AWS Guide de l'utilisateur pour la réponse aux incidents de sécurité

Version December 1, 2024

AWS Guide de l'utilisateur pour la réponse aux incidents de sécurité:

Table of Contents

Qu'est-ce que la réponse aux incidents de AWS sécurité ?

AWS Security Incident Response vous aide à vous préparer rapidement aux incidents de sécurité, à y répondre et à recevoir des conseils pour vous aider à vous remettre d'un incident de sécurité. Cela inclut les incidents tels que le piratage de comptes, les violations de données et les attaques par ransomware.

AWS Security Incident Response trie les résultats, intensifie les événements de sécurité et gère les cas qui nécessitent votre attention immédiate. En outre, vous avez accès à l'équipe de réponse aux incidents AWS clients (CIRT), qui enquêtera sur les ressources concernées.

> **Note**
>
> Il n'y a aucune garantie que les ressources affectées puissent être récupérées. Nous vous recommandons d'établir et de maintenir des sauvegardes pour les ressources susceptibles d'avoir un impact sur les besoins de votre entreprise.

AWS Security Incident Response fonctionne avec d'autres services AWS de détection et de réponse, qui vous guident tout au long du cycle de vie des incidents, de la détection à la restauration.

Table des matières

Configurations prises en charge

AWS Security Incident Response prend en charge les configurations linguistiques et régionales suivantes :

- Langue : AWS Security Incident Response est disponible en anglais.
- AWS Régions prises en charge :

  AWS Security Incident Response est disponible dans un sous-ensemble de Régions AWS. Dans ces régions prises en charge, vous créez un abonnement, vous créez et consultez des dossiers, et vous accédez au tableau de bord.

- USA Est (Ohio)
- USA Ouest (Oregon)
- USA Est (Virginie)
- UE (Francfort)
- UE (Irlande)
- UE (Londres)
- UE (Stockholm)
- Asie-Pacifique (Singapour)
- Asie-Pacifique (Séoul)
- Asie-Pacifique (Sydney)
- Asie-Pacifique (Tokyo)
- Canada (Centre)

Lorsque vous activez la fonctionnalité de surveillance et d'investigation, AWS Security Incident Response surveille les GuardDuty résultats d'Amazon concernant toutes les publicités actives Régions AWS. En tant que bonne pratique en matière de sécurité, AWS recommande de l'activer GuardDuty dans toutes les AWS régions prises en charge. Cette configuration permet GuardDuty de générer des informations concernant des activités non autorisées ou inhabituelles, même Régions AWS lorsque vous ne déployez pas activement de ressources. Ce faisant, vous améliorez votre posture de sécurité globale et maintenez une couverture complète de détection des menaces dans l'ensemble de votre AWS environnement.

> **Note**
>
> Amazon GuardDuty publie les résultats relatifs aux régions configurées. Si vous choisissez de ne pas activer le service dans une région spécifique, les alertes ne seront pas disponibles.

Résumé des fonctionnalités

Surveillance et enquête

AWS Security Incident Response examine rapidement les alertes de sécurité émises par Amazon GuardDuty et les intégrations tierces AWS Security Hub, réduisant ainsi le nombre de cas que votre

équipe doit analyser. Il configure les règles de suppression en fonction de votre environnement afin de réduire les alertes de faible priorité que vous devez trier et étudier.

Simplifier la réponse aux incidents

Adaptez et exécutez la réponse aux incidents en quelques minutes avec les parties prenantes, les services tiers et les outils concernés.

Solutions de sécurité en libre-service

AWS Security Incident APIs Response propose d'intégrer et de vous permettre de créer vos propres solutions de sécurité personnalisées.

Tableau de bord pour plus de visibilité

Surveillez et mesurez la préparation à la réponse aux incidents.

Posture de sécurité

Accédez aux AWS meilleures pratiques et à des outils approuvés pour l'évaluation de la sécurité et les enquêtes de réponse rapide aux incidents.

Assistance accélérée

Connectez-vous à AWS l'équipe de réponse aux incidents clients (CIRT) pour étudier, contenir et recevoir des conseils sur les moyens de récupérer après des événements de sécurité.

Préparation et disponibilité

Mettez en œuvre des notifications rationalisées en configurant votre équipe de réponse aux incidents qui déclenche des alertes auprès de personnes ou de groupes désignés, avec des politiques d'autorisation prédéfinies.

Concepts et terminologie

Les termes et concepts suivants sont importants pour comprendre le service de réponse aux incidents de AWS sécurité et son fonctionnement.

Champ d'application : La réponse aux incidents de AWS sécurité est conforme au guide de gestion des incidents de sécurité informatique 800-61 du National Institute of Standards and Technology (NIST), fournissant une approche cohérente de la gestion des événements de sécurité conformément aux meilleures pratiques du secteur.

Analyse : investigation et examen détaillés d'un événement de sécurité afin de comprendre sa portée, son impact et sa cause première.

AWS Portail de service de réponse aux incidents de sécurité : portail en libre-service qui vous permet de lancer et de gérer les cas d'événements de sécurité. La communication et les rapports continus sont facilités par le système de billetterie, les notifications automatisées et l'engagement direct avec l'équipe de service.

Communication : dialogue permanent et partage d'informations entre l'équipe de réponse aux incidents de AWS sécurité et le client pendant le processus de réponse aux incidents.

Confinement, éradication et restauration : prévention de toute activité non autorisée supplémentaire (confinement), associée à la suppression des ressources non autorisées et de la vulnérabilité d'origine (éradication), et à la récupération des ressources pour reprendre le cours normal des activités.

Amélioration continue : La réponse aux incidents de AWS sécurité intègre les commentaires et les leçons apprises lors d'engagements antérieurs afin d'améliorer ses capacités de détection, ses processus d'enquête et ses mesures correctives. AWS Security Incident Response tient également au up-to-date fait des dernières menaces de sécurité et des meilleures pratiques pour faire face à l'évolution des défis de sécurité.

Événement de cybersécurité : tout événement observable dans un système ou un réseau qui enfreint ou menace de violer les politiques de sécurité, les politiques d'utilisation acceptable ou les pratiques de sécurité standard.

Équipe de réponse aux incidents : groupe de personnes qui fournissent un soutien lors d'événements de sécurité actifs. Pour les cas AWS pris en charge, il s'agit de l'équipe de réponse aux incidents AWS clients (CIRT).

Flux de travail de réponse aux incidents : séquence définie d'étapes et d'activités impliquées dans la end-to-end gestion d'un événement de sécurité, conformément à la norme NIST 800-61.

Outils d'investigation : outils de réponse aux incidents de AWS sécurité et rôles liés aux services utilisés pour examiner l'état de fonctionnement de votre compte et de vos ressources.

Leçons apprises : examen et documentation d'une réponse à un événement de sécurité afin d'identifier les domaines à améliorer et d'éclairer la planification de la réponse aux incidents futurs.

Surveillance et investigation : AWS Security Incident Response examine rapidement les alertes de sécurité d'Amazon GuardDuty, en mettant au premier plan les alertes les plus importantes que votre équipe doit analyser. Il configure les règles de suppression en fonction des spécificités de votre environnement afin d'éviter les alertes inutiles.

Préparation : activités entreprises pour préparer une organisation à réagir efficacement aux événements de sécurité et à les gérer, telles que l'élaboration de plans de réponse aux incidents et de procédures de test.

Rapports et communication : les processus utilisés pour vous tenir informés tout au long du processus de réponse aux incidents, notamment les notifications automatisées, les passerelles d'appels et la livraison d'artefacts d'enquête. AWS Security Incident Response fournit un tableau de bord unique et centralisé AWS Management Console pour gérer tous vos efforts de réponse aux incidents de AWS sécurité.

Renseignements générés par les intervenants : indicateurs de compromission ; tactiques, techniques et procédures ; modèles associés observés lors des AWS CIRT enquêtes.

Expertise en matière d'événements de sécurité : connaissances et compétences spécialisées requises pour répondre et gérer efficacement les événements de sécurité, en particulier dans le contexte du AWS cloud.

Modèle de responsabilité partagée : division des responsabilités en matière de sécurité entre AWS et le client, où AWS est responsable de la sécurité du cloud et le client est responsable de la sécurité dans le cloud.

Renseignements sur les menaces : flux de données internes et externes contenant des informations détaillées sur les activités non autorisées pour aider à identifier les menaces de sécurité en constante évolution et à y répondre.

Système de billetterie : plateforme de gestion des dossiers dédiée qui vous permet d'intégrer et de gérer les cas d'événements de sécurité, d'ajouter des pièces jointes et de suivre le cycle de vie de réponse aux incidents.

Triage : évaluation initiale et hiérarchisation d'un événement de sécurité afin de déterminer la réponse appropriée et les prochaines étapes.

Flux de travail : séquence définie d'étapes et d'activités impliquées dans la end-to-end gestion d'un événement de sécurité.

Démarrage

Table des matières

Sélectionnez un compte d'adhésion

Un compte de membre est le AWS compte utilisé pour configurer les détails du compte, ajouter et supprimer des informations pour votre équipe de réponse aux incidents, et où tous les événements de sécurité actifs et historiques peuvent être créés et gérés. Il est recommandé d'aligner votre compte de membre AWS Security Incident Response sur le même compte que celui que vous avez activé pour des services tels qu'Amazon GuardDuty et AWS Security Hub.

Vous avez deux options pour sélectionner votre compte de membre AWS Security Incident Response à l'aide de AWS Organizations. Vous pouvez créer une adhésion dans le compte de gestion des Organisations ou dans un compte d'administrateur délégué des Organisations.

Utilisez le compte d'administrateur délégué : les tâches administratives de réponse aux incidents de AWS sécurité et la gestion des dossiers se trouvent dans le compte d'administrateur délégué. Nous vous recommandons d'utiliser le même administrateur délégué que celui que vous avez défini pour les autres services AWS de sécurité et de conformité. Fournissez l'identifiant de compte administrateur délégué à 12 chiffres, puis connectez-vous à ce compte pour continuer.

Utiliser le compte actuellement connecté : la sélection de ce compte signifie que le compte actuel sera un compte de membre central pour votre adhésion à AWS Security Incident Response. Les membres de votre organisation devront accéder au service via ce compte pour créer, accéder et gérer les cas actifs et résolus.

Assurez-vous de disposer des autorisations suffisantes pour administrer AWS la réponse aux incidents de sécurité.

Reportez-vous à la section Ajout et suppression IAM d'autorisations d'identité pour connaître les étapes spécifiques à suivre pour ajouter des autorisations.

Reportez-vous aux politiques gérées de réponse aux incidents de AWS sécurité.

Pour vérifier IAM les autorisations, vous pouvez suivre les étapes suivantes :

- Vérifiez la IAM politique : passez en revue la IAM politique associée à votre utilisateur, groupe ou rôle pour vous assurer qu'elle accorde les autorisations nécessaires. Vous pouvez le faire en accédant au https://console.aws.amazon.com/iam/, en sélectionnant l'`Users`option, en choisissant l'utilisateur en question, puis sur sa page de résumé, en accédant à l'`Permissions`onglet où vous pouvez voir la liste de toutes les politiques jointes ; vous pouvez développer chaque ligne de stratégie pour en afficher les détails.
- Testez les autorisations : essayez d'effectuer l'action dont vous avez besoin pour vérifier les autorisations. Par exemple, si vous devez accéder à un dossier, essayez de le faire`ListCases`. Si vous ne disposez pas des autorisations nécessaires, vous recevrez un message d'erreur.
- Utilisez le AWS CLI ou SDK : vous pouvez utiliser l'interface de ligne de AWS Command Line Interface commande (CLI) ou un AWS SDK dans votre langage de programmation préféré pour tester les autorisations. Par exemple, avec le AWS Command Line Interface, vous pouvez exécuter la `aws sts get-caller-identity` commande pour vérifier vos autorisations utilisateur actuelles.
- Vérifiez les AWS CloudTrail journaux : passez en revue les CloudTrail journaux pour voir si les actions que vous essayez d'effectuer sont enregistrées. Cela peut vous aider à identifier les éventuels problèmes d'autorisation.
- Utilisez le simulateur de IAM politiques : le simulateur de IAM politiques est un outil qui vous permet de tester IAM les politiques et de voir l'effet qu'elles ont sur vos autorisations.

> **Note**
>
> Les étapes spécifiques peuvent varier en fonction du AWS service et des actions que vous essayez d'effectuer.

Configurer les détails de l'adhésion

- Sélectionnez l' Région AWS endroit où votre adhésion et vos dossiers seront conservés.

> **Warning**
>
> Vous ne pouvez pas modifier la valeur par défaut Région AWS après l'enregistrement initial de l'adhésion.

- Vous pouvez éventuellement sélectionner un nom pour cette adhésion.
- Vous devez fournir un contact principal et un contact secondaire dans le cadre du processus de création d'adhésion. Ces contacts sont automatiquement inclus dans votre équipe de réponse aux incidents. Au moins deux contacts doivent exister pour un seul abonnement, ce qui garantit également qu'un minimum de deux contacts sont inclus dans l'équipe de réponse aux incidents.
- Définissez des tags facultatifs pour votre adhésion. Les balises vous aident à suivre AWS les coûts et à rechercher des ressources.

Associer des comptes à AWS Organizations

Votre adhésion donne droit à une couverture sur tous les appareils connectés Comptes AWS . AWS Organizations Les comptes associés seront automatiquement mis à jour au fur et à mesure que des comptes seront ajoutés ou supprimés de votre organisation.

Configurez des flux de travail proactifs de réponse et de triage des alertes

Le flux de travail proactif de gestion des réponses et des alertes est une fonctionnalité optionnelle à activer au sein de votre organisation pour surveiller les services de sécurité compatibles. Sélectionnez le bouton situé à côté de la fonctionnalité à activer.

Si vous rencontrez des problèmes d'intégration, veuillez créer un AWS Support dossier pour obtenir une assistance supplémentaire. Assurez-vous d'inclure les détails, y compris l' Compte AWS identifiant et les erreurs que vous pourriez avoir constatées pendant le processus de configuration.

Réponse proactive et triage des alertes : AWS Security Incident Response surveille et étudie les alertes générées par les intégrations d'Amazon GuardDuty et de Security Hub. Pour utiliser cette fonctionnalité, Amazon GuardDuty doit être activé. AWS Security Incident Response trie les alertes de faible priorité grâce à l'automatisation des services afin que votre équipe puisse se concentrer sur les problèmes les plus critiques. Pour plus d'informations sur le fonctionnement AWS de Security Incident Response avec Amazon GuardDuty AWS Security Hub, consultez la section Détecter et analyser du guide de l'utilisateur.

Cette fonctionnalité permet à AWS Security Incident Response de surveiller et d'étudier les résultats concernant tous les comptes et tous les comptes pris Régions AWS en charge actifs au sein de votre organisation. Pour faciliter cette fonctionnalité, AWS Security Incident Response crée automatiquement un rôle lié au service dans tous les comptes membres de votre compte. AWS

Organizations Toutefois, pour le compte de gestion, vous devez créer manuellement le rôle lié au service pour activer la surveillance.

Le service ne peut pas créer le rôle lié au service dans le compte de gestion. Vous devez créer ce rôle manuellement dans le compte de gestion en utilisant des ensembles de AWS CloudFormation piles.

Confinement : en cas d'incident de sécurité, AWS Security Incident Response peut exécuter des actions de confinement pour en atténuer rapidement l'impact, telles que l'isolation des hôtes compromis ou la rotation des informations d'identification. Security Incident Response n'active pas les fonctionnalités de confinement par défaut. Pour exécuter ces actions de confinement, vous devez d'abord accorder les autorisations nécessaires au service. Cela peut être fait en déployant un AWS CloudFormation StackSet, qui crée les rôles requis.

Tâches des utilisateurs

Table des matières

Tableau de bord

Sur la console AWS Security Incident Response, le tableau de bord vous fournit une vue d'ensemble de votre équipe de réponse aux incidents, de l'état de votre réponse proactive et un décompte continu des cas sur quatre semaines.

Sélectionnez cette option `View incident response team` pour accéder aux informations de vos collègues chargés de la réponse aux incidents.

Sélectionnez cette option `proactive response` pour savoir si le triage des alertes est activé. Si le `alert triaging` flux de travail n'est pas activé, vous pouvez surveiller son état et `Proactive Response` choisir de l'activer.

La section Mes dossiers du tableau de bord indique le nombre de dossiers AWS pris en charge ouverts et clôturés, ainsi que les dossiers autogérés qui vous ont été attribués au cours d'une période définie. Il indique également le temps moyen nécessaire pour résoudre les affaires clôturées en heures.

Gérer mon équipe de réponse aux incidents

Vos équipes de réponse aux incidents comprennent les parties prenantes du processus de réponse aux incidents. Vous pouvez configurer jusqu'à dix parties prenantes dans le cadre de votre adhésion.

Parmi les parties prenantes internes, citons par exemple les membres de votre équipe de réponse aux incidents, les analystes de sécurité, les propriétaires d'applications et votre équipe de direction de la sécurité.

Parmi les parties prenantes externes, citons par exemple des personnes travaillant pour des fournisseurs de logiciels indépendants (ISV) et des fournisseurs de services gérés (MSP) que vous souhaitez inclure dans un processus de réponse aux incidents.

> **Note**
>
> La configuration de votre équipe de réponse aux incidents ne permet pas automatiquement aux membres de votre équipe d'accéder aux ressources du service, telles que les adhésions et les dossiers. Vous pouvez utiliser des politiques AWS gérées pour AWS la réponse aux incidents de sécurité afin d'accorder un accès en lecture et en écriture aux ressources. Cliquez ici pour en savoir plus.

Vos collègues de réponse aux incidents spécifiés selon le niveau d'adhésion seront automatiquement ajoutés à tous les dossiers. Vous pouvez ajouter ou supprimer des coéquipiers individuels à tout moment après la création d'un dossier.

L'équipe de réponse aux incidents recevra une notification par e-mail concernant les événements suivants :

- Cas (créer, supprimer, mettre à jour)
- Commentaire (créer, supprimer, mettre à jour)
- Pièce jointe (créer, supprimer, mettre à jour)
- Abonnement (création, mise à jour, annulation, reprise)

Association du compte à AWS Organizations

Lorsque vous activez AWS Security Incident Response, l'adhésion sera créée et alignée sur votre AWS Organizations. Tous les comptes de vos Organizations correspondent à votre adhésion à AWS Security Incident Response.

Pour plus de détails, consultez la section Gestion des comptes de réponse aux incidents de AWS sécurité avec AWS Organizations.

Surveillance et enquête

AWS Security Incident Response examine et trie les alertes de sécurité d'Amazon AWS Security Hub, GuardDuty puis configure les règles de suppression en fonction de votre environnement afin d'éviter les alertes inutiles. L' AWS CIRTéquipe examine les résultats non triés, passe rapidement à l'échelon supérieur et guide votre équipe afin de contenir rapidement les problèmes potentiels. Si vous le souhaitez, vous pouvez autoriser AWS Security Incident Response à mettre en œuvre des actions de confinement en votre nom.

AWS La réponse aux incidents de sécurité s'aligne sur le guide de gestion des événements de sécurité informatique NIST 800-61r2 pour la réponse aux événements de sécurité. En s'alignant sur cette norme du secteur, AWS Security Incident Response fournit une approche cohérente de la gestion des événements de sécurité et adhère aux meilleures pratiques en matière de sécurisation et de réponse aux événements de sécurité dans votre AWS environnement.

Lorsque le service AWS de réponse aux incidents de sécurité identifie une alerte de sécurité ou que vous demandez une assistance en matière de sécurité, il AWS CIRT enquête. L'équipe collecte les événements du journal et les données de service telles que les GuardDuty alertes, trie et analyse ces données, effectue des activités de remédiation et de confinement et fournit des rapports après l'incident.

Table des matières

Préparation

L'équipe de réponse aux incidents de AWS sécurité enquête et collabore avec vous tout au long du cycle de vie de réponse aux événements de sécurité. Il est recommandé de configurer cette équipe et d'attribuer les autorisations nécessaires avant qu'un événement de sécurité ne se produise.

Détecter et analyser

AWS Security Incident Response surveille, trie et étudie les résultats de sécurité d'Amazon GuardDuty et les intégrations via. AWS Security Hub Les mesures supplémentaires susceptibles d'améliorer de manière significative la portée et l'efficacité des capacités de surveillance et d'investigation de AWS Security Incident Response sont notamment les suivantes :

Activation des sources de détection prises en charge

> **Note**
>
> AWS Les coûts du service de réponse aux incidents de sécurité n'incluent pas l'utilisation ni les autres coûts et frais associés aux sources de détection prises en charge ou à l'utilisation d'autres AWS services. Veuillez consulter les pages des fonctionnalités ou des services individuels pour connaître les détails des coûts.

Amazon GuardDuty

GuardDuty est un service de détection des menaces qui surveille, analyse et traite en permanence les sources de données et les journaux de votre AWS environnement. GuardDuty Il n'est pas nécessaire de l'activer pour utiliser AWS Security Incident Response ; toutefois, pour utiliser la fonction de réponse proactive et de triage des alertes, Amazon GuardDuty doit être activé.

Pour l'activer GuardDuty dans l'ensemble de votre organisation, consultez la `Setting up GuardDuty` section du guide de GuardDuty l'utilisateur Amazon.

Nous vous recommandons vivement d'activer toutes les GuardDuty options prises en charge Régions AWS. Cela permet GuardDuty de générer des informations sur des activités non autorisées ou inhabituelles, même dans les régions que vous n'utilisez pas activement. Pour plus d'informations, consultez Amazon GuardDuty Regions and endpoints

L'activation GuardDuty permet d'accéder aux données de détection des menaces critiques en réponse aux incidents de AWS sécurité, améliorant ainsi sa capacité à identifier les problèmes de sécurité potentiels dans votre AWS environnement et à y répondre.

AWS Security Hub

Security Hub peut ingérer les résultats de sécurité provenant de plusieurs AWS services et solutions de sécurité tierces prises en charge. Ces intégrations peuvent aider AWS Security Incident Response à surveiller et à étudier les résultats provenant d'autres outils de détection.

Pour activer l'intégration de Security Hub with Organizations, veuillez consulter le guide de AWS Security Hub l'utilisateur.

Il existe plusieurs manières d'activer les intégrations sur Security Hub. Pour les intégrations de produits tiers, vous devrez peut-être acheter l'intégration auprès du AWS Marketplace, puis la configurer. Les informations d'intégration fournissent des liens permettant d'effectuer ces tâches. Découvrez comment activer les AWS Security Hub intégrations.

AWS Security Incident Response peut surveiller et étudier les résultats à l'aide des outils suivants lorsqu'ils sont intégrés à AWS Security Hub :

- CrowdStrike — CrowdStrike Faucon
- Dentelle — Dentelle
- Trend Micro — Cloud One

En activant ces intégrations, vous pouvez améliorer de manière significative la portée et l'efficacité des capacités de surveillance et d'investigation de AWS Security Incident Response.

Analyser les résultats.

AWS L'équipe de AWS CIRT service et d'automatisation de la réponse aux incidents de sécurité analysera tous les résultats des outils pris en charge. Nous commencerons à en apprendre davantage sur votre environnement en communiquant avec vous à l'aide de dossiers de AWS Support. Par exemple, lorsque nous devons comprendre si une constatation est un comportement attendu ou si elle doit être transformée en incident. Au fur et à mesure que nous en apprendrons davantage sur votre environnement, nous personnaliserons le service et réduirons le nombre de communications.

Signaler un événement.

Vous pouvez déclencher un événement de sécurité via le portail du service AWS Security Incident Response. Il est important de ne pas attendre lors d'un événement de sécurité. AWS La réponse aux incidents de sécurité utilise des techniques automatisées et manuelles pour enquêter sur les événements de sécurité, analyser les journaux et rechercher des modèles anormaux. Votre partenariat et votre compréhension de votre environnement accélèrent cette analyse.

Communiquez.

AWS Security Incident Response vous tient informé tout au long de l'enquête en communiquant avec vos contacts de sécurité par le biais du ticket d'événement. Plusieurs membres de votre équipe

peuvent soutenir votre événement, tous utilisant le ticket d'événement pour accéder au contenu et AWS aux mises à jour fournis par le client.

Les communications peuvent inclure des notifications automatisées lorsqu'une alerte de sécurité est générée, des communications pendant l'analyse d'un événement, l'établissement de passerelles d'appels, l'analyse continue d'artefacts tels que les fichiers journaux et la communication des résultats de l'enquête pendant l'événement de sécurité.

AWS La réponse aux incidents de sécurité utilise deux types de cas différents pour communiquer avec vous : AWS Support pour les communications sortantes afin de vous informer d'un événement, et les cas de réponse aux incidents de AWS sécurité pour communiquer sur un dossier que vous nous avez ouvert.

AWS Dossiers de support : le service utilisera les dossiers de AWS support pour communiquer avec vos équipes. Nous créerons des dossiers de support pour chaque cas Compte AWS dans lequel le résultat est généré. Cette approche facilite la communication avec les multiples équipes responsables des charges de travail spécifiques, car elles auront une meilleure connaissance des événements survenant dans leurs domaines de responsabilité.

AWS Cas de réponse aux incidents de sécurité : si nous déterminons qu'une constatation doit être transformée en incident de sécurité, nous créerons un dossier de réponse aux incidents AWS de sécurité. Cela garantit que les problèmes de sécurité critiques reçoivent le niveau d'attention et de réponse appropriés.

En participant activement à ces communications et en fournissant des réponses rapides, vous pouvez aider le service de réponse aux incidents de AWS sécurité à :

- Comprenez mieux votre environnement et les comportements attendus.
- Réduisez les faux positifs au fil du temps.
- Améliorez la précision et la pertinence des alertes.
- Garantissez une réponse rapide aux véritables incidents de sécurité.
- N'oubliez pas que l'efficacité du service de réponse aux incidents de AWS sécurité s'améliore avec votre collaboration, ce qui se traduit par un AWS environnement plus sûr et surveillé de manière plus efficace.

Contenir

AWS Security Incident Response collabore avec vous pour contenir les événements. Vous pouvez configurer un rôle de service pour AWS Security Incident Response afin d'effectuer des actions

automatisées et manuelles dans votre compte en réponse aux alertes. Vous pouvez également effectuer le confinement vous-même ou en partenariat avec vos relations avec des tiers en utilisant des SSM documents.

La prise de décision est un élément essentiel du confinement, par exemple s'il faut arrêter un système, isoler une ressource du réseau, désactiver l'accès ou mettre fin à des sessions. Ces décisions sont facilitées lorsqu'il existe des stratégies et des procédures prédéterminées pour contenir l'événement. AWS Security Incident Response fournit la stratégie de confinement, vous informe de l'impact potentiel et vous guide dans la mise en œuvre de la solution uniquement après avoir pris en compte et accepté les risques encourus.

AWS Security Incident Response exécute les actions de confinement prises en charge en votre nom afin d'accélérer la réponse et de réduire le temps dont dispose un acteur menaçant pour potentiellement endommager votre environnement. Cette fonctionnalité permet d'atténuer plus rapidement les menaces identifiées, de minimiser l'impact potentiel et d'améliorer votre posture de sécurité globale. Il existe différentes options de confinement en fonction des ressources analysées. Les actions de confinement prises en charge sont les suivantes :

- EC2Confinement : l'automatisation du `AWSSupport-ContainEC2Instance` confinement effectue un confinement réseau réversible d'une EC2 instance, en laissant l'instance intacte et en cours d'exécution, mais en l'isolant de toute nouvelle activité réseau et en l'empêchant de communiquer avec des ressources internes ou externes à votre instance. VPC

  > **Important**
  >
  > Il est important de noter que les connexions suivies existantes ne seront pas interrompues suite à un changement de groupe de sécurité. Seul le trafic futur sera effectivement bloqué par le nouveau groupe de sécurité et ce SSM document. De plus amples informations sont disponibles dans la section sur le confinement des sources du guide technique du service.

- IAMConfinement : l'automatisation du `AWSSupport-ContainIAMPrincipal` confinement effectue un confinement réseau réversible d'un IAM utilisateur ou d'un rôle, en laissant l'utilisateur ou le rôle actifIAM, mais en l'empêchant de communiquer avec les ressources de votre compte.
- Confinement S3 : l'automatisation du `AWSSupport-ContainS3Resource` confinement effectue un confinement réversible d'un compartiment S3, en laissant les objets dans le compartiment et en isolant le compartiment ou l'objet Amazon S3 en modifiant ses politiques d'accès.

> **Important**
>
> AWS Security Incident Response n'active pas les fonctionnalités de confinement par défaut. Pour exécuter ces actions de confinement, vous devez d'abord accorder les autorisations nécessaires au service à l'aide de rôles. Vous pouvez créer ces rôles individuellement par compte ou dans l'ensemble de votre organisation en utilisant des AWS CloudFormation stacksets, qui créent les rôles requis.

AWS Security Incident Response vous encourage à envisager des stratégies de confinement adaptées à votre propension au risque pour chaque type d'événement majeur. Documentez des critères clairs pour faciliter la prise de décision lors d'un événement. Les critères à prendre en compte sont les suivants :

- Dommages potentiels aux ressources
- Préservation des preuves et exigences réglementaires
- Indisponibilité du service (par exemple, connectivité réseau, services fournis à des tiers externes)
- Temps et ressources nécessaires à la mise en œuvre de la stratégie
- Efficacité de la stratégie (par exemple, confinement partiel ou total)
- Permanence de la solution (par exemple, réversible ou irréversible)
- Durée de la solution (par exemple, solution d'urgence, solution temporaire, solution permanente) Appliquez des contrôles de sécurité qui peuvent réduire les risques et laisser le temps de définir et de mettre en œuvre une stratégie de confinement plus efficace.

AWS La réponse aux incidents de sécurité recommande une approche par étapes pour parvenir à un confinement efficient et efficace, impliquant des stratégies à court et à long terme basées sur le type de ressource.

- Stratégie de confinement
  - La réponse aux incidents de AWS sécurité peut-elle identifier l'étendue de l'événement de sécurité ?
    - Dans l'affirmative, identifiez toutes les ressources (utilisateurs, systèmes, ressources).
    - Si ce n'est pas le cas, étudiez en parallèle avec l'exécution de l'étape suivante sur les ressources identifiées.
  - La ressource peut-elle être isolée ?

    - Si c'est le cas, isolez les ressources affectées.
    - Si ce n'est pas le cas, collaborez avec les propriétaires et les gestionnaires du système pour déterminer les mesures supplémentaires nécessaires pour contenir le problème.
  - Toutes les ressources affectées sont-elles isolées des ressources non touchées ?
    - Si c'est le cas, passez à l'étape suivante.
    - Si ce n'est pas le cas, continuez à isoler les ressources affectées afin de les endiguer à court terme et d'empêcher que l'événement ne s'aggrave davantage.
- Sauvegarde du système
  - Des copies de sauvegarde des systèmes concernés ont-elles été créées pour une analyse plus approfondie ?
  - Les copies médico-légales sont-elles cryptées et stockées dans un endroit sûr ?
    - Si c'est le cas, passez à l'étape suivante.
    - Si ce n'est pas le cas, chiffrez les images médico-légales, puis stockez-les dans un endroit sûr pour éviter toute utilisation accidentelle, tout dommage ou toute altération.

Éradiquer

Au cours de la phase d'éradication, il est important d'identifier et de traiter tous les comptes, ressources et instances concernés, par exemple en supprimant les logiciels malveillants, en supprimant les comptes utilisateurs compromis et en atténuant les vulnérabilités découvertes, afin d'appliquer des mesures correctives uniformes dans l'ensemble de l'environnement.

Une bonne pratique consiste à adopter une approche progressive de l'éradication et du rétablissement et à hiérarchiser les étapes de remédiation. L'objectif des premières phases est d'augmenter rapidement la sécurité globale (de quelques jours à plusieurs semaines) grâce à des modifications de grande valeur visant à prévenir de futurs événements. Les phases ultérieures peuvent se concentrer sur les changements à long terme (par exemple, les changements d'infrastructure) et sur le travail continu visant à assurer la sécurité de l'entreprise autant que possible. Chaque cas est unique et AWS CIRT nous travaillerons avec vous pour évaluer les mesures nécessaires.

Éléments à prendre en compte :

- Pouvez-vous redéfinir l'image du système et le renforcer à l'aide de correctifs ou d'autres contre-mesures pour prévenir ou réduire le risque d'attaques ?

- Pouvez-vous remplacer le système infecté par une nouvelle instance ou ressource, afin de garantir une base de référence propre tout en mettant fin à l'élément infecté ?
- Avez-vous supprimé tous les malwares et autres artefacts laissés par l'utilisation non autorisée, et avez-vous renforcé les systèmes concernés contre de nouvelles attaques ?
- Est-il nécessaire de procéder à des analyses médico-légales sur les ressources touchées ?

Récupération

AWS Security Incident Response vous fournit des conseils pour vous aider à rétablir le fonctionnement normal des systèmes, à confirmer qu'ils fonctionnent correctement et à corriger les vulnérabilités afin d'éviter que des événements similaires ne se reproduisent à l'avenir. AWS La réponse aux incidents de sécurité ne contribue pas directement à la restauration des systèmes. Les principales considérations sont les suivantes :

- Les systèmes concernés ont-ils été corrigés et renforcés face à la récente attaque ?
- Quel est le calendrier faisable pour remettre les systèmes en production ?
- Quels outils utiliserez-vous pour tester, surveiller et vérifier les systèmes restaurés ?

Rapport post-incident

AWS Security Incident Response fournit un résumé de l'événement après la fin des activités de sécurité entre votre équipe et la nôtre.

À la fin de chaque mois, le service de réponse aux incidents de AWS sécurité envoie des rapports mensuels par e-mail au point de contact principal de chaque client. Les rapports seront fournis dans un PDF format utilisant les indicateurs décrits ci-dessous. Les clients recevront un rapport par AWS Organizations.

Indicateurs relatifs aux cas

- Dossiers créés
  - Nom de la dimension : Type
  - Valeurs de dimension : AWS prises en charge, autonomes
  - Unité : nombre
  - Description : nombre de dossiers créés.
- Affaires clôturées

  - Nom de la dimension : Type
  - Valeurs de dimension : AWS prises en charge, autogérées
  - Unité : nombre
  - Description : Mesure du nombre total de dossiers clôturés.
- Boîtes ouvertes
  - Nom de la dimension : Type
  - Valeurs de dimension : AWS prises en charge, autonomes
  - Unité : nombre
  - Description : nombre de dossiers ouverts.

Métriques de triage

- Constatations reçues
  - Unité : nombre
  - Description : nombre de résultats envoyés au triage.
- Résultats archivés
  - Unité : nombre
  - Description : nombre de résultats archivés après avoir été traités sans investigation manuelle.
- Constatations examinées manuellement
  - Unité : nombre
  - Description : nombre de constatations ayant fait l'objet d'une investigation manuelle.
- Enquêtes archivées
  - Unité : nombre
  - Description : Le nombre d'enquêtes manuelles aboutissant à des faux positifs et envoyées pour archivage
- Les enquêtes se sont intensifiées
  - Unité : nombre
  - Description : Le nombre d'enquêtes manuelles ayant donné lieu à un incident de sécurité

Cas

AWS Security Incident Response vous permet de créer deux types de cas : les cas AWS pris en charge ou les cas autogérés.

Création d'un dossier AWS pris en charge

Vous pouvez créer un dossier AWS pris en charge à partir de la réponse aux incidents de AWS sécuritéAPI, du, ou du AWS Command Line Interface. AWS les cas pris en charge vous permettent de bénéficier de l'assistance de l'équipe de réponse aux incidents AWS clients (CIRT).

> **Note**
>
> AWS CIRTrépondra à votre demande dans les 15 minutes. Le temps de réponse correspond à une première réponse de AWS CIRT. Nous ferons tous les efforts raisonnables pour répondre à votre demande initiale dans ce délai. Ce délai de réponse ne s'applique pas aux réponses suivantes.

L'exemple suivant décrit l'utilisation de la console.

1. Connectez-vous au AWS Management Console. Ouvrez la console Security Incident Response à l'adresse https://console.aws.amazon.com/security-ir/.
2. Choisissez Create Case
3. Choisissez Résoudre le dossier avec AWS
4. Sélectionnez le type de demande
   a. Incident de sécurité actif : ce type est destiné à l'assistance et aux services de réponse aux incidents urgents.
   b. Enquêtes : les enquêtes vous permettent d'obtenir de l'aide en cas d'incidents de sécurité présumés, dans le cadre desquelles elles AWS CIRT peuvent vous aider à analyser le journal et à obtenir une confirmation secondaire de l'enquête sur la réponse à l'incident.
5. Définissez l'estimation de la date de début à la date du premier indicateur de l'incident. Par exemple, lorsque vous avez connu un comportement anormal pour la première fois ou lorsque vous avez reçu la première alerte de sécurité correspondante.
6. Définissez un titre pour le dossier
7. Fournissez une description détaillée du cas. Tenez compte des aspects suivants qui peuvent aider les intervenants à résoudre les incidents :

a. Que s’est-il passé ?
b. Qui a découvert et signalé l'incident ?
c. Qui est concerné par cette affaire ?
d. Quel est l'impact connu ?
e. Quelle est l'urgence de cette affaire ?
f. Ajoutez un ou plusieurs Compte AWS IDs éléments inclus dans le champ du dossier.

8. Ajoutez des informations facultatives sur le dossier :
   a. Sélectionnez les principaux services concernés dans la liste déroulante.
   b. Sélectionnez les principales régions touchées dans la liste déroulante.
   c. Ajoutez une ou plusieurs adresses IP d'acteurs menaçants que vous avez identifiées dans le cadre de ce dossier.
9. Ajoutez des intervenants supplémentaires facultatifs au dossier qui recevra des notifications. Pour ajouter une personne, procédez comme suit :
   a. Ajoutez une adresse e-mail.
   b. Ajoutez un prénom et un nom de famille facultatifs.
   c. Choisissez Ajouter pour ajouter une autre personne.
   d. Pour supprimer un individu, choisissez l'option Supprimer pour un individu.
   e. Choisissez Ajouter pour ajouter toutes les personnes répertoriées au dossier.
      i. Vous pouvez sélectionner plusieurs personnes et choisir Supprimer pour les supprimer de la liste.
10. Ajoutez des étiquettes facultatives au boîtier.
    a. Pour ajouter une balise, procédez comme suit :
    b. Sélectionnez Ajouter une nouvelle balise.
    c. Pour Clé, entrez le nom de la balise.
    d. Pour Valeur, saisissez la valeur de l‘identification.
    e. Pour supprimer une balise, choisissez l‘option de Suppression pour cette balise.

Une fois qu'un dossier AWS pris en charge a été créé, l'équipe de réponse aux incidents AWS CIRT et votre équipe de réponse aux incidents sont immédiatement informées.

Création d'un dossier autogéré

Vous pouvez créer une solution autogérée à partir de la réponse aux incidents de AWS sécurité, duAPI, ou du AWS Command Line Interface. Ce type de cas DOESNOTengage le AWS CIRT. L'exemple suivant décrit l'utilisation de la console.

1. Connectez-vous au AWS Management Console. Ouvrez la console Security Incident Response à l'adresse https://console.aws.amazon.com/security-ir/.
2. Choisissez Create Case (Créer une demande).
3. Choisissez Résoudre le dossier avec ma propre équipe de réponse aux incidents.
4. Définissez l'estimation de la date de début à la date du premier indicateur de l'incident. Par exemple, lorsque vous avez connu un comportement anormal pour la première fois ou lorsque vous avez reçu la première alerte de sécurité correspondante.
5. Définissez un titre pour le dossier. Il est recommandé d'inclure les données dans le titre du dossier, comme suggéré lors de la sélection de l'option Générer le titre.
6. Entrez Compte AWS IDs ceux qui font partie du dossier. Pour ajouter un identifiant de compte, procédez comme suit :
   a. Entrez l'identifiant de compte à 12 chiffres et choisissez Ajouter un compte.
   b. Pour supprimer un compte, choisissez Supprimer à côté du compte que vous souhaitez supprimer du dossier.
7. Fournissez une description détaillée du cas.
   a. Tenez compte des aspects suivants qui peuvent aider les intervenants à résoudre les incidents :
      i. Que s’est-il passé ?
      ii. Qui a découvert et signalé l'incident ?
      iii. Qui est concerné par cette affaire ?
      iv. Quel est l'impact connu ?
      v. Quelle est l'urgence de cette affaire ?
8. Ajoutez des informations facultatives sur le dossier :
   a. Sélectionnez les principaux services concernés dans la liste déroulante.
   b. Sélectionnez les principales régions touchées dans la liste déroulante.
   c. Ajoutez une ou plusieurs adresses IP d'acteurs menaçants que vous avez identifiées dans le cadre de ce dossier.
9. Ajoutez des intervenants supplémentaires facultatifs au dossier qui recevra des notifications. Pour ajouter une personne, procédez comme suit :

a. Ajoutez une adresse e-mail.

b. Ajoutez un prénom et un nom de famille facultatifs.

c. Choisissez Ajouter pour ajouter une autre personne.

d. Pour supprimer un individu, choisissez l'option Supprimer pour un individu.

e. Choisissez Ajouter pour ajouter toutes les personnes répertoriées au dossier. Vous pouvez sélectionner plusieurs personnes et choisir Supprimer pour les supprimer de la liste.

10 Ajoutez des étiquettes facultatives au boîtier. Pour ajouter une balise, procédez comme suit :

a. Sélectionnez Ajouter une nouvelle balise.

b. Pour Clé, entrez le nom de la balise.

c. Pour Valeur, saisissez la valeur de l‘identification.

d. Pour supprimer une balise, choisissez l‘option de Suppression pour cette balise.

L'équipe de réponse aux incidents sera informée par e-mail une fois le dossier créé.

Répondre à un dossier AWS généré

AWS La réponse aux incidents de sécurité peut créer une notification sortante ou un cas lorsque vous devez agir ou être au courant d'un élément susceptible d'avoir un impact sur votre compte ou vos ressources. Cela ne se produira que si vous avez activé les flux de travail de réponse proactive et de triage des alertes activés dans le cadre de votre abonnement.

Ces notifications apparaîtront dans le AWS Support centre. Le guide de AWS Support l'utilisateur contient des informations et des étapes détaillées pour mettre à jour, résoudre et rouvrir ces dossiers.

Gestion des dossiers

Table des matières

- Pièces jointes
- Balises
- Activités liées aux affaires
- Clôture d'un dossier

Modification du statut du dossier

Un dossier se trouvera dans l'un des états suivants :

- Soumis : il s'agit du statut initial d'un dossier. Les cas présentant ce statut ont été soumis par une personne demandée, mais ne sont pas encore en cours de traitement.
- Détection et analyse : ce statut indique qu'un intervenant a commencé à travailler sur le dossier. Cette phase comprend la collecte de données, le tri de l'événement et la réalisation d'analyses pour tirer des conclusions fondées sur les données.
- Confinement, éradication et rétablissement : dans ce statut, le responsable de l'intervention en cas d'incident a identifié une activité suspecte qui nécessite des efforts supplémentaires pour être supprimée. Le responsable de l'intervention en cas d'incident vous fournira des recommandations pour l'analyse des risques commerciaux et des mesures supplémentaires. Si vous avez activé les fonctionnalités d'abonnement au service, un intervenant en AWS cas d'incident vous demandera votre consentement pour effectuer des actions de confinement avec les SSM documents du ou des comptes concernés.
- Activités après l'incident : Dans ce statut, l'événement de sécurité principal a été maîtrisé. L'accent est désormais mis sur la reprise et le retour à la normale des activités commerciales. Un résumé et une analyse des causes premières sont fournis si le résolveur du dossier est AWS pris en charge.
- Fermé : il s'agit de l'état final du flux de travail. Les dossiers classés indiquent que le travail est terminé. Les dossiers fermés ne peuvent pas être rouverts. Assurez-vous donc que toutes les actions sont terminées avant de passer à ce statut.

Choisissez Action/Update Status pour modifier le statut du dossier pour les cas autogérés. Pour les cas AWS pris en charge, le statut est défini par le AWS CIRT répondeur.

Changer le résolveur

Pour les cas autogérés, votre équipe de réponse aux incidents peut demander de l'aide à AWS. Choisissez Obtenir de l'aide AWS auprès de pour remplacer le résolveur de ce cas par. AWS Une fois que le dossier est considéré comme AWS pris en charge, le statut passe à Soumis. L'historique

du cas existant sera disponible pour AWS CIRT. Une fois que AWS vous aurez demandé de l'aide, vous ne pourrez plus redevenir autogéré.

Eléments d'action

Un AWS CIRT intervenant travaillant sur le dossier peut demander des mesures à votre équipe interne.

Les actions qui apparaissent après la création d'un dossier sont les suivantes :

- Demande d'autorisation permettant à un intervenant chargé de répondre aux incidents d'accéder à un dossier
- Demande de fourniture de plus amples informations sur l'affaire

Élément d'action lorsqu'une action du client est en attente :

- Demande de donner suite à un nouveau commentaire pour poursuivre l'affaire

Mesures à prendre lorsqu'un dossier est prêt à être clôturé :

- Demande de révision du rapport de cas
- Demande de clôture du dossier

Modification d'un cas

Choisissez Modifier pour modifier les détails d'un dossier.

Pour les cas AWS pris en charge et autogérés :

Vous pouvez modifier les informations de dossier suivantes une fois qu'un dossier a été créé :

- Title
- Description

Pour les cas AWS pris en charge uniquement :

Vous pouvez modifier les champs supplémentaires :

- Type de demande :

  - Incident de sécurité actif : ce type est destiné à l'assistance et aux services de réponse aux incidents urgents.
  - Enquêtes : Les enquêtes vous permettent d'obtenir de l'aide en cas d'incident de sécurité perçu, dans le cadre duquel AWS CIRT elles peuvent vous aider à analyser le journal et à obtenir une confirmation secondaire de l'enquête sur la réponse à l'incident.
- Date de début estimée : modifiez ce champ si vous avez reçu des indicateurs pour ce cas antérieurs à la date de début initiale fournie. Envisagez de fournir des détails supplémentaires concernant le nouvel indicateur détecté dans le champ de description ou d'ajouter un commentaire dans l'onglet communications.

Communications

AWS CIRTpeuvent ajouter des commentaires pour documenter leurs activités lorsqu'ils travaillent sur un dossier. Différents AWS CIRT intervenants peuvent travailler sur un dossier en même temps. Ils sont représentés en tant que AWS répondeur dans le journal des communications.

Autorisations

L'onglet Autorisations répertorie toutes les personnes qui seront informées de toute modification apportée au dossier. Vous pouvez ajouter et supprimer des personnes de la liste jusqu'à ce que le dossier soit clos.

> **Note**
>
> Les cas individuels vous permettent d'inclure jusqu'à 30 parties prenantes au total. Une configuration d'autorisation supplémentaire est requise pour accorder un accès au niveau du dossier à ces parties prenantes.

Fournir l'accès à un dossier dans la console

Pour donner accès au dossier figurant dans le AWS Management Console, vous pouvez copier le modèle de politique d'IAMautorisation et ajouter cette autorisation à un utilisateur ou à un rôle.

Ajouter la IAM politique à un utilisateur ou à un rôle :

1. Copiez la politique IAM d'autorisation.
2. Ouvrez IAM dans le via https://console.aws.amazon.com/iam/.

3. Dans le volet de navigation, sélectionnez Utilisateur ou Rôles.
4. Sélectionnez un utilisateur ou un rôle pour ouvrir la page de détails.
5. Dans l'onglet Autorisations, choisissez Ajouter des autorisations.
6. Choisissez Attach policy (Attacher une politique).
7. Sélectionnez la politique gérée de réponse aux incidents de AWS sécurité appropriée.
8. Choisissez Add policy (Ajouter la politique).

Pièces jointes

Vos intervenants en charge des incidents peuvent ajouter des pièces jointes à un dossier afin d'aider les autres intervenants dans leur enquête sur les cas autogérés.

> **Note**
>
> Si vous choisissez un dossier AWS pris en charge, vous AWS ne pouvez pas afficher les pièces jointes. Tous les détails relatifs aux dossiers AWS pris en charge doivent être partagés par le biais de commentaires ou en fournissant un partage d'écran à l'aide de votre technologie de communication préférée.

Choisissez Upload pour sélectionner un fichier sur votre ordinateur à ajouter au dossier.

> **Note**
>
> Toutes les pièces jointes téléchargées sont supprimées sept jours après la réception du dossier`Closed`.

Balises

Une balise est une étiquette facultative que vous pouvez attribuer à vos dossiers pour contenir les métadonnées relatives à cette ressource. Chaque balise est une étiquette composée d'une clé et d'une valeur facultative. Vous pouvez utiliser une balise pour rechercher, répartir les coûts et authentifier les autorisations associées à la ressource.

Pour ajouter une balise, procédez comme suit :

1. Sélectionnez Ajouter une nouvelle balise.

2. Pour Clé, entrez le nom de la balise.
3. Pour Valeur, saisissez la valeur de l'identification.

Pour supprimer une balise, choisissez l'option de Suppression pour cette balise.

Activités liées aux affaires

Les pistes d'audit fournissent des enregistrements chronologiques détaillés de toutes les activités liées aux dossiers. Ils fournissent des informations importantes lors des activités post-événement et aident à identifier les améliorations potentielles. L'heure, l'utilisateur, l'action et les détails de tout changement de dossier sont enregistrés dans la piste d'audit des cas.

Clôture d'un dossier

Pour les dossiers AWS pris en charge, choisissez Fermer le dossier sur la page des détails du dossier pour clôturer définitivement le dossier quel que soit son statut. Un dossier atteint généralement le statut Prêt à fermer avant d'être définitivement clos. Si vous clôturez un dossier prématurément à un statut autre que « Prêt à fermer », vous demandez qu'il AWS CIRT cesse de travailler sur ce dossier AWS pris en charge.

Si votre équipe de réponse aux incidents est chargée de répondre aux incidents, sélectionnez Action/Clore le dossier sur la page des détails du dossier.

> **Note**
>
> Le statut « Prêt à fermer » signifie qu'un dossier peut être définitivement clos et qu'il n'y a aucun travail supplémentaire à effectuer sur un dossier.

Un dossier ne peut pas être rouvert une fois qu'il a été définitivement fermé. Toutes les informations seront disponibles en lecture seule. Pour éviter toute fermeture accidentelle, il vous sera demandé de confirmer que vous souhaitez fermer le boîtier.

Travailler avec des AWS CloudFormation stacksets

> **Important**
>
> AWS Security Incident Response n'active pas les fonctionnalités de confinement par défaut. Pour exécuter ces actions de confinement, vous devez d'abord accorder les autorisations

nécessaires au service à l'aide de rôles. Vous pouvez créer ces rôles individuellement par compte ou dans l'ensemble de votre organisation en les déployant AWS CloudFormation StackSets, ce qui crée les rôles requis.

Vous trouverez des instructions spécifiques sur la façon de créer un ensemble de piles avec des autorisations gérées par le service.

Vous trouverez ci-dessous des ensembles de modèles pour créer les rôles AWSSecurityIncidentResponseContainmentet AWSSecurityIncidentResponseContainmentExecution.

```
AWSTemplateFormatVersion: '2010-09-09'
Description: 'Template for AWS Security Incident Response containment roles'

Resources:
  AWSSecurityIncidentResponseContainment:
    Type: 'AWS::IAM::Role'
    Properties:
      RoleName: AWSSecurityIncidentResponseContainment
      AssumeRolePolicyDocument:
        {
          'Version': '2012-10-17',
          'Statement':
            [
              {
                'Effect': 'Allow',
                'Principal': { 'Service': 'containment.security-ir.amazonaws.com' },
                'Action': 'sts:AssumeRole',
                'Condition': { 'StringEquals': { 'sts:ExternalId': !Sub
 '${AWS::AccountId}' } },
              },
              {
                'Effect': 'Allow',
                'Principal': { 'Service': 'containment.security-ir.amazonaws.com' },
                'Action': 'sts:TagSession',
              },
            ],
        }
      Policies:
        - PolicyName: AWSSecurityIncidentResponseContainmentPolicy
          PolicyDocument:
            {
```

```
              'Version': '2012-10-17',
              'Statement':
                [
                  {
                    'Effect': 'Allow',
                    'Action': ['ssm:StartAutomationExecution'],
                    'Resource':
                      [
                        !Sub 'arn:${AWS::Partition}:ssm:*:*:automation-definition/
AWSSupport-ContainEC2Instance:$DEFAULT',
                        !Sub 'arn:${AWS::Partition}:ssm:*:*:automation-definition/
AWSSupport-ContainS3Resource:$DEFAULT',
                        !Sub 'arn:${AWS::Partition}:ssm:*:*:automation-definition/
AWSSupport-ContainIAMPrincipal:$DEFAULT',
                      ],
                  },
                  {
                    'Effect': 'Allow',
                    'Action':
                      ['ssm:DescribeInstanceInformation', 'ssm:GetAutomationExecution',
 'ssm:ListCommandInvocations'],
                    'Resource': '*',
                  },
                  {
                    'Effect': 'Allow',
                    'Action': ['iam:PassRole'],
                    'Resource': !GetAtt
 AWSSecurityIncidentResponseContainmentExecution.Arn,
                    'Condition': { 'StringEquals': { 'iam:PassedToService':
 'ssm.amazonaws.com' } },
                  },
                ],
            }
  AWSSecurityIncidentResponseContainmentExecution:
    Type: 'AWS::IAM::Role'
    Properties:
      RoleName: AWSSecurityIncidentResponseContainmentExecution
      AssumeRolePolicyDocument:
        {
          'Version': '2012-10-17',
          'Statement':
            [{ 'Effect': 'Allow', 'Principal': { 'Service': 'ssm.amazonaws.com' },
 'Action': 'sts:AssumeRole' }],
        }
```

```
      ManagedPolicyArns:
        - !Sub arn:${AWS::Partition}:iam::aws:policy/SecurityAudit
      Policies:
        - PolicyName: AWSSecurityIncidentResponseContainmentExecutionPolicy
          PolicyDocument:
            {
              'Version': '2012-10-17',
              'Statement':
                [
                  {
                    'Sid': 'AllowIAMContainment',
                    'Effect': 'Allow',
                    'Action':
                      [
                        'iam:AttachRolePolicy',
                        'iam:AttachUserPolicy',
                        'iam:DeactivateMFADevice',
                        'iam:DeleteLoginProfile',
                        'iam:DeleteRolePolicy',
                        'iam:DeleteUserPolicy',
                        'iam:GetLoginProfile',
                        'iam:GetPolicy',
                        'iam:GetRole',
                        'iam:GetRolePolicy',
                        'iam:GetUser',
                        'iam:GetUserPolicy',
                        'iam:ListAccessKeys',
                        'iam:ListAttachedRolePolicies',
                        'iam:ListAttachedUserPolicies',
                        'iam:ListMfaDevices',
                        'iam:ListPolicies',
                        'iam:ListRolePolicies',
                        'iam:ListUserPolicies',
                        'iam:ListVirtualMFADevices',
                        'iam:PutRolePolicy',
                        'iam:PutUserPolicy',
                        'iam:TagMFADevice',
                        'iam:TagPolicy',
                        'iam:TagRole',
                        'iam:TagUser',
                        'iam:UntagMFADevice',
                        'iam:UntagPolicy',
                        'iam:UntagRole',
                        'iam:UntagUser',
```

```
                        'iam:UpdateAccessKey',
                        'identitystore:CreateGroupMembership',
                        'identitystore:DeleteGroupMembership',
                        'identitystore:IsMemberInGroups',
                        'identitystore:ListUsers',
                        'identitystore:ListGroups',
                        'identitystore:ListGroupMemberships',
                      ],
                    'Resource': '*',
                  },
                  {
                    'Sid': 'AllowOrgListAccounts',
                    'Effect': 'Allow',
                    'Action': 'organizations:ListAccounts',
                    'Resource': '*',
                  },
                  {
                    'Sid': 'AllowSSOContainment',
                    'Effect': 'Allow',
                    'Action':
                      [
                        'sso:CreateAccountAssignment',
                        'sso:DeleteAccountAssignment',
                        'sso:DeleteInlinePolicyFromPermissionSet',
                        'sso:GetInlinePolicyForPermissionSet',
                        'sso:ListAccountAssignments',
                        'sso:ListInstances',
                        'sso:ListPermissionSets',
                        'sso:ListPermissionSetsProvisionedToAccount',
                        'sso:PutInlinePolicyToPermissionSet',
                        'sso:TagResource',
                        'sso:UntagResource',
                      ],
                    'Resource': '*',
                  },
                  {
                    'Sid': 'AllowSSORead',
                    'Effect': 'Allow',
                    'Action': ['sso-directory:SearchUsers', 'sso-
directory:DescribeUser'],
                    'Resource': '*',
                  },
                  {
                    'Sid': 'AllowS3Read',
```

```
                'Effect': 'Allow',
                'Action':
                  [
                    's3:GetAccountPublicAccessBlock',
                    's3:GetBucketAcl',
                    's3:GetBucketLocation',
                    's3:GetBucketOwnershipControls',
                    's3:GetBucketPolicy',
                    's3:GetBucketPolicyStatus',
                    's3:GetBucketPublicAccessBlock',
                    's3:GetBucketTagging',
                    's3:GetEncryptionConfiguration',
                    's3:GetObject',
                    's3:GetObjectAcl',
                    's3:GetObjectTagging',
                    's3:GetReplicationConfiguration',
                    's3:ListBucket',
                    's3express:GetBucketPolicy',
                  ],
                'Resource': '*',
              },
              {
                'Sid': 'AllowS3Write',
                'Effect': 'Allow',
                'Action':
                  [
                    's3:CreateBucket',
                    's3:DeleteBucketPolicy',
                    's3:DeleteObjectTagging',
                    's3:PutAccountPublicAccessBlock',
                    's3:PutBucketACL',
                    's3:PutBucketOwnershipControls',
                    's3:PutBucketPolicy',
                    's3:PutBucketPublicAccessBlock',
                    's3:PutBucketTagging',
                    's3:PutBucketVersioning',
                    's3:PutObject',
                    's3:PutObjectAcl',
                    's3express:CreateSession',
                    's3express:DeleteBucketPolicy',
                    's3express:PutBucketPolicy',
                  ],
                'Resource': '*',
              },
```

```
                    {
                      'Sid': 'AllowAutoScalingWrite',
                      'Effect': 'Allow',
                      'Action':
                        [
                          'autoscaling:CreateOrUpdateTags',
                          'autoscaling:DeleteTags',
                          'autoscaling:DescribeAutoScalingGroups',
                          'autoscaling:DescribeAutoScalingInstances',
                          'autoscaling:DescribeTags',
                          'autoscaling:EnterStandby',
                          'autoscaling:ExitStandby',
                          'autoscaling:UpdateAutoScalingGroup',
                        ],
                      'Resource': '*',
                    },
                    {
                      'Sid': 'AllowEC2Containment',
                      'Effect': 'Allow',
                      'Action':
                        [
                          'ec2:AuthorizeSecurityGroupEgress',
                          'ec2:AuthorizeSecurityGroupIngress',
                          'ec2:CopyImage',
                          'ec2:CreateImage',
                          'ec2:CreateSecurityGroup',
                          'ec2:CreateSnapshot',
                          'ec2:CreateTags',
                          'ec2:DeleteSecurityGroup',
                          'ec2:DeleteTags',
                          'ec2:DescribeImages',
                          'ec2:DescribeInstances',
                          'ec2:DescribeSecurityGroups',
                          'ec2:DescribeSnapshots',
                          'ec2:DescribeTags',
                          'ec2:ModifyNetworkInterfaceAttribute',
                          'ec2:RevokeSecurityGroupEgress',
                        ],
                      'Resource': '*',
                    },
                    {
                      'Sid': 'AllowKMSActions',
                      'Effect': 'Allow',
                      'Action':
```

```
                [
                  'kms:CreateGrant',
                  'kms:DescribeKey',
                  'kms:GenerateDataKeyWithoutPlaintext',
                  'kms:ReEncryptFrom',
                  'kms:ReEncryptTo',
                ],
              'Resource': '*',
            },
            {
              'Sid': 'AllowSSMActions',
              'Effect': 'Allow',
              'Action': ['ssm:DescribeAutomationExecutions'],
              'Resource': '*',
            },
          ],
      }
```

Annuler l'adhésion

Un rôle CancelMembership autorisé à répondre aux incidents de AWS sécurité peut annuler son adhésion depuis la consoleAPI, le ou AWS Command Line Interface.

> **Important**
>
> Une fois l'adhésion annulée, vous ne pourrez plus consulter l'historique des dossiers. Les annulations ont lieu à la fin du cycle de facturation. Si vous annulez au cours du mois, votre abonnement sera disponible jusqu'à la fin du mois. Toute ressource ou enquête qui est `Active` ou `ready to close` sera interrompue lors de l'annulation définitive de l'adhésion à la fin du cycle de facturation.

> **Important**
>
> Si vous vous réabonnez au service, un nouvel abonnement sera créé et les ressources relatives aux dossiers qui existaient dans le cadre de l'adhésion précédente ne seront accessibles que si vous les avez téléchargées avant l'annulation.

Une fois l'adhésion annulée, tous les membres de l'équipe de réponse aux incidents d'adhésion sont informés par e-mail.

> **Important**
>
> Si vous avez créé un abonnement à l'aide d'un compte d'administrateur délégué et que vous utilisez le AWS Organizations API pour supprimer la désignation d'administrateur délégué du compte, l'adhésion sera résiliée immédiatement.

Balisage des ressources AWS de réponse aux incidents de sécurité

Une balise est une étiquette de métadonnées que vous attribuez ou que vous AWS attribuez à une AWS ressource. Chaque balise se compose d'une clé et d'une valeur. Pour les balises que vous affectez, vous définissez la clé et la valeur. Par exemple, vous pouvez définir la clé sur `stage` et la valeur pour une ressource sur `test`.

Les balises vous permettent d'effectuer les actions suivantes :

- Identifiez et organisez vos AWS ressources. Beaucoup Services AWS prennent en charge le balisage. Vous pouvez donc attribuer le même tag aux ressources provenant de différents services pour indiquer que les ressources sont liées.
- Suivez vos AWS coûts. Vous activez ces balises sur le AWS Billing tableau de bord. AWS utilise les balises pour classer vos coûts et vous fournir un rapport mensuel de répartition des coûts. Pour plus d'informations, consultez la section Utiliser les balises de répartition des coûts dans le Guide AWS de l'utilisateur de facturation.
- Contrôlez l'accès à vos AWS ressources. Pour plus d'informations, consultez la section Contrôle de l'accès à l'aide de balises dans le Guide de IAM l'utilisateur.

Reportez-vous à la APIréférence relative à la réponse aux incidents de AWS sécurité pour le balisage.

Utilisation AWS CloudShell pour travailler avec AWS Security Incident Response

AWS CloudShell est un shell pré-authentifié basé sur un navigateur que vous pouvez lancer directement depuis le. AWS Management Console Vous pouvez exécuter des AWS CLI commandes sur des AWS services (y compris AWS Security Incident Response) à l'aide de votre shell préféré (Bash PowerShell ou Z shell). Et vous pouvez le faire sans télécharger ou installer des outils de ligne de commande.

Vous lancez AWS CloudShell à partir de AWS Management Console, et les AWS informations d'identification que vous avez utilisées pour vous connecter à la console sont automatiquement disponibles dans une nouvelle session shell. Cette pré-authentification des AWS CloudShell utilisateurs vous permet d'ignorer la configuration des informations d'identification lorsque vous interagissez avec AWS des services tels que Security Incident Response à l'aide de la AWS CLI version 2 (préinstallée sur l'environnement informatique du shell).

Table des matières

Obtention IAM d'autorisations pour AWS CloudShell

À l'aide des ressources de gestion des accès fournies par AWS Identity and Access Management, les administrateurs peuvent accorder des autorisations aux IAM utilisateurs afin qu'ils puissent accéder aux fonctionnalités de l'environnement AWS CloudShell et les utiliser.

Le moyen le plus rapide pour un administrateur d'accorder l'accès aux utilisateurs est d'utiliser une politique AWS gérée. Une politique gérée par AWS est une politique autonome qui est créée et gérée par AWS. La politique AWS gérée suivante pour CloudShell peut être attachée aux IAM identités :

- `AWSCloudShellFullAccess`: accorde l'autorisation d'utilisation AWS CloudShell avec un accès complet à toutes les fonctionnalités.

Si vous souhaitez limiter l'étendue des actions qu'un IAM utilisateur peut effectuer AWS CloudShell, vous pouvez créer une politique personnalisée qui utilise la stratégie `AWSCloudShellFullAccess` gérée comme modèle. Pour plus d'informations sur la limitation des actions disponibles pour

les utilisateurs dans CloudShell, consultez la section Gestion de l' AWS CloudShell accès et de l'utilisation à l'aide de IAM politiques dans le Guide de AWS CloudShell l'utilisateur.

> **Note**
>
> Votre IAM identité nécessite également une politique autorisant le Service d'intervention en cas d'incident de sécurité à passer des appels.

Interaction avec la réponse aux incidents de sécurité à l'aide de AWS CloudShell

Après le lancement AWS CloudShell depuis le AWS Management Console, vous pouvez immédiatement commencer à interagir avec Security Incident Response à l'aide de l'interface de ligne de commande.

> **Note**
>
> Lorsque vous AWS CLI l'utilisez AWS CloudShell, vous n'avez pas besoin de télécharger ou d'installer de ressources supplémentaires. De plus, comme vous êtes déjà authentifié dans le shell, vous n'avez pas besoin de configurer les informations d'identification avant d'effectuer des appels.

Travailler avec les incidents de sécurité AWS CloudShell et y répondre

- À partir de AWS Management Console, vous pouvez lancer CloudShell en choisissant les options suivantes disponibles dans la barre de navigation :
  - Choisissez l' CloudShell icône.
  - Commencez à taper « cloudshell » dans le champ de recherche, puis choisissez l' CloudShelloption.

Enregistrement des API appels de réponse aux incidents de AWS sécurité à l'aide de AWS CloudTrail

AWS La réponse aux incidents de sécurité est intégrée à un service qui fournit un enregistrement des actions entreprises par un utilisateur, un rôle ou un AWS service dans le cadre de la réponse aux incidents de sécurité. AWS CloudTrail CloudTrail capture tous les API appels à la réponse aux incidents de sécurité sous forme d'événements. Les appels capturés incluent des appels provenant de la console de réponse aux incidents de sécurité et des appels de code destinés aux API opérations de réponse aux incidents de sécurité. Si vous créez un suivi, vous pouvez activer la diffusion continue d' CloudTrail événements vers un compartiment Amazon S3, y compris des événements pour la réponse aux incidents de sécurité. 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 Security Incident Response, l'adresse IP à partir de laquelle la demande a été faite, qui a fait la demande, quand elle a été faite et des informations supplémentaires.

Pour en savoir plus CloudTrail, consultez le guide de AWS CloudTrail l'utilisateur.

Informations de réponse aux incidents de sécurité dans CloudTrail

CloudTrail est activé sur votre compte Compte AWS lorsque vous créez le compte. Lorsqu'une activité se produit dans Security Incident Response, 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 Compte AWS. Pour plus d'informations, consultez la section Affichage des événements avec l'historique des CloudTrail événements.

Pour un enregistrement continu des événements de vos 90 Compte AWS derniers jours, créez un magasin de données sur les événements de Trail ou CloudTrailLake.

CloudTrail sentiers

Un suivi permet CloudTrail de fournir des fichiers journaux à un compartiment Amazon S3. Tous les sentiers créés à l'aide du AWS Management Console sont multirégionaux. Vous ne pouvez créer un journal de suivi en une ou plusieurs régions à l'aide de l' AWS CLI. Il est recommandé

de créer un parcours multirégional, car vous capturez l'activité dans l'ensemble Régions AWS de votre compte. Si vous créez un journal de suivi pour une seule région, il convient de n'afficher que les événements enregistrés dans le journal de suivi pour une seule région Région AWS. Pour plus d'informations sur les journaux de suivi, consultez Créez un journal de suivi dans vos Compte AWS et Création d'un journal de suivi pour une organisation dans le AWS CloudTrail Guide de l'utilisateur.

Vous pouvez envoyer une copie de vos événements de gestion en cours dans votre compartiment Amazon S3 gratuitement CloudTrail en créant un journal. Toutefois, des frais de stockage Amazon S3 sont facturés. Pour plus d'informations sur la CloudTrail tarification, consultez la section AWS CloudTrail Tarification. Pour obtenir des informations sur la tarification Amazon S3, consultez Tarification Amazon S3.

CloudTrail Stockages de données sur les événements du lac

CloudTrail Lake vous permet d'exécuter SQL des requêtes basées sur vos événements. CloudTrail Lake convertit les événements existants au JSON format basé sur les lignes au ORC format Apache. ORCest un format de stockage en colonnes optimisé pour une extraction rapide des données. Les événements sont agrégés dans des magasins de données d'événement. Ceux-ci constituent des collections immuables d'événements basées sur des critères que vous sélectionnez en appliquant des sélecteurs d'événements avancés. Les sélecteurs que vous appliquez à un magasin de données d'événement contrôlent les événements qui persistent et que vous pouvez interroger. Pour plus d'informations sur CloudTrail Lake, consultez la section Travailler avec AWS CloudTrail Lake dans le guide de AWS CloudTrail l'utilisateur.

CloudTrail Les stockages et requêtes de données sur les événements de Lake entraînent des coûts. Lorsque vous créez un magasin de données d'événement, vous choisissez l'option de tarification que vous voulez utiliser pour le magasin de données d'événement. L'option de tarification détermine le coût d'ingestion et de stockage des événements, ainsi que les périodes de conservation par défaut et maximale pour le magasin de données d'événement. Pour plus d'informations sur la CloudTrail tarification, consultez la section AWS CloudTrail Tarification.

Toutes les actions de réponse aux incidents de sécurité sont enregistrées CloudTrail et documentées dans la APIréférence de réponse aux incidents de AWS sécurité. Par exemple, les appels au `CreateMembership` `CreateCase` et les `UpdateCase` 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 de l'utilisateur root ou AWS 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 plus d'informations, consultez l'CloudTrail userIdentityélément.

Comprendre les entrées du fichier journal de réponse aux incidents 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 API appels publics, ils n'apparaissent donc pas dans un ordre spécifique.

L'exemple suivant montre une entrée de CloudTrail journal illustrant l' CreateCase action.


```
{
    "eventVersion": "1.09",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AROA00000000000000000:user",
        "arn": "arn:aws:sts::123412341234:assumed-role/Admin/user",
        "accountId": "123412341234",
        "accessKeyId": "****",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AROA00000000000000000",
                "arn": "arn:aws:iam::123412341234:role/Admin",
                "accountId": "123412341234",
                "userName": "Admin"
            },
            "attributes": {
                "creationDate": "2024-10-13T06:32:53Z",
                "mfaAuthenticated": "false"
```

```
            }
        }
    },
    "eventTime": "2024-10-13T06:40:45Z",
    "eventSource": "security-ir.amazonaws.com",
    "eventName": "CreateCase",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "1.2.3.4",
    "userAgent": "aws-cli/2.17.23 md/awscrt#0.20.11 ua/2.0 os/macos#23.6.0 md/
arch#x86_64 lang/python#3.11.9 md/pyimpl#CPython cfg/retry-mode#standard md/
installer#exe md/prompt#off md/command#security-ir.create-case",
    "requestParameters": {
        "impactedServices": [
            "Amazon GuardDuty"
        ],
        "impactedAccounts": [],
        "clientToken": "testToken112345679",
        "resolverType": "Self",
        "description": "***",
        "engagementType": "Investigation",
        "watchers": [
            {
                "email": "***",
                "name": "***",
                "jobTitle": "***"
            }
        ],
        "membershipId": "m-r1abcdabcd",
        "title": "***",
        "impactedAwsRegions": [
            {
                "region": "ap-southeast-1"
            }
        ],
        "reportedIncidentStartDate": 1711553521,
        "threatActorIpAddresses": [
            {
                "ipAddress": "***",
                "userAgent": "browser"
            }
        ]
    },
    "responseElements": {
        "caseId": "0000000001"
```

```
    },
    "requestID": "2db4b08d-94a9-457a-9474-5892e6c8191f",
    "eventID": "b3fa3990-db82-43be-b120-c81262cc2f19",
    "readOnly": false,
    "resources": [
        {
            "accountId": "123412341234",
            "type": "AWS::SecurityResponder::Case",
            "ARN": "arn:aws:security-ir:us-east-1:123412341234:case/*"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "123412341234",
    "eventCategory": "Management"
}
```

Gérer les comptes de réponse aux incidents de AWS sécurité avec AWS Organizations

AWS La réponse aux incidents de sécurité est intégrée à AWS Organizations. Le compte AWS Organizations de gestion de l'organisation peut désigner un compte en tant qu'administrateur délégué pour la réponse aux incidents AWS de sécurité. Cette action active AWS la réponse aux incidents de sécurité en tant que service fiable dans AWS Organizations. Pour plus d'informations sur la manière dont ces autorisations sont accordées, consultez la section Utilisation AWS Organizations avec d'autres AWS services.

Les sections suivantes vous expliqueront les différentes tâches que vous pouvez effectuer en tant qu'administrateur délégué de réponse aux incidents de sécurité.

Table des matières

Considérations et recommandations relatives à l'utilisation AWS de Security Incident Response avec AWS Organizations

Les considérations et recommandations suivantes peuvent vous aider à comprendre le fonctionnement d'un compte administrateur délégué pour la réponse aux incidents de sécurité dans le cadre de la réponse aux incidents AWS de sécurité :

Un compte administrateur délégué pour la réponse aux incidents de sécurité est régional.

> Le compte administrateur délégué de la réponse aux incidents de sécurité et les comptes membres doivent être ajoutés via AWS Organizations.

Compte d'administrateur délégué pour la réponse aux incidents de AWS sécurité.

Vous pouvez désigner un compte membre comme compte administrateur délégué de la réponse aux incidents de sécurité. Par exemple, si vous désignez un compte de membre *111122223333* dans*Europe (Ireland)*, vous ne pouvez pas désigner un autre compte de membre *555555555555* dans*Canada (Central)*. Vous devez utiliser le même compte que le compte administrateur délégué de la réponse aux incidents de sécurité dans toutes les autres régions.

Il n'est pas recommandé de définir la direction de votre organisation en tant que compte administrateur délégué de la réponse aux incidents de sécurité.

La direction de votre organisation peut être le compte administrateur délégué de la réponse aux incidents de sécurité. Cependant, les bonnes pratiques de sécurité AWS suivent le principe du moindre privilège et ne recommandent pas cette configuration.

La suppression d'un compte administrateur délégué pour la réponse aux incidents de sécurité d'un abonnement en ligne annule immédiatement l'abonnement.

Si vous supprimez un compte administrateur délégué de réponse aux incidents de AWS sécurité, Security Incident Response supprime tous les comptes membres associés à ce compte d'administrateur délégué de réponse aux incidents de sécurité. AWS La réponse aux incidents de sécurité ne sera plus activée pour tous ces comptes membres.

Permettre un accès fiable pour AWS Account Management

L'activation d'un accès sécurisé pour la réponse aux incidents de AWS sécurité permet à l'administrateur délégué du compte de gestion de modifier les informations et les métadonnées (par exemple, les coordonnées principales ou secondaires) spécifiques à chaque compte membre dans AWS Organizations.

Utilisez la procédure suivante pour activer un accès sécurisé pour AWS la réponse aux incidents de sécurité dans votre organisation.

Autorisations minimales

Pour effectuer ces tâches, vous devez satisfaire aux exigences suivantes :

- Vous ne pouvez effectuer cette opération qu'à partir du compte de gestion de l'organisation.

- Toutes les fonctions doivent être activées pour votre organisation.

Console

Pour permettre un accès fiable pour la réponse aux incidents AWS de sécurité

1. Connectez-vous à la console AWS Organizations. Vous devez vous connecter en tant qu'IAMutilisateur, assumer un IAM rôle ou vous connecter en tant qu'utilisateur root (ce n'est pas recommandé) dans le compte de gestion de l'organisation.
2. Choisissez Services dans le volet de navigation.
3. Choisissez AWS Security Incident Response dans la liste des services.
4. Choisissez Enable trusted access (Activer l'accès approuvé).
5. Dans la boîte de dialogue Activer l'accès sécurisé pour AWS la réponse aux incidents de sécurité, tapez enable pour le confirmer, puis choisissez Activer l'accès sécurisé.

API/CLI

Pour permettre un accès sécurisé pour AWS Account Management

Après avoir exécuté la commande suivante, vous pouvez utiliser les informations d'identification du compte de gestion de l'organisation pour appeler les API opérations de gestion des comptes qui utilisent le `--accountId` paramètre pour référencer les comptes des membres d'une organisation.

- AWS CLI: enable-aws-service-access

  L'exemple suivant active un accès sécurisé pour AWS la réponse aux incidents de sécurité dans l'organisation du compte appelant.

  ```
  $ aws organizations enable-aws-service-access \
                                        --service-principal security-
  ir.amazonaws.com
  ```

  Cette commande ne produit aucune sortie si elle réussit.

Autorisations requises pour désigner un compte administrateur délégué pour la réponse aux incidents de sécurité

Vous pouvez choisir de configurer votre adhésion à AWS Security Incident Response à l'aide d'un administrateur délégué pour AWS Organizations. Pour plus d'informations sur la manière dont ces autorisations sont accordées, consultez la section Utilisation AWS Organizations avec d'autres AWS services.

> **Note**
>
> AWS La réponse aux incidents de sécurité active automatiquement la relation AWS Organizations de confiance lors de l'utilisation de la console pour la configuration et la gestion. Si vous utilisez leCLI/SDK, vous devez l'activer manuellement en utilisant le EnableAWSService Access API to trust`security-ir.amazonaws.com`.

En tant que AWS Organizations responsable, avant de désigner le compte administrateur délégué de réponse aux incidents de sécurité pour votre organisation, vérifiez que vous pouvez effectuer les actions de réponse aux incidents de AWS sécurité suivantes : `sir:CreateMembership` et`sir:UpdateMembership`. Ces actions vous permettent de désigner le compte administrateur délégué de réponse aux incidents de sécurité pour votre organisation en utilisant AWS Security Incident Response. Vous devez également vous assurer que vous êtes autorisé à effectuer les AWS Organizations actions qui vous aident à récupérer des informations sur votre organisation.

Pour accorder ces autorisations, incluez la déclaration suivante dans une AWS Identity and Access Management (IAM) politique de votre compte :

```
{
    "Sid": "PermissionsForSIRAdmin",
    "Effect": "Allow",
    "Action": [
        "security-ir:CreateMembership",
        "security-ir:UpdateMembership",
        "organizations:EnableAWSServiceAccess",
        "organizations:RegisterDelegatedAdministrator",
        "organizations:ListDelegatedAdministrators",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:DescribeOrganizationalUnit",
```

```
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:ListAccounts"
    ],
    "Resource": "*"
}
```

Si vous souhaitez désigner votre AWS Organizations direction comme compte administrateur délégué de la réponse aux incidents de sécurité, votre compte aura également besoin de l'IAMaction suivante :`CreateServiceLinkedRole`. Cette action vous permet d'initialiser la réponse aux incidents AWS de sécurité pour la direction. Cependant, vérifiez Considérations et recommandations relatives à l'utilisation AWS de Security Incident Response avec AWS Organizations avant de procéder à l'ajout des autorisations.

Pour continuer à désigner la direction en tant que compte administrateur délégué de la réponse aux incidents de sécurité, ajoutez la déclaration suivante à la IAM politique et *111122223333* remplacez-la par l' Compte AWS ID de la direction de votre organisation :

```
{
 "Sid": "PermissionsToEnablesir"
 "Effect": "Allow",
 "Action": [
  "iam:CreateServiceLinkedRole"
 ],
 "Resource": "arn:aws:iam::111122223333:role/aws-service-role/security-
ir.amazonaws.com/AWSServiceRoleForAmazonsir",
 "Condition": {
  "StringLike": {
   "iam:AWSServiceName": "security-ir.amazonaws.com"
  }
 }
}
```

Désignation d'un administrateur délégué pour la réponse aux incidents AWS de sécurité

Cette section décrit les étapes à suivre pour désigner un administrateur délégué au sein de l'organisation AWS Security Incident Response.

En tant que responsable de l' AWS organisation, assurez-vous de lire attentivement le mode de fonctionnement Considérations et recommandations d'un compte administrateur délégué pour la réponse aux incidents de sécurité. Avant de continuer, assurez-vous que vous avezAutorisations requises pour désigner un compte administrateur délégué pour la réponse aux incidents de sécurité.

Choisissez une méthode d'accès préférée pour désigner un compte administrateur délégué de réponse aux incidents de sécurité pour votre organisation. Seule une direction peut effectuer cette étape.

Console

1. Ouvrez la console Security Incident Response à l'adresse https://console.aws.amazon.com/security-ir/

   Pour vous connecter, utilisez les informations d'identification de gestion de votre AWS Organizations organisation.
2. À l'aide du Région AWS sélecteur situé dans le coin supérieur droit de la page, sélectionnez la région dans laquelle vous souhaitez désigner le compte administrateur délégué de réponse aux incidents de sécurité pour votre organisation.
3. Suivez l'assistant de configuration pour créer votre adhésion, y compris le compte d'administrateur délégué.

API/CLI

- CreateMembership Exécuté en utilisant les informations d'identification Compte AWS de la direction de l'organisation.
  - Vous pouvez également utiliser AWS Command Line Interface pour cela. La AWS CLI commande suivante désigne un compte administrateur délégué pour la réponse aux incidents de sécurité. Les options de chaîne disponibles pour configurer votre adhésion sont les suivantes :

```
{
  "customerAccountId": "stringstring",
  "membershipName": "stringstring",
  "customerType": "Standalone",
  "organizationMetadata": {
    "organizationId": "string",
    "managementAccountId": "stringstring",
```

```
      "delegatedAdministrators": [
        "stringstring"
      ]
    },
    "membershipAccountsConfigurations": {
      "autoEnableAllAccounts": true,
      "organizationalUnits": [
        "string"
      ]
    },
    "incidentResponseTeam": [
      {
        "name": "string",
        "jobTitle": "stringstring",
        "email": "stringstring"
      }
    ],
    "internalIdentifier": "string",
    "membershipId": "stringstring",
    "optInFeatures": [
      {
        "featureName": "RuleForwarding",
        "isEnabled": true
      }
    ]
  }
```

Si AWS la réponse aux incidents de sécurité n'est pas activée pour votre compte d'administrateur délégué pour la réponse aux incidents de sécurité, il ne sera pas en mesure de prendre des mesures. Si ce n'est pas déjà fait, assurez-vous d'activer AWS la réponse aux incidents de sécurité pour le compte administrateur délégué de réponse aux incidents de sécurité nouvellement désigné.

Ajouter des membres à la réponse aux incidents de AWS sécurité

Il existe une relation individuelle avec AWS Organizations votre adhésion à AWS Security Incident Response. Au fur et à mesure que des comptes seront ajoutés (ou supprimés) dans vos Organisations, cela se reflétera dans les comptes couverts par votre adhésion à AWS Security Incident Response.

Pour ajouter un compte à votre adhésion, suivez l'une des options de gestion des comptes dans une organisation avec AWS Organizations.

Supprimer des membres de la réponse aux incidents de AWS sécurité

Pour supprimer un compte de votre adhésion, suivez les procédures de suppression d'un compte membre d'une organisation.

Résolution des problèmes

Lorsque vous rencontrez des problèmes liés à l'exécution d'une action spécifique à AWS la réponse aux incidents de sécurité, consultez les rubriques de cette section.

An ERROR est le statut d'une opération indiquant une défaillance dans certaines ou dans toutes les opérations. Vous pouvez également recevoir des avertissements lorsqu'un problème survient mais que la tâche est toujours terminée.

Table des matières

Problèmes

Ne pas envoyer les demandes depuis le bon contexte.

Tous les appels à AWS Security Incident Response APIs doivent provenir IAM d'un administrateur délégué du service ou du compte de membre. Assurez-vous que vous utilisez le bon IAM directeur dans le Compte AWS compte d'administrateur délégué ou de membre chargé de AWS la réponse aux incidents de sécurité de votre organisation.

Erreurs

AccessDeniedException

Vous ne disposez pas d’un accès suffisant pour effectuer cette action.

Contactez votre AWS administrateur pour vous assurer que vous êtes autorisé à assumer un IAM rôle dans votre compte d'administrateur délégué ou de membre chargé de la réponse aux incidents de AWS sécurité. Vérifiez également que le rôle dispose d'une IAM politique qui autorise l'action demandée. Pour plus d'informations, consultez AWS la section Réponse aux incidents de sécurité IAM.

ConflictException

La demande provoque un état incohérent.

Vérifiez que tous les noms de fichiers joints aux dossiers ou les membres de l'équipe d'intervention par défaut que vous avez spécifiés sont uniques. Vérifiez également que votre adhésion au service AWS Security Incident Response n'est pas déjà configurée. Ouvrez la console Security Incident Response sur https://console.aws.amazon.com/security-ir/ et accédez à`Membership Details`.

InternalServerException

Une erreur inattendue s'est produite lors du traitement de la demande. Veuillez réessayer dans quelques minutes. Si le problème persiste, soulevez un dossier auprès de AWS Support.

ResourceNotFoundException

La demande fait référence à une ressource qui n'existe pas.

Une ou plusieurs des ressources spécifiées dans votre demande n'existent pas. Veuillez vérifier que toutes les ressources ARNs indiquées IDs sont correctes. Cela s'applique au compte AWS Organizations IDs, aux IAM rôlesIDs, aux adhésions, aux cas, aux membres de l'équipe d'intervention, aux cas, aux intervenants, aux pièces jointes aux dossiers et aux commentaires sur les cas.

ThrottlingException

La demande a été refusée suite à une limitation des demandes.

Trop de demandes ont été faites par votre IAM directeur à cette API fonction au cours d'une période spécifiée. Patientez une minute et réessayez. Si le problème persiste, pensez à implémenter un algorithme de réduction exponentielle et de nouvelle tentative.

ValidationException

L'entrée ne satisfait pas les contraintes spécifiées par un Service AWS.

Un ou plusieurs champs de données de votre demande ne répondaient pas aux exigences de validation et/ou de combinaison logique. Vérifiez que toutes les ressources sont ARNs complètes et que les valeurs du texte respectent les contraintes de taille et de format énoncées dans le Guide de API référence pour la réponse aux incidents de AWS sécurité. Vérifiez également que toutes les mises à jour de valeurs sont autorisées. Par exemple, il n'est pas possible de passer d'un dossier AWS pris en charge à un dossier autogéré.

AWS Support

Si vous avez besoin d'une assistance supplémentaire, contactez le AWS Support centre à des fins de résolution des problèmes. Veuillez disposer des informations suivantes :

- Celui Région AWS que tu as utilisé
- L' Compte AWS identifiant de l'adhésion
- Votre contenu source, le cas échéant et disponible
- Tout autre détail sur le problème susceptible de faciliter le dépannage

Sécurité

Table des matières

Protection des données dans le cadre AWS de la réponse aux incidents de sécurité

Table des matières

Le modèle de responsabilité AWS partagée s'applique à la protection des données pour le service AWS Security Incident Response. Comme décrit dans ce modèle, AWS est responsable de la protection de l'infrastructure qui exécute les services proposés dans le AWS cloud. La gestion du contrôle de votre contenu hébergé sur cette infrastructure relève de votre responsabilité. Vous êtes également responsable de la configuration de la sécurité et des tâches de gestion des AWS services que vous utilisez. Pour plus d'informations sur la confidentialité des données, consultez la section Confidentialité des données FAQ. Pour plus d'informations sur la protection des données en Europe,

consultez le modèle de responsabilitéAWS partagée et le billet de GDPR blog sur le blog sur la AWS sécurité.

À des fins de protection des données, les meilleures pratiques de AWS sécurité stipulent que vous devez protéger les informations d'identification des AWS comptes et configurer les utilisateurs individuels avec AWS IAM Identity Center ou AWS Identity and Access Management (IAM). De cette façon, chaque utilisateur ne reçoit que les autorisations nécessaires pour accomplir ses tâches. Nous vous recommandons également de sécuriser vos données comme indiqué ci-dessous :

- Utilisez l'authentification multifactorielle (MFA) pour chaque compte.
- UtilisezSSL/TLSpour communiquer avec les AWS ressources. Nous avons besoin de la TLS version 1.2 et recommandons la TLS version 1.3.
- Configuration API et journalisation de l'activité des utilisateurs avec AWS CloudTrail.
- Utilisez des solutions de AWS chiffrement, ainsi que tous les contrôles de sécurité par défaut au sein AWS des services.
- FIPSLe 140-3 n'est actuellement pas pris en charge par le service.

Vous ne devez jamais placer d'informations confidentielles ou sensibles, telles que vos adresses e-mail, dans des balises ou des champs de texte libres tels que le champ Nom. Cela inclut lorsque vous travaillez avec le AWS Support ou d'autres AWS services à l'aide de la consoleAPI, AWS CLI, ou AWS SDKs. Toutes les données que vous saisissez dans des balises ou des champs de texte libre utilisés pour les noms peuvent être utilisées pour les journaux de facturation ou de diagnostic. Si vous fournissez un URL à un serveur externe, nous vous recommandons vivement de ne pas y inclure d'informations d'identification URL pour valider votre demande auprès de ce serveur.

Chiffrement des données

Table des matières

Chiffrement au repos

Les données sont chiffrées au repos à l'aide d'un chiffrement transparent côté serveur. Cela réduit la lourdeur opérationnelle et la complexité induites par la protection des données sensibles. Le

chiffrement au repos vous permet de créer des applications sensibles en matière de sécurité qui sont conformes aux exigences réglementaires et de chiffrement.

Chiffrement en transit

Les données collectées et consultées par AWS Security Incident Response se font exclusivement via un canal protégé par Transport Layer Security (TLS).

Gestion des clés

AWS Security Incident Response met en œuvre des intégrations AWS KMS afin de chiffrer au repos les données relatives aux dossiers et aux pièces jointes.

AWS Security Incident Response ne prend pas en charge les clés gérées par le client.

Confidentialité du trafic inter-réseaux

Trafic entre les clients de service et sur site et les applications

Vous avez deux options de connectivité entre votre réseau privé et AWS :

- Une AWS Site-to-Site VPN connexion. Pour plus d'informations, consultez Présentation d' AWS Site-to-Site VPN dans le Guide de l'utilisateur AWS Site-to-Site VPN .
- Une AWS Direct Connect connexion. Pour plus d'informations, consultez Présentation d' AWS Direct Connect dans le Guide de l'utilisateur AWS Direct Connect .

L'accès à AWS la réponse aux incidents de sécurité via le réseau se fait via la AWS publicationAPIs. Les clients doivent prendre en charge le protocole Transport Layer Security (TLS) 1.2. Nous recommandons la TLS version 1.3. Les clients doivent également prendre en charge les suites de chiffrement dotées de Perfect Forward Secrecy (PFS), telles que Ephemeral Diffie-Hellman () ou Elliptic Curve Diffie-Hellman Ephemeral (DHE). ECDHE La plupart des systèmes modernes tels que Java 7 et les versions ultérieures prennent en charge ces modes. De plus, vous devez signer les demandes à l'aide d'un ID de clé d'accès et d’une clé d'accès secrète, associées à un mandataire IAM. Vous pouvez également utiliser le service AWS Security Token Service (STS) afin de générer des informations d'identification de sécurité temporaires pour signer les demandes.

Trafic entre des ressources AWS dans la même Région

Un point de terminaison Amazon Virtual Private Cloud (AmazonVPC) pour AWS la réponse aux incidents de sécurité est une entité logique au sein d'un VPC qui permet la connectivité uniquement à

AWS la réponse aux incidents de sécurité. Amazon VPC achemine les demandes vers AWS Security Incident Response et redirige les réponses vers leVPC. Pour plus d'informations, consultez la section VPCendpoints dans le guide de l'VPCutilisateur Amazon. Pour des exemples de politiques que vous pouvez utiliser pour contrôler l'accès depuis les VPC points de terminaison, consultez la section Utilisation de IAM politiques pour contrôler l'accès à DynamoDB.

> **Note**
>
> Les VPC points de terminaison Amazon ne sont pas accessibles via AWS Site-to-Site VPN ou AWS Direct Connect.

Gestion de l’identité et des accès

AWS Identity and Access Management (IAM) est un AWS service qui aide un administrateur à contrôler l'accès aux AWS ressources. IAMles administrateurs contrôlent les principaux authentifiés (connectés) et autorisés (autorisés) à utiliser les ressources de réponse aux incidents AWS de sécurité. IAMest un AWS service que vous pouvez utiliser sans frais supplémentaires.

Table des matières

Public

La façon dont vous utilisez AWS Identity and Access Management (IAM) varie en fonction du travail que vous effectuez dans AWS Security Incident Response.

Administrateurs de sécurité

Il est suggéré à ces utilisateurs d'utiliser la politique AWSSecurityIncidentResponseFullAccessgérée pour s'assurer qu'ils disposent d'un accès en lecture et en écriture aux ressources relatives aux membres et aux dossiers.

Case Watchers

Ces personnes n'ont pas un accès autorisé à tous les cas, mais aux cas individuels pour lesquels vous accordez une autorisation explicite.

Membres de l'équipe de réponse aux incidents

Les membres de l'équipe peuvent bénéficier à la fois d'une adhésion complète et d'un accès aux dossiers. Il est recommandé que toutes les personnes ne soient pas habilitées à prendre des mesures en matière d'adhésion au service, mais qu'elles aient accès à tous les dossiers créés et gérés par le biais du service. Pour plus d'informations, reportez-vous à la section Politiques gérées pour la réponse aux incidents de AWS sécurité.

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 AWS compte, en tant qu'IAMutilisateur ou en assumant un IAM rôle.

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 Les utilisateurs d'IAMIdentity Center (Identity Center), 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 aura précédemment configuré une fédération d'identités avec des rôles IAM. 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 à la console AWS de gestion ou au portail AWS d'accès. Pour plus d'informations sur la connexion à AWS, consultez Comment vous connecter à votre AWS compte dans le Guide de l'utilisateur de AWS connexion.

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 la section Signature des AWS API demandes dans le guide de IAM l'utilisateur.

Quelle que soit la méthode d'authentification que vous utilisez, il peut vous être demandé de 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 Authentification multifactorielle dans le guide de l'utilisateur d'AWS IAMIdentity Center et Utilisation de l'authentification multifactorielle (MFA) AWS dans le guide de l'IAMutilisateur.

AWS utilisateur root du compte

Lorsque vous créez un AWS compte, vous commencez par utiliser une seule identité de connexion qui donne un accès complet à tous les AWS services et ressources du compte. Cette identité est appelée utilisateur root du AWS compte et est accessible en vous connectant avec l'adresse 8 et le mot de passe que vous avez utilisés pour créer le compte. N'utilisez jamais l'utilisateur root pour vos tâches quotidiennes et prenez des mesures pour protéger vos informations d'identification d'utilisateur root. Utilisez-les uniquement pour effectuer des 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 utilisateur root dans le guide de IAM l'utilisateur.

Identité fédérée

Il est recommandé d'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 aux AWS services à l'aide d'informations d'identification temporaires.

Une identité fédérée est un utilisateur de l'annuaire des utilisateurs de votre entreprise, un fournisseur d'identité Web, le AWS Directory Service, le répertoire Identity Center ou tout utilisateur qui accède AWS aux services à l'aide des informations d'identification fournies par le biais d'une source d'identité. Lorsque des identités fédérées accèdent à AWS des comptes, elles assument des rôles, qui fournissent des informations d'identification temporaires.

Pour une gestion centralisée des accès, nous vous recommandons AWS IAM d'utiliser 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 sur tous vos AWS comptes et applications. Pour plus d'informations sur IAM Identity Center, consultez Qu'est-ce qu'IAMIdentity Center ? dans le guide de l'utilisateur d'AWS IAMIdentity Center.

IAMutilisateurs et groupes

Un IAMutilisateur est une identité au sein de votre AWS compte qui possède des autorisations spécifiques pour une seule personne ou une seule application. Nous vous recommandons de vous appuyer sur des informations d'identification temporaires plutôt que de créer des IAM utilisateurs dotés d'informations d'identification à long terme, telles que des mots de passe et des clés d'accès. Si vous avez un cas d'utilisation spécifique qui nécessite des informations d'identification à long terme auprès des IAM utilisateurs, nous vous recommandons de faire pivoter les clés d'accès. Pour plus d'informations, voir Rotation régulière des clés d'accès pour les cas d'utilisation nécessitant des informations d'identification à long terme dans le Guide de IAM l'utilisateur.

Un IAMgroupe est une identité qui définit un ensemble d'IAMutilisateurs. 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 pouvez nommer un groupe IAMAdminset lui donner les autorisations nécessaires pour administrer IAM des 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, voir Quand créer un IAM utilisateur (au lieu d'un rôle) dans le Guide de IAM l'utilisateur.

IAM Rôles

Un IAMrôle est une identité au sein de votre AWS compte dotée d'autorisations spécifiques. Le concept ressemble à celui d'utilisateur IAM, mais un rôle n'est pas associé à une personne en particulier. Vous pouvez assumer temporairement un IAM rôle dans la console AWS de gestion en changeant de rôle. Vous pouvez assumer un rôle en appelant une AWS API opération AWS CLI or ou en utilisant une option personnaliséeURL. Pour plus d'informations sur les méthodes d'utilisation des rôles, consultez la section Utilisation IAM des rôles dans le Guide de IAM l'utilisateur.

Les rôles IAM avec des informations d'identification temporaires sont utiles dans les cas suivants :

- Accès utilisateur fédéré : pour attribuer des autorisations à une identité fédérée, vous devez créer un rôle et définir des autorisations pour ce rôle. Quand une identité externe s'authentifie, l'identité est associée au rôle et reçoit les autorisations qui sont définies par celui-ci. Pour plus d'informations sur les rôles pour la fédération, voir Création d'un rôle pour un fournisseur d'identité tiers dans le guide de IAM l'utilisateur. Si vous utilisez IAM Identity Center, vous configurez un ensemble d'autorisations. Pour contrôler les accès auxquels vos identités peuvent accéder après leur authentification, IAM Identity Center met en corrélation l'ensemble d'autorisations avec un rôle dans. IAM Pour plus d'informations sur les ensembles d'autorisations, consultez la section Ensembles d'autorisations dans le guide de l'utilisateur d'AWS IAMIdentity Center.
- Autorisations IAM utilisateur temporaires : un IAM utilisateur ou un rôle peut assumer un IAM rôle afin d'obtenir temporairement différentes autorisations pour une tâche spécifique.
- Accès entre comptes : 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. Cependant, avec certains AWS services, 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, voir Accès aux ressources entre comptes IAM dans le guide de l'IAMutilisateur.

- Accès interservices — Certains AWS services utilisent des fonctionnalités d'autres AWS services. Par exemple, lorsque vous effectuez un appel dans un service, il est courant que ce service exécute des applications dans Amazon EC2 ou stocke des objets dans Amazon S3. Un service peut le faire en utilisant les autorisations d'appel du principal, un rôle de service ou un rôle lié au service.
  - Rôle de service — Un rôle de service est un IAMrôle qu'un service assume pour effectuer des actions en votre nom. Un administrateur IAM peut créer, modifier et supprimer une fonction du service à partir de 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.
  - Rôle lié à un service — Un rôle lié à un service est un type de rôle lié à un service. AWS Le service peut endosser le rôle afin d'effectuer une action en votre nom. Les rôles liés au service apparaissent dans votre AWS compte et appartiennent au service. Un administrateur IAM peut consulter, mais ne peut pas modifier les autorisations concernant 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 EC2 instance et qui font AWS CLI des AWS API demandes. Cette solution est préférable au stockage des clés d'accès au sein de l'instance EC2. Pour attribuer un AWS rôle à une EC2 instance et le mettre à la disposition de ses applications, vous devez créer un profil d'instance attaché à l'instance. Un profil d'instance contient le rôle et permet aux programmes qui s'exécutent sur l'instance EC2 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 EC2 instances Amazon dans le Guide de IAM l'utilisateur.

Pour savoir s'il faut utiliser IAM des rôles ou des IAM utilisateurs, voir Quand créer un IAM rôle (au lieu d'un utilisateur) dans le guide de IAM l'utilisateur.

Comment fonctionne la réponse aux incidents de AWS sécurité avec IAM

AWS Identity and Access Management (IAM) est un AWS service qui permet à un administrateur de contrôler en toute sécurité l'accès aux AWS ressources. IAMles administrateurs contrôlent qui peut être authentifié (connecté) et autorisé (autorisé) à utiliser les ressources de réponse aux incidents AWS de sécurité. IAMest un AWS service que vous pouvez utiliser sans frais supplémentaires.

IAMfonctionnalités que vous pouvez utiliser avec AWS Security Incident Response	
IAMfonctionnalité	Harmonisation des services
Politiques basées sur l’identité	Oui
Politiques basées sur les ressources	Non
Actions de politique	Oui
Ressources de politique	Oui
Clés des conditions de politique	Oui (mondial)
ACLs	Non
ABAC(balises dans les politiques)	Oui
Informations d’identification temporaires	Oui
Sessions d'accès transféré (1) FAS	Oui
Fonctions du service	Non
Rôles liés à un service	Oui

Table des matières

Politiques basées sur l'identité pour la réponse aux incidents AWS de sécurité

Les politiques basées sur l'identité sont JSON des documents de politique d'autorisation que vous pouvez joindre à une identité, telle qu'un IAM utilisateur, 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 savoir comment créer une politique basée sur l'identité, consultez la section Création de IAM politiques dans le Guide de l'IAMutilisateur.

Avec les stratégies IAM basées sur l'identité, vous pouvez spécifier des actions et 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 politique basée sur une identité, car celle-ci s'applique à l'utilisateur ou au rôle auquel elle est attachée. Pour en savoir plus sur tous les éléments que vous pouvez utiliser dans une JSON politique, consultez la référence aux éléments de IAM JSON politique dans le Guide de IAM l'utilisateur.

Table des matières

Exemples de politiques basées sur l'identité

Par défaut, les utilisateurs et les rôles ne sont pas autorisés à créer ou à modifier des ressources de réponse aux incidents de AWS sécurité. Ils ne peuvent pas non plus effectuer de tâches à l'aide de la console AWS de gestion, de l'interface de ligne de AWS commande (AWS CLI) ou AWS API. Un IAM administrateur peut créer des IAM politiques pour autoriser les utilisateurs à effectuer des actions sur les ressources dont ils ont besoin. L'administrateur peut ensuite ajouter les IAM politiques aux rôles, et les utilisateurs peuvent assumer les rôles.

Pour savoir comment créer une politique IAM basée sur l'identité à l'aide de ces exemples de documents de JSON stratégie, consultez la section Création de IAM politiques dans le guide de l'IAMutilisateur.

Pour plus de détails sur les actions et les types de ressources définis par AWS Security Incident Response, y compris le ARNs format de chaque type de ressource, voir Actions, ressources et clés de condition pour la réponse aux incidents de AWS sécurité dans la référence d'autorisation du service.

Bonnes pratiques en matière de politiques

Les politiques basées sur l'identité déterminent si quelqu'un peut créer, accéder ou supprimer des ressources de réponse aux incidents AWS de sécurité dans votre compte. Ces actions peuvent

entraîner des frais pour votre AWS compte. 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 AWS compte. Nous vous recommandons de réduire davantage les autorisations en définissant des politiques gérées par le AWS client spécifiques à vos cas d'utilisation. Pour plus d'informations, consultez les politiques AWS gérées ou les politiques AWS gérées pour les fonctions professionnelles dans le Guide de IAM l'utilisateur.

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 du Guide de IAM 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 rédiger une condition de politique pour spécifier que toutes les demandes doivent être envoyées en utilisantSSL. Vous pouvez également utiliser des conditions pour accorder l'accès aux actions de service si elles sont utilisées par le biais d'un AWS service spécifique, tel que AWS CloudFormation. Pour plus d'informations, voir Éléments IAM JSON de politique : Condition dans le guide de IAM l'utilisateur.

Utilisez IAM Access Analyzer 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 soient conformes au langage des IAM politiques (JSON) et IAM aux meilleures pratiques. 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 politiques d'IAMAccess Analyzer dans le guide de IAM l'utilisateur.

Exiger l'authentification multifactorielle (MFA) : si vous avez un scénario qui nécessite l'utilisation d'IAMutilisateurs ou d'un utilisateur root dans votre AWS compte, activez-la MFA pour une sécurité accrue. Pour exiger le MFA moment où les API opérations sont appelées, ajoutez MFA des conditions à vos politiques. Pour plus d'informations, consultez la section Configuration de l'APIaccès MFA protégé dans le Guide de l'IAMutilisateur.

Pour plus d'informations sur les meilleures pratiques en matière de sécuritéIAM, consultez la section Bonnes pratiques en matière de sécurité IAM dans le Guide de IAM l'utilisateur.

Utilisation de la console AWS Security Incident Response

Pour y accéder https://console.aws.amazon.com/security-ir/, vous devez disposer d'un ensemble minimal d'autorisations. Ces autorisations doivent vous permettre de répertorier et de consulter les informations relatives aux ressources de réponse aux incidents de AWS sécurité de votre AWS compte. Si vous créez une politique basée sur l'identité qui est plus restrictive que l'ensemble minimum d'autorisations requis, la console ne fonctionnera pas comme prévu pour les entités (utilisateurs ou rôles) tributaires de cette politique.

Il n'est pas nécessaire d'accorder des autorisations de console minimales aux utilisateurs qui appellent uniquement le AWS CLI ou le AWS API. Au lieu de cela, autorisez uniquement l'accès aux actions correspondant à l'APIopération qu'ils tentent d'effectuer.

Joignez la politique d'accès ou de ReadOnly AWS gestion des incidents de AWS sécurité pour garantir que les utilisateurs et les rôles peuvent utiliser la console de service. Pour plus d'informations, consultez la section Ajouter des autorisations à un utilisateur dans le Guide de IAM l'utilisateur.

Autorisation accordée aux utilisateurs pour afficher leurs propres autorisations

Cet exemple montre comment créer une stratégie qui permet aux utilisateurs IAM d'afficher les stratégies en ligne et gérées attachées à leur identité d'utilisateur. Cette politique inclut les autorisations permettant d'effectuer cette action sur la console ou par programmation à l'aide du AWS CLI ou. AWS API

```
{
"Version": "2012-10-17",
"Statement": [
{
"Sid": "ViewOwnUserInfo",
"Effect": "Allow",
"Action": [
"iam:GetUserPolicy",
"iam:ListGroupsForUser",
"iam:ListAttachedUserPolicies",
"iam:ListUserPolicies",
"iam:GetUser"
],
"Resource": ["arn:AWS:iam::*:user/${AWS:username}"]
```

```
},
{
"Sid": "NavigateInConsole",
"Effect": "Allow",
"Action": [
"iam:GetGroupPolicy",
"iam:GetPolicyVersion",
"iam:GetPolicy",
"iam:ListAttachedGroupPolicies",
"iam:ListGroupPolicies",
"iam:ListPolicyVersions",
"iam:ListPolicies",
"iam:ListUsers"
],
"Resource": "*"
}
]
}
```

Politiques basées sur les ressources dans le cadre de la réponse aux incidents AWS de sécurité

Prend en charge les politiques basées sur les ressources : non

Les politiques basées sur les ressources sont des documents JSON de stratégie que vous attachez à une ressource. Les politiques de confiance dans les IAM rôles et les politiques relatives aux compartiments Amazon S3 sont des exemples de 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 mandataires peuvent inclure des comptes, des utilisateurs, des rôles, des utilisateurs fédérés ou des services AWS .

Pour plus d'informations, reportez-vous à la section Accès aux ressources entre comptes IAM du Guide de IAM l'utilisateur.

Actions politiques pour la réponse aux incidents de AWS sécurité

Support aux actions politiques : Oui

Les administrateurs peuvent utiliser AWS JSON des politiques 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 Action d'une JSON politique décrit les actions que vous pouvez utiliser pour autoriser ou refuser l'accès dans une politique. Les actions de stratégie portent généralement le même nom que l' AWS APIopération associée. Il existe certaines exceptions, telles que les actions avec autorisation uniquement qui n'ont pas d'opération correspondante. API Certaines opérations nécessitent également plusieurs actions dans une politique. Ces actions supplémentaires sont nommées actions dépendantes.

Intégration d’actions dans une politique afin d’accorder l’autorisation d’exécuter les opérations associées.

Pour consulter la liste des actions de réponse aux incidents de AWS sécurité, voir Actions définies par AWS Security Incident Response dans la référence d'autorisation de service.

Les actions de stratégie dans AWS Security Incident Response utilisent le préfixe suivant avant l'action :

AWS Réponse aux incidents de sécurité - identité

Pour indiquer plusieurs actions dans une seule déclaration, séparez-les par des virgules.

« Action » : ["Réponse aux incidents de AWS sécurité -identity:action1", « Réponse aux incidents de sécurité -identity:action2"AWS]

Ressources relatives aux politiques pour Amazon AWS Security Incident Response

Prend en charge les ressources relatives aux politiques : Oui Les administrateurs peuvent utiliser des AWS JSON politiques 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 Resource JSON policy indique le ou les objets auxquels s'applique l'action. Les instructions doivent inclure une ressource ou un NotResource élément. Il est recommandé de spécifier 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 sont pas compatibles avec les autorisations de niveau ressource, telles que les opérations de liste, utilisez un caractère générique (*) afin d’indiquer que l’instruction s’applique à toutes les ressources.

"Resource": "*"

Clés de conditions de politique pour AWS la réponse aux incidents de sécurité

Prend en charge les clés de condition de politique spécifiques au service : Non

Les administrateurs peuvent utiliser AWS JSON des politiques 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 Condition (ou bloc Condition) vous permet de spécifier 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 de condition dans une instruction ou plusieurs clés dans un seul élément de condition, vous les AWS évaluez à l'aide d'une AND opération logique. Si vous spécifiez plusieurs valeurs pour une seule clé de condition, AWS évalue la condition à l'aide d'une opération OR logique. Toutes les conditions doivent être remplies avant que les autorisations associées à l'instruction ne soient accordées.

Vous pouvez aussi utiliser des variables d'espace réservé quand vous spécifiez des conditions. Par exemple, vous pouvez accorder à un utilisateur IAM l'autorisation d'accéder à une ressource uniquement si elle est balisée avec son nom d'utilisateur IAM . Pour plus d'informations, consultez IAMla section Éléments de politique : variables et balises dans le Guide de IAM l'utilisateur.

AWS prend en charge les clés de condition globales et les clés de condition spécifiques au service. Pour voir toutes les clés de condition AWS globales, voir les clés contextuelles de condition AWS globales dans le guide de IAM l'utilisateur.

Listes de contrôle d'accès (ACLs) dans AWS Security Incident Response

Supports ACLs : Non

Les listes de contrôle d'accès (ACLs) contrôlent les principaux (membres du compte, utilisateurs ou rôles) autorisés à accéder à une ressource. ACLssont similaires aux politiques basées sur les ressources, bien qu'elles n'utilisent pas le format du document JSON de stratégie.

Contrôle d'accès basé sur les attributs (ABAC) avec réponse aux incidents AWS de sécurité

Supports ABAC (balises dans les politiques) : Oui

Le contrôle d'accès basé sur les attributs (ABAC) est une stratégie d'autorisation qui définit les autorisations en fonction des attributs. Dans AWS, ces attributs sont appelés balises. Vous pouvez

associer des balises à IAM des entités (utilisateurs ou rôles) et à de nombreuses AWS ressources. Le balisage des entités et des ressources est la première étape deABAC. Vous concevez ensuite des ABAC politiques pour autoriser les opérations lorsque le tag du principal correspond à celui de la ressource à laquelle il essaie d'accéder. ABACest utile dans les environnements qui se développent rapidement et aide dans les situations où la gestion des politiques devient fastidieuse.

Pour contrôler l'accès en fonction des balises, vous devez fournir des informations sur les balises dans l'élément condition d'une politique à l'aide des clés AWS : ResourceTag /key-name, AWS : RequestTag /key-name ou : condition. AWS TagKeys Si un service prend en charge les trois clés de condition pour chaque type de ressource, la valeur est Oui pour le service. Si un service ne prend en charge les trois clés de condition que pour certains types de ressources, la valeur est Partial. Pour plus d'informationsABAC, voir Qu'est-ce que c'est ABAC ? dans le guide de IAM l'utilisateur. Pour consulter un didacticiel présentant les étapes de configurationABAC, voir Utiliser le contrôle d'accès basé sur les attributs (ABAC) dans le guide de l'IAMutilisateur.

Informations d'identification temporaires avec Amazon AWS Security Incident Response

Prend en charge les informations d’identification temporaires : oui

AWS les services ne fonctionnent pas lorsque vous vous connectez à l'aide d'informations d'identification temporaires. Pour plus d'informations, notamment sur les AWS services qui fonctionnent avec des informations d'identification temporaires, consultez la section AWS Services compatibles IAM dans le Guide de IAM l'utilisateur. Vous utilisez des informations d'identification temporaires si vous vous connectez à la console de AWS gestion à l'aide d'une méthode autre que le nom d'utilisateur et le mot de passe. Par exemple, lorsque vous accédez à AWS l'aide du 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 la section Passage à un rôle (console) dans le guide de IAM l'utilisateur.

Vous pouvez créer manuellement des informations d'identification temporaires à l'aide du AWS CLI ou AWS API. Vous pouvez ensuite utiliser ces informations d'identification temporaires pour y accéder AWS. AWS recommande de générer dynamiquement des informations d'identification temporaires au lieu d'utiliser des clés d'accès à long terme. Pour plus d'informations, consultez la section Informations d'identification de sécurité temporaires dans IAM.

Sessions d'accès transmises pour la réponse aux incidents AWS de sécurité

Prend en charge les sessions d'accès transféré (FAS) : Oui

Lorsque vous utilisez un IAM utilisateur ou un rôle pour effectuer des actions AWS, vous êtes considéré comme un mandant. Lorsque vous utilisez certains services, vous pouvez effectuer une action qui déclenche ensuite une autre action dans un autre service. FASutilise les autorisations du principal appelant un AWS service, combinées au AWS service demandeur pour adresser des demandes aux services en aval. FASles demandes ne sont effectuées que lorsqu'un service reçoit une demande qui nécessite des interactions avec d'autres AWS services ou ressources pour être traitée. Dans ce cas, vous devez disposer d'autorisations nécessaires pour effectuer les deux actions. Pour plus de détails sur les politiques relatives FAS aux demandes, consultez la section Transférer les sessions d'accès.

Résolution des problèmes AWS de sécurité, réponse aux incidents, identité et accès

Utilisez les informations suivantes pour vous aider à diagnostiquer et à résoudre les problèmes courants que vous pouvez rencontrer lors de l'utilisation de AWS Security Incident Response etIAM.

Rubriques

- Je ne suis pas autorisé à exécuter une action
- Je ne suis pas autorisé à effectuer iam : PassRole
- Je souhaite autoriser des personnes extérieures à mon AWS compte à accéder à mes ressources de réponse aux incidents de AWS sécurité

Je ne suis pas autorisé à effectuer une action

Si vous recevez une erreur qui indique que vous n'êtes pas autorisé à effectuer une action, vos politiques doivent être mises à jour afin de vous permettre d'effectuer l'action.

L'exemple d'erreur suivant se produit lorsque l'IAMutilisateur de mateojackson essaie d'utiliser la console pour afficher les détails d'une my-example-widget ressource fictive mais ne dispose pas des autorisations fictives AWS Security Incident Response :GetWidget .

L'utilisateur : arn ::iam AWS : :123456789012:user/mateojackson n'est pas autorisé à effectuer : Security Incident Response : on resource : my -example-widget AWS GetWidget

Dans ce cas, la politique de l'utilisateur de mateojackson doit être mise à jour pour autoriser l'accès à la my-example-widget ressource en utilisant l'action AWS Security Incident Response :GetWidget .

Si vous avez besoin d'aide, contactez votre AWS administrateur. Votre administrateur vous a fourni vos informations d'identification de connexion.

Je ne suis pas autorisé à exécuter l'action iam : PassRole si vous recevez un message d'erreur indiquant que vous n'êtes pas autorisé à exécuter l'PassRole action iam :, vos politiques doivent être mises à jour pour vous permettre de transmettre un rôle à AWS Security Incident Response.

Certains AWS services vous permettent de transmettre un rôle existant à ce service au lieu de créer un nouveau rôle de service ou un rôle lié à un service. Pour ce faire, un utilisateur doit disposer des autorisations nécessaires pour transmettre le rôle au service.

L'exemple d'erreur suivant se produit lorsqu'un IAM utilisateur nommé marymajor essaie d'utiliser la console pour effectuer une action dans AWS Security Incident Response. Toutefois, l'action nécessite que le service ait des autorisations accordées par un rôle de service. Mary ne dispose pas des autorisations nécessaires pour transférer le rôle au service.

L'utilisateur : arn ::iam AWS : :123456789012:user/marymajor n'est pas autorisé à exécuter : iam : PassRole

Dans ce cas, les politiques de Mary doivent être mises à jour pour lui permettre d'effectuer l'PassRole action iam :. Si vous avez besoin d'aide, contactez votre AWS administrateur. Votre administrateur vous a fourni vos informations d'identification de connexion.

Je souhaite autoriser des personnes extérieures à mon AWS compte à accéder à mes ressources de réponse aux incidents de AWS sécurité

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 en savoir plus, consultez les éléments suivants :

- Pour savoir si Amazon AWS Security Incident Response prend en charge ces fonctionnalités, consultez Comment fonctionne AWS Security Incident ResponseIAM.
- Pour savoir comment donner accès à vos ressources sur les AWS comptes que vous possédez, consultez la section Fournir l'accès à un IAM utilisateur sur un autre AWS compte que vous possédez dans le Guide de IAM l'utilisateur.
- Pour savoir comment fournir l'accès à vos ressources à des AWS comptes tiers, consultez la section Fournir un accès aux AWS comptes détenus par des tiers dans le Guide de IAM l'utilisateur.

- Pour savoir comment fournir un accès via la fédération d'identité, consultez la section Fournir un accès aux utilisateurs authentifiés de manière externe (fédération d'identité) dans le guide de l'IAMutilisateur.
- Pour connaître la différence entre l'utilisation de rôles et l'utilisation de politiques basées sur les ressources pour l'accès entre comptes, voir Accès aux ressources entre comptes IAM dans le guide de l'IAMutilisateur.

Utilisation des rôles de service

Supporte les rôles de service : Non

Un rôle de service est un IAMrôle qu'un service assume pour effectuer des actions en votre nom. Un administrateur IAM peut créer, modifier et supprimer une fonction du service à partir de IAM. Pour plus d'informations, consultez la section Création d'un rôle pour déléguer des autorisations à un AWS service dans le Guide de IAM l'utilisateur.

Utilisation des rôles liés à un service

Rôles liés aux services pour la réponse aux incidents AWS de sécurité

Table des matières

Prend en charge les rôles liés aux services : Oui

Un rôle lié à un service est un type de rôle lié à un AWS service. Le service peut endosser le rôle afin d'effectuer une action en votre nom. Les rôles liés à un service s'affichent dans votre compte AWS et sont détenus par le service. Un administrateur IAM peut consulter, mais ne peut pas modifier les autorisations concernant les rôles liés à un service.

Un rôle lié à un service facilite la configuration de la réponse aux incidents de AWS sécurité, car vous n'avez pas à ajouter manuellement les autorisations nécessaires. AWS Security Incident Response définit les autorisations associées à ses rôles liés aux services et, sauf indication contraire, seule la solution AWS Security Incident Response peut assumer ses rôles. Les autorisations

définies comprennent la stratégie d'approbation et la stratégie d'autorisation. De plus, cette stratégie d'autorisation ne peut pas être attachée à une autre entité IAM.

Pour plus d'informations sur les autres services qui prennent en charge les rôles liés à un service, consultez la section AWS Services qui fonctionnent avec IAM et recherchez les services dont la valeur est Oui dans la colonne Rôles liés à un service. Choisissez un Oui ayant un lien permettant de consulter les détails du rôle pour ce service.

AWS SLR: AWSServiceRoleForSecurityIncidentResponse

AWS Security Incident Response utilise le rôle lié au service (SLR) nommé AWSServiceRoleForSecurityIncidentResponse — Politique de réponse aux incidents de AWS sécurité pour identifier les comptes abonnés, créer des dossiers et étiqueter les ressources associées.

Autorisations

Le rôle AWSServiceRoleForSecurityIncidentResponse lié à un service fait confiance au service suivant pour assumer le rôle :

- `triage.security-ir.amazonaws.com`

La politique AWS gérée nommée est attachée à ce rôle AWSSecurityIncidentResponseServiceRolePolicy. Le service utilise le rôle pour effectuer des actions sur les ressources suivantes :

- AWS Organizations: permet au service de rechercher les comptes de membres à utiliser avec le service.
- CreateCase: Permet au service de créer des demandes de service pour le compte des comptes des membres.
- TagResource: autorise les ressources du tag de service configurées dans le cadre du service.

Gérer le rôle

Vous n’avez pas besoin de créer manuellement un rôle lié à un service. Lorsque vous vous inscrivez à AWS Security Incident Response dans le AWS Management Console AWS CLI, le ou le AWS API, le service crée le rôle lié au service pour vous.

> **Note**
>
> Si vous avez créé un abonnement à l'aide d'un compte d'administrateur délégué, les rôles liés au service doivent être créés manuellement dans les comptes AWS Organizations de gestion.

Si vous supprimez ce rôle lié à un service et que vous avez ensuite besoin de le recréer, vous pouvez utiliser la même procédure pour recréer le rôle dans votre compte. Lorsque vous vous inscrivez au service, le rôle lié au service est à nouveau créé pour vous.

Vous devez configurer les autorisations de manière à permettre à une entité IAM (comme un utilisateur, groupe ou rôle) de créer, modifier ou supprimer un rôle lié à un service. Pour plus d'informations, consultez la section Autorisations relatives aux rôles liés à un service dans le Guide de l'IAMutilisateur.

AWS SLR: AWSServiceRoleForSecurityIncidentResponse_Triage

AWS La réponse aux incidents de sécurité utilise le rôle lié au service (SLR) nommé « AWSServiceRoleForSecurityIncidentResponse_Triage Politique de réponse aux incidents de AWS sécurité » pour surveiller en permanence votre environnement afin de détecter les menaces de sécurité, d'ajuster les services de sécurité pour réduire le bruit des alertes et de recueillir des informations pour enquêter sur les incidents potentiels.

Autorisations

Le rôle AWSServiceRoleForSecurityIncidentResponse_Triage lié à un service fait confiance au service suivant pour assumer le rôle :

- `triage.security-ir.amazonaws.com`

La politique AWS gérée est attachée à ce rôle AWSSecurityIncidentResponseTriageServiceRolePolicy. Le service utilise le rôle pour effectuer des actions sur les ressources suivantes :

- Événements : permet au service de créer une règle Amazon EventBridge gérée. Cette règle correspond à l'infrastructure requise dans votre AWS compte pour transmettre les événements de votre compte au service. Cette action est exécutée sur n'importe quelle AWS ressource gérée par`triage.security-ir.amazonaws.com`.

- Amazon GuardDuty : permet au service de régler les services de sécurité afin de réduire le bruit des alertes et de recueillir des informations pour enquêter sur les incidents potentiels. Cette action est exécutée sur n'importe quelle AWS ressource.
- AWS Security Hub: permet au service de régler les services de sécurité afin de réduire le bruit des alertes et de recueillir des informations pour enquêter sur les incidents potentiels. Cette action est exécutée sur n'importe quelle AWS ressource.

Gérer le rôle

Vous n’avez pas besoin de créer manuellement un rôle lié à un service. Lorsque vous vous inscrivez à AWS Security Incident Response dans le AWS Management Console AWS CLI, le ou le AWS API, le service crée le rôle lié au service pour vous.

Si vous supprimez ce rôle lié à un service et que vous avez ensuite besoin de le recréer, vous pouvez utiliser la même procédure pour recréer le rôle dans votre compte. Lorsque vous vous inscrivez au service, le rôle lié au service est à nouveau créé pour vous.

Vous devez configurer les autorisations de manière à permettre à une entité IAM (comme un utilisateur, groupe ou rôle) de créer, modifier ou supprimer un rôle lié à un service. Pour plus d'informations, consultez la section Autorisations relatives aux rôles liés à un service dans le Guide de l'IAMutilisateur.

Régions prises en charge pour les AWS rôles liés au service de réponse aux incidents de sécurité

AWS Security Incident Response prend en charge l'utilisation de rôles liés au service dans toutes les régions où le service est disponible.

- USA Est (Ohio)
- USA Ouest (Oregon)
- USA Est (Virginie)
- UE (Francfort)
- UE (Irlande)
- UE (Londres)
- UE (Stockholm)
- Asie-Pacifique (Singapour)

- Asie-Pacifique (Séoul)
- Asie-Pacifique (Sydney)
- Asie-Pacifique (Tokyo)
- Canada (Centre)

AWS Stratégies gérées

Une politique AWS gérée est une politique autonome créée et administrée par AWS. AWS les politiques gérées 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.

Pour ajouter des autorisations aux utilisateurs, aux groupes et aux rôles, il est plus facile d'utiliser des politiques AWS gérées que de les rédiger vous-même. Il faut du temps et de l'expertise pour créer des politiques IAM gérées par le client qui ne fournissent à votre équipe que les autorisations dont elle a besoin. Pour démarrer rapidement, vous pouvez utiliser nos politiques AWS gérées. Ces politiques couvrent les cas d'utilisation courants et sont disponibles dans votre AWS compte. Pour plus d'informations sur les politiques AWS gérées, voir les politiques AWS gérées dans le Guide de IAM l'utilisateur.

AWS les services maintiennent et mettent à jour leurs politiques AWS gérées associées. Vous ne pouvez pas modifier les autorisations dans les politiques AWS gérées. Les services ajoutent occasionnellement des autorisations à une politique gérée par AWS pour prendre en charge de nouvelles fonctionnalités. Ce type de mise à jour affecte toutes les identités (utilisateurs, groupes et rôles) auxquelles la politique est attachée. Les services sont très susceptibles de mettre à jour une politique gérée par AWS quand une nouvelle fonctionnalité est lancée ou quand de nouvelles opérations sont disponibles. Les services ne suppriment pas les autorisations d'une politique AWS gérée. Les mises à jour des politiques n'endommageront donc pas vos autorisations existantes.

En outre, AWS prend en charge les politiques gérées pour les fonctions professionnelles qui couvrent plusieurs services. Par exemple, la politique ReadOnlyAccess AWS gérée fournit un accès en lecture seule à tous les AWS services et ressources. Lorsqu'un service lance une nouvelle fonctionnalité, il AWS ajoute des autorisations en lecture seule pour les nouvelles opérations et ressources. Pour obtenir une liste et une description des politiques relatives aux fonctions de travail, voir les politiques AWS gérées pour les fonctions de travail dans le Guide de IAM l'utilisateur.

Table des matières

- AWS politique gérée : AWSSecurityIncidentResponseServiceRolePolicy
- AWS politique gérée : AWSSecurityIncidentResponseFullAccess
- AWS politique gérée : AWSSecurityIncidentResponseReadOnlyAccess
- AWS politique gérée : AWSSecurityIncidentResponseCaseFullAccess
- AWS politique gérée : AWSSecurityIncidentResponseTriageServiceRolePolicy
- AWS Mises à jour de réponse aux incidents de sécurité SLRs et politiques gérées

AWS politique gérée : AWSSecurityIncidentResponseServiceRolePolicy

AWS Security Incident Response utilise la politique AWSSecurityIncidentResponseServiceRolePolicy AWS gérée. Cette politique AWS gérée est attachée au rôle AWSServiceRoleForSecurityIncidentResponselié au service. La politique permet à AWS Security Incident Response d'identifier les comptes abonnés, de créer des dossiers et d'étiqueter les ressources associées.

> **Important**
>
> Ne stockez pas d'informations personnellement identifiables (PII) ou d'autres informations confidentielles ou sensibles dans des balises. AWS Security Incident Response utilise des balises pour vous fournir des services d'administration. Les balises ne sont pas destinées à être utilisées pour des données privées ou sensibles

Détails des autorisations

Le service utilise cette politique pour effectuer des actions sur les ressources suivantes :

- AWS Organizations: permet au service de rechercher les comptes de membres à utiliser avec le service.
- CreateCase: Permet au service de créer des demandes de service pour le compte des comptes des membres.
- TagResource: autorise les ressources du tag de service configurées dans le cadre du service.

Vous pouvez consulter les autorisations associées à cette politique dans les politiques AWS gérées pour AWSSecurityIncidentResponseServiceRolePolicy.

AWS politique gérée : AWSSecurityIncidentResponseFullAccess

AWS Security Incident Response utilise la politique AWSSecurityIncidentResponseAdmin AWS gérée. Cette politique accorde un accès complet aux ressources du service et aux ressources connexes Services AWS. Vous pouvez utiliser cette politique avec vos IAM responsables afin d'ajouter rapidement des autorisations pour la réponse aux incidents AWS de sécurité.

> **Important**
>
> Ne stockez pas d'informations personnellement identifiables (PII) ou d'autres informations confidentielles ou sensibles dans des balises. AWS Security Incident Response utilise des balises pour vous fournir des services d'administration. Les balises ne sont pas destinées à être utilisées pour des données privées ou sensibles

Détails des autorisations

Le service utilise cette politique pour effectuer des actions sur les ressources suivantes :

- IAMaccès principal en lecture seule : permet à un utilisateur du service d'effectuer des actions en lecture seule sur les ressources existantes de réponse aux incidents AWS de sécurité.
- IAMaccès principal en écriture : permet à un utilisateur du service de mettre à jour, de modifier, de supprimer et de créer des ressources de réponse aux incidents de AWS sécurité.

Vous pouvez consulter les autorisations associées à cette politique dans les politiques AWS gérées pour AWSSecurityIncidentResponseFullAccess.

AWS politique gérée : AWSSecurityIncidentResponseReadOnlyAccess

AWS Security Incident Response utilise la politique AWSSecurityIncidentResponseReadOnlyAccess AWS gérée. La politique accorde un accès en lecture seule aux ressources des dossiers de service. Vous pouvez utiliser cette politique avec vos IAM responsables afin d'ajouter rapidement des autorisations pour la réponse aux incidents AWS de sécurité.

> **Important**
>
> Ne stockez pas d'informations personnellement identifiables (PII) ou d'autres informations confidentielles ou sensibles dans des balises. AWS Security Incident Response utilise des

balises pour vous fournir des services d'administration. Les balises ne sont pas destinées à être utilisées pour des données privées ou sensibles

Détails des autorisations

Le service utilise cette politique pour effectuer des actions sur les ressources suivantes :

- IAMaccès principal en lecture seule : permet à un utilisateur du service d'effectuer des actions en lecture seule sur les ressources existantes de réponse aux incidents AWS de sécurité.

Vous pouvez consulter les autorisations associées à cette politique dans les politiques AWS gérées pour AWSSecurityIncidentResponseReadOnlyAccess.

AWS politique gérée : AWSSecurityIncidentResponseCaseFullAccess

AWS Security Incident Response utilise la politique AWSSecurityIncidentResponseCaseFullAccess AWS gérée. La politique accorde un accès complet aux ressources relatives aux dossiers de service. Vous pouvez utiliser cette politique avec vos IAM responsables afin d'ajouter rapidement des autorisations pour la réponse aux incidents AWS de sécurité.

Important

Ne stockez pas d'informations personnellement identifiables (PII) ou d'autres informations confidentielles ou sensibles dans des balises. AWS Security Incident Response utilise des balises pour vous fournir des services d'administration. Les balises ne sont pas destinées à être utilisées pour des données privées ou sensibles

Détails des autorisations

Le service utilise cette politique pour effectuer des actions sur les ressources suivantes :

- IAMaccès en lecture seule aux dossiers principaux : permet à un utilisateur du service d'effectuer des actions en lecture seule sur des cas de réponse aux incidents de AWS sécurité existants.
- IAMaccès principal à la rédaction des dossiers : permet à un utilisateur du service de mettre à jour, de modifier, de supprimer et de créer des cas de réponse aux incidents de AWS sécurité.

Vous pouvez consulter les autorisations associées à cette politique dans les politiques AWS gérées pour AWSSecurityIncidentResponseCaseFullAccess.

AWS politique gérée : AWSSecurityIncidentResponseTriageServiceRolePolicy

AWS Security Incident Response utilise la politique AWSSecurityIncidentResponseTriageServiceRolePolicy AWS gérée. Cette politique AWS gérée est attachée au rôle lié au service AWSServiceRoleForSecurityIncidentResponse_Triage.

La politique donne accès à la réponse aux incidents de AWS sécurité afin de surveiller en permanence votre environnement pour détecter les menaces de sécurité, d'ajuster les services de sécurité pour réduire le bruit des alertes et de recueillir des informations pour enquêter sur les incidents potentiels. Vous ne pouvez pas attacher cette politique à vos entités IAM.

> **Important**
>
> Ne stockez pas d'informations personnellement identifiables (PII) ou d'autres informations confidentielles ou sensibles dans des balises. AWS Security Incident Response utilise des balises pour vous fournir des services d'administration. Les balises ne sont pas destinées à être utilisées pour des données privées ou sensibles

Détails des autorisations

Le service utilise cette politique pour effectuer des actions sur les ressources suivantes :

- Événements : autorise le service à créer une règle EventBridge gérée par Amazon. Cette règle correspond à l'infrastructure requise dans votre AWS compte pour transmettre les événements de votre compte au service. Cette action est exécutée sur n'importe quelle AWS ressource gérée par`triage.security-ir.amazonaws.com`.
- Amazon GuardDuty : permet au service de régler les services de sécurité afin de réduire le bruit des alertes et de recueillir des informations pour enquêter sur les incidents potentiels. Cette action est exécutée sur n'importe quelle AWS ressource.
- AWS Security Hub: permet au service de régler les services de sécurité afin de réduire le bruit des alertes et de recueillir des informations pour enquêter sur les incidents potentiels. Cette action est exécutée sur n'importe quelle AWS ressource.

Vous pouvez consulter les autorisations associées à cette politique dans les politiques AWS gérées pour AWSSecurityIncidentResponseTriageServiceRolePolicy.

AWS Mises à jour de réponse aux incidents de sécurité SLRs et politiques gérées

Consultez les informations relatives aux mises à jour apportées aux rôles relatifs à la réponse aux incidents de AWS sécurité SLRs et aux politiques gérées depuis que ce service a commencé à suivre ces modifications.

Modification	Description	Date
Nouveau SLR — AWSServiceRoleForSecurityIncidentResponse Nouvelle politique gérée — AWSSecurityIncidentResponseServiceRolePolicy.	Nouveau rôle lié au service et politique associée permettant d'accéder au service dans vos AWS Organizations comptes afin d'identifier les membres.	1er décembre 2016
Nouveau SLR — AWSServiceRoleForSecurityIncidentResponse_Triage Nouvelle politique gérée — AWSSecurityIncidentResponse	Nouveau rôle lié au service et politique associée permettant d'accéder au service à vos AWS Organizations comptes pour effectuer le triage des événements de sécurité.	1er décembre 2016

Modification	Description	Date
TriageServiceRolePolicy		
Nouvelle politique gérée — AWSSecurityIncidentResponseFullAccess	AWS Security Incident Response ajoute un nouveau code SLR à joindre IAM aux principes pour les actions de lecture et d'écriture du service.	1er décembre 2016
Nouveau rôle de politique géré — AWSSecurityIncidentResponseReadOnlyAccess	AWS Réponse aux incidents de sécurité : ajoutez un nouveau SLR message à joindre aux IAM principes pour les actions de lecture	1er décembre 2016
Nouveau rôle de politique géré — AWSSecurityIncidentResponseCaseFullAccess	AWS Security Incident Response ajoute un nouveau SLR code à joindre IAM aux principes pour les actions de lecture et d'écriture relatives aux dossiers de service.	1er décembre 2016
J'ai commencé à suivre les modifications.	A commencé à suivre les modifications relatives à AWS la réponse aux incidents de sécurité SLRs et aux politiques gérées	1er décembre 2016

Intervention en cas d’incidents

La sécurité et la conformité sont une responsabilité partagée entre le client AWS et le client. Ce modèle partagé peut contribuer à alléger la charge opérationnelle du client en AWS exploitant, en gérant et en contrôlant les composants, depuis le système d'exploitation hôte et la couche de virtualisation jusqu'à la sécurité physique des installations dans lesquelles le service fonctionne. Le client assume la responsabilité et la gestion du système d'exploitation client (y compris les mises à jour et les correctifs de sécurité), des autres logiciels d'application associés ainsi que de la

configuration du pare-feu du groupe de sécurité AWS fourni. Pour plus d'informations, reportez-vous au modèle de responsabilitéAWS partagée.

En établissant une base de sécurité répondant aux objectifs de vos applications exécutées dans le cloud, vous êtes en mesure de détecter les écarts auxquels vous pouvez réagir. La réponse aux incidents de sécurité étant un sujet complexe, nous vous encourageons à consulter les ressources suivantes afin de mieux comprendre l'impact de la réponse aux incidents et de vos choix sur les objectifs de votre entreprise : livre blanc sur les meilleures pratiques en matière de AWS sécurité et livre blanc sur la perspective de sécurité du cadre d'adoption du AWS cloud (CAF).

Validation de la conformité

Des auditeurs tiers évaluent la sécurité et la conformité des AWS services dans le cadre de multiples programmes de AWS conformité. Il s'agit SOC PCI notamment de RAMP la Fed HIPAA et d'autres.

AWS La réponse aux incidents de sécurité n'a pas été évaluée quant à sa conformité avec les programmes susmentionnés.

Pour une liste des AWS services concernés par des programmes de conformité spécifiques, voir AWS Services concernés par programme de conformité. Pour des informations générales, consultez AWS la section Programmes de conformité.

Vous pouvez télécharger des rapports d'audit tiers à l'aide d' AWS Artifact. Pour plus d'informations, consultez la section Téléchargement de rapports dans AWS Artifact.

Lorsque vous utilisez AWS des services, votre responsabilité en matière de conformité dépend de la sensibilité de vos données, des objectifs de conformité de votre entreprise et des lois AWS et réglementations applicables. AWS fournit les ressources suivantes pour faciliter la mise en conformité :

- Guides de démarrage rapide sur la sécurité et la conformité : ces guides de déploiement abordent les considérations architecturales et indiquent les étapes à suivre pour déployer des environnements de base axés sur la sécurité et la conformité sur. AWS
- Livre blanc sur l'architecture au service de la HIPAA sécurité et de la conformité — Ce livre blanc décrit comment les entreprises peuvent créer des applications AWS conformes. HIPAA
- AWS ressources de conformité : collection de cahiers de travail et de guides applicables par secteur d'activité et/ou par site.
- L'évaluation des ressources à l'aide AWS des règles de AWS configuration du manuel Config Developer Guide — AWS Config permet d'évaluer dans quelle mesure vos configurations

de ressources sont conformes aux pratiques internes, aux directives du secteur et aux réglementations.

- AWS Security Hub — Ce AWS service fournit une vue complète de l'état de votre sécurité interne AWS. Security Hub utilise des contrôles de sécurité pour évaluer vos AWS ressources 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 AWS service détecte les menaces potentielles qui pèsent sur vos AWS comptes, vos charges de travail, vos conteneurs et vos données en surveillant votre environnement pour détecter toute activité suspecte ou malveillante. GuardDuty peut vous aider à répondre à diverses exigences de conformité PCIDSS, par exemple en répondant aux exigences de détection des intrusions imposées par certains cadres de conformité.
- AWS Audit Manager : ce AWS service vous aide à auditer en permanence votre AWS utilisation afin de simplifier la gestion des risques et la conformité aux réglementations et aux normes du secteur.

Enregistrement et surveillance dans le cadre de la réponse aux incidents AWS de sécurité

La surveillance joue un rôle important dans le maintien de la fiabilité, de la disponibilité et des performances de AWS Security Incident Response et de vos autres AWS solutions. AWS Security Incident Response prend actuellement en charge les AWS services suivants pour surveiller votre organisation et les activités qui s'y déroulent.

AWS CloudTrail — Avec CloudTrail vous pouvez capturer les API appels depuis la console AWS Security Incident Response. Par exemple, lorsqu'un utilisateur s'authentifie, il CloudTrail peut enregistrer des informations telles que l'adresse IP de la demande, l'auteur de la demande et la date à laquelle elle a été faite.

Amazon CloudWatch Metrics — Grâce aux CloudWatch métriques, vous pouvez surveiller, signaler et prendre des mesures automatiques en cas d'événement en temps quasi réel. Par exemple, vous pouvez créer des CloudWatch tableaux de bord sur les indicateurs fournis afin de surveiller votre utilisation de la réponse aux incidents de AWS sécurité, ou vous pouvez créer des CloudWatch alarmes sur les indicateurs fournis pour vous avertir en cas de dépassement d'un seuil défini.

L'espace de noms du service est AWS/Usage/ServiceName. Les noms de métriques disponibles sont ActiveManagedCases et SelfManagedCases.

Conformément aux conditions de AWS service, l'équipe d'intervention en cas d'incident de AWS sécurité aura accès à votre historique DNS et aux données du CloudTrail journal S3. VPC Ces données peuvent être utilisées lors d'incidents de sécurité actifs lorsqu'un dossier est ouvert sur le portail du service AWS Security Incident Response.

Résilience

L'infrastructure AWS mondiale est construite autour des AWS régions et des zones de disponibilité. Les régions 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 plus d'informations sur AWS les régions et les zones de disponibilité, consultez la section Infrastructure AWS globale.

Sécurité de l'infrastructure

AWS La réponse aux incidents de sécurité est protégée par la sécurité du réseau AWS mondial. Pour plus d'informations sur les services AWS de sécurité et sur la manière dont AWS l'infrastructure est protégée, consultez la section Sécurité du AWS cloud. Pour concevoir votre AWS environnement en utilisant les meilleures pratiques en matière de sécurité de l'infrastructure, consultez la section Protection de l'infrastructure dans le cadre AWS bien architecturé du pilier de sécurité.

Vous utilisez les API appels AWS publiés pour accéder à AWS Security Incident Response via le réseau. Les clients doivent prendre en charge les éléments suivants :

- Sécurité de la couche de transport (TLS). Nous avons besoin de la TLS version 1.2 et recommandons la TLS version 1.3.
- Des suites de chiffrement parfaitement confidentielles (PFS) telles que (Ephemeral Diffie-Hellman) ou DHE ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). La plupart des systèmes modernes tels que Java 7 et les versions ultérieures prennent en charge ces modes.

En outre, les demandes doivent être signées à l'aide d'un ID de clé d'accès et d'une clé d'accès secrète associée à un principal IAM. Vous pouvez également utiliser le service AWS de jeton

de sécurité (AWS STS) pour générer des informations de sécurité temporaires afin de signer les demandes.

Analyse de la configuration et des vulnérabilités

Vous êtes responsable de la gestion des rôles de contention des services et des ensembles de AWS CloudFormation piles associés.

AWS gère les tâches de sécurité de base, telles que l'application de correctifs au système d'exploitation client (OS) et aux bases de données, la configuration du pare-feu et la reprise après sinistre. Ces procédures ont été vérifiées et certifiées par les tiers appropriés. Pour plus de détails, consultez les ressources AWS suivantes :

- Modèle de responsabilité partagée
- Bonnes pratiques en matière de sécurité, d'identité et de conformité

Prévention du problème de l’adjoint confus entre services

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. En AWS, l'usurpation d'identité interservices peut entraîner la confusion des adjoints. L’usurpation d’identité entre services 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 auprès des principaux fournisseurs de services qui ont obtenu l'accès aux ressources de votre compte.

Nous recommandons d'utiliser les clés contextuelles de condition SourceAccount globale AWSAWS: SourceArn et : dans les politiques de ressources afin de limiter les autorisations qu'Amazon Connect accorde à un autre service à la ressource. Si vous utilisez les deux clés contextuelles de condition globale, la SourceAccount valeur AWS : et le compte dans la SourceArn valeur AWS : doivent utiliser le même identifiant de compte lorsqu'ils sont utilisés dans la même déclaration de politique.

Le moyen le plus efficace de se protéger contre le problème de confusion des adjoints est d'utiliser le nom de ressource Amazon exact (ARN) de la ressource que vous souhaitez autoriser. Si vous ne connaissez pas l'intégralité ARN de la ressource ou si vous spécifiez plusieurs ressources, utilisez la clé de condition AWS : contexte SourceArn global avec des caractères génériques (*) pour les parties inconnues duARN. Par exemple, arn ::servicename : :region-name AWS : :your account ID :*. AWS

Pour un exemple de politique d'attribution de rôles qui montre comment éviter un problème de confusion entre les adjoints, voir Politique de prévention de la confusion chez les adjoints.

Service Quotas

AWS Réponse aux incidents de sécurité

Les tableaux suivants répertorient les quotas, pour les ressources de réponse aux incidents de AWS sécurité pour votre AWS-account ;. Certains quotas peuvent être augmentés au-delà de ceux indiqués ci-dessous avec l'approbation du responsable du service. Sauf indication contraire, ces quotas s'appliquent par région.

	Nom	Par défaut	Ajustable	Commentaires
1	Cas AWS pris en charge actifs	10	Oui (jusqu'à 50)	Le nombre de dossiers actifs demandant de l'aide auprès de AWS CIRT.
2	Cas autogérés actifs	50	Oui (jusqu'à 100)	Le nombre de cas actifs utilisant la plateforme sans l'assistance de AWS CIRT.
3	Dossiers pris en charge par le service créés dans les 24 heures	10	Non	Le nombre de demandes d'assistance créées au cours d' AWS CIRTune période continue de 24 heures.
4	Nombre maximum d'entités dans l'équipe de réponse aux	10	Non	Le nombre maximum d'entités dans l'équipe de réponse aux

	Nom	Par défaut	Ajustable	Commentaires
	incidents par défaut			incidents par défaut.
5	Nombre maximum de membres supplémentaires par dossier	30	Non	Le nombre maximum d'entités associées à un dossier. Il sera initialem ent renseigné avec les entités de votre équipe de réponse aux incidents par défaut.
6	Nombre maximum de pièces jointes au boîtier	50	Oui (jusqu'à 100)	Le nombre maximum de fichiers pouvant être joints à un dossier.
7	Taille maximale des commentai res relatifs au dossier	1 000	Non	Le nombre maximum de caractères dans un commentaire de dossier.
8	Taille maximale du nom de fichier des pièces jointes	255	Non	Le nombre maximal de caractères d'un nom de fichier.

AWS Guide technique de réponse aux incidents de sécurité

Table des matières

Résumé

Ce guide présente un aperçu des principes fondamentaux de la réponse aux incidents de sécurité dans l'environnement cloud Amazon Web Services (AWS) d'un client. Il fournit une vue d’ensemble des concepts de sécurité du cloud et de réponse aux incidents, et il identifie les fonctionnalités, les services et les mécanismes du cloud mis à la disposition des clients qui répondent à des problèmes de sécurité.

Ce guide est destiné aux personnes occupant des postes techniques et suppose que vous connaissez les principes généraux de la sécurité de l'information, que vous avez une compréhension de base de la réponse aux incidents de sécurité dans vos environnements sur site actuels et que vous êtes familiarisé avec les services cloud.

Êtes-vous Well-Architected ?

Le AWS Well-Architected Framework vous aide à comprendre les avantages et les inconvénients des décisions que vous prenez lors de la création de systèmes dans le cloud. Les six piliers du cadre vous permettent d'apprendre les meilleures pratiques architecturales pour concevoir et exploiter des systèmes fiables, sécurisés, efficaces, rentables et durables. À l'aide du AWS Well-Architected

Tool, disponible gratuitement dans la AWS Well-Architected Tool console, vous pouvez évaluer vos charges de travail par rapport à ces meilleures pratiques en répondant à une série de questions pour chaque pilier.

Pour obtenir des conseils d'experts supplémentaires et les meilleures pratiques relatives à votre architecture cloud (déploiements d'architecture de référence, diagrammes et livres blancs), consultez le Centre d'architecture.AWS

Introduction

La sécurité est la priorité absolue de AWS. AWS les clients bénéficient de centres de données et d'une architecture réseau conçus pour répondre aux besoins des entreprises les plus sensibles en matière de sécurité. AWS a un modèle de responsabilité partagée : AWS gère la sécurité du cloud, et les clients sont responsables de la sécurité dans le cloud. Cela signifie que vous avez le contrôle total de la mise en œuvre de votre sécurité, y compris l'accès à plusieurs outils et services pour vous aider à atteindre vos objectifs de sécurité. Ces fonctionnalités vous aident à établir une base de sécurité pour les applications exécutées dans le AWS Cloud.

Lorsqu'un écart par rapport à la base de référence se produit, par exemple en raison d'une mauvaise configuration ou de l'évolution de facteurs externes, vous devez réagir et enquêter. Pour y parvenir, vous devez comprendre les concepts de base de la réponse aux incidents de sécurité dans votre AWS environnement et les exigences relatives à la préparation, à la formation et à la formation des équipes cloud avant que des problèmes de sécurité ne surviennent. Il est important de connaître les contrôles et les fonctionnalités que vous pouvez utiliser, de consulter des exemples thématiques pour résoudre les problèmes potentiels et d'identifier les méthodes de correction qui utilisent l'automatisation pour améliorer la vitesse et la cohérence des réponses. En outre, vous devez comprendre vos exigences en matière de conformité et de réglementation en ce qui concerne l'élaboration d'un programme de réponse aux incidents de sécurité pour répondre à ces exigences.

La réponse aux incidents de sécurité peut être complexe, c'est pourquoi nous vous encourageons à mettre en œuvre une approche itérative : commencez par les principaux services de sécurité, développez les capacités de détection et de réponse de base, puis élaborez des manuels pour créer une bibliothèque initiale de mécanismes de réponse aux incidents sur laquelle vous pourrez itérer et améliorer.

Avant de commencer

Avant de commencer à vous renseigner sur la réponse aux incidents liés aux événements de sécurité AWS, familiarisez-vous avec les normes et cadres pertinents en matière de AWS sécurité

et de réponse aux incidents. Ces bases vous aideront à comprendre les concepts et les meilleures pratiques présentés dans ce guide.

AWS normes et cadres de sécurité

Pour commencer, nous vous encourageons à consulter les meilleures pratiques en matière de sécurité, d'identité et de conformité, Security Pillar - AWS Well-Architected Framework et la perspective de sécurité du livre blanc Overview of AWS the Cloud Adoption Framework AWS CAF ().

AWS CAFIl fournit des conseils pour faciliter la coordination entre les différents services des organisations qui migrent vers le cloud. Les AWS CAF conseils sont divisés en plusieurs domaines d'intérêt, appelés perspectives, qui sont pertinents pour la création de systèmes informatiques basés sur le cloud. Le point de vue de la sécurité décrit comment mettre en œuvre un programme de sécurité dans tous les flux de travail, notamment la réponse aux incidents. Ce document est le fruit de nos expériences de travail avec les clients pour les aider à mettre en place des programmes et des capacités de réponse aux incidents de sécurité efficaces et efficients.

Normes et cadres de réponse aux incidents du secteur

Ce livre blanc suit les normes de réponse aux incidents et les meilleures pratiques du Guide de gestion des incidents de sécurité informatique SP 800-61 r2, créé par le National Institute of Standards and Technology (). NIST Lire et comprendre les concepts introduits par NIST est une condition préalable utile. Les concepts et les meilleures pratiques de ce NIST guide seront appliqués aux AWS technologies décrites dans ce paper. Toutefois, les scénarios d'incidents sur site ne sont pas couverts par ce guide.

AWS aperçu de la réponse aux incidents

Pour commencer, il est important de comprendre en quoi les opérations de sécurité et la réponse aux incidents sont différentes dans le cloud. Pour créer des capacités de réponse efficaces AWS, vous devez comprendre les écarts par rapport à la réponse sur site traditionnelle et leur impact sur votre programme de réponse aux incidents. Chacune de ces différences, ainsi que les principes fondamentaux de conception de la réponse aux AWS incidents, sont détaillés dans cette section.

Aspects de la réponse aux AWS incidents

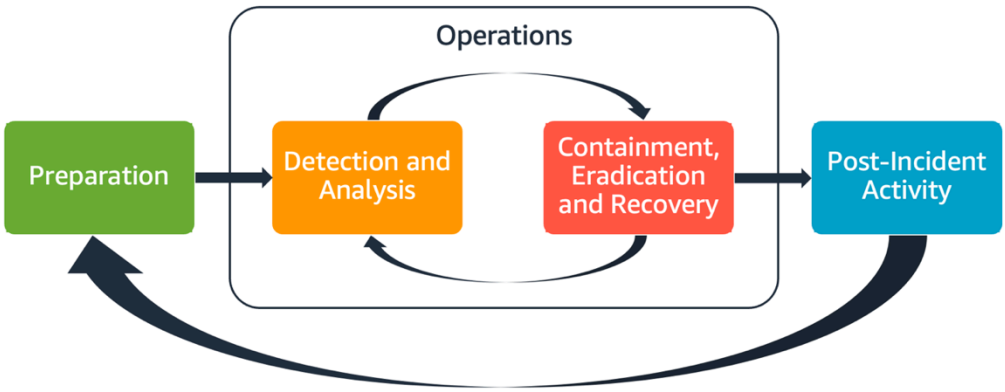
Tous les AWS utilisateurs d'une organisation doivent avoir une connaissance de base des processus de réponse aux incidents de sécurité, et le personnel de sécurité doit savoir comment répondre aux problèmes de sécurité. L’éducation, la formation et l’expérience sont essentielles à la réussite d’un

programme de réponse aux incidents dans le cloud et sont idéalement mises en œuvre bien avant de devoir gérer un éventuel incident de sécurité. La base d'un programme de réponse aux incidents réussi dans le cloud repose sur la préparation, les opérations et l'activité post-incident.

Pour comprendre chacun de ces aspects, tenez compte des descriptions suivantes :

- Préparation — Préparez votre équipe de réponse aux incidents à détecter les incidents et à y répondre AWS en interne en activant des contrôles de détection et en vérifiant l'accès approprié aux outils et services cloud nécessaires. De plus, préparez les playbooks nécessaires (manuels et automatisés) pour garantir des réponses fiables et cohérentes.
- Opérations — Gérez les événements de sécurité et les incidents potentiels en suivant les NIST phases de réponse aux incidents : détecter, analyser, contenir, éradiquer et récupérer.
- Activité après un incident : répétez les résultats de vos événements de sécurité et de vos simulations pour améliorer l'efficacité de votre réponse, augmenter la valeur dérivée de la réponse et de l'enquête, et réduire davantage les risques. Vous devez tirer les leçons des incidents et vous impliquer pleinement dans les activités d'amélioration.

Chacun de ces aspects est exploré et détaillé dans ce guide. Le schéma suivant montre le flux de ces aspects, en s'alignant sur le cycle de vie de réponse aux NIST incidents mentionné précédemment, mais avec des opérations comprenant la détection et l'analyse avec le confinement, l'éradication et le rétablissement.



Aspects de la réponse aux AWS incidents

AWS principes de réponse aux incidents et objectifs de conception

Bien que les processus et mécanismes généraux de réponse aux incidents tels que définis dans le Guide de gestion des incidents de sécurité informatique NIST SP 800-61 soient bons, nous vous

encourageons également à prendre en compte ces objectifs de conception spécifiques qui sont pertinents pour répondre aux incidents de sécurité dans un environnement cloud :

- Établissez des objectifs de réponse — Travaillez avec les parties prenantes, les conseillers juridiques et les dirigeants de l'organisation pour déterminer l'objectif de réponse à un incident. Parmi les objectifs communs, citons la maîtrise et l'atténuation du problème, le rétablissement des ressources affectées, la préservation des données à des fins de criminalistique, le retour à des opérations sûres connues et, en fin de compte, les leçons à tirer des incidents.
- Réagissez en utilisant le cloud : implémentez des modèles de réponse dans le cloud, là où l'événement et les données se produisent.
- Sachez ce que vous avez et ce dont vous avez besoin : préservez les journaux, les ressources, les instantanés et les autres preuves en les copiant et en les stockant dans un compte cloud centralisé dédié à la réponse. Utilisez des balises, des métadonnées et des mécanismes qui appliquent des stratégies de conservation. Vous devez comprendre quels services vous utilisez, puis identifier les exigences pour étudier ces services. Pour vous aider à comprendre votre environnement, vous pouvez également utiliser le balisage, dont il sera question plus loin dans la the section called “Élaboration et mise en œuvre d’une stratégie de marquage” section de ce document.
- Utiliser des mécanismes de redéploiement : si une anomalie de sécurité peut être attribuée à une mauvaise configuration, la correction peut consister simplement à supprimer la variation en redéployant les ressources avec la configuration appropriée. Si un compromis possible est identifié, vérifiez que votre redéploiement inclut une atténuation réussie et vérifiée des causes profondes.
- Automatisez dans la mesure du possible : au fur et à mesure que les problèmes surviennent ou que les incidents se répètent, créez des mécanismes pour trier les événements courants et y répondre de manière programmatique. Utilisez des réponses humaines pour les incidents uniques, complexes ou sensibles pour lesquels les automatisations sont insuffisantes.
- Choisissez des solutions évolutives : efforcez-vous de correspondre à l'évolutivité de l'approche de votre organisation en matière de cloud computing. Mettez en œuvre des mécanismes de détection et de réponse qui s'adaptent à l'ensemble de vos environnements afin de réduire efficacement le délai entre la détection et la réponse.
- Apprenez et améliorez votre processus — Soyez proactif en identifiant les lacunes dans vos processus, vos outils ou votre personnel, et mettez en œuvre un plan pour les corriger. Les simulations sont des méthodes sûres pour identifier les lacunes et améliorer les processus. Reportez-vous à la the section called “Activité postérieure à l’incident” section de ce document pour plus de détails sur la façon d'itérer vos processus.

Ces objectifs de conception vous rappellent que vous devez examiner la mise en œuvre de votre architecture afin de déterminer si elle est capable de répondre aux incidents et de détecter les menaces. Lorsque vous planifiez vos mises en œuvre dans le cloud, pensez à répondre à un incident, idéalement à l'aide d'une méthodologie de réponse fiable. Dans certains cas, cela signifie que plusieurs organisations, comptes et outils peuvent être spécifiquement configurés pour ces tâches de réponse. Ces outils et fonctions doivent être mis à la disposition du gestionnaire de l'incident par le biais d'un pipeline de déploiement. Ils ne doivent pas être statiques, car cela peut entraîner un risque plus important.

Domaines d'incidents de sécurité dans le cloud

Pour vous préparer et réagir efficacement aux événements de sécurité dans votre AWS environnement, vous devez comprendre les types courants d'incidents de sécurité dans le cloud. Les incidents de sécurité peuvent survenir dans trois domaines relevant de la responsabilité du client : le service, l'infrastructure et les applications. Les différents domaines nécessitent des connaissances, des outils et des processus de réponse différents. Tenez compte des domaines suivants :

- Domaine de service : les incidents dans le domaine de service peuvent affecter vos Compte AWSAWS Identity and Access Management(IAM) autorisations, les métadonnées des ressources, la facturation ou d'autres domaines. Un événement de domaine de service est un événement auquel vous répondez exclusivement par AWS API des mécanismes, ou dont les causes profondes sont associées à votre configuration ou à vos autorisations de ressources, et qui peut être associé à une journalisation axée sur les services.
- Domaine de l'infrastructure — Les incidents dans le domaine de l'infrastructure incluent les données ou les activités liées au réseau, telles que les processus et les données sur vos instances Amazon Elastic Compute Cloud (AmazonEC2), le trafic vers vos EC2 instances Amazon au sein du cloud privé virtuel (VPC) et d'autres domaines, tels que les conteneurs ou d'autres services futurs. Votre réponse aux événements du domaine de l'infrastructure implique souvent l'acquisition de données relatives aux incidents à des fins d'analyse judiciaire. Cela inclut probablement une interaction avec le système d'exploitation d'une instance et, dans certains cas, peut également impliquer des AWS API mécanismes. Dans le domaine de l'infrastructure, vous pouvez utiliser une combinaison d'outils de AWS APIs criminalistique numérique/de réponse aux incidents (DFIR) au sein d'un système d'exploitation client, comme une EC2 instance Amazon dédiée à la réalisation d'analyses et d'enquêtes médico-légales. Les incidents liés au domaine de l'infrastructure peuvent impliquer l'analyse de captures de paquets réseau, de blocs de disques sur un volume Amazon Elastic Block Store (AmazonEBS) ou de mémoire volatile acquise à partir d'une instance.
- Domaine d'application : les incidents dans le domaine d'application se produisent dans le code de l'application ou dans le logiciel déployé sur les services ou l'infrastructure. Ce domaine doit

être inclus dans vos manuels de détection et de réponse aux menaces dans le cloud et peut intégrer des réponses similaires à celles du domaine de l'infrastructure. Avec une architecture d'application appropriée et réfléchie, vous pouvez gérer ce domaine à l'aide d'outils cloud en utilisant l'acquisition, la restauration et le déploiement automatisés.

Dans ces domaines, considérez les acteurs susceptibles d'agir contre AWS des comptes, des ressources ou des données. Que ce soit à l'interne ou à l'externe, utilisez un cadre de gestion des risques pour déterminer les risques spécifiques auxquels l'organisation est exposée et préparez-vous en conséquence. En outre, vous devez développer des modèles de menace, qui peuvent vous aider à planifier la réponse aux incidents et à élaborer une architecture réfléchie.

Principales différences en matière de réponse aux incidents dans AWS

La réponse aux incidents fait partie intégrante d'une stratégie de cybersécurité, que ce soit sur site ou dans le cloud. Les principes de sécurité tels que le moindre privilège et la défense en profondeur visent à protéger la confidentialité, l'intégrité et la disponibilité des données sur site et dans le cloud. Plusieurs modèles de réponse aux incidents qui soutiennent ces principes de sécurité emboîtent le pas, notamment la conservation des journaux, la sélection des alertes dérivée de la modélisation des menaces, le développement de playbooks et l'intégration des informations de sécurité et de la gestion des événements (SIEM). Les différences commencent lorsque les clients commencent à concevoir et à concevoir ces modèles dans le cloud. Voici les principales différences entre la réponse aux incidents dans AWS.

Différence #1 : la sécurité en tant que responsabilité partagée

La responsabilité de la sécurité et de la conformité est partagée entre AWS et ses clients. Ce modèle de responsabilité partagée allège une partie de la charge opérationnelle du client en AWS exploitant, en gérant et en contrôlant les composants, depuis le système d'exploitation hôte et la couche de virtualisation jusqu'à la sécurité physique des installations dans lesquelles le service fonctionne. Pour plus de détails sur le modèle de responsabilité partagée, reportez-vous à la documentation du modèle de responsabilité partagée.

À mesure que votre responsabilité partagée dans le cloud évolue, vos options de réponse aux incidents changent également. Planifier et comprendre ces compromis et les adapter à vos besoins de gouvernance est une étape cruciale de la réponse aux incidents.

Outre la relation directe que vous entretenez avec vous AWS, d'autres entités peuvent avoir des responsabilités dans votre modèle de responsabilité particulier. Par exemple, vous pouvez avoir des unités organisationnelles internes qui sont responsables de certains aspects de vos opérations. Vous

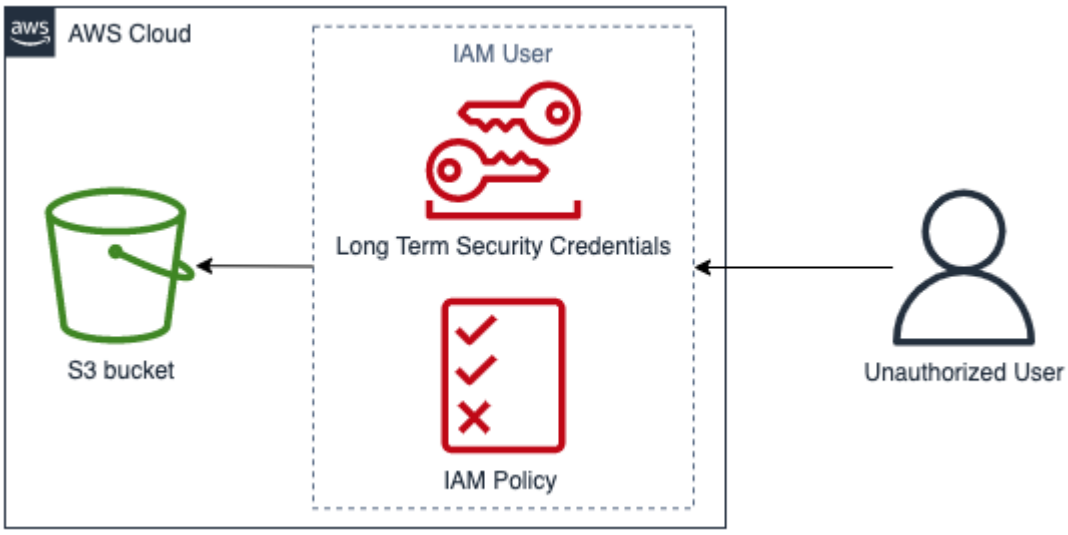
pouvez également avoir des relations avec d'autres parties qui développent, gèrent ou exploitent certaines de vos technologies cloud.

Il est extrêmement important de créer et de tester un plan de réponse aux incidents approprié et des playbooks adaptés à votre modèle opérationnel.

Différence #2 : domaine de service cloud

En raison des différences de responsabilité en matière de sécurité qui existent dans les services cloud, un nouveau domaine pour les incidents de sécurité a été introduit : le domaine des services, qui a été expliqué plus haut dans la section Domaine des incidents. Le domaine de service englobe le AWS compte d'un client, IAM les autorisations, les métadonnées des ressources, la facturation et d'autres domaines. Ce domaine est différent pour la réponse aux incidents en raison de la façon dont vous réagissez. La réponse dans le domaine de service se fait généralement en examinant et en émettant des API appels, plutôt qu'une réponse traditionnelle basée sur l'hôte et basée sur le réseau. Dans le domaine des services, vous n'interagirez pas avec le système d'exploitation d'une ressource affectée.

Le schéma suivant montre un exemple d'événement de sécurité dans le domaine des services basé sur un anti-modèle architectural. Dans ce cas, un utilisateur non autorisé obtient les informations de sécurité à long terme d'un IAM utilisateur. L'IAMutilisateur dispose d'une IAM politique qui lui permet de récupérer des objets depuis un compartiment Amazon Simple Storage Service (Amazon S3). Pour répondre à cet événement de sécurité, vous AWS APIs devez analyser AWS des journaux tels que AWS CloudTraillles journaux d'accès Amazon S3. Vous l'utiliseriez également AWS APIs pour contenir l'incident et vous en remettre.



Exemple de domaine de service

Différence #3 : APIs pour le provisionnement de l'infrastructure

Une autre différence réside dans la caractéristique cloud du libre-service à la demande. Le principal établissement avec lequel les clients interagissent AWS Cloud en utilisant des points RESTful API de terminaison publics et privés disponibles dans de nombreuses zones géographiques du monde entier. Les clients peuvent y accéder à l'APIsaide d' AWS informations d'identification. Contrairement au contrôle d'accès sur site, ces informations d'identification ne sont pas nécessairement liées à un réseau ou à un domaine Microsoft Active Directory. Les informations d'identification sont plutôt associées à un IAM principal au sein d'un AWS compte. Ces API points de terminaison sont accessibles en dehors du réseau de votre entreprise, ce qui sera important à comprendre lorsque vous répondez à un incident au cours duquel les informations d'identification sont utilisées en dehors du réseau ou de la zone géographique auxquels vous vous attendez.

En raison de la nature API basée sur AWS, une source de journal importante pour répondre aux événements de sécurité est AWS CloudTrail le suivi des API appels de gestion effectués dans vos AWS comptes et où vous pouvez trouver des informations sur la source des API appels.

Différence #4 : nature dynamique du cloud

Le cloud est dynamique ; il permet de créer et de supprimer rapidement des ressources. Grâce à la mise à l'échelle automatique, les ressources peuvent être augmentées ou diminuées en fonction de l'augmentation du trafic. Avec une infrastructure éphémère et des changements rapides, il est possible qu'une ressource que vous étudiez n'existe plus ou ait été modifiée. Pour l'analyse des incidents, il sera important de AWS comprendre la nature éphémère des AWS ressources et de savoir comment suivre leur création et leur suppression. Vous pouvez l'utiliser AWS Configpour suivre l'historique de configuration de vos AWS ressources.

Différence #5 : Accès aux données

L'accès aux données est également différent dans le cloud. Vous ne pouvez pas vous connecter à un serveur pour collecter les données dont vous avez besoin pour une enquête de sécurité. Les données sont collectées par fil et par le biais d'APIappels. Vous devrez vous entraîner et comprendre comment effectuer la collecte de données afin de APIs vous préparer à ce changement, et vérifier que le stockage est approprié pour une collecte et un accès efficaces.

Différence #6 : Importance de l'automatisation

Pour que les clients puissent pleinement tirer parti des avantages de l'adoption du cloud, leur stratégie opérationnelle doit intégrer l'automatisation. L'infrastructure en tant que code (IaC) est un modèle d'environnements automatisés hautement efficaces dans lesquels les AWS services sont

déployés, configurés, reconfigurés et détruits à l'aide de code facilité par des services iAc natifs tels que AWS CloudFormationdes solutions tierces. Cela pousse la mise en œuvre de la réponse aux incidents à être hautement automatisée, ce qui est souhaitable pour éviter les erreurs humaines, en particulier lors du traitement des preuves. Bien que l'automatisation soit utilisée sur site, elle est essentielle et plus simple dans le AWS Cloud.

Aborder ces différences

Pour remédier à ces différences, suivez les étapes décrites dans la section suivante pour vérifier que votre programme de réponse aux incidents en termes de personnel, de processus et de technologie est bien préparé.

Préparation

Pour une réponse rapide et efficace aux incidents, la préparation est essentielle. La préparation couvre trois domaines :

- Personnel — Pour préparer votre personnel à un incident de sécurité, vous devez identifier les parties prenantes concernées par la réponse aux incidents et les former à la réponse aux incidents et aux technologies cloud.
- Processus — La préparation de vos processus en cas d'incident de sécurité implique de documenter les architectures, d'élaborer des plans de réponse aux incidents complets et de créer des guides pour une réponse cohérente aux événements de sécurité.
- Technologie — Pour préparer votre technologie à un incident de sécurité, vous devez configurer l'accès, agréger et surveiller les journaux nécessaires, mettre en œuvre des mécanismes d'alerte efficaces et développer des capacités de réponse et d'investigation.

Chacun de ces domaines joue un rôle tout aussi important pour une réponse efficace aux incidents. Aucun programme de réponse aux incidents n’est complet ou efficace sans ces trois aspects. Au cours de la préparation, vous devez intégrer étroitement le personnel, les processus et la technologie afin de pouvoir faire face aux incidents.

Personnes

Pour répondre à un événement de sécurité, vous devez identifier les parties prenantes susceptibles de soutenir la réponse à un événement de sécurité. En outre, il est essentiel pour une réponse efficace de les former aux AWS technologies et à votre AWS environnement.

Définissez les rôles et les responsabilités

La gestion des événements de sécurité exige une discipline interorganisationnelle et une volonté d'action. Au sein de votre structure organisationnelle, de nombreuses personnes doivent être responsables, tenues de rendre des comptes, consultées ou tenues informées lors d'un incident. Il peut notamment s'agir de représentants des ressources humaines (RH), de l'équipe de direction et du service juridique. Tenez compte de ces rôles et responsabilités et déterminez si des tiers doivent être impliqués. Notez que dans de nombreuses zones géographiques, des lois locales régissent ce qui doit être fait et ce qui ne doit pas être fait. Bien que l'élaboration d'un tableau responsable, responsable, consulté et informé (RACI) pour vos plans d'intervention en matière de sécurité puisse sembler bureaucratique, cela permet une communication rapide et directe et décrit clairement le leadership à suivre aux différentes étapes de l'événement.

Lors d'un incident, il est essentiel d'inclure les propriétaires/développeurs des applications et des ressources touchées, car ce sont des experts en la matière (SMEs) qui peuvent fournir des informations et un contexte pour aider à mesurer l'impact. Assurez-vous d'établir et de maintenir des relations avec les développeurs et les propriétaires d'applications avant de vous fier à leur expertise pour répondre aux incidents. Les propriétaires d'applications ouSMEs, tels que vos administrateurs ou ingénieurs cloud, peuvent avoir besoin d'agir dans des situations où l'environnement n'est pas familier ou complexe, ou lorsque les intervenants n'y ont pas accès.

Enfin, des relations de confiance peuvent être impliquées dans l'enquête ou l'intervention, car elles peuvent apporter une expertise supplémentaire et un examen minutieux. Si vous ne possédez pas ces compétences au sein de votre propre équipe, vous pouvez faire appel à un tiers pour obtenir de l'aide.

Former le personnel de réponse aux incidents

Il sera essentiel de former votre personnel de réponse aux incidents aux technologies utilisées par leur organisation pour qu'il puisse réagir de manière adéquate à un événement de sécurité. Les réponses peuvent être prolongées si les membres de votre personnel ne comprennent pas les technologies sous-jacentes. Outre les concepts traditionnels de réponse aux incidents, il est également important qu'ils comprennent les AWS services et leur AWS environnement. Il existe un certain nombre de mécanismes traditionnels pour former le personnel chargé de votre incident, tels que la formation en ligne et la formation en classe. Vous devriez également envisager d'organiser des journées de jeu ou des simulations comme mécanisme d'entraînement. Pour plus de détails sur la façon d'exécuter des simulations, consultez la the section called "Exécutez des simulations régulières" section de ce document.

Comprendre les AWS Cloud technologies

Pour réduire les dépendances et réduire le temps de réponse, assurez-vous que vos équipes de sécurité et les intervenants sont formés aux services cloud et qu'ils ont la possibilité de s'entraîner sur le terrain avec l'environnement cloud spécifique utilisé par votre entreprise. Pour que les intervenants en cas d'incident soient efficaces, il est important de comprendre AWS les fondementsIAM, AWS Organizations les services de AWS journalisation et de surveillance, ainsi que les services AWS de sécurité.

AWS propose des ateliers de sécurité en ligne (voir Ateliers de AWS sécurité) où vous pouvez acquérir une expérience pratique des services AWS de sécurité et de surveillance. AWS propose également un certain nombre d'options de formation et de parcours d'apprentissage par le biais de la formation numérique, de la formation en classe, de partenaires de AWS formation et de certifications. Pour en savoir plus, reportez-vous à la section AWS Formation et certification.

Comprenez votre AWS environnement

Outre la compréhension AWS des services, de leurs cas d'utilisation et de la manière dont ils s'intègrent les uns aux autres, il est tout aussi important de comprendre comment l' AWS environnement de votre organisation est réellement conçu et quels sont les processus opérationnels en place. Souvent, de telles connaissances internes ne sont pas documentées et ne sont comprises que par quelques experts du domaine, ce qui peut créer des dépendances, entraver l'innovation et ralentir le temps de réponse.

Pour éviter ces dépendances et accélérer les temps de réponse, les connaissances internes de votre AWS environnement doivent être documentées, accessibles et comprises par vos analystes de sécurité. Comprendre l'ensemble de votre empreinte cloud nécessitera une collaboration entre les acteurs de sécurité concernés et les administrateurs du cloud. La préparation de vos processus de réponse aux incidents inclut notamment la documentation et la centralisation des diagrammes d'architecture, dont il sera question the section called “Documenter et centraliser les diagrammes d'architecture” plus loin dans ce livre blanc. Cependant, du point de vue des personnes, il est important que vos analystes puissent accéder aux diagrammes et aux processus opérationnels liés à votre AWS environnement et les comprendre.

Comprenez les équipes d' AWS intervention et le support

AWS Support

AWS Supportpropose une gamme de plans qui donnent accès à des outils et à une expertise qui favorisent le succès et la santé opérationnelle de vos AWS solutions. Si vous avez besoin d'un

support technique et de ressources supplémentaires pour planifier, déployer et optimiser votre AWS environnement, vous pouvez sélectionner le plan de support le mieux adapté à votre cas AWS d'utilisation.

Considérez le Centre de support situé dans le AWS Management Console (connexion requise) comme point de contact central pour obtenir de l'aide en cas de problème affectant vos AWS ressources. L'accès à AWS Support est contrôlé parIAM. Pour plus d'informations sur l'accès aux fonctionnalités de AWS Support, reportez-vous à la section Mise en route avec AWS Support.

De plus, si vous devez signaler un abus, contactez l'équipe AWS Tust and Safety.

AWS Équipe de réponse aux incidents clients (CIRT)

L'équipe de réponse aux incidents AWS clients (CIRT) est une AWS équipe mondiale spécialisée toujours disponible qui fournit une assistance aux clients lors d'événements de sécurité actifs du côté client dans le cadre du modèle de responsabilitéAWS partagée.

Lorsqu'il vous AWS CIRT soutiendra, vous recevrez une assistance pour le triage et le rétablissement en cas d'événement de sécurité actif. AWS Ils vous aideront à analyser les causes profondes grâce à l'utilisation des journaux de AWS service et vous fourniront des recommandations pour le rétablissement. Ils fourniront également des recommandations de sécurité et les meilleures pratiques pour vous aider à éviter les événements de sécurité à l'avenir.

AWS les clients peuvent les contacter AWS CIRT par le biais d'un dossier d'AWS assistance.

- Tous les clients :
  1. Account and billing (Compte et facturation)
  2. Service : Compte
  3. Catégorie : Sécurité
  4. Gravité : question générale

- Clients disposant de AWS Support forfaits pour développeurs :
  1. Account and billing (Compte et facturation)
  2. Service : Compte
  3. Catégorie : Sécurité
  4. Gravité : question importante

- Clients disposant d'un AWS Support plan d'affaires :

1. Account and billing (Compte et facturation)
2. Service : Compte
3. Catégorie : Sécurité
4. Gravité : question urgente ayant un impact sur les activités

- Clients disposant d'un AWS Support forfait Enterprise :
  1. Account and billing (Compte et facturation)
  2. Service : Compte
  3. Catégorie : Sécurité
  4. Gravité : question critique du risque commercial

- Clients abonnés à AWS Security Incident Response : Ouvrez la console Security Incident Response à l'adresse https://console.aws.amazon.com/security-ir/

DDoSsupport de réponse

AWS offers AWS Shield, qui fournit un service de protection géré par déni de service distribué (DDoS) qui protège les applications Web exécutées sur AWS. AWS Shield fournit une détection permanente et des mesures d'atténuation automatiques en ligne qui peuvent minimiser les temps d'arrêt et la latence des applications, de sorte qu'il n'est pas nécessaire de s'engager AWS Support pour bénéficier de la protection. DDoS Il existe deux niveaux AWS Shield : Shield Standard et Shield Advanced. Pour en savoir plus sur les différences entre ces deux niveaux, consultez la documentation des fonctionnalités du Shield.

AWS Managed Services (AMS)

AWS Managed Services(AMS) assure la gestion continue de votre AWS infrastructure afin que vous puissiez vous concentrer sur vos applications. En mettant en œuvre les meilleures pratiques pour maintenir votre infrastructure, vous AMS contribuez à réduire vos frais d'exploitation et vos risques. AMSautomatise les activités courantes telles que les demandes de modification, la surveillance, la gestion des correctifs, la sécurité et les services de sauvegarde, et fournit des services de cycle de vie complets pour fournir, exécuter et soutenir votre infrastructure.

AMSassume la responsabilité du déploiement d'une suite de contrôles de sécurité et fournit une première ligne de réponse quotidienne aux alertes. Lorsqu'une alerte est déclenchée, AMS suivez un ensemble standard de playbooks automatisés et manuels pour vérifier une réponse cohérente. Ces

playbooks sont partagés avec les AMS clients lors de l'intégration afin qu'ils puissent développer et coordonner une réponse avec. AMS

Processus

L'élaboration de processus de réponse aux incidents complets et clairement définis est essentielle à la réussite et à l'évolutivité du programme de réponse aux incidents. Lorsqu'un événement de sécurité survient, des étapes et des flux de travail clairs vous aideront à réagir rapidement. Il se peut que vous disposiez déjà d'un processus de réponse aux incidents. Quel que soit votre état actuel, il est important de mettre à jour, d'itérer et de tester régulièrement vos processus de réponse aux incidents.

Élaboration et test d'un plan de réponse aux incidents

Le premier document à développer pour la réponse aux incidents est le plan de réponse aux incidents. Le plan d'intervention en cas d'incident est conçu pour servir de base à votre programme et à votre stratégie de réponse aux incidents. Un plan de réponse aux incidents est un document de haut niveau qui comprend généralement les sections suivantes :

- Vue d'ensemble de l'équipe de réponse aux incidents : décrit les objectifs et les fonctions de l'équipe de réponse aux incidents
- Rôles et responsabilités — Répertorie les parties prenantes de la réponse aux incidents et détaille leurs rôles en cas d'incident
- Un plan de communication — Détaille les informations de contact et la manière dont vous communiquerez lors d'un incident

  Il est recommandé d'utiliser la out-of-band communication comme solution de rechange à la communication en cas d'incident. AWS Wickr est un exemple d'application fournissant un canal de out-of-band communication sécurisé.
- Phases de réponse aux incidents et mesures à prendre — Énumère les phases de réponse aux incidents (par exemple, détecter, analyser, éradiquer, contenir et rétablir), y compris les actions de haut niveau à prendre au cours de ces phases
- Définitions de la gravité et de la hiérarchisation des incidents : explique comment classer la gravité d'un incident, comment hiérarchiser l'incident, puis comment les définitions de gravité affectent les procédures d'escalade

Bien que ces sections soient communes à des entreprises de tailles et de secteurs différents, le plan d’intervention en cas d’incident de chaque organisation est unique. Vous devrez élaborer un plan de réponse aux incidents qui convient le mieux à votre organisation.

Documenter et centraliser les diagrammes d'architecture

Pour réagir rapidement et avec précision à un événement de sécurité, vous devez comprendre l'architecture de vos systèmes et réseaux. La compréhension de ces modèles internes est non seulement importante pour la réponse aux incidents, mais également pour vérifier la cohérence entre les applications avec lesquelles les modèles sont conçus, conformément aux meilleures pratiques. Vous devez également vérifier que cette documentation est à jour et régulièrement mise à jour conformément aux nouveaux modèles d'architecture. Vous devez développer une documentation et des référentiels internes détaillant des éléments tels que :

- AWS structure du compte - Vous devez savoir :
  - Combien de AWS comptes possédez-vous ?
  - Comment sont organisés ces AWS comptes ?
  - Qui sont les propriétaires commerciaux des AWS comptes ?
  - Utilisez-vous les politiques de contrôle des services (SCPs) ? Dans l'affirmative, quels sont les garde-fous organisationnels mis en œuvre en utilisant ? SCPs
  - Limitez-vous les régions et les services qui peuvent être utilisés ?
  - Quelles sont les différences entre les unités commerciales et les environnements (dev/test/prod) ?
- AWS modèles de service
  - Quels sont AWS les services que vous utilisez ?
  - Quels sont les AWS services les plus utilisés ?
- Modèles d'architecture
  - Quelles architectures cloud utilisez-vous ?
- AWS modèles d'authentification
  - Comment vos développeurs s'authentifient-ils généralement ? AWS
  - Utilisez-vous IAM des rôles ou des utilisateurs (ou les deux) ? Votre système d'authentification est-il AWS connecté à un fournisseur d'identité (IdP) ?
  - Comment associer un IAM rôle ou un utilisateur à un employé ou à un système ?
  - Comment l'accès est-il révoqué lorsqu'une personne n'est plus autorisée ?
- AWS modèles d'autorisation

  - Quelles sont IAM les politiques utilisées par vos développeurs ?
  - Utilisez-vous des politiques basées sur les ressources ?
- Journalisation et surveillance
  - Quelles sources de journalisation utilisez-vous et où sont-elles stockées ?
  - Agrégez-vous AWS CloudTrail les journaux ? Dans l'affirmative, où sont-ils conservés ?
  - Comment interrogez-vous CloudTrail les journaux ?
  - Amazon est-il GuardDuty activé ?
  - Comment accèdez-vous aux GuardDuty résultats (par exemple, console, système de billetterieSIEM) ?
  - Les résultats ou les événements sont-ils agrégés dans un SIEM ?
  - Les tickets sont-ils créés automatiquement ?
  - Quels sont les outils mis en place pour analyser les journaux dans le cadre d'une enquête ?
- Topologie du réseau
  - Comment les appareils, les points de terminaison et les connexions de votre réseau sont-ils organisés physiquement ou logiquement ?
  - Comment se connecte votre réseau AWS ?
  - Comment le trafic réseau est-il filtré entre les environnements ?
- Infrastructures externes
  - Comment sont déployées les applications orientées vers l'extérieur ?
  - Quelles sont les AWS ressources accessibles au public ?
  - Quels AWS comptes contiennent des infrastructures orientées vers l'extérieur ?
  - Qu'est-ce qu'il y a un filtrage DDoS ou un filtrage externe ?

La documentation des schémas techniques et des processus internes facilite le travail de l'analyste de réponse aux incidents, en l'aidant à acquérir rapidement les connaissances institutionnelles nécessaires pour répondre à un événement de sécurité. Une documentation complète des processus techniques internes simplifie non seulement les enquêtes de sécurité, mais permet également de rationaliser et d'évaluer les processus.

Élaborez des manuels de réponse aux incidents

L’élaboration de playbooks est une étape clé de la préparation de vos processus de réponse aux incidents. Les playbooks de réponse aux incidents fournissent une série de recommandations et

d’étapes à suivre en cas d’événement de sécurité. Le fait de disposer d’une structure et d’étapes claires simplifie la réponse et réduit le risque d’erreur humaine.

Pour quoi créer des playbooks

Il est recommandé de créer des playbooks dans les scénarios d’incidents suivants :

- Incidents attendus — Des playbooks doivent être créés pour les incidents que vous anticipez. Cela inclut des menaces telles que le déni de service (DoS), les rançongiciels et la compromission des informations d’identification.
- Constatations ou alertes de sécurité connues — Des playbooks doivent être créés pour vos découvertes et alertes de sécurité connues, telles que GuardDuty les découvertes. Vous pourriez recevoir une GuardDuty découverte et vous demander : « Et maintenant ? » Pour éviter de mal gérer un GuardDuty résultat ou de l'ignorer, créez un manuel pour chaque résultat potentiel GuardDuty. Vous trouverez des informations et des conseils sur les mesures correctives dans la GuardDutydocumentation. Il convient de noter que cela n' GuardDuty est pas activé par défaut et qu'il entraîne un coût. GuardDuty Vous trouverez plus de détails à ce sujet dans l'annexe A : Définitions des fonctionnalités cloud -the section called “Visibilité et alertes”.

Ce qu'il faut inclure dans les playbooks

Les playbooks doivent contenir les étapes techniques qu’un analyste de sécurité doit suivre afin d’enquêter de manière adéquate et de répondre à un éventuel incident de sécurité.

Les éléments à inclure dans un playbook incluent :

- Présentation du playbook — Quel scénario de risque ou d'incident ce playbook aborde-t-il ? Quel est l’objectif du playbook ?
- Conditions préalables — Quels journaux et mécanismes de détection sont nécessaires pour ce scénario d'incident ? Quelle est la notification attendue ?
- Informations sur les parties prenantes — Qui est impliqué et quelles sont ses coordonnées ? Quelles sont les responsabilités de chacune des parties prenantes ?
- Étapes de réponse — Quelles mesures tactiques devraient être prises au cours des différentes phases de la réponse aux incidents ? Quelles requêtes un analyste doit-il exécuter ? Quel code doit être exécuté pour obtenir le résultat souhaité ?
  - Détecter — Comment l'incident sera-t-il détecté ?
  - Analyser — Comment l'ampleur de l'impact sera-t-elle déterminée ?
  - Contenir — Comment l'incident sera-t-il isolé pour en limiter la portée ?

  - Éradiquer — Comment la menace sera-t-elle éliminée de l'environnement ?
  - Restaurer — Comment le système ou la ressource concernés seront-ils remis en production ?
- Résultats attendus — Une fois les requêtes et le code exécutés, quel est le résultat attendu du playbook ?

Pour vérifier la cohérence des informations contenues dans chaque playbook, il peut être utile de créer un modèle de playbook à utiliser dans vos autres playbooks de sécurité. Certains des éléments listés précédemment, tels que les informations sur les parties prenantes, peuvent être partagés entre plusieurs playbooks. Si tel est le cas, vous pouvez créer une documentation centralisée pour ces informations et la référencer dans le playbook, puis énumérer les différences explicites dans le playbook. Cela vous évitera d'avoir à mettre à jour les mêmes informations dans tous vos playbooks individuels. En créant un modèle et en identifiant les informations communes ou partagées dans les playbooks, vous pouvez simplifier et accélérer le développement des playbooks. Enfin, vos playbooks évolueront probablement au fil du temps ; une fois que vous aurez confirmé que les étapes sont cohérentes, cela constitue la condition requise pour l'automatisation.

Exemples de playbooks

Vous trouverez un certain nombre d'exemples de playbooks à l'annexe B dansthe section called “Ressources du Playbook”. Les exemples présentés ici peuvent vous aider à choisir les playbooks à créer et les éléments à inclure dans vos playbooks. Cependant, il est important que vous élaboriez des stratégies qui intègrent les risques les plus pertinents pour votre entreprise. Vous devez vérifier que les étapes et les flux de travail de vos playbooks incluent vos technologies et processus.

Exécutez des simulations régulières

Organisations grandissent et évoluent au fil du temps, tout comme le paysage des menaces. C'est pourquoi il est important de revoir en permanence vos capacités de réponse aux incidents. Les simulations sont l'une des méthodes qui peuvent être utilisées pour effectuer cette évaluation. Les simulations utilisent des scénarios d'événements de sécurité réels conçus pour imiter les tactiques, les techniques et les procédures d'un acteur menaçant (TTPs) et permettre à une organisation d'exercer et d'évaluer ses capacités de réponse aux incidents en réagissant à ces cyberévénements simulés tels qu'ils peuvent se produire dans la réalité.

Les simulations présentent de nombreux avantages, notamment :

- Validation de l’état de préparation à la cybersécurité et renforcement de la confiance de vos intervenants en cas d’incident.

- Test de la précision et de l’efficacité des outils et des flux de travail.
- Amélioration des méthodes de communication et de remontées en fonction de votre plan d’intervention en cas d’incident.
- Possibilité de répondre à des vecteurs moins courants.

Types de simulations

Il existe trois principaux types de simulations :

- Exercices sur table — L'approche théorique des simulations est strictement une session basée sur des discussions impliquant les différents acteurs de la réponse aux incidents afin de mettre en pratique leurs rôles et responsabilités et d'utiliser les outils de communication et les manuels de stratégie établis. La facilitation des exercices peut généralement être réalisée en une journée complète dans un lieu virtuel, un lieu physique ou une combinaison des deux. En raison de sa nature basée sur la discussion, l'exercice sur table met l'accent sur les processus, les personnes et la collaboration. La technologie fait partie intégrante de la discussion ; toutefois, l'utilisation réelle d'outils ou de scripts de réponse aux incidents ne fait généralement pas partie de l'exercice théorique.
- Exercices Purple Team — Les exercices Purple Team augmentent le niveau de collaboration entre les intervenants en cas d'incident (équipe bleue) et les acteurs de menaces simulés (équipe rouge). L'équipe bleue est généralement composée de membres du Security Operations Center (SOC), mais peut également inclure d'autres parties prenantes qui seraient impliquées lors d'un véritable cyberévénement. L'équipe rouge est généralement composée d'une équipe de tests d'intrusion ou de parties prenantes clés formées à la sécurité offensive. L'équipe rouge travaille en collaboration avec les animateurs de l'exercice lors de la conception d'un scénario afin que celui-ci soit précis et réalisable. Au cours des exercices Purple Team, l'accent est mis principalement sur les mécanismes de détection, les outils et les procédures opérationnelles standard (SOPs) qui soutiennent les efforts de réponse aux incidents.
- Exercices de l'équipe rouge — Au cours d'un exercice de l'équipe rouge, l'attaque (l'équipe rouge) effectue une simulation pour atteindre un certain objectif ou un ensemble d'objectifs dans un cadre prédéterminé. Les défenseurs (Blue Team) ne connaîtront pas nécessairement la portée et la durée de l'exercice, ce qui permet une évaluation plus réaliste de la manière dont ils réagiraient en cas d'incident réel. Comme les exercices Red Team peuvent être des tests invasifs, vous devez faire preuve de prudence et mettre en place des contrôles pour vérifier que l'exercice ne cause pas de dommages réels à votre environnement.

> **Note**
>
> AWS demande aux clients de consulter la politique relative aux tests d'intrusion disponible sur le site Web des tests de pénétration avant d'effectuer des exercices Purple Team ou Red Team.

Le tableau 1 résume quelques différences clés entre ces types de simulations. Il est important de noter que les définitions sont généralement considérées comme des définitions vagues et peuvent être personnalisées pour répondre aux besoins de votre organisation.

Tableau 1 — Types de simulations

	Exercice sur table	Exercice Purple Team	Exercice Red Team
Résumé	Des exercices sur support papier qui se concentrent sur un scénario d'incident de sécurité spécifique. Ils peuvent être de haut niveau ou techniques et sont entraînés par une série d'injections de papier.	Une offre plus réaliste que les exercices sur table. Au cours des exercices Purple Team, les animateurs travaillent en collaboration avec les participants pour accroître leur engagement et proposer des formations si nécessaire.	Il s'agit généralement d'une offre de simulation plus avancée. Il y a généralement un niveau élevé de discrétion, les participants ne connaissant peut-être pas tous les détails de l'exercice.
Ressources nécessaires	Ressources techniques limitées requises	Diverses parties prenantes sont requises et des ressources techniques de haut niveau sont nécessaires	Diverses parties prenantes sont requises et des ressources techniques de haut niveau sont nécessaires
Complexité	Faible	Medium	Élevé

Envisagez d’animer des simulations cybernétiques à intervalles réguliers. Chaque type d'exercice peut apporter des avantages uniques aux participants et à l'organisation dans son ensemble. Vous pouvez donc choisir de commencer par des types de simulation moins complexes (tels que des exercices sur table) et de passer à des types de simulation plus complexes (exercices Red Team). Vous devez sélectionner un type de simulation en fonction de la maturité de votre sécurité, de vos ressources et des résultats souhaités. Certains clients peuvent choisir de ne pas effectuer les exercices Red Team en raison de leur complexité et de leur coût.

Cycle de vie des exercices

Quel que soit le type de simulation que vous choisissez, les simulations suivent généralement les étapes suivantes :

1. Définir les principaux éléments de l'exercice : définissez le scénario de simulation et les objectifs de la simulation. Les deux doivent être acceptés par les dirigeants.
2. Identifier les principales parties prenantes — À tout le moins, un exercice nécessite des animateurs et des participants. Selon le scénario, d’autres parties prenantes telles que les services juridiques, l’équipe de communication ou la direction, peuvent être impliquées.
3. Élaborez et testez le scénario : le scénario devra peut-être être redéfini au fur et à mesure de sa création si certains éléments ne sont pas réalisables. Un scénario finalisé est attendu à l’issue de cette étape.
4. Faciliter la simulation — Le type de simulation détermine la facilitation utilisée (scénario papier par rapport à un scénario simulé hautement technique). Les animateurs doivent adapter leurs tactiques d’animation aux objectifs de l’exercice et impliquer tous les participants dans l’exercice dans la mesure du possible afin d’en tirer le meilleur parti.
5. Rédiger le rapport après action (AAR) — Identifiez les domaines qui se sont bien déroulés, ceux qui peuvent être améliorés et les lacunes potentielles. Ils AAR doivent mesurer l'efficacité de la simulation ainsi que la réponse de l'équipe à l'événement simulé afin que les progrès puissent être suivis au fil du temps lors de futures simulations.

Technologie

Si vous développez et mettez en œuvre les technologies appropriées avant un incident de sécurité, votre personnel de réponse aux incidents sera en mesure d'enquêter, d'en comprendre la portée et de prendre des mesures en temps opportun.

Développer la structure des AWS comptes

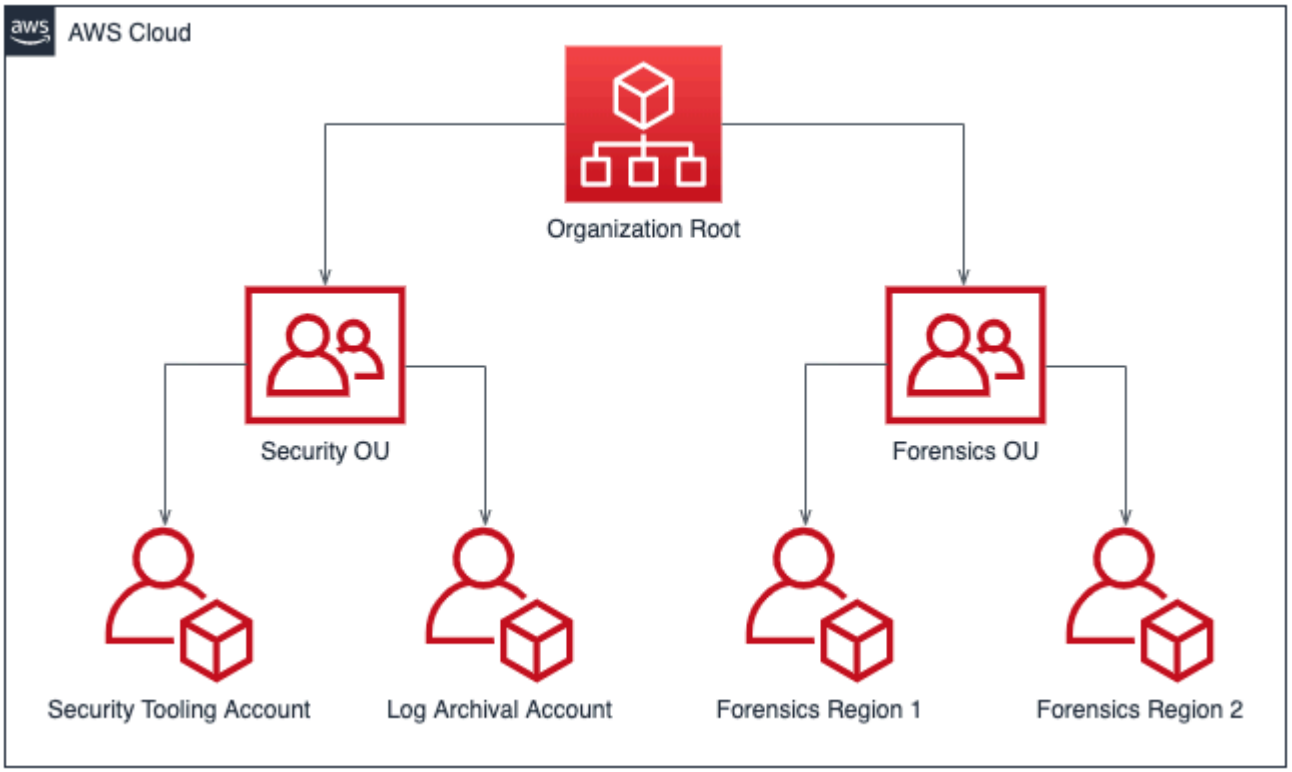
AWS Organizationspermet de gérer et de gouverner de manière centralisée un AWS environnement à mesure que vous développez et augmentez AWS les ressources. Une AWS organisation consolide vos AWS comptes afin que vous puissiez les administrer en tant qu'unité unique. Vous pouvez utiliser les unités organisationnelles (OUs) pour regrouper les comptes afin de les administrer en tant qu'unité unique.

Pour la réponse aux incidents, il est utile de disposer d'une structure de AWS compte prenant en charge les fonctions de réponse aux incidents, qui comprend une unité d'organisation de sécurité et une unité d'organisation médico-légale. Au sein de l'unité d'organisation de sécurité, vous devez disposer de comptes pour :

- Archivage des journaux — Regroupez les journaux dans un compte d'archivage des AWS journaux.
- Outils de sécurité — Centralisez les services de sécurité dans un compte d'outil AWS de sécurité. Ce compte joue le rôle d'administrateur délégué pour les services de sécurité.

Au sein de l'unité d'organisation d'analyse poussée, vous avez la possibilité de mettre en place un ou plusieurs comptes d'analyse poussée pour chaque région dans laquelle vous opérez, selon ce qui convient le mieux à votre entreprise et à votre modèle opérationnel. Par exemple, si vous opérez uniquement dans l'est des États-Unis (Virginie du Nord) (us-east-1) et dans l'ouest des États-Unis (Oregon) (us-west-2), vous aurez deux comptes dans l'unité d'organisation forensics : un pour us-east-1 et un pour us-west-2. Étant donné que la mise en place de nouveaux comptes prend du temps, il est impératif de créer et d'instrumenter les comptes d'analyse poussée bien avant un incident afin que les intervenants puissent être prêts à les utiliser efficacement pour intervenir.

Le diagramme suivant présente un exemple de structure de compte, y compris une unité d'organisation d'analyse poussée avec des comptes d'analyse poussée par région :



Structure de compte par région pour la réponse aux incidents

Élaboration et mise en œuvre d’une stratégie de marquage

Il peut être difficile d'obtenir des informations contextuelles sur le cas d'utilisation métier et les parties prenantes internes concernées par une AWS ressource. Pour ce faire, vous pouvez notamment utiliser des balises, qui attribuent des métadonnées à vos AWS ressources et consistent en une clé et une valeur définies par l'utilisateur. Vous pouvez créer des balises pour classer les ressources par objectif, propriétaire, environnement, type de données traitées et d’autres critères de votre choix.

Une stratégie de balisage cohérente peut accélérer les temps de réponse en vous permettant d'identifier et de discerner rapidement les informations contextuelles relatives à une ressource. AWS Les balises peuvent également servir de mécanisme pour initier l’automatisation des réponses. Pour plus d'informations sur les éléments à étiqueter, reportez-vous à la documentation sur le balisage AWS des ressources. Vous devez d’abord définir les balises que vous souhaitez implémenter dans votre organisation. Ensuite, vous mettez en œuvre et appliquez cette stratégie de balisage. Vous trouverez des détails sur la mise en œuvre et l'application dans le AWS blog Implémenter une stratégie de balisage AWS des ressources à l'aide des politiques de AWS balise et des politiques de contrôle des services (SCPs).

Mettre à jour les informations de contact du AWS compte

Pour chacun de vos AWS comptes, il est important de disposer d'informations et de up-to-date coordonnées précises afin que les parties prenantes concernées reçoivent des notifications importantes AWS sur des sujets tels que la sécurité, la facturation et les opérations. Pour chaque AWS compte, vous avez un contact principal et des contacts alternatifs pour la sécurité, la facturation et les opérations. Les différences entre ces contacts peuvent être trouvées dans le Guide de référence AWS sur la gestion des comptes.

Pour plus de détails sur la gestion des contacts alternatifs, reportez-vous à la AWS documentation sur l'ajout, la modification ou la suppression de contacts alternatifs. Il est recommandé d'utiliser une liste de distribution d'e-mails si votre équipe gère les problèmes liés à la facturation, aux opérations et à la sécurité. Une liste de distribution d'e-mails supprime les dépendances à l'égard d'une seule personne, ce qui peut entraîner des blocages si cette personne n'est pas au bureau ou quitte l'entreprise. Vous devez également vérifier que l'adresse e-mail et les coordonnées du compte, y compris le numéro de téléphone, sont bien protégés afin de vous protéger contre la réinitialisation du mot de passe du compte root et la réinitialisation de l'authentification multifactorielle (MFA).

Pour les clients utilisateurs AWS Organizations, les administrateurs de l'organisation peuvent gérer de manière centralisée les contacts alternatifs pour les comptes des membres à l'aide du compte de gestion ou d'un compte d'administrateur délégué sans avoir besoin d'informations d'identification pour chaque AWS compte. Vous devrez également vérifier que les informations de contact des comptes nouvellement créés sont exactes. Reportez-vous à la section Mettre à jour automatiquement les contacts alternatifs pour les articles de Comptes AWS blog nouvellement créés.

Préparez l'accès à Comptes AWS

Lors d'un incident, vos équipes de réponse aux incidents doivent avoir accès aux environnements et aux ressources impliqués dans l'incident. Assurez-vous que vos équipes disposent d'un accès approprié pour accomplir leurs tâches avant qu'un événement ne se produise. Pour ce faire, vous devez connaître le niveau d'accès dont les membres de votre équipe ont besoin (par exemple, les types d'actions qu'ils sont susceptibles d'entreprendre) et vous devez prévoir à l'avance un accès avec le moindre privilège.

Pour mettre en œuvre et fournir cet accès, vous devez identifier et discuter de la stratégie de AWS compte et de la stratégie d'identité cloud avec les architectes cloud de votre entreprise afin de comprendre quelles méthodes d'authentification et d'autorisation sont configurées. En raison de la nature privilégiée de ces informations d'identification, vous devez envisager d'utiliser des flux d'approbation ou de récupérer des informations d'identification dans un coffre-fort ou un coffre-fort

dans le cadre de votre implémentation. Après la mise en œuvre, vous devez documenter et tester l'accès des membres de l'équipe bien avant qu'un événement ne se produise afin de vous assurer qu'ils peuvent réagir sans délai.

Enfin, les utilisateurs créés spécifiquement pour répondre à un incident de sécurité sont souvent privilégiés afin de fournir un accès suffisant. Par conséquent, l'utilisation de ces informations d'identification doit être restreinte, surveillée et ne pas être utilisée pour les activités quotidiennes.

Comprenez le paysage des menaces

Développez des modèles de menaces

En développant des modèles de menaces, les entreprises peuvent identifier les menaces et les mesures d'atténuation avant qu'un utilisateur non autorisé ne le fasse. Il existe un certain nombre de stratégies et d'approches en matière de modélisation des menaces ; consultez le billet de blog Comment aborder la modélisation des menaces. Pour la réponse aux incidents, un modèle de menace peut aider à identifier les vecteurs d'attaque qu'un acteur de la menace aurait pu utiliser lors d'un incident. Il sera essentiel de comprendre ce contre quoi vous vous défendez afin de réagir rapidement. Vous pouvez également utiliser an AWS Partner pour la modélisation des menaces. Pour rechercher un AWS partenaire, utilisez le AWS Partner Network.

Intégrez et utilisez les renseignements sur les cybermenaces

Les renseignements sur les cybermenaces sont les données et l'analyse de l'intention, de l'opportunité et des capacités d'un acteur menaçant. L'obtention et l'utilisation de renseignements sur les menaces sont utiles pour détecter un incident à un stade précoce et pour mieux comprendre le comportement des auteurs de menaces. Les informations sur les cybermenaces incluent des indicateurs statiques tels que les adresses IP ou les hachages de fichiers contenant des logiciels malveillants. Il comprend également des informations de haut niveau, telles que les modèles de comportement et les intentions. Vous pouvez collecter des informations sur les menaces auprès d'un certain nombre de fournisseurs de cybersécurité et de référentiels open source.

Pour intégrer et optimiser les informations sur les menaces pour votre AWS environnement, vous pouvez utiliser certaines out-of-the-box fonctionnalités et intégrer vos propres listes de renseignements sur les menaces. Amazon GuardDuty utilise des sources AWS internes et tierces de renseignements sur les menaces. D'autres AWS services, tels qu'un DNS pare-feu et des AWS WAF règles, prennent également en compte les informations d'un AWS« groupe avancé de renseignement sur les menaces ». Certains GuardDuty résultats sont mis en correspondance avec le cadre MITRE ATT &CK, qui fournit des informations sur des observations réelles sur les tactiques et techniques de l'adversaire.

Sélection et configuration de journaux à des fins d’analyse et d’alerte

Au cours d’une enquête de sécurité, vous devez être en mesure d’examiner les journaux pertinents pour consigner et comprendre la portée et la chronologie complètes de l’incident. Des journaux sont également requis pour la génération d’alertes, indiquant que certaines actions intéressantes ont eu lieu. Il est essentiel de sélectionner, d’activer, de stocker et de configurer les mécanismes d’interrogation et de récupération et de configurer les alertes. Chacune de ces actions est examinée dans cette section. Pour plus de détails, consultez le billet de AWS blog sur les stratégies de journalisation pour la réponse aux incidents de sécurité.

Sélection et activation des sources de journalisation

Avant une enquête de sécurité, vous devez capturer les journaux pertinents afin de reconstituer rétroactivement l'activité d'un AWS compte. Sélectionnez et activez les sources de journal adaptées à la charge de travail de leur AWS compte.

AWS CloudTrail est un service de journalisation qui suit les API appels passés par rapport à un AWS compte et capture l'activité AWS du service. Il est activé par défaut avec une conservation de 90 jours des événements de gestion qui peuvent être récupérés via CloudTrail la fonction d'historique des événements à l'aide AWS Management Console de AWS CLI, ou un AWS SDK. Pour une conservation et une visibilité plus longues des événements liés aux données, vous devez créer un CloudTrail Trail associé à un compartiment Amazon S3, et éventuellement à un groupe de CloudWatch journaux. Vous pouvez également créer un CloudTrail lac, qui conserve CloudTrail les journaux pendant sept ans au maximum et fournit une fonction de requête SQL basée.

AWS recommande aux clients utilisant un trafic réseau VPC activé et DNS des journaux utilisant, respectivement, les journaux de requêtes VPCFlow Logs et Amazon Route 53 Resolver, en les diffusant soit vers un compartiment Amazon S3, soit vers un groupe de CloudWatch journaux. Vous pouvez créer un journal de VPC flux pour une interface réseauVPC, un sous-réseau ou un sous-réseau. Pour les journaux de VPC flux, vous pouvez choisir comment et où activer les journaux de flux afin de réduire les coûts.

AWS CloudTrail Les journaux, les journaux de VPC flux et les journaux de requêtes du résolveur Route 53 constituent les trois éléments de journalisation de base nécessaires aux enquêtes de sécurité. AWS

AWS les services peuvent générer des journaux qui ne sont pas capturés par les trifectas de journalisation de base, tels que les journaux Elastic Load Balancing, les journaux, AWS WAF les journaux des AWS Config enregistreurs, les GuardDuty résultats d'Amazon, les journaux d'audit

Amazon Elastic Kubernetes Service (EKSAmazon) et les journaux du système d'exploitation EC2 et des applications des instances Amazon. Consultez la liste complète the section called “Annexe A : Définitions des fonctionnalités du cloud” des options de journalisation et de surveillance.

Sélectionnez le stockage des journaux

Le choix du stockage des journaux dépend généralement de l'outil de requête que vous utilisez, des capacités de rétention, de la familiarité et du coût. Lorsque vous activez les journaux de AWS service, fournissez une installation de stockage, généralement un compartiment ou un groupe de CloudWatch journaux Amazon S3.

Un compartiment Amazon S3 fournit un stockage durable et rentable avec une politique de cycle de vie facultative. Les journaux stockés dans des compartiments Amazon S3 peuvent être interrogés de manière native à l'aide de services tels qu'Amazon Athena. Un groupe de CloudWatch journaux fournit un stockage durable et une fonction de requête intégrée via CloudWatch Logs Insights.

Identifier la conservation appropriée des journaux

Lorsque vous utilisez un compartiment ou un groupe de CloudWatch journaux S3 pour stocker des journaux, vous devez établir des cycles de vie adéquats pour chaque source de journaux afin d'optimiser les coûts de stockage et de récupération. Les clients disposent généralement de 3 à 12 mois de journaux facilement disponibles pour les requêtes, avec une durée de conservation pouvant aller jusqu'à sept ans. Le choix de la disponibilité et de la conservation doit correspondre à vos exigences en matière de sécurité et à un ensemble d’obligations statutaires, réglementaires et opérationnelles.

Sélection et mise en œuvre de mécanismes d'interrogation pour les journaux

Dans AWS, les principaux services que vous pouvez utiliser pour interroger les CloudWatch journaux sont Logs Insights pour les données stockées dans des groupes de CloudWatch journaux, et Amazon Athena et Amazon OpenSearch Service pour les données stockées dans Amazon S3. Vous pouvez également utiliser des outils de requête tiers tels que la gestion des informations et des événements de sécurité (SIEM).

Le processus de sélection d’un outil d’interrogation de journaux doit tenir compte des aspects humains, technologiques et de processus de vos opérations de sécurité. Choisissez un outil qui répond aux exigences opérationnelles, commerciales et de sécurité, et qui est à la fois accessible et maintenable à long terme. Gardez à l’esprit que les outils d’interrogation de journaux fonctionnent de manière optimale lorsque le nombre de journaux à analyser est maintenu dans les limites de l’outil. Il n'est pas rare que les clients disposent de plusieurs outils de requête en raison de contraintes

financières ou techniques. Par exemple, les clients peuvent faire appel SIEM à un tiers pour effectuer des requêtes portant sur les données des 90 derniers jours, et utiliser Athena pour effectuer des requêtes au-delà de 90 jours en raison du coût d'ingestion du journal d'un. SIEM Quelle que soit la mise en œuvre, vérifiez que votre approche minimise le nombre d'outils nécessaires pour optimiser l'efficacité opérationnelle, en particulier lors d'une enquête sur un événement de sécurité.

Utiliser les journaux pour les alertes

AWS fournit nativement des alertes via des services de sécurité, tels qu'Amazon GuardDuty AWS Security Hub, et. AWS Config Vous pouvez également utiliser des moteurs de génération d'alertes personnalisés pour les alertes de sécurité non couvertes par ces services ou pour les alertes spécifiques à votre environnement. La création de ces alertes et détections est abordée dans la section intitulée the section called “Détection” dans ce document.

Développer les capacités de criminalistique

Pour anticiper un incident de sécurité, envisagez de développer des fonctionnalités d’analyse poussée pour faciliter les enquêtes sur les événements de sécurité. Le Guide d'intégration des techniques médico-légales dans la réponse aux incidents NIST fournit de tels conseils.

Forensics sur AWS

Les concepts issus de la criminalistique traditionnelle sur site s'appliquent à. AWS Les stratégies relatives à l'environnement d'investigation médico-légale présentées dans le billet de AWS Cloud blog vous fournissent des informations clés vers lesquelles commencer à migrer leur expertise médico-légale. AWS

Une fois que vous aurez configuré votre environnement et votre structure de AWS compte pour la criminalistique, vous devrez définir les technologies nécessaires pour appliquer efficacement des méthodologies fiables sur le plan médico-légal au cours des quatre phases :

- Collecte — Collectez les AWS journaux pertinents AWS CloudTrail AWS Config, tels que les journaux de VPC flux et les journaux au niveau de l'hôte. Collectez des instantanés, des sauvegardes et des vidages de mémoire des ressources concernées AWS .
- Examen — Examinez les données collectées en extrayant et en évaluant les informations pertinentes.
- Analyse — Analysez les données collectées afin de comprendre l'incident et d'en tirer des conclusions.
- Rapports — Présentez les informations issues de la phase d'analyse.

Conservez les sauvegardes et les instantanés

La configuration de sauvegardes des systèmes et des bases de données clés s'avère essentielle pour récupérer d'un incident de sécurité et à des fins d'analyse poussée. Une fois les sauvegardes en place, vous pouvez restaurer vos systèmes à leur état stable antérieur. AWS Activé, vous pouvez prendre des instantanés de différentes ressources. Les instantanés vous fournissent des point-in-time copies de sauvegarde de ces ressources. De nombreux services AWS peuvent vous aider en matière de sauvegarde et de restauration. Reportez-vous au guide prescriptif de sauvegarde et de restauration pour plus de détails sur ces services et approches de sauvegarde et de restauration. Pour plus de détails, consultez le billet de blog Utiliser les sauvegardes pour récupérer après un incident de sécurité.

Il est essentiel que vos sauvegardes soient bien protégées, en particulier dans le cas de rançongiciels. Reportez-vous aux 10 meilleures pratiques de sécurité pour sécuriser les sauvegardes dans le billet de AWS blog pour obtenir des conseils sur la sécurisation de vos sauvegardes. Outre la sécurisation de vos sauvegardes, vous devez régulièrement tester vos processus de sauvegarde et de restauration pour vérifier que la technologie et les processus que vous avez mis en place fonctionnent comme prévu.

Automatisation de la criminalistique sur AWS

Lors d'un événement de sécurité, votre équipe de réponse aux incidents doit être en mesure de recueillir et d'analyser les preuves rapidement tout en maintenant la précision pendant la période entourant l'événement. Il est à la fois difficile et chronophage pour l'équipe de réponse aux incidents de collecter manuellement les preuves pertinentes dans un environnement cloud, en particulier sur un grand nombre d'instances et de comptes. De plus, la collecte manuelle peut faire l'objet d'erreurs humaines. Pour ces raisons, les clients doivent développer et mettre en œuvre l'automatisation pour la criminalistique.

AWS propose un certain nombre de ressources d'automatisation pour la criminalistique, qui sont regroupées dans l'annexe ci-dessous. the section called "Ressources médico-légales" Ces ressources sont des exemples de modèles d'analyse poussée que nous avons développés et que les clients ont mis en œuvre. Bien qu'elles puissent constituer une architecture de référence utile au départ, envisagez de les modifier ou de créer de nouveaux modèles d'automatisation de l'analyse poussée en fonction de votre environnement, de vos exigences, de vos outils et de vos processus d'analyse poussée.

Résumé des éléments de préparation

Une préparation minutieuse pour répondre aux événements de sécurité est essentielle pour une réponse rapide et efficace aux incidents. La préparation de la réponse aux incidents implique des personnes, des processus et des technologies. Ces trois domaines sont d'égale importance pour la préparation. Vous devez préparer et faire évoluer votre programme de réponse aux incidents dans les trois domaines.

Le tableau 2 résume les éléments de préparation détaillés dans cette section.

Tableau 2 — Éléments de préparation à la réponse aux incidents

Domaine	Article de préparation	Éléments d’action
Gens	Définissez les rôles et les responsabilités.	• Identifiez les parties prenantes concernées par la réponse aux incidents. • Élaborez un tableau responsable, responsable, informé et consulté (RACI) pour un incident.
Gens	Formez le personnel d'intervention en cas d'incident sur AWS.	• Formez les parties prenantes de la réponse aux incidents sur AWS les bases. • Formez les parties prenantes de la réponse aux incidents sur les services de AWS sécurité et de surveillance. • Formez les parties prenantes de la réponse aux incidents à votre AWS environnement et à son architecture.

Domaine	Article de préparation	Éléments d’action
Gens	Comprenez AWS les options de support.	• Comprenez les différenc es entre le AWS support, l'équipe de réponse aux incidents clients (CIRT), l'équipe de DDoS réponse (DRT) etAMS. • Comprenez le chemin de triage et d'escalade à suivre CIRT lors d'un événement de sécurité actif, si nécessaire.
Procédé	Élaborez un plan de réponse aux incidents.	• Créez un document de haut niveau qui définit votre programme et votre stratégie de réponse aux incidents. • Incluez un plan de communicationRACI, des définitions des incidents et les phases de réponse aux incidents dans le plan de réponse aux incidents.

Domaine	Article de préparation	Éléments d’action
Procédé	Documentez et centralisez les diagrammes d'architecture.	• Documentez les détails de la configuration de votre AWS environnement en termes de structure de compte, d'utilisation des services, de IAM modèles et d'autres fonctionnalités essentielles de votre AWS configuration. • Développez des diagramme s d'architecture de vos architectures cloud.
Procédé	Développez des manuels de réponse aux incidents.	• Créez un modèle pour la structure de vos playbooks. • Créez des playbooks pour les événements de sécurité attendus. • Créez des playbooks pour les alertes de sécurité connues, telles que GuardDuty les résultats.
Procédé	Effectuez régulièrement des simulations.	• Développez une cadence régulière pour exécuter des simulations d'incidents. • Utilisez les résultats et les leçons apprises pour peaufiner votre programme de réponse aux incidents.

Domaine	Article de préparation	Éléments d’action
Technologie	Développez une structure de AWS compte.	• Planifiez une structure de compte pour la façon dont les charges de travail sont séparées par AWS des comptes. • Créez une unité d'organisation de sécurité avec un outil de sécurité et un compte d'archivage des journaux. • Créez une UO de criminalistique avec des comptes de criminalistique pour chaque région dans laquelle vous exercez vos activités.
Technologie	Élaborez et mettez en œuvre une stratégie de marquage qui aide les intervenants à identifier la propriété et le contexte des résultats.	• Planifiez une stratégie de balisage et définissez les balises que vous souhaitez associer à vos AWS ressources. • Mettez en œuvre et appliquez la stratégie de balisage.

Domaine	Article de préparation	Éléments d’action
Technologie	Mettez à jour les informations de contact du AWS compte.	• Vérifiez que les informations de contact des AWS comptes sont répertoriées. • Créez des listes de distribution d'e-mails contenant les informations de contact afin de supprimer les points de défaillance uniques. • Protégez les comptes de messagerie associés aux informations du AWS compte.
Technologie	Préparez l'accès aux AWS comptes.	• Définissez les accès dont les intervenants auront besoin pour répondre à un incident. • Implémentez, testez et surveillez l'accès.
Technologie	Comprenez le paysage des menaces.	• Développez des modèles de menace pour votre environnement et vos applications. • Intégrez et utilisez les renseignements sur les cybermenaces.

Domaine	Article de préparation	Éléments d’action
Technologie	Sélectionnez et configurez les journaux.	• Identifiez et activez les journaux pour les enquêtes. • Sélectionnez le stockage des journaux. • Identifiez et implémentez la conservation des journaux. • Développez un mécanisme pour récupérer et interroger les journaux et les artefacts. • Utilisez les journaux pour les alertes.
Technologie	Développez des capacités de criminalistique.	• Identifiez les artefacts nécessaires à la collecte de données médico-légales. • Capturez et sécurisez les sauvegardes des principaux systèmes. • Définissez les mécanisme s d'analyse des journaux et artefacts identifiés. • Mettez en œuvre l'automat isation pour l'analyse médico-légale.

Une approche itérative est recommandée pour la préparation de la réponse aux incidents. Tous ces éléments de préparation ne peuvent pas être effectués du jour au lendemain ; vous devez créer un plan pour commencer modestement et améliorer continuellement vos capacités de réponse aux incidents au fil du temps.

Opérations

Les opérations sont au cœur de la réponse aux incidents. C’est à ce niveau que se déroulent les actions de réponse et de résolution des incidents de sécurité. Les opérations comprennent les cinq phases suivantes : détection, analyse, confinement, éradication et rétablissement. Les descriptions de ces phases et des objectifs se trouvent dans le tableau 3.

Tableau 3 — Phases d'exploitation

Phase	Objectif
Détection	Identifiez un événement de sécurité potentiel.
Analyse	Déterminez si un événement de sécurité est un incident et évaluez l'ampleur de l'incident.
Confinement	Minimisez et limitez la portée de l’événement de sécurité.
Éradication	Éliminez les ressources ou artefacts non autorisés liés à l’événement de sécurité. Mettez en œuvre les mesures d’atténuation à l’origine de l’incident de sécurité.
Récupération	Restaurez les systèmes dans un état sûr connu et surveillez ces systèmes pour vérifier que la menace ne revient pas.

Utilisez ces phases à titre de référence pour réagir de manière efficace et robuste aux incidents. Les actions que vous effectuerez varieront en fonction de l’incident lui-même. Un incident impliquant un rançongiciel, par exemple, nécessite un ensemble d’étapes de réponse différent de celui d’un incident impliquant un compartiment Amazon S3 public. De plus, ces phases ne se déroulent pas nécessairement de manière séquentielle. Après la maîtrise et l’éradication, vous devrez peut-être revenir à l’analyse pour déterminer si vos actions ont été efficaces.

Détection

L'alerte est l'élément principal de la phase de détection. Il génère une notification pour lancer le processus de réponse aux incidents en fonction de l'activité du AWS compte qui vous intéresse.

La précision des alertes est un défi ; il n'est pas toujours possible de déterminer avec une certitude absolue si un incident s'est produit, est en cours ou s'il se produira dans le futur. Voici quelques raisons :

- Les mécanismes de détection sont basés sur l'écart de référence, les modèles connus et les notifications émanant d'entités internes ou externes.
- En raison de la nature imprévisible de la technologie et des personnes, respectivement des moyens et des acteurs des incidents de sécurité, les données de référence changent au fil du temps. Des modèles malhonnêtes apparaissent grâce à des tactiques, techniques et procédures nouvelles ou modifiées utilisées par les auteurs de menaces (TTPs).
- Les modifications apportées aux personnes, aux technologies et aux processus ne sont pas immédiatement intégrées dans le processus de réponse aux incidents. Certains sont découverts au cours d'une enquête.

Sources d'alerte

Vous devriez envisager d'utiliser les sources suivantes pour définir les alertes :

- Résultats : AWS des services tels qu'Amazon GuardDuty AWS Security Hub, Amazon Macie, Amazon Inspector AWS Config, IAMAccess Analyzer et Network Access Analyzer génèrent des résultats qui peuvent être utilisés pour créer des alertes.
- Journaux : les journaux de AWS service, d'infrastructure et d'application stockés dans des compartiments et des groupes de CloudWatch journaux Amazon S3 peuvent être analysés et corrélés pour générer des alertes.
- Activité de facturation — Une modification soudaine de l'activité de facturation peut indiquer un événement de sécurité. Suivez la documentation sur la création d'une alarme de facturation pour surveiller vos AWS frais estimés afin de contrôler cela.
- Renseignements sur les cybermenaces — Si vous vous abonnez à un flux de renseignements tiers sur les cybermenaces, vous pouvez corréler ces informations avec d'autres outils de journalisation et de surveillance afin d'identifier les indicateurs potentiels d'événements.
- Outils destinés aux partenaires : Partners in the AWS Partner Network (APN) propose des produits haut de gamme qui peuvent vous aider à atteindre vos objectifs de sécurité. Pour la réponse aux incidents, des produits partenaires dotés de la technologie Endpoint Detection and Response (EDR) ou SIEM peuvent vous aider à atteindre vos objectifs de réponse aux incidents. Pour plus d'informations, consultez les sections Solutions pour partenaires de sécurité et Solutions de sécurité dans le AWS Marketplace.

- AWS confiance et sécurité : nous AWS Support pouvons contacter les clients si nous détectons une activité abusive ou malveillante.
- Contact ponctuel : comme ce sont peut-être vos clients, développeurs ou autres membres du personnel de votre entreprise qui remarquent quelque chose d'inhabituel, il est important de disposer d'une méthode connue et largement diffusée pour contacter votre équipe de sécurité. Les choix populaires incluent les systèmes de billetterie, les adresses e-mail de contact et les formulaires Web. Si votre organisation travaille avec le grand public, vous pourriez également avoir besoin d'un mécanisme de contact de sécurité destiné au public.

Pour plus d'informations sur les fonctionnalités du cloud que vous pouvez utiliser lors de vos enquêtes, reportez-vous the section called “Annexe A : Définitions des fonctionnalités du cloud” à ce document.

Détection dans le cadre de l'ingénierie des contrôles de sécurité

Les mécanismes de détection font partie intégrante du développement des contrôles de sécurité. Au fur et à mesure que les contrôles directifs et préventifs sont définis, des contrôles détectifs et réactifs connexes doivent être mis en place. Par exemple, une organisation établit un contrôle directif relatif à l'utilisateur root d'un AWS compte, qui ne doit être utilisé que pour des activités spécifiques et très bien définies. Ils l'associent à un contrôle préventif mis en œuvre en utilisant la politique de contrôle des services d'une AWS organisation (SCP). Si l'activité de l'utilisateur root dépasse le niveau de référence attendu, un contrôle de détection implémenté avec une EventBridge règle et un SNS sujet alertera le centre des opérations de sécurité (SOC). Le contrôle réactif implique de SOC sélectionner le playbook approprié, d'effectuer une analyse et de travailler jusqu'à ce que l'incident soit résolu.

La meilleure façon de définir les contrôles de sécurité est de modéliser les menaces associées aux charges de travail. AWS La criticité des contrôles de détection sera définie en examinant l'analyse de l'impact commercial (BIA) pour la charge de travail particulière. Les alertes générées par les contrôles de détection ne sont pas traitées telles qu'elles arrivent, mais plutôt en fonction de leur criticité initiale, à ajuster lors de l'analyse. L'ensemble de criticité initial est une aide à la priorisation ; le contexte dans lequel l'alerte s'est produite déterminera sa véritable criticité. Par exemple, une organisation utilise Amazon GuardDuty comme composant du contrôle de détection utilisé pour les EC2 instances faisant partie d'une charge de travail. Le résultat `Impact:EC2/SuspiciousDomainRequest.Reputation` est généré, vous informant que l'EC2instance Amazon répertoriée dans votre charge de travail interroge un nom de domaine soupçonné d'être malveillant. Cette alerte est définie par défaut comme étant de faible gravité et, au fur et à mesure que la phase d'analyse progresse, il a été déterminé que plusieurs centaines d'EC2instances de ce type `p4d.24xlarge` avaient été déployées par un acteur non autorisé, ce qui augmentait

considérablement les coûts d'exploitation de l'organisation. À ce stade, l'équipe de réponse aux incidents prend la décision d'ajuster le niveau de criticité de cette alerte à un niveau élevé, ce qui accroît le sentiment d'urgence et accélère les mesures à prendre. Notez que la gravité du GuardDuty résultat ne peut pas être modifiée.

Implémentations de Detective Control

Il est important de comprendre comment les contrôles de détection sont mis en œuvre, car ils permettent de déterminer comment l'alerte sera utilisée pour un événement donné. Il existe deux implémentations principales des contrôles techniques de détection :

- La détection comportementale repose sur des modèles mathématiques communément appelés apprentissage automatique (ML) ou intelligence artificielle (IA). La détection se fait par inférence ; par conséquent, l'alerte ne reflète pas nécessairement un événement réel.
- La détection basée sur des règles est déterministe ; les clients peuvent définir les paramètres exacts de l'activité pour laquelle ils doivent être alertés, et c'est certain.

Les implémentations modernes de systèmes de détection, tels qu'un système de détection d'intrusion (IDS), sont généralement équipées des deux mécanismes. Voici quelques exemples de détections basées sur des règles et comportementales avec. GuardDuty

- Lorsque le résultat `Exfiltration:IAMUser/AnomalousBehavior` est généré, il vous informe qu' « une API demande anormale a été observée dans votre compte ». En parcourant la documentation, vous découvrirez que « le modèle ML évalue toutes les API demandes de votre compte et identifie les événements anormaux associés aux techniques utilisées par les adversaires », ce qui indique que cette constatation est de nature comportementale.
- Pour le résultat`Impact:S3/MaliciousIPCaller`, GuardDuty il faut analyser les API appels provenant du service Amazon S3 en CloudTrail comparant l'élément du `SourceIPAddress` journal avec un tableau d'adresses IP publiques qui inclut des flux de renseignements sur les menaces. Une fois qu'il trouve une correspondance directe avec une entrée, il génère le résultat.

Nous vous recommandons de mettre en œuvre une combinaison d'alertes comportementales et basées sur des règles, car il n'est pas toujours possible de mettre en œuvre des alertes basées sur des règles pour chaque activité de votre modèle de menace.

Détection basée sur les personnes

Jusqu'à présent, nous avons discuté de la détection basée sur la technologie. L'autre source importante de détection provient des personnes internes ou externes à l'organisation du client. Les initiés peuvent être définis comme un employé ou un sous-traitant, et les étrangers sont des entités telles que les chercheurs en sécurité, les forces de l'ordre, les actualités et les réseaux sociaux.

Bien que la détection basée sur la technologie puisse être configurée de manière systématique, la détection basée sur les personnes se présente sous diverses formes, telles que les e-mails, les tickets, le courrier, les articles de presse, les appels téléphoniques et les interactions en personne. On peut s'attendre à ce que les notifications de détection basées sur la technologie soient transmises en temps quasi réel, mais aucun calendrier n'est prévu pour la détection basée sur les personnes. Il est impératif que la culture de sécurité intègre, facilite et renforce les mécanismes de détection basés sur les personnes pour une approche de défense approfondie en matière de sécurité.

Récapitulatif

En matière de détection, il est important de combiner des alertes basées sur des règles et des alertes basées sur le comportement. En outre, vous devez mettre en place des mécanismes permettant aux personnes internes et externes de soumettre un ticket concernant un problème de sécurité. Les humains peuvent être l'une des sources les plus précieuses d'incidents de sécurité. Il est donc important de mettre en place des processus permettant aux utilisateurs de faire part de leurs préoccupations. Vous devez utiliser les modèles de menace de votre environnement pour commencer à détecter les bâtiments. Les modèles de menaces vous aideront à créer des alertes basées sur les menaces les plus pertinentes pour votre environnement. Enfin, vous pouvez utiliser des frameworks tels que MITRE ATT &CK pour comprendre les tactiques, les techniques et les procédures des auteurs de menaces (TTPs). Le framework MITRE ATT &CK peut être utile à utiliser en tant que langage commun à vos différents mécanismes de détection.

Analyse

Les journaux, les fonctionnalités de requête et les informations sur les menaces ne sont que quelques-uns des éléments de support nécessaires à la phase d'analyse. La plupart des journaux utilisés pour la détection sont également utilisés pour l'analyse et nécessiteront l'intégration et la configuration d'outils de requête.

Valider, définir et évaluer l'impact de l'alerte

Au cours de la phase d'analyse, une analyse complète des journaux est effectuée dans le but de valider les alertes, de définir la portée et d'évaluer l'impact d'une éventuelle compromission.

- La validation de l'alerte est le point d'entrée de la phase d'analyse. Les intervenants en cas d'incident rechercheront des entrées de journal provenant de diverses sources et dialogueront directement avec les responsables de la charge de travail concernée.
- Le cadrage est l'étape suivante, lorsque toutes les ressources impliquées sont inventoriées et que la criticité des alertes est ajustée une fois que les parties prenantes ont convenu qu'il est peu probable qu'il s'agisse d'un faux positif.
- Enfin, l'analyse d'impact détaille l'interruption réelle de l'activité.

Une fois les composants de la charge de travail concernés identifiés, les résultats du cadrage peuvent être corrélés à l'objectif de point de reprise (RPO) et à l'objectif de temps de reprise () de la charge de travail correspondanteRTO, en ajustant la criticité des alertes, ce qui déclenchera l'allocation des ressources et toutes les activités suivantes. Tous les incidents ne perturberont pas directement le fonctionnement d'une charge de travail supportant un processus métier. Les incidents tels que la divulgation de données sensibles, le vol de propriété intellectuelle ou le détournement de ressources (comme dans le cas du minage de cryptomonnaies) peuvent ne pas arrêter ou affaiblir un processus métier immédiatement, mais peuvent avoir des conséquences ultérieurement.

Enrichissez les journaux de sécurité et les résultats

Enrichissement grâce aux renseignements sur les menaces et au contexte organisationnel

Au cours de l'analyse, les observables présentant un intérêt doivent être enrichis pour une meilleure contextualisation de l'alerte. Comme indiqué dans la section Préparation, l'intégration et l'exploitation des renseignements sur les cybermenaces peuvent être utiles pour mieux comprendre une constatation de sécurité. Les services de renseignement sur les menaces sont utilisés pour attribuer la réputation et la propriété aux adresses IP publiques, aux noms de domaine et aux hachages de fichiers. Ces outils sont disponibles sous forme de services payants et gratuits.

Les clients qui adoptent Amazon Athena comme outil de recherche de logs tirent parti des tâches AWS Glue pour charger les informations relatives aux menaces sous forme de tableaux. Les tables de renseignements sur les menaces peuvent être utilisées dans les SQL requêtes pour corréler les éléments du journal tels que les adresses IP et les noms de domaine, afin de fournir une vue enrichie des données à analyser.

AWS ne fournit pas de renseignements sur les menaces directement aux clients, mais des services tels qu'Amazon GuardDuty utilisent les renseignements sur les menaces pour les enrichir et générer des résultats. Vous pouvez également télécharger des listes de menaces personnalisées en GuardDuty fonction de vos propres informations sur les menaces.

Enrichissement grâce à l'automatisation

L'automatisation fait partie intégrante de la AWS Cloud gouvernance. Il peut être utilisé tout au long des différentes phases du cycle de vie de la réponse aux incidents.

Pour la phase de détection, l'automatisation basée sur des règles fait correspondre les modèles intéressants issus du modèle de menace dans les journaux et prend les mesures appropriées, telles que l'envoi de notifications. La phase d'analyse peut tirer parti du mécanisme de détection et transmettre le corps de l'alerte à un moteur capable d'interroger les journaux et d'enrichir les observables pour contextualiser l'événement.

Le corps d'alerte, dans sa forme fondamentale, est composé d'une ressource et d'une identité. Par exemple, vous pouvez implémenter une automatisation CloudTrail pour rechercher l' AWS APIactivité effectuée par l'identité ou la ressource de l'organisme d'alerte au moment de l'alerte, en fournissant des informations supplémentaires`eventSource`, notamment`eventName`,`SourceIPAddress`, et sur `userAgent` l'APIactivité identifiée. En effectuant ces requêtes de manière automatisée, les intervenants peuvent gagner du temps lors du triage et obtenir un contexte supplémentaire pour prendre des décisions plus éclairées.

Consultez le billet de blog How to enrich AWS Security Hub with account metadata (Comment enrichir les résultats du Security Hub avec les métadonnées des comptes) pour découvrir comment utiliser l'automatisation pour enrichir les résultats de sécurité et simplifier les analyses.

Recueillir et analyser des preuves médico-légales

La criminalistique, comme indiqué dans la the section called “Préparation” section de ce document, est le processus de collecte et d'analyse d'artefacts lors de la réponse à un incident. Activé AWS, il s'applique aux ressources du domaine de l'infrastructure telles que les captures de paquets de trafic réseau, le vidage de la mémoire du système d'exploitation et aux ressources du domaine de service telles que AWS CloudTrail les journaux.

Le processus de criminalistique présente les caractéristiques fondamentales suivantes :

- Cohérent — Il suit exactement les étapes documentées, sans écarts.
- Répétable — Il produit exactement les mêmes résultats lorsqu'il est répété sur le même artefact.
- Usuel — Il est documenté publiquement et largement adopté.

Il est important de maintenir une chaîne de traçabilité pour les artefacts collectés lors de l'intervention en cas d'incident. L'automatisation et la génération automatique de la documentation de cette

collection peuvent être utiles, en plus de stocker les artefacts dans des référentiels en lecture seule. L'analyse ne doit être effectuée que sur des répliques exactes des artefacts collectés afin de préserver l'intégrité.

Collectez des artefacts pertinents

Compte tenu de ces caractéristiques, et sur la base des alertes pertinentes et de l'évaluation de l'impact et de la portée, vous devrez collecter les données qui seront pertinentes pour une enquête et une analyse plus approfondies. Différents types et sources de données susceptibles d'être pertinents pour l'investigation, notamment les journaux de service/plan de contrôle (CloudTrailévénements de données Amazon S3, journaux de VPC flux), les données (métadonnées et objets Amazon S3) et les ressources (bases de données, EC2 instances Amazon).

Les journaux du plan de service/de contrôle peuvent être collectés pour une analyse locale ou, idéalement, directement interrogés à l'aide des AWS services natifs (le cas échéant). Les données (y compris les métadonnées) peuvent être directement consultées pour obtenir des informations pertinentes ou pour acquérir les objets sources ; par exemple, utilisez le AWS CLI pour acquérir les métadonnées du bucket et de l'objet Amazon S3 et acquérir directement les objets source. Les ressources doivent être collectées conformément au type de ressource et à la méthode d'analyse prévue. Par exemple, les bases de données peuvent être collectées en créant une partie copy/snapshot of the system running the database, creating a copy/snapshot de la base de données elle-même, ou en interrogeant et en extrayant certaines données et certains journaux de la base de données pertinents pour l'enquête.

Pour les EC2 instances Amazon, un ensemble spécifique de données doit être collecté et un ordre de collecte spécifique doit être exécuté afin d'acquérir et de conserver le plus grand nombre de données à des fins d'analyse et d'investigation.

Plus précisément, l'ordre de réponse permettant d'acquérir et de conserver le plus grand nombre de données d'une EC2 instance Amazon est le suivant :

1. Acquérir les métadonnées d'instance : acquérez les métadonnées d'instance pertinentes pour l'investigation et les requêtes de données (ID d'instance, type, adresse IP, ID VPC /subnet, région, ID Amazon Machine Image (AMI), groupes de sécurité attachés, heure de lancement).
2. Activez les protections et les balises d'instance : activez des protections d'instance telles que la protection contre la résiliation, la définition du comportement d'arrêt (s'il est défini pour s'arrêter), la désactivation des attributs Supprimer en cas de résiliation pour les EBS volumes attachés et l'application de balises appropriées à la fois pour la dénotation visuelle et pour l'utilisation dans d'éventuelles automatisations de réponse (par exemple, lors de l'application d'une balise avec le

nom `Status` et la valeur de`Quarantine`, effectuez une acquisition scientifique des données et isolez l'instance).

3. Acquérir un disque (EBSinstantanés) : obtenez un EBS instantané des EBS volumes attachés. Chaque instantané contient les informations dont vous avez besoin pour restaurer vos données (à partir du moment où l'instantané a été pris) sur un nouveau EBS volume. Consultez l'étape à suivre pour effectuer une collecte de réponses en temps réel/d'artefacts si vous utilisez des volumes de stockage d'instance.
4. Acquérir de la mémoire : étant donné que les EBS instantanés ne capturent que les données écrites sur votre EBS volume Amazon, ce qui peut exclure les données stockées ou mises en cache en mémoire par vos applications ou votre système d'exploitation, il est impératif d'acquérir une image de la mémoire du système à l'aide d'un outil tiers open source ou commercial approprié afin d'acquérir les données disponibles sur le système.
5. (Facultatif) Réaliser une réponse en temps réel/collecte d'artefacts : effectuez une collecte de données ciblée (disk/memory/logs) via une réponse en direct sur le système uniquement s'il est impossible d'acquérir le disque ou la mémoire autrement, ou pour une raison commerciale ou opérationnelle valide. Cela modifiera les données et artefacts importants du système.
6. Mettez l'instance hors service : détachez l'instance des groupes Auto Scaling, annulez-la des équilibreurs de charge et ajustez ou appliquez un profil d'instance prédéfini avec des autorisations minimisées ou nulles.
7. Isoler ou contenir l'instance : vérifiez que l'instance est efficacement isolée des autres systèmes et ressources de l'environnement en mettant fin aux connexions actuelles et futures vers et depuis l'instance et en empêchant les connexions actuelles et futures. Reportez-vous à la the section called “Maîtrise” section de ce document pour plus de détails.
8. Choix du répondant — En fonction de la situation et des objectifs, sélectionnez l'une des options suivantes :
   - Mettez le système hors service et arrêtez le système (recommandé).

     Arrêtez le système une fois que les preuves disponibles ont été recueillies afin de vérifier l'atténuation la plus efficace par rapport à un éventuel impact futur de l'instance sur l'environnement.
   - Continuez à exécuter l'instance dans un environnement isolé instrumenté pour la surveillance.

     Bien que cette approche ne soit pas recommandée comme approche standard, si une situation justifie une surveillance continue de l'instance (par exemple lorsque des données ou des indicateurs supplémentaires sont nécessaires pour effectuer une investigation et une analyse complètes de l'instance), vous pouvez envisager de fermer l'instance, AMI de créer une instance

et de relancer l'instance dans votre compte médico-légal dédié dans un environnement sandbox pré-instrumenté pour être complètement isolé et configuré avec des instruments permettant une surveillance quasi continue de l'instance (par exemple, VPC Flow Logs ou VPC Traffic Mirroring).

> **Note**
>
> Il est essentiel de capturer la mémoire avant les activités de réponse en direct, l'isolation ou l'arrêt du système afin de capturer les données volatiles (et précieuses) disponibles.

Développez des récits

Au cours de l'analyse et de l'investigation, documentez les mesures prises, les analyses effectuées et les informations identifiées, à utiliser lors des phases suivantes et, finalement, dans un rapport final. Ces récits doivent être succincts et précis, afin de confirmer que les informations pertinentes sont incluses afin de vérifier la bonne compréhension de l'incident et de maintenir un calendrier précis. Ils sont également utiles lorsque vous impliquez des personnes extérieures à l'équipe principale de réponse aux incidents. Voici un exemple :

> Le service marketing et commercial a reçu une demande de rançon le 15 mars 2022 demandant un paiement en cryptomonnaie afin d'éviter la publication d'éventuelles données sensibles. Ils ont SOC déterminé que la RDS base de données Amazon appartenant au marketing et aux ventes était accessible au public le 20 février 2022. Les journaux RDS d'accès SOC interrogés ont déterminé que l'adresse IP 198.51.100.23 avait été utilisée le 20 février 2022 avec les informations d'identification *`mm03434`* appartenant au major Mary, l'un des développeurs Web. Les journaux de VPC flux SOC interrogés ont déterminé qu'environ 256 Mo de données étaient sortis vers la même adresse IP à la même date (horodatage : 02-20T 15:50+00Z). Ils ont SOC déterminé, grâce à des informations sur les menaces open source, que les informations d'identification sont actuellement disponibles en texte brut dans le référentiel *`https[:]//example[.]com/majormary/rds-utils`* public.

Maîtrise

L'une des définitions du confinement, en ce qui concerne la réponse aux incidents, est le processus ou la mise en œuvre d'une stratégie lors de la gestion d'un événement de sécurité qui vise à

minimiser la portée de l'événement de sécurité et à contenir les effets d'une utilisation non autorisée dans l'environnement.

Une stratégie de confinement dépend d'une multitude de facteurs et peut être différente d'une organisation à l'autre en termes d'application des tactiques de confinement, de calendrier et d'objectif. Le Guide de gestion des incidents de sécurité informatique NIST SP 800-61 décrit plusieurs critères pour déterminer la stratégie de confinement appropriée, notamment :

- Dommages potentiels et vol de ressources
- Nécessité de préserver les preuves
- Disponibilité des services (connectivité réseau, services fournis à des tiers externes)
- Temps et ressources nécessaires à la mise en œuvre de la stratégie
- Efficacité de la stratégie (confinement partiel ou total)
- Durée de la solution (solution d'urgence à supprimer dans quatre heures, solution temporaire à supprimer dans deux semaines, solution permanente)

En ce qui concerne les services AWS, toutefois, les étapes de confinement fondamentales peuvent être réparties en trois catégories :

- Confinement de la source : utilisez le filtrage et le routage pour empêcher l'accès à partir d'une certaine source.
- Technique et limitation des accès : supprimez l'accès pour empêcher tout accès non autorisé aux ressources concernées.
- Confinement des destinations : utilisez le filtrage et le routage pour empêcher l'accès à une ressource cible.

Confinement de la source

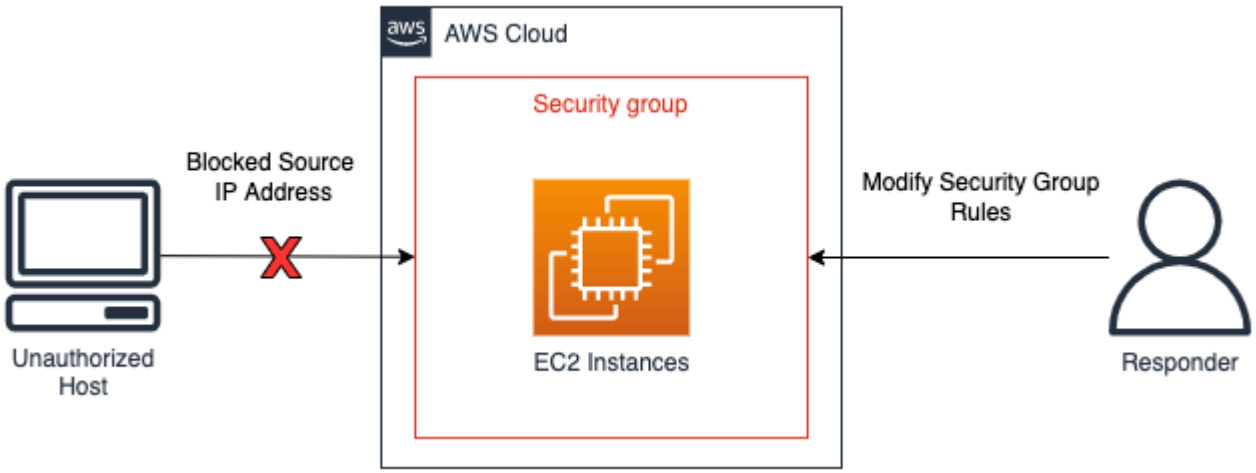
Le confinement des sources est l'utilisation et l'application du filtrage ou du routage au sein d'un environnement pour empêcher l'accès aux ressources provenant d'une adresse IP source ou d'une plage réseau spécifique. Des exemples de confinement des sources à l'aide de AWS services sont présentés ici :

- Groupes de sécurité : la création et l'application de groupes de sécurité d'isolation aux EC2 instances Amazon ou la suppression de règles d'un groupe de sécurité existant peuvent contribuer à contenir le trafic non autorisé vers une EC2 instance ou une AWS ressource Amazon. Il est

important de noter que les connexions suivies existantes ne seront pas interrompues en cas de changement de groupe de sécurité. Seul le trafic futur sera effectivement bloqué par le nouveau groupe de sécurité (consultez ce manuel de réponse aux incidents et le suivi des connexions des groupes de sécurité pour plus d'informations sur les connexions suivies et non suivies).

- Politiques — Les politiques relatives aux compartiments Amazon S3 peuvent être configurées pour bloquer ou autoriser le trafic provenant d'une adresse IP, d'une plage réseau ou d'un VPC point de terminaison. Les politiques permettent de bloquer les adresses suspectes et l'accès au compartiment Amazon S3. Des informations supplémentaires sur les politiques de compartiment sont disponibles sur Ajouter une politique de compartiment à l'aide de la console Amazon S3.
- AWS WAF — Les listes de contrôle d'accès Web (WebACLs) peuvent être configurées AWS WAF pour fournir un contrôle précis des demandes Web auxquelles les ressources répondent. Vous pouvez ajouter une adresse IP ou une plage réseau à un ensemble d'adresses IP configuré sur AWS WAF et appliquer des conditions de correspondance, telles que le blocage, à l'ensemble d'adresses IP. Cela bloquera les requêtes Web adressées à une ressource si l'adresse IP ou les plages de réseau du trafic d'origine correspondent à celles configurées dans les règles définies dans les règles IP définies.

Le schéma suivant illustre un exemple de confinement des sources, dans lequel un analyste de réponse aux incidents modifie un groupe de sécurité d'une EC2 instance Amazon afin de limiter les nouvelles connexions à certaines adresses IP uniquement. Comme indiqué dans la bullet relative aux groupes de sécurité, les connexions suivies existantes ne seront pas interrompues suite à un changement de groupe de sécurité.



Exemple de confinement de source

Technique et confinement des accès

Empêchez l'utilisation non autorisée d'une ressource en limitant les fonctions et IAM les principaux ayant accès à la ressource. Cela inclut la restriction des autorisations des IAM principaux ayant accès à la ressource ; cela inclut également la révocation temporaire des informations d'identification de sécurité. Des exemples de techniques et de limitation d'accès à l'aide de AWS services sont présentés ici :

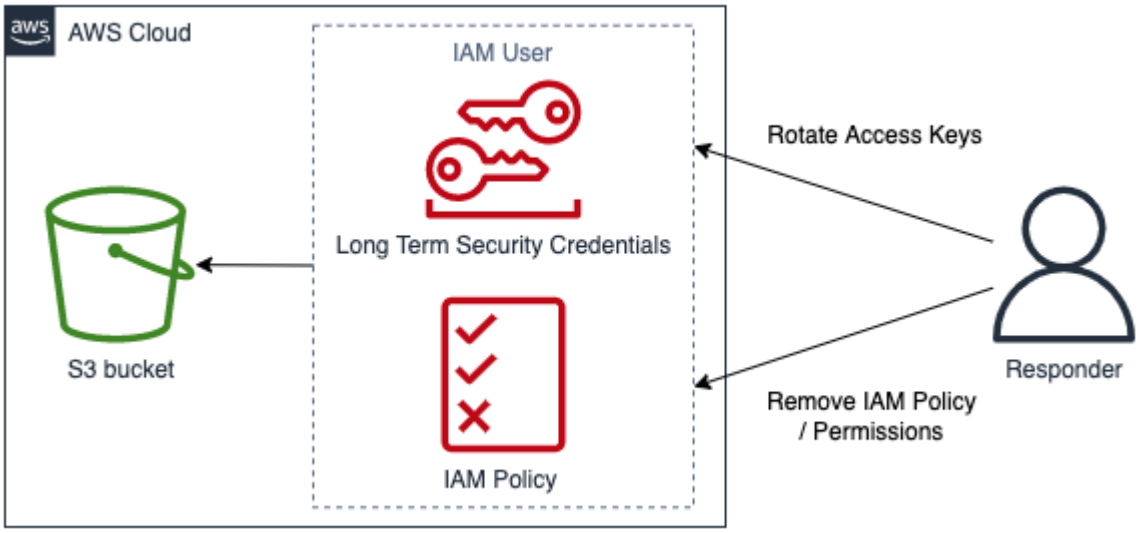
- Restreindre les autorisations — Les autorisations attribuées à un IAM directeur doivent respecter le principe du moindre privilège. Toutefois, lors d'un événement de sécurité actif, il se peut que vous deviez restreindre davantage l'accès à une ressource ciblée à partir d'un IAM principal spécifique. Dans ce cas, il est possible de limiter l'accès à une ressource en supprimant les autorisations du IAM principal à contenir. Cela se fait avec le IAM service et peut être appliqué à l'aide du AWS Management Console AWS CLI, du ou d'un AWS SDK.
- Révoquer les clés : les clés IAM d'accès sont utilisées par IAM les directeurs pour accéder aux ressources ou les gérer. Il s'agit d'informations d'identification statiques à long terme permettant de signer les demandes programmatiques adressées au AWS CLI ou AWS API en commençant par le préfixe AKIA(pour plus d'informations, reportez-vous à la section Comprendre les préfixes d'identification uniques dans IAM la section Identifiants). Pour limiter l'accès d'un IAM mandant lorsqu'une clé d'IAMaccès a été compromise, la clé d'accès peut être désactivée ou supprimée. Il est important de noter ce qui suit :
  - Une clé d'accès peut être réactivée après avoir été désactivée.
  - Une clé d'accès n'est pas récupérable une fois qu'elle a été supprimée.
  - Un IAM mandant peut avoir jusqu'à deux clés d'accès à la fois.
  - Les utilisateurs ou les applications utilisant la clé d'accès perdront l'accès une fois la clé désactivée ou supprimée.
- Révoquer les identifiants de sécurité temporaires — Les identifiants de sécurité temporaires peuvent être utilisés par une organisation pour contrôler l'accès aux AWS ressources, en commençant par le préfixe ASIA(pour plus d'informations, voir la section Comprendre les préfixes d'identification uniques dans IAM Identifiants). Les informations d'identification temporaires sont généralement utilisées par IAM les rôles et il n'est pas nécessaire de les modifier ou de les révoquer explicitement car leur durée de vie est limitée. Dans les cas où un événement de sécurité implique un identifiant de sécurité temporaire avant son expiration, vous devrez peut-être modifier les autorisations effectives des identifiants de sécurité temporaires existants. Cela peut être effectué à l'aide du IAM service fourni AWS Management Console. Des informations d'identification de sécurité temporaires peuvent également être délivrées aux IAM utilisateurs (par opposition aux

IAM rôles) ; toutefois, au moment de la rédaction de cet article, il n'existe aucune option permettant de révoquer les informations de sécurité temporaires pour un IAM utilisateur au sein du AWS Management Console. Pour les événements de sécurité dans lesquels la clé d'IAMaccès d'un utilisateur est compromise par un utilisateur non autorisé qui a créé des identifiants de sécurité temporaires, les identifiants de sécurité temporaires peuvent être révoqués de deux manières :

- Attachez à l'IAMutilisateur une politique intégrée qui empêche l'accès en fonction de l'heure d'émission du jeton de sécurité (reportez-vous à la section Refus d'accès aux informations d'identification de sécurité temporaires émises avant une heure précise dans Désactivation des autorisations pour les informations d'identification de sécurité temporaires pour plus de détails).
- Supprimez l'IAMutilisateur propriétaire des clés d'accès compromises. Recréez l'utilisateur si nécessaire.

- AWS WAF- Certaines techniques utilisées par des utilisateurs non autorisés incluent des modèles de trafic malveillants courants, tels que les demandes contenant des SQL injections et des scripts intersites ()XSS. AWS WAF peut être configuré pour faire correspondre et refuser le trafic en utilisant ces techniques à l'aide des instructions de règles AWS WAF intégrées.

Un exemple de technique et de limitation des accès est illustré dans le schéma suivant, avec un intervenant en cas d'incident faisant pivoter les clés d'accès ou supprimant une IAM politique empêchant un IAM utilisateur d'accéder à un compartiment Amazon S3.



Exemple de technique et de confinement des accès

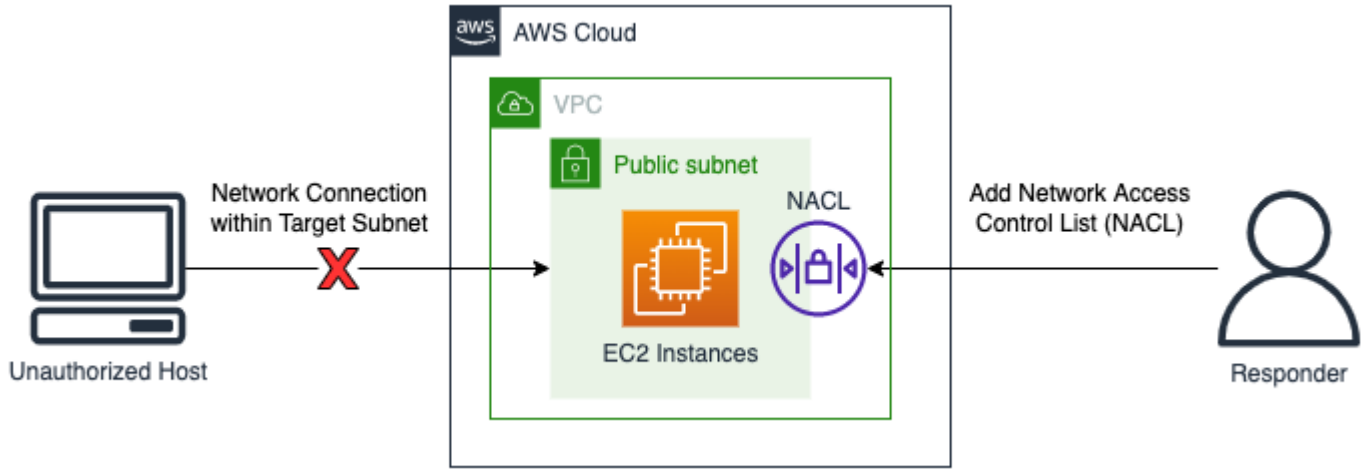
Confinement des destinations

Le confinement des destinations est l'application du filtrage ou du routage au sein d'un environnement pour empêcher l'accès à un hôte ou à une ressource ciblés. Dans certains cas, le confinement des destinations implique également une forme de résilience visant à vérifier que les ressources légitimes sont répliquées pour des raisons de disponibilité ; les ressources doivent être détachées de ces formes de résilience à des fins d'isolation et de confinement. Voici des exemples de confinement des destinations à l'aide de AWS services :

- Réseau ACLs — Des règles de refus peuvent être ajoutées aux réseaux ACLs (réseauACLs) configurés sur des sous-réseaux contenant des AWS ressources. Ces règles de refus peuvent être appliquées pour empêcher l'accès à une AWS ressource particulière ; toutefois, l'application d'une liste de contrôle d'accès réseau (réseauACL) affectera toutes les ressources du sous-réseau, et pas seulement les ressources auxquelles on accède sans autorisation. Les règles répertoriées au sein d'un réseau ACL sont traitées du haut vers le bas. La première règle d'un réseau existant ACL doit donc être configurée pour empêcher le trafic non autorisé vers la ressource et le sous-réseau ciblés. Il est également ACL possible de créer un tout nouveau réseau avec une règle de refus unique pour le trafic entrant et sortant, et de l'associer au sous-réseau contenant la ressource ciblée afin d'empêcher l'accès au sous-réseau via le nouveau réseau. ACL
- Arrêt — L'arrêt complet d'une ressource peut être efficace pour contenir les effets d'une utilisation non autorisée. La fermeture d'une ressource empêchera également tout accès légitime pour répondre aux besoins de l'entreprise et empêchera l'obtention de données médico-légales volatiles. Cette décision doit donc être réfléchie et doit être évaluée à la lumière des politiques de sécurité de l'entreprise.
- Isolation VPCs — L'isolation VPCs peut être utilisée pour contenir efficacement les ressources tout en fournissant un accès au trafic légitime (tel qu'un antivirus (AV) ou EDR des solutions nécessitant un accès à Internet ou à une console de gestion externe). L'isolation VPCs peut être préconfigurée avant un événement de sécurité pour autoriser des adresses IP et des ports valides, et les ressources ciblées peuvent être immédiatement déplacées vers cette isolation VPC lors d'un événement de sécurité actif afin de contenir la ressource tout en permettant à un trafic légitime d'être envoyé et reçu par la ressource ciblée lors des phases suivantes de réponse aux incidents. Un aspect important de l'utilisation d'un isolement VPC est que les ressources, telles que EC2 les instances, doivent être arrêtées et relancées dans le nouvel isolement VPC avant d'être utilisées. Les EC2 instances existantes ne peuvent pas être déplacées vers une autre VPC ou une autre zone de disponibilité. Pour ce faire, suivez les étapes décrites dans la section Comment déplacer mon EC2 instance Amazon vers un autre sous-réseau, une autre zone de disponibilité ou VPC ?

- Groupes Auto Scaling et équilibreurs de charge : les AWS ressources associées aux groupes Auto Scaling et aux équilibreurs de charge doivent être détachées et désenregistrées dans le cadre des procédures de confinement des destinations. Le détachement et le désenregistrement des AWS ressources peuvent être effectués à l'aide des touches, et. AWS Management Console AWS CLI AWS SDK

Un exemple de confinement des destinations est illustré dans le schéma suivant : un analyste de réponse aux incidents ajoute un réseau ACL à un sous-réseau afin de bloquer une demande de connexion réseau émanant d'un hôte non autorisé.



Exemple de confinement des destinations

Récapitulatif

Le confinement est une étape du processus de réponse aux incidents et peut être manuel ou automatisé. La stratégie globale de confinement doit être alignée sur les politiques de sécurité et les besoins commerciaux de l'organisation, et vérifier que les effets négatifs sont atténués le plus efficacement possible avant l'éradication et le rétablissement.

Éradication

L'éradication, en relation avec la réponse aux incidents de sécurité, consiste à supprimer les ressources suspectes ou non autorisées dans le but de remettre le compte dans un état sûr connu. La stratégie d'éradication dépend de plusieurs facteurs, qui dépendent des exigences commerciales de votre organisation.

Le Guide de gestion des incidents de sécurité informatique NIST SP 800-61 propose plusieurs étapes pour les éradiquer :

1. Identifiez et atténuez toutes les vulnérabilités qui ont été exploitées.
2. Supprimez les logiciels malveillants, les contenus inappropriés et les autres composants.
3. Si d'autres hôtes affectés sont découverts (par exemple, de nouvelles infections par des logiciels malveillants), répétez les étapes de détection et d'analyse pour identifier tous les autres hôtes concernés, puis contenir et éradiquer l'incident pour eux.

En ce qui concerne les AWS ressources, cela peut être affiné grâce aux événements détectés et analysés par le biais des journaux disponibles ou d'outils automatisés tels que CloudWatch Logs et Amazon GuardDuty. Ces événements devraient servir de base pour déterminer les mesures correctives à effectuer pour rétablir correctement l'environnement dans un état sûr connu.

La première étape de l'éradication consiste à déterminer quelles ressources ont été affectées au sein du AWS compte. Cela se fait grâce à l'analyse de vos sources de données de journal disponibles, de vos ressources et de vos outils automatisés.

- Identifiez les actions non autorisées entreprises par les IAM identités de votre compte.
- Identifiez les accès non autorisés ou les modifications apportées à votre compte.
- Identifiez la création de ressources ou d'IAMutilisateurs non autorisés.
- Identifiez les systèmes ou les ressources dont les modifications ne sont pas autorisées.

Une fois la liste des ressources identifiée, vous devez évaluer chacune d'elles afin de déterminer l'impact commercial de la suppression ou de la restauration de la ressource. Par exemple, si un serveur Web héberge votre application professionnelle et que sa suppression entraînerait une interruption de service, vous devez envisager de récupérer la ressource à partir de sauvegardes sécurisées vérifiées ou de relancer le système après un nettoyage AMI avant de supprimer le serveur concerné.

Une fois que vous avez terminé votre analyse d'impact commercial, vous devez, à l'aide des événements de votre analyse des journaux, accéder aux comptes et effectuer les mesures correctives appropriées, telles que :

- Faire pivoter ou supprimer les touches : cette étape empêche l'acteur de continuer à effectuer des activités dans le compte.
- Alternez les informations IAM d'identification des utilisateurs potentiellement non autorisés.
- Supprimez les ressources non reconnues ou non autorisées.

> **Important**
>
> Si vous devez conserver des ressources pour votre enquête, pensez à les sauvegarder. Par exemple, si vous devez conserver une EC2 instance Amazon pour des raisons légales, réglementaires ou de conformité, créez un EBS instantané Amazon avant de supprimer l'instance.

- Pour les infections par des logiciels malveillants, vous devrez peut-être contacter l'un AWS Partner ou l'autre fournisseur. AWS ne propose pas d'outils natifs pour l'analyse ou la suppression des malwares. Toutefois, si vous utilisez le module GuardDuty Malware pour AmazonEBS, des recommandations peuvent être disponibles pour les résultats fournis.

Une fois que vous avez éradiqué les ressources affectées identifiées, il vous AWS recommande de procéder à un examen de sécurité de votre compte. Cela peut être fait en utilisant des AWS Config règles, en utilisant des solutions open source telles que Prowler et/ou par le biais d' ScoutSuiteautres fournisseurs. Vous devriez également envisager d'effectuer des analyses de vulnérabilité sur vos ressources accessibles au public (Internet) afin d'évaluer le risque résiduel.

L'éradication est une étape du processus de réponse aux incidents et peut être manuelle ou automatisée, en fonction de l'incident et des ressources concernées. La stratégie globale doit être alignée sur les politiques de sécurité et les besoins commerciaux de l'entreprise, et vérifier que les effets négatifs sont atténués lorsque des ressources ou des configurations inappropriées sont supprimées.

Récupération

La restauration est le processus qui consiste à restaurer les systèmes dans un état sûr connu, à valider que les sauvegardes sont sûres ou non affectées par l'incident avant la restauration, à tester pour vérifier que les systèmes fonctionnent correctement après la restauration et à corriger les vulnérabilités associées à l'événement de sécurité.

L'ordre de reprise dépend des exigences de votre organisation. Dans le cadre du processus de reprise, vous devez effectuer une analyse de l'impact commercial afin de déterminer, au minimum :

- Priorités commerciales ou de dépendance
- Le plan de restauration
- Authentification et autorisation

Le guide de gestion des incidents de sécurité informatique NIST SP 800-61 fournit plusieurs étapes pour restaurer les systèmes, notamment :

- Restauration des systèmes à partir de sauvegardes propres.
  - Vérifiez que les sauvegardes sont évaluées avant de les restaurer sur les systèmes afin de vous assurer de l'absence d'infection et d'empêcher la résurgence de l'événement de sécurité.

    Les sauvegardes doivent être évaluées régulièrement dans le cadre des tests de reprise après sinistre afin de vérifier que le mécanisme de sauvegarde fonctionne correctement et que l'intégrité des données répond aux objectifs du point de reprise.
  - Si possible, utilisez des sauvegardes antérieures à l'horodatage du premier événement identifié dans le cadre de l'analyse des causes premières.
- Reconstruire les systèmes à partir de zéro, y compris le redéploiement à partir d'une source fiable à l'aide de l'automatisation, parfois dans un nouveau AWS compte.
- Remplacement des fichiers compromis par des versions propres.

  Vous devez faire preuve d'une grande prudence en procédant ainsi. Vous devez être absolument certain que le fichier que vous récupérez est connu, sûr et non affecté par l'incident.
- Installation de correctifs.
- Modification des mots de passe.
  - Cela inclut les mots de passe IAM des principaux susceptibles d'avoir été utilisés à mauvais escient.
  - Dans la mesure du possible, nous recommandons d'utiliser des rôles pour IAM les principaux et pour la fédération dans le cadre d'une stratégie de moindre privilège.
- Renforcement de la sécurité du périmètre du réseau (ensembles de règles de pare-feu, listes de contrôle d'accès aux routeurs périphériques).

Une fois les ressources récupérées, il est important de tirer les leçons apprises afin de mettre à jour les politiques, les procédures et les guides de réponse aux incidents.

En résumé, il est impératif de mettre en œuvre un processus de rétablissement qui facilite le retour à des opérations sûres connues. Le rétablissement peut prendre du temps et nécessite un lien étroit avec les stratégies de confinement afin de trouver un équilibre entre l'impact commercial et le risque de réinfection. Les procédures de recouvrement doivent inclure des étapes pour rétablir les ressources et les services, IAM les principaux et effectuer un examen de sécurité du compte afin d'évaluer le risque résiduel.

Conclusion

Chaque phase des opérations comporte des objectifs, des techniques, des méthodologies et des stratégies uniques. Le tableau 4 résume ces phases ainsi que certaines des techniques et méthodologies abordées dans cette section.

Tableau 4 — Phases opérationnelles : objectifs, techniques et méthodologies

Phase	Objectif	Techniques et méthodologies
Détection	Identifiez un événement de sécurité potentiel.	• Contrôles de sécurité pour la détection • Détection basée sur le comportement et les règles • Détection basée sur les personnes
Analyse	Déterminez si l'événement de sécurité est un incident et évaluez l'ampleur de l'incident.	• Valider et définir l'alerte • Journaux de requêtes • Renseignements sur les menaces • Automatisation
Confinement	Minimisez et limitez l'impact de l'événement de sécurité.	• Confinement de la source • Technique et confinement des accès • Confinement des destinations
Éradication	Éliminez les ressources ou artefacts non autorisés liés à l’événement de sécurité.	• Rotation ou suppression d'informations d'identification compromises ou non autorisées • Suppression de ressources non autorisée • Suppression des logiciels malveillants

Phase	Objectif	Techniques et méthodologies
		• Analyses de sécurité
Récupération	Restaurez les systèmes dans un état dont le bon état a été vérifié et surveille z ces systèmes pour vous assurer que la menace ne se reproduise pas.	• Restauration du système à partir de sauvegardes • Systèmes reconstruits à partir de zéro • Fichiers compromis remplacés par des versions propres

Activité postérieure à l’incident

Les menaces existantes sont en constante évolution. La capacité de votre organisation à protéger efficacement vos environnements doit suivre le rythme. La clé de l'amélioration continue consiste à réitérer les résultats de vos incidents et de vos simulations afin d'améliorer vos capacités à détecter, à répondre et à enquêter efficacement sur les incidents de sécurité potentiels, en réduisant vos vulnérabilités éventuelles, les délais de réponse et le retour à des opérations sûres. Les mécanismes suivants peuvent vous aider à vérifier que votre organisation dispose de toutes les capacités et les connaissances les plus récentes nécessaires pour réagir efficacement, quelle que soit la situation.

Mettre en place un cadre pour tirer les leçons des incidents

La mise en œuvre d'un cadre et d'une méthodologie en matière de leçons apprises permettra non seulement d'améliorer les capacités de réponse aux incidents, mais également d'empêcher que l'incident ne se reproduise. En tirant les leçons de chaque incident, vous pouvez éviter de répéter les mêmes erreurs, expositions ou mauvaises configurations, non seulement en améliorant votre posture de sécurité, mais également en minimisant le temps perdu dans des situations évitables.

Il est important de mettre en œuvre un cadre des leçons apprises qui établit et atteint, à un niveau élevé, les points suivants :

- Quand se déroule un processus des enseignements tirés ?
- En quoi consiste le processus des enseignements tirés ?
- Comment se déroule un processus des enseignements tirés ?
- Qui est impliqué dans le processus et comment ?

- Comment les domaines à améliorer seront-ils identifiés ?
- Comment allez-vous vous assurer que les améliorations sont suivies et mises en œuvre de manière efficace ?

Outre ces résultats de haut niveau énumérés, il est important de vous assurer de poser les bonnes questions pour tirer le meilleur parti du processus (informations menant à des améliorations réalisables). Posez-vous les questions suivantes pour commencer à développer vos discussions sur les enseignements tirés :

- Quel a été l'incident ?
- Quand l'incident a-t-il été identifié pour la première fois ?
- Comment a-t-il été identifié ?
- Quels systèmes ont alerté sur l'activité ?
- Quels systèmes, services et données étaient concernés ?
- Que s'est-il passé précisément ?
- Qu'est-ce qui a bien fonctionné ?
- Qu'est-ce qui n'a pas bien fonctionné ?
- Quels processus ou procédures ont échoué ou n'ont pas pu être mis à l'échelle pour répondre à l'incident ?
- Qu'est-ce qui peut être amélioré dans les domaines suivants :
  - Personnes
    - Les personnes à contacter étaient-elles réellement disponibles et la liste de contacts était-elle à jour ?
    - Les personnes manquaient-elles de formation ou n'avaient-elles pas les capacités nécessaires pour intervenir et enquêter efficacement sur l'incident ?
    - Les ressources appropriées étaient-elles prêtes et disponibles ?
  - Processus
    - Les processus et procédures ont-ils été suivis ?
    - Les processus et procédures étaient-ils documentés et disponibles pour cet incident ou ce type d'incident ?
    - Les processus et procédures requis étaient-ils absents ?
    - Les intervenants ont-ils pu accéder en temps opportun aux informations requises pour répondre au problème ?

  - Technologie
    - Les systèmes d’alerte existants ont-ils identifié l’activité et ont-ils envoyé des alertes efficaces ?
    - Les alertes existantes doivent-elles être améliorées ou de nouvelles alertes doivent-elles être créées pour cet incident ou ce type d’incident ?
    - Les outils existants ont-ils permis une investigation efficace (recherche/analyse) de l'incident ?
- Que peut-on faire pour identifier cet incident ou ce type d’incident plus rapidement ?
- Que peut-on faire pour éviter que cet incident ou ce type d’incident ne se reproduise ?
- À qui appartient le plan d’amélioration et comment allez-vous vérifier qu’il a été mis en œuvre ?
- Quel est le calendrier de mise en œuvre et monitoring/preventative controls/process de test de l'additif ?

Cette liste n'est pas exhaustive ; elle est destinée à servir de point de départ pour identifier les besoins de l'organisation et de l'entreprise et la manière dont vous pouvez les analyser afin de tirer le meilleur parti des incidents et d'améliorer continuellement votre posture de sécurité. Le plus important est de commencer par intégrer les enseignements tirés dans le cadre standard de votre processus de réponse aux incidents, de la documentation et des attentes des parties prenantes.

Établissez des indicateurs de réussite

Les métriques sont nécessaires pour mesurer, évaluer et améliorer efficacement vos capacités de réponse aux incidents. Sans indicateurs, il n'existe aucune référence permettant de mesurer avec précision ou même d'identifier les performances (ou non) de votre organisation. Quelques indicateurs communs à la réponse aux incidents constituent un bon point de départ pour une organisation qui cherche à établir des attentes et des références pour atteindre l'excellence opérationnelle.

Temps moyen de détection

Le temps moyen de détection est le temps moyen nécessaire pour découvrir un éventuel incident de sécurité. Plus précisément, il s'agit du délai entre l'apparition du premier indicateur de compromission et l'identification ou l'alerte initiale.

Vous pouvez utiliser cette métrique pour suivre l'efficacité de vos systèmes de détection et d'alerte. Des mécanismes de détection et d'alerte efficaces sont essentiels pour garantir que d'éventuels incidents de sécurité ne persistent pas dans vos environnements.

Plus le temps moyen de détection est long, plus il est nécessaire de créer des alertes et des mécanismes supplémentaires ou plus efficaces pour identifier et découvrir d'éventuels incidents de sécurité. Plus le temps moyen de détection est court, meilleur est le fonctionnement de vos mécanismes de détection et d'alerte.

Temps moyen pour accuser réception

Le délai moyen de reconnaissance est le temps moyen nécessaire pour reconnaître et hiérarchiser un éventuel incident de sécurité. Plus précisément, il s'agit du délai entre la génération d'une alerte et le moment où un membre de votre équipe SOC ou du personnel de réponse aux incidents identifie et hiérarchise l'alerte à traiter.

Vous pouvez utiliser cette métrique pour suivre dans quelle mesure votre équipe traite et hiérarchise les alertes. Si votre équipe n'est pas en mesure d'identifier et de hiérarchiser efficacement les alertes, les réponses seront retardées et inefficaces.

Plus le délai moyen d'accusé de réception est long, plus il est nécessaire de vérifier que votre équipe dispose des ressources nécessaires et est formée pour reconnaître rapidement un éventuel incident de sécurité et prioriser sa réponse par ordre de priorité. Plus le délai moyen d'accusé de réception est court, plus votre équipe est en mesure de répondre aux alertes de sécurité, démontrant ainsi qu'elle est bien préparée et capable de bien les hiérarchiser.

Temps moyen de réponse

Le temps moyen de réponse est le temps moyen nécessaire pour commencer la réponse initiale à un éventuel incident de sécurité. Plus précisément, il s'agit du délai entre l'alerte initiale ou la découverte d'un éventuel incident de sécurité et les premières mesures prises pour y répondre. Ce délai est similaire au délai moyen pour accuser réception, mais il s'agit de la mesure des actions réactives spécifiques (par exemple, acquérir des données du système, contenir le système) par rapport à la simple reconnaissance ou à la reconnaissance de la situation.

Vous pouvez utiliser cette métrique pour suivre votre niveau de préparation à répondre aux incidents de sécurité. Comme nous l'avons mentionné, la préparation est essentielle à une intervention efficace. Reportez-vous à la the section called “Préparation” section de ce document.

Plus le délai moyen de réponse est long, plus il est nécessaire de vérifier que votre équipe est correctement formée à la manière de réagir afin que les processus de réponse soient documentés et utilisés efficacement. Plus le délai moyen de réponse est court, plus votre équipe est en mesure d'identifier une réponse appropriée aux alertes identifiées et de prendre les mesures nécessaires pour commencer le retour à des opérations sûres.

Temps moyen de confinement

Le temps moyen de confinement est le temps moyen nécessaire pour contenir un éventuel incident de sécurité. Plus précisément, il s'agit du délai entre l'alerte initiale ou la découverte d'un éventuel incident de sécurité et l'exécution des actions réactives qui empêchent efficacement l'attaquant ou les systèmes compromis de causer des dommages supplémentaires.

Vous pouvez utiliser cet indicateur pour savoir dans quelle mesure votre équipe est capable d'atténuer ou de contenir les éventuels incidents de sécurité. L'incapacité à contenir rapidement et efficacement les éventuels incidents de sécurité augmente l'impact, la portée et l'exposition à d'éventuelles nouvelles compromissions.

Plus le délai moyen de confinement est long, plus il est nécessaire de développer à la fois les connaissances et les capacités nécessaires pour atténuer et contenir rapidement et efficacement les incidents de sécurité que vous rencontrez. Plus le délai moyen de confinement est court, plus votre équipe est en mesure de comprendre et de mettre en œuvre les mesures nécessaires pour atténuer et contenir les menaces identifiées afin de réduire l'impact, la portée et les risques pour l'entreprise.

Temps moyen de rétablissement

Le temps moyen de rétablissement est le temps moyen nécessaire pour rétablir complètement les opérations afin de protéger les opérations contre un éventuel incident de sécurité. Plus précisément, il s'agit du délai entre l'alerte initiale ou la découverte d'un éventuel incident de sécurité et le moment où l'entreprise reprend ses activités normalement et en toute sécurité sans être affectée par l'incident.

Vous pouvez utiliser cet indicateur pour suivre l'efficacité de vos équipes lorsqu'il s'agit de rétablir la sécurité des systèmes, des comptes et des environnements après un incident de sécurité. L'incapacité de reprendre des activités sûres rapidement ou efficacement peut non seulement avoir un impact sur la sécurité, mais également augmenter l'impact et les dépenses de l'entreprise et de ses opérations.

Plus le temps moyen de restauration est long, plus il est nécessaire de préparer vos équipes et vos environnements à disposer des mécanismes appropriés (par exemple, des processus de basculement et des pipelines CI/CD pour redéployer en toute sécurité des systèmes propres) afin de minimiser l'impact des incidents de sécurité sur les opérations et l'entreprise. Plus le délai moyen de restauration est court, plus vos équipes sont efficaces pour minimiser l'impact des incidents de sécurité sur vos opérations et votre activité.

Temps de séjour de l'attaquant

Le temps d'attente d'un attaquant est le temps moyen pendant lequel un utilisateur non autorisé a accès à un système ou à un environnement. Ce délai est similaire au délai moyen de confinement, sauf que le délai commence au moment où l'attaquant a accédé au système ou aux environnements, ce qui peut être antérieur à l'alerte ou à la découverte initiale.

Vous pouvez utiliser cette métrique pour déterminer dans quelle mesure vos systèmes et mécanismes fonctionnent ensemble afin de réduire le temps, l'accès et les opportunités d'impact d'un attaquant ou d'une menace sur votre environnement. La réduction du temps passé par les attaquants doit être une priorité absolue pour vos équipes et votre entreprise.

Plus le temps passé par les attaquants est long, plus il est nécessaire d'identifier les aspects du processus de réponse aux incidents qui doivent être améliorés afin de garantir la capacité de vos équipes à minimiser l'impact et la portée des menaces ou des attaques dans vos environnements. Plus le temps passé par les attaquants est faible, plus vos équipes sont en mesure de minimiser le temps et les opportunités que représente une menace ou un attaquant dans vos environnements, réduisant ainsi les risques et l'impact sur vos opérations et votre activité.

Récapitulatif des métriques

L'établissement et le suivi de mesures de réponse aux incidents vous permettent de mesurer, d'évaluer et d'améliorer efficacement vos capacités de réponse aux incidents. Pour y parvenir, un certain nombre de mesures courantes de réponse aux incidents ont été mises en évidence dans cette section. Le tableau 5 résume ces indicateurs.

Tableau 5 — Mesures de réponse aux incidents

Métrique	Description
Temps moyen de détection	Temps moyen nécessaire pour découvrir un éventuel incident de sécurité
Temps moyen pour accuser réception	Temps moyen nécessaire pour reconnaître (et hiérarchiser) un éventuel incident de sécurité
Temps moyen de réponse	Temps moyen nécessaire pour commencer la réponse initiale à un éventuel incident de sécurité

Métrique	Description
Temps moyen de confinement	Temps moyen nécessaire pour contenir un éventuel incident de sécurité
Temps moyen de rétablissement	Temps moyen nécessaire pour un retour complet afin de protéger les opérations contre un éventuel incident de sécurité
Temps de séjour de l'attaquant	Durée moyenne pendant laquelle un attaquant a accès à un système ou à un environnement

Utiliser des indicateurs de compromis (IOCs)

Un indicateur de compromission (IOC) est un artefact observé dans ou sur un réseau, un système ou un environnement qui peut (avec un niveau de confiance élevé) identifier une activité malveillante ou un incident de sécurité. IOCspeuvent exister sous diverses formes, notamment des adresses IP, des domaines, des artefacts au niveau du réseau tels que des TCP drapeaux ou des charges utiles, des artefacts au niveau du système ou de l'hôte tels que des exécutables, des noms de fichiers et des hachages, des entrées de fichiers journaux ou de registre, etc. Il peut également s'agir d'une combinaison d'éléments ou d'activités, tels que l'existence d'éléments ou d'artefacts spécifiques sur un système (un certain fichier ou ensemble de fichiers et éléments de registre), des actions effectuées dans un certain ordre (connexion à un système depuis une certaine adresse IP suivie de commandes anormales spécifiques) ou une activité réseau (trafic entrant ou sortant anormal vers ou depuis certains domaines) qui peuvent indiquer une menace, une attaque ou une méthodologie d'attaque spécifique.

Alors que vous vous efforcez d'améliorer de manière itérative votre programme de réponse aux incidents, vous devez mettre en œuvre un cadre de collecte, de gestion et d'utilisation en IOCs tant que mécanisme permettant de créer et d'améliorer en permanence les détections et les alertes et d'améliorer la rapidité et l'efficacité des enquêtes. Vous pouvez commencer par intégrer la collecte et la gestion des IOCs dans les phases d'analyse et d'investigation de vos processus de réponse aux incidents. En identifiant, en collectant et en stockant IOCs de manière proactive dans le cadre de votre processus, vous pouvez créer un référentiel de données (dans le cadre d'un programme de renseignement sur les menaces plus complet) qui peut à son tour être utilisé pour améliorer les détections et alertes existantes, créer des détections et des alertes supplémentaires, identifier où et

quand un artefact a déjà été vu, créer et référencer des documents sur la manière dont les enquêtes étaient précédemment effectuées impliquant des IOCs appariements, etc.

Éducation et formation continues

L'éducation et la formation sont à la fois des efforts évolutifs et continus qui devraient être poursuivis et maintenus avec détermination. Il existe divers mécanismes permettant de vérifier que votre équipe est sensibilisée, informée et dotée de capacités adaptées à l'évolution de l'état de la technologie ainsi qu'au paysage des menaces.

L'un des mécanismes consiste à intégrer la formation continue dans le cadre des objectifs et des opérations de vos équipes. Comme indiqué dans la section Préparation, votre personnel de réponse aux incidents et les parties prenantes doivent être formés efficacement à la détection, à la réponse et à l'investigation des incidents internes AWS. Cependant, l'éducation n'est pas un effort « ponctuel ». La formation doit être poursuivie en permanence pour vérifier que votre équipe est au courant des dernières avancées technologiques, des mises à jour et des améliorations qui peuvent être mises à profit pour améliorer l'efficacité et l'efficience de la réponse, ainsi que des ajouts ou des mises à jour des données qui peuvent être exploités pour améliorer les enquêtes et les analyses.

Un autre mécanisme consiste à vérifier que les simulations sont effectuées régulièrement (par exemple, tous les trimestres) et axées sur des résultats spécifiques pour l'entreprise. Reportez-vous à la the section called “Exécutez des simulations régulières” section de ce document.

Bien que les exercices de simulation initiaux constituent un excellent moyen de générer une base initiale d'amélioration, les tests continus sont essentiels pour obtenir des améliorations durables up-to-date et refléter fidèlement l'état actuel des opérations. En effectuant des tests par rapport aux situations de sécurité les plus récentes et les plus critiques et en utilisant les capacités de réponse les plus importantes ou les plus récentes, et en intégrant les leçons apprises dans la formation, les opérations et les processus/procédures, vous pourrez vérifier que vous êtes en mesure d'améliorer en permanence vos processus de réponse et votre programme dans leur ensemble.

Conclusion

Alors que vous poursuivez votre transition vers le cloud, il est important que vous preniez en compte les concepts fondamentaux de réponse aux incidents de sécurité pour votre AWS environnement. Vous pouvez combiner les contrôles disponibles, les fonctionnalités cloud et les options de correction pour vous aider à améliorer la sécurité de votre environnement cloud. Vous pouvez également commencer modestement et itérer à mesure que vous adoptez des fonctionnalités d'automatisation qui améliorent votre vitesse de réponse, afin d'être mieux préparé en cas d'événements de sécurité.

Collaborateurs

Les contributeurs actuels et passés à ce document incluent :

- Anna McAbee, architecte senior des solutions de sécurité, Amazon Web Services
- Freddy Kasprzykowski, consultant senior en sécurité, Amazon Web Services
- Jason Hurst, ingénieur en sécurité senior, Amazon Web Services
- Jonathon Poling, consultant principal en sécurité, Amazon Web Services
- Josh Du Lac, directeur principal de l'architecture des solutions de sécurité, Amazon Web Services
- Paco Hope, ingénieur principal en sécurité, Amazon Web Services
- Ryan Tick, ingénieur en sécurité senior, Amazon Web Services
- Steve de Vera, ingénieur en sécurité senior, Amazon Web Services

Annexe A : Définitions des fonctionnalités du cloud

AWS propose plus de 200 services cloud et des milliers de fonctionnalités. Nombre d'entre elles fournissent des fonctionnalités natives de détection, de prévention et de réactivité, tandis que d'autres peuvent être utilisées pour concevoir des solutions de sécurité personnalisées. Cette section inclut un sous-ensemble des services les plus pertinents pour la réponse aux incidents dans le cloud.

Rubriques

Journalisation et événements

AWS CloudTrail— AWS CloudTrail service permettant la gouvernance, la conformité, l'audit opérationnel et l'audit des risques des AWS comptes. Vous pouvez ainsi enregistrer CloudTrail, surveiller en permanence et conserver l'activité du compte liée aux actions menées dans l'ensemble AWS des services. CloudTrail fournit un historique des événements relatifs à l'activité de votre AWS compte, y compris les actions AWS Management Console effectuées AWS SDKs via les outils de

ligne de commande et d'autres AWS services. Cet historique des événements simplifie l'analyse de sécurité, le suivi des modifications des ressources et le dépannage. CloudTrail enregistre deux types d' AWS APIactions différents :

- CloudTrail les événements de gestion (également appelés opérations du plan de contrôle) indiquent les opérations de gestion effectuées sur les ressources de votre AWS compte. Cela inclut des actions telles que la création d'un compartiment Amazon S3 et la configuration de la journalisation.
- CloudTrail les événements de données (également appelés opérations du plan de données) indiquent les opérations de ressources effectuées sur ou au sein d'une ressource de votre AWS compte. Ces opérations sont souvent des activités à volume élevé. Cela inclut des actions telles que l'APIactivité au niveau des objets Amazon S3 (par exemple, `GetObject`Delete`Object`, et les `PutObject` API opérations) et l'activité d'invocation de la fonction Lambda.

AWS Config— AWS Config est un service permettant aux clients d'évaluer, d'auditer et d'évaluer les configurations de vos AWS ressources. AWS Config surveille et enregistre en permanence les configurations de vos AWS ressources et vous permet d'automatiser l'évaluation des configurations enregistrées par rapport aux configurations souhaitées. Grâce à AWS Config, les clients peuvent consulter les modifications apportées aux configurations et aux relations entre les AWS ressources, manuellement ou automatiquement, l'historique détaillé de la configuration des ressources et déterminer la conformité globale par rapport aux configurations spécifiées dans les directives du client. Cela permet de simplifier l'audit de conformité, l'analyse de sécurité, la gestion des modifications et le dépannage opérationnel.

Amazon EventBridge — Amazon EventBridge fournit un flux quasi en temps réel d'événements système décrivant les modifications apportées aux AWS ressources ou lorsque des API appels sont publiés par AWS CloudTrail. À l'aide de règles simples que vous pouvez configurer rapidement, vous pouvez associer des événements et les acheminer vers une ou plusieurs fonctions ou flux cibles. EventBridge prend connaissance des changements opérationnels au fur et à mesure qu'ils se produisent. EventBridge peut répondre à ces changements opérationnels et prendre des mesures correctives si nécessaire, en envoyant des messages pour répondre à l'environnement, en activant des fonctions, en apportant des modifications et en capturant des informations d'état. Certains services de sécurité, tels qu'Amazon GuardDuty, produisent leurs résultats sous forme d' EventBridge événements. De nombreux services de sécurité proposent également la possibilité d'envoyer leurs résultats à Amazon S3.

Journaux d'accès Amazon S3 : si des informations sensibles sont stockées dans un compartiment Amazon S3, les clients peuvent activer les journaux d'accès Amazon S3 pour enregistrer chaque

chargement, téléchargement et modification de ces données. Ce journal est distinct des CloudTrail journaux qui enregistrent les modifications apportées au compartiment lui-même (telles que les modifications des politiques d'accès et des politiques de cycle de vie). Il convient de noter que les enregistrements des journaux d'accès sont fournis dans la mesure du possible. La plupart des demandes pour un compartiment correctement configuré pour l'enregistrement se traduisent par un enregistrement de journal distribué. L'exhaustivité et la disponibilité de la journalisation du serveur ne sont pas garanties.

Amazon CloudWatch Logs — Les clients peuvent utiliser Amazon CloudWatch Logs pour surveiller, stocker et accéder aux fichiers journaux provenant de systèmes d'exploitation, d'applications et d'autres sources exécutées sur des EC2 instances Amazon avec un agent CloudWatch Logs. CloudWatch Les journaux peuvent être une destination pour les AWS CloudTrail DNS requêtes Route 53, les journaux de VPC flux, les fonctions Lambda, etc. Les clients peuvent ensuite récupérer les données de journal associées dans CloudWatch Logs.

Amazon VPC Flow Logs — VPC Flow Logs permet aux clients de capturer des informations sur le trafic IP à destination et en provenance des interfaces réseau entrantesVPCs. Une fois les journaux de flux activés, ils peuvent être diffusés vers Amazon CloudWatch Logs et Amazon S3. VPC Flow Logs aide les clients à effectuer un certain nombre de tâches, telles que le dépannage des raisons pour lesquelles un trafic spécifique n'atteint pas une instance, le diagnostic des règles trop restrictives des groupes de sécurité et leur utilisation comme outil de sécurité pour surveiller le trafic vers les EC2 instances. Utilisez la version la plus récente de la journalisation des VPC flux pour obtenir les champs les plus robustes.

AWS WAF Journaux : AWS WAF prend en charge la journalisation complète de toutes les requêtes Web inspectées par le service. Les clients peuvent les stocker dans Amazon S3 pour répondre aux exigences de conformité et d'audit, ainsi qu'aux fins de débogage et de criminalistique. Ces journaux aident les clients à déterminer la cause première des règles initiées et des requêtes Web bloquées. Les journaux peuvent être intégrés à des outils tiers SIEM et à des outils d'analyse de journaux.

Journaux de requêtes Route 53 Resolver — Les journaux de requêtes Route 53 Resolver vous permettent de consigner toutes les DNS requêtes effectuées par les ressources d'Amazon Virtual Private Cloud (AmazonVPC). Qu'il s'agisse d'une EC2 instance Amazon, d'une AWS Lambda fonction ou d'un conteneur, s'il réside dans votre Amazon VPC et émet une DNS requête, cette fonctionnalité l'enregistrera ; vous pourrez alors explorer et mieux comprendre le fonctionnement de vos applications.

Autres AWS journaux : publie AWS en permanence des fonctionnalités et des capacités de service pour les clients grâce à de nouvelles fonctionnalités de journalisation et de surveillance. Pour

plus d'informations sur les fonctionnalités disponibles pour chaque AWS service, consultez notre documentation publique.

Visibilité et alertes

AWS Security Hub— AWS Security Hub fournit aux clients une vue complète des alertes de sécurité prioritaires et de l'état de conformité des comptes. AWS Security Hub regroupe, organise et hiérarchise les résultats provenant de AWS services tels qu'Amazon, Amazon GuardDuty Inspector, Amazon Macie et de solutions. AWS Partner Les résultats sont résumés visuellement sur des tableaux de bord intégrés avec des graphiques et des tableaux exploitables. Vous pouvez également surveiller en permanence votre environnement à l'aide de contrôles de conformité automatisés basés sur les AWS meilleures pratiques et les normes du secteur suivies par votre entreprise.

Amazon GuardDuty — Amazon GuardDuty est un service géré de détection des menaces qui surveille en permanence les comportements malveillants ou non autorisés afin d'aider les clients à protéger leurs AWS comptes et leurs charges de travail. Il surveille les activités telles que les API appels inhabituels ou les déploiements potentiellement non autorisés indiquant une possible compromission du compte ou des ressources des EC2 instances Amazon, des compartiments Amazon S3 ou une reconnaissance par des acteurs malveillants.

GuardDuty identifie les acteurs présumés malveillants grâce à des flux intégrés de renseignements sur les menaces utilisant l'apprentissage automatique pour détecter les anomalies dans l'activité des comptes et de la charge de travail. Lorsqu'une menace potentielle est détectée, le service envoie une alerte de sécurité détaillée à la GuardDuty console et aux CloudWatch événements. Cela rend les alertes exploitables et simples à intégrer dans les systèmes de gestion des événements et de flux de travail existants.

GuardDuty propose également deux modules complémentaires pour surveiller les menaces avec des services spécifiques : Amazon GuardDuty pour la protection Amazon S3 et Amazon GuardDuty pour EKS la protection Amazon. La protection Amazon S3 permet GuardDuty de surveiller les API opérations au niveau des objets afin d'identifier les risques de sécurité potentiels pour les données contenues dans les compartiments Amazon S3. La protection Kubernetes permet GuardDuty de détecter les activités suspectes et les compromissions potentielles des clusters Kubernetes au sein d'Amazon. EKS

Amazon Macie — Amazon Macie est un service de sécurité basé sur l'IA qui aide à prévenir les pertes de données en découvrant, en classant et en protégeant automatiquement les données sensibles qui y sont stockées. AWS Macie utilise l'apprentissage automatique (ML) pour reconnaître les données sensibles telles que les informations personnelles identifiables (PII) ou la propriété

intellectuelle, attribuer une valeur commerciale et fournir une visibilité sur l'endroit où ces données sont stockées et sur la manière dont elles sont utilisées dans votre organisation. Amazon Macie surveille en permanence les activités d'accès aux données pour détecter les anomalies et émet des alertes lorsqu'il détecte un risque d'accès non autorisé ou de fuite de données par inadvertance.

AWS Config Rules— Une AWS Config règle représente les configurations préférées pour une ressource et est évaluée par rapport aux modifications de configuration apportées aux ressources pertinentes, telles qu'enregistrées par AWS Config. Vous pouvez consulter les résultats de l'évaluation d'une règle par rapport à la configuration d'une ressource sur un tableau de bord. À l'aide de AWS Config règles, vous pouvez évaluer votre état global de conformité et de risque du point de vue de la configuration, visualiser les tendances en matière de conformité au fil du temps et déterminer quel changement de configuration a entraîné la non-conformité d'une ressource à une règle.

AWS Trusted Advisor— AWS Trusted Advisor est une ressource en ligne qui vous aide à réduire les coûts, à augmenter les performances et à améliorer la sécurité en optimisant votre AWS environnement. Trusted Advisor fournit des conseils en temps réel pour vous aider à provisionner vos ressources en suivant les AWS meilleures pratiques. L'ensemble complet des Trusted Advisor contrôles, y compris l'intégration CloudWatch des événements, est disponible pour les clients des plans Business et Enterprise Support.

Amazon CloudWatch — Amazon CloudWatch est un service de surveillance des AWS Cloud ressources et des applications que vous utilisez AWS. Vous pouvez l'utiliser CloudWatch pour collecter et suivre les métriques, collecter et surveiller les fichiers journaux, définir des alarmes et réagir automatiquement aux modifications de vos AWS ressources. CloudWatch peut surveiller les AWS ressources, telles que les EC2 instances Amazon, les tables Amazon DynamoDB et les instances RDS Amazon DB, ainsi que les métriques personnalisées générées par vos applications et services, et tous les fichiers journaux générés par vos applications. Vous pouvez utiliser Amazon CloudWatch pour obtenir une visibilité à l'échelle du système sur l'utilisation des ressources, les performances des applications et la santé opérationnelle. Vous pouvez utiliser ces informations pour réagir en conséquence et assurer le bon fonctionnement de votre application.

Amazon Inspector — Amazon Inspector est un service d'évaluation automatique de la sécurité qui permet d'améliorer la sécurité et la conformité des applications déployées sur AWS. Amazon Inspector évalue automatiquement les applications pour détecter les vulnérabilités ou les écarts par rapport aux meilleures pratiques. Après avoir effectué une évaluation, Amazon Inspector produit une liste détaillée des résultats de sécurité classés par niveau de gravité. Ces résultats peuvent être consultés directement ou dans le cadre de rapports d'évaluation détaillés disponibles via la console Amazon Inspector ouAPI.

Amazon Detective — Amazon Detective est un service de sécurité qui collecte automatiquement les données des journaux à partir de vos AWS ressources et utilise l'apprentissage automatique, l'analyse statistique et la théorie des graphes pour créer un ensemble de données liées qui vous permet de mener des enquêtes de sécurité plus rapides et plus efficaces. Detective peut analyser des milliards d'événements provenant de plusieurs sources de données, telles que les journaux de VPC flux CloudTrail GuardDuty, et crée automatiquement une vue unifiée et interactive de vos ressources, de vos utilisateurs et des interactions entre eux au fil du temps. Grâce à cette vue unifiée, vous pouvez visualiser tous les détails et le contexte en un seul endroit afin d'identifier les raisons sous-jacentes des résultats, d'explorer les activités historiques pertinentes et d'en déterminer rapidement la cause première.

Automatisation

AWS Lambda— AWS Lambda est un service de calcul sans serveur qui exécute votre code en réponse à des événements et gère automatiquement les ressources de calcul sous-jacentes pour vous. Vous pouvez utiliser Lambda pour étendre d'autres AWS services avec une logique personnalisée ou créer vos propres services principaux qui fonctionnent en termes d' AWS échelle, de performance et de sécurité. Lambda exécute votre code sur une infrastructure informatique à haute disponibilité et gère les ressources de calcul pour vous. Cela inclut la maintenance des serveurs et des systèmes d'exploitation, le provisionnement des capacités et le dimensionnement automatique, le déploiement du code et des correctifs de sécurité, ainsi que la surveillance et la journalisation du code. Tout ce que vous avez à faire est de fournir le code.

AWS Step Functions— AWS Step Functions simplifie la coordination des composants des applications distribuées et des microservices à l'aide de flux de travail visuels. Step Functions fournit une console graphique qui vous permet d'organiser et de visualiser les composants de votre application sous forme d'une série d'étapes. Cela facilite la création et l'exécution d'applications en plusieurs étapes. Step Functions démarre et suit automatiquement chaque étape, puis réessaie en cas d'erreur, afin que votre application s'exécute dans l'ordre et comme prévu.

Step Functions enregistre l'état de chaque étape. Ainsi, en cas de problème, vous pouvez diagnostiquer et corriger rapidement les problèmes. Vous pouvez modifier et ajouter des étapes sans écrire de code, afin de faire évoluer votre application et d'innover plus rapidement. AWS Step Functions fait partie de AWS Serverless et simplifie l'orchestration des AWS Lambda fonctions pour les applications sans serveur. Vous pouvez également utiliser Step Functions pour l'orchestration de microservices à l'aide de ressources de calcul telles qu'Amazon et EC2 Amazon. ECS

AWS Systems Manager : vous AWS Systems Manager donne la visibilité et le contrôle de votre infrastructure sur AWS. Systems Manager fournit une interface utilisateur unifiée qui vous permet

de visualiser les données opérationnelles de plusieurs AWS services et d'automatiser les tâches opérationnelles sur l'ensemble de vos AWS ressources. Avec Systems Manager, vous pouvez regrouper les ressources par application, consulter les données opérationnelles à des fins de surveillance et de dépannage, et agir sur vos groupes de ressources. Systems Manager peut maintenir vos instances dans leur état défini, effectuer des modifications à la demande, telles que la mise à jour d'applications ou l'exécution de scripts shell, et effectuer d'autres tâches d'automatisation et de correction.

Stockage sécurisé

Amazon Simple Storage Service — Amazon S3 est un système de stockage d'objets conçu pour stocker et récupérer n'importe quel volume de données, où que vous soyez. Il est conçu pour offrir une durabilité de 99,999999999 % et stocke les données de millions d'applications utilisées par les leaders du marché dans tous les secteurs. Amazon S3 fournit une sécurité complète et est conçu pour vous aider à répondre à vos exigences réglementaires. Il offre aux clients une flexibilité dans les méthodes qu'ils utilisent pour gérer les données à des fins d'optimisation des coûts, de contrôle d'accès et de conformité. Amazon S3 fournit des query-in-place fonctionnalités qui vous permettent d'exécuter de puissantes analyses directement sur vos données au repos dans Amazon S3. Amazon S3 est un service de stockage dans le cloud hautement pris en charge, intégrant l'une des plus grandes communautés de solutions tierces, de partenaires intégrateurs de systèmes et d'autres AWS services.

Amazon S3 Glacier — Amazon S3 Glacier est un service de stockage cloud sécurisé, durable et extrêmement économique pour l'archivage des données et la sauvegarde à long terme. Il est conçu pour offrir une durabilité de 99,999999999 %, fournit une sécurité complète et est conçu pour vous aider à répondre à vos exigences réglementaires. S3 Glacier fournit des query-in-place fonctionnalités qui vous permettent d'exécuter de puissantes analyses directement sur vos données d'archive au repos. Pour réduire les coûts tout en répondant aux différents besoins de récupération, S3 Glacier propose trois options d'accès aux archives, allant de quelques minutes à plusieurs heures.

Capacités de sécurité futures et personnalisées

Les services et fonctionnalités mentionnés ci-dessus ne constituent pas une liste exhaustive. AWS ajoute continuellement de nouvelles fonctionnalités. Pour plus d'informations, nous vous invitons à consulter les pages Nouveautés chez AWS et AWS Cloud Security. Outre les services de sécurité proposés en tant que AWS services cloud natifs, vous souhaiterez peut-être développer vos propres capacités en plus des AWS services.

Bien que nous vous recommandions d'activer un ensemble de services de sécurité de base au sein de vos comptes AWS CloudTrail, tels qu'Amazon et Amazon Macie, vous souhaiterez peut-être étendre ces fonctionnalités afin de tirer une valeur supplémentaire de vos ressources de journal. GuardDuty Un certain nombre d'outils destinés aux partenaires sont disponibles, tels que ceux répertoriés dans notre programme de compétences en APN matière de sécurité. Vous pouvez également écrire vos propres requêtes pour effectuer des recherches dans vos journaux. Avec le grand nombre de services gérés AWS proposés, cela n'a jamais été aussi simple. Il existe de nombreux AWS services supplémentaires qui peuvent vous aider dans vos recherches et qui sortent du cadre de ce paper, tels qu'Amazon Athena, Amazon OpenSearch Service QuickSight, Amazon, Amazon Machine Learning et Amazon. EMR

Annexe B : ressources de réponse aux AWS incidents

AWS publie des ressources pour aider les clients à développer des capacités de réponse aux incidents. La plupart des exemples de code et de procédures se trouvent dans le référentiel GitHub public AWS externe. Voici quelques ressources qui fournissent des exemples de la manière de répondre aux incidents.

Ressources du Playbook

- Framework pour les playbooks de réponse aux incidents : exemple de framework permettant aux clients de créer, développer et intégrer des playbooks de sécurité en prévision de scénarios d'attaque potentiels lors de l'utilisation AWS de services.
- Développez vos propres manuels de réponse aux incidents - Cet atelier est conçu pour vous aider à vous familiariser avec l'élaboration de manuels de réponse aux incidents pour. AWS
- Exemples de playbooks de réponse aux incidents - Playbooks abordant les scénarios courants auxquels AWS sont confrontés les clients.
- Création d'un manuel de réponse aux AWS incidents à l'aide des playbooks Jupyter et de CloudTrail Lake - Cet atelier vous explique comment créer un manuel de réponse aux incidents pour votre AWS environnement à l'aide des blocs-notes Jupyter et de Lake. CloudTrail

Ressources médico-légales

- Cadre de réponse automatique aux incidents et de criminalistique : ce cadre et cette solution fournissent un processus d'investigation numérique standard, comprenant les phases suivantes : confinement, acquisition, examen et analyse. Il utilise les fonctions AWS λ pour déclencher

le processus de réponse aux incidents de manière automatique et reproductible. Il permet de séparer les comptes pour exécuter les étapes d'automatisation, stocker les artefacts et créer des environnements de criminalistique.

- Automated Forensics Orchestrator pour Amazon EC2 : ce guide de mise en œuvre fournit une solution en libre-service permettant de capturer et d'examiner les données des EC2 instances et des volumes attachés à des fins d'analyse judiciaire en cas de détection d'un problème de sécurité potentiel. Il existe un AWS CloudFormation modèle pour déployer la solution.
- Comment automatiser la collecte judiciaire des disques dans AWS — Ce AWS blog explique comment configurer un flux de travail automatisé pour capturer les preuves sur disque à des fins d'analyse afin de déterminer l'étendue et l'impact des incidents de sécurité potentiels. Un AWS CloudFormation modèle est également inclus pour déployer la solution.

Avis

Il incombe aux clients de procéder à une évaluation indépendante des informations contenues dans le présent document. Ce document : (a) est fourni à titre informatif uniquement, (b) représente les offres de AWS produits et les pratiques actuelles, qui sont susceptibles d'être modifiées sans préavis, et (c) ne crée aucun engagement ni aucune assurance de la part de AWS ses filiales, fournisseurs ou concédants de licence. AWS les produits ou services sont fournis « tels quels » sans garanties, déclarations ou conditions d'aucune sorte, qu'elles soient explicites ou implicites. Les responsabilités et obligations AWS de ses clients sont régies par AWS des accords, et ce document ne fait partie d'aucun accord conclu entre AWS et ses clients et ne les modifie pas.

Historique du document

Modification	Description	Date
Mise à jour : mises à jour à partir des commentaires des clients sur les documents.	Mise à jour https://docs.aws.amazon.com/security-ir/ latest/ userguide/setup : monitoring-and-investigation-workflows .html vers le modèle stackset. Entrées corrigées triage.security-ir.com to triage.security-ir.amazonaws.com Ajout d'une note sur les connexions suivies pour AWSSupport -Contain EC2Reversible on https:// docs.aws.amazon.com/ security-ir/ latest/userguide/contain .html. Correction d'un lien cassé sur le https://docs.aws.amazon.com/security-ir/ latest/ userguide/managing fichier - associated-accounts.html. Ajout d'une définition du compte de membre à l'adresse https://docs.aws.amazon.com /security-ir/ latest/userguide/ select - a-membership-account .html. Ajout d'une note de clarification à https://docs.aws.a	20 décembre 2024

Modification	Description	Date
	mazon.com/en_us/ security-ir/latest/userguide/using - service-linked-roles .html pour les comptes AWS Organizat ions de gestion.	

Modification	Description	Date
Mise à jour : mises à jour à partir des commentaires des clients sur les documents.	Suppression de plusieurs doublons AWS AWS dans le texte. Correction de liens brisés sur https://docs.aws.amazon.com/security-ir/ latest/userguide/sir_tagging.html and https://docs.aws.amazon.com/security-ir/latest/userguide/service - name-info-in-cloudtrail .html. Mises à jour du https://docs.aws.amazon.com/security-ir/ latest/userguide/ contain fichier .html. Le > a été supprimé du premier paragraphe. Remplacé AWSSupport -Contain par EC2Reversible AWSSupport EC2Instance -Contain. A remplacé AWSSupport -ContainIAMReversible par AWSSupport ontainIAM Principal -C. Remplacé AWSSupport -Contains 3Reversible par -Contains 3Resource. AWSSupport Mise à jour du formatage sur le fichier https://docs.aws.amazon.com/en_us/ de sécurité - ir/latest/userguide/ issues .html	10 décembre 2024

Modification	Description	Date
	Lorsque vous demandez aux clients de contacter CIRT via un ticket d'assistance, https://docs.aws.amazon.com /security-ir/ latest/userguide/u nderstand - response-teams- and-support .html propose désormais des options à sélectionner dans les formulair es d'assistance. CloudWatch Events supprimés et remplacés par EventBrid ge on https://docs.aws.a mazon.com/security-ir/ latest/ userguide/logging -and-even ts.html. Mises à jour grammatic ales sur https://docs.aws.a mazon.com/security-ir/ latest/ userguide/technique -access-c ontainment.html. Date de publication supprimée de https://docs.aws.a mazon.com/security-ir/ latest/userguide/security - incident-response-guide .html, remplacée par des mises à jour dans ce tableau.	
Mise à jour : politiques AWS gérées et rôles liés aux services.	Mises à jour des politiques gérées et des rôles liés aux services.	1er décembre 2016

Modification	Description	Date
Lancement de service	Documents de service initiaux pour le lancement du service lors de re:Invent 2024	1er décembre 2016

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.