sélectionnez l'une des options suivantes :
   - Choisissez Créer une instance de compte pour créer une nouvelle instance de compte IAM Identity Center
   - Si une instance d'organisation existe déjà dans la même région, AWS Security Agent s'y connecte automatiquement

   > **Note**
   >
   > Une fois qu'AWS Security Agent est connecté à IAM Identity Center, vous pouvez gérer l'accès en affectant des utilisateurs à l'application dans IAM Identity Center.

3. Si vous vous connectez à Active Directory ou à un fournisseur d'identité externe, consultez l'alerte d'information.

> **Important**
>
> Si vous gérez déjà des utilisateurs dans Active Directory ou dans une autre source d'identité et que vous prévoyez de connecter cette source d'identité à IAM Identity Center, annulez la configuration et accédez d'abord à la console IAM Identity Center. Choisissez la source d'identité à laquelle vous souhaitez vous connecter avant de configurer AWS Security Agent. La modification ultérieure des sources d'identité peut entraîner la suppression des assignations utilisateur existantes.

Étape 3 : Configuration des autorisations (facultatif)

Configurez le rôle IAM que votre application Web Security Agent utilise pour accéder aux services, aux API et aux comptes AWS.

1. Localisez la section Configuration des autorisations - facultative.

2. Si la section est réduite, choisissez la section Configuration des autorisations pour la développer.
3. Sélectionnez l'une des options suivantes :
   - Créer un rôle par défaut : AWS Security Agent crée automatiquement un nouveau rôle IAM avec les autorisations nécessaires pour l'application Web
   - Utiliser un autre rôle : sélectionnez un rôle IAM existant parmi les options disponibles
4. Consultez la description du rôle :

> **Note**
>
> Un rôle IAM par défaut sera créé pour que votre application Web accède à d'autres services, API et comptes AWS. Le rôle bénéficiera des autorisations requises pour les opérations d'évaluation de la sécurité.

Étape 4 : terminer la configuration

Après avoir configuré tous les paramètres requis, terminez la configuration pour créer votre premier espace d'agent et établir l'application Web Security Agent.

1. Passez en revue toutes les sections de configuration pour vous assurer de leur exactitude.
2. Choisissez Set up (Configurer).
3. AWS Security Agent crée votre espace d'agent, établit l'application Web et configure les ressources AWS nécessaires.

> **Note**
>
> Après la configuration initiale, vous aurez la possibilité de configurer les fonctionnalités, notamment les limites des tests d'intrusion, les exigences de sécurité et GitHub l'intégration.

Étapes suivantes

Après avoir configuré AWS Security Agent :

- Définissez les exigences de sécurité pour votre organisation

- Configurez les fonctionnalités de test d'intrusion, y compris la vérification de domaine et l'accès VPC pour votre espace d'agent
- Connectez GitHub les référentiels pour la révision du code et le contexte des tests de pénétration
- (Si vous utilisez IAM Identity Center) Affectez des utilisateurs à l'espace agent dans la console AWS Security Agent
- (Si vous utilisez l' IAM-only accès) Lancez l'application Web via le lien d'accès administrateur dans la console AWS
- Créez des espaces d'agent supplémentaires pour d'autres applications (voirthe section called "Création d'un espace d'agent")

Création d'un espace d'agent

Créez des espaces d'agents pour sécuriser les applications ou les projets de votre organisation. Chaque espace d'agent fournit un espace de travail pour les évaluations de sécurité, les résultats et les configurations spécifiques à cette application ou à ce projet et est accessible à plusieurs utilisateurs.

Cette procédure suppose que vous avez déjà terminé la configuration initiale d'AWS Security Agent. Si vous n'avez pas encore configuré AWS Security Agent, consultezthe section called "Configuration de l'agent de sécurité AWS".

Présentation de

Comprendre les espaces réservés aux agents

Un espace d'agent est un espace de travail dédié à la sécurisation d'une application ou d'un projet spécifique. Il contient tous les examens de sécurité, les référentiels de code éventuellement connectés, les configurations des tests d'intrusion, les résultats et les conclusions relatifs à cette application.

Les espaces d'agent vous aident à organiser le travail de sécurité en séparant les évaluations de sécurité de chaque application, ce qui permet aux équipes de se concentrer sur leur application spécifique. Nous vous recommandons de créer un espace agent par application ou projet afin de maintenir des limites claires.

Pour une explication complète des espaces d'agents et de leur intégration dans la structure de sécurité de votre organisation, consultezthe section called "Comprendre la hiérarchie et le cycle de vie des ressources".

Ce qui est inclus dans un espace d'agents

Chaque espace d'agent contient :

- Référentiels de code éventuellement connectés associés à l'application ou au projet
- Révisions de conception antérieures pour l'application ou le projet
- Configurations et limites des tests d'intrusion spécifiques à l'application
- Résultats des tests de pénétration et résultats de sécurité

Création d'un espace d'agent

Créez un nouvel espace d'agent pour une application ou un projet que vous souhaitez sécuriser.

1. Dans la console AWS Security Agent, accédez à la page Agent Spaces.
2. Choisissez Create Agent Space.
3. Dans le champ Nom de l'espace agent, entrez le nom de votre espace agent.

> **Note**
>
> Le nom de l'espace agent est affiché aux utilisateurs dans l'application Web et permet d'identifier l'application ou le projet que cet espace représente.

4. (Facultatif) Dans le champ Description, fournissez une description qui aide à distinguer l'objectif de l'espace agent.

> **Tip**
>
> La description permet de distinguer l'objectif de l'espace agent. Nous vous recommandons de décrire l'application ou le projet spécifique que cet espace d'agent sécurisera, par exemple « application Web du portail client », « microservices de traitement des paiements » ou « plateforme d'analyse interne ».

5. Choisissez Créer.

> **Note**
>
> AWS Security Agent créera votre espace d'agent. Vous pouvez désormais configurer les fonctionnalités et connecter les ressources spécifiques à cette application.

Étapes suivantes

Après avoir créé votre espace d'agent :

- Connectez les référentiels de code source (GitHub, GitLab, Bitbucket ou GitHub Enterprise Server) pour la révision du code et le contexte des tests de pénétration
- Connect Confluence pour le contexte de la documentation lors des révisions de conception et des tests d'intrusion
- Activer la fonctionnalité de révision du code pour les référentiels connectés (voirthe section called "Activer la révision du code de pull request pour les GitHub référentiels")
- Configurer les fonctionnalités de test d'intrusion, y compris la vérification de domaine
- (Si vous utilisez IAM Identity Center) Affectez des utilisateurs à cet espace agent dans la section Web App de la page Agent Space. (voirthe section called "Autoriser les utilisateurs à accéder à l'application Web AWS Security Agent")
- (En cas d'utilisation de l' IAM-only accès) Les utilisateurs disposant d'un accès à la console peuvent lancer l'application Web via le lien d'accès administrateur de cet espace agent

Intégrations Connect

Connectez et gérez les fournisseurs de code source (GitHub, GitLab, Bitbucket et GitHub Enterprise Server) et les fournisseurs de documentation (Confluence), ainsi que la connectivité au réseau privé, que vos agents Spaces utilisent pour la révision du code, les tests de pénétration et la modélisation des menaces.

Comment fonctionnent les intégrations avec Agent Spaces

AWS Security Agent se connecte à des fournisseurs de code source et de documentation tiers afin qu'il puisse analyser votre code et votre documentation lors des évaluations de sécurité. Avant de connecter un fournisseur spécifique, il est utile de comprendre le lien entre les intégrations et les espaces et fonctionnalités des agents.

Enregistrez-vous une fois, réutilisez-le partout

La connexion d'un fournisseur à AWS Security Agent implique deux étapes distinctes qui se déroulent à différents niveaux :

1. Enregistrez l'intégration (au niveau du compte). Vous enregistrez un fournisseur une seule fois depuis la page Intégrations de la console de gestion des agents de sécurité AWS. Un enregistrement représente la connexion autorisée à un compte fournisseur, tel qu'une GitHub organisation, un GitLab groupe, un espace de travail Bitbucket ou un site Confluence. Les inscriptions sont des ressources au niveau du compte.
2. Connectez des ressources à un espace agent (niveau Agent Space). Depuis un espace agent, vous connectez les ressources d'une intégration enregistrée (référentiels pour les fournisseurs de code source ou pages pour Confluence) et configurez la manière dont l'agent les utilise. Cette étape est spécifique à chaque espace d'agent.

Une seule inscription est réutilisée dans chaque espace agent de votre compte. Si vous avez enregistré un fournisseur lors de la configuration d'un agent space, ce même enregistrement est disponible lorsque vous connectez des ressources à un autre agent space. Vous n'enregistrez pas à nouveau le même fournisseur.

Une connexion unique, partagée entre les différentes fonctionnalités

Lorsque vous connectez une ressource à un espace d'agent, cette ressource est partagée entre toutes les fonctionnalités de l'agent. Vous ne connectez pas un référentiel séparément pour chaque fonctionnalité.

- L'accès en lecture est accordé en connectant la ressource. La connexion d'un référentiel permet à AWS Security Agent de le lire pour des analyses complètes du code (révision du code), le contexte des tests d'intrusion, la modélisation des menaces et la révision de la conception. La connexion d'une page Confluence permet à l'agent de la lire pour accéder au contexte de la documentation lors des révisions de conception, de la modélisation des menaces et des tests de pénétration.
- Les actions d'écriture sont facultatives, par référentiel. Lorsque vous connectez des référentiels de code source à un espace agent, vous pouvez également activer des actions d'écriture pour chaque référentiel :
  - Commentaires relatifs à la révision du code : l'agent de sécurité AWS publie les résultats de la révision sous forme de commentaires sur les pull requests (ou les demandes de fusion GitLab).

- Correction du code : AWS Security Agent ouvre des pull requests (ou des demandes de fusion) contenant des correctifs pour les vulnérabilités découvertes.

  Ces actions d'écriture ne sont pas disponibles pour les référentiels publics. Read-only l'analyse s'applique toujours.

> **Note**
>
> Confluence est un fournisseur de documentation plutôt qu'un fournisseur de code source. AWS Security Agent lit les pages Confluence connectées afin de fournir un contexte pour les révisions de conception, la modélisation des menaces et les tests de pénétration. La sélection d'une page autorise l'accès en lecture ; aucune fonctionnalité par page n'est activée.

Fournisseurs pris en charge

AWS Security Agent prend en charge les fournisseurs suivants :

- Code source : GitHub (GitHub entreprise hébergée dans le cloud GitHub et hébergée dans le cloud), GitHub Enterprise Server (auto-hébergé), GitLab (hébergé dans le cloud), GitLab Self-Managed (auto-hébergé) et Bitbucket Cloud.
- Documentation - Confluence Cloud.

Pour les fournisseurs auto-hébergés qui ne sont pas accessibles via l'Internet public, vous pouvez acheminer le trafic de l'agent via une connexion privée. Pour de plus amples informations, veuillez consulter the section called “Connectez-vous au contrôle de source hébergé en privé”.

Étapes suivantes

- Enregistrez un fournisseur depuis la page Intégrations. Consultez la rubrique relative à la connexion de votre fournisseur, telle quethe section called “Connect AWS Security Agent aux GitHub référentiels”.
- Connectez les ressources à un espace agent et configurez les fonctionnalités. Consultez the section called “Activer la révision du code” et the section called “Activer le test de pénétration”.

Connect AWS Security Agent aux GitHub référentiels

Connectez votre agent de sécurité AWS à GitHub des référentiels pour activer la révision du code, la modélisation des menaces, les tests de pénétration et les fonctionnalités de correction automatisées. AWS Security Agent prend en charge à la fois les entreprises hébergées dans le cloud GitHub et les entreprises hébergées dans le cloud GitHub . Avant de commencer, examinez the section called "Comment fonctionnent les intégrations avec Agent Spaces" comment un enregistrement est réutilisé dans Agent Spaces et partagé entre les fonctionnalités.

GitHub l'intégration répond à de multiples objectifs :

> **Note**
>
> Cette page couvre les entreprises hébergées dans le cloud GitHub (github.com) et les entreprises hébergées dans le cloud. GitHub Pour un serveur GitHub d'entreprise auto-hébergé, voirthe section called "Connect AWS Security Agent au serveur GitHub d'entreprise".

- Révision du code : analysez automatiquement les modifications de code dans chaque pull request par rapport aux exigences de sécurité de votre organisation, et exécutez des analyses complètes du référentiel à la demande
- Modélisation des menaces : améliorez la compréhension des applications en analysant le code source, les flux de données et l'architecture
- Contexte des tests de pénétration - Fournir une compréhension des applications pour les tests de pénétration en analysant le code source
- Correction automatisée : envoyez des pull requests contenant des correctifs pour les vulnérabilités découvertes lors des évaluations de sécurité

GitHub Pour vous connecter à AWS Security Agent, vous devez autoriser l' GitHub application AWS Security Agent pour votre GitHub organisation ou votre compte utilisateur, puis enregistrer la connexion dans la console AWS.

Comment fonctionne GitHub l'intégration

L'analyse des pull requests s'effectue au sein de GitHub. Une fois que vous avez autorisé l' GitHub application, connecté des référentiels et activé les commentaires de révision du code dans l'AWS Management Console, AWS Security Agent analyse automatiquement les modifications apportées

à chaque nouvelle pull request (analyse différentielle du code modifié uniquement) et publie les résultats sous forme de commentaires de pull request.

Vous créez et exécutez des révisions de code complètes, qui analysent la base de code complète d'un référentiel, dans l'application Web AWS Security Agent, et non dans GitHub.

Les tests de pénétration et la modélisation des menaces sont lancés dans l'application Web AWS Security Agent. Les utilisateurs sélectionnent les référentiels connectés pour fournir le contexte de l'application et spécifient les domaines cibles pour les tests de pénétration. Si vous activez la correction automatique, les utilisateurs peuvent demander à AWS Security Agent de corriger les résultats en ouvrant des pull requests vers des référentiels connectés.

Conditions préalables

Avant de commencer, assurez-vous de disposer des éléments suivants :

- GitHub accès administrateur de l'organisation ou accès du propriétaire du compte GitHub utilisateur
- Autorisations pour configurer les intégrations pour votre espace d'agent dans l'AWS Management Console
- Compréhension des référentiels auxquels vous souhaitez vous connecter pour la révision du code, la modélisation des menaces et les tests de pénétration

> **Important**
>
> Une GitHub application ne peut être installée qu'une seule fois sur un GitHub compte ou une GitHub organisation. Si vous devez connecter la même GitHub organisation à AWS Security Agent, vous devez utiliser le compte AWS sur lequel l'intégration a été enregistrée pour la première fois.

> **Note**
>
> Si l'organisation de votre GitHub entreprise a activé la liste d'adresses IP autorisées, vous devez accepter les adresses IP autorisées dans l' GitHub application. Vous pouvez également choisir d'ajouter automatiquement les adresses IP à votre liste d'autorisations. Pour plus d'informations, consultez les sections Autoriser l'accès par GitHub les applications et Activation des adresses IP autorisées dans la GitHub documentation.

Les adresses IP suivantes sont utilisées pour accéder à vos GitHub ressources :

- USA Est (Virginie du Nord) (us-east-1)
  - 34.228.181.128
  - 44.219.176.187
  - 54.226.244.221
- USA Ouest (Oregon) (us-west-2)
  - 34.212.16.133
  - 52.89.67.212
  - 54.187.135.61
- Asie-Pacifique (Mumbai) (ap-south-1)
  - 13.126.209.199
  - 13.234.6.24
  - 35.154.102.216
- Asie-Pacifique (Singapour) (ap-southeast-1)
  - 18.139.13.125
  - 47.130.240.215
  - 54.179.238.173
- Asie-Pacifique (Sydney) (ap-southeast-2)
  - 13.237.95.197
  - 13.238.84.102
  - 52.64.174.242
- Asie-Pacifique (Tokyo) (ap-northeast-1)
  - 13.192.12.233
  - 35.74.181.230
  - 57.183.50.158
- Europe (Francfort) (eu-central-1)
  - 18.158.110.140
  - 52.57.96.160
  - 52.59.55.56
- Europe (Irlande) (eu-west-1)

    - 34.251.85.24
    - 52.30.157.157
    - 52.51.192.222
  - Amérique du Sud (São Paulo) (sa-east-1)
    - 54.94.247.213
    - 54.207.222.14
    - 54.232.201.242

Autoriser et enregistrer l' GitHub application AWS Security Agent

Autorisez l' GitHub application AWS Security Agent à accéder à votre GitHub organisation ou à votre compte utilisateur, puis enregistrez la connexion dans la console AWS.

> **Important**
>
> Effectuez toutes les étapes de ce processus sans fermer votre navigateur ni quitter le navigateur. Si le processus d'enregistrement est interrompu, vous devrez peut-être désinstaller l' GitHub application et recommencer.

1. Dans la console de gestion des agents de sécurité AWS, accédez à Intégrations.
2. Choisissez Ajouter une intégration.
3. Sélectionnez GitHub.
4. Choisissez Suivant.
5. Choisissez Installer et autoriser.

   Vous êtes redirigé GitHub vers pour terminer l'autorisation. Assurez-vous d'être connecté GitHub avec un compte doté d'un accès administrateur à l'organisation ou au compte utilisateur que vous souhaitez connecter.
6. Dans GitHub, sélectionnez le compte ou l'organisation sur lequel vous souhaitez installer l' GitHub application AWS Security Agent.
7. Sélectionnez les référentiels auxquels AWS Security Agent peut accéder :
   - Tous les référentiels : accordez l'accès à tous les référentiels actuels et futurs de l'organisation ou du compte utilisateur

- Sélectionnez uniquement les référentiels : choisissez des référentiels spécifiques dans la liste déroulante. Vous pouvez sélectionner plusieurs référentiels un par un.

> **Note**
>
> Vous pouvez modifier l'accès au référentiel à tout moment en accédant aux paramètres de l' GitHub application dans votre GitHub organisation ou dans les paramètres du compte utilisateur.

8. Choisissez Installer et autoriser.
9. Vous êtes redirigé vers la console de gestion AWS pour terminer l'enregistrement.
10. Dans la section Détails de l'enregistrement, configurez les champs suivants :
    a. Nom d'enregistrement : entrez un nom descriptif pour cette GitHub connexion. Utilisez un nom qui identifie l' GitHub organisation ou le compte utilisateur, tel que « Acme-Corp-Org » ou « Production-Repos ».
    b. Type de compte : sélectionnez l'une des options suivantes dans le menu déroulant :
        - Organisation : si vous avez connecté un compte d' GitHub organisation
        - Utilisateur - Si vous avez connecté un compte GitHub utilisateur personnel
    c. Nom de l'organisation (apparaît uniquement si vous avez sélectionné Organisation) - Entrez le nom exact de votre GitHub organisation tel qu'il apparaît dans GitHub.
11. Choisissez Se connecter.
12. Un message de confirmation s'affiche et vous revenez à la page Intégrations, où votre nouvelle GitHub connexion apparaît avec son nom d'enregistrement. Pour connecter d'autres GitHub organisations ou comptes d'utilisateurs, répétez cette procédure en sélectionnant à nouveau Ajouter une intégration.

Résoudre les problèmes d'intégration GitHub

Si vous rencontrez des problèmes au cours du processus GitHub d'intégration, suivez les instructions suivantes pour résoudre les problèmes courants.

Impossible de terminer l'enregistrement

Si vous n'avez pas pu terminer le processus d'enregistrement (par exemple, si votre navigateur a été fermé, si vous avez quitté la page d'inscription ou si vous avez rencontré une interruption de session),

l' GitHub application AWS Security Agent peut être installée dans votre GitHub organisation mais pas enregistrée dans la console AWS.

Symptômes :

- Lorsque vous essayez à nouveau d'autoriser l' GitHub application, le message « Configurer » s' GitHub affiche au lieu de « Installer »
- Vous ne pouvez pas terminer l'enregistrement dans la console AWS
- L'intégration n'apparaît pas dans votre liste d'intégrations

Résolution :

1. Désinstallez l' GitHub application AWS Security Agent de votre GitHub organisation ou de votre compte utilisateur.
2. Retournez à la console AWS Security Agent et recommencez le processus d'intégration depuis le début.

Plusieurs comptes AWS tentent d'intégrer la même GitHub organisation

Une GitHub application ne peut être installée qu'une seule fois sur un GitHub compte ou une GitHub organisation. Si vous devez utiliser les référentiels d'une GitHub organisation déjà intégrée à un autre compte AWS Security Agent, vous devez utiliser le compte AWS sur lequel l'intégration a été enregistrée pour la première fois.

Résolution :

- Identifiez le compte AWS Security Agent sur lequel l' GitHub intégration est enregistrée
- Utilisez ce compte AWS pour créer des espaces d'agent et connecter des référentiels
- Si vous devez déplacer l'intégration vers un autre compte AWS, désinstallez d'abord l' GitHub application du compte AWS d'origine, puis intégrez-la au nouveau compte

Étapes suivantes

Après la connexion GitHub à AWS Security Agent :

- Accédez à l'espace agent dans lequel vous souhaitez utiliser ces référentiels.

- Choisissez Activer la révision du code ou Configurer les tests de pénétration pour connecter des référentiels spécifiques à votre espace agent et configurer leur utilisation.
- Activez la correction automatique pour permettre à AWS Security Agent de soumettre des pull requests contenant des correctifs de vulnérabilité
- Vérifiez les autorisations des GitHub applications et l'accès au référentiel dans les paramètres de votre GitHub organisation

Supprimer une GitHub intégration

Supprimez une GitHub intégration lorsque vous n'avez plus besoin d'AWS Security Agent pour accéder aux référentiels depuis une GitHub organisation ou un compte utilisateur spécifique. Vous devez d'abord désinstaller l' GitHub application AWS Security Agent GitHub avant de supprimer l'intégration dans la console AWS.

Conditions préalables à la suppression

Avant de supprimer une GitHub intégration, assurez-vous d'avoir :

- J'ai vérifié quels agents Spaces ont des référentiels connectés à partir de cette intégration
- J'ai compris l'impact : la suppression de cette intégration interrompra les connexions aux référentiels pour la révision du code, le contexte des tests d'intrusion et la correction des tests d'intrusion dans tous les espaces d'agent utilisant les référentiels issus de cette intégration
- GitHub accès administrateur de l'organisation ou accès du propriétaire du compte utilisateur pour désinstaller l' GitHub application

Étape 1 : désinstallez l' GitHub application AWS Security Agent de GitHub

Tout d'abord, désinstallez l' GitHub application AWS Security Agent de votre GitHub organisation ou de votre compte utilisateur.

Pour les GitHub Organisations :

1. Accédez à github.com et ouvrez la page de votre organisation.
2. Dans la barre latérale gauche, choisissez Réglages.
3. Sous Code, planification et automatisation, sélectionnez GitHub Applications installées.
4. Recherchez l'application AWS Security Agent dans la liste.

5. Choisissez Configurer à côté de l'application AWS Security Agent.
6. Faites défiler la page de configuration vers le bas et choisissez Désinstaller.
7. Confirmez la désinstallation lorsque vous y êtes invité.

Pour les comptes GitHub d'utilisateurs :

1. Accédez à github.com.
2. Choisissez votre photo de profil.
3. Cliquez sur Paramètres.
4. Dans la barre latérale gauche, sélectionnez Applications.
5. Ouvrez l'onglet GitHub Applications installées.
6. Recherchez l'application AWS Security Agent dans la liste.
7. Choisissez Configurer à côté de l'application AWS Security Agent.
8. Faites défiler la page de configuration vers le bas et choisissez Désinstaller.
9. Confirmez la désinstallation lorsque vous y êtes invité.

Étape 2 : supprimer l'intégration d'AWS Security Agent

Après avoir désinstallé l' GitHub application, supprimez l'enregistrement de l'intégration dans la console AWS.

1. Dans la console de gestion des agents de sécurité AWS, accédez à Intégrations.
2. Localisez l' GitHub intégration que vous souhaitez supprimer dans la liste des intégrations.
3. Sélectionnez l'intégration en cliquant dessus.
4. Cliquez sur Supprimer.
5. Consultez la boîte de dialogue de confirmation, qui vous avertit de l'impact :

> **Warning**
>
> La suppression de cette intégration affectera tous les espaces d'agent auxquels des référentiels sont connectés depuis cette GitHub organisation ou ce compte utilisateur. Cela va casser :
>
> - Fonctionnalité de révision du code pour les référentiels connectés

- Contexte des tests d'intrusion à partir de référentiels connectés
- Fonctionnalités de correction des tests d'intrusion pour les référentiels connectés

Assurez-vous d'avoir désinstallé l' GitHub application AWS Security Agent GitHub avant de continuer.

6. Si vous n'avez pas encore désinstallé l' GitHub application de GitHub, vous recevrez un avertissement. Retournez à l'étape 1 pour terminer d'abord la désinstallation.
7. Si vous avez désinstallé l' GitHub application et que vous en comprenez l'impact, choisissez Confirmer la suppression.
8. L'intégration est supprimée de votre liste d'intégrations. Tous les espaces d'agent dotés de référentiels issus de cette intégration n'ont plus accès à ces référentiels pour la révision du code, le contexte des tests d'intrusion ou la correction automatique.

Connect AWS Security Agent aux GitLab référentiels

Connectez votre agent de sécurité AWS aux référentiels GitLab cloud pour activer la révision du code, la modélisation des menaces, les tests de pénétration et les fonctionnalités de correction automatisées. Avant de commencer, examinez the section called “Comment fonctionnent les intégrations avec Agent Spaces” comment un enregistrement est réutilisé dans Agent Spaces et partagé entre les fonctionnalités.

GitLab l'intégration répond à de multiples objectifs :

- Révision du code : analysez automatiquement les modifications de code dans chaque demande de fusion par rapport aux exigences de sécurité de votre organisation, et exécutez des analyses complètes du référentiel à la demande
- Modélisation des menaces : améliorez la compréhension des applications en analysant le code source, les flux de données et l'architecture
- Contexte des tests de pénétration - Fournir une compréhension des applications pour les tests de pénétration en analysant le code source
- Correction automatique : envoyez des demandes de fusion contenant des correctifs pour les vulnérabilités découvertes lors des évaluations de sécurité

La connexion GitLab à AWS Security Agent nécessite de fournir un jeton d' GitLab accès avec les autorisations appropriées, puis d'enregistrer la connexion dans la console AWS.

Comment fonctionne GitLab l'intégration

L'analyse des demandes de fusion s'effectue dans GitLab. Une fois que vous avez fourni votre jeton d'accès, connecté des projets et activé les commentaires de révision de code dans l'AWS Management Console, AWS Security Agent analyse automatiquement les modifications apportées à chaque nouvelle demande de fusion (analyse différentielle du code modifié uniquement) et publie les résultats sous forme de commentaires de demande de fusion.

Vous créez et exécutez des révisions de code complètes, qui analysent la base de code complète d'un projet, dans l'application Web AWS Security Agent, et non dans GitLab.

Les tests de pénétration et la modélisation des menaces sont lancés dans l'application Web AWS Security Agent. Les utilisateurs spécifient les domaines cibles et sélectionnent les référentiels connectés pour fournir le contexte de l'application. Si vous activez la correction automatique, les utilisateurs peuvent demander à AWS Security Agent de corriger les résultats en ouvrant des demandes de fusion vers des référentiels connectés.

> **Note**
>
> La correction automatique n'est pas disponible pour les GitLab référentiels publics afin d'éviter de révéler les vulnérabilités avant qu'elles ne soient corrigées.

Conditions préalables

Avant de commencer, assurez-vous de disposer des éléments suivants :

- Un GitLab.com compte avec accès du responsable ou du propriétaire aux projets que vous souhaitez connecter
- Un jeton GitLab d'accès avec les étendues requises pour votre type de connexion :
  - Personnel - Un jeton d'accès personnel avec toutes les autorisations de lecture et l'`api`autorisation.
  - Groupe : jeton d'accès au groupe avec les `read_repository` étendues `read_api` et.
- Autorisations pour configurer les intégrations dans la console de gestion des agents de sécurité AWS

Important

Définissez l'expiration du jeton sur un maximum de 365 jours après la date actuelle.

Note

GitLab Les jetons d'accès personnels peuvent être utilisés sur plusieurs comptes AWS. Contrairement GitHub aux intégrations Atlassian, il n'existe aucune restriction quant à la connexion d'un même GitLab compte à plusieurs instances d'AWS Security Agent.

Enregistrer une GitLab connexion

1. Dans la console de gestion des agents de sécurité AWS, accédez à Intégrations.
2. Choisissez Ajouter une intégration.
3. Sélectionnez GitLab, puis choisissez Next.
4. Sous Choisir un type de compte, sélectionnez l'une des options suivantes :
   - Personnel - Connectez votre compte GitLab utilisateur individuel.
   - Groupe : connectez un GitLab groupe contenant plusieurs projets. Entrez votre identifiant de groupe.
5. Dans le champ Jeton d'accès, collez votre jeton GitLab d'accès.
6. Dans le champ Nom d'enregistrement, entrez un nom descriptif pour cette connexion, tel que`Engineering-Team-GitLab`. Les caractères valides sont les lettres, les chiffres, les points, les traits de soulignement et les traits d'union.
7. Choisissez Se connecter.

   Vous revenez à la page Intégrations, où la nouvelle connexion apparaît avec son nom d'enregistrement.

Résoudre les problèmes d'intégration GitLab

Si vous rencontrez des problèmes au cours du processus GitLab d'intégration, suivez les instructions suivantes pour résoudre les problèmes courants.

Jeton non valide ou expiré

Symptômes

- L'intégration ne parvient pas à se connecter
- L'intégration qui fonctionnait auparavant cesse de fonctionner
- Message d'erreur indiquant un échec de l'authentification

Résolution

1. Dans GitLab, accédez à vos paramètres utilisateur et sélectionnez Access Tokens.
2. Vérifiez que votre jeton n'a pas expiré.
3. Vérifiez que le jeton possède les étendues requises pour son type.
4. Si le jeton a expiré, créez-en un nouveau et mettez à jour l'intégration dans la console AWS.

Limitation du débit

Symptômes

- Défaillances intermittentes lors de la révision du code
- Analyse différée des demandes de fusion

Résolution

- GitLab applique des limites de débit aux demandes d'API. Si vous disposez d'un grand nombre de référentiels ou de demandes de fusion fréquentes, certaines demandes peuvent être limitées.
- Attendez que la fenêtre de limite de débit soit réinitialisée ou contactez l' GitLab assistance pour augmenter vos limites de taux.

Étapes suivantes

Après la connexion GitLab à AWS Security Agent :

- Accédez à l'espace agent dans lequel vous souhaitez utiliser ces référentiels.
- Choisissez Activer la révision du code ou Configurer les tests d'intrusion pour connecter des projets spécifiques à votre espace agent et configurer leur utilisation.

- Activez la correction du code pour permettre à AWS Security Agent de soumettre des demandes de fusion contenant des correctifs de vulnérabilité
- Pour les GitLab instances hébergées en privé, voir the section called "Connectez l'agent de sécurité AWS à GitLab Self-Managed"

Connectez l'agent de sécurité AWS à GitLab Self-Managed

Connectez votre agent de sécurité AWS à une GitLab Self-Managed instance pour activer la révision du code, la modélisation des menaces, les tests de pénétration et les fonctionnalités de correction automatisées pour les référentiels hébergés sur votre propre infrastructure.

GitLab Self-Managed l'intégration fonctionne de la même manière que le GitLab Cloud (voirthe section called "Connect AWS Security Agent aux GitLab référentiels") avec une configuration supplémentaire pour la connectivité réseau à votre instance privée. Avant de commencer, examinez the section called "Comment fonctionnent les intégrations avec Agent Spaces" comment un enregistrement est réutilisé dans Agent Spaces et partagé entre les fonctionnalités.

> **Note**
>
> GitLab Self-Managed est enregistré par le biais de l'GitLabintégration, et non d'un type d'intégration distinct. Dans le flux d'enregistrement, sélectionnez Utiliser un point de terminaison GitLab auto-hébergé et fournissez l'URL de votre instance. Le GitLab flux hébergé dans le cloud est décrit dans. the section called "Connect AWS Security Agent aux GitLab référentiels"

Conditions préalables

Avant de commencer, assurez-vous de disposer des éléments suivants :

- Une GitLab Self-Managed instance qui est soit :
  - Accessible au public sur Internet, OU
  - Accessible via une connexion privée (voirthe section called "Connectez-vous au contrôle de source hébergé en privé")
- Un jeton GitLab d'accès avec les étendues requises pour votre type de connexion :
  - Personnel - Un jeton d'accès personnel avec toutes les autorisations de lecture et l'`api`autorisation.

  - Groupe : jeton d'accès au groupe avec les `read_repository` étendues `read_api` et.
- Accès du responsable ou du propriétaire aux projets que vous souhaitez connecter
- Votre GitLab instance doit servir le trafic HTTPS avec une version TLS minimale de 1.2

> **Note**
>
> Si votre GitLab Self-Managed instance utilise des certificats TLS émis par une autorité de certification privée, vous pouvez fournir la clé PEM-encoded publique du certificat lors de la création d'une connexion privée. Cela permet à AWS Security Agent de faire confiance à la connexion TLS à votre instance.

Enregistrer une GitLab Self-Managed connexion

1. Dans la console de gestion des agents de sécurité AWS, accédez à Intégrations.
2. Choisissez Ajouter une intégration.
3. Sélectionnez GitLab, puis choisissez Next.
4. Sous Choisir un type de compte, sélectionnez Personnel ou Groupe. Si vous sélectionnez Groupe, entrez votre ID de groupe.
5. Sélectionnez Utiliser un point de terminaison GitLab auto-hébergé.
6. Dans le champ URL du point de terminaison GitLab auto-hébergé, entrez l'URL de votre instance, par exemple`https://gitlab.example.com`.
7. Si votre instance n'est pas accessible au public, sélectionnez Connect to endpoint using a private connection, puis choisissez une connexion privée existante ou créez-en une nouvelle. Consultez the section called “Connectez-vous au contrôle de source hébergé en privé”.
8. Dans le champ Jeton d'accès, collez votre jeton GitLab d'accès.
9. Dans le champ Nom d'enregistrement, entrez un nom descriptif pour cette connexion. Les caractères valides sont les lettres, les chiffres, les points, les traits de soulignement et les traits d'union.
10. Choisissez Se connecter.

    Vous revenez à la page Intégrations, où la nouvelle connexion apparaît avec son nom d'enregistrement.

Connectivité privée

Si votre GitLab Self-Managed instance n'est pas accessible au public, vous devez créer une connexion privée avant d'enregistrer l'intégration. Consultez the section called "Connectez-vous au contrôle de source hébergé en privé" les instructions détaillées.

> **Important**
>
> Service-managed les connexions privées nécessitent que l' GitLab Self-Managed instance soit exécutée dans le même compte AWS où l'agent Space est créé. Pour un accès entre comptes, utilisez une connexion privée autogérée dans laquelle vous fournissez votre propre configuration de ressources VPC Lattice.

Résoudre les problèmes d'intégration GitLab Self-Managed

Outre les étapes de résolution des problèmes décrites ci-dessousthe section called "Connect AWS Security Agent aux GitLab référentiels", les problèmes suivants sont spécifiques aux instances autogérées :

Instance inaccessible

Symptômes

- Échec de la connexion en raison d'un délai d'attente ou d'une erreur réseau
- L'intégration fonctionnait auparavant mais cesse de fonctionner

Résolution

- Vérifiez que votre GitLab instance est en cours d'exécution et accessible
- Si vous utilisez une connexion privée, vérifiez que la passerelle de ressources VPC Lattice est saine et que les ENI disposent d'une connectivité réseau avec votre instance
- Vérifiez que les groupes de sécurité autorisent le trafic sur le port configuré
- Vérifiez que le certificat TLS est valide et qu'il n'a pas expiré

Erreurs de certificat TLS

Symptômes

- Échec de la connexion avec SSL/TLS erreur

Résolution

- Vérifiez que votre instance utilise le protocole HTTPS avec TLS 1.2 ou supérieur
- Si vous utilisez une autorité de certification privée, assurez-vous que la clé PEM-encoded publique a été fournie lors de la configuration de la connexion privée
- Vérifiez que le certificat n'est pas expiré

Étapes suivantes

Après vous GitLab Self-Managed être connecté à AWS Security Agent :

- Accédez à l'espace agent dans lequel vous souhaitez utiliser ces référentiels
- Choisissez Activer la révision du code ou Configurer les tests de pénétration pour connecter des projets spécifiques
- Activer la correction du code pour les correctifs basés sur les demandes de fusion

Supprimer une GitLab intégration

Supprimez une GitLab intégration lorsque vous n'avez plus besoin d'AWS Security Agent pour accéder aux référentiels depuis un GitLab compte ou un groupe spécifique.

Conditions préalables à la suppression

Avant de supprimer une GitLab intégration, assurez-vous d'avoir :

- J'ai vérifié quels agents Spaces ont des référentiels connectés à partir de cette intégration
- J'ai compris l'impact : la suppression de cette intégration interrompra les connexions aux référentiels pour la révision du code, le contexte des tests d'intrusion, la modélisation des menaces et la correction automatique dans tous les espaces d'agent utilisant les référentiels issus de cette intégration

Supprimer l'intégration d'AWS Security Agent

1. Dans la console de gestion des agents de sécurité AWS, accédez à Intégrations.
2. Localisez l' GitLab intégration que vous souhaitez supprimer.
3. Sélectionnez l'intégration en cliquant dessus.
4. Cliquez sur Supprimer.
5. Consultez la boîte de dialogue de confirmation et choisissez Confirmer la suppression.

> **Note**
>
> Après avoir supprimé l'intégration, vous souhaiterez peut-être également révoquer le jeton d'accès personnel GitLab pour empêcher tout accès ultérieur. Accédez à vos paramètres GitLab utilisateur et supprimez ou révoquez le jeton.

Le même processus s'applique aux GitLab Self-Managed intégrations.

Connect AWS Security Agent au serveur GitHub d'entreprise

Connectez votre agent de sécurité AWS à une instance de serveur GitHub d'entreprise (GHES) pour activer la révision du code, la modélisation des menaces, les tests de pénétration et les fonctionnalités de correction automatisées pour les référentiels hébergés sur votre propre infrastructure.

GitHub L'intégration d'un serveur d'entreprise fournit les mêmes fonctionnalités que l'hébergement dans le cloud GitHub (voir Connect AWS Security Agent aux GitHub référentiels) avec une configuration supplémentaire pour la connectivité réseau à votre instance auto-hébergée. Avant de commencer, examinez the section called “Comment fonctionnent les intégrations avec Agent Spaces” comment un enregistrement est réutilisé dans Agent Spaces et partagé entre les fonctionnalités.

> **Note**
>
> GitHub Enterprise Server est enregistré par le biais de l'GitHubintégration, et non d'un type d'intégration distinct. Dans le flux d'enregistrement, vous choisissez GitHub Enterprise Server comme type d'instance. Le GitHub.com flux hébergé dans le cloud est décrit dans. the section called “Connect AWS Security Agent aux GitHub référentiels”

Comment fonctionne l'intégration des serveurs d' GitHub entreprise

L'analyse des pull requests s'effectue au sein GitHub d'Enterprise Server. Une fois que vous avez autorisé la connexion, connecté des référentiels et activé les commentaires de révision du code dans l'AWS Management Console, AWS Security Agent analyse automatiquement les modifications apportées à chaque nouvelle pull request (analyse différentielle du code modifié uniquement) et publie les résultats sous forme de commentaires de pull request.

Vous créez et exécutez des révisions de code complètes, qui analysent la base de code complète d'un référentiel, dans l'application Web AWS Security Agent, et non dans GitHub Enterprise Server.

Les tests de pénétration et la modélisation des menaces sont lancés dans l'application Web AWS Security Agent. Les utilisateurs spécifient les domaines cibles et sélectionnent les référentiels connectés pour fournir le contexte de l'application. Si vous activez la correction automatique, les utilisateurs peuvent demander à AWS Security Agent de corriger les résultats en ouvrant des pull requests vers des référentiels connectés.

Conditions préalables

Avant de commencer, assurez-vous de disposer des éléments suivants :

- Une instance de serveur GitHub d'entreprise qui est soit :
  - Accessible au public sur Internet, OU
  - Accessible via une connexion privée (voirthe section called “Connectez-vous au contrôle de source hébergé en privé”)
- Accès à l'administrateur du site ou à l'administrateur de l'organisation sur votre instance GHES
- Votre instance GHES doit traiter le trafic HTTPS avec une version TLS minimale de 1.2
- Autorisations pour configurer les intégrations dans la console de gestion des agents de sécurité AWS

> **Note**
>
> GitHub Les intégrations de serveurs d'entreprise peuvent être utilisées sur plusieurs comptes AWS.

Enregistrer une connexion GitHub Enterprise Server

L'enregistrement d'une connexion GitHub Enterprise Server utilise un flux OAuth-based d'autorisation.

> **Important**
>
> Effectuez toutes les étapes de ce processus sans fermer votre navigateur ni quitter le navigateur. Si le processus d'enregistrement est interrompu, vous devrez peut-être recommencer depuis le début.

1. Dans la console de gestion des agents de sécurité AWS, accédez à Intégrations.
2. Choisissez Ajouter une intégration.
3. Sélectionnez GitHub, puis choisissez Next.
4. Sous Type d'instance, sélectionnez GitHub Enterprise Server.
5. Dans le champ URL du serveur d'GitHub entreprise, entrez l'URL HTTPS de votre instance, par exemple`https://github.example.com`.
6. Si votre instance n'est pas accessible au public, sélectionnez Connect to endpoint using a private connection, puis choisissez une connexion privée existante ou créez-en une nouvelle. Consultez the section called “Connectez-vous au contrôle de source hébergé en privé”.
7. Dans la section Détails du registre, configurez les champs suivants :
   a. Nom d'enregistrement : entrez un nom descriptif pour cette connexion. Les caractères valides sont les lettres, les chiffres, les points, les traits de soulignement et les traits d'union.
   b. GitHub type de compte : sélectionnez une organisation ou un utilisateur.
   c. Nom de l'organisation (apparaît uniquement si vous avez sélectionné Organisation) : entrez le nom exact de votre organisation GitHub Enterprise Server. Les noms sont sensibles à la casse.
8. Choisissez Se connecter.

> **Note**
>
> AWS Security Agent vous redirige hors de la console pour terminer l'autorisation avec votre instance de serveur GitHub d'entreprise. Une fois l'autorisation terminée, vous revenez à la console et la nouvelle connexion apparaît sur la page Intégrations.

Connectivité privée

Si votre instance GitHub Enterprise Server n'est pas accessible au public, vous devez créer une connexion privée avant d'enregistrer l'intégration. Consultez the section called “Connectez-vous au contrôle de source hébergé en privé” les instructions détaillées.

> **Important**
>
> Service-managed les connexions privées nécessitent que l'instance GHES soit exécutée dans le même compte AWS où l'agent Space est créé. Pour un accès entre comptes, utilisez une connexion privée autogérée.

> **Note**
>
> Si votre instance GHES utilise des certificats TLS émis par une autorité de certification privée, fournissez la clé PEM-encoded publique du certificat lors de la création de la connexion privée.

Résoudre les problèmes d' GitHub intégration d'Enterprise Server

Si vous rencontrez des problèmes lors de la connexion d'AWS Security Agent à GitHub Enterprise Server, suivez les instructions suivantes pour diagnostiquer et résoudre les problèmes courants.

Échec de redirection OAuth

Symptômes

- Les redirections du navigateur échouent pendant le flux d'autorisation
- Page d'erreur affichée après l'autorisation sur GHES

Résolution

- Vérifiez que votre instance GHES est accessible depuis votre navigateur
- Assurez-vous que l'URL de rappel OAuth est correctement configurée
- Redémarrer le processus d'intégration depuis le début

Instance inaccessible

Symptômes

- Échec de la connexion en raison d'un délai d'attente ou d'une erreur réseau

Résolution

- Vérifiez que votre instance GHES est en cours d'exécution et accessible
- Si vous utilisez une connexion privée, vérifiez la connectivité VPC Lattice
- Vérifiez que les groupes de sécurité autorisent le trafic sur le port configuré
- Vérifiez que le certificat TLS est valide (TLS 1.2 minimum)

Étapes suivantes

Après avoir connecté le serveur d' GitHub entreprise à AWS Security Agent :

- Accédez à l'espace agent dans lequel vous souhaitez utiliser ces référentiels
- Choisissez Activer la révision du code ou Configurer les tests de pénétration pour connecter des référentiels spécifiques
- Activez la correction du code pour permettre à AWS Security Agent de soumettre des pull requests contenant des correctifs de vulnérabilité

Supprimer une intégration de serveur d' GitHub entreprise

Supprimez une intégration de serveur d' GitHub entreprise lorsque vous n'avez plus besoin d'AWS Security Agent pour accéder aux référentiels à partir d'une instance GHES spécifique.

Conditions préalables à la suppression

Avant de supprimer une intégration GHES :

- Vérifiez quels sont les agents Spaces auxquels des référentiels sont connectés à partir de cette intégration
- Comprenez l'impact : la suppression perturbera la révision du code, le contexte des tests d'intrusion, la modélisation des menaces et la correction automatique de tous les référentiels connectés

Supprimer l'intégration

1. Dans la console de gestion des agents de sécurité AWS, accédez à Intégrations.
2. Localisez l'intégration GitHub Enterprise Server que vous souhaitez supprimer.
3. Sélectionnez l'intégration.
4. Cliquez sur Supprimer.
5. Consultez la boîte de dialogue de confirmation et choisissez Confirmer la suppression.

> **Note**
>
> Après la suppression, vous souhaiterez peut-être également révoquer l'application OAuth sur votre instance GHES. Accédez aux paramètres de votre organisation GHES et supprimez l'application autorisée.

Trouvez votre identifiant d'installation Atlassian

Avant d'enregistrer une intégration Bitbucket ou Confluence dans la console AWS, vous devez trouver l'ID d'installation de l'application AWS Security Agent Forge installée sur votre site Atlassian. Vous collez cet identifiant dans le flux d'enregistrement.

Pour Bitbucket

1. Dans Bitbucket, accédez aux paramètres de votre espace de travail.
2. Sélectionnez Forge Apps dans la barre latérale.
3. Localisez Connect with AWS Security Agent dans la liste des applications installées.
4. Choisissez Copier dans le presse-papiers pour copier l'ID d'installation.

Pour Confluence

1. Dans Confluence, accédez à l'administration de Confluence.
2. Sélectionnez Applications dans la barre latérale.
3. Localisez Connect with AWS Security Agent dans la liste des applications installées.
4. Choisissez Copier dans le presse-papiers pour copier l'ID d'installation.

Vous aurez besoin de cet ID d'installation pour terminer l'enregistrement dans la console de gestion des agents de sécurité AWS.

Connect AWS Security Agent aux référentiels Bitbucket

Connectez votre agent de sécurité AWS aux référentiels Bitbucket Cloud pour activer la révision du code, la modélisation des menaces, les tests de pénétration et les fonctionnalités de correction automatisées. Avant de commencer, examinez the section called "Comment fonctionnent les intégrations avec Agent Spaces" comment un enregistrement est réutilisé dans Agent Spaces et partagé entre les fonctionnalités.

L'intégration de Bitbucket répond à plusieurs objectifs :

- Révision du code : analysez automatiquement les modifications de code dans chaque pull request par rapport aux exigences de sécurité de votre organisation, et exécutez des analyses complètes du référentiel à la demande
- Modélisation des menaces : améliorez la compréhension des applications en analysant le code source, les flux de données et l'architecture
- Contexte des tests d'intrusion - Fournir une compréhension des applications pour les tests d'intrusion
- Correction automatisée : envoyez des pull requests contenant des correctifs pour les vulnérabilités découvertes lors des évaluations de sécurité

Pour connecter Bitbucket à AWS Security Agent, vous devez installer l'application AWS Security Agent Forge sur votre site Atlassian et terminer le flux d'autorisation OAuth.

> **Note**
>
> AWS Security Agent prend uniquement en charge Bitbucket Cloud. Bitbucket Server et Bitbucket Data Center ne sont pas pris en charge.

Comment fonctionne l'intégration de Bitbucket

L'analyse des pull requests s'effectue au sein de Bitbucket. Après avoir installé l'application Forge, connecté des référentiels et activé les commentaires de révision de code dans l'AWS Management Console, AWS Security Agent analyse automatiquement les modifications apportées à chaque

nouvelle pull request (analyse différentielle du code modifié uniquement) et publie les résultats sous forme de commentaires de pull request.

Vous créez et exécutez des révisions de code complètes, qui analysent la base de code complète d'un référentiel, dans l'application Web AWS Security Agent, et non dans Bitbucket.

Les tests de pénétration et la modélisation des menaces sont lancés dans l'application Web AWS Security Agent. Les utilisateurs spécifient les domaines cibles et sélectionnent les référentiels connectés pour fournir le contexte de l'application.

> **Note**
>
> La correction automatique n'est pas disponible pour les référentiels Bitbucket publics afin d'éviter de révéler les vulnérabilités avant qu'elles ne soient corrigées.

Conditions préalables

Avant de commencer, assurez-vous de disposer des éléments suivants :

- Un espace de travail Bitbucket Cloud avec accès administrateur
- Un compte Atlassian avec des privilèges d'administrateur du site
- Autorisations pour configurer les intégrations dans la console de gestion des agents de sécurité AWS

> **Important**
>
> Un site Atlassian ne peut être associé qu'à un seul compte AWS par région. Si vous devez connecter le même site Bitbucket à AWS Security Agent via un autre compte AWS au sein de la même région, vous devez d'abord supprimer l'intégration existante.

> **Note**
>
> La tarification de l'application Atlassian Forge s'applique à cette intégration. Pour plus d'informations, consultez la tarification de la plateforme Forge dans la documentation Atlassian.

Enregistrer une connexion Bitbucket

1. Dans la console de gestion des agents de sécurité AWS, accédez à Intégrations.
2. Choisissez Ajouter une intégration.
3. Sélectionnez Bitbucket, puis Next.
4. Installez l'application AWS Security Agent Forge dans votre espace de travail Bitbucket, en suivant les instructions affichées à l'écran. Après l'installation, copiez l'ID d'installation. Consultez the section called “Trouvez votre identifiant d'installation Atlassian”.
5. Dans le champ ID d'installation, collez l'ID d'installation que vous avez copié depuis Bitbucket.
6. Dans le champ Espace de travail Bitbucket, entrez votre slug d'espace de travail Bitbucket, par exemple. `acme-corp`
7. Choisissez Authorize (Autoriser).

   Vous êtes redirigé vers Atlassian pour autoriser AWS Security Agent à accéder à votre espace de travail Bitbucket. Une fois l'autorisation terminée, vous revenez à la console.
8. Dans la section Détails du registre, entrez un nom d'enregistrement pour cette connexion. Les caractères valides sont les lettres, les chiffres, les points, les traits de soulignement et les traits d'union.
9. Choisissez Se connecter.

> **Note**
>
> Délai de provisionnement après la connexion
>
> Une fois que vous avez choisi Connect, le provisionnement côté Atlassian peut prendre quelques minutes. Pendant ce temps, l'intégration signale un statut en attente. Si vous essayez de sélectionner des référentiels ou d'activer la révision du code avant la fin du provisionnement, un message indiquant que l'installation n'est pas encore disponible peut s'afficher. Patientez quelques minutes et réessayez.

Résoudre les problèmes liés à l'intégration de Bitbucket

Si vous rencontrez des problèmes lors du processus d'intégration de Bitbucket, suivez les instructions suivantes pour résoudre les problèmes courants.

Impossible de terminer l'enregistrement

Si le processus d'enregistrement est interrompu (fermeture du navigateur, expiration de la session), il se peut que l'application Forge soit installée sur votre site Atlassian mais qu'elle ne soit pas enregistrée dans la console AWS.

Résolution

- Retournez à la console AWS Security Agent et redémarrez le processus d'intégration.
- L'application Forge reste installée et n'a pas besoin d'être réinstallée.

Site déjà connecté à un autre compte AWS

Symptômes

- Erreur indiquant que le site Atlassian est déjà associé à un autre compte

Résolution

- Un site Atlassian ne peut être connecté qu'à un seul compte AWS par région.
- Identifiez le compte AWS doté de l'intégration existante et utilisez-le, ou supprimez d'abord l'intégration existante.

L'installation n'est pas disponible

Symptômes

- Lorsque vous sélectionnez des référentiels ou que vous activez la révision du code, un message s'affiche indiquant que l'installation de Bitbucket est en cours et non`PENDING_INSTALLATION`. `AVAILABLE`

Résolution

- L'installation est toujours en cours de provisionnement du côté Atlassian. Le provisionnement se termine normalement en quelques minutes. Patientez quelques minutes, puis réessayez.
- Si le statut n'est pas disponible au bout de quelques minutes, supprimez l'intégration et enregistrez-la à nouveau. Avant de vous réinscrire, désinstallez l'application Forge de votre espace de travail Bitbucket. Pour obtenir des instructions, consultez Supprimer une intégration Bitbucket. Si vous

vous réinscrivez sans désinstaller l'ancienne application Forge, l'installation peut rester bloquée en attente.

Étapes suivantes

Après avoir connecté Bitbucket à AWS Security Agent :

- Accédez à l'espace agent dans lequel vous souhaitez utiliser ces référentiels.
- Choisissez Activer la révision du code ou Configurer les tests de pénétration pour connecter des référentiels spécifiques à votre espace agent
- Activez la correction du code pour permettre à AWS Security Agent de soumettre des pull requests contenant des correctifs de vulnérabilité

Supprimer une intégration Bitbucket

Supprimez une intégration Bitbucket lorsque vous n'avez plus besoin d'AWS Security Agent pour accéder aux référentiels depuis un espace de travail Bitbucket spécifique.

Conditions préalables à la suppression

Avant de supprimer une intégration Bitbucket :

- Vérifiez quels sont les agents Spaces auxquels des référentiels sont connectés à partir de cette intégration
- Comprenez l'impact : la suppression perturbera la révision du code, le contexte des tests d'intrusion, la modélisation des menaces et la correction automatique de tous les référentiels connectés

Étape 1 : supprimer l'intégration d'AWS Security Agent

1. Dans la console de gestion des agents de sécurité AWS, accédez à Intégrations.
2. Localisez l'intégration Bitbucket que vous souhaitez supprimer.
3. Sélectionnez l'intégration.
4. Cliquez sur Supprimer.
5. Consultez la boîte de dialogue de confirmation et choisissez Confirmer la suppression.

Étape 2 : désinstallez l'application Forge

Après avoir supprimé l'intégration d'AWS Security Agent, désinstallez l'application Forge de votre site Atlassian :

1. Dans Bitbucket, accédez aux paramètres de l'espace de travail.
2. Sélectionnez Forge Apps.
3. Localisez Connect with AWS Security Agent.
4. Choisissez Désinstaller.

> **Important**
>
> L'application Forge n'est pas désinstallée automatiquement
>
> La suppression de l'intégration dans la console AWS Security Agent ne désinstalle pas l'application Forge de votre site Atlassian. Si vous prévoyez d'enregistrer à nouveau le même espace de travail Bitbucket, vous devez d'abord désinstaller l'application Forge. Dans le cas contraire, la nouvelle installation risque de rester en attente.

Connectez l'agent de sécurité AWS à Confluence

Connectez votre agent de sécurité AWS à Confluence Cloud pour fournir un contexte de documentation pour les évaluations de sécurité. Contrairement aux fournisseurs de code, Confluence est une source de documentation qui fournit des modèles de menaces, des documents d'architecture, des spécifications d'API et d'autres supports destinés à améliorer la qualité des évaluations de sécurité. Avant de commencer, vérifiez the section called “Comment fonctionnent les intégrations avec Agent Spaces” comment un enregistrement est réutilisé dans Agent Spaces.

L'intégration de Confluence répond à de multiples objectifs :

- Contexte de révision de la conception - Fournir des documents architecturaux et des spécifications de conception pour les examens de conception de sécurité
- Modélisation des menaces - Fournissez les modèles de menaces existants et la documentation du système pour l'analyse des menaces
- Contexte des tests d'intrusion - Fournissez la documentation de l'application pour une meilleure compréhension lors des tests d'intrusion

Pour connecter Confluence à AWS Security Agent, vous devez installer l'application AWS Security Agent Forge sur votre site Atlassian et terminer le flux d'autorisation OAuth.

> **Note**
>
> AWS Security Agent prend uniquement en charge Confluence Cloud. Confluence Data Center et Confluence Server ne sont pas pris en charge.

Comment fonctionne l'intégration de Confluence

Confluence est un fournisseur de documentation plutôt qu'un fournisseur de code source. Après avoir installé l'application Forge et connecté des espaces ou des pages dans l'AWS Management Console, AWS Security Agent peut accéder à votre contenu Confluence pour fournir un contexte lors des évaluations de sécurité.

AWS Security Agent lit le contenu des pages pour comprendre l'architecture de votre application, les exigences de sécurité et les décisions de conception. Ce contexte améliore la qualité et la pertinence des résultats de sécurité lors des révisions de conception, des révisions de code et des tests de pénétration.

Conditions préalables

Avant de commencer, assurez-vous de disposer des éléments suivants :

- Un site Confluence Cloud avec accès administrateur
- Un compte Atlassian avec des privilèges d'administrateur du site
- Autorisations pour configurer les intégrations dans la console de gestion des agents de sécurité AWS

> **Important**
>
> Un site Atlassian ne peut être associé qu'à un seul compte AWS par région. Si vous devez connecter le même site Confluence à AWS Security Agent via un autre compte AWS au sein de la même région, vous devez d'abord supprimer l'intégration existante.

> **Note**
>
> La tarification de l'application Atlassian Forge s'applique à cette intégration. Pour plus d'informations, consultez la tarification de la plateforme Forge dans la documentation Atlassian.

Enregistrer une connexion Confluence

1. Dans la console de gestion des agents de sécurité AWS, accédez à Intégrations.
2. Choisissez Ajouter une intégration.
3. Sélectionnez Confluence, puis Next.
4. Installez l'application AWS Security Agent Forge sur votre site Atlassian en suivant les instructions affichées à l'écran. Après l'installation, copiez l'ID d'installation. Consultez the section called "Trouvez votre identifiant d'installation Atlassian".
5. Dans le champ URL du site Confluence, saisissez l'URL de votre site, par exemple`https://acme.atlassian.net`.
6. Dans le champ ID d'installation, collez l'identifiant d'installation que vous avez copié depuis Confluence.
7. Choisissez Authorize (Autoriser).

   Vous êtes redirigé vers Atlassian pour autoriser AWS Security Agent à accéder à votre site Confluence. Une fois l'autorisation terminée, vous revenez à la console.
8. Dans la section Détails du registre, entrez un nom d'enregistrement pour cette connexion. Les caractères valides sont les lettres, les chiffres, les points, les traits de soulignement et les traits d'union.
9. Choisissez Se connecter.

Sélectionnez les pages d'un espace d'agent

Après avoir enregistré l'intégration Confluence, connectez des pages spécifiques à un espace agent. La sélection d'une page accorde à AWS Security Agent un accès en lecture (extraction) au contenu de cette page. Il n'existe aucune option de fonctionnalité par page : l'agent lit toutes les pages connectées. Au cours de l'étape de révision de l'assistant de connexion, vous pouvez supprimer les pages auxquelles vous ne souhaitez pas que l'agent accède.

Résoudre les problèmes liés à l'intégration de Confluence

Si vous rencontrez des problèmes lors du processus d'intégration de Confluence, suivez les instructions suivantes pour résoudre les problèmes courants.

Impossible de terminer l'enregistrement

Si le processus d'enregistrement est interrompu, il se peut que l'application Forge soit installée sur votre site Atlassian mais qu'elle ne soit pas enregistrée dans la console AWS.

Résolution

- Retournez à la console AWS Security Agent et redémarrez le processus d'intégration.
- L'application Forge reste installée et n'a pas besoin d'être réinstallée.

L'application Forge a été désinstallée d'Atlassian

Si l'application AWS Security Agent Forge est désinstallée de votre site Atlassian alors que l'intégration existe toujours dans AWS Security Agent :

Symptômes

- L'intégration apparaît dans la console AWS mais ne permet pas d'accéder au contenu de Confluence
- Erreurs lors de la tentative de listage ou de lecture de pages

Résolution

- Réinstallez l'application Forge depuis l'Atlassian Marketplace
- Si le problème persiste, supprimez l'intégration dans la console AWS et enregistrez-vous à nouveau

Le site est déjà connecté à un autre compte AWS

Résolution

- Un site Atlassian ne peut être connecté qu'à un seul compte AWS par région.
- Identifiez le compte AWS doté de l'intégration existante et utilisez-le, ou supprimez d'abord l'intégration existante.

Étapes suivantes

Après avoir connecté Confluence à AWS Security Agent :

- Accédez à l'espace agent dans lequel vous souhaitez utiliser cette documentation
- Sélectionnez des pages spécifiques à inclure comme contexte pour les révisions de conception et les tests de pénétration
- Téléchargez de la documentation supplémentaire via S3 si nécessaire (voirthe section called "Fournir des ressources aux agents à partir d'un compartiment S3")

Supprimer une intégration Confluence

Supprimez une intégration Confluence lorsque vous n'avez plus besoin d'AWS Security Agent pour accéder à la documentation d'un site Confluence spécifique.

Conditions préalables à la suppression

Avant de supprimer une intégration Confluence :

- Vérifiez quels agents Spaces ont des pages connectées à partir de cette intégration
- Comprenez l'impact : la suppression perturbera le contexte de la documentation pour les révisions de conception, les tests d'intrusion et la modélisation des menaces dans tous les espaces d'agent utilisant le contenu de cette intégration

Étape 1 : supprimer l'intégration d'AWS Security Agent

1. Dans la console de gestion des agents de sécurité AWS, accédez à Intégrations.
2. Localisez l'intégration Confluence que vous souhaitez supprimer.
3. Sélectionnez l'intégration.
4. Cliquez sur Supprimer.
5. Consultez la boîte de dialogue de confirmation et choisissez Confirmer la suppression.

Étape 2 : désinstallez l'application Forge (facultatif)

Après avoir supprimé l'intégration d'AWS Security Agent, vous pouvez éventuellement désinstaller l'application Forge de votre site Atlassian :

1. Dans Confluence, accédez à l'administration de Confluence.
2. Sélectionnez Apps.
3. Localisez Connect with AWS Security Agent.
4. Choisissez Désinstaller.

Connectez-vous au contrôle de source hébergé en privé

> **Important**
>
> Les connexions privées sont en version préliminaire d'AWS Security Agent et sont susceptibles d'être modifiées.

AWS Security Agent peut se connecter à des systèmes de contrôle de source exécutés sur des réseaux privés, tels que GitLab Self-Managed des instances et des serveurs GitHub d'entreprise. Les connexions privées utilisent Amazon VPC Lattice pour établir une connectivité sécurisée entre AWS Security Agent et votre infrastructure privée sans exposer vos systèmes à l'Internet public.

Comment fonctionnent les connexions privées

Une connexion privée crée un chemin réseau sécurisé entre AWS Security Agent et une ressource cible dans votre VPC. En fait, AWS Security Agent utilise Amazon VPC Lattice pour établir cette connectivité. VPC Lattice est un service de mise en réseau d'applications AWS permettant de connecter, de sécuriser et de surveiller le trafic entre les services sur les VPC et les comptes, sans que vous ayez à gérer l'infrastructure réseau sous-jacente.

Lorsque vous créez une connexion privée :

1. Vous fournissez le VPC, les sous-réseaux et (éventuellement) les groupes de sécurité dotés d'une connectivité réseau avec votre service cible.
2. AWS Security Agent crée une passerelle de ressources gérée par des services et fournit des interfaces réseau élastiques (ENI) dans les sous-réseaux que vous avez spécifiés.
3. L'agent utilise la passerelle de ressources pour acheminer le trafic vers l'adresse IP ou le nom DNS de votre service cible via le chemin du réseau privé.

Service-managed par rapport aux connexions privées autogérées

AWS Security Agent prend en charge deux modes pour les connexions privées :

Service-managed(recommandé pour les configurations simples) :

- AWS Security Agent crée et gère la passerelle de ressources VPC Lattice pour vous.
- Le service cible doit être exécuté dans le même compte AWS où l'agent Space a été créé.
- Impossible de couvrir plusieurs comptes AWS.

Self-managed(pour les configurations avancées ou entre comptes) :

- Vous créez et gérez votre propre configuration de ressources VPC Lattice.
- Vous fournissez le nom de ressource Amazon (ARN) de votre configuration de ressources existante.
- Prend en charge l'accès entre comptes (le client gère le réseau entre comptes).

Conditions préalables

Avant de créer une connexion privée, vérifiez que vous disposez des éléments suivants :

- Un espace d'agents actif
- Un service cible (GitLab Self-Managed ou serveur GitHub d'entreprise) accessible de manière privée à une adresse IP privée ou à un nom DNS connus
- Le service cible doit servir le trafic HTTPS avec une version TLS minimale de 1.2
- Sous-réseaux de votre VPC (1 à 20 sous-réseaux). Nous vous recommandons de sélectionner des sous-réseaux dans plusieurs zones de disponibilité pour une haute disponibilité.
- (Facultatif) Groupes de sécurité pour contrôler le trafic vers les ENI (jusqu'à 5)

> **Note**
>
> Les zones de disponibilité suivantes ne sont pas prises en charge par VPC Lattice :`use1-az3`,,`usw1-az2`,`apne1-az3`,, `apne2-az2euc1-az2`,`euw1-az4`. `cac1-az3` `ilc1-az2`

> **Note**
>
> Les connexions privées sont des ressources au niveau du compte. Après avoir créé une connexion privée, vous pouvez la réutiliser dans plusieurs intégrations et espaces d'agent qui doivent atteindre le même hôte.

> **Note**
>
> Lorsque vous sélectionnez une connexion privée pour un fournisseur qui utilise l'authentification OAuth, la connexion privée s'applique à la fois au point de terminaison du fournisseur et au point de terminaison d'échange de jetons. Assurez-vous que la connexion privée est configurée avec une adresse hôte capable d'acheminer le trafic vers les deux points de terminaison.

Création d'une connexion privée

1. Dans la console de gestion des agents de sécurité AWS, accédez à Intégrations.
2. Choisissez l'onglet Connexions privées.
3. Choisissez Créer une connexion privée.
4. Sous Détails de la connexion, entrez un nom. Les noms peuvent contenir des lettres minuscules, des chiffres et des traits d'union, et doivent commencer et se terminer par une lettre ou un chiffre.
5. Dans la section Détails de la connexion, choisissez le mode de connexion d'AWS Security Agent à votre service cible :
   - Pour qu'AWS Security Agent crée et gère la connexion, laissez la case Utiliser la configuration des ressources existante désactivée, puis complétez les sections Emplacement des ressources, Contrôle d'accès et Détails de la cible du service.
   - Pour effectuer un routage via une configuration de ressources VPC Lattice que vous avez déjà créée, sélectionnez Utiliser la configuration des ressources existantes, puis complétez la section Configuration des ressources existantes. Les sections gérées par les services ne s'appliquent pas.
6. (Service-managed) Sous Emplacement des ressources :
   a. Sélectionnez le VPC où se trouve votre ressource.

b. Sélectionnez un ou plusieurs sous-réseaux. Nous vous recommandons de sélectionner des sous-réseaux dans au moins deux zones de disponibilité.

c. (Facultatif) Sélectionnez un type d'adresse IP (IPv4, IPv6 ou Dual Stack).

7. (Service-managed) Sous Contrôle d'accès :

a. Sélectionnez les groupes de sécurité associés à vos ressources connectées.

b. (Facultatif) Sous Configuration avancée, entrez des plages de ports, par exemple jusqu'à 11 ports ou plages TCP séparés par des virgules. `443, 8080-8090`

8. (Service-managed) Sous Détails de l'objectif du service :

a. Dans le champ Adresse de l'hôte, entrez le nom d'hôte DNS ou l'adresse IP de votre service cible.

b. Pour la résolution DNS, sélectionnez Public pour une adresse hôte pouvant être résolue publiquement ou In VPC (DNS privé) pour une adresse pouvant être résolue uniquement au sein du VPC.

c. (Facultatif) Dans le champ Clé publique du certificat, entrez la clé PEM-encoded publique si votre cible utilise un certificat auto-signé ou une autorité de certification privée. Cela permet à AWS Security Agent de faire confiance à la connexion TLS.

9. (Self-managed) Sous Configuration des ressources existantes, pour Configuration des ressources, sélectionnez une configuration de ressource VPC Lattice dans la liste ou entrez un ID de configuration de ressource (commençant par`rcfg-`) ou son ARN. La liste indique les configurations de ressources dans la région actuelle.

10. Choisissez Créer une connexion.

L'état de la connexion passe à Créer en cours. Cela peut prendre jusqu'à 10 minutes. Lorsque vous avez terminé, le statut passe à Disponible.

Utiliser une connexion privée avec une intégration

Lorsque vous enregistrez une intégration GitLab Self-Managed ou une intégration GitHub Enterprise Server, sélectionnez Se connecter au point de terminaison à l'aide d'une connexion privée, puis choisissez votre connexion dans la liste des connexions privées. L'agent de sécurité AWS achemine le trafic vers le fournisseur via cette connexion. Seules les connexions dont le statut est Disponible apparaissent dans la liste.

Vous pouvez également choisir Créer une connexion privée lors de l'enregistrement. AWS Security Agent conserve votre brouillon d'enregistrement pendant que vous créez la connexion, puis vous renvoie au flux d'enregistrement.

Sécurité

- Aucune exposition publique à Internet : tout le trafic reste sur le réseau AWS.
- Customer-controlled groupes de sécurité : vous gérez les règles de trafic entrant et sortant.
- Service-linked rôle avec le moins de privilèges : l'agent de sécurité AWS utilise un rôle lié à un service limité aux ressources étiquetées avec. `AWSSecurityAgentManaged`

> **Note**
>
> Si votre organisation dispose de politiques de contrôle des services (SCP) qui limitent les actions de l'API VPC Lattice, la passerelle de ressources gérée par les services est créée via un rôle lié à un service. Assurez-vous que vos SCP autorisent les actions nécessaires pour le rôle lié au service.

Vérifier une connexion privée

Une fois que la connexion privée a atteint le statut Disponible, vérifiez la connectivité :

- Assurez-vous que votre service cible fonctionne et accepte les connexions sur le port attendu
- Vérifiez que les groupes de sécurité attachés aux ENI autorisent le trafic sortant sur le port cible
- Vérifiez que le groupe de sécurité de votre service autorise le trafic entrant provenant des adresses IP du plan de données VPC Lattice comprises dans la plage d'adresses CIDR de votre VPC
- Vérifiez que les tables de routage des sous-réseaux autorisent le trafic entre les sous-réseaux ENI et votre service

Supprimer une connexion privée

1. Dans la console AWS Security Agent, accédez à Integrations.
2. Choisissez l'onglet Connexions privées.
3. Sélectionnez la connexion privée que vous souhaitez supprimer.
4. Sélectionnez Delete (Supprimer).

> **Important**
>
> Vous ne pouvez pas supprimer une connexion privée actuellement utilisée par une intégration. Supprimez d'abord l'intégration, puis supprimez la connexion privée.

Étapes suivantes

- the section called "Connectez l'agent de sécurité AWS à GitLab Self-Managed"- Connectez une GitLab instance privée
- the section called "Connect AWS Security Agent au serveur GitHub d'entreprise"- Connectez un serveur GitHub d'entreprise privé

Connect l'agent aux ressources VPC privées

Si l'application sur laquelle vous souhaitez exécuter un test d'intrusion n'est pas disponible sur l'Internet public, vous devez fournir à AWS Security Agent une configuration VPC. AWS Security Agent utilisera cette configuration VPC, y compris un VPC, un sous-réseau et des groupes de sécurité, pour accéder à l'application.

> **Note**
>
> Lorsque vous testez des points de terminaison dans un VPC privé, seuls les points de terminaison se résolvant en adresses IP situées dans des plages d'adresses IP privées connues sont autorisés (voir Blocs d'adresse CIDR VPC pour plus d'informations). Les plages IPv4 et IPv6 suivantes sont autorisées :
>
> ```
> 10.0.0.0/8
> 172.16.0.0/12
> 192.168.0.0/16
> fd00::/8
> ```

> **Note**
>
> Lors de la connexion à un sous-réseau, AWS Security Agent crée une ENI (Elastic Network Interface) dans le sous-réseau configuré pour le test d'intrusion. Cette ENI n'a pas d'adresse

IP publique associée, ce qui signifie qu'elle ne peut pas communiquer avec les passerelles Internet VPC dans les sous-réseaux publics. Si votre test de pénétration nécessite un accès Internet ouvert, veuillez plutôt utiliser un sous-réseau privé associé à une passerelle NAT VPC

Vous accordez à AWS Security Agent un accès général à un VPC depuis l'AWS Management Console. Dans l'application Web Security Agent, les utilisateurs sélectionnent la configuration spécifique pour un test d'intrusion.

Pour ajouter un VPC dans l'espace agent

1. Accédez à la page de présentation de l'Agent Space
2. Sélectionnez Actions, puis Modifier la configuration du test d'intrusion
3. Sous le titre VPC, spécifiez le VPC, les sous-réseaux et les groupes de sécurité

Vous pouvez ajouter jusqu'à 5 VPC.

Autorisations de rôle de service d'espace agent requises

Pour exécuter un test de pénétration avec un VPC, votre rôle de service d'espace agent doit inclure les autorisations suivantes :

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ec2:CreateNetworkInterface",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeNetworkInterfaceAttribute",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeVpcs",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:DeleteNetworkInterface"
      ],
```

```
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": "ec2:CreateNetworkInterfacePermission",
      "Resource": "arn:aws:ec2:{{region}}:{{accountId}}:network-interface/*",
      "Condition": {
        "ArnEquals": {
          "ec2:Subnet": [
            "arn:aws:ec2:{{region}}:{{accountId}}:subnet/[[subnetIds]]"
          ]
        }
      }
    }
  ]
}
```

Pour sélectionner une configuration VPC spécifique pour un test de pénétration dans l'application Web Security Agent

1. Accédez à la page de présentation des tests de pénétration
2. Sélectionnez le test de pénétration pour lequel vous devez ajouter une configuration VPC, puis choisissez Modifier les détails du pentest
3. Sélectionnez Suivant pour accéder à la section Ressources VPC
4. Sélectionnez le VPC, le sous-réseau et les groupes de sécurité
5. Sélectionnez Suivant pour accéder à la dernière section et enregistrer le test de pénétration

> **Note**
>
> Cross-account les tests de pénétration sont actuellement pris en charge pour les ressources VPC (sous-réseaux et groupes de sécurité) partagées à l'aide d'AWS Resource Access Manager. Les secrets de Secrets Manager et les fonctions Lambda utilisés pour les informations d'authentification doivent être configurés dans le même compte AWS que votre AWS Security Agent.

Exécution d'un test de pénétration sur les ressources VPC d'un autre compte AWS

Vous pouvez exécuter des tests de pénétration sur les ressources VPC partagées avec votre compte à l'aide d'AWS Resource Access Manager. Les deux comptes doivent appartenir à la même organisation AWS.

1. (Facultatif) Activez le partage automatique des ressources pour votre organisation AWS

```
aws ram enable-sharing-with-aws-organization
```

2. À l'aide des informations d'identification du compte AWS propriétaire des ressources VPC, partagez les ressources du sous-réseau et du groupe de sécurité avec le compte propriétaire du test d'intrusion

```
aws ram create-resource-share \
    --name SharePentestResources \
    --resource-arns <subnet ARN> <security group ARN> \
    --principals <penetration test owner account ID>
```

3. Accédez à la page de présentation de l'Agent Space
4. Sélectionnez Test de pénétration et recherchez le nom du rôle de service
5. Vérifiez que le rôle IAM accorde l'accès aux ressources VPC partagées
6. Sélectionnez Actions, puis Modifier la configuration du test d'intrusion
7. Sous l'en-tête VPC, spécifiez le VPC, les sous-réseaux et les groupes de sécurité partagés et enregistrez la configuration mise à jour.
8. Accédez à la page de présentation des tests de pénétration sur l'application Web AWS Security Agent
9. Sélectionnez le test de pénétration pour lequel vous devez ajouter une configuration VPC, puis choisissez Modifier les détails du pentest
10. Mettre à jour le test d'intrusion pour utiliser les ressources VPC partagées

Configurer les fonctionnalités

Activez et configurez les tests de pénétration, la révision du code et la modélisation des menaces pour vos espaces d'agents, y compris les mesures correctives, les sources S3 et les domaines cibles.

Activer le test de pénétration

Configurez AWS Security Agent pour exécuter des tests de pénétration autonomes sur vos applications. Cette configuration permet à AWS Security Agent d'accéder à vos ressources AWS, de vérifier la propriété du domaine et d'effectuer des tests de sécurité complets qui identifient les vulnérabilités exploitables dans vos applications Web et vos API.

L'activation des tests d'intrusion permet à AWS Security Agent de valider en permanence la sécurité de votre application sans les délais liés aux tests manuels. En configurant les intégrations AWS nécessaires, vous vous assurez qu'AWS Security Agent peut tester les applications publiques et privées, consigner les résultats et accéder aux informations d'identification pour les tests authentifiés. CloudWatch

Dans cette procédure, vous allez configurer les domaines cibles, éventuellement configurer le VPC, la CloudWatch journalisation, le stockage des informations d'identification et les fonctions Lambda pour les tests, configurer les intégrations S3 pour fournir un contexte supplémentaire et configurer l'accès aux services via des rôles IAM.

Conditions préalables

Avant de commencer, assurez-vous de disposer des éléments suivants :

- Compte AWS avec autorisations administratives pour créer des rôles IAM
- Capacité de vérification de la propriété du domaine (modification des enregistrements DNS ou HTTP)
- Domaines cibles ou applications à tester
- (Facultatif) Détails de configuration du VPC lors du test d'applications privées
- (Facultatif) Compartiment S3 si vous fournissez des artefacts supplémentaires à AWS Security Agent

Étape 1 : Configuration du domaine

Dans la première étape de l'assistant, spécifiez les domaines cibles que vous souhaitez tester et la manière dont AWS Security Agent doit vérifier la propriété.

1. Dans la section Domaines cibles, entrez votre domaine dans le champ Domaine.
2. Sélectionnez une méthode de vérification :
   - DNS_TXT — Prouvez la propriété du domaine en ajoutant un enregistrement TXT à la configuration DNS de votre domaine.
   - HTTP_ROUTE — Prouvez la propriété du domaine en hébergeant un fichier de vérification à une URL spécifique de votre domaine.
   - PRIVATE_VPC - Utilisable uniquement pour les tests de pénétration de VPC privés. Vérifie que le domaine correspond à une adresse IP dans une plage CIDR privée
   - Pour de plus amples informations, veuillez consulter the section called “Activer un domaine d'application pour les tests de pénétration”.
3. Choisissez Ajouter un autre domaine pour ajouter des domaines supplémentaires (jusqu'à 5 au total).
4. Choisissez Next pour procéder à la vérification du domaine.

Étape 2 : vérifier les domaines

Dans la deuxième étape de l'assistant, vérifiez la propriété de chaque domaine que vous avez configuré. AWS Security Agent nécessite une vérification de propriété avant de pouvoir effectuer des tests d'intrusion.

1. Passez en revue les domaines répertoriés dans le tableau des domaines cibles.
2. Pour chaque domaine, sélectionnez-le et déclenchez la vérification en fonction de la méthode que vous avez choisie :
   - Route 53 domaines (même compte AWS) : choisissez la One-click vérification. AWS Security Agent crée automatiquement l'enregistrement DNS et effectue la vérification.
   - DNS TXT (autres fournisseurs DNS) : copiez le jeton de vérification, ajoutez l'enregistrement TXT auprès de votre bureau d'enregistrement DNS, puis sélectionnez le domaine et choisissez Vérifier.

- Route HTTP : placez le jeton de vérification sur le chemin de route requis sur votre serveur Web, puis sélectionnez le domaine et choisissez Vérifier. Pour en savoir plus, consultez the section called "Activer un domaine d'application pour les tests de pénétration".

3. Choisissez Next pour passer à la configuration facultative.

> **Note**
>
> Sub-domains d'un domaine vérifié ne nécessitent pas de vérification individuelle lors de l'utilisation du DNS TXT ou de la vérification de route HTTP. Pour la vérification d'un VPC privé, le nom de domaine du point de terminaison cible doit correspondre au nom de domaine complet configuré pour la vérification.

> **Note**
>
> Pour les domaines privés au sein d'un VPC, vous pouvez continuer même si le statut de vérification du domaine est INACCESSIBLE. L'agent de sécurité AWS tentera de vérifier le domaine pour les points de terminaison privés au début de chaque pentest.

Étape 3 : (Facultatif) Configurer des fonctionnalités supplémentaires

La troisième étape de l'assistant vous permet de configurer des ressources AWS facultatives afin d'étendre la portée de vos tests d'intrusion. Toutes les sections de cette étape sont facultatives et réduites par défaut.

(Facultatif) Configurer les paramètres VPC

Si vous envisagez de tester des domaines cibles privés hébergés au sein d'un VPC, configurez les paramètres VPC pour AWS Security Agent. Cette section est facultative et réduite par défaut.

1. Développez la section VPC.
2. Dans le menu déroulant VPC, sélectionnez le VPC qui héberge vos domaines cibles privés.
3. Dans la liste déroulante Sous-réseau, sélectionnez les sous-réseaux VPC que l'agent de sécurité AWS doit utiliser :

> **Tip**
>
> Pour une haute disponibilité, sélectionnez plusieurs sous-réseaux dans plusieurs zones de disponibilité. Assurez-vous que vos sous-réseaux incluent une passerelle NAT pour la connectivité sortante.

4. Dans le menu déroulant Groupe de sécurité, sélectionnez les groupes de sécurité VPC que l'agent de sécurité AWS doit utiliser :

> **Important**
>
> Assurez-vous que vos groupes de sécurité autorisent les connexions sortantes pour qu'AWS Security Agent puisse effectuer des tests de pénétration.

(Facultatif) Configurer la CloudWatch journalisation

Configurez CloudWatch pour stocker les journaux de vos tests d'intrusion. Cette section est facultative et réduite par défaut.

1. Développez la section CloudWatch des journaux.
2. Dans le menu déroulant Groupes de journaux, sélectionnez les groupes de CloudWatch journaux existants
3. Si aucun groupe de journaux n'est sélectionné, AWS Security Agent créera un groupe de journaux `/aws/securityagent/<agent name>/<pentest id>` doté des autorisations appropriées.

> **Note**
>
> Assurez-vous que votre rôle IAM est autorisé à écrire dans le groupe de CloudWatch journaux sélectionné.

(Facultatif) Configurer les secrets pour les informations d'identification des tests

Si votre application nécessite des informations d'authentification pour les tests, AWS Security Agent peut les récupérer en toute sécurité depuis AWS Secrets Manager. Cette section est facultative et réduite par défaut.

1. Développez la section Secrets.
2. Sélectionnez les secrets AWS Secrets Manager qui contiennent les informations d'identification de votre application.
3. Lorsque vous configurez un test d'intrusion dans l'application Web, vous pouvez faire référence à ces secrets pour des tests authentifiés.

> **Important**
>
> Les informations d'identification sont cryptées et stockées dans AWS Secrets Manager. Assurez-vous que votre rôle IAM est autorisé à accéder à Secrets Manager for AWS Security Agent afin d'utiliser ces informations d'identification lors des tests.

(Facultatif) Configurer les fonctions Lambda pour les informations d'identification des tests

Configurez les fonctions Lambda qui peuvent fournir des informations d'identification pour votre application lors des tests. Cette section est facultative et réduite par défaut.

1. Développez la section des fonctions Lambda.
2. Sélectionnez les fonctions Lambda qui peuvent fournir des informations d'authentification pour votre application.
3. AWS Security Agent invoquera ces fonctions lors des tests d'intrusion afin d'obtenir des informations d'identification de manière dynamique.

> **Note**
>
> Assurez-vous que votre rôle IAM est autorisé à appeler les fonctions Lambda spécifiées. Les fonctions Lambda doivent renvoyer les informations d'identification dans le format attendu pour qu'AWS Security Agent puisse les utiliser lors des tests.

(Facultatif) Configurer le compartiment S3

Fournissez les détails du compartiment S3 si vous prévoyez de télécharger des documents ou des artefacts à fournir en entrée à AWS Security Agent. Cette section est facultative et réduite par défaut.

1. Développez la section des compartiments S3.

2. Dans le champ Bucket, entrez ou recherchez le nom de votre compartiment S3.

> **Note**
>
> Vous pouvez également connecter GitHub des référentiels ultérieurement ou télécharger des fichiers directement dans l'application Web. Les informations fournies peuvent garantir une couverture complète, réduire les faux positifs et fournir des résultats exploitables.

(Facultatif) Configurer l'accès au service

AWS Security Agent nécessite un rôle IAM pour accéder à vos ressources AWS (VPC CloudWatch , groupes de logs, Secrets Manager, fonctions Lambda, etc.) pour les tests d'intrusion. Cette section est facultative et réduite par défaut.

1. Développez la section Accès au service.
2. Par défaut, AWS Security Agent utilise un rôle IAM par défaut avec les autorisations requises pour les tests d'intrusion.
3. Pour personnaliser le rôle IAM, sélectionnez l'une des options suivantes :
   a. Créer un rôle par défaut : AWS Security Agent crée automatiquement un nouveau rôle IAM avec les autorisations nécessaires
   b. Utiliser un rôle de service existant : sélectionnez un rôle IAM existant dans le menu déroulant
4. Si vous utilisez un rôle existant :
   a. Choisissez le menu déroulant sous Choisir un rôle existant
   b. Sélectionnez votre rôle IAM dans la liste
   c. Choisissez l'icône d'actualisation pour mettre à jour la liste si nécessaire

> **Note**
>
> Le rôle IAM par défaut inclut les autorisations d'accès aux ressources VPC, aux groupes de journaux CloudWatch , à Secrets Manager, aux fonctions Lambda et aux autres services requis pour les tests d'intrusion. Il est recommandé d'utiliser le rôle IAM par défaut, sauf si vous avez des exigences de sécurité spécifiques.

Étape 4 : enregistrer et activer les tests de pénétration

Après avoir configuré tous les paramètres requis, activez les tests d'intrusion pour votre agent AWS Security Agent.

1. Passez en revue toutes les sections de configuration pour vous assurer de leur exactitude.
2. Choisissez Enregistrer.
3. AWS Security Agent valide votre configuration et crée les ressources AWS nécessaires.

Étapes suivantes

Après avoir activé les tests de pénétration :

- Configurer les étendues des tests d'intrusion dans l'application Web AWS Security Agent
- Configurer les préférences de notification pour les résultats des tests
- Examiner les résultats des tests d'intrusion et y répondre dès qu'ils sont découverts
- (Facultatif) Configurer des référentiels supplémentaires pour la correction des résultats

Pour plus d'informations sur l'exécution et la gestion des tests d'intrusion, consultez la documentation de l'application Web AWS Security Agent.

Activer la révision du code de pull request pour les GitHub référentiels

La révision du code par pull request est désormais configurée dans le cadre de l'assistant de configuration de la révision du code. Lorsque vous connectez GitHub des référentiels à votre espace agent, vous pouvez activer les commentaires de demandes d'extraction pour des référentiels individuels afin qu'AWS Security Agent analyse automatiquement les pull requests et publie les résultats de sécurité.

Pour obtenir des instructions de configuration complètes, voirthe section called “Activer la révision du code”.

Pour plus d'informations sur la manière dont les résultats des pull requests apparaissent GitHub et sur la manière d'y répondre, consultezthe section called “Passez en revue les résultats de sécurité du code dans les pull requests”.

Activer la révision du code

Configurez votre espace agent pour permettre la révision du code en connectant le code source à partir de GitHub référentiels ou de compartiments S3. La révision du code analyse votre code source pour détecter les failles de sécurité et sa conformité aux exigences de sécurité personnalisées de votre entreprise.

La configuration des configurations de révision du code est une Space-wide opération de l'agent. Les intégrations et les compartiments S3 que vous connectez sont partagés entre les fonctionnalités, y compris la révision du code et les tests de pénétration.

Une fois la configuration terminée, les utilisateurs peuvent créer et exécuter des révisions de code dans l'application Web AWS Security Agent pour analyser les référentiels et les sources S3 afin de détecter les problèmes de sécurité.

> **Note**
>
> Si des GitHub référentiels sont déjà connectés à votre espace agent (par exemple, par le biais de la configuration de tests d'intrusion), la révision du code est déjà activée. Vous pouvez ignorer cette configuration et accéder directement à l'application Web pour créer des révisions de code. Consultez the section called “Création d'une révision de code”.

Conditions préalables

Avant de commencer, assurez-vous de disposer des éléments suivants :

- Un espace d'agent créé dans l'AWS Management Console (voirthe section called “Création d'un espace d'agent”)
- Au moins l'une des entrées de code source suivantes :
  - Un compte d' GitHub organisation ou d'utilisateur sur lequel l' GitHub application AWS Security Agent est installée (voirthe section called “Connect AWS Security Agent aux GitHub référentiels”)
  - Un compartiment S3 contenant le code source que vous souhaitez consulter
- Autorisations pour configurer les intégrations pour votre espace d'agent
- (Facultatif) Au moins une exigence de sécurité activée dans un pack d'exigences de sécurité si vous prévoyez d'utiliser la validation des exigences de sécurité (voirthe section called “Gérer les exigences de sécurité”)

Accédez à l'assistant de configuration de la révision du code

Accédez à la configuration de révision du code pour votre espace agent.

1. Dans la console AWS Security Agent, sélectionnez votre espace agent.
2. Choisissez Activer la révision du code depuis l'un des emplacements suivants :
   - La carte de révision du Code
   - L'onglet Révision du code, puis choisissez Activer la révision du code

> **Tip**
>
> Si vous souhaitez qu'AWS Security Agent réponde automatiquement aux commentaires relatifs à la révision du code, activez également la correction du code. Consultez the section called “Permettre aux utilisateurs de commencer à corriger les résultats des tests d'intrusion et de la révision du code” pour plus de détails.

Vous êtes dirigé vers l'assistant de révision des configurations du code d'installation.

Étape 1 : Connecter les intégrations, les dépôts et les buckets

Dans la première étape de l'assistant, connectez vos entrées de code source et configurez les paramètres de révision du code. Vous devez ajouter au moins un GitHub référentiel ou un compartiment S3 pour continuer.

> **Important**
>
> Les intégrations et les compartiments S3 configurés ici sont partagés dans votre espace d'agent. Les modifications s'appliquent à la fois aux fonctionnalités de révision du code et de test d'intrusion.

Connect les GitHub référentiels

Ajoutez GitHub des référentiels provenant de vos GitHub organisations ou comptes d'utilisateurs autorisés. Choisir Ajouter ouvre l' GitHubassistant Connect en deux étapes, dans lequel vous sélectionnez d'abord les référentiels, puis configurez les actions qu'AWS Security Agent peut effectuer sur chacun d'eux.

1. Dans la section Intégrations connectées, choisissez Ajouter.
2. Sélectionnez l' GitHub enregistrement qui contient les référentiels que vous souhaitez consulter.
3. À l'étape Connecter GitHub les référentiels, cochez la case correspondant à chaque référentiel que vous souhaitez connecter.
4. Choisissez Suivant pour accéder à Gérer les fonctionnalités.

> **Note**
>
> Les référentiels connectés sont accessibles en lecture seule pour l'analyse du code lors de la révision du code et des tests de pénétration. Vous configurez les actions d'écriture telles que la publication de commentaires de révision et l'ouverture de pull requests de correction à l'étape suivante.

> **Note**
>
> Si vous n'avez pas encore enregistré d' GitHub intégration, choisissez Paramètres pour accéder à la page Intégrations où vous pouvez autoriser l' GitHub application AWS Security Agent. Pour de plus amples informations, veuillez consulter the section called “Connect AWS Security Agent aux GitHub référentiels”.

Configuration des fonctionnalités GitHub du référentiel

À l'étape Gérer les fonctionnalités de l' GitHubassistant Connect, choisissez ce qu'AWS Security Agent peut faire dans chaque référentiel. Les commentaires relatifs à la révision du code et à la correction du code sont définis indépendamment par référentiel.

1. Pour chaque référentiel, activez les commentaires de révision du code pour qu'AWS Security Agent publie les résultats de sécurité sous forme de commentaires sur les pull requests.
2. Pour chaque référentiel, activez la correction du code pour permettre à AWS Security Agent de corriger les résultats. Lorsque cette option est activée, les utilisateurs de l'application Web peuvent demander des pull requests qui corrigent les résultats, et les auteurs des pull requests peuvent commenter `@AWS-Security-Agent fix all findings.` pour que l'agent réponde à ses commentaires de révision.

3. Choisissez Enregistrer pour appliquer vos sélections et revenir à l'assistant de configuration de révision du code.

Lorsque les commentaires de révision du code sont activés pour un référentiel :

- AWS Security Agent analyse automatiquement les pull requests lorsqu'elles sont marquées comme « prêtes à être examinées ». Les brouillons de pull requests ne sont pas analysés.
- Les résultats de sécurité sont publiés sous forme de commentaires directement sur la pull request avec des conseils de correction spécifiques.
- L'analyse utilise les paramètres de révision du code que vous avez configurés (vulnérabilités de sécurité, exigences personnalisées, ou les deux).

> **Note**
>
> Les commentaires de pull request ne sont disponibles que pour les GitHub référentiels privés.

Lorsque la correction du code est activée pour un référentiel, les utilisateurs de l'application Web peuvent commencer à corriger le code à la fois pour la révision du code et les résultats des tests d'intrusion sur ce référentiel, et AWS Security Agent fournit chaque correctif sous forme de pull request. Pour de plus amples informations, veuillez consulter the section called “Permettre aux utilisateurs de commencer à corriger les résultats des tests d'intrusion et de la révision du code”.

Pour plus d'informations sur la manière dont les résultats des pull requests apparaissent GitHub et sur la manière d'y répondre, consultezthe section called “Passez en revue les résultats de sécurité du code dans les pull requests”.

Ajouter des compartiments S3

Ajoutez des compartiments S3 contenant du code source ou des ressources contextuelles pour la révision du code.

1. Dans la section compartiments S3, choisissez Ajouter une ressource S3.
2. Entrez l'URI S3 du compartiment ou du préfixe contenant votre code source.
3. Choisissez Ajouter.

> **Note**
>
> Vous pouvez ajouter jusqu'à 10 ressources S3. Les compartiments S3 sont partagés entre différentes fonctionnalités, notamment la révision du code et les tests de pénétration.

> **Tip**
>
> Vous pouvez ajouter des compartiments S3 contenant du code source, des fichiers de configuration, des modèles d'infrastructure sous forme de code ou d'autres artefacts que vous souhaitez qu'AWS Security Agent analyse pour détecter des problèmes de sécurité.

Configurer les paramètres de révision du code

Configurez les types de problèmes de sécurité analysés par AWS Security Agent lors des révisions de code. Ce paramètre s'applique à tous les référentiels et sources pour lesquels la révision de code est activée dans cet espace agent.

1. Dans la section Paramètres de révision du code, sélectionnez l'une des options suivantes :
   - Validation des exigences de sécurité : vérifiez si le code est conforme aux exigences de sécurité que vous avez activées dans vos packs d'exigences de sécurité.
   - Découverte des failles de sécurité — Identifiez les failles de sécurité courantes dans le code.
   - Exigences de sécurité et découverte des vulnérabilités : analysez le code pour vérifier sa conformité aux exigences de sécurité que vous avez activées et les vulnérabilités de sécurité courantes. Il s'agit du paramètre par défaut.

> **Note**
>
> Lorsque la validation des exigences de sécurité est activée, AWS Security Agent vérifie le code par rapport aux exigences de sécurité que vous avez activées dans vos packs d'exigences de sécurité. Si vous sélectionnez la validation des exigences de sécurité mais qu'au moins une exigence de sécurité n'est activée, AWS Security Agent n'identifiera pas les résultats basés sur les exigences. Pour plus d'informations sur les conditions de sécurité, consultez the section called "Gérer les exigences de sécurité".

1. Choisissez Next pour passer aux configurations facultatives.

Étape 2 : Configurations facultatives

Dans la deuxième étape de l'assistant, configurez les paramètres facultatifs de CloudWatch journalisation et d'accès aux services pour votre environnement de révision de code.

(Facultatif) Configurer CloudWatch les journaux

Configurez des groupes de CloudWatch journaux pour capturer et analyser le comportement des applications lors de la révision du code.

1. Développez la section CloudWatch des journaux.
2. Dans le menu déroulant Groupes de journaux, sélectionnez un ou plusieurs groupes de CloudWatch journaux existants depuis votre compte AWS.

> **Note**
>
> Si vous ne sélectionnez aucun groupe de journaux, AWS Security Agent crée automatiquement un groupe de journaux par défaut pour stocker les journaux d'exécution des révisions de code.

(Facultatif) Configurer l'accès au service

Configurez le rôle de service IAM utilisé par l'agent de sécurité AWS pour accéder à vos ressources AWS, telles que les compartiments S3 et les CloudWatch journaux pour la révision du code.

1. Développez la section Accès au service.
2. Sélectionnez l'une des options suivantes :
   - Créer un rôle par défaut : AWS Security Agent crée automatiquement un nouveau rôle IAM avec les autorisations nécessaires pour la révision du code.
   - Utiliser un rôle de service existant : sélectionnez un rôle IAM existant dans le menu déroulant.
3. Si vous utilisez le rôle par défaut, entrez un nom de rôle de service. Le nom doit être unique pour tous les rôles du compte, utiliser des caractères alphanumériques et `+=,.@-_` ne pas inclure d'espaces.

> **Note**
>
> Le nom du rôle de service a une longueur maximale de 64 caractères. Un rôle de service est automatiquement créé si vous ne sélectionnez aucun rôle existant.

1. Choisissez Enregistrer pour terminer la configuration.

Après la configuration

Après avoir terminé l'assistant de configuration de la révision du code :

- La carte de révision du code sur votre page Agent Space indique le statut Prêt.
- Les utilisateurs peuvent lancer l'application Web et créer des révisions de code pour analyser les référentiels connectés et les sources S3.
- Vous pouvez modifier votre configuration à tout moment en choisissant Modifier la configuration dans l'onglet Révision du code.

Modifier la configuration de révision du code

Pour modifier votre configuration de révision de code après la configuration initiale, procédez comme suit :

1. Accédez à votre espace d'agent dans la console AWS Security Agent.
2. Sélectionnez l'onglet Révision du code.
3. Choisissez Modifier la configuration.
4. Mettez à jour vos intégrations, vos compartiments S3, vos paramètres de révision du code, vos CloudWatch journaux ou votre accès aux services selon vos besoins.
5. Choisissez Enregistrer.

Étapes suivantes

Après avoir configuré les configurations de révision du code :

- Lancez l'application Web pour créer et exécuter des révisions de code (voirthe section called "Création d'une révision de code")

- Connectez des GitHub référentiels ou des compartiments S3 supplémentaires à mesure que votre base de code augmente
- Configurer les packs d'exigences de sécurité pour une validation spécifique à l'organisation (voir) the section called “Gérer les exigences de sécurité”
- Vérifiez comment les résultats des pull requests apparaissent dans GitHub (voirthe section called “Passez en revue les résultats de sécurité du code dans les pull requests”)

Activez la modélisation des menaces

Configurez votre espace agent pour permettre la modélisation des menaces en connectant les référentiels de code source et en configurant les ressources AWS. La modélisation des menaces analyse l'architecture de votre application et identifie les menaces de sécurité à partir du code source, des documents de conception, ou des deux.

La configuration des configurations de modélisation des menaces est une Space-wide opération de l'agent. Les intégrations et les compartiments S3 que vous connectez sont partagés entre les fonctionnalités, notamment la modélisation des menaces, la révision du code et les tests de pénétration.

Une fois la configuration terminée, les utilisateurs peuvent créer et exécuter des modèles de menace dans l'application Web AWS Security Agent.

> **Note**
>
> Si des référentiels ou des compartiments S3 sont déjà connectés à votre espace agent (par exemple, par le biais de la révision du code ou de la configuration de tests d'intrusion), la modélisation des menaces est peut-être déjà activée. Vous pouvez accéder directement à l'application Web pour créer un modèle de menace. Consultez the section called “Création d'un modèle de menace”.

Conditions préalables

Avant de commencer, assurez-vous de disposer des éléments suivants :

- Un espace d'agent créé dans l'AWS Management Console (voirthe section called “Création d'un espace d'agent”)

- Autorisations pour configurer les intégrations pour votre espace d'agent
- (Facultatif) Une GitHub ou une organisation Bitbucket sur laquelle l'application AWS Security Agent est installée (voir Connect AWS Security Agent aux GitHub référentiels, Connect AWS Security Agent aux GitLab référentiels ou Connect AWS Security Agent aux référentiels Bitbucket) GitLab

Accédez à l'assistant de configuration de la modélisation des menaces

Accédez à la configuration de modélisation des menaces pour votre espace agent.

1. Dans la console AWS Security Agent, sélectionnez votre espace agent.
2. Choisissez Configurer le modèle de menace dans la fiche Modèle de menace ou dans l'onglet Modèle de menace.

Vous êtes dirigé vers l'assistant de configuration du modèle de menace, qui comporte deux étapes facultatives.

Étape 1 : Connecter les référentiels de code source (facultatif)

Connectez les GitHub référentiels ou Bitbucket pour lesquels vous souhaitez activer la modélisation des menaces. GitLab Les modèles de menace eux-mêmes sont créés et visualisés dans l'application Web.

> **Important**
>
> Les intégrations configurées ici sont partagées dans votre espace agent. Les modifications s'appliquent aux capacités de modélisation des menaces, de révision du code et de tests de pénétration.

Connect les référentiels

1. Dans la section Intégrations connectées, choisissez Ajouter.
2. Sélectionnez l'enregistrement qui contient les référentiels que vous souhaitez utiliser.
3. Cochez la case correspondant à chaque référentiel que vous souhaitez connecter.
4. Choisissez Enregistrer pour appliquer vos sélections.

> **Note**
>
> Si vous n'avez pas encore enregistré d'intégration, choisissez Paramètres pour accéder à la page Intégrations où vous pouvez autoriser l'application AWS Security Agent. Pour plus d'informations, consultez Connect AWS Security Agent aux GitHub référentiels, Connect AWS Security Agent aux GitLab référentiels ou Connect AWS Security Agent aux référentiels Bitbucket.

1. Choisissez Next pour passer aux configurations facultatives.

Étape 2 : Configurations facultatives

Configurez les compartiments S3, la CloudWatch journalisation et les paramètres d'accès aux services pour votre environnement de modélisation des menaces. Ces paramètres sont partagés avec d'autres fonctionnalités de votre espace agent.

Seaux S3 (en option)

Ajoutez des compartiments S3 contenant le code source que vous souhaitez que l'agent utilise comme contexte lors de la modélisation des menaces.

1. Dans la section compartiments S3, choisissez Ajouter une ressource S3.
2. Entrez l'URI S3 pour le compartiment ou le préfixe.
3. Choisissez Ajouter.

> **Note**
>
> Vous pouvez ajouter jusqu'à 10 ressources S3.

CloudWatch journaux (facultatif)

Configurez des groupes de CloudWatch journaux pour capturer et analyser le comportement des applications lors de l'exécution du modèle de menace.

1. Dans la section CloudWatch journaux, sélectionnez un ou plusieurs groupes de CloudWatch journaux existants depuis votre compte AWS.

Accès au service

Configurez le rôle de service IAM utilisé par l'agent de sécurité AWS pour accéder à vos ressources AWS, telles que les compartiments S3 et les CloudWatch journaux pour la modélisation des menaces. Un rôle de service est requis pour permettre la modélisation des menaces.

1. Dans la section Accès au service, sélectionnez un rôle de service IAM existant dans la liste déroulante, ou laissez-le vide pour qu'un rôle de service soit automatiquement créé.

> **Note**
>
> Un rôle de service sera automatiquement créé si vous ne sélectionnez aucun rôle existant.

1. Choisissez Enregistrer pour terminer la configuration.

Après la configuration

Une fois la configuration de modélisation des menaces terminée :

- La carte Modèle de menace sur votre page Agent Space indique le statut Prêt.
- Les utilisateurs peuvent lancer l'application Web et créer des modèles de menace à partir du code source connecté, des documents de scope téléchargés, des pages Confluence ou d'une combinaison de ces entrées.

Étapes suivantes

Après avoir activé la modélisation des menaces :

- Lancez l'application Web pour créer et exécuter des modèles de menace (voir Création d'un modèle de menace)
- Connectez des référentiels ou des compartiments S3 supplémentaires à mesure que votre base de code augmente
- Connect Confluence pour permettre de sélectionner des pages comme documents de portée (voir Connecter l'agent de sécurité AWS à Confluence)

Permettre aux utilisateurs de commencer à corriger les résultats des tests d'intrusion et de la révision du code

Dans l'AWS Management Console, vous pouvez activer la correction automatique afin que les utilisateurs de l'application Web AWS Security Agent puissent demander des corrections pour un résultat spécifique. AWS Security Agent fournit chaque correctif sous forme de GitHub pull request sur le référentiel concerné.

Vous activez la correction par référentiel depuis un espace agent. Les onglets Test de pénétration et Révision du code ouvrent le même assistant de configuration du référentiel. Vous pouvez donc utiliser l'un ou l'autre onglet pour gérer le paramètre d'activation de la correction automatique. La correction s'applique aux résultats des deux fonctionnalités. Vous ne devez donc l'activer qu'une seule fois par référentiel.

Conditions préalables

Avant de commencer, assurez-vous de disposer des éléments suivants :

1. Tests de pénétration activés (voirthe section called “Activer le test de pénétration”) ou révision du code (voirthe section called “Activer la révision du code”)
2. Vous avez installé et autorisé l' GitHub application AWS Security Agent pour votre GitHub organisation (voirthe section called “Connect AWS Security Agent aux GitHub référentiels”)

Ouvrez l'assistant de configuration du référentiel

Choisissez le point d'entrée correspondant à la configuration de vos référentiels.

Depuis l'onglet Test de pénétration

Utilisez ce chemin pour ajouter GitHub des référentiels destinés aux tests de pénétration et configurer la correction en même temps.

1. Accédez à la page de présentation de l'Agent Space.
2. Choisissez l'onglet Test de pénétration.
3. Sélectionnez un GitHub enregistrement propriétaire de vos référentiels :
   a. Si vous n'avez associé aucun GitHub enregistrement à l'espace agent, choisissez Ajouter dans le champ d'informations Connect GitHub to AWS Security Agent pour sélectionner un enregistrement.

b. Si un ou plusieurs GitHub enregistrements sont déjà associés, choisissez Ajouter dans la section Intégrations connectées pour en sélectionner un autre.

4. Choisissez Next pour sélectionner les GitHub référentiels.
5. Choisissez Next pour configurer les fonctionnalités du référentiel.

Depuis l'onglet Révision du code

Utilisez ce chemin lorsque vos référentiels sont déjà connectés pour la révision du code.

1. Accédez à la page de présentation de l'Agent Space.
2. Choisissez l'onglet Révision du code.
3. Dans le tableau GitHub des référentiels, choisissez Modifier pour ouvrir l'assistant de configuration des référentiels.

Activez la correction automatique et économisez

Une fois que vous avez atteint les fonctionnalités du référentiel, suivez l'un des chemins ci-dessus :

1. Dans la colonne Correction automatique activée, marquez chaque référentiel que vous souhaitez corriger comme Activé.
2. Choisissez Connect pour enregistrer la configuration.

Les utilisateurs de l'application Web peuvent désormais commencer à corriger les résultats trouvés dans ces référentiels, et AWS Security Agent ouvrira les pull requests avec les correctifs proposés.

Fournir des ressources aux agents à partir d'un compartiment S3

Vous pouvez accorder à AWS Security Agent l'accès aux ressources d'un compartiment S3, telles que les documents d'API, les documents de modèles de menaces et le code source qui prennent en charge les tests d'intrusion.

Vous accordez à AWS Security Agent un accès en lecture à un compartiment S3 dans l'AWS Management Console. Dans l'application Web Security Agent, les utilisateurs sélectionnent les ressources individuelles de S3 selon les besoins.

1. Accédez à la page de présentation de l'Agent Space

2. Sélectionnez Actions, puis Modifier la configuration du test d'intrusion
3. Dans la section des compartiments S3, définissez l'URI S3 contenant le compartiment S3. Vous pouvez ajouter plusieurs compartiments S3.

Activer un domaine d'application pour les tests de pénétration

Avant de pouvoir exécuter un test d'intrusion sur une application, vous devez ajouter un domaine cible et en vérifier la propriété. AWS Security Agent n'effectuera des tests de pénétration que sur des domaines vérifiés.

> **Note**
>
> Il n'est pas nécessaire de valider les domaines auxiliaires que votre application peut utiliser. Il vous suffit de valider le domaine sur lequel vous allez effectuer activement des tests d'intrusion.

Étape 1 : ajouter un domaine cible

Pour ajouter un domaine cible, accédez à l'onglet Test de pénétration sur la page de présentation de l'Agent Space. Selon que vous avez déjà configuré les tests d'intrusion, appliquez l'une des méthodes suivantes :

- First-time configuration : choisissez Configurer le test d'intrusion pour ouvrir l'assistant de test d'intrusion. Dans un premier temps, entrez le domaine et choisissez une méthode de vérification.
- Ajouter un domaine à une configuration existante : dans le tableau Domaines cibles, sélectionnez Ajouter un domaine. Entrez le domaine et choisissez une méthode de vérification dans le modal.

Vous pouvez ajouter un domaine de base ou un sous-domaine, tel que `example.com` ou`billing.example.com`. AWS suggère d'utiliser un sous-domaine dans lequel vous êtes autorisé à créer des TXT enregistrements.

> **Note**
>
> Lorsque vous vérifiez un domaine à l'aide de la vérification de route DNS TXT ou HTTP, les sous-domaines de ce domaine sont automatiquement couverts. Par exemple, la vérification vous `example.com` permet de tester `api.example.com` ou `billing.example.com`

sans vérification supplémentaire. Pour la vérification d'un VPC privé, le nom de domaine du point de terminaison cible doit correspondre au nom de domaine complet configuré pour la vérification.

Choisissez l'une des méthodes de vérification suivantes :

- Enregistrement DNS TXT : prouvez la propriété du domaine en créant un enregistrement DNS TXT auprès de votre fournisseur DNS.
- Route HTTP : prouvez la propriété du domaine en créant une route sur votre serveur Web contenant un jeton unique fourni par l'agent de sécurité AWS.
- VPC privé : utilisable uniquement pour les tests de pénétration de VPC privés. Vérifie que le domaine est résolu en une adresse IP dans une plage d'adresses CIDR privée. Le nom de domaine configuré doit correspondre au nom de domaine complet de tous les points de terminaison cibles associés

Étape 2 : vérifier la propriété du domaine

Après avoir ajouté le domaine, vérifiez la propriété à l'aide de la méthode que vous avez sélectionnée. Vous pouvez déclencher la vérification à tout moment depuis le tableau des domaines cibles en sélectionnant le domaine et en choisissant Vérifier.

Vérifier à l'aide d'un enregistrement DNS TXT

AWS Security Agent génère une valeur d'enregistrement DNS TXT. Vous devez ajouter cet enregistrement auprès de votre fournisseur DNS pour prouver que vous en êtes le propriétaire.

Si le domaine est enregistré sur Route 53 (même compte AWS) :

AWS Security Agent peut créer l'enregistrement DNS automatiquement. Sélectionnez le domaine dans le tableau des domaines cibles et choisissez la One-click vérification. AWS Security Agent crée l'enregistrement de validation DNS et effectue la vérification automatiquement.

Si le domaine est enregistré auprès d'un autre fournisseur DNS :

1. Copiez la valeur d'enregistrement TXT fournie par l'agent de sécurité AWS.
2. Ajoutez l'enregistrement TXT auprès de votre bureau d'enregistrement DNS.
3. Revenez au tableau des domaines cibles, sélectionnez le domaine, puis choisissez Vérifier.

Vérifiez à l'aide de la validation de route HTTP

Cette méthode prouve la propriété du domaine en plaçant un jeton unique sur votre serveur Web. Seuls les propriétaires de domaines ou les administrateurs Web autorisés peuvent créer des itinéraires sur un serveur Web, ce qui prouve qu'ils en sont propriétaires.

1. Créez un fichier au chemin suivant sur votre serveur Web :

```
.well-known/aws/securityagent-domain-verification.json
```

2. Placez le jeton fourni par l'agent de sécurité AWS dans le fichier en utilisant le format suivant :

```
{
  "tokens": ["<insert-token>"]
}
```

3. Revenez au tableau des domaines cibles, sélectionnez le domaine, puis choisissez Vérifier. AWS Security Agent envoie une demande HTTPS GET à l'URL de vérification et valide le jeton.
4. Si le domaine est accessible sur l'Internet public, assurez-vous qu'il possède un certificat SSL valide avant d'exécuter la vérification.

> **Note**
>
> Si votre domaine est enregistré dans plusieurs espaces d'agent et que vous utilisez la validation de route HTTP, vous pouvez placer les jetons des deux espaces d'agent dans le même `tokens` tableau.

Contourner la vérification de la propriété du domaine

Les clients autorisés à effectuer des tests de pénétration sur un terminal mais ne pouvant pas effectuer la vérification de propriété peuvent nous demander une vérification manuelle. Veuillez ouvrir un dossier d'assistance client pour effectuer cette demande. Votre demande doit inclure votre cas d'utilisation professionnelle et votre justification de la vérification manuelle de propriété (c'est-à-dire la raison pour laquelle vous êtes autorisé à effectuer des tests de pénétration sur le terminal).

Domaines cibles gérés utilisés pour les tests de pénétration

Dans l'AWS Management Console, vous pouvez ajouter et gérer des domaines cibles utilisés par les espaces d'agent pour les tests d'intrusion. Ces domaines cibles devront être vérifiés avant de pouvoir être utilisés dans un test de pénétration. Pour plus d'informations sur la vérification des domaines cibles, voir the section called “Activer le test de pénétration”

Conditions préalables

Avant de commencer, assurez-vous de disposer des éléments suivants :

1. Test de pénétration activé (voirthe section called “Activer le test de pénétration”)

Gérer les ressources du domaine cible

- Accédez à la page de présentation des domaines cibles.
- Vous devriez voir toutes les ressources du domaine cible associées à votre compte
  - Si aucun domaine cible n'est associé à votre compte, suivez les étapes décrites the section called “Activer le test de pénétration” pour créer et vérifier un domaine cible
- Les domaines cibles peuvent être réutilisés entre les espaces d'agents et le statut de vérification du partage
  - Pour ajouter un domaine cible existant à un espace d'agent, accédez à l'onglet Test de pénétration de l'espace d'agent. Sélectionnez Ajouter un domaine et choisissez le domaine souhaité sous Sélectionner parmi les domaines déjà enregistrés disponibles dans le champ Nom de domaine
  - Les domaines cibles doivent être associés à un espace d'agent avant de pouvoir être utilisés dans un test d'intrusion
- La suppression d'un domaine d'un espace agent ne supprime pas le domaine. Le domaine cible associé peut être définitivement supprimé de la page d'aperçu des domaines cibles

Vérifier les domaines cibles

Pour qu'un domaine cible soit utilisé dans un test de pénétration, il doit d'abord être vérifié à l'aide de l'une des méthodes ci-dessous :

- Route 53 domaines (même compte AWS) : choisissez la One-click vérification. AWS Security Agent crée automatiquement l'enregistrement DNS et effectue la vérification.

- DNS TXT (autres fournisseurs DNS) : copiez le jeton de vérification, ajoutez l'enregistrement TXT auprès de votre bureau d'enregistrement DNS, puis sélectionnez le domaine et choisissez Vérifier.
- Route HTTP : placez le jeton de vérification sur le chemin de route requis sur votre serveur Web, puis sélectionnez le domaine et choisissez Vérifier. Pour en savoir plus, consultez the section called "Activer un domaine d'application pour les tests de pénétration".
- VPC privé : vérifie que l'adresse IP du domaine cible se situe dans une plage d'adresses CIDR privées (voir la liste des plages the section called "Connect l'agent aux ressources VPC privées" d'adresses CIDR privées). Le nom de domaine du point de terminaison cible du test d'intrusion doit correspondre au nom de domaine complet configuré pour la vérification. Utilisable uniquement pour les tests de pénétration de VPC privés

> **Note**
>
> Pour la vérification DNS TXT, HTTP Route et Route 53, les sous-domaines d'un domaine vérifié sont automatiquement couverts et ne nécessitent pas de vérification séparée. Pour la vérification d'un VPC privé, chaque domaine doit être vérifié individuellement.

Gérer les exigences de sécurité

Définissez les exigences de sécurité qu'AWS Security Agent évalue lors de la conception et de la révision du code, à l'aide de AWS-managed packs, de packs personnalisés ou d'exigences importées à partir de votre propre documentation.

Gérer les exigences de sécurité

Organisez les exigences de sécurité utilisées par AWS Security Agent pour analyser vos applications dans des packs d'exigences de sécurité. Un pack est un ensemble d'exigences de sécurité. Vous pouvez activer les packs AWS gérés, créer vos propres packs personnalisés et définir les exigences relatives à un pack personnalisé en téléchargeant votre documentation de sécurité.

Présentation de

Une exigence de sécurité définit une norme ou une politique de sécurité par rapport à laquelle AWS Security Agent évalue votre application lors des révisions de conception et de code. Lorsqu'un design ou un code ne répond pas à une exigence, AWS Security Agent signale une constatation. Chaque

exigence de sécurité fait partie d'un pack d'exigences de sécurité. Les exigences de sécurité sont partagées entre tous les espaces d'agent et évaluées lors des révisions de conception et de code.

AWS Security Agent propose deux types de packs, présentés dans des onglets distincts :

- Packs d'exigences de sécurité gérés : packs d'exigences de sécurité AWS fournis sur la base des normes du secteur et des meilleures pratiques. Vous pouvez activer ces packs instantanément pour les évaluer par rapport aux politiques de sécurité courantes sans configuration personnalisée. Les exigences d'un pack géré sont en lecture seule. Vous pouvez utiliser une exigence AWS gérée comme modèle pour une exigence personnalisée. Pour obtenir la liste des packs gérés disponibles, consultez la section Packs d'exigences de sécuritéAWS gérés.
- Packs d'exigences de sécurité personnalisés : packs que vous créez pour appliquer les politiques et normes spécifiques de votre organisation. Vous créez les exigences dans un pack personnalisé à partir de zéro, vous personnalisez les exigences AWS gérées comme point de départ ou vous les générez en téléchargeant votre documentation de sécurité.

> **Note**
>
> Les packs de cadres de conformité sont conçus pour aider à identifier les exigences de sécurité susceptibles d'être pertinentes pour la conformité à certains cadres. Ils n'évaluent pas votre conformité et ne garantissent pas que vous réussirez un audit.

Vous activez et désactivez les packs en tant qu'unité. Lorsqu'un pack est activé, AWS Security Agent évalue vos applications par rapport aux exigences de ce pack lors de la conception et de la révision du code.

> **Note**
>
> L'activation ou la désactivation d'un pack s'applique aux nouvelles révisions de conception et aux révisions de code. Les avis existants ne sont pas affectés.

Activer ou désactiver un pack géré

Activez un pack AWS géré pour évaluer vos applications par rapport à un ensemble d'exigences de sécurité AWS maintenues. Désactivez-le lorsque vous n'en avez plus besoin.

1. Dans la AWS console, accédez à AWS Security Agent.
2. Dans le volet de navigation, sélectionnez Exigences de sécurité.
3. Choisissez l'onglet Packs d'exigences de sécurité gérés.
4. Sélectionnez le pack que vous souhaitez activer ou désactiver.
5. Effectuez l'une des actions suivantes :
   a. Pour activer le pack, choisissez Activer le pack.
   b. Pour désactiver le pack, choisissez Désactiver le pack.

> **Tip**
>
> Choisissez un pack pour consulter les exigences de sécurité qu'il contient. Choisissez une exigence pour consulter sa définition complète, y compris son applicabilité, ses critères de conformité et ses conseils de correction.

Créez un pack personnalisé

Créez un pack personnalisé pour regrouper les exigences de sécurité spécifiques à votre organisation. Après avoir créé le pack, ajoutez-y des exigences manuellement, personnalisez une exigence AWS gérée ou téléchargez des documents pour générer des exigences.

1. Dans la AWS console, accédez à AWS Security Agent.
2. Dans le volet de navigation, sélectionnez Exigences de sécurité.
3. Choisissez l'onglet Packs d'exigences de sécurité personnalisés.
4. Choisissez Créer un pack d'exigences de sécurité.
5. Entrez le nom du pack d'exigences de sécurité et une description facultative.
6. Choisissez Créer un pack d'exigences de sécurité.

> **Note**
>
> Après avoir créé un pack, vous pouvez ajouter ou télécharger des documents sources afin de définir les exigences de sécurité de votre pack.

Ajouter une exigence de sécurité manuellement

Ajoutez une exigence de sécurité à un pack personnalisé pour définir une norme de sécurité que AWS Security Agent applique.

1. Dans la AWS console, accédez à AWS Security Agent.
2. Dans le volet de navigation, sélectionnez Exigences de sécurité.
3. Choisissez l'onglet Packs d'exigences de sécurité personnalisées, puis choisissez le pack auquel vous souhaitez ajouter une exigence.
4. Choisissez Ajouter une exigence manuellement.
5. Configurez les champs suivants :
   a. Nom de l'exigence de sécurité — Entrez un nom descriptif identifiant le contrôle de sécurité, par exemple `enforce-encryption-at-rest` (80 caractères maximum).
   b. Description — Fournissez une brève description de ce que cette exigence de sécurité vérifie (500 caractères maximum).
   c. Applicabilité — Décrivez les scénarios, les types de systèmes ou les conditions dans lesquels cette exigence de sécurité doit être évaluée. Incluez les scénarios dans lesquels l'exigence doit être marquée NOT_APPLICABLE (maximum 10 000 caractères).
   d. Critères de conformité — Définissez ce qui constitue la conformité par rapport à la non-conformité pour cette exigence de sécurité. Fournissez les indicateurs, les exemples et les détails techniques que AWS Security Agent recherche lorsqu'il évalue la conformité (10 000 caractères maximum).
   e. Conseils de correction (facultatif) — Fournissez des conseils sur la manière de corriger les violations, y compris des liens vers la documentation ou les normes internes de votre organisation (10 000 caractères maximum).
6. Effectuez l'une des actions suivantes :
   a. Pour créer l'exigence sans l'activer, choisissez Créer une exigence de sécurité.
   b. Pour créer l'exigence et l'activer, choisissez Créer et activer l'exigence de sécurité.

> **Note**
>
> Une exigence est évaluée lors des examens de sécurité uniquement lorsque le pack qui la contient est activé. Pour contrôler si un pack est évalué, activez ou désactivez le pack.

Personnalisez un AWS-exigence de sécurité gérée

Créez une exigence de sécurité personnalisée qui utilise une exigence AWS gérée comme point de départ. AWS Security Agent préremplit les détails des exigences à partir de l'exigence gérée, et vous les modifiez pour les adapter à votre organisation.

1. Dans la AWS console, accédez à AWS Security Agent.
2. Dans le volet de navigation, sélectionnez Exigences de sécurité.
3. Choisissez l'onglet Packs d'exigences de sécurité personnalisés, puis choisissez le pack personnalisé auquel ajouter l'exigence.
4. Choisissez Créer une exigence de sécurité personnalisée.
5. Pour préremplir le formulaire, dans la section Personnaliser une exigence de sécurité AWS gérée, recherchez et sélectionnez une exigence AWS gérée à utiliser comme modèle.
6. Modifiez l'un des champs en fonction des besoins de votre organisation.
7. Effectuez l'une des actions suivantes :
   a. Pour créer l'exigence sans l'activer, choisissez Créer une exigence de sécurité.
   b. Pour créer et activer immédiatement l'exigence, choisissez Créer et activer l'exigence de sécurité.

> **Note**
>
> La personnalisation d'une exigence AWS gérée crée une exigence de sécurité personnalisée indépendante. Les modifications ultérieures apportées à l'exigence AWS-managed n'affectent pas votre version personnalisée.

Générez des exigences en téléchargeant des documents

Générez les exigences de sécurité pour un pack personnalisé à partir de votre documentation de sécurité existante au lieu de rédiger chaque exigence à la main. AWS L'agent de sécurité lit les documents que vous téléchargez, identifie le contenu pertinent pour la sécurité et génère des exigences structurées que vous pouvez consulter et modifier. Pour la procédure complète, voir Générer des exigences de sécurité à partir de documents. Pour obtenir des conseils sur les éléments à inclure dans les documents que vous chargez, voir Préparer les documents pour la génération d'exigences.

> **Important**
>
> Le téléchargement de nouveaux documents sources régénère toutes les exigences du pack. Toutes les exigences existantes, y compris celles que vous avez ajoutées manuellement, sont remplacées.

Modifier une exigence de sécurité personnalisée

Modifiez une exigence de sécurité personnalisée pour mettre à jour sa définition, ses critères ou ses instructions de correction. Vous ne pouvez pas modifier les exigences dans un pack AWS géré.

1. Dans la AWS console, accédez à AWS Security Agent.
2. Dans le volet de navigation, sélectionnez Exigences de sécurité.
3. Choisissez l'onglet Packs d'exigences de sécurité personnalisées, puis choisissez le pack contenant l'exigence.
4. Sélectionnez l'exigence que vous souhaitez modifier, puis choisissez Modifier l'exigence de sécurité personnalisée.
5. Mettez à jour les champs d'exigences selon les besoins. Le nom de l'exigence de sécurité ne peut pas être modifié après sa création.
6. Choisissez Mettre à jour les exigences de sécurité.

> **Note**
>
> Les modifications apportées à une exigence de sécurité s'appliquent aux nouvelles révisions de conception et aux révisions de code. Les avis existants ne sont pas affectés.

Activer ou désactiver un pack

Activez ou désactivez un pack d'exigences de sécurité pour contrôler si AWS Security Agent évalue les exigences qu'il contient. Vous activez et désactivez les packs en tant qu'unité.

1. Dans la AWS console, accédez à AWS Security Agent.
2. Dans le volet de navigation, sélectionnez Exigences de sécurité.
3. Choisissez l'onglet correspondant au type de pack, puis sélectionnez le pack.

4. Effectuez l'une des actions suivantes :
   a. Pour activer le pack, choisissez Activer le pack.
   b. Pour désactiver le pack, choisissez Désactiver le pack.

> **Note**
>
> Lorsqu'un pack est activé, les exigences du pack sont évaluées lors des examens de sécurité. Lorsqu'un pack est désactivé, ses exigences ne sont pas évaluées.

Supprimer une exigence de sécurité personnalisée

Supprimez une exigence de sécurité personnalisée lorsque vous ne souhaitez plus que AWS Security Agent l'évalue.

1. Dans la AWS console, accédez à AWS Security Agent.
2. Dans le volet de navigation, sélectionnez Exigences de sécurité.
3. Choisissez l'onglet Packs d'exigences de sécurité personnalisées, puis choisissez le pack contenant l'exigence.
4. Sélectionnez une ou plusieurs exigences de sécurité, puis choisissez Supprimer les exigences de sécurité.
5. Confirmez la suppression.

> **Note**
>
> Lorsque vous supprimez les exigences de sécurité, elles ne sont plus évaluées dans les futures révisions. Les exigences restent visibles dans les révisions précédentes sous forme de résultats en lecture seule.

Bonnes pratiques pour définir les exigences de sécurité

Lorsque vous créez une exigence de sécurité, suivez ces directives pour aider AWS Security Agent à évaluer vos applications avec précision et à fournir des résultats exploitables.

Nom de l'exigence de sécurité : utilisez un nom clair et spécifique qui identifie le contrôle de sécurité. Évitez les termes génériques qui ne reflètent pas l'objectif de l'exigence.

Description — Expliquez ce que le contrôle vérifie et les risques qu'il atténue. Cela permet aux utilisateurs de comprendre pourquoi l'exigence est importante.

Applicabilité — Décrivez les charges de travail, les types de systèmes ou les conditions dans lesquels l'exigence doit être évaluée. Indiquez à quel moment l'exigence doit être marquée NOT_APPLICABLE, avec des scénarios spécifiques, pour éviter les faux positifs. Des phrases telles que « Ce contrôle s'applique à TOUTES les charges de travail qui... » et « Marquer comme NON APPLICABLE si... » fixent des limites de portée claires.

Critères de conformité — Structurez-le en deux parties : ce qui démontre la conformité et ce qui indique une non-conformité. Soyez précis en ce qui concerne les indicateurs techniques et incluez les cas extrêmes. Commencez par « Un design est conforme s'il démontre... » suivi des détails techniques, puis « Un design n'est pas conforme s'il... » avec les modèles indiquant une violation.

Conseils de correction — Fournissez des conseils avec des détails techniques et des exemples de configuration. Incluez des liens vers la documentation interne de votre organisation afin que les développeurs disposent des ressources dont ils ont besoin pour corriger les violations.

Étapes suivantes

Après avoir configuré vos packs d'exigences de sécurité :

- Créez une revue de conception ou une révision de code pour évaluer votre application par rapport aux packs que vous avez activés.
- Activez les tests d'intrusion pour compléter vos révisions de conception et de code.
- Accordez aux utilisateurs l'accès à l'application Web AWS Security Agent.

Packs d'exigences de sécurité gérés par AWS

Un pack d'exigences de sécurité AWS géré est un ensemble d'exigences de sécurité qui AWS crée et gère, sur la base des normes du secteur et des meilleures pratiques. Vous activez un pack géré pour évaluer vos applications par rapport à ses exigences lors des révisions de conception et de code, sans avoir à rédiger vous-même les exigences.

Les exigences de sécurité d'un pack géré sont en lecture seule. Vous ne pouvez pas les modifier. Vous pouvez utiliser une exigence AWS gérée comme modèle pour créer une exigence

personnalisée, puis modifier la copie pour l'adapter à votre organisation. Pour plus d'informations, consultez la section Gérer les exigences de sécurité.

AWS met à jour les packs gérés au fil du temps. Lorsque AWS vous ajoutez ou modifiez une exigence dans un pack géré, la modification s'applique à tous les comptes sur lesquels le pack est activé.

> **Note**
>
> Les packs de cadres de conformité sont conçus pour aider à identifier les exigences de sécurité susceptibles d'être pertinentes pour la conformité à certains cadres. Ils n'évaluent pas votre conformité et ne garantissent pas que vous réussirez un audit.

Pack géré par AWS : pack de base ASA

Ensemble d'exigences de sécurité de base qui s'appliquent à la plupart des charges de travail. Ce pack couvre les problèmes courants de sécurité des applications tels que l'authentification et l'autorisation, la protection des données, la journalisation et la validation des entrées. Activez ce pack pour établir une base de sécurité pour vos révisions de conception et de code.

Pack géré par AWS : AWS Well-Architected Pack

Les exigences en matière de sécurité découlent du pilier de sécurité du AWS Well-Architected cadre. Ce pack évalue votre application par rapport AWS aux directives relatives à la protection des données, à la gestion des identités et des autorisations, ainsi qu'à la détection et à la réponse aux événements de sécurité. Pour plus d'informations sur le framework, consultez Security Pillar - AWS Well-Architected Framework.

Pack géré par AWS : pack NIST CSF

Exigences de sécurité dérivées du cadre de cybersécurité (CSF) du NIST. Ce pack évalue votre application par rapport aux domaines de contrôle définis dans le framework, tels que la gestion des identités et des accès, la sécurité des données et les technologies de protection. Activez ce pack pour aligner votre conception et vos révisions de code sur le NIST CSF.

Pack géré par AWS : pack PCI DSS

Exigences de sécurité dérivées de la norme de sécurité des données de l'industrie des cartes de paiement (PCI DSS). Ce pack évalue votre application par rapport aux domaines de contrôle relatifs

au traitement des données des titulaires de cartes, tels que le contrôle d'accès, le chiffrement des données en transit et au repos, et la journalisation. Activez ce pack pour aligner vos révisions de conception et de code sur la norme PCI DSS.

Générez des exigences de sécurité à partir de documents

Générez les exigences de sécurité pour un pack personnalisé en téléchargeant votre documentation de sécurité existante. AWS Security Agent lit les documents que vous téléchargez, identifie le contenu pertinent pour la sécurité et génère des exigences de sécurité structurées avec des critères d'applicabilité, de conformité et des conseils de correction. Vous pouvez consulter et modifier les exigences générées avant qu'elles ne soient utilisées dans les révisions.

Utilisez-le au lieu de rédiger chaque exigence à la main alors que vous disposez déjà de politiques, de normes ou de directives de sécurité documentées. Pour obtenir des conseils sur les éléments à inclure dans les documents que vous chargez, voir Préparer les documents pour la génération d'exigences.

Formats de fichier pris en charge

Vous pouvez télécharger les formats de fichier suivants :

- DOC
- DOCX
- MD
- PDF
- TXT

Générer des exigences

1. Dans la AWS console, accédez à AWS Security Agent.
2. Dans le volet de navigation, sélectionnez Exigences de sécurité.
3. Choisissez l'onglet Packs d'exigences de sécurité personnalisés.
4. Créez un pack ou choisissez un pack personnalisé existant pour lequel générer les exigences.
5. Choisissez Choisir des fichiers ou glissez et déposez vos documents dans la zone de téléchargement.
6. Choisissez Générer les exigences.

7. Attendez que l'agent de AWS sécurité traite les documents. La génération s'exécute en arrière-plan et peut prendre quelques minutes pour les fichiers volumineux. Vous ne pouvez pas lancer un autre téléchargement pour le pack pendant que la génération est en cours.
8. Passez en revue les exigences de sécurité générées. Modifiez, supprimez ou ajoutez des exigences selon vos besoins. Activez le pack lorsque vous souhaitez que AWS Security Agent évalue ses exigences lors des révisions de sécurité.

> **Note**
>
> AWS Security Agent génère des exigences au niveau de la charge de travail et se concentre sur le contenu pertinent pour la sécurité de vos documents. Le nombre d'exigences qu'il génère dépend du contenu que vous fournissez. Passez en revue les exigences générées pour confirmer qu'elles reflètent votre intention.

Remplacez les exigences par un nouveau téléchargement

Le téléchargement de nouveaux documents sources régénère les exigences relatives à un pack.

> **Important**
>
> Lorsque vous chargez de nouveaux documents sources dans un pack, AWS Security Agent régénère toutes les exigences relatives à ce pack. Toutes les exigences existantes, y compris celles que vous avez ajoutées manuellement, sont remplacées. Pour conserver vos exigences actuelles, ne téléchargez pas de nouveaux documents.

1. Dans la AWS console, accédez à AWS Security Agent.
2. Dans le volet de navigation, sélectionnez Exigences de sécurité.
3. Choisissez l'onglet Packs d'exigences de sécurité personnalisées, puis choisissez le pack.
4. Lancez un nouveau téléchargement et reconnaissez que le téléchargement de nouveaux documents sources remplace les exigences existantes.
5. Choisissez vos fichiers, puis sélectionnez Générer les exigences.

Étapes suivantes

- Vérifiez et activez les exigences générées. Consultez la section Gérer les exigences de sécurité.
- Créez une revue de conception ou une révision de code pour évaluer votre application par rapport au pack.

Préparer les documents pour la génération d'exigences

Lorsque vous générez des exigences de sécurité à partir de documents, AWS Security Agent lit vos documents et produit des exigences structurées à partir du contenu pertinent qu'il trouve en matière de sécurité. Vous n'avez pas besoin de formater vos documents d'une manière particulière ni de rédiger au préalable l'applicabilité, les critères de conformité et les conseils de correction. AWS Security Agent les obtient à partir du contenu que vous fournissez. Téléchargez la documentation de sécurité dont vous disposez déjà, rédigée avec vos propres mots.

Cette page décrit les éléments à inclure pour que AWS Security Agent génère des exigences précises et utiles. Pour la procédure de téléchargement et les limites de fichiers, voir Générer des exigences de sécurité à partir de documents.

Ce qu'il faut inclure

AWS L'agent de sécurité recherche le contenu qui décrit vos attentes en matière de sécurité. Les documents qui couvrent les sujets suivants présentent les exigences les plus strictes :

- Contrôle d'accès et autorisation
- Authentification
- Protection et chiffrement des données
- Sécurité du réseau
- Journalisation et audit
- Intervention en cas d'incidents
- Gestion des vulnérabilités et des correctifs
- Obligations de conformité applicables à vos charges de travail

Les bons documents sources incluent les politiques de sécurité, les normes d'ingénierie, les catalogues de contrôle, les directives d'architecture et les normes de codage sécurisées.

Écrire au niveau de la charge de travail

AWS Security Agent génère des exigences qui s'appliquent à une charge de travail ou à une application individuelle, la même portée qu'il évalue lors de la conception et de la révision du code. Le contenu qui décrit comment créer et exploiter une charge de travail sécurisée génère des exigences. Organization-wide les sujets de gouvernance, tels que la stratégie multi-comptes, la gestion des utilisateurs root et la configuration de la journalisation au niveau du compte, ne relèvent pas de ce champ d'application et ne génèrent pas d'exigences de charge de travail.

Décrivez le résultat, pas une seule mise en œuvre

Indiquez le résultat de sécurité que vous attendez plutôt qu'un seul produit ou configuration prescrit. AWS Security Agent génère des exigences qui se concentrent sur les capacités de sécurité nécessaires et permettent plusieurs implémentations valides. Par exemple, « les données au repos sont cryptées » génère une exigence plus claire et plus largement applicable qu'une déclaration désignant un service ou un paramètre spécifique.

Soyez précis sur ce à quoi ressemble une belle apparence

Plus vos documents décrivent le comportement attendu de manière précise, plus AWS Security Agent est en mesure de définir les critères de conformité. Dans la mesure du possible, décrivez ce que démontre une conception conforme et ce qui indique une violation. Les déclarations vagues ou purement ambitieuses génèrent des exigences moins nombreuses et plus faibles que les déclarations concrètes liées à la charge de travail.

Passez en revue ce que vous recevez en retour

Chaque exigence générée inclut un nom, une applicabilité, des critères de conformité et des conseils de correction que AWS Security Agent a dérivés de vos documents. Passez en revue les exigences générées, modifiez celles qui doivent être affinées et activez celles que vous souhaitez que AWS Security Agent évalue. Pour plus d'informations, consultez la section Gérer les exigences de sécurité.

Gérer les utilisateurs et les accès

Contrôlez qui peut accéder à chaque espace d'agent et configurez les rôles IAM et les clés de chiffrement utilisés par AWS Security Agent.

Autoriser les utilisateurs à accéder à l'application Web AWS Security Agent

AWS Security Agent propose deux méthodes permettant aux utilisateurs d'accéder à l'application Web, en fonction de la façon dont vous avez configuré votre espace agent lors de l'installation.

Vue d'ensemble des méthodes d'accès

IAM Identity Center (SSO) : si vous avez activé IAM Identity Center lors de la création de votre espace agent, les utilisateurs peuvent accéder à l'application Web directement via SSO. Vous assignez des utilisateurs à l'espace agent via la console AWS Security Agent, et les utilisateurs se connectent à l'aide de leurs informations d'identification Identity Center.

Accès administrateur : les utilisateurs ayant accès à la console AWS peuvent lancer l'application Web via un lien d'accès administrateur sur la page de présentation de l'espace agent dans l'AWS Management Console.

Accorder l'accès avec IAM Identity Center (SSO)

Si vous avez configuré votre espace agent avec IAM Identity Center, vous pouvez attribuer des utilisateurs à l'espace agent à l'aide de la console AWS Security Agent.

Attribuez des utilisateurs via la console AWS Security Agent

1. Dans la console de gestion des agents de sécurité AWS, accédez à votre espace d'agent.
2. Sélectionnez l'onglet Web app.
3. Dans le tableau Utilisateurs, sélectionnez Ajouter des utilisateurs.
4. Sélectionnez les utilisateurs existants dans IAM Identity Center ou créez-en de nouveaux.
5. Confirmez les affectations des utilisateurs.

> **Tip**
>
> Les utilisateurs affectés à l'espace agent peuvent accéder à l'application Web en se connectant via IAM Identity Center à l'aide de leurs informations d'identification SSO.

Accédez à l'application Web avec SSO

Une fois les utilisateurs affectés à l'espace agent :

1. Les utilisateurs accèdent à l'URL de l'application Web pour l'espace agent.

> **Tip**
>
> Trouvez l'URL de l'application Web sur la page détaillée de l'espace agent de la console AWS Security Agent en sélectionnant Copier l'URL de l'application Web. Les utilisateurs doivent ajouter cette URL à leurs favoris pour y accéder facilement.

2. Les utilisateurs se connectent à l'aide de leurs identifiants SSO.
3. Après l'authentification, les utilisateurs peuvent sélectionner l'espace agent et commencer à effectuer des évaluations de sécurité.

Accorder l'accès avec IAM-only accès

Si vous avez configuré l' IAM-only accès à votre espace agent, les utilisateurs disposant d'un accès à la console AWS peuvent lancer l'application Web via un lien d'accès administrateur.

Utilisez le lien d'accès administrateur

1. Connectez-vous à la console AWS Security Agent.
2. Accédez à l'espace agent auquel vous souhaitez accéder.
3. Dans l'onglet Application Web de la page d'accueil d'Agent Space, cliquez sur le bouton d'accès administrateur pour lancer l'application Web.
4. L'application Web s'ouvre dans un nouvel onglet et l'utilisateur est automatiquement authentifié.

> **Note**
>
> Le lien d'accès administrateur n'est disponible que pour les utilisateurs déjà authentifiés sur la console AWS avec les autorisations AWS Security Agent appropriées. Cette méthode ne nécessite pas de configuration du centre d'identité IAM.

Étapes suivantes

Après avoir accordé aux utilisateurs l'accès à l'application Web :

- Les utilisateurs peuvent créer et gérer des configurations et des exécutions de tests d'intrusion

- Les utilisateurs peuvent créer et gérer des révisions de conception
- Les utilisateurs peuvent consulter les résultats de sécurité et les conseils de correction
- Configuration des préférences de notification pour les résultats de sécurité

Création d'un rôle IAM pour AWS Security Agent

AWS Security Agent utilise les rôles IAM de trois manières :

1. Rôle de l'application : utilisé lors de la création de l'application AWS Security Agent. Pour les cas d'utilisation du centre d'identité IAM et du lien d'accès administrateur, le service assume ce rôle pour accorder aux WebApp utilisateurs les autorisations nécessaires pour interagir avec les API d'AWS Security Agent.
2. Rôle du service de test d'intrusion : spécifié lors de la création des espaces d'agent sous forme de liste des rôles disponibles. WebApp Les utilisateurs sélectionneront ultérieurement l'un de ces rôles lors de la création d'un test d'intrusion. Le service AWS Security Agent assume ce rôle pour accéder à vos ressources AWS pendant les tests.
3. Rôle d'acteur : utilisé pour authentifier et autoriser les demandes adressées à votre application Web cible (par exemple, les API AWS API Gateway). Ces rôles sont fournis lors de la création de l'espace agent. L'agent AWS Security Agent joue le rôle d'acteur pour interagir avec votre application cible.

Rôle de l'application

Le rôle d'application est utilisé lors de la création de votre application AWS Security Agent dans le service. Pour les scénarios d'authentification du centre d'identité IAM et du lien d'accès administrateur, le service AWS Security Agent assume ce rôle afin d'accorder WebApp aux utilisateurs les autorisations nécessaires pour interagir avec les API d'AWS Security Agent.

Autorisations nécessaires

Ce rôle nécessite des autorisations pour :

- Invoquer les opérations de l'API AWS Security Agent
- Lire et écrire les données de configuration des applications
- Accès aux informations de session utilisateur
- Gérer les jetons d'authentification pour WebApp les utilisateurs

Stratégie d'approbation

La politique de confiance doit permettre au service AWS Security Agent d'assumer ce rôle :

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "securityagent.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

Stratégie d'autorisations

Le rôle doit inclure des autorisations pour :

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "securityagent:GetApplication",
        "securityagent:UpdateApplication",
        "securityagent:ListAgentInstances",
        "securityagent:CreatePentestSession"
      ],
      "Resource": "arn:aws:securityagent:*:*:application/*"
    }
  ]
}
```

> **Note**
>
> Personnalisez les autorisations en fonction des exigences spécifiques de votre application et du principe du moindre privilège.

Rôle du service de test de pénétration

Le rôle du service de test de pénétration est spécifié lors de la création d'espaces d'agent sous la forme d'une liste de rôles disponibles. Lorsque WebApp les utilisateurs créent un test d'intrusion, ils sélectionnent l'un de ces rôles. Le service AWS Security Agent assume ensuite ce rôle pour accéder à vos ressources AWS et les tester.

Autorisations nécessaires

Ce rôle a besoin d'autorisations pour accéder à vos ressources AWS et les analyser lors des tests d'intrusion :

- Lire et décrire les configurations VPC et la topologie du réseau
- Inspectez les instances EC2, les groupes de sécurité et les ACL réseau
- Analyser les politiques IAM et les autorisations de ressources
- Lire CloudWatch les journaux et les statistiques
- Accédez aux configurations des services AWS pertinentes pour les tests de sécurité

Stratégie d'approbation

La politique de confiance doit permettre au service AWS Security Agent d'assumer ce rôle pour les opérations de test d'intrusion :

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "securityagent.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "sts:ExternalId": "your-external-id"
        }
      }
    }
  ]
```

```
}
```

> **Note**
>
> Utilisez un identifiant externe pour renforcer la sécurité lorsque vous autorisez l'accès entre comptes ou services.

Stratégie d'autorisations

Le rôle doit inclure un accès en lecture seule à vos ressources AWS. Envisagez d'utiliser les politiques gérées suivantes :

- `SecurityAudit`- Politique gérée par AWS pour l'audit de sécurité
- `ViewOnlyAccess`- Read-only accès à la plupart des services AWS

Ou créez une politique personnalisée avec des autorisations spécifiques :

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ec2:Describe*",
        "vpc:Describe*",
        "iam:Get*",
        "iam:List*",
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams",
        "cloudwatch:Describe*",
        "cloudwatch:Get*",
        "cloudwatch:List*",
        "s3:GetObject",
        "s3:ListBucket"
      ],
      "Resource": "*"
    }
  ]
}
```

> **Important**
>
> N'accordez que les autorisations minimales requises pour la portée de vos tests d'intrusion. Passez en revue et ajustez les autorisations en fonction des services AWS que vous souhaitez inclure dans les tests de sécurité.

Rôle d'acteur

Le rôle d'acteur est utilisé pour authentifier et autoriser les demandes adressées à votre application Web cible lors des tests d'intrusion. Ces rôles sont fournis lors de la création de l'espace agent, et l'agent AWS Security Agent suppose qu'ils interagissent avec les points de terminaison de votre application cible (tels que les API AWS API Gateway, les URL des fonctions Lambda ou AWS-hosted d'autres applications).

Autorisations nécessaires

Ce rôle nécessite des autorisations pour :

- Invoquer les points de terminaison API Gateway
- Exécuter les fonctions Lambda
- Accédez à des ressources AWS spécifiques aux applications
- Authentifiez-vous à l'aide des mécanismes d'authentification de votre application cible
- Effectuez des opérations HTTP sur les points de terminaison de votre application

Stratégie d'approbation

La politique de confiance doit permettre au service d'agent de sécurité AWS d'assumer ce rôle :

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "securityagent.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
```

```
      "Condition": {
        "StringEquals": {
          "sts:ExternalId": "your-external-id"
        }
      }
    }
  ]
}
```

Stratégie d'autorisations

Les autorisations dépendent de l'architecture de votre application cible. Voici des exemples de scénarios courants :

Pour les applications API Gateway

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "execute-api:Invoke"
      ],
      "Resource": "arn:aws:execute-api:us-east-1:*:your-api-id/*"
    }
  ]
}
```

Pour les URL des fonctions Lambda

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "lambda:InvokeFunctionUrl",
        "lambda:InvokeFunction"
      ],
      "Resource": "arn:aws:lambda:us-east-1:*:function:your-function-name"
    }
  ]
```

```
}
```

Pour Application Load Balancer avec authentification Cognito

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "cognito-idp:InitiateAuth",
        "cognito-idp:RespondToAuthChallenge"
      ],
      "Resource": "arn:aws:cognito-idp:us-east-1:*:userpool/your-user-pool-id"
    }
  ]
}
```

> **Important**
>
> Configurez les autorisations de rôle d'acteur en fonction des exigences d'authentification et d'autorisation de votre application cible. Le rôle doit avoir le même niveau d'accès que les utilisateurs ou les services que l'agent de sécurité simulera lors des tests d'intrusion.

Clés gérées par le client pour AWS Security Agent

Par défaut, AWS Security Agent chiffre toutes les données inactives à l'aide de clés de AWS chiffrement gérées. Vous pouvez éventuellement utiliser une clé gérée par le client du service de gestion des AWS clés (AWS KMS) pour chiffrer vos données, ce qui vous donne un contrôle total sur les clés de chiffrement qui protègent vos ressources.

AWS Security Agent prend en charge les clés gérées par le client au niveau des ressources. Lorsque vous créez une ressource de haut niveau telle qu'un espace agent ou une intégration, vous pouvez spécifier une clé KMS pour chiffrer toutes les données appartenant à cette ressource et à ses sous-ressources. Par exemple, la spécification d'une clé gérée par le client lors de la création d'un espace agent chiffre toutes les données associées à cet espace agent, y compris les configurations de l'espace agent, les configurations des tests de pénétration, les tâches et les détails d'exécution, les résultats de sécurité, les points de terminaison découverts et les captures d'écran. Vous pouvez également fournir des AWS ressources déjà chiffrées avec votre propre clé gérée par le client, telles

que des compartiments S3, des groupes de CloudWatch journaux Logs ou des secrets Secrets Manager. Pour connaître les autorisations KMS requises, consultezthe section called "Autorisations KMS requises".

Comment fonctionnent les clés gérées par le client

AWS L'agent de sécurité utilise le jeu de clés hiérarchique AWS KMS pour chiffrer vos données à l'aide de clés gérées par le client. Lorsque vous spécifiez une clé KMS lors de la création d'une ressource, le service crée une clé de branche protégée par votre clé KMS et la stocke dans un magasin de DynamoDB-based clés Amazon. Pour chaque opération de chiffrement, le jeu de clés hiérarchique déduit une clé d'encapsulation unique à partir de la clé de branche active, qui chiffre une clé de chiffrement des données unique pour chaque demande.

Le porte-clés hiérarchique offre les avantages suivants :

- Per-resource étendue du chiffrement : chaque ressource de niveau supérieur possède sa propre clé de branche, de sorte que les données des différentes ressources sont chiffrées sous des clés distinctes.
- Rotation automatique des clés : AWS Security Agent fait régulièrement pivoter les clés de branche. Après la rotation, les nouvelles données sont chiffrées avec la nouvelle version de clé de branche, tandis que les anciennes versions sont conservées pour déchiffrer les données précédemment chiffrées.

Contexte de chiffrement

AWS L'agent de sécurité utilise le contexte de chiffrement dans toutes les opérations cryptographiques effectuées avec votre clé KMS. Le contexte de chiffrement est un ensemble de paires clé-valeur non secrètes qui fournit des données authentifiées supplémentaires pour l'opération de chiffrement.

La clé de contexte de chiffrement suit le format`aws:securityagent:_<resource-type>_`, où *`<resource-type>`* est le type de ressource cryptée (par exemple, `agent-space` ou`integration`). La valeur est le Amazon Resource Name (ARN) de la ressource.

> **Note**
>
> Pour les intégrations, la clé de contexte de chiffrement inclut le `aws-crypto-ec:` préfixe, ce qui donne le format. `aws-crypto-ec:aws:securityagent:integration`

Vous pouvez utiliser le contexte de chiffrement pour étendre votre politique de clé KMS à des types de ressources spécifiques. Pour de plus amples informations, veuillez consulter the section called "Autorisations KMS requises".

Default encryption (Chiffrement par défaut)

Lorsque vous créez une ressource sans spécifier de clé gérée par le client, AWS Security Agent chiffre la ressource à l'aide de clés de AWS chiffrement gérées fournies par les services de stockage sous-jacents (Amazon DynamoDB et Amazon S3). Aucune configuration supplémentaire n'est requise pour le chiffrement par défaut.

Clé KMS par défaut pour les applications

Vous pouvez définir une clé KMS par défaut au niveau de l'application. Lorsqu'une clé KMS par défaut est configurée, AWS Security Agent l'utilise comme solution de secours pour les nouveaux espaces d'agent et les intégrations lorsque vous ne spécifiez pas explicitement de clé KMS lors de la création de ressources.

Pour définir une clé KMS par défaut, spécifiez le `defaultKmsKeyId` paramètre lors de la création ou de la mise à jour de votre application à l'aide de la AWS CLI ou du SDK. La console vous invite à spécifier une clé KMS par défaut lors de la configuration de l'application.

Lorsque vous spécifiez explicitement une clé KMS lors de la création d'une ressource, celle-ci a priorité sur la valeur par défaut au niveau de l'application.

Conditions préalables

Avant de configurer une clé gérée par le client, remplissez les conditions préalables suivantes :

- Créez une clé KMS de chiffrement symétrique dans AWS KMS. La clé doit répondre aux exigences suivantes :
  - Type de clé : symétrique
  - Utilisation de la clé : crypter et déchiffrer
  - Spécification clé : `SYMMETRIC_DEFAULT`
  - État de la clé : Activé

    Pour obtenir des instructions, consultez la section Création de clés dans le guide du développeur du service de gestion des AWS clés.

- Configurez la politique des clés KMS et les politiques IAM pour accorder à AWS Security Agent les autorisations requises. Pour en savoir plus, consultez the section called "Autorisations KMS requises".

Autorisations KMS requises

AWS L'agent de sécurité nécessite des autorisations KMS dans deux scénarios :

- Chiffrement des données dans AWS Security Agent : lorsque vous spécifiez une clé gérée par le client pour un espace agent ou une intégration, le service a besoin d'autorisations pour utiliser cette clé pour effectuer des opérations cryptographiques sur vos données.
- Utilisation CMK-encrypted AWS des ressources : lorsque vous fournissez des AWS ressources chiffrées à l'aide d'une clé gérée par le client (telles que des compartiments S3, CloudWatch des groupes de journaux Logs ou des secrets de Secrets Manager), le service a besoin d'autorisations pour utiliser ces clés afin d'accéder aux ressources chiffrées.

AWS L'agent de sécurité accède à votre clé KMS en utilisant différentes identités en fonction de l'opération :

- AWS Opérations de la console de gestion : lorsque les administrateurs créent ou gèrent des ressources dans la console de AWS gestion (par exemple, en créant un espace agent ou en mettant à jour une application), le service utilise le rôle d'administrateur pour appeler AWS KMS.
- Opérations des applications Web : lorsque les utilisateurs d'IAM Identity Center accèdent aux données via l'application Web AWS Security Agent (par exemple, en consultant les résultats d'un test d'intrusion ou en démarrant un test d'intrusion), le service utilise le rôle d'application créé lors de la configuration de l'agent de AWS sécurité pour appeler AWS KMS.
- Accès aux ressources fournies par le client : lorsque le service accède aux AWS ressources fournies par le client pendant les tests d'intrusion (telles que les compartiments S3, les groupes de CloudWatch journaux et les secrets de Secrets Manager), il utilise le rôle de service de test d'intrusion pour appeler KMS. AWS
- Flux de travail asynchrones : pour les opérations en arrière-plan exécutées en dehors de toute session utilisateur (par exemple, l'exécution de tests d'intrusion, le traitement de révision du code et la rotation des clés de branche), le service utilise son propre principal de service (`securityagent.amazonaws.com`) pour appeler AWS KMS en votre nom.

Les sections suivantes décrivent les autorisations requises pour chaque identité.

Stratégie de clé

Votre politique de clé KMS doit autoriser l'agent de AWS sécurité à utiliser la clé pour des opérations cryptographiques. Les déclarations de politique clés requises dépendent des types de ressources que vous prévoyez de chiffrer et des CMK-encrypted AWS ressources que vous fournissez au service.

Politique clé pour Agent Spaces

La politique clé suivante accorde à AWS Security Agent les autorisations nécessaires pour chiffrer et déchiffrer les données de l'Agent Space, y compris les résultats des tests d'intrusion et les captures d'écran.

Remplacez les valeurs d'espace réservé suivantes dans la politique :

- *111122223333* — Votre identifiant AWS de compte
- *MyRole* — Le rôle IAM que vous utilisez pour gérer l'agent AWS de sécurité dans la console
- *MyApplicationRole* — Le rôle d'application créé lors de la configuration AWS de l'agent de sécurité
- *us-east-1* — La AWS région dans laquelle vous utilisez AWS Security Agent

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowKeyMetadataValidationForApplicationAndAgentSpaces",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::111122223333:role/MyRole"
      },
      "Action": [
        "kms:DescribeKey"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "kms:ViaService": "securityagent.us-east-1.amazonaws.com"
        }
      }
    },
    {
```

```
      "Sid": "AllowUseOfHierarchicalKeyringForAgentSpaces",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::111122223333:role/MyRole"
      },
      "Action": [
        "kms:GenerateDataKeyWithoutPlaintext",
        "kms:ReEncryptTo",
        "kms:ReEncryptFrom",
        "kms:Decrypt"
      ],
      "Resource": "*",
      "Condition": {
        "StringLike": {
          "kms:EncryptionContext:aws:securityagent:agent-space":
"arn:aws:securityagent:us-east-1:111122223333:agent-space/*"
        },
        "StringEquals": {
          "kms:ViaService": "securityagent.us-east-1.amazonaws.com"
        }
      }
    },
    {
      "Sid": "AllowSynchronousDataAccessForAgentSpaces",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::111122223333:role/MyApplicationRole"
      },
      "Action": [
        "kms:GenerateDataKey",
        "kms:Decrypt"
      ],
      "Resource": "*",
      "Condition": {
        "StringLike": {
          "kms:EncryptionContext:aws:securityagent:agent-space":
"arn:aws:securityagent:us-east-1:111122223333:agent-space/*"
        },
        "StringEquals": {
          "kms:ViaService": "securityagent.us-east-1.amazonaws.com"
        }
      }
    },
    {
```

```
      "Sid": "AllowAsynchronousDataAccessForAgentSpaces",
      "Effect": "Allow",
      "Principal": {
        "Service": "securityagent.amazonaws.com"
      },
      "Action": [
        "kms:GenerateDataKeyWithoutPlaintext",
        "kms:Decrypt",
        "kms:ReEncryptTo",
        "kms:ReEncryptFrom"
      ],
      "Resource": "*",
      "Condition": {
        "StringLike": {
          "kms:EncryptionContext:aws:securityagent:agent-space":
 "arn:aws:securityagent:us-east-1:111122223333:agent-space/*"
        },
        "ArnLike": {
          "aws:SourceArn": "arn:aws:securityagent:us-east-1:111122223333:agent-space/*"
        }
      }
    },
    {
      "Sid": "AllowAsynchronousDataAccessForCodeRemediation",
      "Effect": "Allow",
      "Principal": {
        "Service": "securityagent.amazonaws.com"
      },
      "Action": [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource": "*"
    }
  ]
}
```

Important

Pour effectuer une rotation des clés de branche, votre politique de clés KMS doit accorder `kms:GenerateDataKeyWithoutPlaintextkms:ReEncryptTo`, et `kms:ReEncryptFrom` les autorisations accordées au responsable du service AWS Security Agent (`securityagent.amazonaws.com`), faute de quoi la rotation des clés de branche

échouera. Pour plus d'informations sur les autorisations requises, voir Rotation d'une clé de branche.

Politique clé en matière d'intégrations

La politique clé suivante accorde à AWS Security Agent les autorisations nécessaires pour chiffrer et déchiffrer les données d'intégration, y compris les résultats de la révision du code.

Remplacez les valeurs d'espace réservé suivantes dans la politique :

- *111122223333* — Votre identifiant AWS de compte
- *MyRole* — Le rôle IAM que vous utilisez pour gérer l'agent AWS de sécurité dans la console
- *us-east-1* — La AWS région dans laquelle vous utilisez AWS Security Agent

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowKeyAccessValidationForIntegrations",
      "Effect": "Allow",
      "Principal": {
          "AWS": "arn:aws:iam::111122223333:role/MyRole"
      },
      "Action": [
        "kms:GenerateDataKeyWithoutPlaintext",
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:ReEncryptTo",
        "kms:ReEncryptFrom"
      ],
      "Resource": "*",
      "Condition": {
        "StringLike": {
          "kms:EncryptionContext:aws-crypto-ec:aws:securityagent:integration":
 "arn:aws:securityagent:us-east-1:111122223333:integration/*"
        },
        "StringEquals": {
          "kms:ViaService": "securityagent.us-east-1.amazonaws.com"
        }
      }
```

```
    },
    {
      "Sid": "AllowKeyMetadataValidationForIntegrations",
      "Effect": "Allow",
      "Principal": {
        "Service": "securityagent.amazonaws.com"
      },
      "Action": "kms:DescribeKey",
      "Resource": "*"
    },
    {
      "Sid": "AllowAsynchronousDataAccessForIntegrations",
      "Effect": "Allow",
      "Principal": {
        "Service": "securityagent.amazonaws.com"
      },
      "Action": [
        "kms:GenerateDataKeyWithoutPlaintext",
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:ReEncryptTo",
        "kms:ReEncryptFrom"
      ],
      "Resource": "*",
      "Condition": {
        "ArnLike": {
          "aws:SourceArn": "arn:aws:securityagent:us-east-1:111122223333:integration/*"
        },
        "StringLike": {
          "kms:EncryptionContext:aws-crypto-ec:aws:securityagent:integration":
 "arn:aws:securityagent:us-east-1:111122223333:integration/*"
        }
      }
    }
  ]
}
```

> **Note**
>
> Vous pouvez combiner les déclarations de politique clé du pack d'exigences relatives à l'espace agent, à l'intégration et à la sécurité en une seule politique clé si vous souhaitez utiliser la même clé KMS pour plusieurs types de ressources.

Politique clé pour les packs d'exigences de sécurité

La politique clé suivante accorde à AWS Security Agent les autorisations nécessaires pour chiffrer et déchiffrer les données du pack d'exigences de sécurité. Les packs d'exigences de sécurité n'utilisent pas de rôle d'application Web. La politique utilise deux chemins d'accès :

- Chemin synchrone : lorsque vous appelez l'API, le service utilise vos informations d'identification transférées pour appeler AWS KMS en votre nom (via la `kms:ViaService` condition).
- Chemin asynchrone : pour les opérations asynchrones dans lesquelles les packs peuvent être utilisés, le service utilise son propre principal de service pour appeler directement KMS. AWS

Remplacez les valeurs suivantes dans la politique :

- *111122223333* — Votre identifiant AWS de compte
- *MyRole* — Le rôle IAM que vous utilisez pour appeler les opérations du pack d'exigences de sécurité
- *us-east-1* — La AWS région dans laquelle vous utilisez AWS Security Agent

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowKeyMetadataValidation",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::111122223333:role/MyRole"
      },
      "Action": [
        "kms:DescribeKey"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "kms:ViaService": "securityagent.us-east-1.amazonaws.com"
        }
      }
    },
    {
      "Sid": "AllowUseOfHierarchicalKeyringForSecurityPacks",
      "Effect": "Allow",
```

```
      "Principal": {
        "AWS": "arn:aws:iam::111122223333:role/MyRole"
      },
      "Action": [
        "kms:GenerateDataKeyWithoutPlaintext",
        "kms:ReEncryptTo",
        "kms:ReEncryptFrom",
        "kms:Decrypt"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "kms:ViaService": "securityagent.us-east-1.amazonaws.com"
        },
        "StringLike": {
          "kms:EncryptionContext:aws:securityagent:security-requirement-pack":
 "arn:aws:securityagent:us-east-1:111122223333:security-requirement-pack/*"
        }
      }
    },
    {
      "Sid": "AllowAsynchronousDataAccessForSecurityPacks",
      "Effect": "Allow",
      "Principal": {
        "Service": "securityagent.amazonaws.com"
      },
      "Action": [
        "kms:GenerateDataKeyWithoutPlaintext",
        "kms:Decrypt",
        "kms:ReEncryptTo",
        "kms:ReEncryptFrom"
      ],
      "Resource": "*",
      "Condition": {
        "StringLike": {
          "kms:EncryptionContext:aws:securityagent:security-requirement-pack":
 "arn:aws:securityagent:us-east-1:111122223333:security-requirement-pack/*"
        },
        "ArnLike": {
          "aws:SourceArn": "arn:aws:securityagent:us-east-1:111122223333:security-
requirement-pack/*"
        }
      }
    }
```

```
  ]
}
```

La politique contient trois déclarations :

- AllowKeyMetadataValidation— Des autorisations `kms:DescribeKey` permettant à AWS Security Agent de valider que la clé gérée par le client existe, est activée et utilise un chiffrement symétrique lorsque vous spécifiez une clé CMK lors de la création de ressources. Utilise la `kms:ViaService` condition pour s'assurer que l'appel provient du service.
- AllowUseOfHierarchicalKeyringForSecurityPacks— Accorde `kms:GenerateDataKeyWithoutPlaintext` (création de nouvelles clés de branche), `kms:ReEncryptTo` `kms:ReEncryptFrom` (rotation des clés de branche existantes) et `kms:Decrypt` (récupération des clés de branche existantes) pour les opérations de jeu de clés hiérarchiques. Ces opérations utilisent vos informations d'identification transmises via le chemin synchrone et sont limitées aux ressources du pack d'exigences de sécurité en fonction de la condition de contexte de chiffrement.
- AllowAsynchronousDataAccessForSecurityPacks— Accordekms:GenerateDataKeyWithoutPlaintext, `kms:Decryptkms:ReEncryptTo`, et `kms:ReEncryptFrom` au principal du service AWS Security Agent pour les opérations asynchrones lorsqu'aucune information d'identification de l'appelant n'est disponible.

Contrairement à la politique clé d'Agent Spaces, la politique du pack d'exigences de sécurité n'inclut pas de principal de rôle d'application Web. Les packs d'exigences de sécurité sont accessibles via la console de AWS gestion en utilisant votre rôle d'administrateur, et non via l'application Web AWS Security Agent. Toutes les opérations synchrones utilisent le rôle d'appelant unique (viakms:ViaService).

> **Note**
>
> Si vous utilisez la même clé KMS pour Agent Spaces et pour les packs d'exigences de sécurité, vous pouvez combiner les déclarations de politique clés des deux sections en une seule politique clé.

Politique clé pour CMK-encrypted AWS resources

Si vous fournissez des AWS ressources chiffrées à l'aide d'une clé gérée par le client à AWS Security Agent, vous devez mettre à jour la politique relative aux clés KMS de chaque ressource afin d'accorder les autorisations nécessaires. Cela s'applique aux ressources suivantes :

- Compartiments S3 : si vous fournissez des ressources d'apprentissage à partir d'un compartiment S3 chiffré à l'aide d'une clé gérée par le client (SSE-KMS), la politique en matière de clés doit autoriser le rôle de service de test d'intrusion à déchiffrer les objets.
- Secrets Manager : si vos identifiants de test d'intrusion sont stockés dans des secrets de Secrets Manager chiffrés à l'aide d'une clé gérée par le client, la politique en matière de clés doit autoriser le rôle de service de test d'intrusion à déchiffrer ces secrets. Si l'application Web crée des secrets en votre nom, la politique clé doit également autoriser le rôle de l'application à chiffrer ces secrets.
- CloudWatch Groupes de journaux : si le groupe de CloudWatch journaux utilisé pour stocker les journaux d'exécution des tests d'intrusion est chiffré à l'aide d'une clé gérée par le client, la politique en matière de clés doit permettre à CloudWatch Logs de valider la clé KMS via le rôle de service et au principal du service CloudWatch Logs d'effectuer des opérations cryptographiques.

> **Important**
>
> AWS Security Agent peut également créer des CloudWatch journaux, des groupes de journaux et des secrets Secrets Manager en votre nom. Lorsque vous configurez votre politique de clés KMS, incluez également les instructions correspondantes pour ces ressources créées par le service.

Les principales déclarations de politique suivantes accordent les autorisations requises pour les CMK-encrypted ressources. N'incluez que les instructions qui s'appliquent à votre configuration. Si une ressource utilise la même clé KMS que celle que vous avez spécifiée pour votre espace agent, ajoutez ces instructions à la politique de cette clé. Si une ressource utilise une autre clé KMS, ajoutez plutôt ces instructions à la politique de cette clé.

Remplacez les valeurs d'espace réservé suivantes dans la politique :

- *111122223333* — Votre identifiant AWS de compte
- *MyApplicationRole* — Le rôle d'application créé lors de la configuration AWS de l'agent de sécurité

- *MyPenTestServiceRole* — Le rôle du service de test d'intrusion
- *us-east-1* — La AWS région dans laquelle vous utilisez AWS Security Agent

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowKmsKeyAccessForCreatingSecrets",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::111122223333:role/MyApplicationRole"
      },
      "Action": [
        "kms:GenerateDataKey",
        "kms:Decrypt"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "aws:ResourceAccount": "111122223333"
        },
        "StringLike": {
          "kms:ViaService": "secretsmanager.*.amazonaws.com",
          "kms:EncryptionContext:SecretARN": "arn:aws:secretsmanager:us-
east-1:111122223333:secret:*"
        }
      }
    },
    {
      "Sid": "AllowKmsKeyDecryptionForS3Objects",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::111122223333:role/MyPenTestServiceRole"
      },
      "Action": [
        "kms:Decrypt"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "aws:ResourceAccount": "111122223333"
        },
```

```
        "StringLike": {
          "kms:ViaService": "s3.*.amazonaws.com",
          "kms:EncryptionContext:aws:s3:arn": "arn:aws:s3:::YOUR-BUCKET-NAME*"
        }
      }
    },
    {
      "Sid": "AllowKmsKeyDecryptionForSecretsManagerSecrets",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::111122223333:role/MyPenTestServiceRole"
      },
      "Action": [
        "kms:Decrypt"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "aws:ResourceAccount": "111122223333"
        },
        "StringLike": {
          "kms:ViaService": "secretsmanager.*.amazonaws.com",
          "kms:EncryptionContext:SecretARN": "arn:aws:secretsmanager:us-
east-1:111122223333:secret:YOUR-SECRET-NAME*"
        }
      }
    },
    {
      "Sid": "AllowKmsKeyValidationForCloudWatchLogsLogGroups",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::111122223333:role/MyPenTestServiceRole"
      },
      "Action": [
        "kms:DescribeKey"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "aws:ResourceAccount": "111122223333"
        },
        "StringLike": {
          "kms:ViaService": "logs.*.amazonaws.com"
        }
```

```
      }
    },
    {
      "Sid": "AllowKmsKeyAccessForCloudWatchLogsLogGroups",
      "Effect": "Allow",
      "Principal": {
        "Service": "logs.us-east-1.amazonaws.com"
      },
      "Action": [
        "kms:Encrypt",
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "aws:ResourceAccount": "111122223333"
        },
        "StringLike": {
          "kms:EncryptionContext:aws:logs:arn": "arn:aws:logs:us-
east-1:111122223333:log-group:YOUR-LOG-GROUP-NAME*"
        }
      }
    }
  ]
}
```

> **Note**
>
> - La `AllowKmsKeyDecryptionForS3Objects` déclaration n'est requise que si vous fournissez des ressources d'apprentissage à partir de compartiments S3 chiffrés à l'aide d'une clé gérée par le client. Pour plus d'informations sur la configuration SSE-KMS pour S3, consultez la section Protection des données avec SSE-KMS.
> - La `AllowKmsKeyDecryptionForSecretsManagerSecrets` déclaration n'est requise que si les informations d'identification de votre test d'intrusion sont stockées dans les secrets de Secrets Manager chiffrés à l'aide d'une clé gérée par le client. Le rôle de service a besoin d'un accès pour déchiffrer les secrets lors des tests d'intrusion. Pour plus d'informations sur le chiffrement secret, consultez la section Chiffrement secret et déchiffrement dans Secrets Manager.

- L'`AllowKmsKeyValidationForCloudWatchLogsLogGroups`instruction accorde le rôle de service `kms:DescribeKey` afin que CloudWatch Logs puisse valider la clé KMS via le rôle de service lorsqu'il l'associe à un groupe de journaux.
- La `AllowKmsKeyAccessForCreatingSecrets` déclaration est obligatoire si l'application Web crée des secrets Secrets Manager en votre nom à l'aide d'une clé gérée par le client. Le rôle d'application a besoin `kms:GenerateDataKey` et `kms:Decrypt` doit chiffrer le secret avec votre clé KMS.
- L'`AllowKmsKeyAccessForCloudWatchLogsLogGroups`instruction accorde au principal du service CloudWatch Logs (`logs.`*`us-east-1`*`.amazonaws.com`) les autorisations dont il a besoin pour chiffrer et déchiffrer les données des journaux. Cette déclaration est également requise si AWS Security Agent crée un groupe de journaux en votre nom alors que vous n'en fournissez pas un existant. Pour plus d'informations, voir Chiffrer les données des CloudWatch journaux dans les journaux à l'aide de AWS KMS.
- Si plusieurs ressources partagent la même clé KMS, vous pouvez combiner les instructions en une seule politique de clé.

Rôle d'administrateur

Aucune politique IAM supplémentaire n'est requise pour le rôle d'administrateur (le rôle IAM que vous utilisez pour gérer l'agent AWS de sécurité dans la console).

Rôle de l'application

Outre la politique de clé KMS, associez la stratégie IAM suivante au rôle d'application spécifié lors de la configuration de l'agent AWS de sécurité. Cette politique accorde au rôle l'autorisation d'utiliser les clés gérées par le client pour chiffrer et déchiffrer les données Agent Space et créer des secrets dans Secrets Manager. AWS

Remplacez les valeurs d'espace réservé suivantes dans la politique :

- *111122223333* — Votre identifiant AWS de compte
- *us-east-1* — La AWS région dans laquelle vous utilisez AWS Security Agent
- Les ARN de la clé KMS entrés `Resource` — Les ARN de vos clés KMS

```
{
  "Version": "2012-10-17",
```

```
  "Statement": [
    {
      "Sid": "AllowSynchronousDataAccessForAgentSpaces",
      "Effect": "Allow",
      "Action": [
        "kms:GenerateDataKey",
        "kms:Decrypt"
      ],
      "Resource": [
        "arn:aws:kms:us-east-1:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
        "arn:aws:kms:us-east-1:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890cd"
      ],
      "Condition": {
        "StringEquals": {
          "aws:ResourceAccount": "111122223333",
          "kms:ViaService": "securityagent.us-east-1.amazonaws.com"
        },
        "StringLike": {
          "kms:EncryptionContext:aws:securityagent:agent-space":
 "arn:aws:securityagent:us-east-1:111122223333:agent-space/*"
        }
      }
    },
    {
      "Sid": "AllowKmsKeyAccessForCreatingSecrets",
      "Effect": "Allow",
      "Action": [
        "kms:GenerateDataKey",
        "kms:Decrypt"
      ],
      "Resource": [
        "arn:aws:kms:us-east-1:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
        "arn:aws:kms:us-east-1:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890cd"
      ],
      "Condition": {
        "StringEquals": {
          "aws:ResourceAccount": "111122223333"
        },
        "StringLike": {
          "kms:ViaService": "secretsmanager.*.amazonaws.com",
          "kms:EncryptionContext:SecretARN": "arn:aws:secretsmanager:us-
east-1:111122223333:secret:*"
        }
      }
```

```
    }
  ]
}
```

> **Note**
>
> Le rôle d'application est un rôle IAM que vous spécifiez ou que la console crée lors de l'installation AWS de Security Agent. L'application Web assume ce rôle pour récupérer les journaux d'exécution des tests d'intrusion et créer des secrets Secrets Manager en votre nom.
>
> - L'`AllowKmsKeyAccessForCreatingSecrets`instruction est requise si vous configurez des ressources d'authentification pour les tests d'intrusion et que vous choisissez de saisir directement les informations d'identification au lieu de spécifier un secret existant. L'application Web crée un secret en votre nom, et le rôle d'application a besoin des autorisations indiquées dans cette instruction pour chiffrer le secret avec la clé gérée par le client spécifiée pour votre espace agent. Mettez à jour `Resource` les ARN de cette instruction pour qu'ils correspondent à la clé KMS utilisée pour votre espace agent.

Rôle de service

Pendant les tests d'intrusion, AWS Security Agent joue le rôle de service de test d'intrusion pour accéder à vos AWS ressources. Si l'une de ces ressources est chiffrée à l'aide d'une clé gérée par le client, vous devez accorder au rôle de service l'autorisation d'utiliser les clés KMS correspondantes. Cela s'applique aux ressources suivantes :

- Compartiments S3 : si vous fournissez des ressources d'apprentissage (telles que des documents d'API, des modèles de menaces ou du code source) à partir d'un compartiment S3 chiffré à l'aide d'une clé gérée par le client, le rôle de service a besoin d'autorisations pour déchiffrer les objets de ce compartiment. Pour plus d'informations sur la configuration SSE-KMS pour S3, consultez la section Protection des données avec SSE-KMS.
- Secrets Manager : si vos identifiants de test d'intrusion sont stockés dans des secrets de Secrets Manager chiffrés à l'aide d'une clé gérée par le client, le rôle de service a besoin d'autorisations pour déchiffrer ces secrets. Pour plus d'informations sur le chiffrement secret, consultez la section Chiffrement secret et déchiffrement dans Secrets Manager.
- CloudWatch Groupes de journaux : si le groupe de CloudWatch journaux utilisé pour stocker les journaux d'exécution des tests d'intrusion est chiffré à l'aide d'une clé gérée par le client (y compris

les groupes de journaux créés par AWS Security Agent en votre nom), le rôle de service doit être `kms:DescribeKey` autorisé pour valider la clé. Le principal du service CloudWatch Logs gère le chiffrement et le déchiffrement effectifs des données des journaux, et ces autorisations sont accordées par le biais de la politique des clés (voirthe section called "Stratégie de clé"). Pour plus d'informations sur le chiffrement des données de journal, voir Chiffrer les données de journal dans les CloudWatch journaux à l'aide AWS de KMS.

> **Important**
>
> Si vous utilisez une clé KMS différente de celle que vous avez spécifiée pour votre espace agent pour chiffrer ces ressources, vous devez accorder des autorisations de rôle de service pour chaque clé KMS qui protège une ressource à laquelle le rôle de service accède lors des tests d'intrusion.

Associez la politique IAM suivante au rôle de service de test d'intrusion. N'incluez que les instructions qui s'appliquent à votre configuration.

Remplacez les valeurs d'espace réservé suivantes dans la politique :

- *111122223333* — Votre identifiant AWS de compte
- *us-east-1* — La AWS région dans laquelle vous utilisez AWS Security Agent
- Les ARN de la clé KMS `Resource` entrés : les ARN des clés gérées par le client utilisées pour chiffrer chaque ressource

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowKmsAccessForEncryptedS3Buckets",
      "Effect": "Allow",
      "Action": [
        "kms:Decrypt"
      ],
      "Resource": [
        "arn:aws:kms:us-east-1:111122223333:key/EXAMPLE-S3-KEY-ID"
      ],
      "Condition": {
```

```
        "StringEquals": {
          "aws:ResourceAccount": "111122223333"
        },
        "StringLike": {
          "kms:ViaService": "s3.*.amazonaws.com",
          "kms:EncryptionContext:aws:s3:arn": "arn:aws:s3:::YOUR-BUCKET-NAME*"
        }
      }
    },
    {
      "Sid": "AllowKmsAccessForEncryptedSecrets",
      "Effect": "Allow",
      "Action": [
        "kms:Decrypt"
      ],
      "Resource": [
        "arn:aws:kms:us-east-1:111122223333:key/EXAMPLE-SECRETS-KEY-ID"
      ],
      "Condition": {
        "StringEquals": {
          "aws:ResourceAccount": "111122223333"
        },
        "StringLike": {
          "kms:ViaService": "secretsmanager.*.amazonaws.com",
          "kms:EncryptionContext:SecretARN": "arn:aws:secretsmanager:us-
east-1:111122223333:secret:YOUR-SECRET-NAME*"
        }
      }
    },
    {
      "Sid": "AllowKmsKeyValidationForCloudWatchLogsLogGroups",
      "Effect": "Allow",
      "Action": [
        "kms:DescribeKey"
      ],
      "Resource": [
        "arn:aws:kms:us-east-1:111122223333:key/EXAMPLE-CLOUDWATCH-LOGS-KEY-ID"
      ],
      "Condition": {
        "StringEquals": {
          "aws:ResourceAccount": "111122223333"
        },
        "StringLike": {
          "kms:ViaService": "logs.*.amazonaws.com"
```

```
        }
      }
    }
  ]
}
```

> **Note**
>
> - La `AllowKmsAccessForEncryptedS3Buckets` déclaration n'est requise que si vous fournissez des ressources d'apprentissage à partir de compartiments S3 chiffrés à l'aide d'une clé gérée par le client. Mettez à jour l'`Resource`ARN pour qu'il corresponde à la clé KMS utilisée pour chiffrer votre compartiment S3, et mettez à jour la `kms:EncryptionContext:aws:s3:arn` valeur pour qu'elle corresponde au nom de votre compartiment.
> - La `AllowKmsAccessForEncryptedSecrets` déclaration n'est requise que si les informations d'identification de votre test d'intrusion sont stockées dans les secrets de Secrets Manager chiffrés à l'aide d'une clé gérée par le client. Mettez à jour l'`Resource`ARN pour qu'il corresponde à la clé KMS utilisée pour chiffrer vos secrets, et mettez à jour la `kms:EncryptionContext:Secret`ARN valeur pour qu'elle corresponde à votre nom de secret.
> - La `AllowKmsKeyValidationForCloudWatchLogsLogGroups` déclaration n'est requise que si votre groupe de CloudWatch journaux Logs est chiffré à l'aide d'une clé gérée par le client, y compris les groupes de journaux créés par AWS Security Agent en votre nom. Mettez à jour l'`Resource`ARN pour qu'il corresponde à la clé KMS utilisée pour chiffrer votre groupe de journaux.
> - Si plusieurs ressources partagent la même clé KMS, vous pouvez combiner les instructions et répertorier l'ARN de la clé partagée une fois `Resource` sur le terrain.

Création d'une ressource à l'aide d'une clé gérée par le client

Vous pouvez spécifier une clé gérée par le client lors de la configuration AWS de Security Agent ou lors de la création de ressources individuelles. La clé KMS chiffre toutes les données appartenant à cette ressource et à ses sous-ressources.

Définir une clé KMS par défaut lors de l'installation (console)

Vous pouvez configurer une clé KMS par défaut lors de la configuration initiale AWS de l'agent de sécurité. Cette clé est utilisée par défaut pour les nouveaux espaces d'agent et les intégrations, sauf si vous spécifiez une autre clé.

1. Sur la page Configurer l'agent de sécurité AWS, développez la section Chiffrement - facultatif.
2. Sélectionnez Personnaliser les paramètres de chiffrement (avancés).
3. Pour Choisir une clé AWS KMS, sélectionnez une clé KMS dans votre compte ou entrez un ARN de clé KMS.
4. Effectuez les étapes de configuration restantes et choisissez Configurer AWS Security Agent.

AWS L'agent de sécurité valide la clé KMS pour confirmer qu'elle existe, qu'elle est activée et qu'elle utilise un chiffrement symétrique. Si la validation échoue, l'installation ne se poursuit pas et vous recevez un message d'erreur.

Création d'un espace d'agent avec une clé gérée par le client (console)

1. Dans la console AWS Security Agent, accédez à la page Agent Spaces.
2. Choisissez Create Agent Space.
3. Entrez un nom et une description facultative pour votre espace agent.
4. Développez la section Avancé.
5. Sous Chiffrement des données, sélectionnez l'une des options suivantes :
   - Utiliser la clé par défaut de l'application — Utilise la clé KMS par défaut configurée lors AWS de l'installation de l'agent de sécurité. Cette option est sélectionnée par défaut si une clé par défaut est configurée.
   - Utiliser une autre clé : spécifiez une clé KMS différente pour cet espace agent. Sélectionnez Personnaliser les paramètres de chiffrement (avancés), puis pour Choisir une clé AWS KMS, sélectionnez une clé KMS dans votre compte ou entrez un ARN.
6. Choisissez Créer.

Création d'une intégration à l'aide d'une clé gérée par le client (console)

1. Dans la console AWS Security Agent, accédez à la page Intégrations.
2. Choisissez Ajouter une intégration et sélectionnez votre fournisseur (par exemple, GitHub).

3. Terminez l'étape 1 : installez et autorisez l'application du fournisseur.
4. À l'étape 2 : informations d'enregistrement, entrez un nom d'enregistrement et configurez les paramètres du fournisseur.
5. Dans la section Chiffrement des données, sélectionnez Personnaliser les paramètres de chiffrement (avancés).
6. Pour Choisir une clé AWS KMS, sélectionnez une clé KMS dans votre compte ou entrez un ARN de clé KMS.
7. Choisissez Se connecter.

Créez une ressource à l'aide d'une clé gérée par le client (AWS CLI ou SDK)

Pour spécifier une clé gérée par le client à l'aide de la AWS CLI ou du SDK :

- Incluez le `defaultKmsKeyId` paramètre lors de `CreateApplication` l'appel pour définir une clé KMS par défaut pour votre application. Cette clé est utilisée comme solution de secours lors de la création d'espaces d'agents ou d'intégrations sans clé KMS explicite.
- Incluez le `kmsKeyId` paramètre lors de l'appel `CreateAgentSpace` ou `CreateIntegration` pour chiffrer une ressource spécifique. Cela a priorité sur la valeur par défaut au niveau de l'application.

Pour plus de détails sur les paramètres, consultez le document AWS de référence de l'API Security Agent.

Si vous ne spécifiez pas de clé KMS, AWS Security Agent utilise la clé KMS par défaut au niveau de l'application si elle est configurée. Dans le cas contraire, la ressource est chiffrée avec des clés AWS gérées par -managed.

Rotation des clés d'accès

AWS Security Agent fait automatiquement pivoter les clés de branche de façon périodique. La rotation de la clé de branche crée une nouvelle version active de la clé de branche tout en conservant toutes les versions précédentes. Après la rotation :

- Les nouvelles données sont cryptées avec la nouvelle version de la clé de branche.
- Les données précédemment chiffrées restent déchiffrables à l'aide de l'ancienne version de clé de branche.

- Aucun rechiffrement des données n'est requis.

La rotation des clés de branche est distincte de la rotation des clés KMS. Vous pouvez activer la rotation automatique des clés KMS pour votre clé gérée par le client de manière indépendante. Pour plus d'informations, voir Rotation des clés KMS dans le Guide du développeur du service de gestion des AWS clés.

Après une rotation de clé de branche, il existe une brève période pendant laquelle les copies mises en cache de la clé de branche précédente peuvent encore être utilisées pour de nouvelles opérations de chiffrement. Cette fenêtre est déterminée par la durée de vie du cache interne (TTL) et n'affecte pas la sécurité de vos données.

Considérations

Tenez compte des points suivants lorsque vous utilisez des clés gérées par le client avec AWS Security Agent :

- Les clés gérées par le client s'appliquent uniquement aux nouvelles ressources. Les ressources existantes créées avant de configurer une clé gérée par le client continuent d'utiliser le AWS chiffrement géré par le client. Il n'y a pas de migration des données existantes.
- Les clés gérées par le client sont spécifiées au moment de la création. Vous spécifiez la clé KMS lors de la création d'une ressource. Vous ne pouvez pas ajouter ou modifier la clé KMS pour une ressource existante.
- Plusieurs clés KMS sont prises en charge. Vous pouvez utiliser différentes clés KMS pour différentes ressources. Par exemple, vous pouvez utiliser une clé pour les Agent Spaces de production et une autre clé pour les Agent Spaces de développement.
- La désactivation ou la suppression d'une clé KMS rend les données inaccessibles. Si vous désactivez ou planifiez la suppression d'une clé KMS, AWS Security Agent ne peut pas déchiffrer les données chiffrées sous cette clé. Les ressources affectées deviennent inaccessibles jusqu'à ce que la clé soit réactivée. La suppression d'une clé KMS empêche définitivement l'accès à toutes les données chiffrées sous cette clé.
- Les principales autorisations politiques sont requises. Si vous supprimez les autorisations requises de votre politique de clés KMS, AWS Security Agent ne peut pas accéder aux données chiffrées. Assurez-vous que la politique clé accorde des autorisations pour le rôle d'administrateur (utilisé pour gérer le service dans la AWS console), le rôle d'application (utilisé par l'application Web), le rôle de service de test d'intrusion (assumé par les agents pour exécuter les tests d'intrusion) et le

rôle principal du service AWS Security Agent, comme décrit dansthe section called "Autorisations KMS requises".

- AWS Les quotas KMS s'appliquent. Les opérations cryptographiques effectuées sur votre clé KMS sont prises en compte dans le calcul de vos quotas de demandes AWS KMS. Dans des conditions normales d'utilisation, l'architecture hiérarchique du trousseau de clés minimise les appels KMS grâce à la mise en cache des clés de branche. Pour plus d'informations, consultez la section Demander des quotas dans le Guide du développeur du service de gestion des AWS clés.

Résolution des problèmes

Trouvez des solutions aux erreurs fréquemment rencontrées lors de l'utilisation d'AWS Security Agent.

Accès refusé : type de GitHub compte sélectionné incorrect ou nom d'organisation incorrect spécifié

- Vous avez installé l'application AWS Security Agent dans l' GitHub organisation de votre choix, mais vous avez défini incorrectement le `GitHub Account Type` to `User` au lieu de `Organization`
- Vous avez installé l'application AWS Security Agent dans l' GitHub organisation de votre choix et vous avez correctement défini le paramètre « `GitHub Account Type` to »`Organization`, mais vous avez laissé le `Organization Name` champ vide ou vous avez saisi un nom d'organisation incorrect qui ne correspond pas à l'organisation dans laquelle vous avez installé l'application.

Solution :

1. Accédez à l'application dans l'organisation GitHub et désinstallez-la. Pour de plus amples informations, veuillez consulter the section called "Étape 1 : désinstallez l' GitHub application AWS Security Agent de GitHub".
2. Revenez à la page des intégrations et relancez le processus d'intégration en cliquant à nouveau sur`Add Integrations`, installez et autorisez l'application dans GitHub l'organisation de votre choix.
3. Sélectionnez `Organization` dans le menu déroulant de `GitHub account type`
4. Assurez-vous que la `Organization Name` saisie est exactement la même que celle dans laquelle vous avez installé l'application.

5. Choisissez Connect pour créer GitHub l'intégration de votre organisation.

Accès refusé : autorisations insuffisantes pour installer GitHub l'application dans l'organisation

Lorsque vous tentez d'installer l'application AWS Security Agent dans GitHub l'organisation de votre choix, deux messages différents s'affichent sur le bouton de la page d'installation.

- Une organisation `Member` verra `Authorize & Request`
- Une organisation `Owner` verra `Install & Authorize`

Vous pouvez vérifier si vous êtes membre `Member` ou non `Owner` de l' GitHub organisation en suivant les étapes ci-dessous.

1. Accédez à github.com
2. Choisissez votre profil sur le site
3. Accédez `Organizations` au menu déroulant et choisissez-le
4. Recherchez l'organisation dans laquelle vous souhaitez installer AWS Security Agent dans la liste des organisations, elle indiquera si vous êtes un `Member` ou un nom à `Owner` côté du nom de l'organisation.

Solutions possibles :

- Demandez à un propriétaire d'approuver votre demande d'installation AVANT d'essayer de créer l'intégration
- Demandez à un propriétaire de mettre à jour votre rôle au GitHub sein de l'organisation de a `Member` à an `Owner` et de relancer le processus d'intégration

L'agent ne peut pas se connecter au terminal pendant un test d'intrusion

Si l'agent de test d'intrusion ne parvient pas à appeler l'URL cible configurée ou ne parvient pas à naviguer avec succès vers le point de terminaison cible :

- Si votre point de terminaison appelle des domaines en dehors de l'URL cible configurée, vérifiez que les domaines supplémentaires sont ajoutés en tant qu'URL accessibles dans votre configuration de pentest
- Les tests de pénétration ne sont actuellement disponibles que pour les HTTP/HTTPS terminaux desservant le trafic sur les ports 80 ou 443.
- Si vous avez configuré un WAF, vérifiez que votre WAF ne bloque pas le trafic des tests d'intrusion. Vous pouvez autoriser le trafic des tests de pénétration des listes par `User-Agent` en-tête, qui sera défini `securityagent` par défaut sur

Aide supplémentaire

Si vous continuez à rencontrer des problèmes après avoir essayé ces étapes de résolution des problèmes :

- Consultez la page d'état du service AWS Security Agent
- Contactez le support AWS pour obtenir de l'aide concernant des problèmes de configuration complexes

Pour les utilisateurs et les développeurs (application Web et IDE)

Exécutez des révisions de conception, des modèles de menaces, des révisions de code et des tests de pénétration dans l'application Web, un IDE ou un fournisseur de source connecté, puis examinez les résultats et corrigez les résultats.

Connectez-vous à l'application Web AWS Security Agent

Vous devez vous connecter à l'application Web AWS Security Agent pour effectuer des tâches telles que :

- Réaliser une revue de conception
- Réaliser un test de pénétration

Modes d'accès

AWS Security Agent propose différentes méthodes pour accéder à l'application Web, selon la manière dont votre organisation a configuré l'accès lors de la configuration initiale et selon que vous disposez ou non d'un accès à la console AWS.

IAM Identity Center (SSO) : si votre organisation a activé IAM Identity Center, vous pouvez vous connecter à l'aide de vos informations d'identification SSO. Vous devez être affecté à au moins un espace agent dans IAM Identity Center avant de pouvoir accéder à l'application Web.

Accès administrateur (IAM) : si vous avez accès à la console AWS avec les autorisations appropriées, vous pouvez lancer l'application Web via le lien d'accès administrateur figurant sur n'importe quelle page de l'espace agent. Cette méthode permet l'authentification par le biais de votre session de console existante.

> **Note**
>
> La principale méthode d'accès utilisée par votre organisation a été déterminée lors de la configuration initiale d'AWS Security Agent. Pour plus d'informations sur la configuration de l'accès et des attributions des utilisateurs, consultezthe section called “Autoriser les utilisateurs à accéder à l'application Web AWS Security Agent”.

Connectez-vous avec IAM Identity Center (SSO)

Si votre organisation a configuré l'accès à IAM Identity Center, vous pouvez vous connecter à l'application Web à l'aide de vos informations d'identification SSO via plusieurs points d'entrée.

Conditions préalables

- Vous avez été affecté à au moins un espace d'agent dans IAM Identity Center
- Vous disposez de vos identifiants SSO IAM Identity Center

Accédez à l'application Web

Choisissez l'une des méthodes suivantes en fonction de vos besoins :

Pour afficher tous les espaces d'agent auxquels vous êtes affecté :

1. Dans la console AWS Security Agent, accédez à Paramètres.
2. Localisez le domaine de l'application Web et copiez l'URL.

> **Tip**
>
> Ajoutez cette URL à vos favoris pour y accéder facilement. Il s'agit du point d'entrée universel pour voir tous les espaces d'agent auxquels vous êtes affectés.

3. Accédez à l'URL de l'application Web.
4. Entrez vos informations d'identification IAM Identity Center lorsque vous y êtes invité.
5. Après l'authentification, vous verrez une liste de tous les espaces d'agent auxquels vous êtes affectés.
6. Sélectionnez l'espace agent dans lequel vous souhaitez travailler.

Pour accéder directement à un espace d'agent spécifique (nécessite un accès à la console AWS) :

1. Connectez-vous à la console de gestion AWS.
2. Accédez à la console AWS Security Agent.
3. Accédez à l'espace agent auquel vous souhaitez accéder.
4. Sélectionnez l'une des méthodes suivantes :

- Bouton de lancement de l'application Web sur la page de présentation de l'Agent Space
- Lancer le bouton de l'application Web dans la section de révision du code
- Bouton de lancement de l'application Web dans la section Tests de pénétration

5. Entrez vos informations d'identification IAM Identity Center lorsque vous y êtes invité.
6. Après l'authentification, vous serez redirigé directement vers cet espace agent dans l'application Web.

> **Note**
>
> Si vous n'avez pas accès à la console AWS, utilisez le domaine de l'application Web depuis la page Paramètres pour accéder à tous les espaces d'agent qui vous sont assignés.

Connectez-vous avec un accès administrateur (IAM)

Si vous avez accès à la console AWS avec les autorisations appropriées de l'agent de sécurité AWS, vous pouvez lancer l'application Web via le lien d'accès administrateur avec authentification automatique.

Conditions préalables

- Vous êtes connecté à la console de gestion AWS
- Vous disposez des autorisations appropriées pour accéder aux ressources d'AWS Security Agent

Accédez à l'application Web

Choisissez l'une des méthodes suivantes :

Pour accéder à un espace d'agent spécifique :

1. Connectez-vous à la console de gestion AWS.
2. Accédez à la console AWS Security Agent.
3. Accédez à l'espace agent auquel vous souhaitez accéder.
4. Cliquez sur le bouton d'accès administrateur sur la page de présentation de l'espace agent.
5. L'application Web s'ouvre dans un nouvel onglet avec authentification automatique pour cet espace agent.

> **Note**
>
> Le bouton d'accès administrateur est toujours disponible pour les utilisateurs ayant accès à la console AWS, que votre organisation utilise ou non IAM Identity Center comme méthode d'accès principale.

Création d'une revue de conception

Évaluez vos documents de conception par rapport aux exigences de sécurité de l'organisation en téléchargeant des fichiers pour qu'AWS Security Agent les examine. Les révisions de conception aident à identifier les problèmes de sécurité dès le début du cycle de développement, ce qui vous permet de résoudre les problèmes d'architecture au moment où ils sont les plus rentables.

AWS Security Agent analyse vos documents de conception par rapport aux exigences de sécurité de votre organisation et fournit des résultats de sécurité détaillés afin d'améliorer le niveau de sécurité avant le début de la mise en œuvre.

Dans cette procédure, vous allez créer une révision de conception en téléchargeant des fichiers de conception à des fins d'analyse.

Conditions préalables

Avant de commencer, assurez-vous de disposer des éléments suivants :

- Accès à l'application Web AWS Security Agent
- Documents de conception prêts à être téléchargés (DOC, DOCX, JPEG, MD, PDF, PNG et TXT)
- Chaque fichier doit être inférieur ou égal à 2 Mo, avec un total combiné de 6 Mo pour tous les fichiers
- Compréhension des exigences de sécurité activées pour votre organisation

Étape 1 : Commencez à créer une révision de conception

Accédez à la page de création de la révision de conception dans l'application Web Agent.

1. Connectez-vous à l'application Web AWS Security Agent.
2. Accédez à la section Révisions de conception.
3. Choisissez Create Design Review.

> **Tip**
>
> Vous pouvez consulter les exigences de sécurité activées par votre organisation en accédant à la page Exigences de sécurité de la console AWS Security Agent. Sélectionnez une exigence activée pour en afficher les détails. Ces exigences sont utilisées pour analyser vos fichiers de conception.

Étape 2 : Donnez un nom à votre critique de conception

Fournissez un nom descriptif qui aide à identifier l'objectif et la portée de cette revue de conception.

1. Dans la section Nom de la révision de conception, recherchez le champ Nom.
2. Entrez un nom descriptif pour votre révision de conception.

> **Note**
>
> Le nom doit clairement identifier le projet, la fonctionnalité ou le composant examiné. 80 caractères maximum.

Étape 3 : Téléchargez les fichiers de conception

Téléchargez les documents de conception que vous souhaitez qu'AWS Security Agent analyse pour vérifier leur conformité en matière de sécurité.

1. Dans la section Fichiers à examiner, passez en revue les exigences relatives aux fichiers :

> **Important**
>
> Un maximum de 5 fichiers peuvent être téléchargés par révision de conception. Chaque fichier doit être inférieur ou égal à 2 Mo, avec un total combiné de 6 Mo pour l'ensemble des fichiers. Formats pris en charge : DOC, DOCX, JPEG, MD, PDF, PNG et TXT.

2. Téléchargez vos fichiers en utilisant l'une des méthodes suivantes :
   a. Glisser-déposer — Faites glisser les fichiers directement dans la zone de dépôt des fichiers
   b. Parcourir : utilisez le bouton Choisir des fichiers pour parcourir et sélectionner des fichiers sur votre ordinateur

3. Vérifiez que tous les fichiers requis sont chargés.

> **Tip**
>
> Pour de meilleurs résultats, incluez des diagrammes d'architecture, des spécifications de conception et de la documentation technique décrivant les composants et les flux de données liés à la sécurité de votre système.

Étape 4 : Lancer la révision de la conception

Après avoir configuré toutes les informations requises, lancez l'analyse de sécurité de vos documents de conception.

1. Vérifiez tous les fichiers et paramètres téléchargés pour garantir leur exactitude.
2. Choisissez Commencer la révision de la conception.
3. AWS Security Agent analyse vos documents de conception par rapport aux exigences de sécurité activées.

> **Note**
>
> Le processus de révision de la conception se termine généralement en quelques minutes, en fonction du nombre et de la taille des fichiers téléchargés. Vous recevez des résultats de sécurité basés sur les exigences de sécurité de votre organisation.

Étapes suivantes

Après avoir commencé votre révision de conception :

- Surveiller la progression de la révision dans l'Agent Web App
- Passez en revue les résultats de sécurité
- Partagez les résultats avec votre équipe de développement
- Tenez compte des problèmes de sécurité identifiés dans votre conception
- Mettez à jour les documents de conception et soumettez-les à nouveau si nécessaire

Examiner les résultats d'une revue de conception

Les résultats de l'examen vous aident à comprendre quelles exigences de sécurité sont satisfaites, lesquelles nécessitent une attention particulière et quelles mesures prendre pour améliorer le niveau de sécurité de votre conception avant le début de la mise en œuvre.

Dans cette procédure, vous allez apprendre à accéder aux résultats de l'examen de conception, à les filtrer et à les interpréter afin de traiter efficacement les problèmes de sécurité.

Conditions préalables

Avant de commencer, assurez-vous de disposer des éléments suivants :

- Une revue de conception terminée
- Accès à l'application Web AWS Security Agent
- Connaissance des exigences de sécurité activées de votre organisation

Étape 1 : Accédez à la revue de conception

Accédez à votre revue de conception pour consulter les résultats et les informations récapitulatives.

1. Connectez-vous à l'application Web AWS Security Agent.
2. Accédez à la section Révisions de conception.
3. Sélectionnez la révision de conception que vous souhaitez examiner dans la liste.

> **Tip**
>
> La page des détails de la révision de conception affiche un résumé de l'état de la révision, de la date d'achèvement et du nombre de fichiers examinés.

Étape 2 : Examiner le résumé des résultats

Examinez le résumé de haut niveau pour comprendre le niveau de sécurité global de votre conception.

1. Localisez la section Résumé.

2. Vérifiez le nombre pour chaque catégorie de statut de conformité : Conforme Non-compliant, Données insuffisantes et Non applicable.

> **Note**
>
> Le résumé fournit des chiffres pour chaque type de statut, ce qui vous permet d'évaluer rapidement le nombre de constatations nécessitant une attention particulière. Pour obtenir des explications détaillées sur chaque statut, reportez-vous à l'étape 4.

Étape 3 : Filtrer et parcourir les résultats

Utilisez les fonctionnalités de filtrage et de recherche pour vous concentrer sur des résultats ou des statuts de conformité spécifiques.

1. Dans la section Révision des résultats, localisez les commandes du filtre.
2. Pour filtrer par statut :
   a. Choisissez le menu déroulant d'état.
   b. Sélectionnez un statut de conformité spécifique pour afficher uniquement les résultats correspondant à ce statut.
3. Pour rechercher des exigences de sécurité spécifiques, procédez comme suit :
   a. Entrez des mots clés dans le champ de recherche.
   b. Les résultats sont mis à jour automatiquement à mesure que vous tapez.
4. Utilisez les commandes de pagination pour parcourir plusieurs pages de résultats.

> **Tip**
>
> Filtrez Non-compliantd'abord par statut pour hiérarchiser les résultats qui nécessitent une attention immédiate lors de votre conception.

Étape 4 : Comprendre les statuts de conformité

Chaque résultat indique un statut de conformité qui indique comment votre conception répond à une exigence de sécurité spécifique :

- Conforme — Votre conception répond aux exigences de sécurité sur la base de l'analyse
- Non-compliant— Votre conception enfreint ou ne répond pas de manière adéquate aux exigences de sécurité
- Données insuffisantes : les fichiers téléchargés ne contiennent pas suffisamment d'informations pour déterminer la conformité
- Non applicable — Les exigences de sécurité ne s'appliquent pas à la conception de votre système

> **Important**
>
> Concentrez-vous sur Non-compliantles états de données insuffisants, car ils nécessitent une action. Corrigez les résultats non conformes en mettant à jour votre conception, et corrigez les problèmes de données insuffisants en téléchargeant de la documentation de conception supplémentaire.

Étape 5 : Afficher les détails de la recherche

Sélectionnez les résultats individuels pour afficher une justification détaillée et des conseils de correction.

1. Dans le tableau des résultats, sélectionnez le nom d'une exigence de sécurité.
2. Passez en revue les détails des résultats, notamment :
   - L'exigence de sécurité spécifique en cours d'évaluation
   - Un commentaire expliquant pourquoi le résultat a reçu son statut de conformité, y compris des détails spécifiques sur ce qui est manquant ou non conforme
   - Conseils de remédiation recommandés pour donner suite à cette constatation
   - Liens vers la documentation interne ou les normes de votre organisation concernant les exigences de sécurité

> **Note**
>
> Le commentaire explique le raisonnement de l'agent de sécurité AWS avec des détails spécifiques. En cas de données insuffisantes, le commentaire identifie les informations manquantes, telles que « Les documents de conception ne mentionnent pas les mécanismes

d'authentification » ou « Aucune information trouvée sur le chiffrement des données au repos ».

Étape 6 : Résoudre les problèmes

Agissez en fonction des résultats qui nécessitent une attention particulière afin d'améliorer le niveau de sécurité de votre conception.

Pour les Non-compliantrésultats :

1. Consultez les conseils de correction recommandés.
2. Passez en revue toute documentation interne liée pour plus de contexte.
3. Mettez à jour vos documents de conception pour répondre aux exigences de sécurité.
4. Documentez les modifications que vous apportez pour référence future.

Pour les résultats de données insuffisants :

1. Lisez attentivement le commentaire pour comprendre quelles informations spécifiques sont manquantes.
2. Créez ou mettez à jour des documents de conception avec les détails manquants.
3. Préparez les fichiers mis à jour pour les soumettre à nouveau.

Étapes suivantes

Après avoir examiné les résultats de votre conception :

- Téléchargez le rapport des résultats sous forme de fichier CSV à partager avec votre équipe
- Mettre à jour les documents de conception pour traiter les résultats non conformes
- Créez une documentation supplémentaire pour les résultats de données insuffisants
- Partagez les résultats avec votre équipe de développement pour en discuter
- Clonez cette révision de conception pour créer une nouvelle révision avec les documents originaux préchargés, ce qui vous permettra de mettre à jour le nom et de réexécuter l'analyse pour vérifier les améliorations
- Procéder à la mise en œuvre des conceptions répondant aux exigences de conformité

Pour plus d'informations sur la gestion des exigences de sécurité, consultezthe section called "Gérer les exigences de sécurité".

Pour plus d'informations sur la création de révisions de conception, consultezthe section called "Création d'une revue de conception".

Création d'un modèle de menace

Créez des modèles de menaces dans l'application Web AWS Security Agent pour analyser l'architecture de votre application et identifier les menaces de sécurité. Un modèle de menace produit deux résultats principaux : une vue d'ensemble du système qui décrit la façon dont votre système est construit et se comporte, et un ensemble de menaces décrivant la manière dont le système pourrait être attaqué, chacune avec un niveau de gravité, une classification STRIDE et des recommandations exploitables.

Un modèle de menace accepte deux types d'entrées, et vous pouvez fournir l'un ou l'autre ou les deux :

- Documents relatifs au champ d'application : documents de conception technique, spécifications d'API ou documentation d'architecture qui définissent les objectifs du modèle de menace. Lorsqu'il est fourni, l'agent adapte son analyse au contexte décrit dans ces documents. Vous pouvez télécharger des fichiers (DOC, DOCX, JPEG, MD, PDF, PNG, TXT), fournir des URI S3 ou connecter des pages Confluence via une intégration.
- Sources : code source provenant de référentiels connectés (GitHub GitHub Enterprise Server ou Bitbucket) ou d'emplacements S3. GitLab GitLab Self-Managed AWS Security Agent lit le code source pour comprendre votre système existant. Lorsqu'il est combiné à la documentation de portée, le code source fournit un contexte sur l'implémentation actuelle.

Dans cette procédure, vous créez un modèle de menace en configurant ses entrées et ses autorisations, puis vous lancez une exécution.

Conditions préalables

Avant de commencer, assurez-vous de disposer des éléments suivants :

- Accès à l'application Web AWS Security Agent
- Au moins l'un des éléments suivants :

- Un référentiel connecté (GitHub GitHub Enterprise Server ou Bitbucket) à utiliser comme source (voirthe section called "Activez la modélisation des menaces") GitLab GitLab Self-Managed
- Un compartiment S3 contenant le code source
- Concevez des documents à télécharger sous forme de scope, de documents ou d'intégration Confluence

> **Tip**
>
> Si vous avez déjà des référentiels ou des compartiments S3 connectés à votre espace agent (par exemple, par le biais d'une révision du code ou de la configuration de tests d'intrusion), vous pouvez créer un modèle de menace immédiatement. Aucune configuration supplémentaire n'est requise.

Comment l'agent de sécurité AWS exécute un modèle de menace

Les entrées que vous fournissez déterminent la manière dont AWS Security Agent exécute le modèle de menace. Il existe trois scénarios.

Entrées que vous fournissez	Comment l'agent de sécurité AWS exécute le modèle de menace
Sources uniquement (code source)	AWS Security Agent analyse le code source pour comprendre la structure de votre application, classe les composants, extrait les flux de données, crée un modèle de menace et identifie les menaces en fonction de la manière dont le système est réellement mis en œuvre.
Documents relatifs au champ d'application uniquement (documents de conception)	AWS Security Agent exécute un modèle de menace axé sur la conception décrite dans vos documents. Il identifie les menaces en fonction de l'architecture, des flux de données et des composants décrits dans les documents de portée, ce qui est utile pour modéliser les menaces d'une conception avant qu'un code n'existe.
Documents relatifs aux sources et au champ d'application	AWS Security Agent adapte le modèle de menace au contexte décrit dans les documents de portée (par exemple, un document de conception pour une nouvelle fonctionnalité). Il utilise le code source pour comprendre votre système existant, puis modélise les menaces conformément à la

Entrées que vous fournissez	Comment l'agent de sécurité AWS exécute le modèle de menace
	conception décrite dans les documents de portée, que cette conception soit déjà mise en œuvre ou non.

Accédez à la page des modèles de menaces

Accédez à la section de modélisation des menaces dans l'application Web.

1. Connectez-vous à l'application Web AWS Security Agent.
2. Dans la barre latérale gauche, choisissez Threat models.
3. Vous pouvez consulter la liste des modèles de menaces existants avec leur titre, leur état d'exécution le plus récent et le nombre de menaces par gravité.

Création d'un modèle de menace

Configurez un nouveau modèle de menace en configurant ses entrées et ses autorisations.

1. Sur la page Modèles de menace, choisissez Créer un modèle de menace.

Configurer les détails du modèle de menace

Donnez un titre à votre modèle de menace.

1. Dans le champ Titre, entrez un nom descriptif pour votre modèle de menace.

> **Tip**
>
> Utilisez un nom qui identifie l'application ou le service modélisé. Par exemple, « billing-service » ou « checkout-api ».

Ajouter des documents de portée

Fournissez les documents de conception technique qui définissent les objectifs du modèle de menace, tels que la documentation d'architecture, les spécifications des API ou les propositions de

conception. Lorsque des documents de portée sont fournis, l'agent étend son analyse au contexte décrit dans ces documents. Les documents Scope sont facultatifs si vous fournissez des sources.

1. Dans la section Documents de portée, ajoutez des documents en utilisant une ou plusieurs des méthodes suivantes :
   - Télécharger des fichiers : téléchargez directement les documents de conception (DOC, DOCX, JPEG, MD, PDF, PNG ou TXT).
   - URI S3 — Entrez des URI S3 pointant vers des documents stockés dans des compartiments S3 connectés.
   - Pages Confluence : si vous avez une intégration Confluence connectée à votre espace agent, sélectionnez des pages dans votre espace de travail Confluence.

> **Tip**
>
> Pour de meilleurs résultats, incluez des diagrammes d'architecture, des spécifications d'API et de la documentation technique décrivant les composants, les flux de données et les limites de confiance de votre système.

Ajouter des sources

Sélectionnez le code source utilisé par AWS Security Agent pour comprendre votre système existant. Lorsqu'il est associé à la documentation de portée, le code source fournit un contexte sur l'implémentation en cours. L'agent l'utilise pour comprendre ce qui existe déjà. Les sources sont facultatives si vous fournissez des documents de portée.

1. Dans la section Sources, ajoutez du code source en utilisant une ou plusieurs des méthodes suivantes :

Référentiels intégrés

Sélectionnez l'un des référentiels connectés à votre espace agent (GitHub GitHub Enterprise Server, GitLab GitLab Self-Managed, ou Bitbucket).

1. Cochez la case à côté de chaque référentiel que vous souhaitez inclure en tant que source.
2. Utilisez le champ de recherche pour trouver des référentiels spécifiques par nom.

> **Note**
>
> Seuls les référentiels connectés à votre espace agent apparaissent ici. Pour ajouter d'autres référentiels, demandez à votre administrateur de mettre à jour la configuration de l'espace agent.

Sources S3

Ajoutez des URI S3 pointant vers le code source stocké dans des compartiments S3 connectés.

1. Entrez l'URI S3 pour chaque emplacement de code source que vous souhaitez inclure.

Configuration des ressources AWS

Sélectionnez le rôle de service IAM et le groupe de CloudWatch journaux facultatif pour ce modèle de menace.

1. Dans le menu déroulant Rôle de service, sélectionnez le rôle IAM parmi les rôles de service que vous avez configurés.

   > **Note**
   >
   > Le rôle de service doit être autorisé à accéder à votre code source dans S3 et à écrire dans CloudWatch les journaux. Les rôles de service sont configurés lors de la configuration de l'espace agent dans l'AWS Management Console.

2. (Facultatif) Dans le menu déroulant Groupe de journaux, sélectionnez un groupe de CloudWatch journaux pour stocker les journaux d'exécution des modèles de menaces.

Création du modèle de menace

1. Examinez votre configuration.
2. Choisissez Créer un modèle de menace.

Vous êtes redirigé vers la page détaillée du modèle de menace où vous pouvez démarrer une exécution.

Exécutez un modèle de menace

Après avoir créé un modèle de menace, lancez une exécution pour commencer l'analyse.

1. Sur la page détaillée du modèle de menace, choisissez Démarrer l'exécution.
2. AWS Security Agent commence à analyser vos sources et vos documents de portée.

Vous pouvez également démarrer une exécution depuis la page de liste des modèles de menaces en choisissant Démarrer l'exécution à côté du modèle de menace que vous souhaitez exécuter.

Surveiller l'exécution d'un modèle de menace

Suivez l'évolution de votre modèle de menace au fur et à mesure de son exécution.

Statut de l'exécution

L'en-tête de la page d'exécution affiche un indicateur d'état :

- En cours — L'agent du modèle de menace est en cours d'exécution.
- Arrêt : une annulation a été demandée ; l'agent termine sa tâche en cours avant de l'arrêter.
- Terminé — L'exécution s'est terminée avec succès.
- Échec : une erreur s'est produite lors de l'exécution. Un message d'erreur contenant des informations détaillées s'affiche. Commencez une nouvelle course après avoir résolu le problème.
- Arrêté — L'exécution a été annulée par l'utilisateur. Toutes les menaces générées avant l'arrêt sont préservées.

Exécuter des onglets de page

Sur la page détaillée de l'exécution, naviguez entre les onglets :

- Vue d'ensemble : affichez le résumé de l'exécution (identifiant de la tâche, heure de début, statut, durée) avec un graphique circulaire du niveau de gravité indiquant la répartition des menaces par gravité (critique, élevée, moyenne, faible). Sous le résumé, consultez un graphique à barres des catégories de menaces STRIDE indiquant le nombre de menaces entrant dans chaque catégorie STRIDE. Une fois l'exécution terminée, consultez la vue d'ensemble du système produite par l'agent.

- Configuration — Affichez les sources, les documents et les autorisations (rôle de service, groupe de CloudWatch journaux) utilisés pour cette exécution.
- Prévol : consultez l'état des vérifications avant le vol exécutées avant le début de l'analyse des menaces, notamment la configuration de l'infrastructure de journalisation, la validation de l'accès aux sources S3 (le cas échéant) et la configuration de l'environnement de test. Une barre de progression indique le nombre de vérifications effectuées.
- Journaux : affichez une liste filtrable des tâches effectuées par l'agent pendant l'exécution. Sélectionnez une tâche pour afficher les résultats détaillés de son journal dans un panneau latéral.
- Menaces : consultez les menaces identifiées pendant l'exécution (voirthe section called “Analyser les menaces à partir d'un modèle de menace”).

Historique des courses

Chaque modèle de menace conserve un historique de toutes les exécutions. Sur la page détaillée du modèle de menace :

- Le tableau des exécutions répertorie toutes les exécutions avec leur heure de début, leur statut, leur durée, le nombre de menaces et leur identifiant.
- Choisissez le lien vers l'heure de début de n'importe quelle course pour en afficher tous les détails.

> **Tip**
>
> Re-run le même modèle de menace une fois que vous avez mis à jour votre code source ou révisé vos documents de portée pour voir comment la vue d'ensemble du système et les menaces évoluent au fil du temps.

Modifier un modèle de menace

Pour modifier la configuration de votre modèle de menace :

1. Sur la page détaillée du modèle de menace, choisissez Modifier.
2. Mettez à jour le titre, les sources, les documents relatifs au champ d'application ou les ressources AWS selon vos besoins.
3. Sélectionnez Enregistrer les modifications.

> **Note**
>
> La modification d'un modèle de menace n'affecte pas les exécutions effectuées précédemment. Ils préservent l'instantané de configuration utilisé au moment de leur exécution.

Supprimer un modèle de menace

Pour supprimer un modèle de menace ainsi que toutes ses exécutions et menaces associées, procédez comme suit :

1. Sur la page détaillée du modèle de menace, ouvrez le menu des actions et choisissez Supprimer.
2. Confirmez la suppression.

> **Important**
>
> Si une exécution est en cours, vous devez l'arrêter avant de supprimer le modèle de menace.

Étapes suivantes

Après avoir exécuté un modèle de menace :

- Consultez la vue d'ensemble du système et les menaces (voirthe section called “Analyser les menaces à partir d'un modèle de menace”)
- Re-run le modèle de menace après avoir apporté des modifications pour vérifier que les menaces sont prises en compte
- Ajustez vos sources et vos documents de portée au fur et à mesure de l'évolution de votre application

Analyser les menaces à partir d'un modèle de menace

Une fois l'exécution d'un modèle de menace terminée, passez en revue la vue d'ensemble du système et les menaces pour comprendre comment votre application pourrait être attaquée et ce qu'il faut faire pour y remédier. La présentation du système est un document complet décrivant

l'architecture, les limites de confiance, les flux de données et le niveau de sécurité de votre application. Chaque menace inclut une déclaration, un niveau de gravité, une classification STRIDE, les actifs concernés et une recommandation pour y faire face.

Conditions préalables

Avant de commencer, assurez-vous de disposer des éléments suivants :

- Un modèle de menace exécuté
- Accès à l'application Web AWS Security Agent

Étape 1 : Accédez au modèle de menace exécuté

Accédez à l'exécution de votre modèle de menace terminée.

1. Connectez-vous à l'application Web AWS Security Agent.
2. Dans la barre latérale gauche, choisissez Threat models.
3. Sélectionnez le modèle de menace que vous souhaitez examiner.
4. Dans le tableau des exécutions, sélectionnez l'exécution terminée en choisissant son lien avec l'heure de début.

Étape 2 : passez en revue la vue d'ensemble du système

La présentation du système est une description complète de la façon dont AWS Security Agent comprend votre système. Il s'agit d'un document structuré qui peut inclure :

- Objectif — Ce que fait le système et à qui il sert.
- Capacités — Fonctionnalités clés fournies par le système.
- Intention de conception : modification de conception ou fonctionnalité modélisée par la menace (lorsque les documents relatifs au champ d'application sont fournis).
- Architecture : mode de construction du système, y compris les modèles de déploiement et les protocoles de communication.
- Composants : tableau des composants du système avec leur fonction et leurs principales interactions.
- Limites de confiance : les situations dans lesquelles les contextes de sécurité changent, y compris les protections qui existent à chaque point de passage.

- Flux de données : descriptions détaillées de la manière dont les données circulent dans le système, y compris les protocoles, les informations d'identification et les protections à chaque étape.
- Position de sécurité — Mécanismes actuels d'authentification, de chiffrement et de contrôle d'accès.
- Actifs sensibles : données et informations d'identification nécessitant une protection, avec leur classification et leurs points d'exposition.
- Hypothèses clés : Security-relevant hypothèses formulées par l'agent à propos du système.

Pour consulter la vue d'ensemble du système :

1. Sélectionnez l'onglet Vue d'ensemble.
2. Consultez la section Récapitulatif de l'exécution, qui indique l'ID de la tâche, l'heure de début, le statut et la durée.
3. Consultez le graphique des niveaux de gravité, qui montre la répartition des menaces par gravité (critique, élevée, moyenne, faible) avec des chiffres et des pourcentages.
4. Consultez le tableau des catégories de menaces, qui indique le nombre de menaces entrant dans chaque catégorie STRIDE (usurpation d'identité, falsification, répudiation, divulgation d'informations, déni de service, élévation de privilèges).
5. Dans la section Présentation du système, lisez l'analyse complète de l'agent.

> **Tip**
>
> Si la vue d'ensemble du système ne reflète pas exactement votre système, affinez vos entrées (ajoutez des référentiels pertinents en tant que sources ou téléchargez des documents de portée plus complets) et réexécutez le modèle de menace.

Étape 3 : Examiner les menaces

Accédez à l'onglet Menaces pour afficher toutes les menaces identifiées lors de l'exécution.

1. Sélectionnez l'onglet Menaces.

2. Les menaces s'affichent sous forme de liste, chaque carte indiquant le titre de la menace, le badge de gravité, le statut et l'horodatage de la dernière mise à jour. Vous pouvez filtrer les menaces par gravité, par statut ou effectuer une recherche par titre.
3. Sélectionnez une menace dans la liste pour en afficher tous les détails dans le panneau de droite.

Gravité de la menace

Un niveau de gravité est attribué à chaque menace :

- Critique — Nécessite une action immédiate ; l'exploitation peut entraîner la compromission complète du système.
- Élevé — Nécessite une attention rapide ; l'exploitation peut avoir un impact important sur la sécurité.
- Moyen — Doit être traité dans un délai raisonnable ; cela contribue au risque de sécurité global.
- Faible — Peut être traité dans le cadre d'un entretien régulier ; risque immédiat minimal.

Détails de la menace

Sélectionnez une menace pour en afficher les détails dans le panneau de droite. Les détails sont organisés dans les sections suivantes :

Ligne de métadonnées :

- Gravité : niveau de risque attribué par l'agent (critique, élevé, moyen ou faible).
- Catégories STRIDE : classification des menaces : usurpation d'identité, falsification, répudiation, divulgation d'informations, déni de service ou élévation de privilèges.
- Créé à : date à laquelle la menace a été identifiée.
- Dernière mise à jour : date à laquelle la menace a été modifiée pour la dernière fois.

Section de description :

- Déclaration — Description en langage naturel de la menace : ce que la source de la menace peut faire, quel en est l'impact et quelles conditions le permettent.
- Source : acteur ou origine de la menace (par exemple, « utilisateur authentifié » ou « attaquant externe »).

- Action : ce que peut faire la source de la menace (par exemple, « injecter des requêtes SQL dans le paramètre de recherche »).
- Impact : conséquence directe de l'action de menace (par exemple, « accès non autorisé aux dossiers des clients »).

Section des références :

- Actifs concernés : actifs spécifiques concernés par la menace (par exemple, « dossiers de paiement des clients » ou « table DynamoDB »).
- Conditions préalables — Conditions qui doivent être vraies pour que la menace soit exploitable.
- Objectifs concernés — Objectifs de sécurité concernés : confidentialité, intégrité, disponibilité, autorisation, authentification ou Non-repudiation.
- Preuve : chemins de fichiers du code source qui supportent la menace, renvoyant vers des fichiers spécifiques de votre référentiel.
- Ancre : référence de code reliant la menace à un nœud spécifique de votre code source.

Section des recommandations :

- Recommandation — Conseils pratiques pour faire face à la menace.

Étape 4 : créer une menace manuellement

Vous pouvez ajouter des menaces que l'agent n'a pas identifiées, par exemple des menaces découvertes lors d'un examen manuel ou provenant de sources externes.

1. Dans l'onglet Menaces d'une exécution terminée, choisissez Créer une menace.
2. Renseignez les informations relatives à la menace :
   - Déclaration — Description en langage naturel de la menace.
   - Gravité : sélectionnez Critique, Élevé, Moyen ou Faible.
   - Source — L'acteur ou l'origine de la menace.
   - Conditions préalables — Conditions requises pour que la menace soit exploitable.
   - Action : ce que peut faire la source de la menace.
   - Impact : conséquence directe de l'action menaçante.
   - Ressources affectées : ressources spécifiques affectées (séparées par des virgules).

- Objectifs de sécurité concernés : sélectionnez Confidentialité, Intégrité, Disponibilité, Autorisation, Authentification ou Non-repudiation.
- Catégories STRIDE — Sélectionnez les catégories applicables.
- Recommandation — Conseils pour faire face à la menace.

3. Choisissez Créer.

La menace créée manuellement apparaît dans la liste des menaces aux côtés des menaces générées par l'agent.

Étape 5 : Modifier et trier les menaces

Au fur et à mesure que vous examinez les menaces, vous pouvez modifier leurs informations et mettre à jour leur statut pour suivre leur progression.

1. Sélectionnez une menace dans la liste.
2. Cliquez sur l'icône de modification dans le panneau détaillé de la menace pour ouvrir le formulaire de modification.
3. Vous pouvez modifier les champs suivants :
   - État — Suivez le cycle de vie des menaces :
     - Ouvert — La menace est reconnue et nécessite une attention particulière (par défaut).
     - Résolu — Vous avez résolu le problème.
     - Rejeté — Vous avez examiné la menace et déterminé qu'elle n'était pas applicable.
   - Sévérité : ajustez le niveau de gravité si l'évaluation de l'agent ne correspond pas à votre contexte.
   - Déclaration — Affinez la description de la menace.
   - Source, conditions préalables, action, impact : mettez à jour les détails de la menace en fonction de votre connaissance du domaine.
   - Ressources affectées : ajoutez ou supprimez des ressources concernées (séparées par des virgules).
   - Objectifs de sécurité concernés : sélectionnez les objectifs de sécurité concernés (confidentialité, intégrité, disponibilité, autorisation, authentification, Non-repudiation).
4. Choisissez Enregistrer pour appliquer vos modifications.

Étape 6 : Téléchargez un rapport

Une fois l'exécution terminée, vous pouvez télécharger un rapport PDF résumant la vue d'ensemble du système et toutes les menaces identifiées.

1. Sur la page d'exécution terminée, choisissez Generate report.
2. Le PDF est téléchargé sur votre ordinateur.

Étape 7 : Passez en revue les vérifications et les journaux avant le vol

Si vous devez étudier comment l'agent est parvenu à ses conclusions ou corriger un échec partiel :

1. Sélectionnez l'onglet Preflight pour voir l'état des contrôles avant vol exécutés avant le début de l'analyse des menaces. Chaque vérification indique son statut (terminée, en cours ou en attente), et une barre de progression indique le nombre de vérifications effectuées. Vous pouvez développer une vérification terminée pour afficher le résultat détaillé du journal.
2. Sélectionnez l'onglet Logs pour afficher une liste filtrable des tâches effectuées par l'agent pendant l'exécution. Sélectionnez une tâche dans la liste pour afficher les résultats détaillés de son journal dans le panneau latéral.

Étapes suivantes

Après avoir examiné les résultats de votre modèle de menace :

- Traitez d'abord les menaces les plus graves en vous basant sur les recommandations de l'agent
- Mettez à jour le statut des menaces à mesure que vous mettez en œuvre des correctifs
- Exécutez un nouveau modèle de menace pour vérifier que vos modifications répondent aux menaces identifiées
- Ajustez vos sources et vos documents de portée au fur et à mesure de l'évolution de votre application (voirthe section called “Création d'un modèle de menace”)

Passez en revue les résultats de sécurité du code dans les pull requests

Après avoir activé la révision du code pour les pull requests pour vos référentiels, AWS Security Agent analyse automatiquement les pull requests et publie les résultats de sécurité directement dans

votre fournisseur de contrôle de source. Cela permet aux développeurs de résoudre les problèmes de sécurité dans le cadre de leur flux de travail normal sans avoir à quitter la pull request.

> **Note**
>
> Cette page s'applique aux GitHub pull requests, aux demandes de GitLab fusion et aux pull requests Bitbucket. L'expérience est similaire chez tous les fournisseurs.

Comment fonctionne la révision du code dans les pull requests

Lorsque vous soumettez une pull request (ou une demande de fusion GitLab) dans un référentiel où la révision du code est activée, AWS Security Agent lance automatiquement l'analyse.

1. Déclencheur d'analyse des pull requests : la révision du code est déclenchée lorsqu'une pull request est marquée comme « prête à être révisée » dans les référentiels où vous avez activé la fonctionnalité de révision du code. Les brouillons de pull requests ne sont pas analysés.
2. Confirmation de l'analyse : lorsqu'AWS Security Agent commence à analyser votre pull request, il publie un premier commentaire : « L'agent de sécurité AWS analyse votre code... » Cela vous indique que l'analyse a commencé et est en cours.
3. Fin de la révision : une fois l'analyse terminée, l'agent de sécurité AWS publie un avis sur votre pull request avec les résultats. Tous les résultats de sécurité sont regroupés dans un seul examen afin d'organiser votre pull request et de minimiser les notifications.

Comprendre les résultats de la révision du code

AWS Security Agent fournit différents types de résultats en fonction de ce qu'il trouve lors de l'analyse.

Lorsque des problèmes de sécurité sont détectés

Si AWS Security Agent identifie des problèmes de sécurité dans vos modifications de code, il publie un avis qui inclut :

- Résumé - Vue d'ensemble de tous les résultats de sécurité, décrivant les types de problèmes identifiés et leur impact potentiel
- Conclusions individuelles - Les résultats de sécurité détaillés apparaissent sous forme de commentaires sous forme de fil de discussion sous la revue principale, chaque résultat incluant :

- Description du problème de sécurité
- Emplacement dans votre code où le problème a été détecté
- Conseils de correction expliquant comment résoudre le problème
- Contexte pertinent en fonction de vos paramètres de révision du code (violations des exigences de sécurité, vulnérabilités courantes, ou les deux)

> **Note**
>
> Les types de problèmes de sécurité analysés dépendent de vos paramètres de révision du code. Si vous avez configuré la validation des exigences de sécurité, les résultats feront référence aux exigences de sécurité personnalisées de votre organisation. Si vous avez configuré les résultats des vulnérabilités de sécurité, les résultats identifieront les vulnérabilités de sécurité courantes. Pour plus d'informations sur les paramètres de révision du code, consultezthe section called “Activer la révision du code de pull request pour les GitHub référentiels”.

Lorsqu'aucun problème de sécurité n'est détecté

Si AWS Security Agent termine son analyse et ne détecte aucun problème de sécurité dans vos modifications de code, il publie le commentaire suivant : « Aucun problème identifié ». Cela confirme que la révision s'est terminée correctement et que les modifications apportées au code n'ont entraîné aucun résultat de sécurité sur la base des paramètres de révision du code que vous avez configurés.

Réagir aux constatations relatives à la sécurité

Après avoir examiné les résultats de sécurité publiés par l'agent de sécurité AWS, vous pouvez prendre des mesures directement auprès de votre fournisseur de contrôle de source.

- Corriger les résultats : mettez à jour votre code en fonction des conseils de correction fournis dans les résultats, puis envoyez de nouveaux validations à la pull request. L'agent de sécurité AWS analysera le code mis à jour.
- Résoudre les conversations : après avoir répondu à un problème de sécurité, marquez la conversation comme étant résolue pour suivre votre progression.

> **Tip**
>
> Chaque résultat inclut des conseils de correction spécifiques adaptés au problème de sécurité identifié. Lisez attentivement ce guide pour comprendre le risque de sécurité et savoir comment y faire face efficacement.

Résultats de l'examen du code de filtrage

Vous pouvez personnaliser la façon dont AWS Security Agent analyse votre code en ajoutant un `filtering.md` fichier à votre référentiel. Ce fichier vous permet de réduire le nombre de faux positifs en fournissant le contexte de votre base de code et en excluant des fichiers ou des dossiers de l'analyse.

Création du fichier de filtrage

Créez un fichier nommé `filtering.md` dans le `.awssecurityagent` répertoire à la racine de votre dépôt :

```
.awssecurityagent/filtering.md
```

AWS Security Agent lit ce fichier depuis la branche principale de votre référentiel (par exemple, `main` ou`mainline`) lors de l'analyse des pull requests.

Structure de fichier

Le `filtering.md` fichier utilise le format Markdown standard avec des sections spécifiques reconnues par AWS Security Agent. Le fichier doit inclure un `Code Review` titre suivi de l'une ou des deux sections suivantes : `IgnorePatterns` et `ContextHints` (sans espace).

L'exemple suivant montre la structure complète d'un `filtering.md` fichier :

```
# filtering.md

## Code Review

### IgnorePatterns

**/*.md

/myapp/src/**/*.snap
```

```
/myapp/config/README

### ContextHints

- The backend is a trusted system and won't return non-standard protocols.
- URL is generated from server with presigned token, so no SSRF security
 vulnerabilities.
- AppSec has verified that we are allowed to use cache with an eviction policy.
```

Ignorer les modèles

Cette `IgnorePatterns` section indique les fichiers et les dossiers que l'agent de sécurité AWS doit ignorer lors de la révision du code. Permet `glob patterns` de définir les chemins à exclure de l'analyse.

Exigences relatives au format :

- Chaque motif doit être sur sa propre ligne.
- Séparez chaque motif par une ligne vide entre eux. Cela garantit que le fichier s'affiche correctement lorsqu'il est affiché dans les GitHub outils de révision du code.
- Les motifs suivent le format standard du globe. Par exemple, `**/*.md` correspond à tous les fichiers Markdown et `/myapp/src/**/*.snap` correspond à tous les `.snap` fichiers du `/myapp/src/` dossier situé à la racine.
- Nous prenons en charge jusqu'à 1 000 modèles d'ignorance dans cette section.

Indications contextuelles

Cette `ContextHints` section fournit un contexte supplémentaire sur votre base de code afin d'aider AWS Security Agent à effectuer des évaluations plus précises. Utilisez des indications contextuelles pour expliquer les décisions architecturales, les exceptions de sécurité ou d'autres informations susceptibles d'affecter la façon dont les résultats sont interprétés.

Exigences relatives au format :

- Chaque indice doit commencer par un tiret (`-`) suivi d'un espace.
- Écrivez chaque indice sous la forme d'une seule ligne de texte libre limitée à 500 caractères.
- Chaque indice doit décrire un élément de contexte spécifique concernant votre base de code.
- Nous prenons en charge jusqu'à 20 indices contextuels dans cette section.

Les indications contextuelles sont appliquées une fois qu'AWS Security Agent a terminé son analyse initiale, ce qui permet de filtrer les résultats qui ne s'appliquent pas à votre cas d'utilisation spécifique.

Étapes suivantes

Après avoir examiné les résultats relatifs à la sécurité du code :

- Mettez à jour votre code en fonction des conseils de correction
- Proposez de nouvelles validations pour déclencher une nouvelle analyse de vos modifications
- Ajustez les paramètres de révision du code si nécessaire (voirthe section called "Activer la révision du code de pull request pour les GitHub référentiels")
- Passez en revue les exigences de sécurité de votre organisation pour comprendre les critères de validation
- Envisagez des tests de pénétration pour une validation complète de la sécurité des applications déployées

Création d'une révision de code

Révisez le code dans l'application Web AWS Security Agent pour analyser vos référentiels de code source et vos sources S3 afin de détecter les failles de sécurité. Les révisions de code permettent d'effectuer une analyse statique complète de l'ensemble de votre base de code, d'identifier les problèmes de sécurité et de fournir des conseils pour y remédier.

Contrairement à la révision de code basée sur les pull requests qui analyse les modifications de code individuelles (voirthe section called "Passez en revue les résultats de sécurité du code dans les pull requests"), les révisions de code à la demande analysent l'intégralité de votre code source pour identifier les failles de sécurité et valider la conformité aux exigences de sécurité de votre entreprise.

Dans cette procédure, vous allez créer une révision de code en sélectionnant les entrées du code source, en configurant les autorisations et en exécutant la révision.

Conditions préalables

Avant de commencer, assurez-vous de disposer des éléments suivants :

- Accès à l'application Web AWS Security Agent
- Au moins un GitHub référentiel connecté ou un compartiment S3 dans votre espace agent

> **Tip**
>
> Si des GitHub référentiels sont déjà connectés à votre espace agent, la révision du code est prête à être utilisée ; aucune configuration supplémentaire n'est requise. Choisissez Démarrer dans l'application Web depuis la carte de révision du code sur votre page Agent Space, ou lancez directement l'application Web.
> Si vous devez connecter des sources supplémentaires ou configurer des compartiments S3, consultezthe section called "Activer la révision du code".

Accédez à la page de révision du code

Accédez à la section de révision du code dans l'application Web.

1. Connectez-vous à l'application Web AWS Security Agent.
2. Dans la barre latérale gauche, choisissez Code reviews.
3. Vous pouvez consulter la liste des révisions de code existantes avec leurs informations sources, l'état de la dernière exécution et le résumé des résultats.

Création d'une révision de code

Configurez une nouvelle révision de code en configurant les entrées et les autorisations du code source.

1. Sur la page de révision du code, choisissez Créer une révision de code.

Configurer les détails de la révision du code

Entrez un titre et sélectionnez le code source à examiner.

1. Dans le champ Titre, entrez un nom descriptif pour votre révision de code.

> **Tip**
>
> Utilisez un nom qui identifie l'application, le référentiel ou l'étendue de la révision. Par exemple, « billing-service-security-review » ou « infrastructure-code-audit ».

2. Dans la section Sources, sélectionnez les entrées de code source pour cette révision. Choisissez l'un des deux onglets suivants :

GitHub référentiels

Faites votre choix parmi les référentiels connectés à votre espace agent.

1. Choisissez l'onglet GitHub Référentiels.
2. Dans le tableau Référentiels intégrés, cochez la case à côté de chaque référentiel que vous souhaitez inclure dans la révision.
3. Utilisez le champ de recherche pour trouver des référentiels spécifiques par nom.

> **Note**
>
> Seuls les référentiels connectés à votre espace agent via la configuration de révision du code apparaissent ici. Pour ajouter d'autres référentiels, choisissez Gérer dans votre console d'administration ou demandez à votre administrateur de mettre à jour la configuration de l'espace agent.

Sources S3

Sélectionnez les fichiers ZIP dans les compartiments S3 connectés à votre espace agent. Votre administrateur Agent Space configure les compartiments S3 disponibles. Tout fichier ZIP stocké dans l'un de ces compartiments peut être utilisé comme source pour une révision de code.

1. Choisissez l'onglet Sources S3.
2. Entrez l'URI S3 de chaque fichier ZIP que vous souhaitez inclure dans la révision. Vous pouvez ajouter jusqu'à 30 sources S3.

> **Note**
>
> Les sources S3 doivent être des fichiers ZIP stockés dans des compartiments S3 connectés à votre espace agent. Pour mettre des compartiments supplémentaires à disposition, voirthe section called “Activer la révision du code”.

Configurer les autorisations

Sélectionnez le rôle de service IAM et le groupe de CloudWatch journaux facultatif pour cette révision du code.

1. Dans la section Autorisations, recherchez la liste déroulante des rôles de service.
2. Sélectionnez le rôle IAM parmi les rôles de service que vous avez configurés.

> **Note**
>
> Le rôle de service doit être autorisé à accéder à votre code source dans S3 et à écrire dans CloudWatch les journaux, ainsi que dans toute autre ressource AWS nécessaire à la révision du code. Les rôles de service sont configurés lors de la configuration de la révision du code dans l'AWS Management Console.

3. (Facultatif) Dans la liste déroulante des groupes de CloudWatch journaux, sélectionnez un groupe de journaux pour stocker les journaux d'exécution des révisions de code.

> **Note**
>
> Si vous ne sélectionnez aucun groupe de journaux, AWS Security Agent crée un groupe de journaux par défaut pour stocker les journaux de révision du code.

Configurer la correction automatique du code

Activez la correction automatique pour qu'AWS Security Agent génère des correctifs de code pour tous les résultats dès que l'examen est terminé.

1. Dans la section Correction automatique du code, cochez la case Activer la correction automatique du code.

La manière dont AWS Security Agent fournit le correctif dépend de la source :

- GitHub Référentiels privés : AWS Security Agent envoie une pull request contenant le correctif au référentiel.
- GitHub Référentiels publics : pour éviter de révéler la vulnérabilité avant qu'elle ne soit corrigée, AWS Security Agent n'ouvre pas de pull request. Au lieu de cela, il ajoute une suggestion de

différence à la découverte que vous pouvez télécharger depuis l'application Web et postuler en privé.

- Sources S3 : la correction du code n'est pas disponible. Passez en revue les détails des résultats et appliquez les correctifs manuellement.

> **Important**
>
> Les pull requests de correction soumises à des référentiels privés sont visibles par toutes les personnes disposant d'un accès en lecture. Vérifiez les modifications avant de procéder à la fusion. La correction automatique du code n'est disponible que lorsque GitHub les référentiels sont sélectionnés comme source.

> **Note**
>
> Lorsque cette option est désactivée, vous pouvez toujours déclencher manuellement la correction du code en fonction des GitHub-sourced résultats individuels une fois la révision terminée.

Configuration de la validation simulée

Activez la validation simulée pour confirmer dynamiquement si les vulnérabilités découvertes sont exploitables dans une application en cours d'exécution.

1. Dans la section Validation simulée, cochez la case Activer la validation simulée.

Lorsqu'il est activé, AWS Security Agent met en service un environnement simulé une fois l'analyse statique terminée. Il intègre votre code source, démarre les services au sein de l'environnement et tente d'exploiter les vulnérabilités détectées lors de l'analyse. Les résultats sont ensuite mis à jour avec un statut de validation indiquant si la vulnérabilité a été exploitée avec succès.

> **Note**
>
> La validation simulée n'est actuellement disponible que pour les applications dockerisables autonomes. Lorsque plusieurs référentiels sont sélectionnés comme sources, la validation simulée n'est pas disponible.

> **Important**
>
> La validation simulée ajoute du temps de traitement à votre exécution de révision du code. L'étape de validation provisionne un environnement et exécute des tentatives d'exploitation. Cela prend généralement 1 à 3 heures en fonction du nombre de résultats et de la complexité de l'application.

Destinations réseau autorisées

L'accès au réseau sortant de l'environnement simulé est limité à une liste d'autorisation prédéfinie. Votre application peut atteindre les domaines suivants lors de la validation :

Le tableau suivant répertorie les domaines autorisés et leurs objectifs.

Domain	Objectif
`.amazonaws.com` , `.aws.amazon.com`	Services AWS
`.public.ecr.aws`	Amazon ECR Public
`.docker.com` , `.docker.io`	Docker Hub
`.github.com` , `.githubusercontent.com`	GitHub
`.gitlab.com`	GitLab
`.npmjs.com` , `.npmjs.org`	registre npm

Domain	Objectif
`.pypi.org` , `.pypi.python.org` , `.pythonhosted.org`	Index des packages Python
`.crates.io` , `.rustup.rs`	Paquets Rust
`.maven.org` , `.gradle.org`	Java/Gradle colis
`.nuget.org`	Paquets .NET
`.rubygems.org` , `.ruby-lang.org`	Paquets Ruby
`.golang.org` , `.pkg.go.dev` , `.goproxy.io`	Forfaits Go
`.nodejs.org` , `.yarnpkg.com`	Node.js
`.alpinelinux.org` , `.debian.org` , `.ubuntu.com` , `.centos.org` , `.fedoraproject.org`	Référentiels de distribution Linux
`.cloudfront.net`	CloudFront distributions
`.google.com` , `.googleapis.com`	API Google
`.microsoft.com` , `.visualstudio.com`	Services Microsoft
`.sourceforge.net` , `.bitbucket.org`	Hébergement source

> **Note**
>
> Si votre application nécessite un accès réseau à des domaines ne figurant pas dans cette liste, la connexion sera bloquée par le pare-feu réseau. Les applications qui dépendent d'API ou de services externes non répertoriés ci-dessus risquent de ne pas démarrer correctement dans l'environnement simulé.

Création de la révision du code

1. Vérifiez votre configuration pour garantir son exactitude.
2. Choisissez Créer une révision de code.

Vous êtes redirigé vers la page détaillée de révision du code où vous pouvez démarrer une révision.

Exécuter une révision du code

Après avoir créé une révision de code, lancez une exécution pour commencer l'analyse.

1. Sur la page détaillée de la révision du code, choisissez Commencer la révision.
2. AWS Security Agent commence à analyser votre code source.

Vous pouvez également démarrer une révision depuis la page de liste des révisions de code en choisissant Commencer la révision à côté de la révision de code que vous souhaitez exécuter.

Surveiller l'exécution d'une révision de code

Suivez la progression de la révision de votre code au fur et à mesure de son exécution.

Passez en revue les phases d'exécution

Une révision de code passe par les phases suivantes, affichées sous forme d'indicateur de progression :

1. Preflight — L'agent de sécurité AWS valide l'accès à votre code source et configure l'environnement de test. Les contrôles avant vol incluent :
   - Configuration de l'infrastructure de service
   - Validation de l'accès aux sources S3

- Configuration de l'environnement de test

2. Analyse statique : AWS Security Agent analyse votre code source pour détecter les failles de sécurité et les violations des exigences.
3. Validation simulée (facultatif) : si la validation simulée est activée, AWS Security Agent met en service un environnement simulé et déploie votre application. Il tente ensuite d'exploiter les vulnérabilités découvertes lors de l'analyse statique. Cette étape confirme si les résultats sont exploitables dans l'environnement d'exécution cible. Cette phase apparaît uniquement lorsque vous activez la validation simulée lors de la création de la révision du code.
4. Finalisation — L'agent de sécurité AWS compile les résultats et génère le résumé des résultats.

Afficher les détails de la course

Sur la page détaillée de l'exécution, naviguez entre les onglets pour suivre la progression :

- Exécution de la révision du code : affichez le résumé de l'exécution, y compris l'ID d'exécution, l'heure de création, le statut, la durée, les heures de tâche, la répartition des niveaux de gravité et le graphique des types de risques.
- Prévol — Consultez la progression du contrôle avant vol et le statut de chaque étape de validation.
- Journaux de révision du code : consultez les tâches identifiées et effectuées par AWS Security Agent au cours de la révision, avec des journaux de tâches détaillés pour chaque étape.
- Validation simulée : lorsque la validation simulée est activée, consultez l'état du provisionnement, les tâches de validation pour les résultats individuels et leurs résultats.
- Résultats — Consultez les résultats de sécurité une fois l'examen terminé (voirthe section called "Examiner les résultats d'une révision de code").

Historique des courses

Chaque révision de code conserve un historique de toutes les exécutions. Sur la page détaillée de la révision du code :

- La section Dernière exécution indique la dernière exécution avec son heure de début, son statut, sa durée et son ID.
- Le tableau Toutes les exécutions répertorie toutes les exécutions précédentes avec leur heure de début, leur statut, leur durée, le résumé des résultats et leur identifiant.
- Choisissez Surveiller l'exécution pour afficher les détails de la dernière exécution active.

- Choisissez le lien vers l'heure de début de n'importe quelle course pour en afficher tous les détails.

Étapes suivantes

Après avoir effectué une révision du code :

- Consultez les résultats de sécurité et les conseils de correction correspondants (voirthe section called “Examiner les résultats d'une révision de code”)
- Corrigez les résultats par le biais de pull requests automatisées ou de corrections manuelles (voirthe section called “Corriger les résultats de la révision du code”)
- Exécuter des révisions supplémentaires après avoir mis en œuvre les correctifs pour vérifier les mesures correctives
- Ajustez votre configuration de révision de code ou vos sources à mesure que votre base de code évolue

Examiner les résultats d'une révision de code

Une fois la révision du code terminée, consultez le résumé de l'exécution et les résultats de sécurité pour comprendre les vulnérabilités de votre code source. Chaque résultat contient une description, une note de gravité, l'emplacement des codes, une analyse des risques et des suggestions de solutions pour vous aider à hiérarchiser les problèmes de sécurité et à les résoudre.

Conditions préalables

Avant de commencer, assurez-vous de disposer des éléments suivants :

- Une révision de code terminée ou en cours
- Accès à l'application Web AWS Security Agent

Étape 1 : Accédez à l'exécution de la révision du code

Accédez à votre analyse de code terminée pour consulter le résumé et les résultats.

1. Connectez-vous à l'application Web AWS Security Agent.
2. Dans la barre latérale gauche, choisissez Code reviews.
3. Sélectionnez la révision de code que vous souhaitez examiner.

4. Dans le tableau Toutes les exécutions, sélectionnez l'exécution terminée en cliquant sur le lien correspondant à son heure de début. Vous pouvez également choisir Monitor run pour afficher la dernière exécution.

Étape 2 : Surveiller la progression de l'exécution

Suivez la progression de la révision de votre code à l'aide de l'indicateur d'étape.

1. Repérez l'indicateur d'étape horizontal sous l'en-tête de page.
2. Vérifiez le statut de chaque phase :
   - Preflight — Valide l'accès à votre code source et configure l'environnement de numérisation. Les contrôles incluent la configuration de l'infrastructure de service, la validation de l'accès aux sources S3 et la configuration de l'environnement de test, qui inclut les contrôles GitHub d'accès.
   - Analyse statique : analyse votre code source pour détecter les failles de sécurité et les violations des exigences.
   - Validation simulée (facultative) : lorsque cette option est activée, elle fournit un environnement simulé et tente d'exploiter les vulnérabilités découvertes dans l'application en cours d'exécution.
   - Finalisation — Compile les résultats et génère le résumé des résultats.

> **Note**
>
> Chaque étape affiche un indicateur d'état (terminé ou en cours). L'exécution est terminée lorsque toutes les phases sont affichées comme terminées. L'étape de validation simulée apparaît uniquement lorsque vous activez la validation simulée lors de la création de la révision du code.

Étape 3 : consulter le résumé de l'exécution

Accédez à l'onglet Exécution de la révision du code pour afficher les résultats de haut niveau.

1. Sélectionnez l'onglet Exécution de la révision du code.
2. La section Récapitulatif de l'exécution fournit le statut, la durée de l'exécution et d'autres détails de haut niveau. Il fournit également un tableau de bord des résultats de sécurité classés par niveau de gravité et par type de risque.

3. La présentation de l'application par AWS Security Agent fournit un résumé de l'analyse de révision du code une fois l'exécution terminée.

Étape 4 : Examiner les résultats avant le vol

Accédez à l'onglet Preflight pour vérifier que tous les contrôles d'accès à la source ont été réussis.

1. Sélectionnez l'onglet Preflight.
2. Passez en revue l'indicateur de progression avant le vol indiquant le nombre de vérifications effectuées.
3. Vérifiez que chaque vérification indique un statut de réussite :
   - Configuration de l'infrastructure de service : confirme que l'environnement de test est prêt
   - Validation de l'accès à la source S3 — Confirme l'accès au code source S3 (le cas échéant)
   - Configuration de l'environnement de test : confirme que l'environnement d'analyse est configuré

> **Note**
>
> Si une vérification préalable au vol échoue, l'analyse statique ne sera pas exécutée. Passez en revue les détails de la vérification pour identifier et résoudre les problèmes d'accès, puis lancez une nouvelle exécution.

Étape 5 : Examiner les journaux de révision du code

Accédez à l'onglet Journaux de révision du code pour consulter les tâches effectuées par AWS Security Agent pendant l'analyse.

1. Sélectionnez l'onglet Journaux de révision du code.
2. Parcourez la liste des tâches dans le panneau de gauche.
3. Sélectionnez une tâche pour afficher son journal détaillé dans le panneau de droite.

> **Tip**
>
> Utilisez le champ de recherche pour filtrer les tâches par nom. Les journaux fournissent un aperçu de ce que l'agent de sécurité AWS a examiné et de la manière dont il est parvenu à ses conclusions.

Étape 6 : Accédez aux résultats

Sélectionnez l'onglet Résultats pour afficher tous les résultats de sécurité issus de l'exécution.

> **Note**
>
> Filtre de confiance par défaut
>
> Par défaut, vous ne voyez que les résultats présentant un niveau de confiance élevé pour les agents. Pour afficher également les résultats présentant un niveau de confiance moyen ou faible et les faux positifs, désactivez le bouton Masquer les résultats non vérifiés.

1. Sélectionnez l'onglet Résultats.
2. Les résultats s'affichent dans une vue divisée avec la liste des résultats sur la gauche et les détails du résultat sélectionné sur la droite.
3. Passez en revue les informations affichées sur chaque fiche de recherche :
   - Recherche du titre : nom descriptif résumant le problème de sécurité
   - Badge de Color-coded gravité — indicateur de gravité :
     - Critique (rouge) : nécessite une action immédiate ; l'exploitation peut compromettre le système
     - Élevé (rouge) : nécessite une attention rapide ; l'exploitation peut avoir un impact important sur la sécurité
     - Moyen (orange) — Doit être traité dans un délai raisonnable ; contribue au risque de sécurité global
     - Faible (jaune) — Peut être traité dans le cadre d'un entretien régulier ; risque immédiat minimal
   - Dernière mise à jour — Horodatage de la dernière mise à jour du résultat

Étape 7 : Passez en revue les informations de recherche

Sélectionnez des résultats individuels pour afficher des informations complètes sur chaque vulnérabilité.

1. Sélectionnez une recherche dans le panneau de gauche pour afficher ses détails dans le panneau de droite.
2. Passez en revue les actions disponibles :
   - Résoudre le résultat : marquez le résultat comme résolu une fois que vous l'avez corrigé
   - Corriger le code — Génère une pull request avec un correctif (disponible pour les GitHub sources)
3. Faites-nous part de vos commentaires en utilisant Cette constatation était-elle exacte ? — Sélectionnez Oui ou Non pour améliorer la précision des analyses futures.
4. Passez en revue les principaux attributs dans la section Vue d'ensemble :
   - Confiance des agents — Le niveau de confiance d'AWS Security Agent dans cette constatation
   - Sévérité — Le niveau de risque avec un badge à code couleur
   - Type de risque — Catégorie de risque de sécurité
   - État de la validation : lorsque la validation simulée est activée, cela indique si le résultat a été confirmé comme exploitable dans un environnement d'exécution :
     - Confirmé — La vulnérabilité a été exploitée avec succès dans l'environnement simulé
     - Non reproduit — La vulnérabilité n'a pas pu être exploitée dans l'environnement d'exécution cible
     - Échec de la validation — La tentative de validation n'a pas été concluante en raison d'une erreur
     - Non validé — Aucune validation simulée n'a été effectuée pour ce résultat. Cela se produit lorsque la validation n'est pas activée ou que l'étape de validation a expiré avant d'atteindre ce résultat.
   - Résolu — Si le résultat a été résolu (Yes/No)
   - Dernière mise à jour — Horodatage de la dernière mise à jour
5. Développez la section Description pour lire :
   - Une explication détaillée du problème de sécurité
   - Comment la vulnérabilité pourrait être exploitée
   - L'impact potentiel sur votre candidature

- Étapes de vérification effectuées par l'agent pour confirmer le résultat

6. Développez la section Emplacements du code pour afficher :
   - Chemins de fichiers spécifiques dans lesquels le problème a été identifié
   - Une brève description de ce qui a été trouvé à chaque endroit
   - Badges contenant des numéros de ligne renvoyant au code correspondant
7. Développez la section Preuves pour passer en revue :
   - Le code, la configuration ou les observations spécifiques qui appuient le résultat
   - Brève explication des raisons pour lesquelles chaque élément présente la vulnérabilité
   - Les fichiers concernés et les numéros de ligne pour chaque élément de preuve
8. Développez la section Correctif suggéré pour afficher :
   - Les modifications recommandées par AWS Security Agent pour remédier à cette constatation
   - Exemple de code ou de configuration pour chaque modification recommandée

> **Tip**
>
> Utilisez les emplacements du code pour accéder rapidement aux fichiers concernés dans votre référentiel. Chaque emplacement inclut suffisamment de contexte pour comprendre le problème sans lire l'intégralité du fichier.

Étape 8 : Prioriser et traiter les résultats

Validez les résultats et prenez les mesures nécessaires pour corriger les vulnérabilités et améliorer le niveau de sécurité de votre application.

Pour les résultats de gravité élevée associés à un niveau de fiabilité élevé avec un agent :

1. Lisez attentivement les sections Description et Emplacement du code.
2. Utilisez le code de correction pour générer une pull request avec un correctif, ou passez en revue les PR de correction automatique si vous avez activé cette option.
3. Planifiez un examen de code de suivi pour vérifier que le correctif est efficace.

Pour les résultats de gravité moyenne présentant un niveau de fiabilité élevé avec un agent :

1. Établissez vos priorités en fonction de votre tolérance au risque et du contexte commercial.

2. Incluez des tâches de correction dans la planification régulière de votre sprint de développement.
3. Déterminez si plusieurs résultats de gravité moyenne combinés créent un risque plus élevé.

Pour les résultats avec un niveau de confiance moyen ou faible :

1. Consultez les sections Description et Emplacement du code pour valider les hypothèses et les conditions dans lesquelles la vulnérabilité se produit.
2. Si la vulnérabilité est valide, établissez des priorités en fonction de la gravité et de la tolérance au risque et envisagez des tâches de correction.

Étape 9 : suivre la progression des mesures correctives

Utilisez l'interface des résultats et des réexécutions pour savoir quelles vulnérabilités ont été corrigées.

1. Lorsque vous mettez en œuvre des correctifs, utilisez Résoudre les résultats pour marquer les résultats comme corrigés.
2. Effectuez une nouvelle révision du code pour vérifier que les correctifs corrigent les résultats et n'introduisent pas de nouveaux problèmes.
3. Consultez le tableau Toutes les exécutions sur la page détaillée de la révision du code pour comparer les résultats entre les exécutions au fil du temps.

> **Tip**
>
> Après avoir fusionné les pull requests de correction, lancez une nouvelle exécution de la même révision du code pour confirmer que les vulnérabilités sont résolues. Comparez le nombre de résultats entre les courses pour suivre vos progrès.

Étapes suivantes

Après avoir examiné les résultats de votre révision du code :

- Priorisez les résultats les plus graves avec un niveau de fiabilité élevé pour une correction immédiate

- Utilisez le code de correction pour générer des correctifs automatisés en fonction des GitHub-sourced résultats (voirthe section called “Corriger les résultats de la révision du code”)
- Exécutez des révisions de code supplémentaires après avoir mis en œuvre des correctifs pour vérifier la correction
- Ajustez vos sources ou paramètres de révision de code au fur et à mesure de l'évolution de votre base de code (voir) the section called “Activer la révision du code”

Corriger les résultats de la révision du code

Après avoir examiné les résultats de sécurité issus d'une révision du code, vous pouvez utiliser AWS Security Agent pour générer des correctifs de code en fonction des résultats trouvés dans les sources GitHub du référentiel. Pour les référentiels privés, AWS Security Agent ouvre une pull request contenant le correctif proposé. Pour les référentiels publics, AWS Security Agent ajoute une différence téléchargeable à la constatation que vous pouvez appliquer localement. Les résultats provenant de sources S3 doivent être corrigés manuellement.

Conditions préalables

Avant de commencer, assurez-vous de disposer des éléments suivants :

- Une revue de code terminée avec les résultats
- GitHub référentiels connectés en tant que source pour la révision du code
- Accès à l'application Web AWS Security Agent
- Connaissance de l'architecture et des exigences de sécurité de votre application

Fonctionnement de la correction du code

Lorsque vous déclenchez la correction du code pour un résultat, AWS Security Agent analyse le résultat et l'emplacement du code, puis génère un correctif de code. La manière dont le correctif est fourni dépend de la source :

- GitHub Référentiels privés : AWS Security Agent envoie une pull request au référentiel concerné. La pull request inclut une description du problème de sécurité et des modifications apportées.
- GitHub Référentiels publics : l'agent de sécurité AWS ajoute une suggestion de différence à la découverte afin que la vulnérabilité ne soit pas révélée avant d'être corrigée. Vous pouvez

télécharger le diff depuis l'application Web et l'appliquer localement avec`git apply /path/to/code_remediation_changes.diff`.

- Sources S3 : la correction du code n'est pas disponible. Utilisez la description du résultat, l'emplacement des codes et le raisonnement relatif aux risques pour appliquer les correctifs manuellement.

> **Important**
>
> Les pull requests créées par AWS Security Agent sont visibles par tous les utilisateurs disposant d'un accès en lecture au référentiel. Passez en revue les modifications avant de les fusionner pour vous assurer qu'elles correspondent aux exigences de votre application.

Correction automatique du code

Si vous avez activé la correction automatique du code lors de la création de la révision du code, AWS Security Agent génère des correctifs pour tous les résultats éligibles dès que la révision est terminée. Aucune action supplémentaire n'est nécessaire : les pull requests apparaissent dans vos GitHub référentiels privés connectés, et des différences apparaissent sur les résultats des GitHub référentiels publics, au fur et à mesure que l'exécution se termine.

Correction manuelle du code

Si la correction automatique du code est désactivée, vous pouvez déclencher la correction pour les résultats individuels provenant GitHub des sources.

1. Accédez à l'onglet Résultats d'une révision de code terminée.
2. Sélectionnez le résultat que vous souhaitez corriger.
3. Dans le volet détaillé de la recherche, choisissez Corriger le code.
4. AWS Security Agent génère un correctif de code et envoie une pull request au référentiel ou joint un diff téléchargeable au résultat, en fonction de la visibilité du référentiel.

Passez en revue les pull requests de remédiation

Une fois qu'AWS Security Agent a envoyé une pull request de correction à un GitHub référentiel privé :

1. Accédez à votre GitHub référentiel.
2. Localisez la pull request créée par l'agent de sécurité AWS.
3. Passez en revue les modifications, notamment :
   - Description expliquant la découverte et le correctif de sécurité
   - Les modifications du code corrigent la vulnérabilité
   - Tout contexte pertinent concernant l'approche de remédiation
4. Fusionnez la pull request si le correctif est approprié, ou fermez-la et implémentez une solution alternative.

> **Tip**
>
> Après avoir fusionné les pull requests de correction, lancez une nouvelle révision du code pour vérifier que les correctifs corrigent les résultats et n'introduisent pas de nouveaux problèmes de sécurité.

Appliquer des différences de correction

Pour les résultats provenant de GitHub référentiels publics, appliquez la différence téléchargeable localement.

1. Dans le panneau des détails de la recherche, téléchargez le diff depuis la section Correction du code.
2. Dans votre clone local du dépôt, exécutez`git apply /path/to/code_remediation_changes.diff`.
3. Passez en revue les modifications appliquées, testez-les par rapport à votre application et validez-les dans le cadre de votre flux de développement normal.

Limitations

- La correction du code n'est disponible que pour les résultats provenant des sources du GitHub référentiel. Les résultats provenant de sources S3 doivent être corrigés manuellement.
- AWS Security Agent génère des correctifs en fonction de son analyse de la vulnérabilité. Passez en revue toutes les modifications avant de les fusionner ou de les valider afin de vous assurer qu'elles sont adaptées à votre application.

- Certains résultats complexes peuvent nécessiter une intervention manuelle au-delà de la correction automatique.

Étapes suivantes

Après avoir corrigé les résultats :

- Passez en revue et fusionnez les pull requests dans vos GitHub référentiels, ou validez les différences appliquées dans le cadre de votre flux de travail normal
- Exécutez une nouvelle révision du code pour vérifier les correctifs et les problèmes restants
- Résoudre les résultats dans l'application Web après avoir confirmé la correction
- Ajustez les sources ou les paramètres de révision du code selon vos besoins (voirthe section called "Activer la révision du code")

Exécuter un scan de code différentiel avec S3

Exécutez une analyse de code différentielle (diff) pour analyser uniquement les lignes modifiées dans votre code source, plutôt que d'effectuer une analyse complète du référentiel. Les analyses différentielles sont plus rapides que les analyses complètes et produisent des résultats ciblés sur des modifications de code spécifiques, ce qui les rend idéales pour la validation avant la fusion dans les flux de travail de développement.

Contrairement à la révision du code basée sur les pull requests, qui est déclenchée automatiquement par les événements d'un fournisseur de contrôle de source tiers (voirthe section called "Passez en revue les résultats de sécurité du code dans les pull requests"), les analyses différentielles sont lancées par programmation via l'API ou le SDK de l'agent de sécurité AWS. Vous chargez un fichier de comparaison unifié dans S3 et vous le référencez lorsque vous démarrez une tâche de révision de code.

Comment fonctionnent les scans différentiels

Un scan différentiel analyse les modifications de code dans le contexte complet de votre référentiel. Lorsque vous créez une ressource de révision de code avec votre code source téléchargé sur S3, l'analyse différentielle utilise le référentiel complet comme contexte tout en concentrant les résultats spécifiquement sur les lignes modifiées dans votre diff. Cela permet à l'analyse d'identifier les problèmes de sécurité liés à la manière dont vos modifications interagissent avec le code existant,

tels que des flux d'authentification interrompus, une gestion non sécurisée des données entre les modules ou des modifications révélant des vulnérabilités existantes.

Le processus de numérisation :. Vous chargez un fichier diff unifié (la sortie de`git diff`) dans un compartiment S3 connecté à votre espace agent. Vous appelez l'`StartCodeReviewJob`API avec un `diffSource` paramètre pointant vers l'emplacement S3 de votre différence. AWS Security Agent analyse uniquement le code modifié dans le diff pour détecter les vulnérabilités en matière de sécurité et la conformité aux exigences de sécurité de votre organisation. Les résultats sont limités aux lignes modifiées, avec des cotes de gravité, des emplacements de code et des conseils de correction.

Conditions préalables

Avant de commencer, assurez-vous de disposer des éléments suivants :

- Un espace agent avec la révision du code activée (voirthe section called “Activer la révision du code”)
- Une ressource de révision de code déjà créée pour le référentiel cible, avec le code source complet téléchargé dans le compartiment S3 connecté à votre espace agent. Le référentiel complet fournit un contexte qui permet une analyse plus approfondie de la manière dont vos modifications interagissent avec le code existant. Consultez the section called “Création d'une révision de code” les instructions relatives à la création d'une révision de code et au téléchargement du code source.
- Un compartiment S3 connecté à votre espace d'agent
- Autorisations IAM pour le téléchargement vers le compartiment S3 et l'appel `securityagent:StartCodeReviewJob`
- Un fichier de comparaison unifié généré à partir de vos modifications de code (par exemple, la sortie de`git diff main..feature-branch`)

> **Tip**
>
> Pour obtenir les résultats les plus précis, assurez-vous que votre ressource de révision de code dispose de la dernière version de votre code source complet téléchargée sur S3. Le diff scan utilise ce référentiel complet comme contexte pour comprendre l'architecture de votre application, les flux de données et les contrôles de sécurité existants lors de l'analyse des lignes modifiées.

Étape 1 : générer un fichier diff

Générez un diff unifié qui représente les modifications de code que vous souhaitez scanner.

```
git diff main..feature-branch > changes.diff
```

Vous pouvez également générer un diff pour les modifications progressives :

```
git diff --cached > changes.diff
```

> **Tip**
>
> Le fichier diff doit être au format diff unifié standard. AWS Security Agent analyse les chemins des fichiers et modifie les lignes des en-têtes diff afin de préciser son analyse.

Étape 2 : télécharger le diff sur S3

Téléchargez le fichier diff dans un compartiment S3 connecté à votre espace agent.

```
aws s3 cp changes.diff s3://my-security-agent-bucket/diffs/changes.diff
```

> **Important**
>
> Le compartiment S3 doit être déjà connecté à votre espace agent. Le rôle de service IAM associé à votre espace agent doit disposer d'un accès en lecture à cet emplacement. Consultez the section called “Activer la révision du code” les instructions relatives à la connexion des compartiments S3.

Étape 3 : démarrer une tâche de révision du code différentiel

Appelez l'`StartCodeReviewJob`API avec le `diffSource` paramètre pour lancer un scan différentiel.

Utilisation de l'AWS CLI

```
aws securityagent start-code-review-job \
```

```
  --agent-space-id "your-agent-space-id" \
  --code-review-id "your-code-review-id" \
  --diff-source '{"s3Uri": "s3://my-security-agent-bucket/diffs/changes.diff"}'
```

Utilisation du kit SDK AWS (Python)

```
import boto3

client = boto3.client('securityagent')

response = client.start_code_review_job(
    agentSpaceId='your-agent-space-id',
    codeReviewId='your-code-review-id',
    diffSource={
        's3Uri': 's3://my-security-agent-bucket/diffs/changes.diff'
    }
)

print(f"Job started: {response['codeReviewJobId']}")
```

Utilisation du kit SDK AWS () JavaScript/TypeScript

```
import { SecurityAgentClient, StartCodeReviewJobCommand } from '@aws-sdk/client-
securityagent';

const client = new SecurityAgentClient({ region: 'us-east-1' });

const response = await client.send(new StartCodeReviewJobCommand({
  agentSpaceId: 'your-agent-space-id',
  codeReviewId: 'your-code-review-id',
  diffSource: {
    s3Uri: 's3://my-security-agent-bucket/diffs/changes.diff',
  },
}));

console.log(`Job started: ${response.codeReviewJobId}`);
```

L'API revient immédiatement avec un `codeReviewJobId` et un `status` de`IN_PROGRESS`.

Étape 4 : Surveiller le scan

Vérifiez l'état de la tâche de révision du code jusqu'à ce qu'elle soit terminée.

```
aws securityagent get-code-review-job \
  --agent-space-id "your-agent-space-id" \
  --code-review-id "your-code-review-id" \
  --code-review-job-id "the-job-id"
```

Le travail progresse selon les mêmes phases qu'une révision complète du code : Preflight → Analyse statique → Finalisation. Les analyses différentielles sont généralement plus rapides que les analyses complètes, car elles analysent moins de lignes de code.

Étape 5 : Examiner les résultats

Une fois la tâche terminée, dressez la liste des résultats de la tâche de révision du code.

```
aws securityagent list-findings \
  --agent-space-id "your-agent-space-id" \
  --code-review-id "your-code-review-id" \
  --code-review-job-id "the-job-id"
```

Chaque résultat inclut :

- Description du problème de sécurité
- Le niveau de gravité (critique, élevé, moyen ou faible)
- Emplacements du code faisant référence à des lignes spécifiques dans le diff
- Raisonnement fondé sur le risque expliquant l'impact potentiel
- Conseils de remédiation

Pour plus d'informations sur la façon de comprendre les résultats et d'y donner suite, consultezthe section called “Examiner les résultats d'une révision de code”.

Quotas et limites

- Nombre maximum de fichiers modifiés dans un différentiel : 3 000 fichiers ou taille totale du diff de 5 Mo
- Les résultats sont plafonnés à 30 par scan, classés par ordre de gravité (Critique > Élevé > Moyen > Faible)

Étapes suivantes

Après avoir effectué un scan différentiel :

- Examiner les résultats et appliquer les directives de remédiation (voirthe section called "Examiner les résultats d'une révision de code")
- Activez les commentaires sur les pull requests pour une révision automatique du code à chaque pull request (voirthe section called "Activer la révision du code de pull request pour les GitHub référentiels")
- Révisez régulièrement l'intégralité du code pour détecter les problèmes autres que ceux liés à des modifications individuelles (voirthe section called "Création d'une révision de code")
- Utilisez l'intégration IDE pour exécuter des analyses différentielles directement depuis votre environnement de développement (voirthe section called "Exécutez des analyses de sécurité du code à partir de votre IDE")

Exécutez des analyses de sécurité du code à partir de votre IDE

Exécutez des scans de sécurité du code AWS Security Agent directement depuis votre IDE à l'aide de Kiro ou Claude Code. L'intégration de l'IDE vous permet de scanner votre code source local pour détecter les failles de sécurité, d'exécuter des analyses différentielles uniquement sur le code modifié et de passer en revue les modèles de menaces sur les documents de conception, le tout sans quitter votre environnement de développement. Les résultats apparaissent à côté de votre code avec des conseils de correction, et vous pouvez appliquer des correctifs automatisés directement depuis l'IDE.

Comment fonctionne l'intégration IDE

L'intégration IDE utilise le serveur AWS Security Agent MCP (Model Context Protocol) pour connecter votre IDE au service AWS Security Agent :

1. Le serveur MCP empaquète votre code source dans une archive ZIP.
2. L'archive est chargée dans un compartiment S3 que le serveur approvisionne automatiquement dans votre compte AWS.
3. Le serveur appelle l'API AWS Security Agent pour démarrer un scan.
4. L'agent de sécurité AWS analyse le code pour détecter les failles de sécurité et la conformité aux exigences de sécurité de votre organisation.

5. Les résultats sont renvoyés à l'IDE avec l'emplacement des codes, des descriptions, des indices de gravité et des suggestions de mesures correctives.

Le serveur MCP gère toute l'orchestration (provisionnement de l'espace agent, création du compartiment S3, configuration du rôle IAM, empaquetage du code et interrogation de scan). Vous n'avez donc besoin que des informations d'identification AWS configurées localement.

> **Note**
>
> La seule condition préalable est la configuration des informations d'identification AWS dans votre environnement local (par exemple`aws configure`, via AWS SSO ou des variables d'environnement). Le serveur MCP approvisionne automatiquement l'espace agent, le rôle de service IAM et le compartiment S3 lors de la première utilisation.

Conditions préalables

Avant de commencer, assurez-vous de disposer des éléments suivants :

- Informations d'identification AWS configurées localement avec les autorisations suivantes :
  - `iam:CreateRole`, `iam:PutRolePolicy` (pour une configuration unique du rôle de service)
  - `s3:CreateBucket`, `s3:PutObject`, `s3:PutPublicAccessBlock`, `s3:PutLifecycleConfiguration`
  - `securityagent:CreateAgentSpace`, `securityagent:UpdateAgentSpace`, `securityagent:ListAgentSpaces`, `securityagent:BatchGetAgentSpaces`
  - `securityagent:CreateCodeReview`, `securityagent:StartCodeReviewJob`, `securityagent:BatchGetCodeReviewJobs`
  - `securityagent:ListFindings`, `securityagent:BatchGetFindings`
  - `securityagent:StartCodeRemediation`(pour les corrections automatisées)
  - `sts:GetCallerIdentity`
- uv installé (exécuteur de paquets Python)
- Python 3.10 ou version ultérieure
- L'un des IDE suivants :
  - Kiro (installation de l'AWS Security Agent Power)
  - Claude Code (installez le plug-in AWS Security Agent)

Installation du serveur MCP

Kiro

Installez AWS Security Agent Power depuis le Kiro Marketplace. Le Power regroupe la configuration du serveur MCP, les instructions de pilotage et les hooks du cycle de vie pour des suggestions d'analyse de sécurité automatiques.

Vous pouvez également configurer le serveur MCP manuellement dans le fichier de `.kiro/mcp.json` votre projet :

```
{
  "mcpServers": {
    "security-agent": {
      "command": "uvx",
      "args": ["awslabs.security-agent-mcp-server@latest"],
      "env": {
        "AWS_PROFILE": "default",
        "AWS_REGION": "us-east-1",
        "FASTMCP_LOG_LEVEL": "ERROR"
      }
    }
  }
}
```

Claude Code

Installez le plug-in AWS Security Agent, qui fournit des compétences en matière de configuration, d'analyses complètes, d'analyses différentielles, de révision des modèles de menaces et de correction.

Configurez le serveur MCP dans celui de `.mcp.json` votre projet :

```
{
  "mcpServers": {
    "awslabs.security-agent-mcp-server": {
      "command": "uvx",
      "args": ["awslabs.security-agent-mcp-server@latest"],
      "env": {
        "AWS_PROFILE": "default",
        "AWS_REGION": "us-east-1",
```

```
        "FASTMCP_LOG_LEVEL": "ERROR"
      }
    }
  }
}
```

> **Tip**
>
> Vous pouvez également exécuter le serveur MCP via Docker si vous préférez ne pas installer Python localement. Consultez la documentation du serveur MCP pour la configuration de Docker.

First-time configuration

Lors de la première utilisation, le serveur MCP met automatiquement en service les ressources AWS requises :

Ressource	Convention de dénomination	Objectif
Espace des agents	User-chosen ou créé automatiquement	Conteneur pour les scans, les révisions et les pentests
Rôle de service IAM	`SecurityAgentScanRole`	Supposé par `securityagent.amazonaws.com` pour lire le code téléchargé
compartiment S3	`security-agent-scans-{account}-{region}`	Stocke le code source compressé (cycle de vie d'expiration automatique de 30 jours)

Pour déclencher la configuration de manière explicite, demandez à votre IDE :

```
Set up the security agent
```

La configuration vérifie vos informations d'identification AWS, crée ou réutilise un espace d'agent, provisionne le rôle IAM et le compartiment S3, et confirme que vous êtes prêt. Si vous disposez déjà

d'espaces d'agent depuis l'AWS Management Console, le programme d'installation les affiche et vous demande lequel utiliser.

> **Note**
>
> Le programme d'installation s'exécute automatiquement lors de votre première analyse s'il n'est pas déjà configuré. Il n'est pas nécessaire de l'exécuter séparément.

Exécuter une analyse de sécurité complète

Analysez l'ensemble de votre projet pour détecter les failles de sécurité :

```
Scan this project for security issues
```

L'IDE :

1. Archive votre code source (à l'exception `.git` des artefacts de construction et des autres répertoires non essentiels) `node_modules`
2. Télécharge l'archive sur S3
3. Démarre une tâche de révision complète du code
4. Sondages à compléter (généralement environ 1 heure)
5. Présente les résultats regroupés par gravité

Progression du scan

Les analyses complètes prennent généralement environ 1 heure selon la taille de la base de code. L'IDE vérifie la progression toutes les 5 minutes et vous avertit lorsque les résultats sont prêts. Vous pouvez demander le statut à tout moment :

```
How's the scan going?
```

Exécuter un scan différentiel

Pour un feedback plus rapide pendant le développement, scannez uniquement le code qui a changé depuis une référence git :

```
Scan my changes against main for security issues
```

Par défaut, si vous ne spécifiez pas de référence de base, l'analyse compare vos modifications non validées avec celles-ci. `HEAD` Vous pouvez spécifier une base différente de manière explicite :

```
Diff scan my uncommitted changes
```

Les analyses différentielles téléchargent à la fois le contexte complet du référentiel et le correctif git diff, puis exécutent une analyse axée uniquement sur les lignes modifiées. Les résultats arrivent généralement en 5 à 15 minutes.

Pour plus d'informations sur l'API de scan différentiel S3, consultezthe section called “Exécuter un scan de code différentiel avec S3”.

Exécuter un examen du modèle de menace

Analysez les documents de conception pour détecter les changements de posture de sécurité à l'aide de la méthodologie STRIDE :

```
Run a threat model review on my spec
```

L'IDE identifie vos `design.md` fichiers `requirements.md` et (généralement sous `.kiro/specs/`), les télécharge avec votre code source et exécute une analyse du modèle de menace. Les résultats identifient :

- Menaces de sécurité classées par STRIDE (usurpation d'identité, falsification, répudiation, divulgation d'informations, déni de service, élévation de privilèges)
- Cotes de gravité pour chaque menace
- Impact sur des actifs spécifiques de votre base de code
- Recommandations en matière d'atténuation

> **Tip**
>
> Révisez le modèle de menace avant de générer des tâches de mise en œuvre à partir d'une spécification. Cela permet de détecter les problèmes de conception de sécurité avant que le code ne soit écrit.

Examen des résultats

Une fois l'analyse terminée, les résultats apparaissent dans votre IDE regroupés par gravité :

```
# CRITICAL: SQL Injection in user-service.ts
   File: src/api/user-service.ts:45
   User input flows directly into SQL query without parameterization

# HIGH: Hardcoded credentials in config.ts
   File: src/config/database.ts:12
   Database password stored in source code
```

Un rapport détaillé est également rédigé `.security-agent/findings-{scan_id}.md` avec des informations complètes pour chaque constatation, notamment le type de risque, le score de confiance, l'emplacement des codes et le code de correction.

Pour consulter les résultats d'une analyse précédente, procédez comme suit :

```
Show my security findings
```

Appliquer des correctifs automatisés

Après avoir examiné les résultats, appliquez des mesures correctives automatisées :

```
Fix the security findings
```

L'IDE analyse les résultats du haut vers le bas en fonction de leur gravité (Critique → Élevé → Moyen → Faible), en appliquant des corrections de code en utilisant les conseils de correction fournis pour chaque résultat. Une fois tous les correctifs appliqués, il exécute automatiquement un scan de vérification pour confirmer que les problèmes sont résolus.

Vous pouvez également corriger des résultats individuels :

```
Fix the SQL injection in user-service.ts
```

> **Important**
>
> Passez toujours en revue les correctifs automatisés avant de les valider. Vérifiez que les correctifs ne perturbent pas les fonctionnalités existantes et n'introduisent pas de régressions.

Suggestions de numérisation automatique (Kiro)

Lorsque vous utilisez le Kiro Power, l'agent de sécurité AWS peut automatiquement suggérer des analyses différentielles une fois que vous avez apporté des modifications de code sensibles à la sécurité. The Power installe un crochet qui évalue chaque tour de codage terminé et suggère un scan lorsque les modifications affectent :

- Logique d'authentification ou d'autorisation
- Cryptographie ou gestion des secrets
- Validation des entrées ou nettoyage des données
- Demandes réseau ou intégrations externes
- Configuration de sécurité (CORS, en-têtes, gestion de session)

Vous pouvez désactiver les suggestions automatiques à tout moment en les supprimant `.kiro/hooks/security-diff-scan-suggester.kiro.hook`.

Types de scan disponibles

Type d'analyse	Duration	Cas d'utilisation	Commande
Analyse complète	Environ 1 heure	Examen complet de l'ensemble de la base de code	« Scannez mon projet pour détecter des problèmes de sécurité »
Numérisation différentielle	5 à 15 minutes	Code modifié uniquement (pré-commit, pré-PR)	« Analyser mes modifications » ou « Analyser différemment par rapport au fichier principal »
Modèle de la menace	5 à 30 minutes	Documents de conception (requirements.md, design.md)	« Exécuter un examen du modèle de menace selon mes spécifications »

Variables d'environnement

Variable	Description	Par défaut
`AWS_REGION`	Région AWS pour les appels SecurityAgent d'API	`us-east-1`
`AWS_PROFILE`	Nom du profil d'identification AWS	Profil par défaut
`FASTMCP_LOG_LEVEL`	Niveau de journalisation du serveur MCP (DEBUG, INFO, WARNING, ERROR)	`WARNING`

Résolution des problèmes

« Non configuré. Exécutez d'abord le programme d'installation. »

`.security-agent/config.json`Il vous manque ou l'espace agent n'existe plus. Demandez à l'IDE d'exécuter le programme d'installation :

```
Set up the security agent
```

Le scan échoue avec AccessDenied

Assurez-vous que vos informations d'identification AWS disposent des autorisations IAM requises répertoriées dans la section Conditions préalables. L'autorisation manquante la plus courante est `iam:CreateRole` (nécessaire uniquement pour la première configuration).

Le scan expire ou prend trop de temps

- Les analyses complètes sur de grandes bases de code peuvent prendre plus d'une heure
- Utilisez des scans différentiels pour le développement itératif : ils se terminent en quelques minutes
- Vérifiez que votre archive source ne contient pas de répertoires inutiles (le serveur MCP exclut automatiquement les modèles courants)

Différentiel vide : aucune modification à scanner

Si vous exécutez une analyse différentielle sans aucune modification non validée, le serveur MCP indique « Aucune modification par rapport à HEAD » et ne lance pas d'analyse. Commencez par valider ou organiser vos modifications, ou spécifiez une référence de base différente.

Quotas et limites

- Taille maximale de l'archive source : 2 Go
- Cycle de vie du compartiment S3 : le code téléchargé est automatiquement supprimé au bout de 30 jours

Étapes suivantes

Après avoir exécuté votre première analyse de sécurité IDE :

- Activez les commentaires de révision du code pull request pour une GitHub intégration automatisée (voirthe section called “Activer la révision du code de pull request pour les GitHub référentiels”)
- Configurer les exigences de sécurité pour la validation des politiques spécifiques à l'organisation (voir) the section called “Gérer les exigences de sécurité”
- Exécutez des analyses complètes périodiques pour détecter les problèmes dans l'ensemble de votre base de code (voirthe section called “Création d'une révision de code”)
- Utilisez les révisions des modèles de menace pour les nouvelles spécifications des fonctionnalités avant leur mise en œuvre

Créez un test de pénétration

Configurez des tests de pénétration automatisés pour vos applications Web en configurant l'étendue des tests, les domaines cibles et l'accès aux ressources AWS. Les tests d'intrusion aident à identifier les failles de sécurité des applications en cours d'exécution en simulant des scénarios d'attaque réels contre vos domaines vérifiés.

AWS Security Agent effectue des tests de sécurité complets sur vos applications Web en fonction de l'étendue et des autorisations configurées, fournissant des informations détaillées sur les vulnérabilités exploitables avant que les attaquants ne puissent les découvrir.

Dans cette procédure, vous allez créer un test d'intrusion en configurant les détails du test, en définissant la portée du test et en configurant les autorisations requises.

Conditions préalables

Avant de commencer, assurez-vous de disposer des éléments suivants :

- Accès à l'application Web AWS Security Agent
- Au moins un domaine vérifié pour les tests
- Rôle IAM avec les autorisations appropriées pour AWS Security Agent
- Compréhension de l'architecture et des chemins critiques de votre application

Commencez à créer un test de pénétration

Accédez à la page de création du test d'intrusion dans l'application Web Agent.

1. Connectez-vous à l'application Web AWS Security Agent.
2. Accédez à la section Tests de pénétration.
3. Choisissez Créer un test d'intrusion.

> **Tip**
>
> Seuls les domaines vérifiés peuvent être inclus dans les tests d'intrusion. Demandez à votre administrateur de vérifier le domaine dans la console de gestion AWS. Consultez the section called “Activer un domaine d'application pour les tests de pénétration”.

Donnez un nom à votre test de pénétration

Fournissez un nom descriptif qui aide à identifier l'objectif et la portée de ce test d'intrusion.

1. Dans le champ Nom du test de pénétration, entrez un nom descriptif pour votre test d'intrusion.

   Example

   Le nom doit clairement identifier l'application, l'environnement ou le composant testé. 100 caractères maximum.

Configuration de la portée du test de pénétration

Définissez les domaines et les chemins d'URL qui seront testés, et configurez les exclusions facultatives pour contrôler les limites des tests.

Ajouter des domaines cibles

Spécifiez les domaines vérifiés qui seront activement testés pour détecter les failles de sécurité.

1. Dans la section Étendue du test de pénétration, recherchez les URL cibles.
2. Développez la section Domaines vérifiés pour afficher les domaines disponibles.
3. Dans le champ URL cible, entrez l'URL du domaine cible.

> **Important**
>
> Seuls les domaines vérifiés peuvent être testés. L'URL doit appartenir à un domaine que vous avez précédemment vérifié dans AWS Security Agent. Sub-domains d'un domaine vérifié ne nécessitent pas de vérification séparée.

4. Pour ajouter plusieurs domaines cibles :
   a. Choisissez Ajouter un domaine.
   b. Entrez l'URL de chaque domaine supplémentaire.
5. Pour supprimer un domaine cible, choisissez Supprimer à côté de l'URL du domaine.

> **Tip**
>
> Pour de meilleurs résultats, incluez tous les domaines qui font partie du flux utilisateur de votre application, y compris les sous-domaines pour les API, les services d'authentification et la diffusion de contenu. Sub-domains d'un domaine parent vérifié ne nécessitent pas de vérification séparée.

Exclure les types de risques (facultatif)

Choisissez des catégories de risque spécifiques à exclure des tests si elles ne s'appliquent pas à votre application.

1. Localisez le champ Exclure les types de risques.
2. Choisissez le menu déroulant pour afficher les types de risques disponibles.
3. Sélectionnez un ou plusieurs types de risques à exclure du test d'intrusion.

> **Note**
>
> L'exclusion des types de risques limite la portée des tests. Excluez uniquement les types de risques qui ne sont pas pertinents pour votre application ou que vous souhaitez tester séparément.

Ajouter des chemins d'URL hors du champ d'application (facultatif)

Spécifiez les chemins d'URL qui ne doivent pas être testés lors du test de pénétration. AWS Security Agent exclut le chemin spécifié et tous les chemins imbriqués en dessous. Par exemple, si vous l'ajoutez `https://example.com/admin` en tant qu'URL hors champ, `https://example.com/admin/tools` c'est également hors champ d'application.

1. Localisez la section Out-of-scope URL.
2. Dans le champ de saisie Out-of-scope URL, entrez le chemin d'URL à exclure (par exemple, `/admin/delete` ou`/api/reset`).

> **Warning**
>
> Out-of-scope les chemins ne sont pas testés pour détecter les vulnérabilités. Assurez-vous d'exclure uniquement les chemins auxquels vous ne devez pas accéder pendant les tests, tels que les opérations destructives ou les fonctions administratives sensibles.

3. Pour ajouter plusieurs chemins hors champ d'application, procédez comme suit :
   a. Choisissez Ajouter une URL.
   b. Entrez chaque chemin supplémentaire.
4. Pour supprimer un chemin, choisissez Supprimer à côté du chemin.

Ajouter des domaines accessibles (facultatif)

Spécifiez les domaines requis pour le test, mais qui ne sont pas des cibles pour les tests de vulnérabilité.

1. Localisez la section URL accessibles.
2. Dans le champ de saisie URL accessibles, entrez un domaine qui doit être accessible pendant les tests.

> **Note**
>
> Ajoutez des domaines accessibles pour les services tiers (tels que Okta, Auth0, Stripe) situés en dehors de votre domaine cible. Cela est nécessaire pour qu'AWS Security Agent puisse accéder à ces URL pour se connecter et naviguer pendant les tests. AWS Security Agent n'effectue PAS de tests d'intrusion dans ces domaines ; ils sont utilisés uniquement à des fins d'accès. Les domaines accessibles ne nécessitent pas de vérification de propriété, même s'ils appartiennent à un domaine différent de celui de votre cible. Seuls les domaines cibles nécessitent une vérification de propriété.

3. Pour ajouter plusieurs domaines accessibles :
   a. Choisissez Ajouter une URL.
   b. Entrez chaque domaine supplémentaire.
4. Pour supprimer un domaine, choisissez Supprimer à côté du domaine.

Ajouter des en-têtes HTTP personnalisés (facultatif)

Spécifiez les en-têtes HTTP personnalisés qui seront ajoutés à toutes les demandes effectuées par AWS Security Agent lors des tests d'intrusion.

1. Localisez la section En-têtes HTTP personnalisés.
2. Dans le champ de saisie des en-têtes HTTP personnalisés, entrez le nom et la valeur de l'en-tête qui seront associés aux demandes sortantes.

> **Note**
>
> Par défaut, AWS Security Agent ajoute un en-tête personnalisé à User-Agentdéfinir sur securityagent, sauf si une valeur d'User-Agenten-tête personnalisée différente est spécifiée.

3. Pour ajouter plusieurs en-têtes personnalisés :
   a. Sélectionnez Add header.

b. Entrez chaque en-tête personnalisé supplémentaire.

4. Pour supprimer un en-tête personnalisé, choisissez Supprimer à côté de l'en-tête.

Configurer le rôle IAM

Sélectionnez le rôle de service préconfiguré pour ce test d'intrusion. AWS Security Agent utilise un modèle d' Space-based autorisation d'agent dans lequel les administrateurs configurent les rôles IAM lors de la configuration de votre espace agent. Vous pouvez sélectionner des rôles déjà configurés et prêts à être utilisés.

1. Dans la section Autorisations, recherchez la liste déroulante des rôles de service.
2. Sélectionnez le rôle IAM qui accorde à AWS Security Agent l'accès aux ressources AWS requises.

> **Important**
>
> Le rôle IAM sélectionné doit être autorisé à accéder aux ressources VPC CloudWatch , aux journaux et à tout autre service AWS nécessaire au test d'intrusion. Vérifiez que le rôle possède la bonne relation de confiance avec AWS Security Agent.

3. Localisez la liste déroulante des groupes de CloudWatch journaux.
4. Sélectionnez le groupe de journaux dans lequel les journaux des tests d'intrusion seront stockés. (facultatif)

> **Note**
>
> Le groupe de CloudWatch journaux sélectionné stockera des journaux détaillés de l'exécution du test d'intrusion, y compris les demandes effectuées, les réponses reçues et les vulnérabilités découvertes.
> Si vous ne sélectionnez aucun groupe de journaux, un nouveau groupe de CloudWatch journaux sera automatiquement créé avec le `/aws/securityagent` préfixe pour stocker les journaux des tests d'intrusion.

Correction automatique du code

Cochez la case Activer la correction automatique.

> **Important**
>
> Pour remédier aux problèmes de sécurité dans vos référentiels de code source, AWS Security Agent peut envoyer des pull requests à vos référentiels. Les pull requests peuvent être visibles par tous les utilisateurs disposant d'un accès en lecture aux référentiels.

Configurer les ressources VPC (facultatif)

Si vos domaines cibles sont privés et hébergés au sein d'un VPC, configurez les paramètres du VPC dans lequel AWS Security Agent doit exécuter des tests de pénétration. Cette étape n'est nécessaire que pour les applications qui ne sont pas accessibles au public.

> **Note**
>
> Ignorez cette étape si vos domaines cibles sont accessibles au public. La configuration VPC n'est requise que pour tester des applications privées hébergées dans un Amazon Virtual Private Cloud.

Choisissez le VPC, les sous-réseaux et les groupes de sécurité pour l'environnement de test d'intrusion.

1. Dans la section VPC, recherchez le menu déroulant VPC ID.
2. Sélectionnez le VPC sur lequel vos domaines cibles sont hébergés.

> **Important**
>
> Le VPC sélectionné doit contenir les domaines cibles que vous avez spécifiés à l'étape 3. Assurez-vous que le VPC dispose d'un routage et d'une configuration réseau appropriés pour permettre à AWS Security Agent d'accéder à vos applications.

3. Localisez la liste déroulante Sous-réseaux.
4. Sélectionnez un ou plusieurs sous-réseaux sur lesquels le test de pénétration doit être exécuté.

> **Note**
>
> Choisissez des sous-réseaux disposant d'un accès réseau à vos applications cibles. Le test de pénétration sera exécuté à partir des ressources déployées dans ces sous-réseaux.

5. Localisez le menu déroulant Groupe de sécurité.
6. Sélectionnez le groupe de sécurité qui contrôle l'accès au réseau pour le test d'intrusion.

> **Important**
>
> Le groupe de sécurité sélectionné doit autoriser le trafic sortant vers vos domaines cibles et tous les domaines accessibles. Assurez-vous que les règles du groupe de sécurité autorisent l'accès réseau nécessaire pour des tests complets.

Configurer les informations d'authentification (facultatif)

Si vos domaines cibles nécessitent une authentification, fournissez des informations d'identification pour permettre à AWS Security Agent d'accéder aux zones protégées de votre application lors des tests d'intrusion. Cette étape n'est nécessaire que pour les applications qui nécessitent une authentification utilisateur.

> **Note**
>
> Ignorez cette étape si vos domaines cibles ne nécessitent pas d'authentification ou si toutes les zones que vous souhaitez tester sont accessibles au public. Configurez les informations d'identification uniquement lorsque vous avez besoin d'AWS Security Agent pour tester les sections authentifiées de votre application.

Ajout d'informations d'identification

Fournissez des informations d'authentification que l'agent de sécurité AWS utilisera pour accéder à votre application.

1. Dans la section Credential #1, sélectionnez une méthode de saisie des informations d'identification :
   - Entrez vos informations d'identification : entrez vos informations d'identification directement dans AWS Security Agent.
   - Paramètre avancé : pour les informations d'identification sensibles, utilisez des options avancées telles qu'AWS Secrets Manager ou les fonctions AWS Lambda. Consultez the section called "Fournir des informations d'authentification pour les tests de pénétration" pour plus de détails.

   > **Tip**
   >
   > Pour les environnements de production ou les informations d'identification sensibles, nous vous recommandons d'utiliser l'option de configuration avancée pour référencer de manière sécurisée les informations d'identification stockées dans AWS Secrets Manager ou dans le magasin de paramètres Systems Manager.

Entrez les informations d'identification

Entrez le nom d'utilisateur et le mot de passe du compte authentifié.

1. Dans le champ Nom d'utilisateur, entrez le nom d'utilisateur pour l'authentification.
2. Dans le champ Mot de passe, entrez le mot de passe pour l'authentification.

> **Important**
>
> Assurez-vous que les informations d'identification que vous fournissez ont des niveaux d'accès appropriés pour les zones que vous souhaitez tester. Les informations d'identification doivent représenter le niveau d'accès typique d'un utilisateur plutôt que des privilèges administratifs.

Sélectionnez le domaine d'accès

Spécifiez le domaine cible qui utilisera ces informations d'identification pour l'authentification.

1. Dans le menu déroulant Accès au domaine, sélectionnez le domaine dans lequel ces informations d'identification seront utilisées.

> **Note**
>
> Si plusieurs domaines cibles nécessitent des informations d'identification différentes, vous pouvez ajouter des ensembles d'informations d'identification supplémentaires en cliquant sur Ajouter une autre identification après avoir terminé cette configuration d'informations d'identification.

Configurer l'invite de connexion de l'agent (facultatif)

Fournissez des instructions pour guider l'agent de sécurité AWS tout au long du processus d'authentification de votre application.

1. Développez la section d'invite de connexion de l'agent si votre flux d'authentification nécessite des instructions spécifiques.
2. Entrez les instructions décrivant comment utiliser les informations d'identification fournies dans le flux de connexion de votre application.

> **Note**
>
> L'invite de connexion de l'agent indique à l'agent comment appliquer vos informations d'identification à votre application. Cela est utile pour les flux d'authentification complexes, les processus de connexion en plusieurs étapes ou les applications avec des procédures de connexion non standard. Incluez des instructions détaillées telles que « Accédez à / login, entrez le nom d'utilisateur dans le champ « E-mail », entrez le mot de passe et choisissez « Se connecter ».

Ajouter plusieurs informations d'identification (facultatif)

Si votre application nécessite plusieurs ensembles d'informations d'identification ou si différents domaines nécessitent une authentification distincte, ajoutez des ensembles d'informations d'identification supplémentaires.

1. Après avoir terminé la première configuration des informations d'identification, choisissez Ajouter une autre identification.

2. Répétez les étapes de configuration des informations d'identification pour chaque ensemble d'informations d'identification supplémentaire.
3. Pour supprimer un ensemble d'informations d'identification, choisissez Supprimer à côté de l'en-tête des informations d'identification.

> **Tip**
>
> Configurez plusieurs informations d'identification lorsque vous testez différents rôles d'utilisateur, que vous accédez à plusieurs domaines authentifiés ou que vous vérifiez les contrôles d'accès basés sur les rôles dans votre application.

Joindre des ressources supplémentaires (facultatif)

Fournissez des ressources supplémentaires pour aider l'agent de sécurité AWS à effectuer des tests de pénétration plus approfondis et plus précis. Les ressources supplémentaires peuvent inclure des diagrammes d'architecture, de la documentation d'API, des fichiers de configuration, GitHub des référentiels ou S3-hosted des documents fournissant le contexte de votre application.

> **Note**
>
> Des ressources supplémentaires sont facultatives mais recommandées. Fournir des informations complètes sur votre application permet de garantir une couverture complète des tests, de réduire les faux positifs et de fournir des résultats plus exploitables.

Ajoutez des ressources au test d'intrusion

Sélectionnez les ressources existantes ou téléchargez de nouveaux fichiers qui vous aideront à guider le test d'intrusion.

1. Dans la section Ressources connectées, vous pouvez :
   - Choisissez Sélectionner parmi les ressources disponibles pour choisir parmi les ressources déjà connectées à AWS Security Agent (telles que GitHub les référentiels ou les compartiments S3).
   - Choisissez Upload pour ajouter de nouveaux fichiers directement depuis votre système local.

> **Tip**
>
> Les ressources utiles incluent la documentation des API, les diagrammes d'architecture, les OpenAPI/Swagger spécifications, les fichiers de configuration, les diagrammes de flux d'authentification et tout autre matériel décrivant la structure et le comportement de votre application.

Choisissez parmi les ressources disponibles

Choisissez parmi les ressources déjà intégrées à AWS Security Agent.

1. Choisissez Sélectionner parmi les ressources existantes.
2. Parcourez la liste des ressources disponibles à partir de sources connectées telles que :
   - GitHub référentiels, sous l'onglet GitHub référentiels
   - Compartiments S3
   - Fichiers précédemment téléchargés
   - Référentiels de documentation
3. Sélectionnez les ressources que vous souhaitez inclure dans le test d'intrusion.
4. Choisissez Ajouter au test d'intrusion pour associer les ressources sélectionnées.

Example

Nous vous recommandons de sélectionner et d'ajouter GitHub des référentiels pertinents à votre pentest, afin qu'AWS Security Agent puisse mieux comprendre le contexte de votre application et générer des correctifs de code prêts à implémenter par le biais de pull requests (lorsque cette option est activée)

> **Note**
>
> Les ressources sélectionnées parmi les sources disponibles restent synchronisées avec leur emplacement d'origine. Si vous mettez à jour un GitHub référentiel ou un fichier S3, le test d'intrusion utilisera la version mise à jour.

> **Note**
>
> Si vous avez un VPC privé associé à votre pentest et qu'un GitHub référentiel est configuré, assurez-vous qu'il GitHub est accessible via votre VPC privé pour extraire les ressources. GitHub Dans la plupart des cas, vous devrez soit vous assurer que le trafic sortant via la passerelle NAT VPC est autorisé par défaut, soit configurer des règles spécifiques pour autoriser le trafic sortant GitHub pour les adresses IP (GitHub voir Point de terminaison des méta-API)

Téléchargez de nouvelles ressources

Téléchargez des fichiers directement depuis votre système local ou fournissez du contenu en texte brut à AWS Security Agent.

1. Choisissez Charger.
2. Choisissez l'une des méthodes de saisie suivantes :
   - Télécharger des fichiers locaux : sélectionnez un ou plusieurs fichiers de votre système local.
   - Coller du texte brut : saisissez ou collez le contenu du texte directement dans le champ de saisie. Choisissez Charger.
3. Choisissez ensuite Ajouter pour terminer le téléchargement.
4. Les ressources téléchargées apparaissent dans le tableau des ressources connectées.

> **Tip**
>
> Utilisez l'option de texte brut lorsque vous souhaitez fournir rapidement des listes de points de terminaison d'API, des modèles d'URL, des instructions de test ou d'autres informations sous forme de texte sans créer de fichier distinct.

> **Important**
>
> Assurez-vous que les fichiers téléchargés et le contenu collé ne contiennent pas d'informations sensibles telles que les informations d'identification de production, les clés

privées ou les informations personnelles identifiables (PII). Utilisez des versions nettoyées des fichiers de configuration et de la documentation.

Connect les ressources existantes

Les ressources existantes peuvent provenir de ce que vous avez précédemment chargé dans AWS Security Agent, de votre compartiment S3 et de vos GitHub référentiels intégrés. Choisissez Sélectionner parmi les ressources existantes pour les sélectionner.

Gérez les ressources connectées

Passez en revue, organisez et supprimez les ressources associées au test d'intrusion.

Le tableau des ressources connectées affiche toutes les ressources incluses dans le test d'intrusion avec les informations suivantes :

- Nom : nom de fichier ou identifiant de ressource
- Type : catégorie de ressource (fichiers téléchargés, ressources S3, GitHub référentiels, etc.)

Pour gérer les ressources, procédez comme suit :

1. Sélectionnez une ou plusieurs ressources à l'aide des cases à cocher.
2. Choisissez Supprimer du test d'intrusion pour détacher les ressources sélectionnées.

> **Note**
>
> Vous pouvez trier le tableau par nom ou par type en cliquant sur les en-têtes de colonne. Cela permet d'organiser les ressources lorsque vous travaillez avec de nombreux fichiers.

Créez le test de pénétration

Finalisez et lancez la configuration de votre test d'intrusion.

Après avoir configuré tous les paramètres, vous êtes prêt à créer le test d'intrusion.

1. Passez en revue toutes les sections de configuration pour vous assurer de leur exactitude.

2. Choisissez l'une des options suivantes :
   - Choisissez Create penetration pour enregistrer la configuration sans l'exécuter immédiatement.
   - Choisissez Créer et exécuter pour enregistrer la configuration et démarrer immédiatement le test d'intrusion.
   - Choisissez Annuler pour annuler la configuration du test d'intrusion.

> **Important**
>
> Avant d'exécuter un test de pénétration, vérifiez que :
>
> - Tous les domaines cibles sont correctement vérifiés et accessibles
> - Les rôles IAM disposent des autorisations appropriées
> - Out-of-scope les chemins sont correctement configurés pour empêcher les tests d'opérations destructives
> - Vous êtes autorisé à effectuer des tests de sécurité sur tous les domaines cibles

> **Note**
>
> Une fois le test d'intrusion lancé, vous pouvez suivre sa progression dans la section Exécutions des tests de pénétration. Le test peut prendre plusieurs heures. La plupart sont achevés dans un délai de 16 heures, selon la portée et la complexité de votre demande.

Examiner les résultats d'un test de pénétration

Surveillez l'exécution du pentest en temps réel sur la page des journaux des tests de pénétration une fois qu'AWS Security Agent a lancé un pentest. L'agent de sécurité AWS enregistre toutes les actions effectuées pendant le pentest. Une fois terminé, passez en revue le résumé du pentest, qui inclut la présentation de l'application, la couverture des points de terminaison identifiés et l'évaluation des risques liés aux résultats de sécurité.

Évaluez les résultats de sécurité pour corriger les vulnérabilités des applications. Chaque résultat contient une évaluation de l'impact, une évaluation de gravité, des preuves à l'appui et les détails de la demande de correction (lorsque la correction automatique du code est activée).

Conditions préalables

Avant de commencer, assurez-vous de disposer des éléments suivants :

- Un test de pénétration terminé ou en cours
- Accès à l'application Web AWS Security Agent

Étape 1 : Accédez au test de pénétration

Accédez à votre test d'intrusion pour consulter les pages de présentation, de journaux et de résultats.

1. Connectez-vous à l'application Web AWS Security Agent.
2. Accédez à la section Tests de pénétration.
3. Sélectionnez le test d'intrusion que vous souhaitez examiner dans la liste.

> **Tip**
>
> La page des détails du test d'intrusion affiche un résumé de l'état du test, de la date d'achèvement et du nombre de résultats identifiés.

Étape 2 : suivre la progression des tests

Suivez la progression de votre test d'intrusion à l'aide de l'indicateur d'étape.

1. Repérez l'indicateur d'étape horizontal sous l'en-tête de page.
2. Vérifiez l'état de chaque phase de test :
   - Preflight — Configuration initiale et vérifications de connectivité
   - Analyse statique — Analyse du code et de la configuration
   - Pentests — Tests d'exécution et analyse des vulnérabilités
   - Finalisation — Validation finale et génération du rapport

> **Note**
>
> Chaque étape affiche un indicateur d'état (terminée, en cours ou en attente). Les résultats sont découverts et validés tout au long du processus de test, et de nouvelles vulnérabilités apparaissent à la fin de chaque phase.

Étape 3 : Accédez à l'onglet de présentation des tests d'intrusion

1. La section Récapitulatif de l'exécution fournit l'état du test, sa durée et d'autres détails de haut niveau. Il fournit également un tableau de bord des résultats de sécurité classés par niveau de gravité et par type de risque
2. La présentation de l'application par AWS Security Agent fournit un résumé du test d'intrusion effectué
3. Les points de terminaison découverts par l'agent de sécurité AWS fournissent une liste de tous les points de terminaison découverts et testés par l'agent de sécurité AWS lors du pentest

Étape 4 : Accédez à l'onglet journaux des tests d'intrusion

Accédez aux journaux détaillés de toutes les actions exécutées par AWS Security Agent pendant le pentest.

1. Les actions sont classées par type d'action et par type de risque.
2. Sélectionnez une action spécifique pour afficher les journaux détaillés :
   - Résumé des tests : High-level résumé des actions et des résultats de l'agent
   - Journaux de tests d'intrusion : journaux détaillés de toutes les activités de test

> **Note**
>
> Les actions du validateur fournissent des journaux qui valident les résultats dans chaque catégorie.

> **Note**
>
> L'onglet Résultats affiche une vue divisée avec la liste des résultats sur la gauche et les détails des résultats sélectionnés sur la droite.

Étape 5 : Accédez aux résultats

Chaque résultat de la liste contient des informations clés pour vous aider à évaluer rapidement son importance.

> **Note**
>
> Filtre de confiance par défaut
>
> Par défaut, vous ne voyez que les résultats présentant un niveau de confiance élevé pour les agents. Pour afficher également les résultats présentant un niveau de confiance moyen ou faible et les faux positifs, désactivez le bouton Masquer les résultats non vérifiés.

Passez en revue les informations affichées sur chaque fiche de recherche :

- Nom de recherche : titre et identifiant de la vulnérabilité
- Badge de confiance — Indique le niveau de confiance de l'agent dans le résultat (élevé, moyen ou faible)
- Badge de gravité : indique le niveau de risque à l'aide d'un code couleur :
  - Critique (rouge) — Nécessite une action immédiate ; l'exploitation peut compromettre le système
  - Élevé (rouge) — Nécessite une attention rapide ; l'exploitation peut avoir un impact important sur la sécurité
  - Moyen (orange) — Doit être traité dans un délai raisonnable ; contribue au risque de sécurité global
  - Faible (jaune) — Peut être traité dans le cadre d'un entretien régulier ; risque immédiat minimal
  - Informatif (bleu) — À titre informatif ; risque immédiat minime ou nul
- Horodatage de la dernière mise à jour : indique la date à laquelle le résultat a été modifié ou validé pour la dernière fois
- Aperçu de la description — Bref résumé de la vulnérabilité

> **Important**
>
> Priorisez les résultats avec des badges de gravité critique ou élevée et des niveaux de confiance élevés, car ils représentent des vulnérabilités validées nécessitant une correction immédiate.

Étape 6 : Passez en revue les informations de recherche

Sélectionnez des résultats individuels pour afficher des informations complètes sur chaque vulnérabilité.

1. Sélectionnez le nom d'une recherche dans le panneau de gauche pour afficher ses détails dans le panneau de droite.
2. Vérifiez le statut de validation :

> **Note**
>
> Si un résultat affiche le message Inconnu « Ce résultat n'est pas encore validé par AWS Security Agent », cela signifie que la détection de la vulnérabilité est toujours en cours de confirmation. Ces résultats peuvent nécessiter une vérification manuelle.

3. Passez en revue les principaux attributs affichés en haut de la page :
   - Confiance des agents — Le niveau de confiance d'AWS Security Agent dans cette constatation
   - Sévérité — Le niveau de risque avec un badge à code couleur
   - Recherche de journaux — Choisissez « Tracer les actions et les journaux » pour afficher les journaux d'exécution détaillés et les preuves
   - Type de risque : catégorie ou type de risque de sécurité (par exemple, contournement de l'authentification, injection SQL)
4. Développez la section Description pour lire :
   - Explication détaillée de la vulnérabilité
   - Fonctionnement de la vulnérabilité
   - Pourquoi cela représente un risque de sécurité
   - L'impact potentiel sur votre candidature
5. Développez la section Raisonnement des risques pour comprendre le calcul de la gravité :

- Répartition des métriques du CVSS (Common Vulnerability Scoring System)
- Vecteur d'attaque (AV) — Comment exploiter la vulnérabilité
- Complexité de l'attaque (AC) : difficulté de l'exploit
- Privilèges requis (PR) — Quel est le niveau d'accès requis
- Interaction utilisateur (UI) — Si une action de l'utilisateur est requise
- Portée (S) — Si la vulnérabilité affecte d'autres composants
- Impacts sur la confidentialité, l'intégrité et la disponibilité

6. Développez la section Étapes de reproduction pour afficher :
   - Étapes techniques détaillées pour recréer la vulnérabilité
   - Exemples de demandes et de réponses
   - Paramètres ou conditions spécifiques à l'origine du problème
7. La section Script de vérification fournit un moyen exécutable de reproduire le résultat. Développez cette section (si disponible) pour voir :
   - Instructions — Comment configurer et exécuter le script de vérification
   - Variables d'environnement : répertorie les variables obligatoires que vous devez configurer avant d'exécuter le script. Les valeurs sensibles sont supprimées pour des raisons de sécurité.
   - Télécharger le script — Choisissez de télécharger le script de vérification exécutable

> **Note**
>
> Les scripts de vérification ne sont disponibles que pour les vulnérabilités confirmées. L'agent doit avoir correctement généré et validé un script de reproduction exécutable.

> **Note**
>
> Les scripts de vérification sont générés à l'aide de l'IA générative. Passez en revue le script avant de l'exécuter et exécutez-le uniquement sur les systèmes que vous êtes autorisé à tester. Pour obtenir des conseils sur le test responsable AI-generated des scripts, consultez la politique d'AWS en matière d'intelligence artificielle responsable.

> **Tip**
>
> Le script de vérification fournit un moyen exécutable de reproduire le résultat de manière indépendante. Définissez les variables d'environnement requises avec vos propres informations d'identification, puis exécutez le script sur votre système cible pour confirmer l'existence de la vulnérabilité.

> **Tip**
>
> Cliquez sur le lien « Tracer les actions et les journaux » pour accéder à l'ensemble des preuves, y compris les requêtes HTTP, les réponses et les tentatives d'exploitation démontrant la vulnérabilité.

Modifier les résultats

Vous pouvez modifier n'importe quel résultat pour en corriger les détails ou affiner l'évaluation de l'agent. Les champs suivants sont modifiables :

- name — Le titre de la découverte
- description — Description détaillée de la faille de sécurité
- status — État actuel de la découverte
- RiskType — Type de risque de sécurité identifié
- Niveau de risque — Niveau de gravité (CRITIQUE, ÉLEVÉ, MOYEN, FAIBLE, INFORMATIF)
- RiskScore — Score de risque numérique
- raisonnement — Justification de la note de risque attribuée
- AttackScript : Proof-of-concept code illustrant la vulnérabilité
- Note du client — Note facultative expliquant les raisons de la modification

Pour modifier un résultat, procédez comme suit :

1. Accédez à la page détaillée de la recherche.
2. Cliquez sur l'icône d'édition pour modifier l'un des champs de la liste précédente.

3. Enregistrez vos modifications.

> **Note**
>
> Vos modifications sont enregistrées immédiatement et reflétées dans le résultat. Si la personnalisation des résultats est activée, tous les champs modifiables que vous modifiez seront utilisés pour affiner les préférences de l'agent pour les futures exécutions.

Afficher la version originale de l'agent

Lorsque vous modifiez une recherche, un sélecteur de version apparaît dans l'en-tête des détails de la recherche. Cela vous permet de consulter l'évaluation initiale de l'agent :

1. Localisez le sélecteur de version dans l'en-tête des détails de recherche.
2. Sélectionnez Original pour afficher le résultat tel qu'il a été initialement produit par l'agent.
3. Sélectionnez Dernière version pour revenir à la version actuelle avec vos modifications appliquées.

Passez en revue les résultats personnalisés

Lorsque la personnalisation des résultats est activée, AWS Security Agent apprend de vos modifications apportées aux résultats. L'agent applique ces préférences à des résultats similaires lors de futurs tests de pénétration. Lorsqu'un résultat a été ajusté en fonction de vos modifications précédentes, le panneau de détails affiche une section Modifications de personnalisation. Pour plus d'informations sur l'activation de cette fonctionnalité, voir Activer ou désactiver la personnalisation des résultats.

1. Localisez la section Modifications de personnalisation dans le panneau des détails de recherche.

> **Note**
>
> La section Modifications relatives à la personnalisation apparaît uniquement lorsque l'agent de sécurité AWS s'est aligné sur vos modifications précédentes. Les résultats qui ne correspondent à aucune préférence apprise sont affichés exactement tels que l'agent les a produits, sans cette section.

2. Consultez le résumé de ce qui a changé et pourquoi. Le résumé répertorie chaque attribut ajusté avec sa valeur originale produite par l'agent, la valeur personnalisée et le raisonnement. Par exemple :

Sur la base de vos modifications précédentes, les modifications suivantes ont été apportées au résultat initialement produit par le système : le niveau de risque est passé de MOYEN à CRITIQUE ; le score de risque est passé de 5,3 à 9,5 ; raisonnement : gravité accrue pour refléter l'exposition complète du code source de l'application via des cartes sources accessibles au public.

1. Passez en revue le résumé pour comprendre comment le résultat a été ajusté avant de décider comment agir en conséquence.
2. Pour annuler un résultat personnalisé, modifiez-le à nouveau comme vous le feriez pour tout autre résultat (par exemple, modifiez le score de gravité ou de risque). Votre modification la plus récente a toujours la priorité : AWS Security Agent en tire des leçons et applique la préférence mise à jour lors de la prochaine exécution, en remplacement de la règle précédente.

> **Note**
>
> Les modifications de personnalisation ajustent les attributs de recherche tels que RiskLevel, RiskScore, le nom, la description, le raisonnement et AttackScript afin de refléter les normes apprises par AWS Security Agent lors de vos modifications. Tous les champs que vous avez déjà modifiés peuvent être ajustés en fonction de résultats similaires lors de futures éditions.

Comment la personnalisation tire les leçons de vos modifications

Lorsque la personnalisation des résultats est activée, AWS Security Agent apprend de toutes les modifications que vous apportez aux résultats et applique des ajustements similaires aux futures exécutions. Tout champ que vous modifiez (comme indiqué dans la section Modifier les résultats précédente) sera utilisé pour affiner les préférences apprises par l'agent.

> **Note**
>
> Pour le champ d'état, seul le fait de marquer un résultat comme FALSE_POSITIVE est traité comme une préférence pouvant être apprise. Les modifications apportées à d'autres valeurs de statut ne déclenchent pas l'apprentissage.

Lors du prochain pentest, l'agent évalue les nouveaux résultats par rapport à vos préférences apprises et applique les ajustements nécessaires, le cas échéant. Une section sur les modifications de personnalisation apparaît sur chaque résultat ajusté, expliquant ce qui a été modifié.

> **Note**
>
> La personnalisation ne tire des leçons que des modifications apportées lors du dernier pentest terminé. La fonctionnalité doit être activée au moment où le pentest commence pour que l'apprentissage ait lieu. Si vous modifiez le même résultat lors d'une exécution ultérieure, la modification la plus récente est prioritaire : l'agent met à jour ses préférences pour refléter votre dernière décision.

Activer ou désactiver la personnalisation des résultats

La personnalisation des résultats est activée par défaut. Pour le désactiver ou le réactiver :

1. Accédez à la configuration de votre pentest.
2. Localisez le bouton de personnalisation des résultats.
3. Pour activer la personnalisation des résultats, activez le bouton. Pour le désactiver, désactivez-le.

Lorsque cette option est désactivée, les résultats apparaissent dans leur état brut produit par l'agent sans qu'aucune personnalisation ne soit appliquée. Les préférences précédemment apprises sont conservées et seront appliquées à nouveau si la fonctionnalité est réactivée.

Étape 7 : Interpréter les métriques CVSS

Comprendre les métriques CVSS vous aide à évaluer la gravité réelle et à hiérarchiser les efforts de correction.

Lorsque vous consultez la section Raisonnement, faites attention à ces indicateurs clés :

- Vecteur d'attaque (Network/Adjacent/Local/Physical) — Indique à quelle distance l'attaque peut être exécutée
- Complexité de l'attaque (Low/High) — Indique si des conditions spécialisées sont nécessaires pour exploiter
- Privilèges requis (None/Low/High) — Identifie le niveau d'accès dont un attaquant a besoin
- Interaction utilisateur (None/Required) — Détermine si l'exploit nécessite l'implication de l'utilisateur

- Confidentiality/Integrity/Availability Impact (None/Low/High) — Mesure l'impact sur la sécurité de votre système

> **Important**
>
> Les résultats relatifs au vecteur d'attaque réseau, à la faible complexité et à confidentiality/integrity l'impact élevé constituent les vulnérabilités les plus dangereuses nécessitant une attention immédiate.

Étape 8 : Prioriser et traiter les résultats

Agissez en fonction des résultats pour corriger les vulnérabilités et améliorer le niveau de sécurité de votre application.

Pour les résultats critiques et de gravité élevée avec un niveau de confiance élevé :

1. Passez en revue la description et les étapes pour reproduire les sections de manière approfondie.
2. Accédez aux journaux détaillés via le lien « Tracer les actions et les journaux » pour recueillir des preuves complètes.
3. Accédez à des correctifs de code prêts à implémenter via l'une des méthodes suivantes :
   - Pour la correction automatique : utilisez le lien pull request dans la section de correction
   - Pour les demandes manuelles : choisissez « Code de correction » sur la page des résultats pour demander une pull request. Conditions préalables :
   - L'administrateur doit activer la correction du code pour les GitHub référentiels dans la console AWS Security Agent
   - Les référentiels doivent être inclus dans votre configuration de pentest
4. Prévoyez un test de pénétration de suivi pour vérifier que le correctif est efficace.

Pour les résultats de gravité moyenne ou faible :

1. Établissez vos priorités en fonction de votre tolérance au risque et du contexte commercial.
2. Incluez des tâches de correction dans la planification régulière de votre sprint de développement.
3. Déterminez si plusieurs résultats de faible gravité combinés créent un risque plus élevé.
4. Documentez tous les risques acceptés avec une justification appropriée.

> **Important**
>
> N'ignorez pas les résultats de faible gravité. Plusieurs vulnérabilités de faible gravité peuvent souvent être enchaînées pour créer des exploits plus graves, en particulier lorsqu'elles sont associées à de l'ingénierie sociale ou à un accès physique.

Étape 9 : suivre les progrès de la remédiation

Utilisez l'interface des résultats pour savoir quelles vulnérabilités ont été corrigées et lesquelles nécessitent des mesures supplémentaires.

1. Pendant que vous travaillez sur la correction, reportez-vous à la section Étapes de reproduction pour vérifier vos corrections.
2. Documentez votre approche de correction pour chaque résultat pour les futurs audits de référence et de conformité.

> **Tip**
>
> Tenez un journal des mesures correctives qui associe chaque résultat à sa résolution, y compris les modifications de code, les mises à jour de configuration ou les décisions architecturales prises pour remédier à la vulnérabilité.

Étapes suivantes

Après avoir examiné les résultats de votre test d'intrusion :

- Hiérarchisez les résultats critiques et les plus graves avec un niveau de fiabilité élevé pour une correction immédiate
- Téléchargez, examinez et exécutez des scripts de vérification dans votre environnement de test pour tester les scripts et identifier les vulnérabilités
- Créez des tickets de suivi dans votre système de gestion des problèmes avec des liens pour trouver des détails et des preuves
- Mettre en œuvre des correctifs et des contrôles de sécurité pour corriger les vulnérabilités identifiées

- Surveillez l'indicateur de progression des tests d'intrusion pour détecter les vulnérabilités récemment découvertes
- Planifiez un test de pénétration de suivi pour vérifier que les vulnérabilités ont été correctement corrigées
- Mettez à jour le processus de test de sécurité de votre application et votre modèle de menace en fonction des résultats
- Passez en revue les métriques CVSS pour comprendre le niveau de sécurité global de votre application

Pour plus d'informations sur la réalisation de tests de pénétration, consultezthe section called "Créez un test de pénétration".

Pour plus d'informations sur la compréhension du cycle de vie du Security Agent, consultezthe section called "Comprendre la hiérarchie et le cycle de vie des ressources".

Fournir des informations d'authentification pour les tests de pénétration

Fournissez des informations d'identification pour permettre à AWS Security Agent de tester les zones authentifiées de vos applications Web. Sans informations d'identification, l'agent peut uniquement tester les pages et les API accessibles au public.

Configuration des informations d'authentification

1. Dans le flux de travail de création du test d'intrusion, recherchez la section Informations d'authentification - Facultatif.
2. Dans la section Credential #1, choisissez votre méthode de saisie des informations d'identification :
   - Entrez les informations d'identification - Entrez les informations d'identification directement. Idéal pour les environnements de développement et de test.
   - Paramètre avancé : utilisez la gestion AWS-native des informations d'identification. Recommandé pour les environnements de production et les informations d'identification sensibles.

Options avancées

Si vous sélectionnez le paramètre avancé, vous pouvez choisir entre trois stratégies d'identification :

- Hypothèse du rôle IAM : pour les applications utilisant AWS Cognito ou l'authentification IAM
- AWS Secrets Manager : pour un stockage sécurisé des informations d'identification avec chiffrement et rotation
- Fonction Lambda : pour la génération dynamique d'informations d'identification ou les flux d'authentification complexes

Entrez directement les informations d'identification

1. Sélectionnez Entrez les informations d'identification.
2. Entrez le nom d'utilisateur et le mot de passe.
3. Dans le menu déroulant URL d'accès, sélectionnez l'URL dans laquelle ces informations d'identification seront utilisées. Cela doit être sélectionné dans la liste des points de terminaison cibles.
4. (Facultatif) Dans le champ 2FA - facultatif, fournissez un secret TOTP pour les applications qui nécessitent une authentification à deux facteurs. Vous avez le choix entre les options suivantes :
   - Entrez le secret TOTP directement (par exemple,`JBSWY3DPEHPK3PXP`) ou entrez l'`otpauth://totp/`URI complet (par exemple,`otpauth://totp/Example:user@example.com?secret=JBSWY3DPEHPK3PXP&issuer=Example`).
   - Cliquez sur l'icône de téléchargement pour télécharger une image de code QR depuis la page de configuration de votre application d'authentification. Le code QR est scanné localement et l'URI TOTP est extrait automatiquement.

     Lorsqu'un secret TOTP est fourni, l'agent génère automatiquement de nouveaux codes à usage unique et les saisit lorsqu'une invite 2FA est détectée lors de la connexion.
5. (Facultatif) Développez l'invite de connexion à Agent Space pour fournir des instructions de connexion spécifiques si votre application possède un flux d'authentification complexe.

> **Important**
>
> Utilisez des comptes de test dotés d'un accès représentatif plutôt que des comptes personnels ou administratifs.

Utiliser les paramètres avancés

Lorsque vous sélectionnez une stratégie d'identification avancée (rôle Secrets Manager, Lambda ou IAM), AWS Security Agent récupère vos informations d'identification directement depuis la ressource AWS configurée à l'aide du rôle de service. Utilisez l'invite de connexion à Agent Space pour fournir à l'agent des instructions sur la façon d'appliquer ces informations d'identification à votre application, par exemple, l'URL de connexion vers laquelle accéder et les champs de formulaire à remplir.

> **Note**
>
> Les secrets et les fonctions Lambda de Secrets Manager doivent se trouver dans le même compte AWS que celui utilisé pour configurer votre agent de sécurité AWS. Cross-account les informations d'identification ne sont pas prises en charge actuellement.

1. Sélectionnez Réglage avancé.
2. Dans le menu déroulant Stratégie d'accès utilisateur, sélectionnez l'une des options suivantes :

Sélectionnez le rôle IAM disponible que l'agent doit assumer

Utilisez cette option pour les applications utilisant AWS Cognito, API Gateway avec authentification IAM ou d'autres AWS-native systèmes d'authentification. Le rôle IAM doit avoir une relation de confiance permettant à AWS Security Agent de l'assumer et être autorisé à accéder au système d'authentification de votre application.

Sélectionnez les informations d'identification statiques depuis AWS Secrets Manager connecté

Utilisez cette option pour récupérer les informations d'identification en toute sécurité depuis AWS Secrets Manager grâce au chiffrement, à la rotation et à l'audit d'accès.

Le rôle IAM doit disposer `secretsmanager:GetSecretValue` d'`secretsmanager:DescribeSecret`autorisations.

L'agent récupère la valeur secrète directement auprès de Secrets Manager. Utilisez l'invite de connexion à Agent Space pour indiquer à l'agent comment appliquer ces informations d'identification au flux de connexion de votre application, par exemple, l'URL vers laquelle accéder et les champs de formulaire à remplir. Vous pouvez utiliser n'importe quel format pour stocker votre secret, car l'agent interprétera le format en suivant les instructions que vous fournissez dans l'invite de connexion.

Par exemple, si l'agent doit soumettre un formulaire de username/password connexion àhttps://example.com/login, vous pouvez formater votre secret au format JSON avec des `password` champs `username` et. Si l'application nécessite l' TOTP-based authentification à deux facteurs, incluez un `totpSecret` champ contenant soit directement le secret TOTP, soit un URI complet `otpauth://totp/` :

```
{
  "username": "test-user",
  "password": "secure-password-here",
  "totpSecret": "JBSWY3DPEHPK3PXP"
}
```

Ensuite, configurez les instructions d'authentification : Définissez l'URL d'accès sur `https://example.com` (ou toute autre URL sélectionnée dans la liste des points de terminaison cibles). Entrez ce qui suit dans l'invite de connexion à Agent Space : « Accédez au formulaire https://example.com/login et entrez le nom d'utilisateur et le mot de passe fournis ».

Autre exemple, si vous devez plutôt fournir une clé d'API dans un en-tête HTTP, vous pouvez la stocker en texte brut :

```
"api-key-here"
```

Ensuite, configurez les instructions d'authentification : Entrez ce qui suit dans l'invite de connexion à Agent Space : « Définissez l' X-API-Key en-tête sur la clé d'API fournie pour toutes les demandes. »

> **Important**
>
> Seule l' TOTP-based authentification à deux facteurs est prise en charge. Les SMS, les e-mails, les notifications push, les clés matérielles et l'authentification OAuth ne sont pas pris en charge.

Sélectionnez la fonction Lambda disponible pour récupérer les informations d'identification de manière dynamique

Utilisez cette option pour les systèmes d'authentification complexes, la génération dynamique d'informations d'identification ou l'intégration avec des fournisseurs d'identité externes.

Le rôle IAM doit disposer d'`lambda:InvokeFunction`autorisations et la fonction doit être terminée dans les 30 secondes.

Lorsque le test d'intrusion s'exécute, AWS Security Agent appelle votre fonction AWS Lambda de manière synchrone et passe un événement qui identifie le test d'intrusion et les informations d'identification spécifiques à résoudre :

```
{
  "pentest_arn": "arn:aws:securityagent:us-west-2:111122223333:pentest/pt-
abcd1234-5678-90ab-cdef-EXAMPLE11111",
  "actor_identifier": "Credential1"
}
```

- `pentest_arn`— Le nom de ressource Amazon (ARN) du test d'intrusion pour lequel l'identifiant est en cours de résolution. Utilisez-le pour définir, autoriser ou auditer la demande au sein de votre fonction.
- `actor_identifier`— Le nom d'identification que vous avez attribué à cette identification dans la console (par exemple,`Credential1`). Utilisez-le pour renvoyer les informations d'identification correctes lorsqu'une seule fonction fournit plusieurs informations d'identification.

L'agent utilise la sortie de la fonction directement comme identifiant. Utilisez l'invite de connexion à Agent Space pour indiquer à l'agent comment appliquer ces informations d'identification à votre application, de la même manière que vous le feriez avec AWS Secrets Manager. Consultez des exemples the section called “Sélectionnez les informations d'identification statiques depuis AWS Secrets Manager connecté” de formatage de la sortie de votre fonction Lambda et des types d'authentification pris en charge.

Configuration de plusieurs informations d'identification

Pour tester différents rôles d'utilisateurs ou systèmes d'authentification, procédez comme suit :

1. Choisissez Ajouter un autre identifiant.
2. Configurez les informations d'identification supplémentaires à l'aide de l'une ou l'autre méthode de saisie.
3. Pour supprimer un identifiant, choisissez Supprimer dans la section du code d'identification.

Optimisation de connexion

L'optimisation de la connexion permet à AWS Security Agent d'apprendre les modèles de navigation des précédents pentest et de les appliquer aux essais suivants. Ces modèles incluent les flux de

connexion et les flux de travail d'authentification en plusieurs étapes. Cela réduit le temps que l'agent passe à redécouvrir comment s'authentifier, ce qui se traduit par des scans plus rapides et une couverture de test plus cohérente.

Comment fonctionne l'optimisation des connexions

Lors du premier pentest, l'agent découvre comment naviguer dans le flux de connexion de votre application à l'aide des informations d'identification que vous fournissez. Il enregistre les étapes de navigation réussies et génère un fichier de compétences qui capture le flux de travail de connexion appris.

Lors des exécutions suivantes, l'agent lit le fichier de compétences enregistré et applique directement le modèle de navigation appris, sans passer par la phase de découverte. Autrement dit :

- Temps de test authentifié plus court : l'agent applique immédiatement des modèles de navigation éprouvés au lieu d'explorer à partir de zéro
- Comportement plus cohérent : l'agent suit le même chemin éprouvé plutôt que d'explorer des alternatives

> **Note**
>
> L'optimisation de connexion apprend lors de la première session de connexion d'une exécution. Les sessions de connexion suivantes au cours de la même session bénéficieront de ce qui a été appris lors de la première session. Lors des prochaines exécutions, toutes les sessions de connexion bénéficieront de la compétence enregistrée.

Activer ou désactiver l'optimisation de connexion

L'optimisation de connexion est activée par défaut. Pour le désactiver ou le réactiver :

1. Dans la configuration du pentest, accédez à la section Authentification accréditations - facultatif.
2. Localisez le bouton d'optimisation de connexion.
3. Pour activer l'optimisation de la connexion, activez le bouton. Pour le désactiver, désactivez-le.

Lorsque cette option est désactivée, l'agent redécouvre le flux de connexion en partant de zéro à chaque exécution. Les compétences de navigation précédemment acquises sont préservées et seront appliquées à nouveau si la fonctionnalité est réactivée.

> **Tip**
>
> Si le flux de connexion de votre application change de manière significative (par exemple, une page de connexion redessinée ou une nouvelle étape d'authentification), l'agent s'adapte automatiquement en mettant à jour ses compétences apprises lors de la prochaine exécution. Il n'est pas nécessaire de réinitialiser manuellement l'optimisation.

Corriger les résultats d'un test d'intrusion

Lorsque vous consultez les résultats d'un test d'intrusion, vous pouvez demander à AWS Security Agent de tenter de corriger un résultat. Pour les GitHub référentiels privés, AWS Security Agent ouvre une pull request contenant le correctif proposé. Pour les référentiels publics, la correction est disponible sous forme de fichier de comparaison téléchargeable que vous pouvez appliquer localement.

Vous devez activer la recherche de mesures correctives dans l'AWS Management Console. (Consultez the section called “Permettre aux utilisateurs de commencer à corriger les résultats des tests d'intrusion et de la révision du code”.) Les utilisateurs peuvent commencer à corriger une découverte spécifique à partir de l'application Web AWS Security Agent.

Conditions préalables

Avant de commencer, assurez-vous de disposer des éléments suivants :

- Un test de pénétration terminé ou en cours
- Accès à l'application Web AWS Security Agent
- Connaissance de l'architecture et des exigences de sécurité de votre application

Étape 1 : activer ou désactiver la correction automatique

Vous pouvez configurer les options de correction du code lorsque vous créez ou modifiez un test d'intrusion. Si vous activez la correction automatique, AWS Security Agent tentera automatiquement de corriger les GitHub référentiels associés s'il confirme un résultat lors du pentest. Vous pouvez également démarrer manuellement la correction du code. Dans la vue permettant de modifier les détails du test d'intrusion, dans la section Correction automatique du code, activez ou désactivez la correction du code.

Étape 2 : Sélection des référentiels pour la correction du code

1. Choisissez Suivant jusqu'à la dernière étape Ressources pédagogiques supplémentaires.
2. Choisissez Sélectionner parmi les ressources.
3. Choisissez des GitHub référentiels.
4. Sélectionnez les référentiels que vous souhaitez utiliser pour la correction du code.
5. Enregistrez le test de pénétration.
6. Vous pouvez voir les référentiels associés avec succès sous l'onglet Ressources de formation sur les tests de pénétration.

Étape 3 : Lancer un test d'intrusion et consulter les résultats

Exécutez le test de pénétration pour détecter les résultats. Pour de plus amples informations, veuillez consulter the section called “Examiner les résultats d'un test de pénétration”.

Étape 4 : démarrer et afficher la correction du code

1. Naviguez jusqu'à la découverte.
2. Si vous avez activé la correction automatique du code, une correction de code sera lancée une fois que l'agent de sécurité AWS aura confirmé une découverte.
3. Si vous souhaitez démarrer manuellement une correction de code, cliquez sur le bouton Corriger le code.
4. Dans la section Correction du code du résultat, vous pouvez consulter l'état de la correction du code et les liens vers les pull requests. Si le GitHub référentiel est public, la correction du code est disponible sous forme de fichier téléchargeable au lieu d'une pull request. Vous pouvez exécuter la modification localement `git apply /path/to/code_remediation_changes.diff` pour appliquer la modification à votre dépôt.

Sécurité et référence

Conseils de sécurité, quotas de service et historique des documents pour AWS Security Agent.

Sécurité dans AWS Security Agent

La sécurité du cloud AWS est la priorité absolue. En tant que AWS client, vous bénéficiez d'un centre de données et d'une architecture réseau conçus pour répondre aux exigences des entreprises les plus sensibles en matière de sécurité.

La sécurité est une responsabilité partagée entre vous AWS et vous. Le modèle de responsabilité partagée décrit cette notion par les termes sécurité du cloud et sécurité dans le cloud :

- Sécurité du cloud : AWS est chargée de protéger l'infrastructure qui exécute l'agent de sécurité AWS dans le AWS cloud. Cela inclut l'infrastructure de services, les modèles d'IA et les agents de test de pénétration. Third-party les auditeurs testent et vérifient régulièrement l'efficacité de notre sécurité dans le cadre des programmes de AWS conformité.
- Sécurité dans le cloud : votre responsabilité englobe les domaines suivants :
  - Gestion de l'accès à AWS Security Agent par le biais de politiques et d'autorisations IAM
  - Protection du contenu que vous fournissez au service, y compris les documents de conception, les référentiels de code et les URL des applications pour les tests d'intrusion
  - Configuration des référentiels et applications surveillés
  - Examiner les constatations de sécurité fournies par le service et y donner suite
  - Sécurisation de vos applications en fonction des conseils de correction fournis
  - La sensibilité de vos données, les exigences de votre entreprise,et la législation et la réglementation applicables

Cette documentation vous aide à comprendre comment appliquer le modèle de responsabilité partagée lors de l'utilisation d'AWS Security Agent.

Considérations relatives à la sécurité relatives à AWS Security Agent et aux tests de pénétration assistés par l'IA

AWS Security Agent est un agent novateur qui sécurise de manière proactive vos applications tout au long du cycle de développement dans tous vos environnements. Il réalise des évaluations de sécurité

automatisées adaptées à vos besoins, les équipes de sécurité définissant de manière centralisée les normes qui sont automatiquement validées lors des révisions. Security Agent effectue des tests de pénétration à la demande adaptés à votre application, afin de découvrir et de signaler les risques de sécurité vérifiés. Cette approche permet d'étendre l'expertise en matière de sécurité à l'ensemble de vos applications pour qu'elle corresponde à la vitesse de développement tout en fournissant une couverture de sécurité complète. En intégrant la sécurité de la conception au déploiement, il permet de prévenir les vulnérabilités à un stade précoce et à grande échelle.

Les équipes de sécurité définissent les exigences de sécurité de l'organisation une fois dans la console AWS : bibliothèques d'autorisations approuvées, normes de journalisation et politiques d'accès aux données. AWS Security Agent applique automatiquement ces exigences de sécurité tout au long du développement, en évaluant les documents architecturaux et le code par rapport à vos normes et en fournissant des conseils spécifiques lorsqu'il détecte des violations. Cela permet d'appliquer la sécurité de manière cohérente au sein des équipes et d'adapter les révisions à la vitesse de développement.

Pour la validation du déploiement, AWS Security Agent transforme les tests d'intrusion d'un goulot d'étranglement périodique en une fonctionnalité à la demande. Les équipes de sécurité fournissent les URL cibles, les informations d'authentification, le code source et la documentation. AWS Security Agent développe une compréhension approfondie des applications et exécute des chaînes d'attaque sophistiquées pour découvrir et valider les vulnérabilités, ce qui permet aux équipes de procéder à des tests chaque fois que cela est nécessaire.

Capacités clés

AWS Security Agent fournit des fonctionnalités de sécurité complètes couvrant l'ensemble du cycle de développement.

Examen de la sécurité de la conception

AWS Security Agent fournit des commentaires de sécurité à la demande sur les documents de conception et évalue la conformité aux exigences de sécurité de l'organisation avant l'écriture du code. Les équipes de sécurité téléchargent les documents de conception via l'application Web, où l'agent les analyse par rapport à vos exigences de sécurité et fait ressortir les résultats avec des conseils de correction. Cela permet d'accélérer les révisions manuelles de plusieurs heures pour les transformer en analyses ciblées, ce qui permet aux équipes de résoudre les problèmes de sécurité au moment où les mesures correctives sont les plus efficaces.

Révision de la sécurité du code

AWS Security Agent analyse les pull requests ou le code chargé afin de vérifier les exigences de sécurité de l'organisation et les problèmes de sécurité courants tels que l'absence de validation des entrées et les risques d'injection de code SQL. L'agent fournit des conseils de correction directement au sein de votre plateforme de référentiel de code. Les équipes de sécurité configurent les référentiels à surveiller, en adaptant l'évaluation à toutes les bases de code tout en surveillant les problèmes critiques.

On-demand tests de pénétration

AWS Security Agent propose des tests de pénétration à la demande qui découvrent et signalent les vulnérabilités de sécurité validées par le biais de scénarios d'attaque personnalisés en plusieurs étapes. AWS Security Agent déploie des agents d'intelligence artificielle spécialisés qui développent le contexte des applications à partir de la documentation et des informations d'identification fournies, puis exécutent des chaînes d'attaque sophistiquées pour identifier les vulnérabilités complexes que les outils classiques passent inaperçues. Il documente les résultats à l'aide d'une analyse d'impact, de trajectoires d'attaque reproductibles et de correctifs de code prêts à mettre en œuvre, accélérant ainsi les tests de pénétration de plusieurs semaines à quelques heures et étendant la validation à l'ensemble de votre portefeuille d'applications.

FAQ

&Contrôle de sécurité

Comment l'agent de sécurité AWS authentifie-t-il et maintient-il l'accès aux systèmes ?

Les tests d'intrusion sont la seule fonctionnalité d'AWS Security Agent capable de s'authentifier auprès du système d'un utilisateur au moment de l'exécution. L'AWS Security Agent accepte les informations d'identification sous forme de nom d'utilisateur et de mot de passe statiques (stockées dans Secrets Manager) ou d'un fournisseur d'informations d'identification (sous forme de fonction Lambda) comme configuration avant de démarrer le test du stylo. Ces informations d'identification sont utilisées pour exercer les fonctionnalités normales de l'utilisateur tout system/application au long du cycle de vie du test du stylo. Nous encourageons les utilisateurs à créer de nouvelles informations d'identification avec des autorisations correctement définies à des fins de pentests.

Les utilisateurs peuvent-ils contrôler l'étendue et la profondeur des tests afin d'éviter des impacts imprévus sur le système ?

AWS Security Agent permet aux clients de sélectionner une catégorie spécifique de vulnérabilité à explorer sur un terminal. Les utilisateurs peuvent spécifier des URL hors champ d'application pour empêcher AWS Security Agent d'effectuer des tests de pénétration sur ces cibles. https://docs.aws.amazon.com/securityagent/latest/userguide/perform-penetration-test.html

L'agent de sécurité AWS lui-même peut-il présenter un risque de sécurité ?

AWS Security Agent est chargé de détecter les risques de sécurité, mais de le faire en utilisant des charges utiles intentionnellement minimes (par exemple en extrayant la version SQL au lieu de supprimer une table lorsqu'une attaque par injection de code SQL est découverte). AWS Security Agent est également limité à des barrières de sécurité déterministes pour empêcher les comportements risqués tels que la création d'une charge excessive sur l'application cible. Tant que les garde-fous sont en place, il peut toujours y avoir des interactions involontaires ou non évidentes avec la logique métier. C'est pourquoi nous recommandons toujours d'effectuer des tests d'intrusion dans un environnement de pré-production.

Quelles sont les données collectées par l'agent de sécurité AWS et où sont-elles stockées ?

AWS Security Agent permet aux utilisateurs de télécharger des artefacts pour fournir le contexte de leur application testée. Pour plus d'informations sur la protection des données, consultezthe section called “Protection des données”. AWS Security Agent sélectionnera automatiquement la région optimale au sein de votre zone géographique pour traiter vos demandes d'inférence. Cela permet d'optimiser les ressources informatiques disponibles, la disponibilité des modèles et d'offrir la meilleure expérience client. Vos données resteront stockées uniquement dans la région d'origine de la demande. Toutefois, les demandes de saisie et les résultats de sortie peuvent être traités en dehors de cette région. Toutes les données sont transmises chiffrées sur l'ensemble du réseau sécurisé d'Amazon. Pour plus d'informations, consultez la section Inférence interrégionale.

Quels sont les contrôles mis en place pour bloquer les tests non autorisés sur un terminal ?

Les points de terminaison spécifiés comme URL cibles pour le pentesting nécessiteront une validation DNS ou une validation HTTP comme mesure de propriété. AWS Security Agent demandera au client d'ajouter un enregistrement TXT au DNS du terminal ou d'exposer une route HTTP renvoyant une chaîne de validation comme preuve de propriété. Ce n'est qu'après avoir démontré la preuve de propriété que l'utilisateur pourra procéder à un pentest. Les demandes adressées à des URL situées en dehors des URL cibles et accessibles seront bloquées par le réseau.

Les clients sont tenus de s'assurer qu'ils disposent de l'autorisation appropriée pour tester tous les systèmes susceptibles d'être affectés par leurs activités de test d'intrusion. Toute utilisation d'AWS Security Agent doit être conforme à la politique d'utilisation acceptable d'AWS (https://aws.amazon.com/aup/).

Comment les utilisateurs bloquent-ils et signalent-ils les abus à l'aide d'AWS Security Agent ?

AWS Security Agent surveille en permanence les demandes et les tentatives d'accès aux URL situées en dehors des URL cibles. Si un abus est détecté, par exemple une tentative d'utilisation d'AWS Security Agent pour effectuer des tests non autorisés sur un terminal tiers, tous les tests préliminaires en cours sur le compte seront interrompus. Les clients peuvent contacter le support AWS ou l'équipe chargée de leur compte AWS pour obtenir de l'aide.

L'agent de sécurité AWS peut-il remplacer le flux de travail de test du stylo ?

AWS Security Agent n'est pas un service de test d'intrusion professionnel, et nous encourageons les utilisateurs à intégrer AWS Security Agent dans leur flux de travail de révision de sécurité. AWS Security Agent peut fournir un accès aux tests d'intrusion à la demande pendant la phase de développement du cycle de vie du logiciel lorsqu'il est trop tôt, peu pratique ou qu'il est trop tôt de faire appel à des professionnels du pentesting ou qu'il est nécessaire de le réévaluer trop fréquemment. Les professionnels de la sécurité peuvent examiner les résultats de l'agent de sécurité AWS pour les valider, les expliquer ou les développer pour de nouvelles découvertes (s'ils existent).

Les utilisateurs peuvent-ils configurer un contrôle d'accès basé sur les rôles (RBAC) pour les différents membres de l'équipe ?

Oui. AWS Security Agent s'intègre à AWS IAM Identity Center, permettant aux administrateurs de gérer les membres de l'équipe qui peuvent accéder à l'application Web AWS Security Agent, qui permet aux utilisateurs de créer, de gérer et de consulter des révisions de conception et des pentests.

Capacités de test

Quels types de vulnérabilités l'agent de sécurité AWS peut-il détecter ?

AWS Security Agent détecte des vulnérabilités dans le Top 10 de l'OWASP pour les applications Web. AWS Security Agent fournit des types de risques spécifiques que vous pouvez inclure ou exclure dans les tests décrits ci-dessous. Les résultats peuvent découler de ces catégories de risque ou de nouveaux résultats découverts en suivant les pistes issues d'une combinaison de ces catégories de risque.

- Téléchargement de fichiers arbitraire
  - Le téléchargement arbitraire de fichiers confirme que l'application doit être capable de repousser les fichiers faux et malveillants de manière à assurer la sécurité de l'application et des utilisateurs
- Injection de code
  - L'injection de code est le terme général désignant les types d'attaques qui consistent à injecter du code qui est ensuite envoyé interpreted/executed par l'application.
- Injection de commande
  - L'injection de commandes est une attaque dont le but est l'exécution de commandes arbitraires sur le système d'exploitation hôte via une application vulnérable
- Cross-Site Scriptage (XSS)
  - Cross-Site Les attaques par script (XSS) sont un type d'injection, dans lequel des scripts malveillants sont injectés dans des sites Web par ailleurs bénins et fiables
- Référence directe à un objet non sécurisée
  - Les références directes aux objets (IDOR) non sécurisées se produisent lorsqu'une application fournit un accès direct aux objets en fonction des entrées fournies par l'utilisateur
- Vulnérabilités des jetons Web JSON
  - Les JWT sont une source courante de vulnérabilités, à la fois dans la manière dont ils sont implémentés dans les applications et dans les bibliothèques sous-jacentes
- Inclusion de fichiers locaux
  - La vulnérabilité d'inclusion de fichiers permet à un attaquant d'inclure un fichier, en exploitant généralement un mécanisme d' « inclusion dynamique de fichier » implémenté dans l'application cible
- Traversée du chemin
  - L'attaque par traversée de chemin (également connue sous le nom de traversée de répertoire) vise à accéder à des fichiers et à des répertoires stockés en dehors du dossier racine du Web
- Escalade de privilèges
  - L'augmentation des privilèges se produit lorsqu'un utilisateur a accès à plus de ressources ou de fonctionnalités que ce qui lui est normalement autorisé, et qu'une telle élévation ou modification aurait dû être empêchée par l'application
- Server-Side Falsification de demandes (SSRF)
  - Server-Side La falsification de requêtes (SSRF) se produit lorsque l'attaquant peut abuser des fonctionnalités du serveur pour lire ou mettre à jour des ressources internes

- Server-Side Injection de modèles
  - Des vulnérabilités d'injection de modèles côté serveur (SSTI) se produisent lorsque les entrées utilisateur sont intégrées dans un modèle de manière non sécurisée et entraînent l'exécution de code à distance sur le serveur
- Injection SQL
  - L'attaque par injection SQL consiste en l'insertion ou « l'injection » d'une requête SQL via les données d'entrée du client vers l'application
- Entité externe XML
  - L'attaque d'entité externe XML est un type d'attaque contre une application qui analyse les entrées XML. Cette attaque se produit lorsqu'une entrée XML contenant une référence à une entité externe est traitée par un analyseur XML faiblement configuré

Quelles sont les méthodes d'authentification prises en charge par AWS Security Agent ?

AWS Security Agent prend en charge les méthodes d'authentification courantes, notamment OAuth et JWT. Pour plus d'informations, consultez la documentation .

Comment l'agent de sécurité AWS gère-t-il la limitation du débit et la prévention du déni de service (DOS) ?

L'agent de sécurité AWS est doté de barrières de sécurité qui l'empêchent de perturber ou de détruire les terminaux en cours de test, y compris le DOS. Il est doté de contrôles de vitesse internes pour détecter et gérer les modèles de trafic inattendus.

L'agent de sécurité AWS peut-il tester à la fois les API REST et GraphQL ?

Oui, AWS Security Agent peut tester les points de terminaison des API. Nous encourageons les clients à fournir de la documentation sur les API sous forme de ressources d'apprentissage supplémentaires permettant à AWS Security Agent de mieux comprendre la forme et les fonctionnalités de chaque API testée.

Comment les utilisateurs peuvent-ils vérifier qu'AWS Security Agent couvre l'ensemble de la logique et des points de terminaison critiques de l'application ?

L'agent de sécurité AWS effectuera d'abord une exploration approfondie de la ou des applications cibles et tentera de l'utiliser normalement avant de tenter un exploit. Cela lui permet d'acquérir une compréhension pratique de l'application au moment de l'exécution et de découvrir la logique et

les points de terminaison critiques de l'application. Compte tenu de sa nature stochastique, il n'est pas garanti qu'AWS Security Agent découvre et teste toutes les applications et tous les points de terminaison critiques pour une application cible. L'application Web AWS Security Agent fournit une visibilité sur tous les points de terminaison découverts et sur les actions entreprises dans les journaux des tests d'intrusion.

Précision & et fiabilité

Comment l'agent de sécurité AWS valide-t-il les résultats avant de les signaler ?

AWS Security Agent utilise des validateurs déterministes pour valider le résultat signalé. Dans les types de risques pour lesquels il n'est pas possible d'utiliser des validateurs déterministes, AWS Security Agent réexécutera indépendamment les étapes de recherche afin de s'assurer de la validité du résultat. AWS Security Agent ne signale que les résultats présentant un niveau de confiance élevé ou moyen et masque les résultats non vérifiés par défaut.

L'agent de sécurité AWS peut-il s'adapter à une logique d'application personnalisée ?

AWS Security Agent accepte éventuellement le code source, le modèle de menace, les documents de conception et la documentation d'API en tant que ressources d'apprentissage supplémentaires afin d'obtenir un contexte orienté vers l'utilisateur sur l'application cible utilisée dans le cycle de vie d'un pentest.

Les utilisateurs peuvent-ils consulter la méthodologie de test d'AWS Security Agent avant de l'exécuter ?

Il n'existe actuellement aucun moyen de prévisualiser le plan d'action d'AWS Security Agent. Le plan AWS Security Agent est de nature dynamique et repose sur l'exploration de l'application cible. Les clients peuvent surveiller l'agent de sécurité AWS tout au long de son exploration en temps réel en consultant les journaux des tests d'intrusion. Si les journaux indiquent une trajectoire non valide ou indésirable, les clients peuvent arrêter le pentest en cours.

&Déploiement d'intégration

L'agent de sécurité AWS s'intègre-t-il aux outils de sécurité (SIEM, gestion des vulnérabilités) ou aux CI/CD pipelines ?

AWS Security Agent ne s'intègre à aucun outil ou CI/CD pipeline de sécurité existant.

Comment l'agent de sécurité AWS gère-t-il les configurations spécifiques à l'environnement ?

AWS Security Agent peut être configuré pour s'exécuter avec des rôles IAM spécifiques, au sein de VPC, avec des informations d'identification pertinentes pour l'application spécifiées par le client, et avec les référentiels sources Github comme référence de code source pour l'application cible.

L'agent de sécurité AWS peut-il s'exécuter dans des environnements isolés ou isolés ?

AWS Security Agent peut être configuré pour être connecté aux VPC, y compris ceux qui ne disposent pas d'un accès Internet sortant.

Plusieurs membres de l'équipe peuvent-ils effectuer des tests simultanément ?

AWS Security Agent prend en charge 5 essais de pentest simultanés par compte, indépendamment de la personne qui lance le test. Les clients peuvent créer un maximum de 100 espaces d'agent et 1 000 projets Pentest.

Impact opérationnel

Quel est l'impact sur les performances des systèmes testés ?

L'agent de sécurité AWS est doté de barrières de sécurité qui l'empêchent de perturber ou de désactiver les terminaux en cours de test. Cela inclut le contrôle de la vélocité du nombre d'appels que l'agent de sécurité AWS peut effectuer vers un point de terminaison. Le système ou le terminal testé doit s'attendre à une certaine augmentation du trafic et à d'éventuelles alertes de surveillance déclenchées en raison de l'activité du test au stylo. Nous vous recommandons de n'exécuter AWS Security Agent ou toute autre activité de test du stylo que dans un environnement de pré-production.

Les utilisateurs peuvent-ils planifier ou limiter AWS Security Agent ?

AWS Security Agent ne dispose pas d'API publiques et n'est pas en mesure de planifier les tests de stylo. AWS Security Agent ne propose pas non plus de contrôle de simultanéité des demandes adressées au point de terminaison cible lors du lancement du test du stylo. Si AWS Security Agent pose des problèmes aux points de terminaison cibles, les clients peuvent arrêter le ou les tests en cours.

Quelle est la durée habituelle d'une évaluation complète de la sécurité ?

Le temps d'exécution de chaque pentest dépend de l'étendue de l'application cible et des types de risques configurés pour être évalués. La plupart des tests de pentest sont terminés en 16 heures.

Politiques gérées par AWS pour les agents de sécurité AWS

Une stratégie gérée par AWS est une stratégie qui est créée et gérée par AWS. Les politiques gérées par AWS sont conçues pour fournir des autorisations pour de nombreux cas d'utilisation courants afin que vous puissiez commencer à attribuer des autorisations aux utilisateurs, aux groupes et aux rôles.

N'oubliez pas que les politiques gérées par AWS peuvent ne pas accorder d'autorisations de moindre privilège pour vos cas d'utilisation spécifiques, car elles sont disponibles pour tous les clients AWS. Nous vous recommandons de réduire encore les autorisations en définissant des politiques gérées par le client qui sont propres à vos cas d'utilisation.

Vous ne pouvez pas modifier les autorisations définies dans les politiques gérées par AWS. Si AWS met à jour les autorisations définies dans une politique gérée par AWS, la mise à jour affecte toutes les identités principales (utilisateurs, groupes et rôles) auxquelles la politique est attachée. AWS est très susceptible de mettre à jour une politique gérée par AWS lorsqu'un nouveau service AWS est lancé ou lorsque de nouvelles opérations d'API sont disponibles pour les services existants.

Pour plus d'informations, consultez les politiques gérées par AWS dans le guide de l'utilisateur IAM.

Politique gérée par AWS : SecurityAgentWebAppAPIPolicy

Accorde les autorisations nécessaires pour interagir avec l'API de l'application Web Security Agent. Cette politique permet aux utilisateurs de configurer et d'exécuter des tests de pénétration de sécurité automatisés, de gérer l'exécution des tests, de consulter les résultats de sécurité et d'accéder aux ressources de l'agent de sécurité. Cette politique fait référence au type de ressource d'instance d'agent existant et à des actions IAM héritées spécifiques.

Détails de l'autorisation

Cette politique accorde des autorisations pour interagir avec le service Security Testing Control (securityagent :*) pour :

- Pentest Management : créer, mettre à jour, supprimer et répertorier les tests de pénétration et leurs tâches d'exécution
- Résultats de sécurité : consultez, décrivez et mettez à jour les résultats de sécurité issus des tests terminés, y compris le contenu et les métadonnées associés.
- Gestion des tâches : répertorier et récupérer les tâches de révision du code et de révision de la documentation

- Découverte des ressources : répertorier et afficher les instances d'agents, les artefacts, les intégrations et les points de terminaison découverts
- Exécution des tests : démarrer et arrêter les exécutions de pentest grâce à des fonctionnalités de surveillance en temps réel
- Correction du code : lancez la correction automatique du code en fonction des résultats de sécurité

Pour consulter la dernière version du document de politique JSON, consultez SecurityAgentWebAppAPIPolicyle guide de référence des politiques gérées par AWS.

Politique gérée par AWS : AWSSecurityAgentWebAppPolicy

Accorde les autorisations nécessaires pour interagir avec l'API de l'application Web Security Agent. Cette politique permet aux utilisateurs de configurer et d'exécuter des tests de pénétration de sécurité automatisés, de gérer l'exécution des tests, de consulter les résultats de sécurité et d'accéder aux ressources de l'agent de sécurité.

Détails de l'autorisation

Cette politique accorde des autorisations pour interagir avec le service Security Testing Control (securityagent :*) pour :

- Pentest Management : créer, mettre à jour, supprimer et répertorier les tests d'intrusion et leurs tâches
- Résultats de sécurité : consultez, décrivez et mettez à jour les résultats de sécurité issus des tests terminés, y compris le contenu et les métadonnées associés.
- Gestion des tâches : Lister et récupérer les tâches de révision de code et de révision de conception
- Découverte des ressources : répertorier et afficher les espaces des agents, les artefacts, les intégrations et les points de terminaison découverts
- Exécution des tests : démarrer et arrêter des tâches de pentest grâce à des fonctionnalités de surveillance en temps réel
- Correction du code : lancez la correction automatique du code en fonction des résultats de sécurité

Pour consulter la dernière version du document de politique JSON, consultez AWSSecurityAgentWebAppPolicyle guide de référence des politiques gérées par AWS.

Mises à jour des politiques gérées par AWS Security Agent

Consultez les informations relatives aux mises à jour des politiques gérées par AWS pour les agents de sécurité AWS depuis que ce service a commencé à suivre ces modifications.

Pour recevoir des notifications concernant toutes les modifications apportées aux fichiers sources de cette page de documentation spécifique, vous pouvez vous abonner à l'URL suivante à l'aide d'un lecteur RSS :

Modifier	Description	Date
Ajout d'autorisations à AWSSecurityAgentWebAppPolicy.	Autorisations ajoutées `TargetDomain` et de `DesignReviewFeedback` ressources pour les nouveaux types de ressources.	31 mars 2026
Ajout d'une nouvelle politique gérée AWSSecurityAgentWebAppPolicy.	Ajout d'une politique gérée `AWSSecurityAgentWebAppPolicy` pour le nouveau type de AgentSpace ressource et les changements de nom d'action IAM.	9 février 2026
Ajout d'autorisations à SecurityAgentWebAppAPIPolicy.	Ajouté `securityagent:StartCodeRemediation` pour permettre aux utilisateurs de démarrer la correction automatique du code en cas de détection de problèmes de sécurité.	20 janvier 2026
Ajout d'autorisations à SecurityAgentWebAppAPIPolicy.	Ajouté `securityagent:BatchGetSecurityTestContentMetadata` pour permettre aux utilisateurs de visualiser des images dans la console.	5 décembre 2025

Modifier	Description	Date
Les agents de sécurité AWS ont commencé à suivre les modifications.	Les agents de sécurité AWS ont commencé à suivre les modifications apportées à ses politiques gérées par AWS.	2 décembre 2025

Protection des données dans AWS Security Agent

Le modèle de responsabilité partagée d'AWS s'applique à la protection des données dans AWS Security Agent. Comme décrit dans ce modèle, AWS est responsable de la protection de l'infrastructure globale sur laquelle l'ensemble du cloud AWS s'exécute. La gestion du contrôle de votre contenu hébergé sur cette infrastructure relève de votre responsabilité. Vous êtes également responsable des tâches de configuration et de gestion de la sécurité pour les services AWS que vous utilisez. Pour plus d'informations sur la protection des données en Europe, consultez le modèle de responsabilité partagée d'AWS et le billet de blog sur le RGPD sur le blog de sécurité AWS. À des fins de protection des données, nous vous recommandons de protéger les informations d'identification des comptes AWS et de configurer des utilisateurs individuels avec AWS IAM Identity Center ou AWS Identity and Access Management (IAM). Ainsi, chaque utilisateur se voit attribuer uniquement les autorisations nécessaires pour exécuter ses tâches. Nous vous recommandons également de sécuriser vos données comme indiqué ci-dessous :

- Utilisez l'authentification multifactorielle (MFA) avec chaque compte.
- SSL/TLS À utiliser pour communiquer avec les ressources AWS. Nous exigeons TLS 1.2 et recommandons TLS 1.3.
- Configurez l'API et la journalisation des activités des utilisateurs avec AWS CloudTrail. Pour plus d'informations sur l'utilisation des CloudTrail sentiers pour capturer les activités AWS, consultez la section Travailler avec des CloudTrail sentiers dans le guide de CloudTrail l'utilisateur AWS.
- Utilisez des solutions de chiffrement AWS, ainsi que tous les contrôles de sécurité par défaut au sein des services AWS.
- Utilisez des services de sécurité gérés avancés tels qu'Amazon Macie, qui contribuent à la découverte et à la sécurisation des données sensibles stockées dans Amazon S3.
- Si vous avez besoin de modules cryptographiques validés par la norme FIPS 140-3 pour accéder à AWS via une interface de ligne de commande ou une API, utilisez un point de terminaison FIPS.

Pour plus d'informations sur les points de terminaison FIPS disponibles, consultez Norme FIPS (Federal Information Processing Standard) 140-3.

Nous vous recommandons fortement de ne jamais placer d'informations confidentielles ou sensibles, telles que les adresses e-mail de vos clients, dans des balises ou des champs de texte libre tels que le champ Nom. Cela inclut lorsque vous travaillez avec l'agent de sécurité AWS ou d'autres services AWS à l'aide de la console, de l'API, de l'interface de ligne de commande AWS ou des kits SDK AWS. Toutes les données que vous entrez dans des balises ou des champs de texte de forme libre utilisés pour les noms peuvent être utilisées à des fins de facturation ou dans les journaux de diagnostic. Si vous fournissez une adresse URL à un serveur externe, nous vous recommandons fortement de ne pas inclure d'informations d'identification dans l'adresse URL permettant de valider votre demande adressée à ce serveur.

Chiffrement au repos

AWS Security Agent chiffre toutes les données au repos à l'aide de clés AWS-managed de chiffrement par défaut. Cela inclut notamment les éléments suivants :

- Documents de conception et code : tous les documents de conception, les référentiels de code et les artefacts d'application que vous fournissez pour les révisions de sécurité sont chiffrés par AES-256 chiffrement.
- Résultats de sécurité : tous les résultats de sécurité, les rapports de vulnérabilité et les recommandations de correction sont chiffrés au repos.
- Données de configuration : les exigences de sécurité, les politiques personnalisées et les configurations de service sont cryptées.
- Journaux d'audit : tous les journaux d'activité des services et les pistes d'audit sont chiffrés.

AWS Security Agent utilise AWS Key Management Service (AWS KMS) pour gérer les clés de chiffrement. Vous pouvez éventuellement utiliser une clé gérée par le client pour chiffrer vos données, ce qui vous donne un contrôle total sur les clés de chiffrement qui protègent vos ressources. Pour de plus amples informations, veuillez consulter the section called "Clés gérées par le client".

Chiffrement en transit

AWS Security Agent chiffre toutes les données en transit à l'aide du protocole TLS (Transport Layer Security) 1.2 ou supérieur. Cela s'applique aux éléments suivants :

- Communications par API : tous les appels d'API entre vos applications et AWS Security Agent utilisent le protocole HTTPS avec chiffrement TLS.
- Accès à la console — La console AWS Security Agent est accessible via HTTPS.
- Connexions aux référentiels : les connexions aux référentiels de code GitHub et à d'autres référentiels utilisent des protocoles chiffrés.
- Communications avec les agents : toutes les communications entre le service AWS Security Agent et les agents de test d'intrusion utilisent des canaux cryptés.

Gestion des clés

AWS Security Agent utilise AWS Key Management Service (AWS KMS) pour gérer les clés de chiffrement. Par défaut, les données sont chiffrées à l'aide de AWS-managed clés. Vous pouvez éventuellement spécifier une clé gérée par le client lors de la création de ressources telles que les espaces d'agent et les intégrations. Pour de plus amples informations, veuillez consulter the section called “Clés gérées par le client”.

Confidentialité du trafic inter-réseau

AWS Security Agent utilise l'Internet public pour communiquer avec les fournisseurs de contrôle de source hébergés dans le cloud (GitHub, GitLab, Bitbucket) et Confluence Cloud.

Pour les fournisseurs auto-hébergés (GitHub Enterprise Server) GitLab Self-Managed, vous pouvez configurer des connexions privées à l'aide d'Amazon VPC Lattice afin de conserver tout le trafic au sein du réseau AWS. Pour de plus amples informations, veuillez consulter the section called “Connectez-vous au contrôle de source hébergé en privé”.

Dans la configuration par défaut, AWS Security Agent utilise l'Internet public pour accéder à votre application à des fins de test d'intrusion. Vous pouvez éventuellement configurer des tests de pénétration pour utiliser un VPC pour accéder à votre application. Pour de plus amples informations, veuillez consulter the section called “Connect l'agent aux ressources VPC privées”.

Cross-Region traitement des données

AWS Security Agent utilise l'inférence entre régions pour optimiser les ressources de calcul disponibles et la disponibilité des modèles. Selon la région d'où provient la demande, nous pouvons traiter les demandes de saisie et les résultats de sortie dans une autre région.

- Dans l'est des États-Unis (Virginie du Nord)`us-east-1`, l'ouest des États-Unis (Oregon)`us-west-2`, l'Asie-Pacifique (Sydney)`ap-southeast-2`, l'Asie-Pacifique (Tokyo)`ap-northeast-1`,

l'Europe (Francfort) et l'Europe (Irlande)`eu-west-1`, AWS Security Agent utilise l'inférence géographique entre régions. `eu-central-1` Pour la plupart des fonctionnalités, le traitement des données reste à l'intérieur de la limite géographique (comme les États-Unis, l'UE, l'Australie ou le Japon) d'où provient la demande. Pour la correction du code, les demandes provenant de l'Australie et du Japon sont traitées dans l'Union européenne. Pour obtenir des informations de routage spécifiques aux fonctionnalités, consultez le tableau d'inférence entre régions.

- En Asie-Pacifique (Mumbai)`ap-south-1`, en Asie-Pacifique (Singapour) `ap-southeast-1` et en Amérique du Sud (São Paulo)`sa-east-1`, AWS Security Agent utilise l'inférence interrégionale globale. Nous pouvons traiter les demandes de saisie et les résultats de sortie dans n'importe quelle région AWS commerciale.

Dans tous les cas, vos données restent stockées uniquement dans la région d'où provient la demande. Toutes les données transmises lors d'opérations interrégionales restent sur le réseau AWS et ne transitent pas par l'Internet public. Nous chiffrons les données en transit entre les régions AWS.

Cross-Region l'inférence est toujours activée et ne peut pas être désactivée. Pour plus de détails sur les régions qui traitent les demandes pour chaque fonctionnalité, consultez la section Inférence entre régions dansthe section called “Bonnes pratiques de sécurité”.

Suppression de données

Lorsque vous supprimez des données d'AWS Security Agent :

- Les données sont marquées pour suppression et ne sont plus accessibles via le service.
- Les données sont supprimées de tous les systèmes AWS Security Agent dans un délai de 30 jours.

Pour supprimer vos données

1. Dans la console AWS, accédez à AWS Security Agent.
2. Choisissez les données que vous souhaitez supprimer (évaluations de sécurité, résultats ou exigences personnalisées).
3. Choisissez Supprimer et confirmez la suppression.

Gestion des identités et des accès pour AWS Security Agent

Gestion des identités et des accès AWS (IAM) est un outil Service AWS qui permet à un administrateur de contrôler en toute sécurité l'accès aux AWS ressources. IAM les administrateurs

contrôlent qui peut être authentifié (connecté) et autorisé (autorisé) à utiliser les ressources d'AWS Security Agent. IAM est un Service AWS ventilateur que vous pouvez utiliser sans frais supplémentaires.

Public ciblé

La façon dont vous utilisez Gestion des identités et des accès AWS (IAM) varie en fonction du travail que vous effectuez dans AWS Security Agent.

Utilisateur du service : si vous utilisez le service AWS Security Agent pour effectuer votre travail, votre administrateur vous fournit les informations d'identification et les autorisations dont vous avez besoin. Au fur et à mesure que vous utilisez de plus en plus de fonctionnalités d'AWS Security Agent dans le cadre de votre travail, il se peut que vous ayez besoin d'autorisations supplémentaires. Si vous comprenez bien la gestion des accès, vous saurez demander les autorisations appropriées à votre administrateur.

Si vous ne pouvez pas accéder à une fonctionnalité d'AWS Security Agent, consultezthe section called “Résolution des problèmes liés à l'identité et à l'accès de l'agent de sécurité AWS”.

Administrateur du service : si vous êtes responsable des ressources d'AWS Security Agent dans votre entreprise, vous avez probablement un accès complet à AWS Security Agent. Il vous incombe de déterminer les fonctionnalités et les ressources de l'agent de sécurité AWS auxquelles les utilisateurs de vos services doivent accéder. Vous devez ensuite envoyer des demandes à votre IAM administrateur pour modifier les autorisations des utilisateurs de votre service. Consultez les informations de cette page pour comprendre les concepts de base de IAM. Pour en savoir plus sur la façon dont votre entreprise peut utiliser IAM AWS Security Agent, consultezthe section called “Comment fonctionne l'agent de sécurité AWS avec IAM”.

IAM administrateur - Si vous êtes IAM administrateur, vous souhaiterez peut-être en savoir plus sur la manière dont vous pouvez rédiger des politiques pour gérer l'accès à AWS Security Agent. Pour consulter des exemples de politiques basées sur l'identité d'AWS Security Agent que vous pouvez utiliser IAM, consultez. the section called “Exemples de politiques basées sur l'identité d'AWS Security Agent”

Authentification par des identités

L'authentification est la façon dont vous vous connectez à AWS l'aide de vos informations d'identification. Vous devez être authentifié (connecté à AWS) en tant qu'utilisateur root du compte AWS Utilisateur IAM, ou en assumant un IAM rôle. AWS suggère d'utiliser un rôle IAM et d'éviter d'utiliser directement l'utilisateur root.

Vous pouvez vous connecter en AWS tant qu'identité fédérée en utilisant les informations d'identification fournies par le biais d'une source d'identité. AWS IAM Identity Center (IAM Identity Center) les utilisateurs, l'authentification unique de votre entreprise et vos informations d'identification Google ou Facebook sont des exemples d'identités fédérées. Lorsque vous vous connectez en tant qu'identité fédérée, votre administrateur a préalablement configuré la fédération d'identité à l'aide de IAM rôles. Lorsque vous accédez à AWS l'aide de la fédération, vous assumez indirectement un rôle.

Selon le type d'utilisateur que vous êtes, vous pouvez vous connecter au portail Console de gestion AWS ou au portail AWS d'accès. Pour plus d'informations sur la connexion à AWS, consultez Comment vous connecter à votre compte AWS dans le guide de Sign-In l'utilisateur AWS.

Si vous y accédez AWS par programmation, AWS fournit un kit de développement logiciel (SDK) et une interface de ligne de commande (CLI) pour signer cryptographiquement vos demandes à l'aide de vos informations d'identification. Si vous n'utilisez pas d' AWS outils, vous devez signer vous-même les demandes. Pour plus d'informations sur l'utilisation de la méthode recommandée pour signer vous-même les demandes, consultez le processus de signature de la version 4 de Signature dans les références générales d'AWS.

Quelle que soit la méthode d'authentification que vous utilisez, vous devrez peut-être également fournir des informations de sécurité supplémentaires. Par exemple, il vous AWS recommande d'utiliser l'authentification multifactorielle (MFA) pour renforcer la sécurité de votre compte. Pour en savoir plus, consultez le guide de l'utilisateur Multi-factor d'AWS IAM Identity Center (successeur d'AWS Single Sign-On) sur l'authentification et l'utilisation de l'authentification multifactorielle (MFA) dans AWS dans le guide de l'utilisateur IAM.

Utilisateur racine d'un compte AWS

Lorsque vous créez un Compte AWS, vous commencez par une identité de connexion unique qui donne un accès complet à toutes Services AWS les ressources du compte. Cette identité est appelée utilisateur racine du compte AWS et elle est accessible après connexion à l'aide de l'adresse e-mail et du mot de passe utilisés pour la création du compte. Il est vivement recommandé de ne pas utiliser l'utilisateur racine pour vos tâches quotidiennes. Protégez vos informations d'identification d'utilisateur racine et utilisez-les pour effectuer les tâches que seul l'utilisateur root peut effectuer. Pour obtenir la liste complète des tâches qui nécessitent que vous vous connectiez en tant qu'utilisateur root, consultez la section Tâches nécessitant des informations d'identification d'utilisateur root dans le Guide de référence sur la gestion des comptes.

Identité fédérée

La meilleure pratique consiste à obliger les utilisateurs humains, y compris ceux qui ont besoin d'un accès administrateur, à utiliser la fédération avec un fournisseur d'identité pour accéder à l'aide Services AWS d'informations d'identification temporaires.

Une identité fédérée est un utilisateur de l'annuaire des utilisateurs de votre entreprise, d'un fournisseur d'identité Web AWS Directory Service, du répertoire Identity Center ou de tout utilisateur qui y accède à l'aide des informations d'identification fournies Services AWS par le biais d'une source d'identité. Lorsque des identités fédérées y accèdent Comptes AWS, elles assument des rôles, qui fournissent des informations d'identification temporaires.

Pour une gestion des accès centralisée, nous vous recommandons d'utiliser AWS IAM Identity Center. Vous pouvez créer des utilisateurs et des groupes dans IAM Identity Center, ou vous pouvez vous connecter et synchroniser avec un ensemble d'utilisateurs et de groupes dans votre propre source d'identité afin de les utiliser dans toutes vos applications Comptes AWS et applications. Pour plus d'informations sur IAM Identity Center, voir Qu'est-ce qu'IAM Identity Center ? dans le guide de l'utilisateur d'AWS IAM Identity Center (successeur d'AWS Single Sign-On).

Utilisateurs IAM et groupes

An Utilisateur IAMest une identité au sein de vous Compte AWS qui possède des autorisations spécifiques pour une seule personne ou une seule application. Dans la mesure du possible, nous vous recommandons de vous fier à des informations d'identification temporaires plutôt que de créer des Utilisateurs IAM personnes possédant des informations d'identification à long terme, telles que des mots de passe et des clés d'accès. Toutefois, si vous avez des cas d'utilisation spécifiques qui nécessitent des informations d'identification à long terme Utilisateurs IAM, nous vous recommandons de faire pivoter les clés d'accès. Pour plus d'informations, consultez Rotation régulière des clés d'accès pour les cas d'utilisation nécessitant des informations d'identification dans le Guide de l'utilisateur IAM.

Un IAM groupe est une identité qui spécifie une collection de Utilisateurs IAM. Vous ne pouvez pas vous connecter en tant que groupe. Vous pouvez utiliser les groupes pour spécifier des autorisations pour plusieurs utilisateurs à la fois. Les groupes permettent de gérer plus facilement les autorisations pour de grands ensembles d'utilisateurs. Par exemple, vous pourriez avoir un groupe nommé IAMadmins et lui donner les autorisations nécessaires pour administrer IAM les ressources.

Les utilisateurs sont différents des rôles. Un utilisateur est associé de manière unique à une personne ou une application, alors qu'un rôle est conçu pour être endossé par tout utilisateur qui en a besoin.

Les utilisateurs disposent d'informations d'identification permanentes, mais les rôles fournissent des informations d'identification temporaires. Pour en savoir plus, consultez la section Quand créer un rôle Utilisateur IAM (au lieu d'un rôle) dans le guide de l'utilisateur IAM.

IAM roles

Un IAM rôle est une identité au sein de Compte AWS vous dotée d'autorisations spécifiques. Il est similaire à un Utilisateur IAM, mais n'est pas associé à une personne en particulier. Vous pouvez assumer temporairement un IAM rôle dans le en Console de gestion AWS changeant de rôle. Vous pouvez assumer un rôle en appelant une opération d' AWS API AWS CLI ou en utilisant une URL personnalisée. Pour plus d'informations sur les méthodes d'utilisation des rôles, consultez la section Utilisation IAM des rôles dans le Guide de l'utilisateur IAM.

IAM les rôles dotés d'informations d'identification temporaires sont utiles dans les situations suivantes :

- Accès utilisateur fédéré : pour attribuer des autorisations à une identité fédérée, vous créez un rôle et définissez des autorisations pour le rôle. Quand une identité externe s'authentifie, l'identité est associée au rôle et reçoit les autorisations qui sont définies par celui-ci. Pour obtenir des informations sur les rôles pour la fédération, consultez Création d'un rôle pour un fournisseur d'identité tiers (fédération) dans le Guide de l'utilisateur IAM. Si vous utilisez IAM Identity Center, vous configurez un jeu d'autorisations. IAM Identity Center met en corrélation le jeu d'autorisations avec un rôle dans IAM afin de contrôler à quoi vos identités peuvent accéder après leur authentification. Pour plus d'informations sur les ensembles d'autorisations, consultez la section Ensembles d'autorisations du guide de l'utilisateur d'AWS IAM Identity Center (successeur d'AWS Single Sign-On).
- Utilisateur IAM Autorisations temporaires — An Utilisateur IAM peut assumer un IAM rôle en assumant temporairement différentes autorisations pour une tâche spécifique.
- Cross-account accès : vous pouvez utiliser un IAM rôle pour autoriser une personne (un mandant fiable) d'un autre compte à accéder aux ressources de votre compte. Les rôles constituent le principal moyen d'accorder l'accès intercompte. Toutefois, dans certains Services AWS cas, vous pouvez associer une politique directement à une ressource (au lieu d'utiliser un rôle comme proxy). Pour connaître la différence entre les rôles et les politiques basées sur les ressources pour l'accès entre comptes, consultez la section En quoi les IAM rôles diffèrent des politiques basées sur les ressources dans le Guide de l'utilisateur IAM.
- Cross-service accès — Certains Services AWS utilisent des fonctionnalités dans d'autres Services AWS. Par exemple, lorsque vous effectuez un appel dans un service, il est courant que ce service

exécute des applications Amazon EC2 ou y stocke des objets Amazon S3. Un service peut le faire en utilisant les autorisations d'appel du principal, une fonction du service ou un rôle lié au service.

- Autorisations principales — Lorsque vous utilisez un rôle Utilisateur IAM ou pour effectuer des actions AWS, vous êtes considéré comme un mandant. Les politiques accordent des autorisations au principal. Lorsque vous utilisez certains services, vous pouvez effectuer une action qui déclenche une autre action dans un autre service. Dans ce cas, vous devez disposer des autorisations nécessaires pour effectuer les deux actions.
- Rôle de service — Un rôle de service est un IAM rôle qu'un service assume pour effectuer des actions en votre nom. Un IAM administrateur peut créer, modifier et supprimer un rôle de service de l'intérieur IAM. Pour plus d'informations, consultez Création d'un rôle pour la délégation d'autorisations à un Service AWS dans le Guide de l'utilisateur IAM.
- Service-linked rôle — Un rôle lié à un service est un type de rôle de service lié à un. Service AWS Le service peut assumer le rôle d'effectuer une action en votre nom. Service-linked les rôles apparaissent dans votre fichier Compte AWS et appartiennent au service. Un IAM administrateur peut consulter, mais pas modifier les autorisations pour les rôles liés à un service.

- Applications exécutées sur Amazon EC2 : vous pouvez utiliser un IAM rôle pour gérer les informations d'identification temporaires pour les applications qui s'exécutent sur une Amazon EC2 instance et qui envoient AWS CLI des demandes AWS d'API. Cela est préférable au stockage des clés d'accès dans l' Amazon EC2 instance. Pour attribuer un AWS rôle à une Amazon EC2 instance et le rendre disponible pour toutes ses applications, vous devez créer un profil d'instance attaché à l'instance. Un profil d'instance contient le rôle et permet aux programmes exécutés sur l' Amazon EC2 instance d'obtenir des informations d'identification temporaires. Pour plus d'informations, consultez la section Utilisation d'un IAM rôle pour accorder des autorisations aux applications exécutées sur des Amazon EC2 instances dans le Guide de l'utilisateur IAM.

Pour savoir s'il faut utiliser IAM des rôles, voir Quand créer un IAM rôle (au lieu d'un utilisateur) dans le guide de l'utilisateur IAM.

Gestion de l'accès à l'aide de politiques

Vous contrôlez l'accès en AWS créant des politiques et en les associant à AWS des identités ou à des ressources. Une politique est un objet AWS qui, lorsqu'il est associé à une identité ou à une ressource, définit leurs autorisations. AWS évalue ces politiques lorsqu'un principal (utilisateur, utilisateur root ou session de rôle) fait une demande. Les autorisations dans les politiques déterminent si la demande est autorisée ou refusée. La plupart des politiques sont stockées AWS sous forme de documents JSON. Pour plus d'informations sur la structure et le contenu des

documents de politique JSON, consultez Vue d'ensemble des politiques JSON dans le Guide de l'utilisateur IAM.

Les administrateurs peuvent utiliser les politiques AWS JSON pour spécifier qui a accès à quoi. C'est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

Chaque IAM entité (utilisateur ou rôle) démarre sans aucune autorisation. Par défaut, les utilisateurs ne peuvent rien faire, pas même changer leur propre mot de passe. Pour autoriser un utilisateur à effectuer une opération, un administrateur doit lui associer une politique d'autorisations. Il peut également ajouter l'utilisateur à un groupe disposant des autorisations prévues. Lorsqu'un administrateur accorde des autorisations à un groupe, tous les utilisateurs de ce groupe se voient octroyer ces autorisations.

IAM les politiques définissent les autorisations pour une action, quelle que soit la méthode que vous utilisez pour effectuer l'opération. Par exemple, supposons que vous disposiez d'une politique qui autorise l'action `iam:GetRole`. Un utilisateur appliquant cette politique peut obtenir des informations sur le rôle à partir de Console de gestion AWS AWS CLI, de ou de l' AWS API.

Identity-based politiques

Identity-based les politiques sont des documents de politique d'autorisations JSON que vous pouvez joindre à une identité, telle qu'un Utilisateur IAM, un rôle ou un groupe. Ces politiques contrôlent quel type d'actions des utilisateurs et des rôles peuvent exécuter, sur quelles ressources et dans quelles conditions. Pour savoir comment créer une politique basée sur l'identité, consultez la section Création de IAM politiques dans le guide de l'utilisateur IAM.

Identity-based les politiques peuvent également être classées en tant que politiques intégrées ou politiques gérées. Les politiques en ligne sont intégrées directement à un utilisateur, groupe ou rôle. Les politiques gérées sont des politiques autonomes que vous pouvez associer à plusieurs utilisateurs, groupes et rôles au sein de votre Compte AWS. Les politiques gérées incluent les politiques AWS gérées et les politiques gérées par le client. Pour découvrir comment choisir entre une politique gérée et une politique en ligne, consultez Choix entre les politiques gérées et les politiques en ligne dans le Guide de l'utilisateur IAM.

Resource-based politiques

Resource-based les politiques sont des documents de politique JSON que vous attachez à une ressource telle qu'un Amazon S3 bucket. Les administrateurs de service peuvent utiliser ces

politiques pour définir les actions qu'un principal spécifié (membre du compte, utilisateur ou rôle) peut effectuer sur cette ressource et dans quelles conditions. Resource-based les politiques sont des politiques intégrées. Il ne s'agit pas de politiques gérées basées sur les ressources.

Listes de contrôle d'accès (ACL)

Les listes de contrôle d'accès (ACL) sont un type de politique qui permet de définir les mandataires (membres de compte, utilisateurs ou rôles) ayant l'autorisation d'accéder à une ressource. Les ACL sont similaires aux politiques basées sur les ressources, bien qu'elles n'utilisent pas le format de document de politique JSON. Amazon S3 AWS WAF, et Amazon VPC sont des exemples de services qui prennent en charge les ACL. Pour en savoir plus sur les listes de contrôle d'accès, consultez Présentation des listes de contrôle d'accès (ACL) dans le Guide du développeur Amazon Simple Storage Service.

Autres types de politique

AWS prend en charge d'autres types de politiques moins courants. Ces types de politiques peuvent définir le nombre maximum d'autorisations qui vous sont accordées par des types de politiques plus courants.

- Limites d'autorisations — Une limite d'autorisations est une fonctionnalité avancée dans laquelle vous définissez le maximum d'autorisations qu'une politique basée sur l'identité peut accorder à une IAM entité (Utilisateur IAM ou à un rôle). Vous pouvez définir une limite d'autorisations pour une entité. Les autorisations qui en résultent sont l'intersection des politiques basées sur l'identité de l'entité et de ses limites d'autorisations. Resource-based les politiques qui spécifient l'utilisateur ou le rôle `Principal` sur le terrain ne sont pas limitées par la limite des autorisations. Un refus explicite dans l'une de ces politiques annule l'autorisation. Pour plus d'informations sur les limites d'autorisations, consultez la section Limites d'autorisations pour les IAM entités dans le guide de l'utilisateur IAM.
- Politiques de contrôle des services (SCP) — Les SCP sont des politiques JSON qui spécifient les autorisations maximales pour une organisation ou une unité organisationnelle (UO) dans. AWS Organizations AWS Organizations est un service permettant de regrouper et de gérer de manière centralisée Comptes AWS les multiples propriétés de votre entreprise. Si vous activez toutes les fonctionnalités d'une organisation, vous pouvez appliquer les politiques de contrôle des services (SCP) à l'un ou à l'ensemble de vos comptes. La SCP limite les autorisations pour les entités dans les comptes membres, y compris dans chaque utilisateur racine d'un compte AWS. Pour plus d'informations sur les Organisations et les SCP, consultez Fonctionnement des stratégies de contrôle de service dans le Manuel de l'utilisateur AWS Organizations.

- Politiques de session : les politiques de session sont des politiques avancées que vous utilisez en tant que paramètre lorsque vous créez par programmation une session temporaire pour un rôle ou un utilisateur fédéré. Les autorisations de la session obtenue sont une combinaison des politiques basées sur l'identité de l'utilisateur ou du rôle et des politiques de session. Les autorisations peuvent également provenir d'une politique basée sur les ressources. Un refus explicite dans l'une de ces politiques annule l'autorisation. Pour plus d'informations, consultez Politiques de session dans le Guide de l'utilisateur IAM.

Plusieurs types de politique

Lorsque plusieurs types de politiques s'appliquent à la requête, les autorisations en résultant sont plus compliquées à comprendre. Pour savoir comment AWS déterminer s'il faut autoriser une demande lorsque plusieurs types de politiques sont impliqués, consultez la section Logique d'évaluation des politiques dans le guide de l'utilisateur IAM.

Comment fonctionne l'agent de sécurité AWS avec IAM

Avant de commencer IAM à gérer l'accès à AWS Security Agent, découvrez quelles IAM fonctionnalités sont disponibles avec AWS Security Agent.

Fonctionnalité IAM	Support pour les agents de sécurité AWS
the section called "Identity-based politiques relatives à l'agent de sécurité AWS"	Oui
the section called "Resource-based politiques au sein d'AWS Security Agent"	Non
the section called "Actions de politique pour AWS Security Agent"	Oui
the section called "Ressources relatives aux politiques pour AWS Security Agent"	Partielle
the section called "Clés de conditions de politique pour AWS Security Agent"	Oui
the section called "Listes de contrôle d'accès (ACL) dans AWS Security Agent"	Non

Fonctionnalité IAM	Support pour les agents de sécurité AWS
the section called “Attribute-based contrôle d'accès (ABAC) avec AWS Security Agent”	Non
the section called “Utilisation d'informations d'identification temporaires avec AWS Security Agent”	Oui
the section called “Transférer les sessions d'accès pour AWS Security Agent”	Oui
the section called “Rôles de service pour AWS Security Agent”	Non
the section called “Service-linked rôles pour AWS Security Agent”	Oui

Pour obtenir une vue d'ensemble de la façon dont AWS Security Agent et les autres agents Services AWS fonctionnent avec IAM, consultez Services AWS le guide IAM de l'utilisateur d'IAM.

Identity-based politiques relatives à l'agent de sécurité AWS

Prend en charge les politiques basées sur l'identité : oui

Identity-based les politiques sont des documents de politique d'autorisation JSON que vous pouvez associer à une identité, telle qu'un utilisateur IAM, un groupe d'utilisateurs ou un rôle. Ces politiques contrôlent quel type d'actions des utilisateurs et des rôles peuvent exécuter, sur quelles ressources et dans quelles conditions. Pour découvrir comment créer une politique basée sur l'identité, consultez Définition d'autorisations IAM personnalisées avec des politiques gérées par le client dans le Guide de l'utilisateur IAM.

Avec les politiques IAM basées sur l'identité, vous pouvez spécifier les actions et les ressources autorisées ou refusées ainsi que les conditions dans lesquelles les actions sont autorisées ou refusées. Vous ne pouvez pas spécifier le principal dans une stratégie basée sur l'identité car il s'applique à l'utilisateur ou au rôle auquel il est attaché. Pour en savoir plus sur tous les éléments que vous utilisez dans une politique JSON, consultez la référence des éléments de stratégie IAM JSON dans le guide de l'utilisateur IAM.

Identity-based exemples de politiques pour AWS Security Agent

Pour consulter des exemples de politiques basées sur l'identité d'AWS Security Agent, consultez. the section called "Exemples de politiques basées sur l'identité d'AWS Security Agent"

Resource-based politiques au sein d'AWS Security Agent

Prend en charge les politiques basées sur les ressources : non

Resource-based les politiques sont des documents de politique JSON que vous attachez à une ressource. Par exemple, les politiques de confiance de rôle IAM et les politiques de compartiment Amazon S3 sont des politiques basées sur les ressources. Dans les services qui sont compatibles avec les politiques basées sur les ressources, les administrateurs de service peuvent les utiliser pour contrôler l'accès à une ressource spécifique. Pour la ressource dans laquelle se trouve la politique, cette dernière définit quel type d'actions un principal spécifié peut effectuer sur cette ressource et dans quelles conditions. Vous devez spécifier un principal dans une politique basée sur les ressources. Les principaux peuvent inclure des comptes, des utilisateurs, des rôles, des utilisateurs fédérés ou des services AWS.

Pour permettre un accès intercompte, vous pouvez spécifier un compte entier ou des entités IAM dans un autre compte en tant que principal dans une politique basée sur les ressources. L'ajout d'un principal intercompte à une politique basée sur les ressources ne représente qu'une partie de l'instauration de la relation d'approbation. Lorsque le principal et la ressource se trouvent dans des comptes AWS différents, un administrateur IAM du compte sécurisé doit également accorder à l'entité principale (utilisateur ou rôle) l'autorisation d'accéder à la ressource. Pour ce faire, il attache une politique basée sur une identité à l'entité. Toutefois, si une politique basée sur des ressources accorde l'accès à un principal dans le même compte, aucune autre politique basée sur l'identité n'est requise. Pour plus d'informations, consultez la section Accès aux ressources entre comptes dans IAM dans le guide de l'utilisateur d'IAM.

Actions de politique pour AWS Security Agent

Soutient les actions Oui

Les administrateurs peuvent utiliser les stratégies AWS JSON pour spécifier qui a accès à quoi. C'est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

L'`Action`élément d'une politique IAM basée sur l'identité décrit l'action ou les actions spécifiques qui seront autorisées ou refusées par la politique. Les actions de stratégie portent généralement le même

nom que l'opération AWS d'API associée. L'action est utilisée dans une politique pour permettre d'effectuer l'opération associée.

Les actions de politique dans AWS Security Agent utilisent le préfixe suivant avant l'action : `securityagent:` Par exemple, pour autoriser une personne à créer un environnement avec l'opération d'`CreateEnvironment`API AWS Security Agent, vous devez inclure l'`securityagent:CreateEnvironment`action dans sa politique. Les déclarations de politique doivent inclure un élément `Action` ou `NotAction`. AWS Security Agent définit son propre ensemble d'actions décrivant les tâches que vous pouvez effectuer avec ce service.

Pour spécifier plusieurs actions dans une seule déclaration, séparez-les par des virgules comme suit :

```
"Action": [
      "securityagent:action1",
      "securityagent:action2"
```

Vous pouvez aussi spécifier plusieurs actions à l'aide de caractères génériques (*). Par exemple, pour spécifier toutes les actions qui commencent par le mot `List`, incluez l'action suivante :

```
"Action": "securityagent:List*"
```

Ressources relatives aux politiques pour AWS Security Agent

Prend en charge les ressources de politique : partiellement

Les administrateurs peuvent utiliser les stratégies AWS JSON pour spécifier qui a accès à quoi. C'est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

L'élément de politique JSON `Resource` indique le ou les objets auxquels l'action s'applique. Les instructions doivent inclure un élément `Resource` ou `NotResource`. Il est recommandé de définir une ressource à l'aide de son Amazon Resource Name (ARN). Vous pouvez le faire pour des actions qui prennent en charge un type de ressource spécifique, connu sous la dénomination autorisations de niveau ressource.

Pour les actions qui ne prennent pas en charge les autorisations au niveau des ressources, telles que les opérations de listage, utilisez un caractère générique (*) pour indiquer que la déclaration s'applique à toutes les ressources.

```
"Resource": "*"
```

Certaines actions de l'API AWS Security Agent prennent en charge plusieurs ressources. Par exemple, plusieurs environnements peuvent être référencés lors de l'appel de l'action `ListEnvironments` API. Pour spécifier plusieurs ressources dans une seule instruction, séparez leurs ARN par des virgules.

```
"Resource": [
      "EXAMPLE-RESOURCE-1",
      "EXAMPLE-RESOURCE-2"
```

Par exemple, la ressource d'environnement AWS Security Agent possède l'ARN suivant :

```
arn:${Partition}:securityagent:${Region}:${Account}:environment/${EnvironmentId}
```

Pour spécifier les environnements `my-environment-1` et `my-environment-2` dans votre déclaration, utilisez les exemples d'ARN suivants :

```
"Resource": [
        "arn:aws:securityagent:us-east-1:123456789012:environment/my-environment-1",
        "arn:aws:securityagent:us-east-1:123456789012:environment/my-environment-2"
```

Pour spécifier tous les environnements appartenant à un compte spécifique, utilisez le caractère générique (*) :

```
"Resource": "arn:aws:securityagent:us-east-1:123456789012:environment/*"
```

Clés de conditions de politique pour AWS Security Agent

Prend en charge les clés de condition de politique spécifiques au service : oui

Les administrateurs peuvent utiliser les stratégies AWS JSON pour spécifier qui a accès à quoi. C'est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

L'`Condition`élément (ou le `Condition` bloc) vous permet de définir les conditions dans lesquelles une instruction est effective. L'élément `Condition` est facultatif. Vous pouvez créer des expressions conditionnelles qui utilisent des opérateurs de condition, tels que les signes égal ou inférieur à, pour faire correspondre la condition de la politique aux valeurs de la demande.

Si vous spécifiez plusieurs éléments `Condition` dans une instruction, ou plusieurs clés dans un seul élément `Condition`, AWS les évalue à l'aide d'une opération `AND` logique. Si vous spécifiez plusieurs valeurs pour une seule clé de condition, AWS évalue la condition à l'aide d'une `OR` opération logique. Toutes les conditions doivent être remplies avant que les autorisations de la déclaration ne soient accordées.

Vous pouvez aussi utiliser des variables d'espace réservé quand vous spécifiez des conditions. Par exemple, vous ne pouvez accorder Utilisateur IAM l'autorisation d'accéder à une ressource que si elle Utilisateur IAM porte son nom. Pour plus d'informations, consultez IAM la section Éléments de politique : variables et balises dans le guide de l'utilisateur IAM.

AWS Security Agent définit son propre ensemble de clés de condition et prend également en charge l'utilisation de certaines clés de condition globales. Pour voir toutes les clés de condition AWS globales, voir les clés de contexte de condition AWS globales dans le guide de l'utilisateur IAM.

Listes de contrôle d'accès (ACL) dans AWS Security Agent

Prend en charge les ACL : non

Les listes de contrôle d'accès (ACL) vérifie quels principaux (membres de compte, utilisateurs ou rôles) ont l'autorisation d'accéder à une ressource. Les listes de contrôle d'accès sont similaires aux politiques basées sur les ressources, bien qu'elles n'utilisent pas le format de document de politique JSON.

Attribute-based contrôle d'accès (ABAC) avec AWS Security Agent

Prise en charge d'ABAC (balises dans les politiques) : non

Utilisation d'informations d'identification temporaires avec AWS Security Agent

Prend en charge les informations d'identification temporaires : oui

Certains services AWS ne fonctionnent pas lorsque vous vous connectez à l'aide d'informations d'identification temporaires. Pour plus d'informations, notamment pour savoir quels services AWS fonctionnent avec des informations d'identification temporaires, consultez la section Services AWS compatibles avec IAM dans le guide de l'utilisateur d'IAM.

Vous utilisez des informations d'identification temporaires si vous vous connectez à l'AWS Management Console à l'aide d'une méthode autre que le nom d'utilisateur et le mot de passe. Par exemple, lorsque vous accédez à AWS via le lien d'authentification unique (SSO) de votre entreprise, ce processus crée automatiquement des informations d'identification temporaires. Vous

créez également automatiquement des informations d'identification temporaires lorsque vous vous connectez à la console en tant qu'utilisateur, puis changez de rôle. Pour plus d'informations sur le changement de rôle, consultez Passage d'un rôle utilisateur à un rôle IAM (console) dans le Guide de l'utilisateur IAM.

Vous pouvez créer manuellement des informations d'identification temporaires à l'aide de l'AWS CLI ou de l'API AWS. Vous pouvez ensuite utiliser ces informations d'identification temporaires pour accéder à AWS. AWS vous recommande de générer des informations d'identification temporaires de manière dynamique au lieu d'utiliser des clés d'accès à long terme. Pour plus d'informations, consultez Informations d'identification de sécurité temporaires dans IAM.

Transférer les sessions d'accès pour AWS Security Agent

Prend en charge les sessions d'accès direct (FAS) : oui

Lorsque vous utilisez un utilisateur ou un rôle IAM pour effectuer des actions dans AWS, vous êtes considéré comme un mandant. Lorsque vous utilisez certains services, vous pouvez effectuer une action qui initie une autre action dans un autre service. FAS utilise les autorisations du principal appelant un service AWS, combinées au service AWS demandeur pour adresser des demandes aux services en aval. Les demandes FAS ne sont effectuées que lorsqu'un service reçoit une demande qui nécessite des interactions avec d'autres services ou ressources AWS pour être traitée. Dans ce cas, vous devez disposer d'autorisations nécessaires pour effectuer les deux actions. Pour plus de détails sur une politique lors de la formulation de demandes FAS, consultez Transfert des sessions d'accès.

Rôles de service pour AWS Security Agent

Prend en charge les rôles de service : Non

Un rôle de service est un rôle IAM qu'un service endosse pour accomplir des actions en votre nom. Un administrateur IAM peut créer, modifier et supprimer un rôle de service à partir d'IAM. Pour plus d'informations, consultez la section Créer un rôle pour déléguer des autorisations à un service AWS dans le guide de l'utilisateur IAM.

Service-linked rôles pour AWS Security Agent

Prend en charge les rôles liés à un service : oui

Un rôle lié à un service est un type de rôle de service lié à un service AWS. Le service peut assumer le rôle d'effectuer une action en votre nom. Service-linked les rôles apparaissent dans votre compte

AWS et appartiennent au service. Un administrateur IAM peut consulter, mais ne peut pas modifier, les autorisations concernant les rôles liés à un service.

Exemples de politiques basées sur l'identité d'AWS Security Agent

Par défaut, Utilisateurs IAM les rôles ne sont pas autorisés à créer ou à modifier les ressources d'AWS Security Agent. Ils ne peuvent pas non plus effectuer de tâches à l'aide de l' AWS API Console de gestion AWS AWS CLI, ou. Un IAM administrateur doit créer des IAM politiques qui accordent aux utilisateurs et aux rôles l'autorisation d'effectuer des opérations d'API spécifiques sur les ressources spécifiques dont ils ont besoin. L'administrateur doit ensuite associer ces politiques au Utilisateurs IAM ou aux groupes qui nécessitent ces autorisations.

Pour savoir comment créer une politique basée sur l'identité IAM à l'aide de ces exemples de documents de stratégie JSON, consultez la section Création de politiques à l'aide de l'éditeur JSON dans le guide de l'utilisateur IAM.

Bonnes pratiques en matière de politiques

Identity-based les politiques déterminent si quelqu'un peut créer, accéder ou supprimer des ressources AWS Security Agent dans votre compte. Ces actions peuvent entraîner des frais pour votre Compte AWS. Lorsque vous créez ou modifiez des politiques basées sur l'identité, suivez ces instructions et recommandations :

- Commencez AWS par les politiques gérées et passez aux autorisations du moindre privilège : pour commencer à accorder des autorisations à vos utilisateurs et à vos charges de travail, utilisez les politiques AWS gérées qui accordent des autorisations pour de nombreux cas d'utilisation courants. Ils sont disponibles dans votre Compte AWS. Nous vous recommandons de réduire davantage les autorisations en définissant des politiques gérées par les AWS clients spécifiques à vos cas d'utilisation. Pour plus d'informations, consultez les politiques AWS gérées ou les politiques gérées par AWS pour les fonctions professionnelles dans le guide de l'utilisateur IAM.
- Appliquer les autorisations du moindre privilège : lorsque vous définissez des autorisations à IAM l'aide de politiques, accordez uniquement les autorisations nécessaires à l'exécution d'une tâche. Pour ce faire, vous définissez les actions qui peuvent être entreprises sur des ressources spécifiques dans des conditions spécifiques, également appelées autorisations de moindre privilège. Pour plus d'informations sur l'utilisation IAM pour appliquer des autorisations, consultez la section Politiques et autorisations IAM dans le guide de l'utilisateur IAM.
- Utilisez des conditions dans IAM les politiques pour restreindre davantage l'accès : vous pouvez ajouter une condition à vos politiques pour limiter l'accès aux actions et aux ressources. Par

exemple, vous pouvez écrire une condition de politique pour spécifier que toutes les demandes doivent être envoyées via SSL. Vous pouvez également utiliser des conditions pour accorder l'accès aux actions de service si elles sont utilisées par le biais d'un service spécifique Service AWS, tel que CloudFormation. Pour plus d'informations, consultez la section Éléments de politique IAM JSON : condition dans le guide de l'utilisateur IAM.

- IAM Access Analyzer À utiliser pour valider vos IAM politiques afin de garantir des autorisations sécurisées et fonctionnelles : IAM Access Analyzer valide les politiques nouvelles et existantes afin qu'elles respectent le langage des politiques (JSON) et les IAM meilleures pratiques. IAM IAM Access Analyzer fournit plus de 100 vérifications des politiques et des recommandations exploitables pour vous aider à créer des politiques sécurisées et fonctionnelles. Pour plus d'informations, consultez la section Validation des IAM Access Analyzer politiques dans le guide de l'utilisateur IAM.
- Exiger l'authentification multifactorielle (MFA) : si vous avez un scénario qui Utilisateurs IAM nécessite ou root des utilisateurs sur votre compte, activez l'authentification MFA pour plus de sécurité. Pour exiger la MFA lorsque des opérations d'API sont appelées, ajoutez des conditions MFA à vos politiques. Pour plus d'informations, consultez la section Configuration de MFA-protected l'accès aux API dans le guide de l'utilisateur IAM.

Utilisation de la console AWS Security Agent

Pour accéder à la console AWS Security Agent, un responsable IAM doit disposer d'un ensemble minimal d'autorisations. Ces autorisations doivent permettre au principal de répertorier et de consulter les informations relatives aux ressources de l'agent de sécurité AWS présentes dans votre Compte AWS. Si vous créez une politique basée sur l'identité qui est plus restrictive que les autorisations minimales requises, la console ne fonctionnera pas comme prévu pour les principaux auxquels cette politique est associée.

Pour vous assurer que vos principaux IAM peuvent toujours utiliser la console AWS Security Agent, créez une politique avec votre propre nom unique. Attachez la politique aux principaux. Pour plus d'informations, veuillez consulter Ajout d'autorisations à un utilisateur dans le Guide de l'utilisateur IAM.

Pour plus de détails sur les politiques, voirthe section called "Politique gérée par AWS : SecurityAgentWebAppAPIPolicy".

Il n'est pas nécessaire d'accorder des autorisations de console minimales aux utilisateurs qui appellent uniquement l'API AWS CLI ou l' AWS API. Autorisez plutôt l'accès uniquement aux actions qui correspondent à l'opération API que vous essayez d'effectuer.

Résolution des problèmes liés à l'identité et à l'accès de l'agent de sécurité AWS

Utilisez les informations suivantes pour vous aider à diagnostiquer et à résoudre les problèmes courants que vous pouvez rencontrer lors de l'utilisation d'AWS Security Agent et IAM.

AccessDeniedException

Si vous recevez un message `AccessDeniedException` lors de l'appel d'une opération d'API AWS, cela signifie que les informations d'identification principales IAM que vous utilisez ne disposent pas des autorisations requises pour effectuer cet appel.

```
An error occurred (AccessDeniedException) when calling the CreateEnvironment operation:
User: arn:aws:iam::111122223333:user/user_name is not authorized to perform:
securityagent:CreateEnvironment on resource:
 arn:aws:securityagent:region:111122223333:environment/my-env
```

Dans l'exemple de message précédent, l'utilisateur n'est pas autorisé à appeler l'opération d'`CreateEnvironment`API AWS Security Agent. Pour fournir des autorisations d'administrateur AWS Security Agent à un directeur IAM, consultezthe section called “Exemples de politiques basées sur l'identité d'AWS Security Agent”.

Pour plus d'informations générales sur IAM, consultez la section Contrôler l'accès aux ressources AWS à l'aide de politiques dans le guide de l'utilisateur IAM.

Je souhaite autoriser des personnes extérieures à mon Compte AWS pour accéder à mes ressources d'agent de sécurité AWS

Vous pouvez créer un rôle que les utilisateurs provenant d’autres comptes ou les personnes extérieures à votre organisation pourront utiliser pour accéder à vos ressources. Vous pouvez spécifier qui est autorisé à assumer le rôle. Pour les services qui prennent en charge les politiques basées sur les ressources ou les listes de contrôle d’accès (ACL), vous pouvez utiliser ces politiques pour donner l’accès à vos ressources.

Pour plus d’informations, consultez les éléments suivants :

- Pour savoir si AWS Security Agent prend en charge ces fonctionnalités, consultezthe section called “Comment fonctionne l'agent de sécurité AWS avec IAM”.
- Pour savoir comment fournir l'accès à vos ressources sur un site Comptes AWS qui vous appartient, consultez la section Fournir un accès à un Utilisateur IAM autre Compte AWS que vous possédez dans le Guide de l'utilisateur d'IAM.

- Pour savoir comment fournir l'accès à vos ressources à des tiers Comptes AWS, consultez la section Fournir un accès à des ressources Comptes AWS détenues par des tiers dans le guide de l'utilisateur IAM.
- Pour savoir comment fournir un accès par le biais de la fédération d'identité, consultez Octroi d'accès à des utilisateurs authentifiés en externe (fédération d'identité) dans le Guide de l'utilisateur IAM.
- Pour connaître la différence entre l'utilisation de rôles et de politiques basées sur les ressources pour l'accès entre comptes, consultez la section En quoi les IAM rôles diffèrent des politiques basées sur les ressources dans le Guide de l'utilisateur IAM.

Intervention en cas d'incidents

AWS Security Agent est un service de test de sécurité proactif conçu pour identifier et prévenir les vulnérabilités avant qu'elles ne soient exploitées. Le service se concentre sur la validation préventive de la sécurité par le biais de révisions de conception, d'analyses de code et de tests de pénétration plutôt que sur la détection ou la réponse réactive aux incidents.

Détection des incidents

AWS Security Agent ne fournit pas de fonctionnalités de détection d'incidents. Le service fonctionne comme un outil de test de sécurité proactif qui valide les applications pour détecter les vulnérabilités pendant le développement et avant le déploiement. Pour la surveillance de la sécurité de l'exécution et la détection des incidents, utilisez des services tels qu'Amazon GuardDuty, AWS Security Hub ou Amazon CloudWatch.

Alerte en cas d'incident

AWS Security Agent ne génère pas d'alertes en temps réel pour les incidents de sécurité. Le service fournit des résultats de sécurité via la console AWS après avoir effectué des révisions de conception, des analyses de code ou des missions de tests d'intrusion. Ces résultats représentent des vulnérabilités potentielles découvertes lors des tests plutôt que des incidents de sécurité actifs.

Remédiation des incidents

AWS Security Agent ne fournit pas de solution automatique aux incidents. Le service identifie les failles de sécurité et fournit des conseils pour y remédier, notamment :

- Descriptions détaillées des vulnérabilités identifiées

- Chemins d'exploitation reproductibles pour des résultats validés
- Corrections de code spécifiques et conseils de mise en œuvre
- Analyse d'impact des problèmes découverts

Les équipes de développement et de sécurité utilisent ces instructions pour corriger manuellement les vulnérabilités avant qu'elles n'atteignent les environnements de production.

Soutenir les activités de réponse aux incidents

Bien qu'AWS Security Agent ne soit pas conçu pour répondre aux incidents, les équipes de sécurité peuvent utiliser le service pour prendre en charge les activités post-incident :

Validation des vulnérabilités

: Après un incident de sécurité, utilisez AWS Security Agent pour vérifier si des vulnérabilités similaires existent dans d'autres applications ou environnements.

Évaluation de la posture de sécurité

: Réalisez des tests de pénétration pour valider les améliorations de sécurité mises en œuvre dans le cadre de la résolution des incidents.

Analyse des causes profondes

: Utilisez les fonctionnalités de vérification de la sécurité du code pour identifier les vulnérabilités similaires susceptibles d'exister dans d'autres bases de code.

Validation de conformité pour AWS Security Agent

Pour savoir si un service AWS s'inscrit dans le champ d'application de programmes de conformité spécifiques, consultez la section Services AWS dans Champ d'application par programme de conformité et choisissez le programme de conformité qui vous intéresse. Pour obtenir des informations générales, consultez la page Programmes de conformité AWS.

Vous pouvez télécharger les rapports de l'audit externe avec Artefact AWS. Pour plus d'informations, consultez Téléchargement des rapports dans AWS Artifact.

Lorsque vous utilisez les services AWS, votre responsabilité en matière de conformité dépend de la sensibilité de vos données, des objectifs de conformité de votre entreprise et des lois et réglementations applicables. AWS fournit les ressources suivantes pour faciliter la conformité :

- Conformité et gouvernance de la sécurité : ces guides de mise en œuvre de solutions traitent des considérations architecturales et fournissent les étapes à suivre afin de déployer des fonctionnalités de sécurité et de conformité.
- Référence des services éligibles HIPAA : liste les services éligibles HIPAA. Tous les services AWS ne sont pas éligibles à la loi HIPAA.
- Ressources AWS portant sur la conformité : cet ensemble de manuels et de guides peut renfermer des informations concernant votre secteur et votre région.
- Guides de conformité destinés aux clients AWS : découvrez le modèle de responsabilité partagée sous l'angle de la conformité. Les guides résument les meilleures pratiques en matière de sécurisation des services AWS et décrivent les directives relatives aux contrôles de sécurité dans de nombreux cadres (notamment le National Institute of Standards and Technology (NIST), le Payment Card Industry Security Standards Council (PCI) et l'Organisation internationale de normalisation (ISO)).
- Évaluation des ressources à l'aide de règles dans le Manuel du développeur AWS Config : le service évalue dans quelle mesure vos configurations de ressources sont conformes aux pratiques internes, aux directives sectorielles et aux réglementations.
- AWS Security Hub : ce service AWS fournit une vue complète de votre état de sécurité au sein d'AWS. Security Hub utilise des contrôles de sécurité pour évaluer vos ressources AWS et vérifier votre conformité aux normes et aux meilleures pratiques du secteur de la sécurité. Pour obtenir la liste des services et des contrôles pris en charge, consultez Référence des contrôles Security Hub.
- Amazon GuardDuty — Ce service AWS détecte les menaces potentielles qui pèsent sur vos comptes, charges de travail, conteneurs et données AWS en surveillant votre environnement pour détecter toute activité suspecte ou malveillante. GuardDuty peut vous aider à répondre à diverses exigences de conformité, telles que la norme PCI DSS, en répondant aux exigences de détection des intrusions imposées par certains cadres de conformité.
- AWS Audit Manager : ce service AWS vous aide à auditer en permanence votre utilisation d'AWS afin de simplifier la gestion des risques et la conformité aux réglementations et aux normes du secteur.

Résilience dans AWS Security Agent

> **Note**
>
> AWS Security Agent est disponible dans les régions suivantes : USA Est (Virginie du Nord)`us-east-1`, USA Ouest (Oregon)`us-west-2`, Asie-Pacifique (Mumbai) —`ap-`

south-1, Asie-Pacifique (Singapour) ap-southeast-1 —, Asie-Pacifique (Sydney) ap-southeast-2 —, Asie-Pacifique (Tokyo) —, Europe (Francfort) ap-northeast-1 —, Europe (Irlande) eu-central-1 eu-west-1 — et Amérique du Sud (São Paulo) —. sa-east-1 Il utilise l'inférence entre régions. En Asie-Pacifique (Mumbai), en Asie-Pacifique (Singapour) et en Amérique du Sud (São Paulo), AWS Security Agent utilise l'inférence interrégionale globale, qui achemine les demandes d'inférence vers n'importe quelle région commerciale AWS. Dans toutes les autres régions, il utilise l'inférence géographique interrégionale, qui permet de maintenir le traitement des données dans des limites géographiques spécifiques. AWS Security Agent est un outil utilisé lors du développement de votre application et ne doit pas être déployé en tant qu'infrastructure critique ou destinée aux clients.

L'infrastructure mondiale d'AWS repose sur les régions AWS et les zones de disponibilité. Les régions AWS fournissent plusieurs zones de disponibilité physiquement séparées et isolées, reliées par un réseau à latence faible, à débit élevé et à forte redondance. Avec les zones de disponibilité, vous pouvez concevoir et exploiter des applications et des bases de données qui basculent automatiquement d'une zone à l'autre sans interruption. Les zones de disponibilité sont davantage disponibles, tolérantes aux pannes et ont une plus grande capacité de mise à l'échelle que les infrastructures traditionnelles à un ou plusieurs centres de données.

Pour de plus amples informations sur les régions et les zones de disponibilité AWS, veuillez consulter Infrastructure mondiale AWS.

Sécurité de l'infrastructure dans AWS Security Agent

En tant que service géré, AWS Security Agent est protégé par la sécurité du réseau mondial AWS. Pour plus d'informations sur les services de sécurité AWS et sur la manière dont AWS protège l'infrastructure, consultez AWS Cloud Security. Pour concevoir votre environnement AWS en utilisant les meilleures pratiques en matière de sécurité de l'infrastructure, consultez la section Sécurité dans le Well-Architected cadre AWS.

Isolement de réseau

AWS Security Agent est un service entièrement géré accessible via la console AWS et l'application Web AWS Security Agent. L'accès au service est contrôlé via AWS Identity and Access Management (IAM) ou AWS IAM Identity Center, qui peuvent s'intégrer à votre fournisseur d'identité.

AWS Security Agent prend en charge les points de terminaison VPC d'interface optimisés par AWS PrivateLink, ce qui vous permet d'accéder de manière privée aux API de service depuis votre VPC sans passer par l'Internet public. Pour de plus amples informations, veuillez consulter the section called "Points de terminaison de VPC d'Interface".

AWS Security Agent nécessite un accès à Internet pour effectuer des tests de pénétration sur les applications cibles et pour les opérations du plan de contrôle. Le service utilise l' AWS-managed infrastructure à des fins de test et ne fournit pas d'instances EC2 ni d'autres ressources de calcul dans votre compte. Si vous configurez l'accès VPC pour les tests d'intrusion, Security Agent crée une ENI dans votre sous-réseau, mais cette ENI ne possède pas d'adresse IP publique. Pour de plus amples informations, veuillez consulter the section called "Connect l'agent aux ressources VPC privées".

Multi-tenancy et isolation des ressources

AWS Security Agent est un service mutualisé. Les évaluations de sécurité, les résultats et les données clients sont isolés des comptes AWS individuels et chiffrés au repos. AWS applique des contrôles d'isolation de l'infrastructure standard pour garantir que les activités de test de sécurité d'un client n'ont pas d'impact sur les performances ou la confidentialité d'un autre client.

AWS Agent de sécurité et points de terminaison VPC d'interface (AWS PrivateLink)

Vous pouvez l'utiliser AWS PrivateLink pour créer une connexion privée entre votre VPC et l'agent AWS de sécurité. Vous pouvez accéder à Security Agent comme s'il se trouvait dans votre VPC, sans passer par une passerelle Internet, un périphérique NAT, une connexion VPN ou une connexion Direct Connect. Les instances de votre VPC n'ont pas besoin d'adresses IP publiques pour accéder à Security Agent.

Vous établissez cette connexion privée en créant un point de terminaison d'interface optimisé par AWS PrivateLink. Nous créons une interface réseau de point de terminaison dans chaque sous-réseau que vous activez pour le point de terminaison d'interface. Il s'agit d'interfaces réseau gérées par les demandeurs qui servent de point d'entrée pour le trafic destiné à Security Agent.

Pour plus d'informations, consultez la section Accès aux AWS services AWS PrivateLink dans le AWS PrivateLink Guide.

Considérations relatives à l'agent de sécurité

Avant de configurer un point de terminaison d'interface pour Security Agent, consultez les considérations du AWS PrivateLink guide.

Security Agent prend en charge les appels vers toutes ses actions d'API depuis votre VPC, y compris les opérations de gestion des espaces des agents, les tests de pénétration et les résultats de sécurité.

Vous pouvez sélectionner IPv4, IPv6 ou Dualstack lors de la création d'un point de terminaison.

Les politiques de point de terminaison VPC sont prises en charge pour Security Agent. Par défaut, l'accès complet à Security Agent est autorisé via le point de terminaison de l'interface. Vous pouvez contrôler l'accès en attachant une politique de point de terminaison au point de terminaison de l'interface ou en associant un groupe de sécurité aux interfaces réseau du point de terminaison.

Tous les appels d'API à Security Agent sont chiffrés à l'aide du protocole TLS 1.2 ou supérieur, y compris les appels effectués via des points de terminaison VPC. Pour plus d'informations sur la protection des données, consultez the section called "Protection des données". Les appels d'API de Security Agent sont enregistrés AWS CloudTrail. Pour de plus amples informations, veuillez consulter the section called "Exemple : entrées du fichier journal de l'agent de AWS sécurité".

Création d'un point de terminaison d'interface pour Security Agent

Vous pouvez créer un point de terminaison d'interface pour Security Agent à l'aide de la console Amazon VPC ou de l'interface de ligne de AWS commande (AWS CLI). Pour plus d'informations, consultez la section Création d'un point de terminaison d'interface dans le AWS PrivateLink Guide.

Créez un point de terminaison d'interface pour Security Agent en utilisant le nom de service suivant :

```
com.amazonaws.<region>.securityagent
```

Pour créer le point de terminaison de l'interface à l'aide de la AWS CLI, exécutez la commande suivante. Remplacez la région, l'ID VPC, les ID de sous-réseau et l'ID de groupe de sécurité par vos propres valeurs.

```
aws ec2 create-vpc-endpoint \
    --vpc-id vpc-1a2b3c4d \
    --vpc-endpoint-type Interface \
    --service-name com.amazonaws.<region>.securityagent \
```

```
    --subnet-ids subnet-1a2b3c4d subnet-5e6f7a8b \
    --security-group-ids sg-1a2b3c4d \
    --private-dns-enabled
```

> **Important**
>
> Le DNS privé doit être activé pour le point de terminaison de l'interface. Security Agent vous oblige à utiliser le nom DNS régional par défaut (par exemple,`securityagent.us-east-1.api.aws`) pour effectuer des demandes d'API via le point de terminaison. L'appel direct de l'URL VPCE spécifique au point de terminaison n'est pas pris en charge.

Pour utiliser un DNS privé, vous devez définir à la fois les `enableDnsHostnames` attributs `enableDnsSupport` et sur `true` pour votre VPC. Pour plus d'informations, consultez DNS attributes for your VPC (Attributs DNS pour votre VPC) dans le Guide de l'utilisateur d'Amazon VPC.

Configuration des groupes de sécurité pour le point de terminaison de l'interface

Lorsque vous créez un point de terminaison d'interface, vous pouvez associer des groupes de sécurité aux interfaces réseau du point de terminaison afin de contrôler le trafic vers Security Agent. Créez un groupe de sécurité qui autorise le trafic HTTPS entrant (port 443) depuis les ressources de votre VPC qui doivent communiquer avec Security Agent.

Le groupe de sécurité doit inclure la règle entrante suivante :

- Type : HTTPS
- Protocole : TCP
- Portée du port : 443
- Source : votre bloc d'adresse CIDR VPC (par exemple,`10.0.0.0/16`) ou les identifiants de groupe de sécurité des ressources qui ont besoin d'accéder à Security Agent

Pour plus d'informations, consultez la section Groupes de sécurité dans le AWS PrivateLink Guide.

Création d'une politique de point de terminaison pour votre point de terminaison d'interface

Une politique de point de terminaison est une ressource IAM que vous pouvez attacher à votre point de terminaison d'interface. La politique de point de terminaison par défaut autorise un accès complet

à Security Agent via le point de terminaison de l'interface. Pour contrôler l'accès autorisé à Security Agent depuis votre VPC, associez une politique de point de terminaison personnalisée au point de terminaison de l'interface.

Une politique de point de terminaison spécifie les informations suivantes :

- Principaux habilités à effectuer des actions (AWS comptes, utilisateurs IAM et rôles IAM).
- Les actions qui peuvent être effectuées.
- La ressource sur laquelle les actions peuvent être effectuées.

Pour plus d'informations, consultez la section Contrôler l'accès aux services à l'aide des politiques relatives aux terminaux dans le AWS PrivateLink Guide.

Exemple : politique de point de terminaison VPC pour les actions de l'agent AWS de sécurité

Voici un exemple de politique de point de terminaison pour AWS Security Agent. Lorsqu'elle est attachée à un point de terminaison, cette politique accorde l'accès aux actions de l'agent AWS de sécurité répertoriées à tous les principaux sur toutes les ressources.

```
{
   "Statement": [
      {
         "Effect": "Allow",
         "Principal": "*",
         "Action": [
            "securityagent:CreatePentest",
            "securityagent:ListPentests",
            "securityagent:BatchGetPentests",
            "securityagent:StartPentestExecution",
            "securityagent:StopPentestExecution",
            "securityagent:ListFindings",
            "securityagent:BatchGetFindings"
         ],
         "Resource": "*"
      }
   ]
}
```

Exemple : politique de point de terminaison VPC qui refuse tout accès depuis un compte spécifié AWS

La politique de point de terminaison VPC suivante refuse au AWS compte `123456789012` tout accès aux ressources utilisant le point de terminaison. La politique autorise toutes les actions provenant d'autres comptes.

```
{
   "Statement": [
      {
         "Effect": "Allow",
         "Principal": "*",
         "Action": "securityagent:*",
         "Resource": "*"
      },
      {
         "Effect": "Deny",
         "Principal": {
            "AWS": "123456789012"
         },
         "Action": "securityagent:*",
         "Resource": "*"
      }
   ]
}
```

Résolution des problèmes

La connexion expire lors de l'appel de l'API Security Agent

- Vérifiez que l'état du point de terminaison VPC est le suivant : `available`

```
aws ec2 describe-vpc-endpoints --vpc-endpoint-ids vpce-1a2b3c4d \
    --query "VpcEndpoints[].State"
```

- Vérifiez que le groupe de sécurité associé au point de terminaison autorise le trafic TCP entrant sur le port 443 depuis votre CIDR VPC ou votre groupe de sécurité source.
- Vérifiez que les tables de routage de votre VPC n'acheminent pas le trafic de l'agent de sécurité vers une passerelle Internet ou une passerelle NAT au lieu du point de terminaison.

La résolution DNS échoue pour **`securityagent.<region>.api.aws`**

- Vérifiez que le DNS privé est activé sur le terminal :

```
aws ec2 describe-vpc-endpoints --vpc-endpoint-ids vpce-1a2b3c4d \
    --query "VpcEndpoints[].PrivateDnsEnabled"
```

- Vérifiez que `enableDnsSupport` les deux `enableDnsHostnames` sont définis `true` sur votre VPC :

```
aws ec2 describe-vpc-attribute --vpc-id vpc-1a2b3c4d --attribute enableDnsSupport
aws ec2 describe-vpc-attribute --vpc-id vpc-1a2b3c4d --attribute enableDnsHostnames
```

`Access denied`erreurs lors de l'appel des API de Security Agent

- Vérifiez la politique de point de terminaison du VPC pour vous assurer qu'elle autorise les actions que vous essayez d'effectuer.
- Vérifiez que votre politique d'identité IAM accorde les `securityagent:` autorisations requises.
- Si vous utilisez une politique de point de terminaison personnalisée, vérifiez que la politique de point de terminaison et la politique IAM autorisent la demande.

Analyse de configuration et de vulnérabilité dans AWS Security Agent

La configuration et les contrôles informatiques sont une responsabilité partagée entre AWS et vous, notre client. Pour de plus amples informations, veuillez consulter AWS Modèle de responsabilité partagée.

Cross-service prévention confuse des adjoints

Le problème de député confus est un problème de sécurité dans lequel une entité qui n'est pas autorisée à effectuer une action peut contraindre une entité plus privilégiée à le faire. Dans AWS, l'usurpation d'identité entre services peut entraîner un problème de confusion chez les adjoints. Cross-service l'usurpation d'identité peut se produire lorsqu'un service (le service appelant) appelle un autre service (le service appelé). Le service appelant peut être manipulé et ses autorisations utilisées pour agir sur les ressources d'un autre client auxquelles on ne serait pas autorisé d'accéder autrement. Pour éviter cela, AWS fournit des outils qui vous aident à protéger vos données pour tous les services, les principaux fournisseurs de services ayant obtenu l'accès aux ressources de votre compte. Pour plus d'informations, consultez la section Cross-service Confused Deputy Prevention dans le guide de l'utilisateur d'AWS Identity and Access Management.

Bonnes pratiques de sécurité pour AWS Security Agent

AWS Security Agent fournit un certain nombre de fonctionnalités de sécurité à prendre en compte lors de l'élaboration et de la mise en œuvre de vos propres politiques de sécurité. Les bonnes pratiques suivantes doivent être considérées comme des instructions générales et ne représentent pas une solution de sécurité complète. Étant donné que ces bonnes pratiques peuvent ne pas être appropriées ou suffisantes pour votre environnement, considérez-les comme des remarques utiles plutôt que comme des recommandations.

Utiliser des environnements hors production pour les tests de pénétration

AWS Security Agent utilise une suite complète d'outils de test d'intrusion issus de la distribution Kali Linux. Ces outils sont conçus pour identifier les failles de sécurité et peuvent effectuer des actions qui modifient l'état des applications, les données ou les configurations du système.

Bonne pratique : effectuez des tests de pénétration dans des environnements hors production qui reflètent votre configuration de production. Ces environnements de test doivent :

- Ne pas contenir de données clients en temps réel ni d'informations de production sensibles
- Être isolé des systèmes de production
- Disposer de configurations et de contrôles de sécurité similaires à ceux de la production
- Ne pas utiliser les informations d'identification pour accéder aux systèmes de production

Les tests dans des environnements de production peuvent entraîner :

- Modification ou suppression de données
- Interruptions de service ou dégradation des performances
- Changements d'état involontaires
- Déclenchement d'alertes de sécurité ou de procédures de réponse aux incidents

Valider les résultats AI-generated de sécurité

AWS Security Agent effectue une analyse de sécurité à l'aide d'agents d'intelligence artificielle. En raison de la nature non déterministe des systèmes d'IA, les tests d'intrusion peuvent produire des résultats différents selon les exécutions.

Bonne pratique : validez les résultats de sécurité avant de prendre des mesures correctives :

- Passez en revue les scripts de vérification générés par l'agent de sécurité AWS pour chaque résultat
- Exécutez des scripts de vérification dans votre environnement de test pour confirmer la vulnérabilité
- Envisagez d'effectuer plusieurs tests de pénétration pour garantir une couverture complète
- Faites preuve de jugement professionnel en matière de sécurité pour évaluer la gravité et l'exploitabilité des résultats

Les problèmes identifiés ne représentent peut-être pas tous des vulnérabilités exploitables dans votre contexte de déploiement spécifique.

Vérifiez et testez le code de correction généré

AWS Security Agent peut générer des correctifs de code et des améliorations de sécurité pour les vulnérabilités identifiées. Ces AI-generated correctifs nécessitent une vérification avant le déploiement.

Bonne pratique : passez en revue toutes les modifications de code générées :

- Examiner l'exhaustivité et l'exactitude des correctifs proposés
- Testez les correctifs de manière approfondie dans des environnements hors production
- Vérifiez que les correctifs n'introduisent pas de nouvelles vulnérabilités ou n'interrompent pas les fonctionnalités
- Utilisez AWS Security Agent pour effectuer un nouveau test après avoir appliqué les correctifs, ou exécutez les scripts de vérification fournis
- Suivez les processus de révision et d'approbation du code de votre organisation

Accès au référentiel de code

AWS Security Agent peut fournir des conseils de sécurité sur les modifications de code par le biais de commentaires sur les pull requests et de l'intégration de la révision du code. Pour protéger les informations de sécurité sensibles, cette fonctionnalité fonctionne sous des contraintes spécifiques.

Limitation : les directives de sécurité du code sont limitées aux référentiels privés uniquement. Cela garantit que :

- Les résultats de sécurité restent confidentiels pour votre organisation

- Les vulnérabilités potentielles ne sont pas divulguées publiquement avant la correction
- Les recommandations de correction générées n'exposent pas les détails de l'exploitation

AWS Security Agent ne fournit pas de directives de sécurité du code pour les référentiels publics. Il ne commentera pas les référentiels publics ou les projets open source dans lesquels les résultats de sécurité seraient visibles publiquement.

Les tests de pénétration d'AWS Security Agent permettent d'examiner et de corriger les référentiels privés et publics que vous avez configurés pour le pentest. Si le référentiel est public, le code de correction sera fourni sous forme de fichier diff téléchargeable au lieu d'une pull request.

URL accessibles

Les URL accessibles spécifient des points de terminaison supplémentaires auxquels l'environnement de test d'intrusion peut accéder pendant les tests. Ils sont nécessaires lorsque votre application dépend de services externes tels que des fournisseurs d'authentification tiers ou des CDN. Toutes les dépendances réseau requises pour les tests doivent être spécifiées sous forme d'URL cibles ou d'URL accessibles. Le réseau bloque l'accès à tous les points de terminaison non spécifiés.

Implications en matière de sécurité : l'agent de sécurité AWS n'est pas chargé d'effectuer des tests de sécurité sur les URL accessibles. En spécifiant des URL accessibles, vous attestez de la confiance dans ces dépendances. Les données des tests d'intrusion, y compris les informations d'identification, peuvent être transmises à ces points de terminaison URL accessibles pendant les tests.

Inférence interrégionale

AWS Security Agent sélectionne automatiquement la région optimale pour traiter vos demandes d'inférence. Cela permet d'optimiser les ressources informatiques disponibles, la disponibilité des modèles et d'offrir la meilleure expérience client. Vos données restent stockées uniquement dans la région d'où provient la demande ; toutefois, les demandes de saisie et les résultats de sortie peuvent être traités en dehors de cette région. Nous transmettons toutes les données cryptées sur le réseau AWS.

AWS Security Agent utilise deux types d'inférence entre régions en fonction de la région :

- Inférence géographique entre régions — Maintient le traitement des données à l'intérieur de limites géographiques spécifiques (telles que les États-Unis, l'UE, l'Australie ou le Japon) pour la plupart des fonctionnalités. Pour la correction du code, les demandes provenant de l'Australie et du Japon

sont traitées dans l'Union européenne. Utilisé dans l'est des États-Unis (Virginie du Nord)`us-east-1`, l'ouest des États-Unis (Oregon)`us-west-2`, l'Asie-Pacifique (Sydney)`ap-southeast-2`, l'Asie-Pacifique (Tokyo)`ap-northeast-1`, l'Europe (Francfort) et l'Europe (Irlande) `eu-west-1` —. `eu-central-1`

- Inférence interrégionale globale : achemine les demandes d'inférence vers n'importe quelle région AWS commerciale, optimisant les ressources disponibles et augmentant le débit des modèles. Utilisé en Asie-Pacifique (Mumbai) —`ap-south-1`, Asie-Pacifique (Singapour) `ap-southeast-1` — et en Amérique du Sud (São Paulo) `sa-east-1` —.

Pour les régions utilisant l'inférence interrégionale globale, les invites de saisie et les résultats de sortie peuvent être traités dans n'importe quelle région AWS commerciale. Toutes les données transmises lors d'opérations interrégionales restent sur le réseau AWS et ne transitent pas par l'Internet public. Nous chiffrons les données en transit entre les régions AWS.

Le tableau suivant décrit l'endroit où vos demandes d'inférence sont traitées en fonction de la région d'origine de la demande et de la fonctionnalité utilisée.

Origine de la demande	Toutes les fonctionnalités sauf la correction du code	Correction du code
États-Unis — USA Est (Virginie du Nord) `us-east-1` —, USA Ouest (Oregon) — `us-west-2`	États-Unis	États-Unis
Union européenne — Europe (Irlande) `eu-west-1` —, Europe (Francfort) — `eu-central-1`	Union européenne	Union européenne
Australie — Asie-Pacifique (Sydney) — `ap-southeast-2`	Australie	Union européenne
Japon — Asie-Pacifique (Tokyo) — `ap-northeast-1`	Japon	Union européenne

Origine de la demande	Toutes les fonctionnalités sauf la correction du code	Correction du code
Amérique du Sud — Amérique du Sud (São Paulo) — `sa-east-1`	Toute région AWS commercia le	Toute région AWS commercia le
Inde — Asie-Pacifique (Mumbai) — `ap-south-1`	Toute région AWS commercia le	Toute région AWS commercia le
Asie du Sud-Est — Asie-Paci fique (Singapour) — `ap-southeast-1`	Toute région AWS commercia le	Toute région AWS commercia le

Cross-Region l'inférence est toujours activée et ne peut pas être désactivée. Cross-Region l'inférence n'est pas affectée par les politiques clients contenues dans les politiques de contrôle des services (SCP) ou dans AWS Control Tower qui limitent le contenu client à des régions spécifiques. Pour plus d'informations sur la façon dont AWS Security Agent protège vos données lors du traitement interrégional, consultez la section Traitement Cross-Region des données.

Migration des actions et des ressources IAM

AWS Security Agent est un agent novateur qui sécurise de manière proactive vos applications tout au long du cycle de développement dans tous vos environnements. Si vous avez intégré AWS Security Agent avant le 9 février 2026, vous serez concerné par les modifications à venir apportées le 9 mars 2026 à vos ressources d'instance d'agent existantes et aux actions IAM d'AWS Security Agent. En vue de la publication du API/SDK support public, la ressource Agent Instance est renommée Agent Space, et des actions IAM spécifiques sont renommées. Ces modifications affecteront tous les rôles IAM d'application ou d'instance d'agent que vous avez créés avant le 9 mars 2026. Afin d'éviter de rencontrer des problèmes d'authentification après le 9 mars 2026, vous devrez suivre les étapes décrites dans la section Préparation à la migration.

> **Note**
>
> Si vous créez de nouvelles instances d'agent après le 9 février 2026, la nouvelle instance d'agent sera créée en tant qu'espace d'agent et aucune étape de migration ne sera requise.

Changements planifiés

AWS Security Agent renomme la ressource Agent Instance en Agent Space : `arn:aws:securityagent:us-east-1:{{accountId}}:agent-instance/*` renommée en`arn:aws:securityagent:us-east-1:{{accountId}}:agent-space/*`. En outre, les actions IAM suivantes sont renommées :

- `securityagent:ListAgentInstances`renommé en `securityagent:ListAgentSpaces`
- `securityagent:ListControls`renommé en `securityagent:ListSecurityRequirements`
- `securityagent:BatchGetAgentInstances`renommé en `securityagent:BatchGetAgentSpaces`
- `securityagent:BatchGetSecurityTestContentMetadata`renommé en `securityagent:BatchGetPentestJobContentMetadata`
- `securityagent:BatchGetTasks`renommé en `securityagent:BatchGetPentestJobTasks`
- `securityagent:CreateDocumentReview`renommé en `securityagent:CreateDesignReview`
- `securityagent:GetDocumentReview`renommé en `securityagent:GetDesignReview`
- `securityagent:GetDocumentReviewArtifact`renommé en `securityagent:GetDesignReviewArtifact`
- `securityagent:ListDocumentReviews`renommé en `securityagent:ListDesignReviews`
- `securityagent:ListDocumentReviewComments`renommé en `securityagent:ListDesignReviewComments`
- `securityagent:ListTasks`renommé en `securityagent:ListPentestJobTasks`
- `securityagent:StartPentestExecution`renommé en `securityagent:StartPentestJob`
- `securityagent:StopPentestExecution`renommé en `securityagent:StopPentestJob`
- `securityagent:DeleteDocumentReview`renommé en `securityagent:DeleteDesignReview`

Préparation à la migration

Afin d'éviter de rencontrer des problèmes après le 9 mars 2026 tout en continuant à utiliser AWS Security Agent avant le 9 mars 2026, vous devrez faire confiance aux nouvelles et anciennes ressources et aux actions IAM de votre IAM roles/policies jusqu'au 9 mars 2026. Les instructions ci-dessous fournissent un guide pour la migration vers les nouveaux formats de ressources et d'actions :

1. Connectez-vous à votre compte AWS et accédez à la console AWS Security Agent
2. Dans le panneau de gauche, sélectionnez Paramètres et choisissez le rôle sous Rôle de service
3. Dans la console IAM pour le rôle associé, sélectionnez Ajouter des autorisations et Joindre des politiques
4. Sélectionnez AWSSecurityAgentWebAppPolicyet choisissez Ajouter des autorisations
   a. Remarque importante : vérifiez que vous avez sélectionné AWSSecurityAgentWebAppPolicycomme nouvelle politique et non SecurityAgentWebAppAPIPolicy
5. Vérifiez que votre rôle IAM possède désormais les deux AWSSecurityAgentWebAppPolicyet qu'il est SecurityAgentWebAppAPIPolicysoumis à des politiques d'autorisation
6. Dans la même console de rôle IAM, sélectionnez Relations de confiance, puis Modifier la politique de confiance
7. Mettez à jour votre politique de confiance au format suivant, en remplaçant {{accountId}} par votre identifiant de compte AWS

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "securityagent.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "{{accountId}}"
        },
        "ArnLike": {
```

```
          "aws:SourceArn": [
            "arn:aws:securityagent:us-east-1:{{accountId}}:application/*",
            "arn:aws:securityagent:us-east-1:{{accountId}}:agent-space/*",
            "arn:aws:securityagent:us-east-1:{{accountId}}:agent-instance/*"
          ]
        }
      }
    },
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "securityagent.amazonaws.com"
      },
      "Action": "sts:SetContext",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "{{accountId}}"
        },
        "ForAllValues:ArnEquals": {
          "sts:RequestContextProviders": "arn:aws:iam::aws:contextProvider/
IdentityCenter"
        },
        "ArnLike": {
          "aws:SourceArn": [
            "arn:aws:securityagent:us-east-1:{{accountId}}:application/*",
            "arn:aws:securityagent:us-east-1:{{accountId}}:agent-space/*",
            "arn:aws:securityagent:us-east-1:{{accountId}}:agent-instance/*"
          ]
        }
      }
    }
  ]
}
```

8. Retournez à la console AWS Security Agent. Dans le panneau de gauche, sélectionnez Agent Spaces
9. Pour chaque espace d'agent dont vous disposez sur lequel les tests d'intrusion sont activés, effectuez les étapes suivantes
   a. Accédez à l'espace des agents et sélectionnez Test de pénétration
   b. Sous Accès au service, choisissez le rôle sous Nom du rôle du service

c. Dans la console IAM pour le rôle associé, sélectionnez Relations de confiance, puis Modifier la politique de confiance

d. Mettez à jour votre politique de confiance au format suivant, en remplaçant {{accountId}} par votre identifiant de compte AWS

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "securityagent.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "{{accountId}}"
        },
        "ArnLike": {
          "aws:SourceArn": [
            "arn:aws:securityagent:us-east-1:{{accountId}}:agent-space/*",
            "arn:aws:securityagent:us-east-1:{{accountId}}:agent-instance/*"
          ]
        }
      }
    }
  ]
}
```

Logging AWS Appels d'API Security Agent avec AWS CloudTrail

AWS Security Agent est intégré à AWS CloudTrail un service qui fournit un enregistrement des actions entreprises par un utilisateur, un rôle ou un AWS service dans AWS Security Agent. CloudTrail capture tous les appels d'API pour AWS Security Agent sous forme d'événements. Les appels capturés incluent des appels provenant de la console AWS Security Agent et des appels de code vers les opérations de l'API AWS Security Agent. Si vous créez un suivi, vous pouvez activer la diffusion continue d' CloudTrail événements vers un compartiment Amazon S3, y compris des événements pour AWS Security Agent. Si vous ne configurez pas de suivi, vous pouvez toujours consulter les événements les plus récents dans la CloudTrail console dans Historique des

événements. À l'aide des informations collectées par CloudTrail, vous pouvez déterminer la demande qui a été faite à AWS Security Agent, l'adresse IP à partir de laquelle la demande a été faite, l'auteur de la demande, la date à laquelle elle a été faite et des informations supplémentaires.

Pour en savoir plus CloudTrail, consultez le guide de AWS CloudTrail l'utilisateur.

AWS Informations relatives à l'agent de sécurité dans CloudTrail

CloudTrail est activé sur votre AWS compte lorsque vous le créez. Lorsqu'une activité se produit dans AWS Security Agent, cette activité est enregistrée dans un CloudTrail événement avec d'autres événements de AWS service dans l'historique des événements. Vous pouvez consulter, rechercher et télécharger les événements récents dans votre AWS compte. Pour plus d'informations, consultez la section Affichage des événements à l'aide de l'historique des CloudTrail événements.

Pour un enregistrement continu des événements de votre AWS compte, y compris des événements liés à AWS Security Agent, créez une trace. Un suivi permet CloudTrail de fournir des fichiers journaux à un compartiment Amazon S3. Par défaut, lorsque vous créez un parcours dans la console, celui-ci s'applique à toutes les AWS régions. Le journal enregistre les événements de toutes les régions de la AWS partition et transmet les fichiers journaux au compartiment Amazon S3 que vous spécifiez. En outre, vous pouvez configurer d'autres AWS services pour analyser plus en détail les données d'événements collectées dans les CloudTrail journaux et agir en conséquence. Pour plus d'informations, consultez les ressources suivantes :

- Présentation de la création d'un journal de suivi
- CloudTrail services et intégrations pris en charge
- Configuration des notifications Amazon SNS pour CloudTrail
- Réception de fichiers CloudTrail journaux de plusieurs régions et réception de fichiers CloudTrail journaux de plusieurs comptes

Toutes les actions AWS de l'agent de sécurité sont enregistrées par CloudTrail. Par exemple, les appels aux `CreatePentestBatchGetPentestJobs`, et `ListFindings` les actions génèrent des entrées dans les fichiers CloudTrail journaux.

Chaque événement ou entrée de journal contient des informations sur la personne ayant initié la demande. Les informations relatives à l'identité permettent de déterminer les éléments suivants :

- Si la demande a été faite avec les informations d'identification root ou AWS celles de l'utilisateur Identity and Access Management (IAM).

- Si la demande a été effectuée avec les informations d'identification de sécurité temporaires d'un rôle ou d'un utilisateur fédéré.
- Si la demande a été faite par un autre AWS service.

Pour de plus amples informations, veuillez consulter l'élément userIdentity CloudTrail .

Exemple : AWS Entrées du fichier journal de l'agent de sécurité

Compréhension AWS Entrées du fichier journal de l'agent de sécurité

Un suivi est une configuration qui permet de transmettre des événements sous forme de fichiers journaux à un compartiment Amazon S3 que vous spécifiez. CloudTrail les fichiers journaux contiennent une ou plusieurs entrées de journal. Un événement représente une demande unique provenant de n'importe quelle source et inclut des informations sur l'action demandée, la date et l'heure de l'action, les paramètres de la demande, etc. CloudTrail les fichiers journaux ne constituent pas une trace ordonnée des appels d'API publics, ils n'apparaissent donc pas dans un ordre spécifique.

L'exemple suivant montre une entrée de CloudTrail journal qui illustre l'`CreatePentest`action :

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:iam::123456789012:user/Alice",
        "accountId": "123456789012",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "Alice"
    },
    "eventTime": "2025-01-15T10:30:00Z",
    "eventSource": "securityagent.amazonaws.com",
    "eventName": "CreatePentest",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "203.0.113.12",
    "userAgent": "aws-cli/2.13.0",
    "requestParameters": {
        "pentestName": "WebApp-Security-Test",
        "targetUrl": "https://example.com",
        "testScope": "OWASP-Top-10"
    },
```

```
    "responseElements": {
        "pentestId": "pt-1234567890abcdef0",
        "pentestArn": "arn:aws:securityagent:us-east-1:123456789012:pentest/
pt-1234567890abcdef0"
    },
    "requestID": "a1b2c3d4-e5f6-7890-abcd-ef1234567890",
    "eventID": "12345678-1234-1234-1234-123456789012",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "123456789012",
    "eventCategory": "Management"
}
```

Service Quotas

AWS Security Agent dispose de quotas qui limitent le nombre de ressources que vous pouvez créer et le rythme auquel vous pouvez effectuer des opérations. Les quotas marqués comme ajustables peuvent être augmentés en soumettant une demande via AWS Support. Pour de plus amples informations, veuillez consulter Création de cas de support et de gestion de cas.

Quotas d'opérations

Les quotas d'exploitation limitent l'utilisation mensuelle des fonctionnalités de test et de révision de sécurité pour aider à gérer la capacité des services.

Ressource	Scope	Quota	Ajustable
Revues de design	Par mois, par compte et par région	200	Oui
Révisions du code des relations publiques	Par mois, par compte et par région	1 000	Oui

Quotas de configuration

Les quotas de configuration limitent le nombre de ressources et de paramètres que vous pouvez configurer dans votre environnement AWS Security Agent.

Ressource	Scope	Quota	Ajustable
Espaces réservés aux agents	Par compte et par région	100	Oui
Intégrations	Par compte et par région	20	Non
Ressources intégrées par intégration	Par intégration	50	Non
Exigences de sécurité personnalisées	Par compte et par région	20	Non
Projets Pentest	Par compte et par région	1 000	Oui
Pentests simultanés	Par compte et par région	5	Oui
Projets de révision du code	Par compte et par région	1 000	Oui
Exécutions de révision de code simultanées	Par compte et par région	5	Oui

Historique du document

Le tableau suivant décrit certaines des principales mises à jour et nouvelles fonctionnalités du guide de l'utilisateur d'AWS Security Agents.

Modification	Description	Date
Connexions privées (aperçu)	Ajout de documentation pour les connexions privées. Cette nouvelle fonctionnalité permet à AWS Security Agent de se connecter à des systèmes de contrôle de source exécutés sur des réseaux privés à l'aide d'Amazon VPC Lattice, sans exposer vos systèmes à l'Internet public.	16 juin 2026

Modélisation des menaces (version préliminaire)	Ajout de documentation pour la modélisation des menaces. Cette nouvelle fonctionnalité crée un modèle de menace pour votre application à partir de documents de conceptio n (documents de portée), du code source (sources) ou des deux. Les documents de portée sont des documents de conception des fonctionn alités qui définissent l'objecti f de l'analyse, tandis que le code source fournit le contexte de votre système existant. Si vous ne fournissez pas de documentation sur le périmètre, l'agent génère un modèle de menace uniquemen t à partir du code source. Chaque exécution produit une vue d'ensemble du système et un ensemble de menaces classées par catégorie STRIDE avec des notes de gravité et des recommand ations.	8 juin 2026

Révision complète du code du référentiel (aperçu)	Ajout de documentation pour la révision complète du code du référentiel. Cette nouvelle fonctionnalité effectue une analyse de sécurité contextuelle de l'ensemble de votre base de code et génère des corrections de code en fonction des résultats.	12 mai 2026
Disponibilité de la région mise à jour pour trouver des mesures correctives	La disponibilité régionale pour les tests d'intrusion visant à détecter la correction dans l'application Web AWS Security Agent a été mise à jour.	16 avril 2026
Disponibilité de la région mise à jour pour permettre de trouver des solutions	La disponibilité des régions pour permettre la correction des résultats des tests d'intrusion dans l'AWS Management Console a été mise à jour.	16 avril 2026
Prise en charge des clés gérées par le client	Ajout de documentation pour le support des clés gérées par le client (CMK). Vous pouvez désormais spécifier une clé KMS gérée par le client lors de la création d'espaces d'agent et d'intégrations pour chiffrer vos données à l'aide de clés que vous contrôlez.	31 mars 2026

AWS mises à jour des politiques gérées	Ajout d'une politique AWSSecurityAgentWebAppPolicy gérée pour les nouveaux types TargetDomain et les types de DesignReviewFeedback ressources.	31 mars 2026
AWS mises à jour des politiques gérées	Ajout d'une politique AWSSecurityAgentWebAppPolicy gérée pour le nouveau type de AgentSpace ressource et les changements de nom d'action IAM.	9 février 2026
AWS mises à jour des politiques gérées	Mise SecurityAgentWebAppAPIPolicy à jour pour permettre aux clients de supprimer les avis de conception.	28 janvier 2026
AWS mises à jour des politiques gérées	Mise SecurityAgentWebAppAPIPolicy à jour pour permettre aux clients de lancer la correction automatique du code en cas de détection de problèmes de sécurité.	20 janvier 2026
AWS mises à jour des politiques gérées	Mis à jour SecurityAgentWebAppAPIPolicy pour permettre aux clients de visualiser les images dans la console.	5 décembre 2025
Version initiale des agents de sécurité AWS	Documentation initiale pour le lancement de service	2 décembre 2025

Les traductions sont fournies par des outils de traduction automatique. En cas de conflit entre le contenu d'une traduction et celui de la version originale en anglais, la version anglaise prévaudra.