Guia de implementação

Resposta de segurança automatizada em AWS

Resposta de segurança automatizada em AWS: Guia de implementação

Table of Contents

Aborde automaticamente as ameaças à segurança com ações predefinidas de resposta e remediação no AWS Security Hub

Data de publicação: agosto de 2020 (última atualização: dezembro de 2024)

Este guia de implementação fornece uma visão geral da AWS solução Automated Security Response on, sua arquitetura e componentes de referência, considerações para planejar a implantação e etapas de configuração para implantar a Automated Security Response on na AWS solução para a Amazon Web Services (AWS) Cloud.

Use esta tabela de navegação para encontrar rapidamente respostas para essas perguntas:

Se você deseja...	Leia…
Conheça o custo da execução dessa solução	Custos
Entenda as considerações de segurança dessa solução	Segurança
Saiba como planejar cotas para essa solução	Cotas
Saiba quais AWS regiões são compatíveis com essa solução	AWSRegiões suportadas
Visualize ou baixe o AWS CloudFormation modelo incluído nesta solução para implantar automaticamente os recursos de infraestrutura (a “pilha”) dessa solução	Modelos do AWS CloudFormation
Acesse o código-fonte e, opcionalmente, use o AWS Cloud Developme nt Kit (AWSCDK) para implantar a solução.	GitHub repositório

A evolução contínua da segurança exige etapas proativas para proteger os dados, o que pode tornar a reação das equipes de segurança difícil, cara e demorada. A AWS solução Automated Security Response on ajuda você a reagir rapidamente para resolver problemas de segurança, fornecendo respostas predefinidas e ações de remediação com base nos padrões de conformidade e nas melhores práticas do setor.

O Automated Security Response on AWS é uma AWS solução que trabalha AWS Security Hubpara melhorar sua segurança e ajuda a alinhar suas cargas de trabalho às melhores práticas do pilar Well-Architected Security (0). SEC1 Essa solução facilita que AWS Security Hub os clientes resolvam descobertas de segurança comuns e melhorem sua postura de segurança em AWS.

Você pode selecionar playbooks específicos para implantar na sua conta principal do Security Hub. Cada manual contém as ações personalizadas necessárias, as funções de Identity and Access Management (IAM), EventBridge as regras da Amazon, os documentos de automação do AWS Systems Manager e AWS Lambdaas funções AWS Step Functionsnecessárias para iniciar um fluxo de trabalho de remediação em uma única AWS conta ou em várias contas. As correções funcionam no menu Ações AWS Security Hub e permitem que usuários autorizados corrijam uma descoberta em todas as contas AWS Security Hub gerenciadas com uma única ação. Por exemplo, você pode aplicar as recomendações do Center for Internet Security (CIS) AWS Foundations Benchmark, um padrão de conformidade para proteger AWS recursos, para garantir que as senhas expirem em 90 dias e impor a criptografia dos registros de eventos armazenados. AWS

> **Note**
>
> A remediação é destinada a situações emergentes que exigem ação imediata. Essa solução faz alterações para corrigir as descobertas somente quando iniciada por você por meio do console AWS Security Hub de gerenciamento ou quando a remediação automática é habilitada usando a EventBridge regra da Amazon para um controle específico. Para reverter essas alterações, você deve colocar manualmente os recursos de volta em seu estado original.
>
> Ao remediar AWS recursos implantados como parte da CloudFormation pilha, esteja ciente de que isso pode causar um desvio. Quando possível, corrija os recursos da pilha modificando o código que define os recursos da pilha e atualizando a pilha. Para obter mais informações, consulte O que é deriva? no Guia do AWS CloudFormation usuário.

O Automated Security Response on AWS inclui o manual de correções para os padrões de segurança definidos como parte do seguinte:

- Referência de AWS fundamentos do Center for Internet Security (CIS) v1.2.0
- CISAWSBenchmark de fundações v1.4.0
- CISAWSBenchmark de fundações v3.0.0
- AWSMelhores práticas básicas de segurança (FSBP) v.1.0.0

- Padrão de segurança de dados do setor de cartões de pagamento (PCI-DSS) v3.2.1
- Instituto Nacional de Padrões e Tecnologia (NIST) SP 800-53 Rev. 5

A solução também inclui um manual do Security Controls (SC) para o recurso consolidado de descobertas de controle do AWS Security Hub. Para obter mais informações, consulte Playbooks.

Este guia de implementação discute considerações arquitetônicas e etapas de configuração para implantar a Resposta de Segurança Automatizada em AWS uma solução na nuvem. AWS Ele inclui links para AWS CloudFormationmodelos que iniciam, configuram e executam a AWS computação, a rede, o armazenamento e outros serviços necessários para implantar essa soluçãoAWS, usando as AWS melhores práticas de segurança e disponibilidade.

O guia é destinado a arquitetos, administradores e DevOps profissionais de infraestrutura de TI com experiência prática em arquitetura na AWS nuvem.

Recursos e benefícios

O Automated Security Response on AWS fornece os seguintes recursos:

Corrija automaticamente as descobertas para controles específicos

Ative EventBridge as regras de controles da Amazon para corrigir automaticamente as descobertas desse controle imediatamente após elas aparecerem no AWS Security Hub.

Gerencie remediações em várias contas e regiões a partir de um único local

A partir de uma conta de administrador do AWS Security Hub configurada como o destino de agregação das contas e regiões da sua organização, inicie uma remediação para uma descoberta em qualquer conta e região em que a solução esteja implantada.

Seja notificado sobre ações e resultados de remediação

Inscreva-se no SNS tópico da Amazon implantado pela solução para ser notificado quando as remediações forem iniciadas e se a remediação foi bem-sucedida ou não.

Integre com sistemas de tickets como Jira ou ServiceNow

Para ajudar sua organização a reagir às correções (por exemplo, atualizar seu código de infraestrutura), essa solução pode enviar tickets para seu sistema externo de tíquetes.

Uso AWSConfigRemediations nas partições GovCloud e na China

Algumas das correções incluídas na solução são repacotes de AWSConfigRemediation documentos AWS de propriedade própria que estão disponíveis na partição comercial, mas não na China. GovCloud Implante essa solução para usar esses documentos nessas partições.

Estenda a solução com correções personalizadas e implementações do Playbook

A solução foi projetada para ser extensível e personalizável. Para especificar uma implementação alternativa de remediação, implante documentos e AWS IAM funções de automação personalizados do AWS Systems Manager. Para oferecer suporte a um conjunto totalmente novo de controles que não é implementado pela solução, implante um Playbook personalizado.

Casos de uso

Imponha a conformidade com um padrão em todas as contas e regiões da sua organização

Implante o manual de um padrão (por exemplo, as melhores práticas AWS básicas de segurança) para poder usar as correções fornecidas. Inicie as correções de recursos de forma automática ou manual em qualquer conta e região em que a solução seja implantada para corrigir recursos que estão fora de conformidade.

Implemente correções ou playbooks personalizados para atender às necessidades de conformidade da sua organização

Use os componentes do Orchestrator fornecidos como uma estrutura. Crie correções personalizadas para lidar com out-of-compliance os recursos de acordo com as necessidades específicas da sua organização.

Conceitos e definições

Esta seção descreve os conceitos básicos e define a terminologia específica desta solução:

aplicativo

Um grupo lógico de AWS recursos que você deseja operar como uma unidade.

remediação, caderno de execução de remediação

Uma implementação de um conjunto de etapas que resolve uma descoberta. Por exemplo, uma remediação para o controle Security Control (SC) Lambda.1 “As políticas da função Lambda devem

proibir o acesso público” modificaria a política da Função AWS Lambda relevante para remover declarações que permitem o acesso público.

caderno de controle

Um de um conjunto de documentos de automação do AWS Systems Manager (SSM) que o orquestrador usa para rotear uma remediação iniciada de um controle específico para o runbook de remediação correto. Por exemplo, as correções para SC Lambda.1 e AWS Foundational Security Best Practices (FSBP) Lambda.1 são implementadas com o mesmo runbook de remediação. O orquestrador invoca o runbook de controle para cada controle, que é denominado ASR - AFSBP _Lambda.1 e -SC_2.0.0_Lambda.1, respectivamente. ASR Cada runbook de controle invoca o mesmo runbook de remediação, que neste caso seria -. ASR RemoveLambdaPublicAccess

orquestrador

O Step Functions implantado pela solução que usa como entrada um objeto de busca do AWS Security Hub e invoca o runbook de controle correto na conta e na região de destino. O orquestrador também notifica o SNS tópico da solução quando a remediação é iniciada e quando a correção é bem-sucedida ou falha.

padrão

Um grupo de controles definido por uma organização como parte de uma estrutura de conformidade. Por exemplo, um dos padrões suportados pelo AWS Security Hub e essa solução é AWSFSBP.

controle

Uma descrição das propriedades que um recurso deve ou não ter para estar em conformidade. Por exemplo, o controle AWS FSBP Lambda.1 afirma que as Funções AWS Lambda devem proibir o acesso público. Uma função que permite acesso público falharia nesse controle.

descobertas de controle consolidadas, controle de segurança, visualização de controles de segurança

Um recurso do AWS Security Hub que, quando ativado, exibe as descobertas com seu controle consolidado, IDs em vez de IDs corresponder a um padrão específico. Por exemplo, os controles AWS FSBP S3.2, CIS v1.2.0 2.3, CIS v1.4.0 2.1.5.2 e PCI - DSS v3.2.1 S3.1 são todos mapeados para o controle consolidado (SC) S3.2 “Os buckets do S3 devem proibir o acesso público de leitura”. Quando esse recurso está ativado, os runbooks SC são usados.

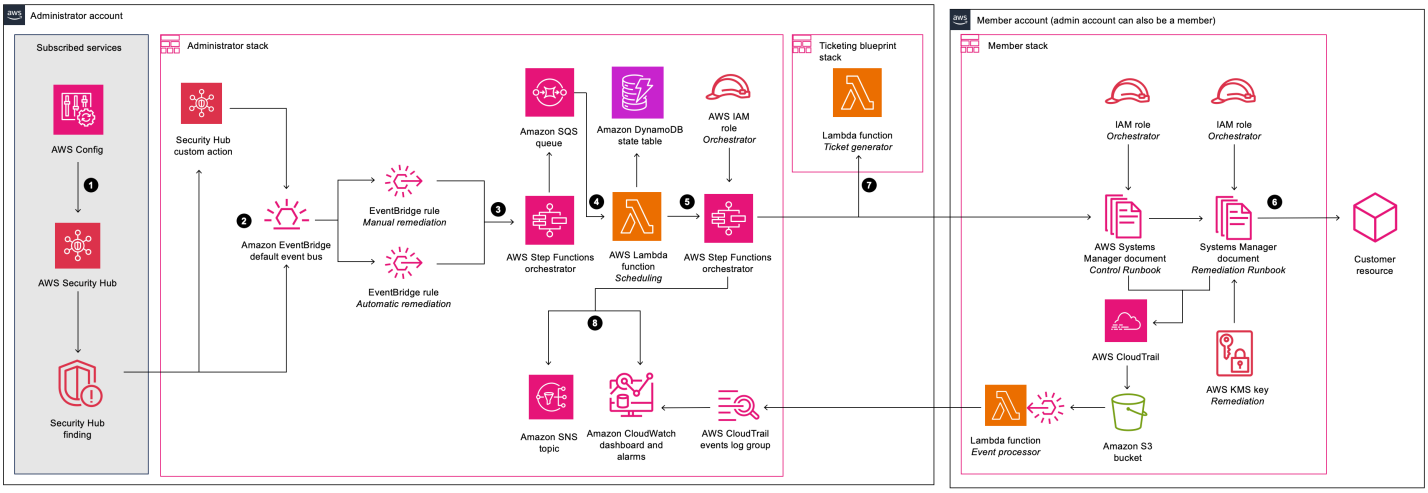
Para obter uma referência geral dos AWS termos, consulte o AWS Glossário.

Visão geral da arquitetura

Esta seção fornece um diagrama de arquitetura de implementação de referência para os componentes implantados com essa solução.

Diagrama de arquitetura

A implantação dessa solução com os parâmetros padrão cria o seguinte ambiente na AWS nuvem.



Resposta de segurança automatizada na AWS arquitetura

> **Note**
>
> AWS CloudFormation os recursos são criados a partir de construções do AWS Cloud Development Kit (AWSCDK).

O fluxo de processo de alto nível para os componentes da solução implantados com o AWS CloudFormation modelo é o seguinte:

1. Detectar: AWS Security Hubfornece aos clientes uma visão abrangente de seu estado AWS de segurança. Isso os ajuda a medir seu ambiente em relação aos padrões e às melhores práticas do setor de segurança. Ele funciona coletando eventos e dados de outros AWS serviços AWS Config, como Amazon Guard Duty e AWS Firewall Manager. Esses eventos e dados são analisados de acordo com padrões de segurança, como o CIS AWS Foundations Benchmark. As exceções são declaradas como descobertas no AWS Security Hub console. Novas descobertas são enviadas como EventBridge eventos da Amazon.

2. Iniciar: você pode iniciar eventos com base nas descobertas usando ações personalizadas, que resultam em EventBridge eventos. AWS Security Hub ações e EventBridge regras personalizadas iniciam a Resposta de Segurança Automatizada em AWS manuais para abordar as descobertas. A solução implanta:

   a. Uma EventBridge regra para corresponder ao evento de ação personalizado

   b. Uma regra de EventBridge evento para cada controle suportado (desativada por padrão) para corresponder ao evento de localização em tempo real

   Você pode usar o menu Ações personalizadas no console do Security Hub para iniciar a correção automática. Depois de testes cuidadosos em um ambiente que não seja de produção, você também pode ativar correções automatizadas. Você pode ativar automações para remediações individuais — você não precisa ativar iniciações automáticas em todas as remediações.

3. Pré-remediação: na conta do administrador, AWS Step Functionsprocessa o evento de remediação e o prepara para ser agendado.

4. Programação: a solução invoca a AWS Lambdafunção de agendamento para colocar o evento de remediação na tabela de estados do Amazon DynamoDB.

5. Orquestrar: na conta de administrador, o Step Functions usa funções cross-account AWS Identity and Access Management()IAM. Step Functions invoca a remediação na conta do membro que contém o recurso que produziu a descoberta de segurança.

6. Remediar: um documento de AWS Systems Managerautomação na conta do membro executa a ação necessária para corrigir a descoberta no recurso de destino, como desativar o acesso público do Lambda.

   Opcionalmente, você pode ativar o recurso Action Log nas pilhas de membros com o EnableCloudTrailForASRActionLogparâmetro. Esse recurso captura as ações realizadas pela solução em suas contas de membros e as exibe no CloudWatch painel da solução na Amazon.

7. (Opcional) Crie um ticket: se você usar o TicketGenFunctionNameparâmetro para ativar a emissão de tíquetes na pilha de administração, a solução invoca a função Lambda do gerador de tickets fornecida. Essa função Lambda cria um ticket em seu serviço de emissão de bilhetes após a correção ter sido executada com sucesso na conta do membro. Fornecemos pilhas para integração com o Jira e. ServiceNow

8. Notificar e registrar: o manual registra os resultados em um CloudWatch grupo de registros, envia uma notificação para um tópico do Amazon Simple Notification Service (AmazonSNS) e atualiza a descoberta do Security Hub. A solução mantém uma trilha de auditoria das ações nas notas de descoberta.

Considerações de design do AWS Well-Architected

Essa solução foi projetada com as melhores práticas do AWS Well-Architected Framework, que ajuda os clientes a projetar e operar cargas de trabalho confiáveis, seguras, eficientes e econômicas na nuvem. Esta seção descreve como os princípios de design e as melhores práticas do Well-Architected Framework foram aplicados ao criar essa solução.

Excelência operacional

Esta seção descreve como arquitetamos essa solução usando os princípios e as melhores práticas do pilar de excelência operacional.

- Recursos definidos como uso CloudFormation de IaC.
- Remediações implementadas com as seguintes características, sempre que possível:
  - Potência igual
  - Tratamento e emissão de relatórios de erros
  - Registro em log
  - Restaurando recursos para um estado conhecido em caso de falha

Segurança

Esta seção descreve como arquitetamos essa solução usando os princípios e as melhores práticas do pilar de excelência operacional.

- IAMusado para autenticação e autorização.

- O escopo das permissões de função deve ser o mais restrito possível, embora, em muitos casos, essa solução exija permissões curinga para poder atuar em qualquer recurso.

Confiabilidade

Esta seção descreve como arquitetamos essa solução usando os princípios e as melhores práticas do pilar de confiabilidade.

- O Security Hub continua criando descobertas se a causa subjacente da descoberta não for resolvida pela remediação.

- Os serviços de tecnologia sem servidor permitem que a solução seja escalada conforme necessário.

Eficiência de desempenho

Esta seção descreve como arquitetamos essa solução usando os princípios e as melhores práticas do pilar de excelência operacional.

- Essa solução foi projetada para ser uma plataforma para você estender sem precisar implementar orquestração e permissões sozinho.

Otimização de custo

Esta seção descreve como arquitetamos essa solução usando os princípios e as práticas recomendadas do pilar de otimização do custo.

- Os serviços de tecnologia sem servidor permitem que você pague apenas pelo que usa.
- Use o nível gratuito para SSM automação em todas as contas

Sustentabilidade

Esta seção descreve como arquitetamos essa solução usando os princípios e as melhores práticas do pilar de sustentabilidade.

- Os serviços de tecnologia sem servidor permitem aumentar a escala da solução verticalmente conforme necessário.

Detalhes de arquitetura

Esta seção descreve os componentes e AWS serviços que compõem essa solução e os detalhes da arquitetura sobre como esses componentes funcionam juntos.

AWS Security Hub integração

A implantação da `aws-sharr-deploy` pilha cria integração com o recurso de ação personalizada do AWS Security Hub. Quando os usuários AWS Security Hub do console selecionam Descobertas para remediação, a solução encaminha o registro de descoberta para remediação usando um. AWS Step Functions

Permissões e AWS Systems Manager runbooks entre contas devem ser implantados em todas as AWS Security Hub contas (administrador e membro) usando os modelos e. `aws-sharr-member.template` `aws-sharr-member-roles.template` CloudFormation Para obter mais informações, consulte Playbooks. Esse modelo permite a remediação automática na conta de destino.

Os usuários podem iniciar automaticamente remediações automatizadas por remediação usando as regras de eventos da Amazon. CloudWatch Essa opção ativa a remediação totalmente automática das descobertas assim que elas são reportadas. AWS Security Hub Por padrão, as iniciações automáticas são desativadas. Essa opção pode ser alterada a qualquer momento durante ou após a instalação do manual, ativando as regras de CloudWatch eventos na conta do AWS Security Hub administrador.

Remediação entre contas

O Automated Security Response on AWS usa funções entre contas para trabalhar em contas primárias e secundárias usando funções entre contas. Essas funções são implantadas nas contas dos membros durante a instalação da solução. Cada remediação recebe uma função individual. O processo de remediação na conta principal recebe permissão para assumir a função de remediação na conta que requer remediação. A correção é realizada pelos runbooks do AWS Systems Manager em execução na conta que requer remediação.

Manuais

Um conjunto de remediações é agrupado em um pacote chamado manual. Os playbooks são instalados, atualizados e removidos usando os modelos dessa solução. Para obter informações sobre as correções suportadas em cada manual, consulte Guia do desenvolvedor -> Manuais. Atualmente, essa solução oferece suporte aos seguintes manuais:

- Security Control, um manual alinhado com o recurso de descobertas de controle consolidadas do AWS Security Hub, publicado em 23 de fevereiro de 2023.

> **Important**
>
> Quando as descobertas de controle consolidadas estão habilitadas no Security Hub, esse é o único manual que deve ser ativado na solução.

- Os benchmarks do Center for Internet Security (CIS) Amazon Web Services Foundations, versão 1.2.0, publicada em 18 de maio de 2018.
- Benchmarks do Center for Internet Security (CIS) Amazon Web Services Foundations, versão 1.4.0, publicada em 9 de novembro de 2022.
- Os benchmarks do Center for Internet Security (CIS) Amazon Web Services Foundations, versão 3.0.0, publicada em 13 de maio de 2024.
- AWS Foundational Security Best Practices (FSBP) versão 1.0.0, publicada em março de 2021.
- Padrões de segurança de dados do setor de cartões de pagamento (PCI-DSS), versão 3.2.1, publicada em maio de 2018.
- Instituto Nacional de Padrões e Tecnologia (NIST) versão 5.0.0, publicada em novembro de 2023.

Registro centralizado

Resposta de segurança automatizada em AWS registros para um único grupo de CloudWatch registros, SO0111-. SHARR Esses registros contêm registros detalhados da solução para solução de problemas e gerenciamento da solução.

Notificações

Essa solução usa um tópico do Amazon Simple Notification Service (AmazonSNS) para publicar resultados de remediação. Você pode usar assinaturas deste tópico para ampliar os recursos da solução. Por exemplo, você pode enviar notificações por e-mail e atualizar os tickets de problemas.

Serviços da AWS nesta solução

A solução usa os seguintes serviços. Os serviços principais são necessários para usar a solução, e os serviços de suporte conectam os serviços principais.

AWS serviço	Descrição
Amazon EventBridge	Principal. Implanta eventos que iniciarão a função de etapa do orquestrador quando uma descoberta estiver sendo corrigida.
AWS IAM	Principal. Implanta várias funções para permitir correções em diferentes recursos.
AWS Lambda	Principal. Implanta várias funções lambda que serão usadas pelo orquestrador de funções step para corrigir problemas.
AWS Security Hub	Principal. Oferece aos clientes uma visão abrangente de seu estado AWS de segurança.
AWS Step Functions	Principal. Implanta um orquestrador que invocará os documentos de remediação com chamadas do Systems Manager. AWS API
AWS Systems Manager (Gerenciador de sistemas)	Principal. Implanta documentos do System Manager (link para o documento) que contêm a lógica de remediação que será executada.
AWS CloudTrail	Suporte. Registra as alterações que a solução faz em seus AWS recursos e as exibe em um CloudWatch painel.

AWS serviço	Descrição
Amazon CloudWatch	Suporte. Implanta grupos de registros que os diferentes playbooks usarão para registrar os resultados. Coleta métricas para exibir em um painel personalizado com alarmes.
AWS DynamoDB	Suporte. Armazena a última correção executada em cada conta e região para otimizar o agendamento das remediações.
Service Catalog AppRegistry	Suporte. Implanta o aplicativo para pilhas implantadas para monitorar o custo e o uso.
Amazon Simple Notification Service	Suporte. Implanta SNS tópicos que recebem uma notificação após a conclusão da remediação.
AWS SQS	Suporte. Auxilia no agendamento de remediaçõ es para que a solução possa executar remediações em paralelo.

Planeje a implantação

Esta seção descreve o custo, a segurança da rede, o suporte Regiões da AWS, as cotas e outras considerações antes da implantação da solução.

Custo

Você é responsável pelo custo dos AWS serviços usados para executar essa solução. A partir dessa revisão, o custo de executar essa solução com as configurações padrão no Leste dos EUA (Norte da Virgínia) Região da AWS é de aproximadamente 21,17 USD por 300 remediações/mês, 134,86 USD por 3.000 remediações/mês e 1.281,01 USD por 30.000 remediações/mês. Os preços estão sujeitos a alterações. Para obter detalhes completos, consulte a página de preços AWS de cada serviço usado nesta solução.

> **Note**
>
> Muitos AWS serviços incluem um nível gratuito — um valor básico do serviço que os clientes podem usar gratuitamente. Os custos reais podem ser maiores ou menores do que os exemplos de preços fornecidos.

Recomendamos criar um orçamentoAWS Cost Explorer para ajudar a gerenciar os custos. Os preços estão sujeitos a alterações. Para obter detalhes completos, consulte a página de preços de cada AWS serviço usado nesta solução.

Tabela de custos da amostra

O custo total para executar essa solução depende dos seguintes fatores:

- O número de contas de AWS Security Hub membros
- O número de remediações ativas invocadas automaticamente
- A frequência da remediação

Essa solução usa os seguintes AWS componentes, que têm um custo com base na sua configuração. Exemplos de preços são fornecidos para organizações de pequeno, médio e grande porte.

Serviço	Nível gratuito	Preços [USD]
AWS Systems Manager Automation - Contagem de etapas	100.000 etapas por conta por mês	Além do nível gratuito, cada etapa básica é cobrada em 0,002 USD por etapa. Para automações de várias contas, todas as etapas, incluindo aquelas executadas em qualquer conta secundária, são contadas somente na conta de origem.
AWS Systems Manager Automation - Duração da etapa	5.000 segundos por mês	Além do nível gratuito, cada etapa do aws: executeScript action é cobrada em 0,00003 USD por cada segundo após um nível gratuito de 5.000 segundos por mês.
AWS Systems Manager Automation — Armazenamento	Sem nível gratuito	0,046 USD por GB por mês
AWS Systems Manager Automation - Transferência de dados	Sem nível gratuito	0,900 USD por GB transferido (para contas cruzadas ou) out-of-Region
AWS Security Hub - Verificações de segurança	Sem nível gratuito	Os primeiros 100.000 checks/account/Region/month custam $0,0010 por cheque Os próximos 400.000 checks/account/Region/month custam $0,0008 por cheque Mais de 500.000 checks/account/Region/month custam $0,0005 por cheque

Serviço	Nível gratuito	Preços [USD]
AWS Security Hub - Encontrar eventos de ingestão	Os primeiros 10.000 events/account/Region/month são gratuitos. Encontrar eventos de ingestão associados às verificações de segurança do Security Hub.	Mais de 10.000 events/account/Region/month custam $0,00003 por evento
Amazon CloudWatch - Métricas	Métricas básicas de monitoramento (com frequência de 5 minutos) 10 métricas de monitoramento detalhadas (com frequência de 1 minuto) 1 milhão de API solicitações (não aplicável a GetMetricData e GetMetricWidgetImage)	As primeiras 10.000 métricas custam 0,30 USD por mês As próximas 240.000 métricas custam 0,10 USD por mês As próximas 750.000 métricas custam 0,05 USD por mês Mais de 1.000.000 de métricas custam 0,02 USD por mês APIas chamadas custam 0,01 USD por 1.000 solicitações
Amazon CloudWatch - Painel de controle	3 painéis para até 50 métricas por mês	$3,00 por painel por mês

Serviço	Nível gratuito	Preços [USD]
Amazon CloudWatch - Alarmes	10 métricas de alarme (não aplicáveis a alarmes de alta resolução)	A resolução padrão (60 segundos) custa 0,10 USD por métrica de alarme A alta resolução (10 segundos) custa 0,30 USD por métrica de alarme A detecção de anomalias com resolução padrão custa 0,30 USD por alarme A detecção de anomalias de alta resolução custa $0,90 por alarme O composto custa $0,50 por alarme
Amazon CloudWatch - Coleção de registros	Dados de 5 GB (ingestão, armazenamento de arquivos e dados digitalizados por consultas do Logs Insights)	0,50 USD por GB
Amazon CloudWatch - Armazenamento de registros	Dados de 5 GB (ingestão, armazenamento de arquivos e dados digitalizados por consultas do Logs Insights)	0,005 USD por GB de dados digitalizados
Amazon CloudWatch - Eventos	Todos os eventos, exceto eventos personalizados, estão incluídos	1,00 USD por milhão de eventos para eventos personalizados 1,00 USD por milhão de eventos para eventos entre contas
AWS Lambda - Solicitações	1 milhão de solicitações gratuitas por mês	0,20 USD por 1 milhão de solicitações

Serviço	Nível gratuito	Preços [USD]
AWS Lambda - Duração	400.000 GB-segundos de tempo de computação por mês	0,0000166667 USD por cada GB-segundo. O preço da duração depende da quantidade de memória que você aloca para sua função. Você pode alocar qualquer quantidade de memória para sua função entre 128 MB e 10.240 MB, em incrementos de 1 MB.
AWS Step Functions - Transições estaduais	4.000 transições de estado gratuitas por mês	0,025 USD por 1.000 transições de estado posteriores
Amazon EventBridge	Todos os eventos de mudança de estado publicados pelos AWS serviços são gratuitos	Eventos personalizados custam 1,00 dólares/milhão de eventos personalizados publicados Eventos de terceiros (SaaS) custam 1,00 USD/milhão de eventos publicados Eventos entre contas custam 1,00 USD/milhão de eventos enviados entre contas
Amazon SNS	Os primeiros 1 milhão de SNS solicitações da Amazon por mês são gratuitas	0,50 USD por 1 milhão de solicitações posteriores
Amazon SQS	Os primeiros 1 milhão de SQS solicitações da Amazon por mês são gratuitas	0,40 USD por 1 milhão a 100 bilhões de solicitações posteriores

Serviço	Nível gratuito	Preços [USD]
Amazon DynamoDB	Os primeiros 25 GB de armazenamento são gratuitos	2,00 USD por 1 milhão de leituras e gravações consistentes a partir de então

Exemplos de preços (mensais)

Exemplo 1:300 remediações por mês

- 10 contas, 1 região
- 30 remediações por account/Region/month
- Custo total $21,17 por mês

Serviço	Suposições	Cobranças mensais [...USD]
AWS Automação do Systems Manager	Etapas: ~4 etapas* 300 remediações* 0,002 USD = 2,40 USD Duração: 10s * 300 remediações* 0,00003 USD = 0,09 USD	$2,49
AWS Security Hub	Nenhum serviço faturável utilizado	$0
CloudWatch Registros da Amazon	300 remediações * 0,000002 USD = 0,0006 USD 0,0006 USD* 0,03 = 0,000018 US$	< 0,01 US$
AWS Lambda - Solicitações	300 remediações * 6 solicitações = 1.800 solicitações	$0,20

Serviço	Suposições	Cobranças mensais [...USD]
	0,20 USD* 1.000.000 de solicitações = 0,20 USD	
AWS Lambda - Duração	256 milhões: 1,875 GB seg * 300 remediações * 0,0000167 USD = 0,009375 USD	< 0,01 US$
AWS Step Functions	17 transições de estado * 300 remediações = 5.100 0,025 USD* (5.100/1.000) transições de estado = 0,15 USD	0,15 US$
EventBridge Regras da Amazon	Sem cobrança pelas regras	$0
AWS Key Management Service	1 chave* 10 contas* 1 região* $1 = $10	$10,00
Amazon DynamoDB	2,00 USD* 1.000.000 de leitura e gravação = 2,00 USD	$2,00
Amazon SQS	0,40 USD* 1.000.000 de solicitações = 0,40 USD	$0,40
Amazon SNS	0,50 USD* 1.000.000 de notificações = 0,50 USD	$0,50
Amazon CloudWatch - Métricas	0,30 USD* 7 métricas personalizadas = 2,10 US$ 0,01 USD* (300 * 3/1.000) API chamadas de métricas de venda = 0,01 USD	$2,11
Amazon CloudWatch - Painéis	$3,00 * 1 painel = $3,00	$3,00

Serviço	Suposições	Cobranças mensais [...USD]
Amazon CloudWatch — Alarmes	0,10 USD* 3 alarmes = 0,30 US$	$0,30
Total		$21,17

Exemplo 2:3.000 remediações por mês

- 100 contas, 1 região
- 30 remediações por account/Region/month
- Custo total: $134,86 por mês

Serviço	Suposições	Cobranças mensais [...USD]
AWS Automação do Systems Manager	Etapas: ~4 etapas* 3.000 remediações* 0,002 USD = 24,00 USD Duração: 10s * 3.000 remediações* 0,00003 USD = 0,90 USD	$24,90
AWS Security Hub	Nenhum serviço faturável utilizado	$0
CloudWatch Registros da Amazon	3.000 remediações * 0,000002 USD = 0,006 USD 0,006 USD* 0,03 = 0,00018 US$	< 0,01 US$
AWS Lambda - Solicitações	3.000 remediações * 6 solicitações = 18.000 solicitações	$0,20

Serviço	Suposições	Cobranças mensais [...USD]
	0,20 USD* 1.000.000 de solicitações = 0,20 USD	
AWS Lambda - Duração	256 milhões: 1,875 GB seg * 3.000 remediações * 0,000167 USD = 0,09375 USD	$0,09
AWS Step Functions	17 transições de estado* 3.000 remediações = 51.000 transições de estado de 0,025 USD* (51.000/1.000) = 1,275 USD	$1,28
EventBridge Regras da Amazon	Sem cobrança pelas regras	$0
AWS Key Management Service	1 chave * 100 contas* 1 região* $1 = $100	100 USD
Amazon DynamoDB	2,00 USD* 1.000.000 de leitura e gravação = 2,00 USD	$2,00
Amazon SQS	0,40 USD* 1.000.000 de solicitações = 0,40 USD	$0,40
Amazon SNS	0,50 USD* 1.000.000 de notificações = 0,50 USD	$0,50
Amazon CloudWatch - Métricas	0,30 USD* 7 métricas personalizadas = 2,10 US$ 0,01 USD* (3000 * 3/1.000) API chamadas de métricas de venda = 0,09 USD	$2,19
Amazon CloudWatch - Painéis	$3,00 * 1 painel = $3,00	$3,00

Serviço	Suposições	Cobranças mensais [...USD]
Amazon CloudWatch — Alarmes	0,10 USD* 3 alarmes = 0,30 US$	$0,30
Total		$134,86

Exemplo 3:30.000 remediações por mês

- 1.000 contas, 1 região
- 30 remediações por account/Region/month
- Custo total: $1.281,01 por mês

Serviço	Suposições	Cobranças mensais [...USD]
AWS Automação do Systems Manager	Etapas: ~4 etapas* 30.000 remediações* 0,002 USD = 240,00 USD Duração: 10s * 30.000 remediações* 0,00003 USD = 9,00 USD	$249,00
AWS Security Hub	Nenhum serviço faturável utilizado	$0
CloudWatch Registros da Amazon	30.000 remediações * 0,000002 USD = 0,06 USD 0,06 USD* 0,03 = 0,0018 US$	< 0,01 US$
AWS Lambda - Solicitações	30.000 remediações * 6 solicitações = 180.000 solicitações 0,20 USD* 1.000.000 de solicitações = 0,20 USD	$0,20

Serviço	Suposições	Cobranças mensais [...USD]
AWS Lambda - Duração	256 milhões: 1,875 GB seg * 30.000 remediações * 0,000167 USD = 0,9375 USD	$0,94
AWS Step Functions	17 transições de estado* 30.000 remediações = 510.000 transições de estado de 0,025 USD* (510.000/1.000) = 12,75 USD	$12,75
EventBridge Regras da Amazon	Sem cobrança pelas regras	$0
AWS Key Management Service	1 chave* 1.000 contas* 1 região* $1 = $1.000	$1.000
Amazon DynamoDB	0,000002 USD* 1.000.000 de leitura e gravação = 2,00 USD	$2,00
Amazon SQS	0,000004 USD* 1.000.000 de solicitações = 0,40 USD	$0,40
Amazon SNS	0,000005 USD* 1.000.000 de notificações = 0,50 USD	$0,50
Amazon CloudWatch - Métricas	0,30 USD* 6 métricas personalizadas = 1,80 USD 0,01 USD* (30.000 * 3/1.000) chamadas de métricas API de venda = 0,90 USD	$2,70
Amazon CloudWatch - Painéis	$3,00 * 1 painel = $3,00	$3,00

Serviço	Suposições	Cobranças mensais [...USD]
Amazon CloudWatch — Alarmes	0,10 USD* 2 alarmes = 0,20 US$	$0,20
Amazon CloudWatch — Application Insights	0,10 USD* 40 alarmes (máximo) = 4,00 US$ 0,53 USD* 10 GB de dados de registro (aprox.) = $5,30 $0,00267 OpsItems * (aprox.) = ~$0,01	$9,31
Total		$1.281,01

Custo adicional para recursos opcionais

Esta seção identifica os custos adicionais associados aos recursos opcionais dessa solução.

CloudWatch Métricas aprimoradas

Se você selecionar `yes` o EnableEnhancedCloudWatchMetricsparâmetro ao implantar a pilha de administração, a solução criará duas métricas personalizadas e um alarme para cada ID de controle. O custo depende do número de controles IDs que você está remediando. Na tabela a seguir, presumimos que você esteja remediando todos os 96 controles diferentes IDs por mês, para determinar o limite superior dos custos.

Serviço	Suposições 96 controles IDs * 2 = 192 métricas personalizadas	Cobranças mensais [...USD]
Amazon CloudWatch - Métricas	0,30 USD* 192 métricas personalizadas = 57,60 USD	$57,60
Amazon CloudWatch - Alarmes	0,10 USD* 96 alarmes = 9,60 US$	$9,60

Serviço	Suposições	Cobranças mensais [...USD]
	96 controles IDs * 2 = 192 métricas personalizadas	
Total		$67,20

CloudTrail Registro de ações

Em cada conta de membro para a qual você ativa o recurso Action Log, as soluções criam uma CloudTrail trilha para registrar todos os eventos de gerenciamento de gravação. Uma função Lambda filtra eventos não relacionados à solução. Isso significa que o custo está relacionado ao número total de eventos de gerenciamento em sua conta, pois os eventos não relacionados à solução ainda são capturados pela trilha e processados pela função Lambda.

Para a tabela a seguir, presumimos 150.000 eventos de gerenciamento por mês na conta. O custo real depende da atividade real do evento de gerenciamento em sua conta.

Serviço	Suposições	Cobranças mensais [...USD]
AWS CloudTrail	150.000 * $2,00/100.000 = $3,00	$3,00
Lambda	150.000 * 0,2 * 0,125 = 3.750 GB por segundo 3.750 * 0,0000166667 USD = custo de tempo de computaçã o de 0,0625 USD 0,15 * 0,20 USD = custo de solicitação de 0,03 USD 0,0625 USD + 0,03 USD = custo total do Lambda de 0,0952 USD	$0,0925
Total		$3,09 por conta de membro

Segurança

Quando você cria sistemas na infraestrutura da AWS, as responsabilidades de segurança são compartilhadas entre você e a AWS. Esse modelo compartilhado reduz sua carga operacional porque AWS opera, gerencia e controla os componentes, incluindo o sistema operacional do host, a camada de virtualização e a segurança física das instalações nas quais os serviços operam. Para obter mais informações sobre AWS segurança, visite o AWSCloud Security.

Funções do IAM

AWSAs funções Identity and Access Management (IAM) permitem que os clientes atribuam políticas e permissões de acesso granulares a serviços e usuários na AWS nuvem. Essa solução cria IAM funções que concedem às funções automatizadas da solução acesso para realizar ações de remediação dentro de um conjunto restrito de permissões específicas para cada remediação.

A função Step da conta de administrador é atribuída à função SO0111-SHARR-Orchestrator-Admin . Somente essa função pode assumir o SO0111-Orchestrator-Member em cada conta de membro. Cada função de remediação permite que a função de membro seja transmitida ao serviço AWS Systems Manager para executar runbooks de remediação específicos. Os nomes das funções de remediação começam com SO0111, seguidos por uma descrição correspondente ao nome do runbook de remediação. Por exemplo, SO0111-R emoveVPCDefault SecurityGroupRules é a função do runbook de remediação -R. ASR emoveVPCDefault SecurityGroupRules

Suportado Regiões da AWS

Nome da região	Código da região
Leste dos EUA (Ohio)	us-east-2
Leste dos EUA (N. da Virgínia)	us-east-1
Oeste dos EUA (Norte da Califórnia)	us-west-1
Oeste dos EUA (Oregon)	us-west-2
África (Cidade do Cabo)	af-south-1
Ásia-Pacífico (Hong Kong)	ap-east-1

Nome da região	Código da região
Ásia-Pacífico (Hyderabad)	ap-south-2
Ásia-Pacífico (Jacarta)	ap-southeast-3
Ásia-Pacífico (Melbourne)	ap-southeast-4
Ásia-Pacífico (Mumbai)	ap-south-1
Ásia-Pacífico (Osaka)	ap-northeast-3
Ásia-Pacífico (Seul)	ap-northeast-2
Ásia-Pacífico (Singapura)	ap-southeast-1
Ásia-Pacífico (Sydney)	ap-southeast-2
Ásia-Pacífico (Tóquio)	ap-northeast-1
Canadá (Central)	ca-central-1
Europa (Frankfurt)	eu-central-1
Europa (Irlanda)	eu-west-1
Europa (Londres)	eu-west-2
Europa (Milão)	eu-south-1
Europa (Paris)	eu-west-3
Europa (Espanha)	eu-south-2
Europa (Estocolmo)	eu-north-1
Europa (Zurique)	eu-central-2
Oriente Médio (Bahrein)	me-south-1
Oriente Médio (UAE)	me-central-1

Nome da região	Código da região
América do Sul (São Paulo)	sa-east-1
AWS GovCloud (Leste dos EUA)	us-gov-east-1
AWS GovCloud (Oeste dos EUA)	us-gov-east-2
China (Pequim)	cn-north-1
China (Ningxia)	cn-northwest-1

Cotas

As service quotas, também chamadas de limites, correspondem ao número máximo de recursos ou operações de serviço para sua conta da AWS.

Cotas para serviços da AWS nesta solução

Verifique se você tem cota suficiente para cada um dos serviços implementados nessa solução. Sim, para mais informações, consulte AWS Service Quotas.

Use os links a seguir para acessar a página desse serviço. Para ver as Cotas de Serviço para todos os AWS serviços na documentação sem trocar de página, veja as informações na página Pontos de extremidade e cotas de serviço em vez disso. PDF

AWS CloudFormation cotas

Sua AWS conta tem AWS CloudFormation cotas que você deve conhecer ao lançar a pilha nesta solução. Ao compreender essas cotas, você pode evitar erros de limitação que o impediriam de implantar essa solução com êxito. Para obter mais informações, consulte Cotas do AWS CloudFormation no Guia do usuário do AWS CloudFormation .

Amazon EventBridge regula cotas

Sua AWS conta tem cotas de EventBridge regras da Amazon que você deve conhecer ao selecionar os manuais a serem implantados com a solução. Cada manual criará uma EventBridge regra para cada controle que possa ser corrigido. Ao implantar vários manuais, é possível atingir a cota de

Regras. Para obter mais informações, consulte as EventBridge cotas da Amazon no Guia do EventBridge usuário da Amazon.

AWSImplantação do Security Hub

AWSA implantação e a configuração do Security Hub são um pré-requisito para essa solução. Para obter mais informações sobre como configurar o AWS Security Hub, consulte Configurando o AWS Security Hub no Guia do Usuário do AWS Security Hub.

No mínimo, você deve ter um Security Hub ativo configurado em sua conta principal. Você pode implantar essa solução na mesma conta (e AWS região) da conta principal do Security Hub. Em cada conta primária e secundária do Security Hub, você também deve implantar o modelo de membro que permite AssumeRole que as AWS Step Functions da solução executem runbooks de remediação na conta.

Empilhamento versus implantação StackSets

Um conjunto de pilhas permite criar pilhas em AWS contas em todas AWS as regiões usando um único AWS CloudFormation modelo. A partir da versão 1.4, essa solução oferece suporte à implantação de conjuntos de pilhas dividindo os recursos com base em onde e como eles são implantados. Clientes com várias contas, especialmente aqueles que usam AWS Organizations, podem se beneficiar do uso de conjuntos de pilhas para implantação em várias contas. Isso reduz o esforço necessário para instalar e manter a solução. Para obter mais informações sobre StackSets, consulte Usando AWS CloudFormation StackSets.

Implante a solução

> **Important**
>
> Se o recurso de descobertas de controle consolidado estiver ativado no Security Hub (isso é padrão em novas implantações), habilite somente o manual do Controle de Segurança (CS) ao implantar essa solução. Se o recurso não estiver ativado, habilite somente os playbooks para os padrões de segurança habilitados no Security Hub. Habilitar manuais adicionais pode resultar no alcance da cota de Regras EventBridge .

Essa solução usa modelos e pilhas do AWS CloudFormation para automatizar sua implantação. Os CloudFormation modelos especificam os AWS recursos incluídos nessa solução e suas propriedades. A CloudFormation pilha provisiona os recursos descritos nos modelos.

Para que a solução funcione, três modelos devem ser implantados. Primeiro, decida onde implantar os modelos e, em seguida, decida como implantá-los.

Essa visão geral descreverá os modelos e como decidir onde e como implantá-los. As próximas seções terão instruções mais detalhadas para implantar cada pilha como uma pilha ou. StackSet

Decidindo onde implantar cada pilha

Os três modelos serão chamados pelos seguintes nomes e conterão os seguintes recursos:

- Pilha de administração: função de etapa do orquestrador, regras de eventos e ação personalizada do Security Hub.
- Pilha de membros: documentos de SSM automação de remediação.
- Pilha de funções dos membros: IAM funções para remediações.

A pilha de administração deve ser implantada uma vez, em uma única conta e em uma única região. Ele deve ser implantado na conta e na região que você configurou como destino de agregação das descobertas do Security Hub para sua organização.

A solução opera com base nas descobertas do Security Hub, portanto, não poderá operar nas descobertas de uma conta e região específicas se essa conta ou região não tiver sido configurada para agregar descobertas na conta e região do administrador do Security Hub.

Por exemplo, uma organização tem contas operando em regiões `us-east-1` e`us-west-2`, com a conta `111111111111` como administrador delegado do Security Hub, na regiã`us-east-1`. Contas `222222222222` e `333333333333` devem ser contas de membros do Security Hub para a conta `111111111111` de administrador delegado. Todas as três contas devem ser configuradas para agregar descobertas `us-west-2` de a. `us-east-1` A pilha de administração deve ser implantada na conta`111111111111`. `us-east-1`

Para obter mais detalhes sobre como encontrar a agregação, consulte a documentação das contas de administrador delegado do Security Hub e da agregação entre regiões.

A pilha de administradores deve concluir a implantação antes de implantar as pilhas de membros para que uma relação de confiança possa ser criada das contas dos membros para a conta do hub.

A pilha de membros deve ser implantada em todas as contas e regiões nas quais você deseja corrigir as descobertas. Isso pode incluir a conta de administrador delegado do Security Hub na qual você implantou anteriormente o ASR Admin Stack. Os documentos de automação devem ser executados nas contas dos membros para usar o nível gratuito de automação. SSM

Usando o exemplo anterior, se você quiser corrigir as descobertas de todas as contas e regiões, a pilha de membros deve ser implantada nas três contas (`111111111111222222222222`, e`333333333333`) e nas duas regiões (`us-east-1`e). `us-west-2`

A pilha de funções dos membros deve ser implantada em todas as contas, mas contém recursos globais (IAMfunções) que só podem ser implantados uma vez por conta. Não importa em qual região você implanta a pilha de funções de membro, então, para simplificar, sugerimos implantá-la na mesma região em que a pilha de administradores está implantada.

Usando o exemplo anterior, sugerimos implantar a pilha de funções de membro em todas as três contas (`111111111111`,`222222222222`, e`333333333333`) em. `us-east-1`

Decidindo como implantar cada pilha

As opções para implantar uma pilha são

- CloudFormation StackSet (permissões autogerenciadas)
- CloudFormation StackSet (permissões gerenciadas pelo serviço)
- CloudFormation Pilha

StackSets com permissões gerenciadas por serviços são as mais convenientes porque não exigem a implantação de suas próprias funções e podem ser implantadas automaticamente em novas contas na organização. Infelizmente, esse método não é compatível com pilhas aninhadas, que usamos tanto na pilha Admin quanto na pilha de membros. A única pilha que pode ser implantada dessa forma é a pilha de funções dos membros.

Lembre-se de que, ao implantar em toda a organização, a conta de gerenciamento da organização não é incluída. Portanto, se você quiser corrigir as descobertas na conta de gerenciamento da organização, deverá implantar nessa conta separadamente.

A pilha de membros deve ser implantada em todas as contas e regiões, mas não pode ser implantada usando StackSets permissões gerenciadas por serviços porque contém pilhas aninhadas. Por isso, sugerimos implantar essa pilha StackSets com permissões autogerenciadas.

A pilha Admin é implantada apenas uma vez, portanto, pode ser implantada como uma CloudFormation pilha simples ou StackSet com permissões autogerenciadas em uma única conta e região.

Descobertas de controle consolidadas

As contas em sua organização podem ser configuradas com o recurso consolidado de descobertas de controle do Security Hub ativado ou desativado. Consulte os resultados do controle consolidado no Guia do Usuário do AWS Security Hub.

> **Important**
>
> Se ativado, você deve usar a versão 2.0.0 da solução ou posterior. Além disso, você deve implantar as pilhas aninhadas de administrador e membro para os padrões “SC” ou “controle de segurança”. Isso implanta os documentos e EventBridge regras de automação para uso com o controle consolidado IDs gerado quando esse recurso é ativado. Não há necessidade de implantar as pilhas aninhadas de administrador ou membro para padrões específicos (por exemplo AWSFSBP) ao usar esse recurso.

AWS CloudFormation modelos

View template

aws-sharr-deploy.template - Use esse modelo para iniciar a AWS solução Automated Security Response

on. O modelo instala os principais componentes da solução, uma pilha aninhada para os AWS Step Functions registros e uma pilha aninhada para cada padrão de segurança que você escolher ativar.

Os serviços usados incluem Amazon Simple Notification Service AWS Key Management Service, AWS Identity and Access Management, AWS Lambda, AWS Step Functions,, Amazon CloudWatch Logs, Amazon S3 e AWS Systems Manager.

Suporte à conta de administrador

Os modelos a seguir são instalados na conta de administrador do AWS Security Hub para ativar os padrões de segurança aos quais você deseja oferecer suporte. Você pode escolher qual dos seguintes modelos instalar ao instalar `aws-sharr-deploy.template` o.

aws-sharr-orchestrator-log.template - Cria um grupo de CloudWatch registros para a função de etapa do orquestrador.

AFSBPStack.template - Regras AWS básicas de melhores práticas de segurança v1.0.0.

CIS120Stack.template — Benchmarks do CIS Amazon Web Services Foundations, regras v1.2.0.

CIS140Stack.template — Benchmarks do CIS Amazon Web Services Foundations, regras da v1.4.0.

PCI321Stack.template - PCI - regras da DSS v3.2.1.

NISTStack.template - Instituto Nacional de Padrões e Tecnologia (NIST), regras da v5.0.0.

SCStack.template - regras do SC v2.0.0.

Contas-membros

View template

aws-sharr-member.template - Use esse modelo depois de configurar a solução principal para instalar os runbooks e permissões de automação do AWS Systems Manager em cada uma das suas contas de membro do AWS Security Hub (incluindo a conta de administrador). Esse modelo permite que você escolha quais playbooks padrão de segurança instalar.

Ele `aws-sharr-member.template` instala os seguintes modelos com base em suas seleções:

aws-sharr-remediations.template - Código de remediação comum usado por um ou mais dos padrões de segurança.

AFSBPMemberStack.template - Configurações, permissões e AWS runbooks de remediação de Práticas Recomendadas de Segurança Fundamental v1.0.0.

CIS120 MemberStack .template - benchmarks do CIS Amazon Web Services Foundations, configurações, permissões e runbooks de remediação da versão 1.2.0.

CIS140 MemberStack .template - benchmarks do CIS Amazon Web Services Foundations, configurações, permissões e runbooks de remediação da versão 1.4.0.

PCI321MemberStack.template - PCI - configurações, permissões e runbooks de remediação da DSS v3.2.1.

NISTMemberStack.template - National Institute of Standards and Technology (NIST), configurações, permissões e runbooks de remediação da v5.0.0.

SCMemberStack.template - Configurações de controle de segurança, permissões e runbooks de remediação.

Funções dos membros

aws-sharr-member-roles.template - Define as funções de remediação necessárias em cada conta de AWS Security Hub membro.

Integração do sistema de tickets

Use um dos modelos a seguir para integrar-se ao seu sistema de emissão de bilhetes.

JiraBlu

- Implante se você usa o Jira como seu sistema de tíquetes.

Service

- Implante se você usar ServiceNow como seu sistema de emissão de bilhetes.

Se quiser integrar um sistema de tíquetes externo diferente, você pode usar qualquer uma dessas pilhas como modelo para entender como implementar sua própria integração personalizada.

Implantação automatizada - StackSets

> **Note**
>
> Recomendamos implantar com StackSets. No entanto, para implantações em uma única conta ou para fins de teste ou avaliação, considere a opção de implantação de pilhas.

Antes de iniciar a solução, analise a arquitetura, os componentes da solução, a segurança e as considerações de design discutidas neste guia. Siga as step-by-step instruções nesta seção para configurar e implantar a solução em seu AWS Organizations.

Tempo de implantação: aproximadamente 30 minutos por conta, dependendo StackSet dos parâmetros.

Pré-requisitos

AWSO Organizations ajuda você a gerenciar e governar centralmente seu AWS ambiente e seus recursos de várias contas. StackSets funcionam melhor com AWS Organizations.

Se você já implantou a versão 1.3.x ou anterior dessa solução, deverá desinstalar a solução existente. Para obter mais informações, consulte Atualizar a solução.

Antes de implantar essa solução, revise sua implantação do AWS Security Hub:

- Deve haver uma conta de administrador delegada do Security Hub em sua AWS organização.
- O Security Hub deve ser configurado para agregar descobertas em todas as regiões. Para obter mais informações, consulte Agregando descobertas entre regiões no Guia do Usuário do AWS Security Hub.
- Você deve ativar o Security Hub para sua organização em cada região em que você AWS usa.

Esse procedimento pressupõe que você tenha várias contas usando AWS Organizations e tenha delegado uma conta de administrador e uma conta de AWS Organizations administrador do AWS Security Hub.

Visão geral da implantação

> **Note**
>
> StackSets a implantação dessa solução usa uma combinação de serviços gerenciados e autogerenciados. StackSets O autogerenciado StackSets deve ser usado atualmente, pois eles usam aninhados StackSets, que ainda não são compatíveis com o gerenciamento de serviços. StackSets

Implante o a StackSets partir de uma conta de administrador delegado em seu AWS Organizations.

Planejamento

Use o formulário a seguir para ajudar na StackSets implantação. Prepare seus dados e, em seguida, copie e cole os valores durante a implantação.

```
AWS Organizations admin account ID: _________________
Security Hub admin account ID: _________________
CloudTrail Logs Group: ____________________________
Member account IDs (comma-separated list):
____________________,
____________________,
____________________,
____________________,
____________________
AWS Organizations OUs (comma-separated list):
____________________,
____________________,
____________________,
____________________,
____________________
```

(Opcional) Etapa 0: implantar a pilha de integração de tíquetes

- Se você pretende usar o recurso de emissão de tíquetes, primeiro implante a pilha de integração de tíquetes em sua conta de administrador do Security Hub.
- Copie o nome da função Lambda dessa pilha e forneça-o como entrada para a pilha de administração (consulte a Etapa 1).

Etapa 1: iniciar a pilha de administração na conta de administrador delegada do Security Hub

- Usando um modelo autogerenciado StackSet, inicie o `aws-sharr-deploy.template` AWS CloudFormation modelo em sua conta de administrador do AWS Security Hub na mesma região do administrador do Security Hub. Esse modelo usa pilhas aninhadas.
- Escolha quais padrões de segurança instalar. Por padrão, somente SC é selecionado (recomendado).
- Escolha um grupo de registros existente do Orchestrator para usar. Selecione `Yes` se `SO0111-SHARR- Orchestrator` já existe em uma instalação anterior.

Para obter mais informações sobre autogerenciamento StackSets, consulte Conceder permissões autogerenciadas no Guia do AWS CloudFormation usuário.

Etapa 2: instalar as funções de remediação na conta de cada AWS Security Hub membro

Aguarde até que a Etapa 1 conclua a implantação, pois o modelo na Etapa 2 faz referência às IAM funções criadas pela Etapa 1.

- Usando um serviço gerenciado StackSet, lance o `aws-sharr-member-roles.template` AWS CloudFormation modelo em uma única região em cada conta do seu. AWS Organizations
- Escolha instalar esse modelo automaticamente quando uma nova conta ingressar na organização.
- Insira o ID da sua conta de AWS Security Hub administrador.

Etapa 3: Inicie a pilha de membros em cada conta de membro e região do AWS Security Hub

- Usando o autogerenciamento StackSets, inicie o `aws-sharr-member.template` AWS CloudFormation modelo em todas as regiões em que você tem AWS recursos em todas as contas AWS da sua organização gerenciadas pelo mesmo administrador do Security Hub.

  > **Note**
  >
  > Até que o StackSets suporte gerenciado por serviços esteja aninhado, você deve executar essa etapa para todas as novas contas que ingressarem na organização.

- Escolha quais playbooks do Security Standard instalar.
- Forneça o nome de um grupo de CloudTrail registros (usado por algumas correções).
- Insira o ID da sua conta de AWS Security Hub administrador.

(Opcional) Etapa 0: iniciar uma pilha de integração do sistema de tickets

1. Se você pretende usar o recurso de emissão de tíquetes, inicie primeiro a respectiva pilha de integração.
2. Escolha as pilhas de integração fornecidas para o Jira ou ServiceNow use-as como um modelo para implementar sua própria integração personalizada.

   Para implantar a pilha do Jira:

   a. Insira um nome para sua pilha.

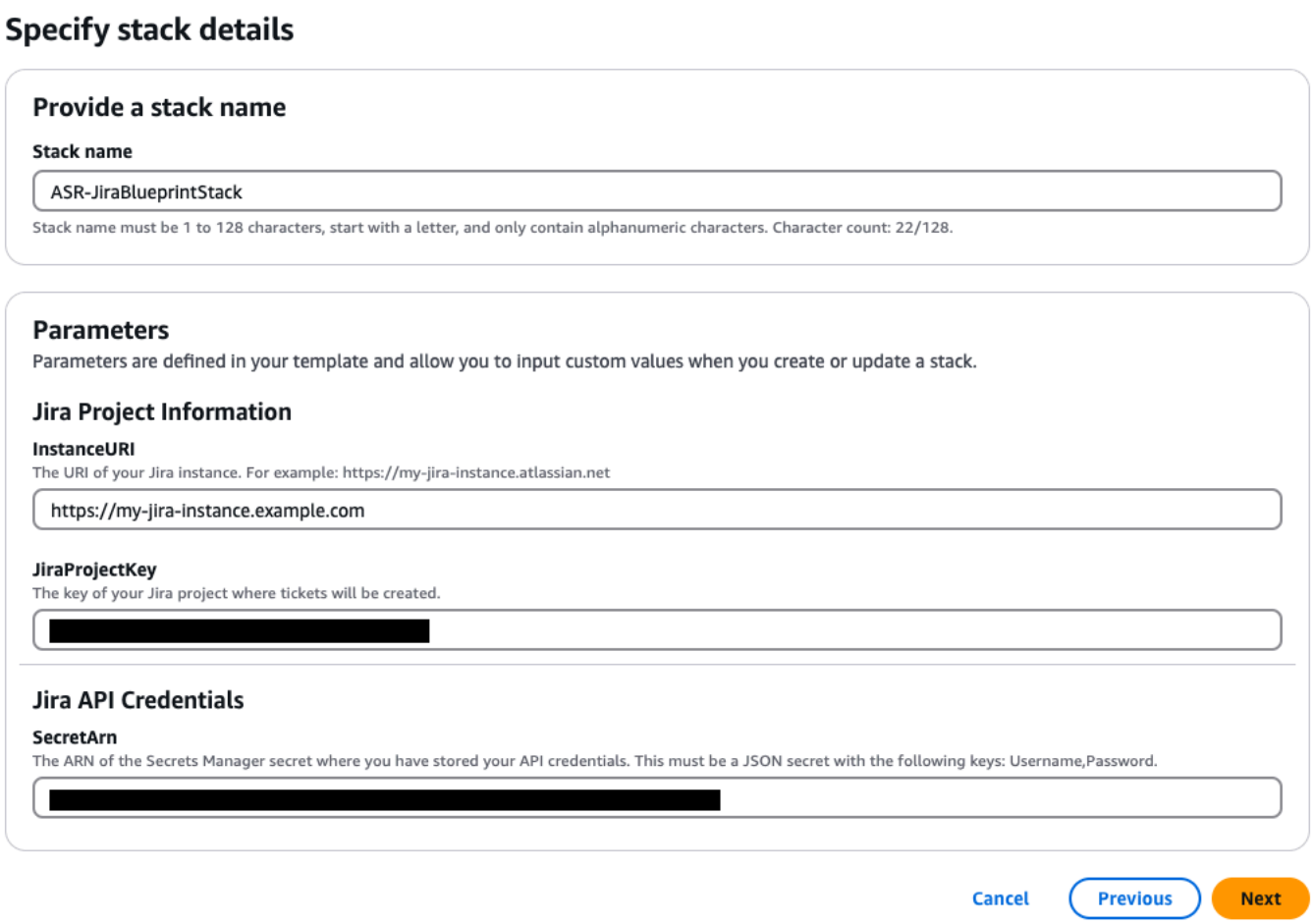
   b. Forneça o URI para sua instância do Jira.

   c. Forneça a chave do projeto do Jira para o qual você deseja enviar tickets.

   d. Crie um novo segredo de valor-chave no Secrets Manager que contenha seu Jira e. `Username` `Password`

   > **Note**
   >
   > Você pode optar por usar uma API chave do Jira no lugar da sua senha, fornecendo seu nome de usuário como `Username` e sua API chave como o. `Password`

   e. Adicione esse segredo como entrada na pilha. ARN



Para implantar a ServiceNow pilha:

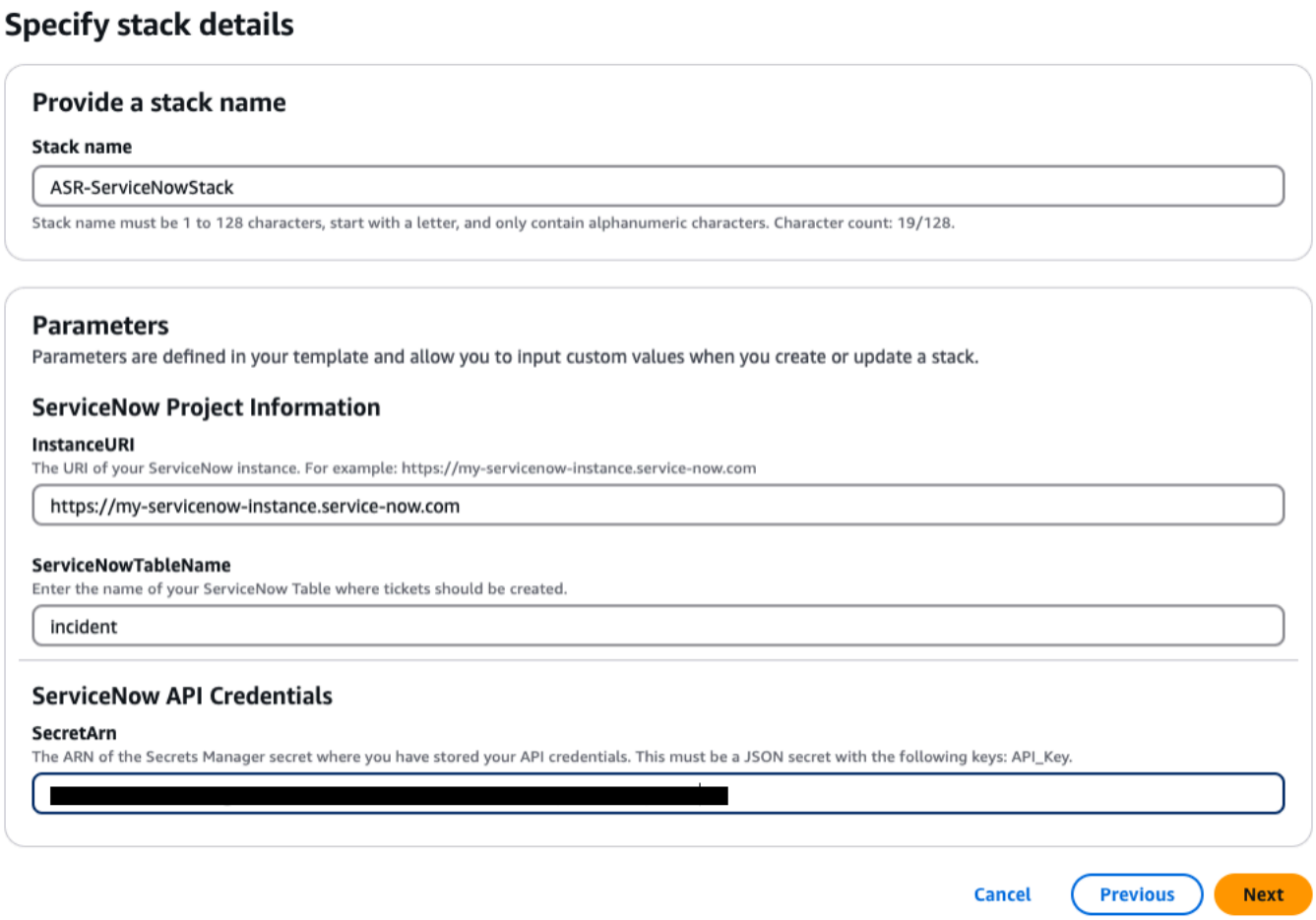
a. Insira um nome para sua pilha.

b. Forneça o URI da sua ServiceNow instância.

c. Forneça o nome ServiceNow da sua tabela.

d. Crie uma API chave ServiceNow com permissão para modificar a tabela na qual você pretende gravar.

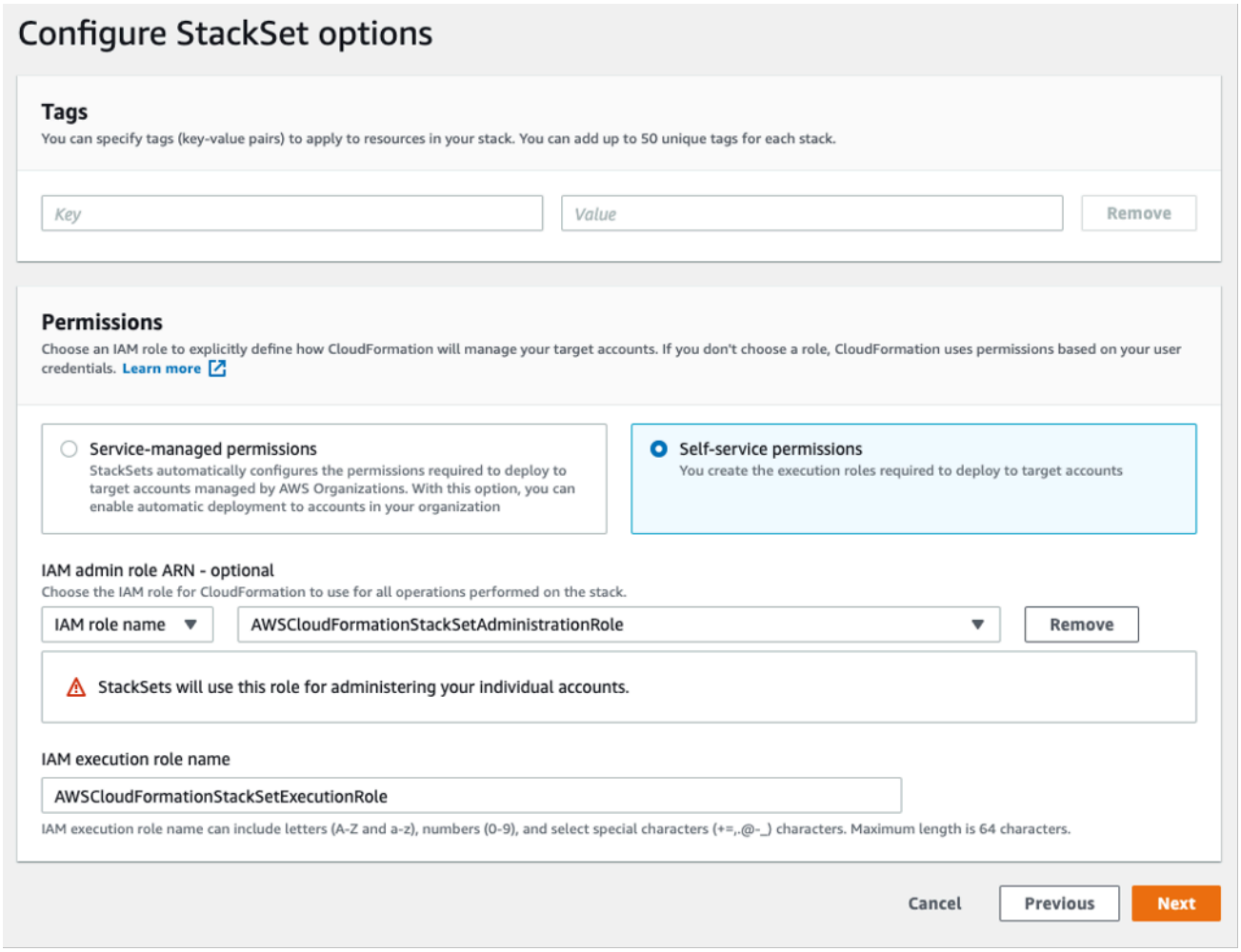
e. Crie um segredo no Secrets Manager com a chave `API_Key` e forneça o segredo ARN como entrada para a pilha.



Para criar uma pilha de integração personalizada: inclua uma função Lambda que o orquestrador de soluções Step Functions possa chamar para cada correção. A função Lambda deve receber a entrada fornecida pelo Step Functions, construir uma carga útil de acordo com os requisitos do seu sistema de emissão de tíquetes e fazer uma solicitação ao sistema para criar o ticket.

Etapa 1: iniciar a pilha de administração na conta de administrador delegada do Security Hub

1. Inicie a pilha de administração,`aws-sharr-deploy.template`, com sua conta de administrador do Security Hub. Normalmente, um por organização em uma única região. Como essa pilha usa pilhas aninhadas, você deve implantar esse modelo como autogerenciado. StackSet



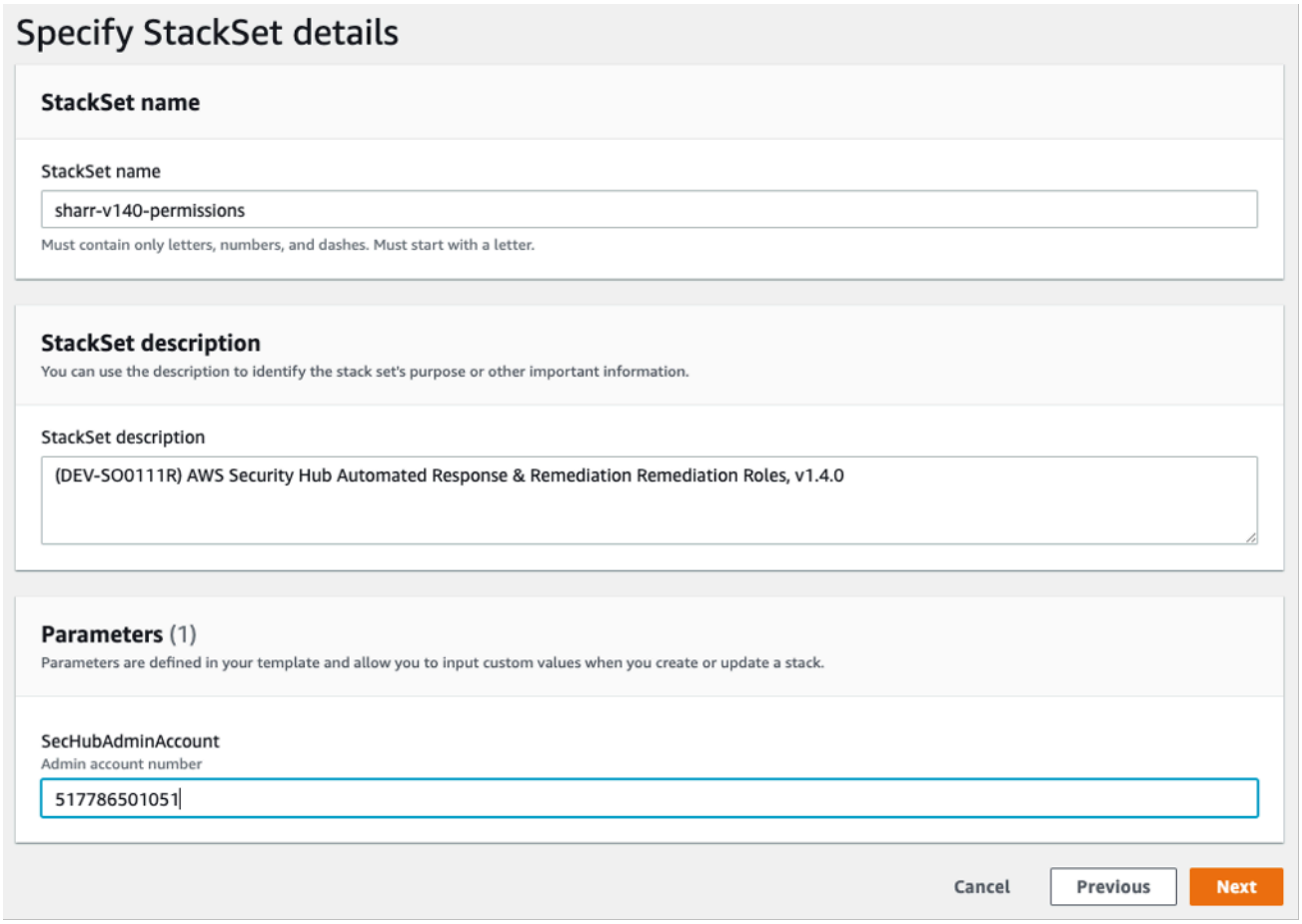
Configurar StackSet opções

2. Para o parâmetro Números da conta, insira o ID da conta de administrador do AWS Security Hub.
3. Para o parâmetro Especificar regiões, selecione somente a região em que o administrador do Security Hub está ativado. Aguarde a conclusão dessa etapa antes de prosseguir para a Etapa 2.

Etapa 2: instalar as funções de remediação em cada conta membro do AWS Security Hub

Use um serviço gerenciado StackSets para implantar o modelo de funções de membro,. `aws-sharr-member-roles.template` Isso StackSet deve ser implantado em uma região por conta de membro. Ele define as funções globais que permitem API chamadas entre contas a partir da função de etapa do SHARR Orchestrator.

1. Implante em toda a organização (típica) ou em unidades organizacionais, de acordo com as políticas de sua organização.
2. Ative a implantação automática para que novas contas nas AWS Organizations recebam essas permissões.
3. Para o parâmetro Especificar regiões, selecione uma única região. IAMas funções são globais. Você pode continuar na Etapa 3 enquanto isso é StackSet implantado.



Especifique StackSet detalhes

Etapa 3: Inicie a pilha de membros em cada conta de membro e região do AWS Security Hub

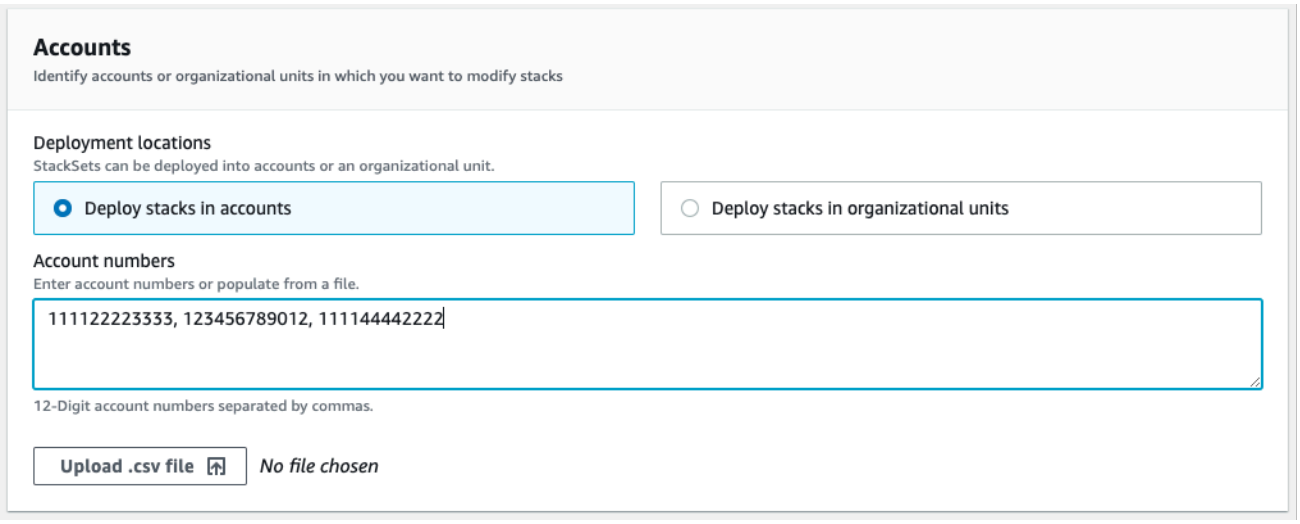
Como a pilha de membros usa pilhas aninhadas, você deve implantá-la como autogerenciada. StackSet Isso não oferece suporte à implantação automática em novas contas na AWS organização.

Parâmetros

LogGroup Configuração: escolha o grupo de registros que recebe CloudTrail os registros. Se não existir nenhum ou se o grupo de registros for diferente para cada conta, escolha um valor conveniente. Os administradores da conta devem atualizar o parâmetro Systems Manager — Parameter Store /Solutions/SO0111/Metrics _ LogGroupName depois de criar um grupo de CloudWatch registros para CloudTrail registros. Isso é necessário para remediações que criam alarmes de métricas nas API chamadas.

Padrões: escolha os padrões a serem carregados na conta do membro. Isso só instala os runbooks do AWS Systems Manager — não ativa o Padrão de Segurança.

SecHubAdminAccount: insira o ID da conta de administrador do AWS Security Hub na qual você instalou o modelo de administração da solução.



Contas

Locais de implantação: você pode especificar uma lista de números de contas ou unidades organizacionais.

Especifique regiões: selecione todas as regiões nas quais você deseja corrigir as descobertas. Você pode ajustar as opções de implantação conforme apropriado para o número de contas e regiões. A simultaneidade de regiões pode ser paralela.

Implantação automatizada - Stacks

> **Note**
>
> Para clientes com várias contas, é altamente recomendável implantar com StackSets.

Antes de iniciar a solução, analise a arquitetura, os componentes da solução, a segurança e as considerações de design discutidas neste guia. Siga as step-by-step instruções nesta seção para configurar e implantar a solução em sua conta.

Tempo de implantação: aproximadamente 30 minutos

Pré-requisitos

Antes de implantar essa solução, verifique se ela AWS Security Hub está na mesma AWS região das suas contas primária e secundária. Se você já implantou essa solução, deverá desinstalar a solução existente. Para obter mais informações, consulte Atualizar a solução.

Visão geral da implantação

Use as etapas a seguir para implantar essa solução emAWS.

(Opcional) Etapa 0: iniciar uma pilha de integração do sistema de tickets

- Se você pretende usar o recurso de emissão de tíquetes, primeiro implante a pilha de integração de tíquetes em sua conta de administrador do Security Hub.
- Copie o nome da função Lambda dessa pilha e forneça-o como entrada para a pilha de administração (consulte a Etapa 1).

Etapa 1: iniciar a pilha de administração

- Inicie o `aws-sharr-deploy.template` AWS CloudFormation modelo em sua conta de AWS Security Hub administrador.
- Escolha quais padrões de segurança instalar.
- Escolha um grupo de registros existente do Orchestrator para usar (selecione `Yes` se `SO0111-SHARR-Orchestrator` já existe em uma instalação anterior).

Etapa 2: instalar as funções de remediação na conta de cada AWS Security Hub membro

- Inicie o `aws-sharr-member-roles.template` AWS CloudFormation modelo em uma região por conta de membro.
- Insira o IG da conta de 12 dígitos para a conta de AWS Security Hub administrador.

Etapa 3: iniciar a pilha de membros

- Especifique o nome do grupo de CloudWatch registros a ser usado com as correções CIS 3.1-3.14. Ele deve ser o nome de um grupo de CloudWatch registros de registros que recebe CloudTrail registros.
- Escolha se deseja instalar as funções de remediação. Instale essas funções somente uma vez por conta.
- Selecione quais playbooks instalar.
- Insira o ID da conta de AWS Security Hub administrador.

Etapa 4: (opcional) ajustar as remediações disponíveis

- Remova todas as correções por conta de membro. Esta etapa é opcional.

(Opcional) Etapa 0: iniciar uma pilha de integração do sistema de tickets

1. Se você pretende usar o recurso de emissão de tíquetes, inicie primeiro a respectiva pilha de integração.
2. Escolha as pilhas de integração fornecidas para o Jira ou ServiceNow use-as como um modelo para implementar sua própria integração personalizada.

   Para implantar a pilha do Jira:

   a. Insira um nome para sua pilha.

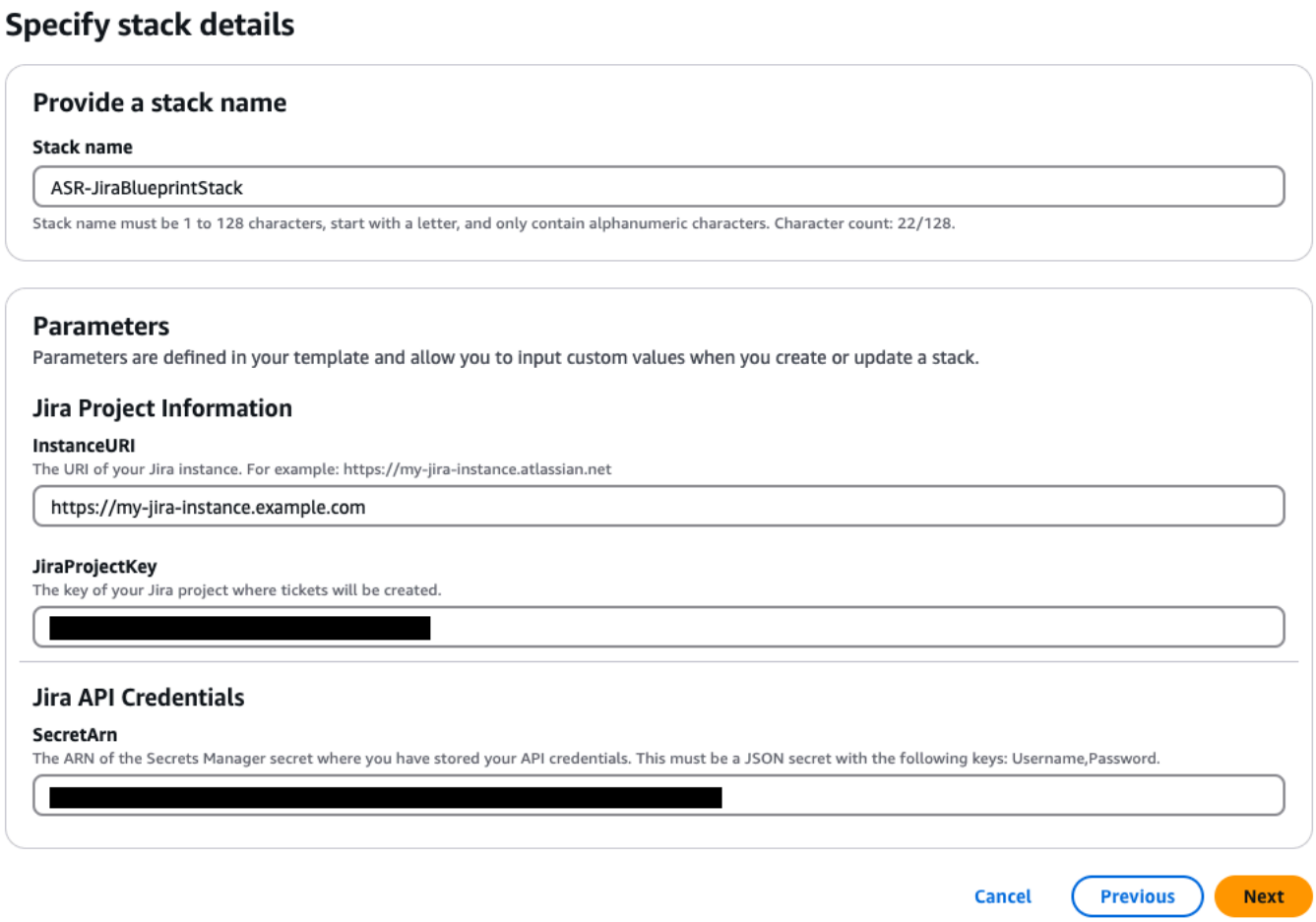
   b. Forneça o URI para sua instância do Jira.

   c. Forneça a chave do projeto do Jira para o qual você deseja enviar tickets.

   d. Crie um novo segredo de valor-chave no Secrets Manager que contenha seu Jira e. `Username` `Password`

> **Note**
>
> Você pode optar por usar uma API chave do Jira no lugar da sua senha, fornecendo seu nome de usuário como `Username` e sua API chave como o. `Password`

e. Adicione esse segredo como entrada na pilha. ARN



Para implantar a ServiceNow pilha:

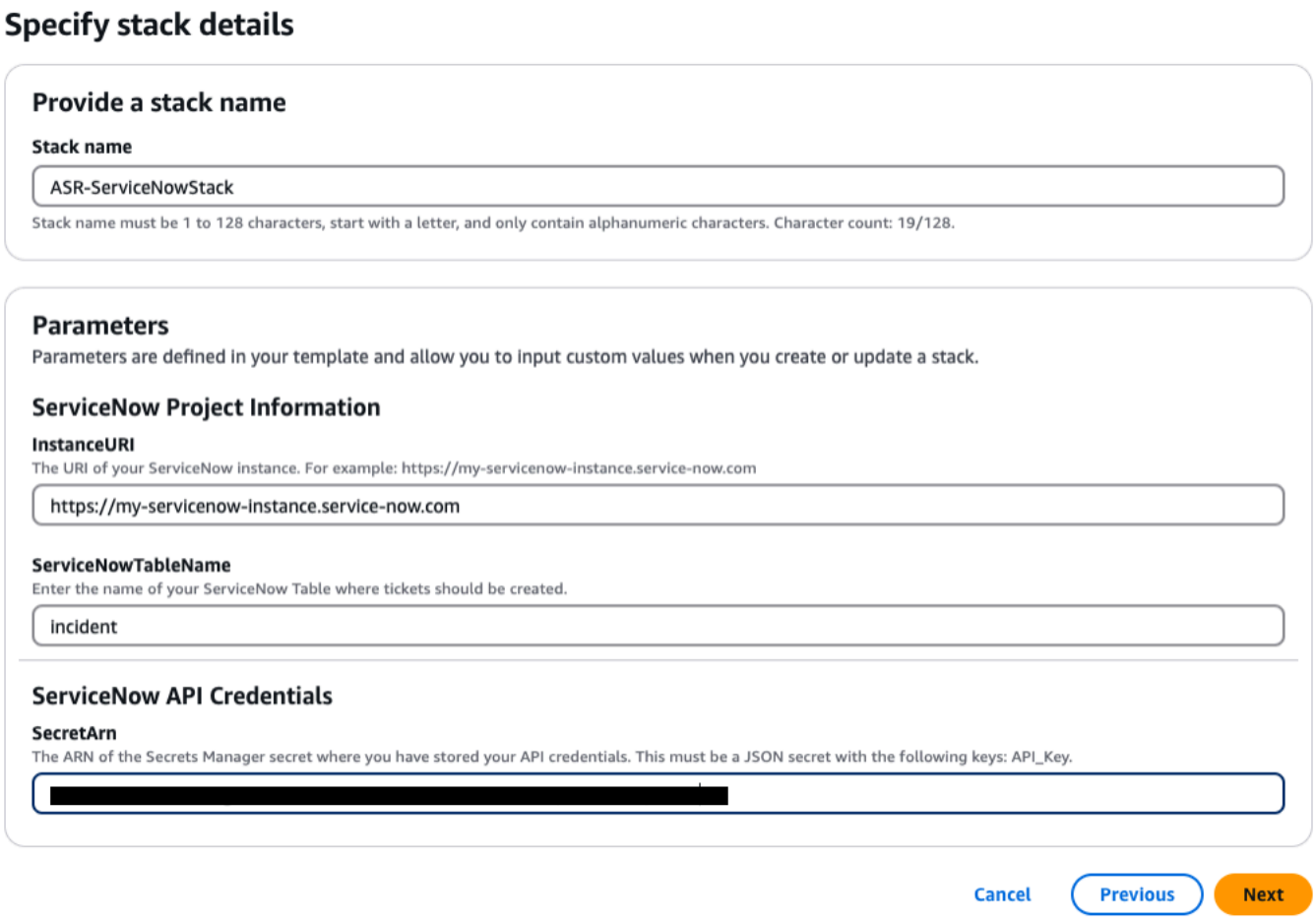
a. Insira um nome para sua pilha.

b. Forneça o URI da sua ServiceNow instância.

c. Forneça o nome ServiceNow da sua tabela.

d. Crie uma API chave ServiceNow com permissão para modificar a tabela na qual você pretende gravar.

e. Crie um segredo no Secrets Manager com a chave `API_Key` e forneça o segredo ARN como entrada para a pilha.



Para criar uma pilha de integração personalizada: inclua uma função Lambda que o orquestrador de soluções Step Functions possa chamar para cada correção. A função Lambda deve receber a entrada fornecida pelo Step Functions, construir uma carga útil de acordo com os requisitos do seu sistema de emissão de tíquetes e fazer uma solicitação ao sistema para criar o ticket.

Etapa 1: iniciar a pilha de administração

Important

Essa solução inclui uma opção para enviar métricas operacionais anônimas para a AWS. Usamos esses dados para entender melhor como os clientes usam essa solução e os serviços e produtos relacionados. A AWS possui dados coletados por meio desta pesquisa. A coleta de dados está sujeita ao AWS Aviso de Privacidade.

Para desativar esse recurso, baixe o modelo, modifique a seção de mapeamento do AWS CloudFormation e use o console do AWS CloudFormation para carregar seu modelo

atualizado e implantar a solução. Para obter mais informações, consulte a seção Coleta de dados anônimos deste guia.

Esse AWS CloudFormation modelo automatizado implanta a Resposta de Segurança Automatizada na AWS solução na AWS nuvem. Antes de iniciar a pilha, você deve habilitar o Security Hub e preencher os pré-requisitos.

> **Note**
>
> Você é responsável pelo custo dos serviços da AWS usados durante a execução dessa solução. Para obter mais detalhes, visite a seção Custo neste guia e consulte a página de preços de cada AWS serviço usado nesta solução.

1. Faça login na AWS Management Console conta em que o AWS Security Hub está configurado atualmente e use o botão abaixo para iniciar o `aws-sharr-deploy.template` AWS CloudFormation modelo.

   Launch solution

   Também é possível fazer download do modelo para usá-lo como ponto de partida para a sua própria implantação.

2. Por padrão, esse modelo é iniciado na região Leste dos EUA (Norte da Virgínia). Para iniciar essa solução em uma AWS região diferente, use o seletor de região na barra de AWS Management Console navegação.

   > **Note**
   >
   > Essa solução usa AWS Systems Manager o que está atualmente disponível somente em AWS regiões específicas. A solução funciona em todas as regiões que oferecem suporte a esse serviço. Para obter a disponibilidade mais atual por região, consulte a Lista de serviços regionais da AWS.

3. Na página Criar pilha, verifique se o modelo correto URL está na caixa de texto Amazon URL S3 e escolha Avançar.

4. Na página Especificar detalhes da pilha, insira um nome para a pilha. Para obter informações sobre limitações de nomes de caracteres, consulte IAMe STS limites no Guia do AWS Identity and Access Management usuário.
5. Na página Parâmetros, escolha Avançar.

Parameter	Padrão	Descrição
Carregar SC Admin Stack	`yes`	Especifique se deseja instalar os component es administrativos para remediação automatizada dos controles SC.
Carregar pilha de AFSBP administração	no	Especifique se deseja instalar os component es administrativos para remediação automatizada dos FSBP controles.
Carregar CIS12 0 pilha de administração	no	Especifique se deseja instalar os component es administrativos para remediação automática de CIS12 0 controles.
Carregar CIS14 0 pilha de administração	no	Especifique se deseja instalar os component es administrativos para remediação automática de CIS14 0 controles.
Carregar CIS3 00 Admin Stack	no	Especifique se deseja instalar os component es administrativos para remediação automática dos controles CIS3 00.

Parameter	Padrão	Descrição
Carregar pilha de PC1321 administração	no	Especifique se deseja instalar os component es administrativos para remediação automatizada dos PC1321 controles.
Carregar pilha de NIST administração	no	Especifique se deseja instalar os component es administrativos para remediação automatizada dos NIST controles.
Reutilizar o grupo de registros do Orchestrator	no	Selecione se deseja ou não reutilizar um grupo de `S00111-SHARR-Orche strator` CloudWatch registros existente. Isso simplifica a reinstalação e as atualizações sem perder os dados de log de uma versão anterior. Se você estiver atualizando da versão 1.2 ou superior, selecione. `yes`
Use CloudWatch métricas	`yes`	Especifique se deseja ativar CloudWatch as métricas para monitorar a solução. Isso criará um CloudWatc h painel para visualizar métricas.

Parameter	Padrão	Descrição
Use CloudWatch alarmes de métricas	`yes`	Especifique se deseja ativar os alarmes de CloudWatch métricas para a solução. Isso criará alarmes para determinadas métricas coletadas pela solução.
RemediationFailureAlarmThreshold	5	Especifique o limite para a porcentagem de falhas de remediação por ID de controle. Por exemplo, se você entrar5, receberá um alarme se um ID de controle falhar em mais de 5% das remediações em um determinado dia. Esse parâmetro funciona somente se os alarmes forem criados (consulte o parâmetro Use CloudWatch Metrics Alarms).
EnableEnhancedCloudWatchMetrics	no	Se`yes`, cria CloudWatch métricas adicionais para rastrear todos os controles IDs individualmente no CloudWatch painel e como CloudWatch alarmes. Consulte a seção Custo para entender o custo adicional que isso acarreta.

Parameter	Padrão	Descrição
TicketGenFunctionName	(Entrada opcional)	Opcional. Deixe em branco se você não quiser integrar um sistema de bilhetagem. Caso contrário, forneça o nome da função Lambda da saída da pilha da Etapa 0, por exemplo:. `SO0111-ASR-ServiceNow-TicketGenerator`

6. Na página Configurar opções de pilha, selecione Avançar.
7. Na página Revisar, verifique e confirme as configurações. Marque a caixa confirmando que o modelo criará AWS Identity and Access Management (IAM) recursos.
8. Selecione Create stack (Criar pilha) para implantar a pilha.

Você pode ver o status da pilha no AWS CloudFormation console na coluna Status. Você deve receber o COMPLETE status CREATE _ em aproximadamente 15 minutos.

Etapa 2: instalar as funções de remediação em cada conta membro do AWS Security Hub

O `aws-sharr-member-roles.template` StackSet deve ser implantado em apenas uma região por conta de membro. Ele define as funções globais que permitem API chamadas entre contas a partir da função de etapa do SHARR Orchestrator.

1. Faça login no AWS Management Console para cada conta de AWS Security Hub membro (incluindo a conta de administrador, que também é membro). Selecione o botão para iniciar o `aws-sharr-member-roles.template` AWS CloudFormation modelo. Também é possível fazer download do modelo para usá-lo como ponto de partida para a sua própria implantação.

   Launch solution

2. Por padrão, esse modelo é iniciado na região Leste dos EUA (Norte da Virgínia). Para iniciar essa solução em uma AWS região diferente, use o seletor de região na barra de navegação do AWS Management Console.

3. Na página Criar pilha, verifique se o modelo correto URL está na caixa de texto Amazon URL S3 e escolha Avançar.
4. Na página Especificar detalhes da pilha, insira um nome para a pilha. Para obter informações sobre limitações de nomes de caracteres, consulte IAM e STS limites no Guia do Usuário do AWS Identity and Access Management.
5. Na página Parâmetros, especifique os parâmetros a seguir e escolha Avançar.

Parameter	Padrão	Descrição
Namespace	*<Requires input>*	Insira uma sequência de até 9 caracteres alfanumér icos minúsculos. Essa string se torna parte dos nomes das IAM funções. Use o mesmo valor para implantaç ão de pilha de membros e implantação de pilha de funções de membros.
Administrador da conta Sec Hub	*<Requires input>*	Insira o ID da conta de 12 dígitos para a conta de AWS Security Hub administr ador. Esse valor concede permissões para a função de solução da conta de administrador.

6. Na página Configurar opções de pilha, selecione Avançar.
7. Na página Revisar, verifique e confirme as configurações. Marque a caixa confirmando que o modelo criará AWS Identity and Access Management (IAM) recursos.
8. Selecione Create stack (Criar pilha) para implantar a pilha.

   Você pode ver o status da pilha no AWS CloudFormation console na coluna Status. Você deve receber o COMPLETE status CREATE _ em aproximadamente 5 minutos. Você pode continuar com a próxima etapa enquanto essa pilha é carregada.

Etapa 3: iniciar a pilha de membros

> **Important**
>
> Essa solução inclui uma opção para enviar métricas operacionais anônimas para a AWS. Usamos esses dados para entender melhor como os clientes usam essa solução e os serviços e produtos relacionados. A AWS possui dados coletados por meio desta pesquisa. A coleta de dados está sujeita à AWS Política de Privacidade.
> Para desativar esse recurso, baixe o modelo, modifique a seção de mapeamento do AWS CloudFormation e use o console do AWS CloudFormation para carregar seu modelo atualizado e implantar a solução. Para obter mais informações, consulte a seção Coleção de métricas operacionais deste guia.

A `aws-sharr-member` pilha deve ser instalada em cada conta de membro do Security Hub. Essa pilha define os runbooks para remediação automatizada. O administrador da conta de cada membro pode controlar quais remediações estão disponíveis por meio dessa pilha.

1. Faça login na conta AWS Management Console de cada AWS Security Hub membro (incluindo a conta de administrador, que também é membro). Selecione o botão para iniciar o `aws-sharr-member.template` AWS CloudFormation modelo.

   Launch solution

   Também é possível fazer download do modelo para usá-lo como ponto de partida para a sua própria implantação.
2. Por padrão, esse modelo é iniciado na região Leste dos EUA (Norte da Virgínia). Para iniciar essa solução em uma AWS região diferente, use o seletor de região na barra de AWS Management Console navegação.

   > **Note**
   >
   > Essa solução usa AWS Systems Manager, que atualmente está disponível na maioria das AWS regiões. A solução funciona em todas as regiões que oferecem suporte a esses serviços. Para obter a disponibilidade mais atual por região, consulte a Lista de serviços regionais da AWS.

3. Na página Criar pilha, verifique se o modelo correto URL está na caixa de texto Amazon URL S3 e escolha Avançar.
4. Na página Especificar detalhes da pilha, insira um nome para a pilha. Para obter informações sobre limitações de nomes de caracteres, consulte IAMe STS limites no Guia do AWS Identity and Access Management usuário.
5. Na página Parâmetros, especifique os parâmetros a seguir e escolha Avançar.

Parameter	Padrão	Descrição
Forneça o nome do LogGroup a ser usado para criar filtros métricos e alarmes	*<Requires input>*	Especifique o nome de um grupo de CloudWatch registros em que CloudTrail registra API chamadas. Isso é usado para remediações CIS 3.1-3.14.
Carregar pilha de membros SC	`yes`	Especifique se deseja instalar os componentes do membro para remediação automatizada dos controles SC.
Carregar pilha de AFSBP membros	no	Especifique se deseja instalar os componentes do membro para remediaçã o automatizada dos FSBP controles.
Carregar pilha de CIS12 0 membros	no	Especifique se deseja instalar os componentes do membro para remediação automatizada de CIS12 0 controles.
Carregar pilha de CIS14 0 membros	no	Especifique se deseja instalar os componentes do membro para remediação

Parameter	Padrão	Descrição
		automatizada de CIS14 0 controles.
Carregar pilha de CIS3 100 membros	no	Especifique se deseja instalar os componentes do membro para remediação automatizada dos controles CIS3 00.
Carregar pilha de PC1321 membros	no	Especifique se deseja instalar os componentes do membro para remediação automatizada dos PC1321 controles.
Carregar pilha de NIST membros	no	Especifique se deseja instalar os componentes do membro para remediaçã o automatizada dos NIST controles.
Crie um bucket S3 para o registro de auditoria do Redshift	no	Selecione `yes` se o bucket do S3 deve ser criado para a remediação FSBP RedShift .4. Para obter detalhes sobre o bucket do S3 e a remediação, consulte a correção do Redshift.4 no Guia do usuário.AWS Security Hub
Conta de administrador do Sec Hub	*<Requires input>*	Insira o ID da conta de 12 dígitos para a conta de administrador do AWS Security Hub.

Parameter	Padrão	Descrição
Namespace	*<Requires input>*	Insira uma sequência de até 9 caracteres alfanuméricos minúsculos. Essa string se torna parte dos nomes das IAM funções e do bucket do Action Log S3. Use o mesmo valor para implantação de pilha de membros e implantação de pilha de funções de membros. Essa string deve seguir as regras de nomenclatura do Amazon S3 para buckets S3 de uso geral.
EnableCloudTrailForASRActionLog	no	Selecione `yes` se você deseja monitorar os eventos de gerenciamento conduzidos pela solução no CloudWatch painel. A solução cria uma CloudTrail trilha em cada conta de membro seleciona `dayes`. Consulte a seção Custo para entender o custo adicional que isso acarreta.

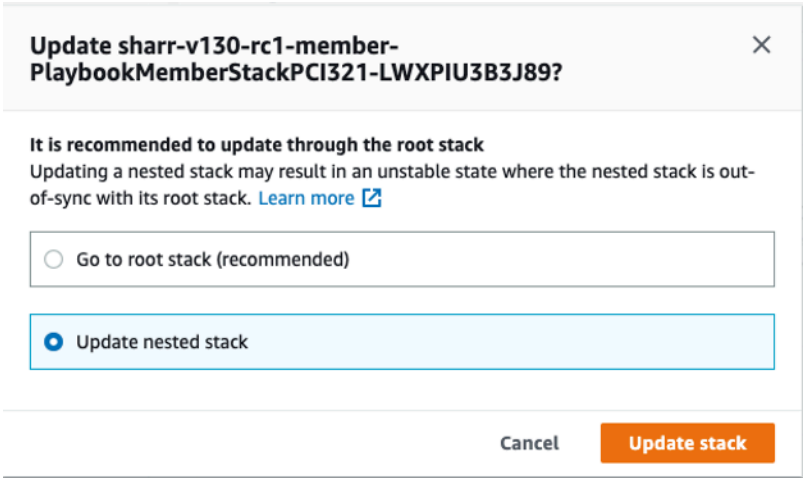
6. Na página Configurar opções de pilha, selecione Avançar.
7. Na página Revisar, verifique e confirme as configurações. Marque a caixa confirmando que o modelo criará AWS Identity and Access Management (IAM) recursos.
8. Selecione Create stack (Criar pilha) para implantar a pilha.

Você pode ver o status da pilha no AWS CloudFormation console na coluna Status. Você deve receber o COMPLETE status CREATE _ em aproximadamente 15 minutos.

Etapa 4: (opcional) ajustar as remediações disponíveis

Se quiser remover correções específicas da conta de um membro, você pode fazer isso atualizando a pilha aninhada de acordo com o padrão de segurança. Para simplificar, as opções de pilha aninhada não são propagadas para a pilha raiz.

1. Faça login no AWS CloudFormation console e selecione a pilha aninhada.
2. Selecione Atualizar.
3. Selecione Atualizar pilha aninhada e escolha Atualizar pilha.



Atualizar pilha aninhada

4. Selecione Usar modelo atual e escolha Avançar.
5. Ajuste as remediações disponíveis. Altere os valores dos controles desejados para `Available` e dos controles indesejados para`Not available`.

> **Note**
>
> Desativar uma remediação remove o runbook de remediação de soluções para o padrão e controle de segurança.

6. Na página Configurar opções de pilha, selecione Avançar.
7. Na página Revisar, verifique e confirme as configurações. Marque a caixa confirmando que o modelo criará AWS Identity and Access Management (IAM) recursos.
8. Escolha Atualizar pilha.

Você pode ver o status da pilha no AWS CloudFormation console na coluna Status. Você deve receber o COMPLETE status CREATE _ em aproximadamente 15 minutos.

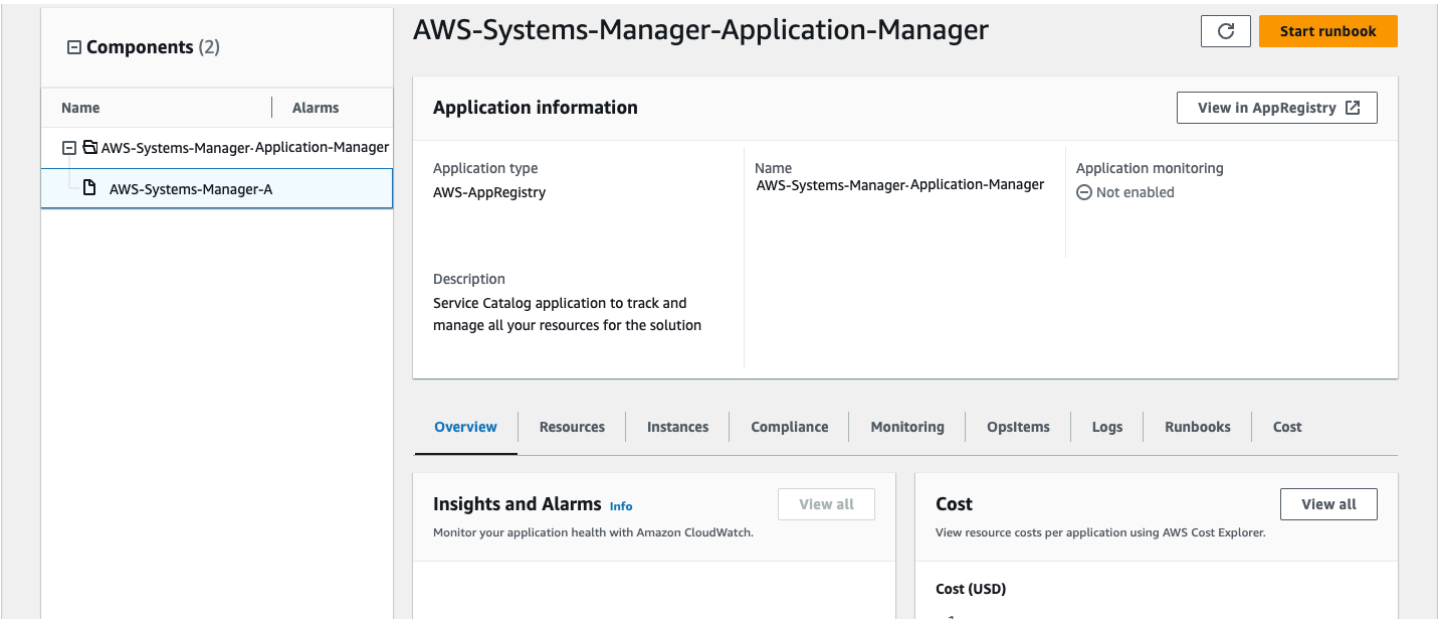
Monitore a solução com o Service Catalog AppRegistry

Essa solução inclui um AppRegistry recurso do Service Catalog para registrar o CloudFormation modelo e os recursos subjacentes como um aplicativo no Service Catalog AppRegistry e no AWS Systems Manager Application Manager.

AWS O Systems Manager Application Manager oferece uma visão em nível de aplicativo dessa solução e de seus recursos para que você possa:

- Monitore seus recursos, custos dos recursos implantados em pilhas e Contas da AWS registros associados a essa solução a partir de um local central.
- Visualize os dados operacionais dos recursos dessa solução (como status de implantação, CloudWatch alarmes, configurações de recursos e problemas operacionais) no contexto de um aplicativo.

  A figura a seguir mostra um exemplo da visualização do aplicativo para a pilha de soluções no Application Manager.



Pilha de soluções no Application Manager

Use o CloudWatch Application Insights

Essa solução se integra automaticamente ao CloudWatch Application Insights após a implantação. CloudWatch O Application Insights ajuda você a ver e entender a integridade e o desempenho da solução ao:

- Descobrindo e monitorando automaticamente os principais recursos do aplicativo.
- Criação de alarmes personalizados para identificar proativamente possíveis problemas.
- Geração automática do Systems Manager OpsItems quando anomalias ou falhas são detectadas. Eles OpsItems servem como notificações acionáveis que informam imediatamente sobre problemas que afetam a solução.

Siga estas etapas para visualizar o painel de monitoramento do CloudWatch Application Insights, onde você pode ver a integridade da solução e monitorar os principais componentes por meio de painéis e alarmes pré-configurados.

1. Navegue até o console do CloudWatch .
2. Escolha a guia Insights e selecione Application Insights.
3. Escolha a guia Aplicativos e selecione o aplicativo associado à solução.

Você também pode importar o CloudWatch painel da solução para consolidar seu monitoramento da integridade da solução. Enquanto estiver no painel de aplicativos da solução no CloudWatch Application Insights, siga estas etapas:

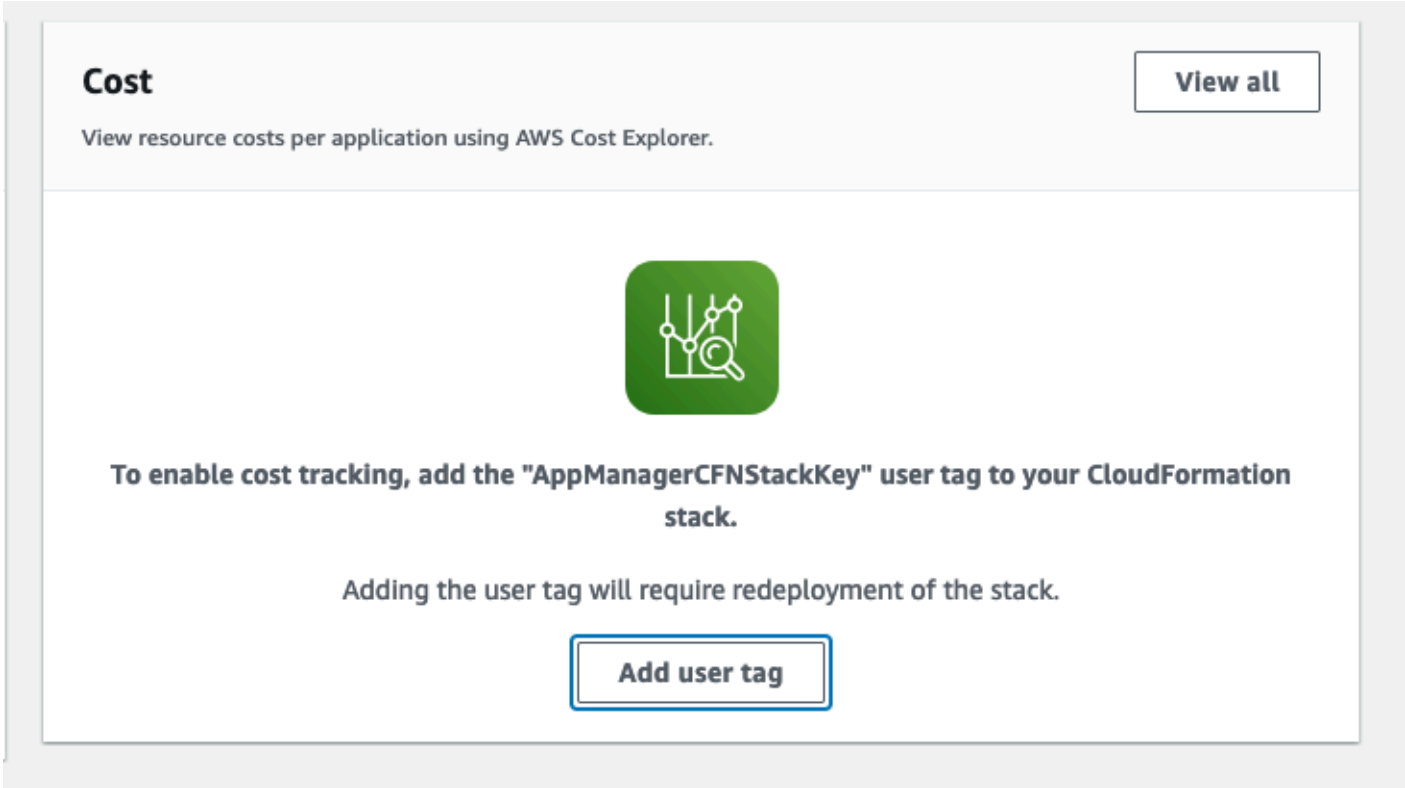
1. Escolha a guia CloudWatch Painel personalizado.
2. Escolha Importar CloudWatch painel.
3. Na caixa de pesquisa`ASR-Remediation-Metrics-Dashboard`, insira e selecione a Resposta de Segurança Automatizada no AWS painel.
4. Escolha Importar.

Agora você pode visualizar o painel do CloudWatch Application Insights e o painel personalizado da solução no console do CloudWatch Application Insights, sem precisar alternar entre as páginas.

Confirme as tags de custos associadas à solução

Depois de ativar as etiquetas de alocação de custos associadas à solução, você deve confirmar as etiquetas de alocação de custos para ver os custos dessa solução. Para confirmar as tags de alocação de custos:

1. Faça login no console do Systems Manager.
2. No painel de navegação, escolha Application Manager.
3. Em Aplicativos, escolha o nome do aplicativo para essa solução e selecione-o.
4. Na guia Visão geral, em Custo, selecione Adicionar tag de usuário.



5. Na página Adicionar tag de usuário, insira `confirm` e selecione Adicionar tag de usuário.

O processo de ativação pode levar até 24 horas para que os dados da tag apareçam.

Ative as tags de alocação de custos associadas à solução

Depois de confirmar as etiquetas de custo associadas a essa solução, você deve ativar as etiquetas de alocação de custos para ver os custos dessa solução. As tags de alocação de custos só podem ser ativadas pela conta de gerenciamento da organização.

Para ativar as tags de alocação de custos:

1. Faça login no console AWS Billing and Cost Management de gerenciamento de custos.
2. No painel de navegação, selecione Tags de alocação de custos.
3. Na página Tags de alocação de custos, filtre a `AppManagerCFNStackKey` tag e selecione a tag nos resultados mostrados.
4. Selecione Ativar.

AWS Cost Explorer

Você pode ver a visão geral dos custos associados ao aplicativo e aos componentes do aplicativo no console do Application Manager por meio da integração com o AWS Cost Explorer. O Cost Explorer ajuda você a gerenciar custos fornecendo uma visão dos custos e do uso dos recursos da AWS ao longo do tempo.

1. Faça login no Console de Gerenciamento de custos da AWS.
2. No menu de navegação, selecione Cost Explorer para visualizar os custos e o uso da solução ao longo do tempo.

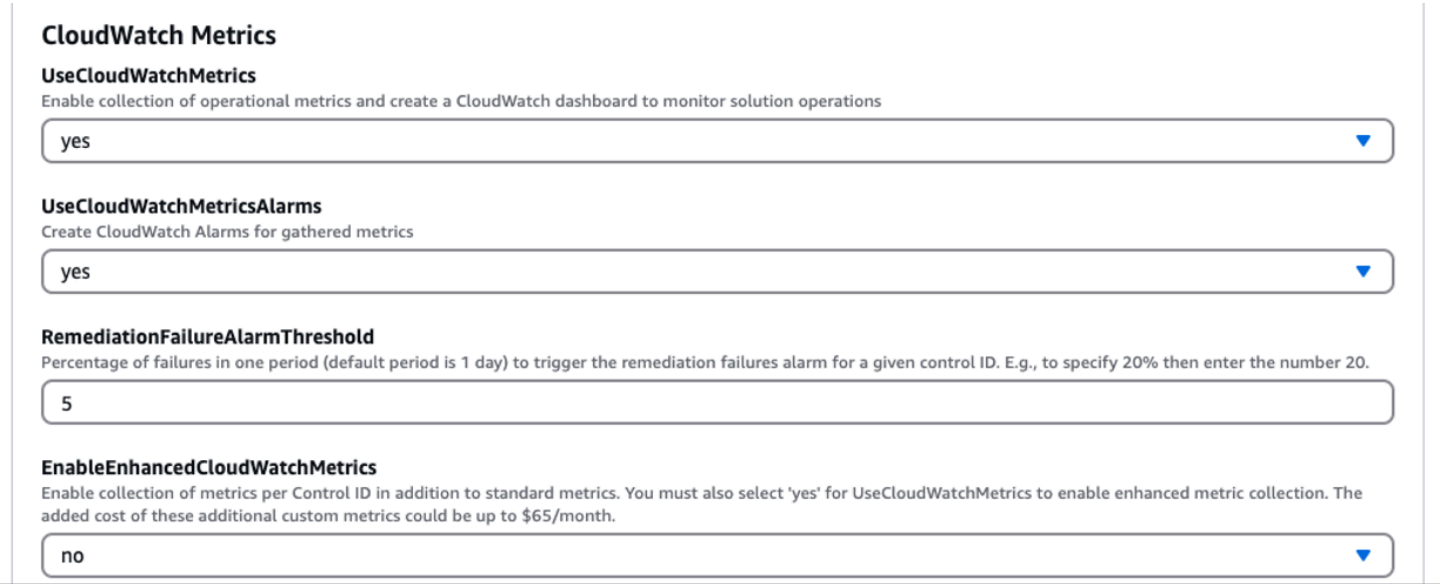
Monitore as operações da solução com um CloudWatch painel da Amazon

Essa solução inclui métricas e alarmes personalizados exibidos em um CloudWatch painel da Amazon.

O CloudWatch painel e os alarmes monitoram as operações da solução e alertam quando há um possível problema.

Ativando CloudWatch métricas, alarmes e painel

Há quatro parâmetros CloudFormation de modelo para CloudWatch funcionalidade.



1. UseCloudWatchMetrics— Definir isso para `yes` permitir a coleta de métricas operacionais e cria um CloudWatch painel para visualizar essas métricas.
2. UseCloudWatchAlarms— Definir isso para `yes` ativar os alarmes padrão da solução.
3. RemediationFailureAlarmThreshold— A porcentagem de falhas nas correções em um período para acionar um alarme.
4. EnableEnhancedCloudWatchMetrics— Defina esse parâmetro `yes` para coletar métricas individuais por ID de controle. Por padrão, esse parâmetro é definido comono, de forma que somente as métricas sobre o número total de remediações em todo o controle IDs sejam coletadas. Métricas e alarmes individuais por ID de controle incorrem em custos adicionais.

Usando o CloudWatch painel

Para ver o painel:

1. Navegue até Amazon CloudWatch e depois Dashboards.
2. Selecione o painel chamado "ASR-Remediation-Metrics-Dashboard”.

O CloudWatch painel contém as seguintes seções:

1. Total de remediações bem-sucedidas — fornece uma visão sobre o número de descobertas do Security Hub que foram corrigidas com sucesso pela solução.
2. Falhas de remediação — Mostra quantas correções falharam, no total e em porcentagem, e a causa da falha. Um grande número de falhas pode sugerir um problema técnico com a solução que talvez você precise investigar com mais detalhes.
3. Sucesso/falha da correção por ID de controle — Se você ativou as Métricas aprimoradas no momento da implantação, esta seção lista os resultados da remediação por ID de controle. Quando a seção Falhas de Remediação mostra uma alta taxa de falhas em geral, esta seção mostra se as falhas estão distribuídas em vários controles IDs ou se apenas determinados controles IDs estão falhando.
4. Runbook Assume Role Failures — Mostra o número de falhas que ocorreram devido a tentativas de remediação em contas que não têm a função de membro da solução instalada. Falhas repetidas por tentativas automatizadas de remediação devido à falta de funções causam custos desnecessários. Reduza isso instalando a pilha de funções de membro nas contas em questão, desativando todas as EventBridge regras criadas pela solução ou desassociando a conta no Security Hub.
5. Cloud Trail Management Actions by ASR — Lista as ações de gerenciamento da solução em todas as contas de membros nas quais você ativou os registros de ação com o EnableCloudTrailForASRActionLogparâmetro no momento da implantação. Quando você observa mudanças inesperadas de recursos em qualquer uma das suas AWS contas, esse widget pode ajudá-lo a entender se os recursos foram modificados pela solução.

O CloudWatch painel também vem com alarmes predefinidos que alertam sobre erros operacionais comuns.

1. Execuções do State Machine > 1000 em um período de 24 horas.

   a. Um grande aumento nas execuções de remediação pode indicar que uma regra de evento está sendo iniciada com mais frequência do que o pretendido.

   b. O limite pode ser alterado usando o CloudFormation parâmetro.

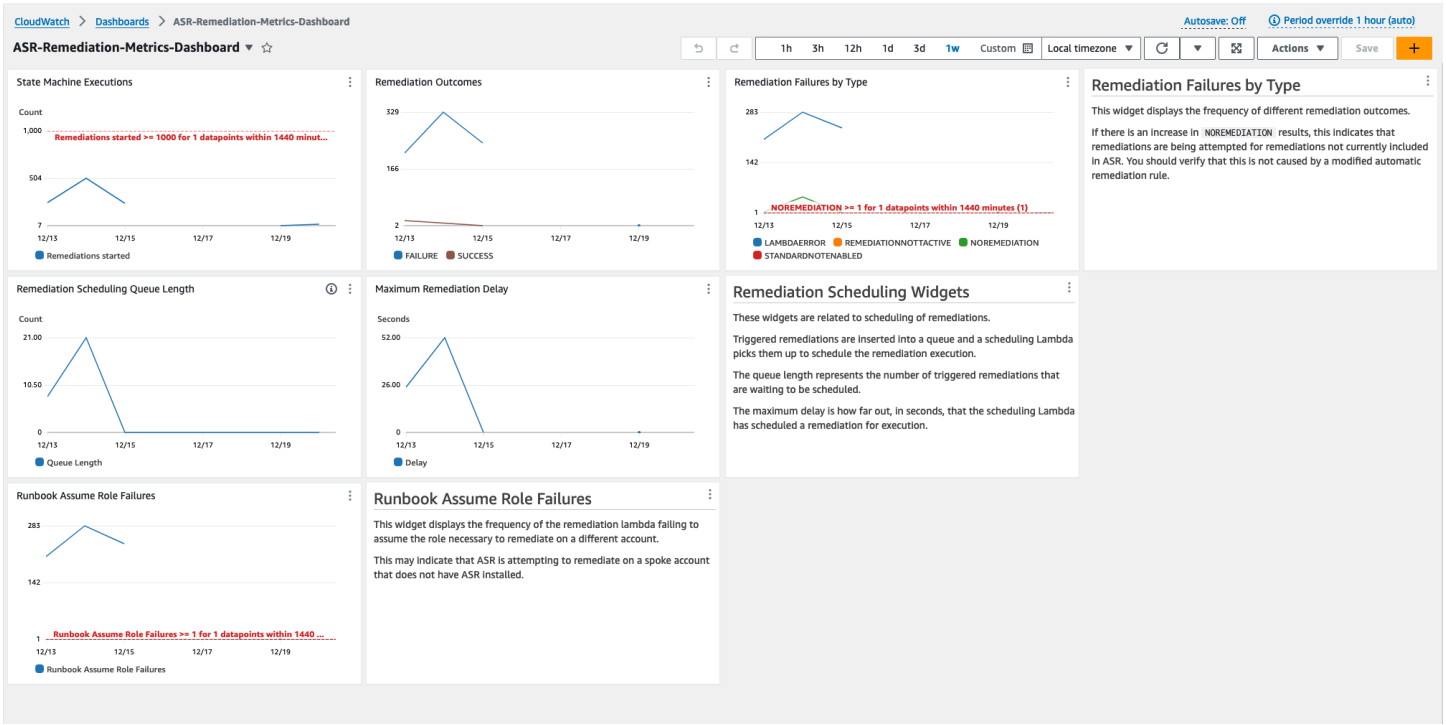
2. Falhas de remediação por tipo = NOREMEDIATION > 0

   a. Correções estão sendo tentadas para remediações que não estão incluídas em. ASR Isso pode indicar que uma regra de evento foi modificada para incluir mais do que as remediações pretendidas.

3. Falhas de função do Runbook Assume > 0

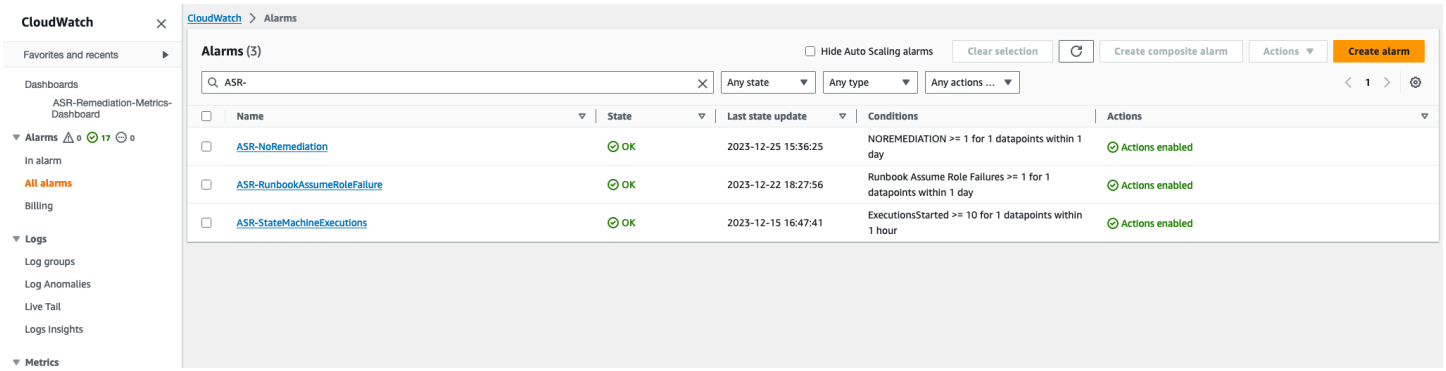
   a. As correções estão sendo tentadas em contas ou regiões que não têm a solução implantada adequadamente. Isso pode indicar que uma regra de evento foi modificada para incluir mais contas do que o pretendido.

Todos os limites de alarme podem ser modificados para atender às necessidades individuais de implantação.

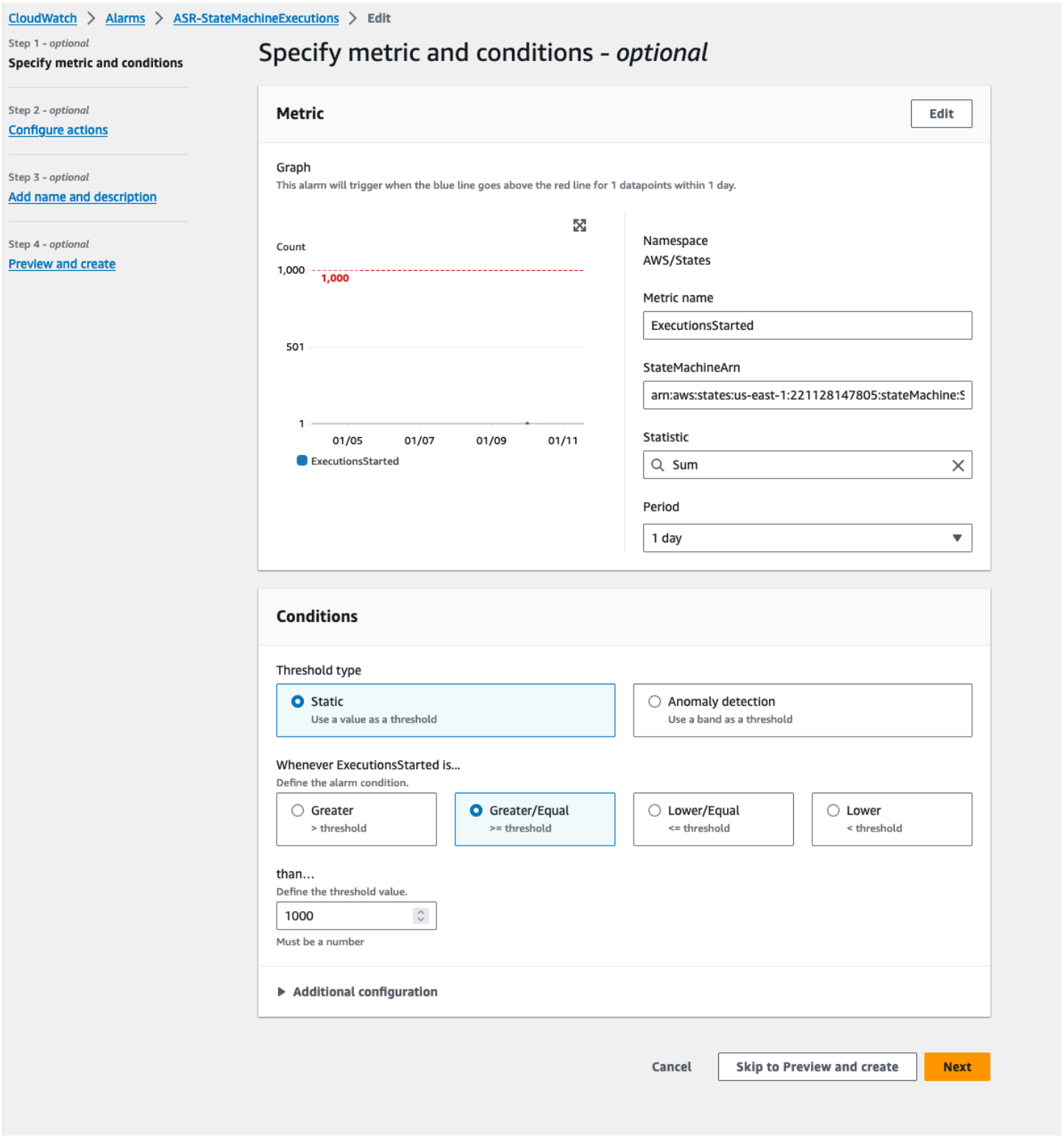


Modificando os limites de alarme

1. Navegue até Amazon CloudWatch -> Alarmes -> Todos os alarmes.
2. Escolha o alarme que você gostaria de modificar e selecione Ações -> Editar.



3. Altere o limite para o valor desejado e salve.



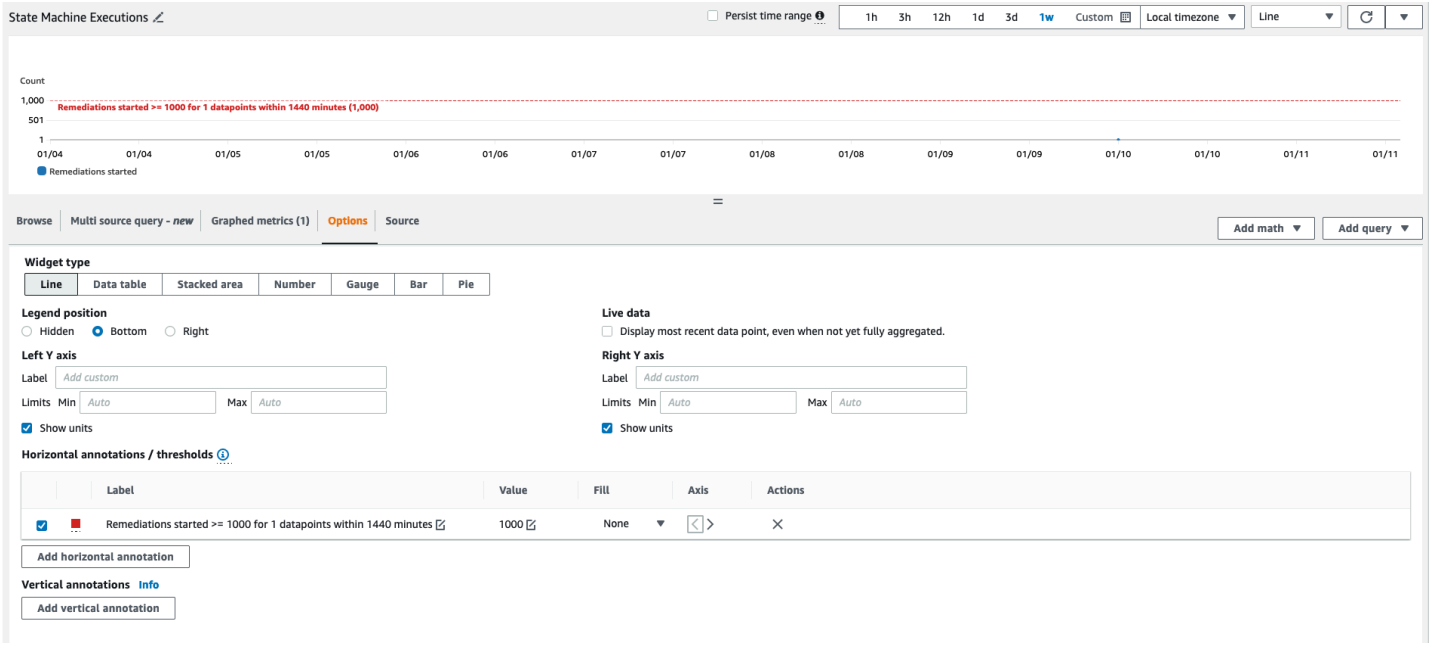
4. Navegue até o CloudWatch painel para modificar os gráficos de acordo com as novas configurações.

   a. Selecione as reticências no canto superior direito do widget correspondente.

b. Selecione Edit (Editar).

c. Vá para a guia Opções.

d. Modifique a anotação do alarme para corresponder às novas configurações.



Inscrever-se para receber notificações de alarme

Na conta de administrador, assine o SNS tópico da Amazon criado pela pilha de administradores, SO0111- _Alarm_Topic. ASR Isso o notificará quando um alarme entrar no ALARM estado.

Atualizar a solução

Atualização de versões anteriores à v1.4

Se você já implantou a solução antes da v1.4.x, desinstale e instale a versão mais recente:

1. Desinstale a solução implantada anteriormente. Consulte Desinstalar a solução.
2. Inicie o modelo mais recente. Consulte Implantar a solução.

> **Note**
>
> Se você estiver atualizando da v1.2.1 ou anterior para a v1.3.0 ou posterior, defina Usar grupo de registros do orquestrador existente como. No Se você estiver reinstalando a v1.3.0 ou posterior, poderá selecionar essa opçãoYes. Essa opção permite que você continue fazendo login no mesmo grupo de registros do Orchestrator Step Functions.

Atualizando da versão 1.4 e versões posteriores

Se você estiver atualizando da v1.4.x, atualize todas as pilhas da seguinte forma: StackSets

1. Atualize a pilha na conta de administrador do Security Hub usando o modelo mais recente.
2. Em cada conta de membro, atualize as permissões do modelo mais recente.
3. Em cada conta de membro em todas as regiões em que está implantada atualmente, atualize a pilha de membros a partir do modelo mais recente.

Atualizando a partir da v2.0.x

Se você estiver atualizando da v2.0.x, atualize para a v2.1.2 ou posterior. A atualização para v2.1.0 - v2.1.1 falhará. CloudFormation

Solução de problemas

A resolução de problemas conhecidos fornece instruções para mitigar erros conhecidos. Se essas instruções não resolverem seu problema, o Contact AWS Support fornecerá instruções para abrir um caso de AWS suporte para essa solução.

Registros da solução

Esta seção inclui informações sobre solução de problemas dessa solução. Consulte a navegação à esquerda para ver os tópicos.

Essa solução coleta a saída dos runbooks de remediação, que são executados em AWS Systems Manager, e registra o resultado no grupo CloudWatch Logs `SO0111-SHARR` na conta do AWS Security Hub administrador. Há um stream por controle por dia.

O Orchestrator Step Functions registra todas as transições de etapas no Grupo `SO0111-SHARR-Orchestrator` CloudWatch Logs na conta de administrador do AWS Security Hub. Esse log é uma trilha de auditoria para registrar as transições de estado para cada instância do Step Functions. Há um fluxo de log por execução do Step Functions.

Ambos os grupos de registros são criptografados usando uma chave do AWS KMS gerente do cliente ()CMK.

As informações de solução de problemas a seguir usam o grupo de `SO0111-SHARR` registros. Use esse registro, bem como o console do AWS Systems Manager Automation, os registros do Automation Executions, o console Step Function e os registros do Lambda para solucionar problemas.

Se uma correção falhar, uma mensagem semelhante à seguinte será registrada `SO0111-SHARR` no fluxo de log para o padrão, o controle e a data. Por exemplo: CIS-2.9-2021-08-12

```
ERROR: a4cbb9bb-24cc-492b-a30f-1123b407a6253: Remediation failed for CIS control
 2.9 in account 123412341234: See Automation Execution output for details (AwsEc2Vpc
 vpc-0e92bbe911cf08acb)
```

As mensagens a seguir fornecem detalhes adicionais. Essa saída é do SHARR runbook do padrão e controle de segurança. Por exemplo: SHARR- CIS _1.2.0_2.9

```
Step fails when it is Execution complete: verified. Failed to run automation with
 executionId: eecdef79-9111-4532-921a-e098549f5259 Failed :
{Status=[Failed], Output=[No output available yet because the step is not successfully
 executed], ExecutionId=[eecdef79-9111-4532-921a-e098549f5259]}. Please refer to
 Automation Service Troubleshooting Guide for more diagnosis details.
```

Essas informações apontam para a falha, que nesse caso foi uma automação infantil em execução na conta do membro. Para solucionar esse problema, você deve fazer login na conta do membro (AWS Management Console na mensagem acima), acessar AWS Systems Manager, navegar até Automação e examinar a saída do log para a ID `eecdef79-9111-4532-921a-e098549f525` de execução.

Resolução de problemas conhecidos

- Problema: A implantação da solução falha com um erro informando que os recursos já estão disponíveis na Amazon CloudWatch.

  Resolução: verifique se há uma mensagem de erro na seção CloudFormation recursos/eventos indicando que grupos de registros já existem. Os modelos SHARR de implantação permitem a reutilização de grupos de registros existentes. Verifique se você selecionou a reutilização.
- Problema: a solução falha ao ser implantada com um erro em uma pilha aninhada do manual em que uma EventBridge regra não é criada

  Resolução: você provavelmente atingiu a cota de EventBridge regras com o número de manuais implantados. Você pode evitar isso usando as descobertas de controle consolidadas no Security Hub combinadas com o manual do SC nesta solução, implantando somente os manuais dos padrões usados ou solicitando um aumento na cota de regras. EventBridge
- Problema: eu executo o Security Hub em várias regiões na mesma conta. Quero implantar essa solução em várias regiões.

  Resolução: implante a pilha administrativa na mesma conta e região do administrador do Security Hub. Instale o modelo de membro em cada conta e região em que você tem um membro do Security Hub configurado. Ative a agregação no Security Hub.
- Problema: imediatamente após a implantação, o SO0111- SHARR -Orchestrator está falhando no estado do documento Get Automation com um erro 502: “O Lambda não conseguiu descriptografar as variáveis de ambiente porque o acesso foi negado. KMS Verifique as configurações das KMS teclas da função. KMS Exceção: UnrecognizedClientException KMS Mensagem: o token de

segurança incluído na solicitação é inválido. (Serviço: AWSLambda; Código de status: 502; Código de erro:KMSAccessDeniedException; ID da solicitação:...”

Resolução: aguarde a estabilização da solução por cerca de 10 minutos antes de executar as correções. Se o problema persistir, abra um ticket de suporte ou GitHub problema.

- Problema: tentei corrigir uma descoberta, mas nada aconteceu.

  Resolução: Verifique as notas da descoberta para saber os motivos pelos quais ela não foi corrigida. Uma causa comum é que a descoberta não tem remediação automática. No momento, não há como fornecer feedback direto ao usuário quando não existe nenhuma correção além das notas. Analise os registros da solução. Abra CloudWatch Logs no console. Encontre o grupo de SHARR CloudWatch registros SO0111-. Classifique a lista para que os streams atualizados mais recentemente apareçam primeiro. Selecione o fluxo de log para a descoberta que você tentou executar. Você deve encontrar algum erro lá. Alguns motivos para a falha podem ser: incompatibilidade entre o controle de descoberta e o controle de remediação, remediação entre contas (ainda não suportada) ou o fato de a descoberta já ter sido corrigida. Se não conseguir determinar o motivo da falha, colete os registros e abra um ticket de suporte.
- Problema: depois de iniciar uma correção, o status no console do Security Hub não foi atualizado.

  Resolução: o console do Security Hub não é atualizado automaticamente. Atualize a exibição atual. O status da descoberta deve ser atualizado. Pode levar várias horas para que a descoberta passe de Falha para Aprovada. As descobertas são criadas a partir de dados de eventos enviados por outros serviços, como AWS Config, para o AWS Security Hub. O tempo até que uma regra seja reavaliada depende do serviço subjacente. Se isso não resolver o problema, consulte a resolução anterior para “Eu tentei corrigir uma descoberta, mas nada aconteceu”.
- Problema: a função de etapa do orquestrador falha em Obter estado do documento de automação: ocorreu um erro (AccessDenied) ao chamar a AssumeRole operação.

  Resolução: O modelo de membro não foi instalado na conta do membro em SHARR que está tentando corrigir uma descoberta. Siga as instruções para a implantação do modelo de membro.
- Problema: o runbook do Config.1 falha porque o gravador ou o canal de entrega já existe.

  Resolução: inspecione suas AWS Config configurações cuidadosamente para garantir que o Config esteja configurado corretamente. A correção automatizada não é capaz de corrigir as configurações existentes do AWS Config em alguns casos.
- Problema: a correção foi bem-sucedida, mas retorna a mensagem `"No output available yet because the step is not successfully executed."`

Resolução: Esse é um problema conhecido nesta versão em que determinados runbooks de correção não retornam uma resposta. Os runbooks de remediação falharão adequadamente e sinalizarão a solução se não funcionarem.

- Problema: a resolução falhou e enviou um rastreamento de pilha.

  Resolução: ocasionalmente, perdemos a oportunidade de lidar com uma condição de erro que resulta em um rastreamento de pilha em vez de uma mensagem de erro. Tente solucionar o problema a partir dos dados de rastreamento. Abra um ticket de suporte se precisar de ajuda.

- Problema: a remoção da pilha v1.3.0 falhou no recurso de ação personalizada.

  Resolução: a remoção do modelo administrativo pode falhar na remoção da Ação Personalizada. Esse é um problema conhecido que será corrigido na próxima versão. Se isso ocorrer:

  1. Faça login no console de gerenciamento do AWS Security Hub.
  2. Na conta de administrador, acesse Configurações.
  3. Selecione a guia Ações personalizadas
  4. Exclua manualmente a entrada Remediar com SHARR.
  5. Exclua a pilha novamente.

- Problema: depois de reimplantar a pilha de administração, a função step está falhando. `AssumeRole`

  Resolução: a reimplantação da pilha de administração quebra a conexão de confiança entre a função de administrador na conta de administrador e a função de membro nas contas de membros. Você deve reimplantar a pilha de funções dos membros em todas as contas dos membros.

- Problema: as remediações CIS 3.x não aparecem `PASSED` após mais de 24 horas.

  Resolução: Essa é uma ocorrência comum se você não tiver assinaturas do `S00111-SHARR_LocalAlarmNotification` SNS tópico na conta do membro.

Problemas com correções específicas

A etSSLBucket política S falha com AccessDenied erro

Controles associados: AWS FSBP v1.0.0 S3.5, PCI v3.2.1 PCI .S3.5, v1.4.0 2.1.2, SC v2.0.0 S3.5 CIS

Problema: a etSSLBucket política S falha com um AccessDenied erro:

Ocorreu um erro (AccessDenied) ao chamar a PutBucketPolicy operação: Acesso negado

Se a configuração Bloquear acesso público tiver sido ativada para um bucket, as tentativas de colocar uma política de bucket que inclua instruções que permitam o acesso público falharão com esse erro. Esse estado pode ser alcançado colocando uma política de bucket que contenha essas declarações e, em seguida, habilitando o bloco de acesso público para esse bucket.

O ConfigureS3 de remediação BucketPublicAccessBlock (controles associados: AWS FSBP v1.0.0 S3.2, PCI v3.2.1 PCI .S3.2, CIS v1.4.0 2.1.5.2, SC v2.0.0 S3.2) também pode colocar um bucket nesse estado porque define a configuração do bloco de acesso público sem alterar a política do bucket.

A etSSLBucket Política S adiciona uma declaração à política do bucket para negar solicitações que não são usadasSSL. Ela não modifica as outras declarações na política, portanto, se houver declarações que permitam o acesso público, a remediação falhará ao tentar colocar a política de bucket modificada que ainda inclua essas declarações.

Resolução: modifique a política do bucket para remover declarações que permitem acesso público em conflito com a configuração de bloqueio de acesso público no bucket.

O PuTs3 falha BucketPolicyDeny

Controles associados: AWS FSBP v1.0.0 S3.6, NIST.800-53.r5 CA-9 (1), .800-53.r5 CM-2 NIST

Problema: O PuTs3 BucketPolicyDeny com o seguinte erro:

```
Unable to create an explicit deny statement for {bucket_name}.
```

Se os principais de todas as políticas no intervalo de destino forem “*”, a solução não poderá adicionar a política de negação ao intervalo de destino, pois isso bloquearia todas as ações do intervalo de todos os principais.

Resolução: modifique a política do bucket para permitir ações em contas específicas em vez de usar os principais “*” e restrinja as ações negadas.

Como desativar a solução

No caso de um incidente, você pode achar que precisa desativar a solução sem remover nenhuma infraestrutura. Esses cenários detalham como desativar diferentes componentes na solução.

Cenário 1: desative a correção automática para um único controle.

1. Navegue até EventBridge no AWS CloudFormation console.
2. Selecione Regras na barra lateral.
3. Selecione o barramento de eventos padrão e procure o controle que você gostaria de desativar.
4. Selecione a regra e selecione o botão Desativar.

Cenário 2: desative a correção automática para todos os controles.

1. Navegue até EventBridge no console.
2. Selecione Regras na barra lateral.
3. Selecione o ônibus de eventos “padrão” e selecione todas as regras abaixo.
4. Selecione o botão “Desativar”. Observe que talvez seja necessário fazer isso para várias páginas de regras.

Cenário 3: desabilitar a correção manual para uma conta

1. Navegue até EventBridge no console.
2. Selecione Regras na barra lateral.
3. Selecione o barramento de eventos “padrão” e pesquise por “SHARRRemediate_with_ _” CustomAction
4. Selecione a regra e selecione o botão “Desativar”.

Entre em contato Support

Se você tem AWSDeveloper Support, AWS Business Support ou AWSEnterprise Support, você pode usar o Support Center para obter assistência especializada com essa solução. As seções a seguir dão instruções.

Criar caso

1. Faça login no Support Center.
2. Escolha Criar caso.

Como podemos ajudar?

1. Escolha Técnico.
2. Em Serviço, selecione Soluções.
3. Em Categoria, selecione Outras soluções.
4. Em Severidade, selecione a opção que melhor corresponda ao seu caso de uso.
5. Quando você insere o Serviço, a Categoria e a Gravidade, a interface preenche links para perguntas comuns de solução de problemas. Se você não conseguir resolver sua pergunta com esses links, escolha Próxima etapa: Informações adicionais.

Mais informações

1. Em Assunto, insira um texto resumindo sua pergunta ou problema.
2. Em Descrição, descreva o problema em detalhes.
3. Escolha Anexar arquivos.
4. Anexe as informações Support necessárias para processar a solicitação.

Ajude-nos a resolver seu caso com mais rapidez

1. Insira as informações solicitadas.
2. Escolha Próxima etapa: solucione ou entre em contato conosco.

Resolva agora ou entre em contato conosco

1. Analise as soluções Solve now.
2. Se você não conseguir resolver seu problema com essas soluções, escolha Fale conosco, insira as informações solicitadas e escolha Enviar.

Desinstalar a solução

Use o procedimento a seguir para desinstalar a solução com AWS Management Console o.

V1.0.0-V1.2.1

Para as versões v1.0.0 a v1.2.1, use o Service Catalog para desinstalar e/ou Playbooks. CIS FSBP Com a v1.3.0, o Service Catalog não é mais usado.

1. Entre no AWS CloudFormation console e navegue até a conta principal do Security Hub.
2. Escolha Service Catalog para encerrar qualquer manual provisionado, remover grupos de segurança, funções ou usuários.
3. Remova o `CISPermissions.template` modelo spoke das contas dos membros do Security Hub.
4. Remova o `AFSBPMemberStack.template` modelo spoke das contas de administrador e membro do Security Hub.
5. Navegue até a conta principal do Security Hub, selecione a pilha de instalação da solução e escolha Excluir.

> **Note**
>
> CloudWatch Os registros do grupo de registros são retidos. Recomendamos reter esses registros conforme exigido pela política de retenção de registros da sua organização.

V1.3.x

1. Remova o `aws-sharr-member.template` da conta de cada membro.
2. Remova o `aws-sharr-admin.template` da conta de administrador.

> **Note**
>
> A remoção do modelo administrativo na v1.3.0 provavelmente falhará na remoção da Ação Personalizada. Esse é um problema conhecido que será corrigido na próxima versão. Use as instruções a seguir para corrigir esse problema:

1. Faça login no console de gerenciamento do AWS Security Hub.
2. Na conta de administrador, acesse Configurações.
3. Selecione a guia Ações personalizadas.
4. Exclua manualmente a entrada Remediar com SHARR.
5. Exclua a pilha novamente.

V1.4.0 e versões posteriores

Implantação do Stack

1. Remova o `aws-sharr-member.template` da conta de cada membro.
2. Remova o `aws-sharr-admin.template` da conta de administrador.

StackSet implantação

Para cada uma StackSet, remova as pilhas e, em seguida, remova-as StackSet na ordem inversa da implantação.

Observe que as IAM funções do `aws-sharr-member-roles.template` são mantidas mesmo que o modelo seja removido. Isso é para que as remediações usando essas funções continuem funcionando. Essas funções SO0111-* podem ser removidas manualmente após a verificação de que não estão mais em uso por meio de remediações ativas, como CloudTrail registro ou monitoramento aprimorado. CloudWatch RDS

Guia do administrador

Ativando e desativando partes da solução

Como administrador da solução, você tem os seguintes controles sobre quais funcionalidades da solução estão habilitadas.

Onde as pilhas de membros e funções de membros são implantadas:

- A pilha administrativa só poderá iniciar correções (por meio de ações personalizadas ou EventBridge regras totalmente automatizadas) em contas nas quais as pilhas de funções de membro e membro tenham sido implantadas com o número da conta do administrador fornecido como um valor de parâmetro.
- Para isentar completamente as contas ou regiões do controle da solução, não implante as pilhas de membros ou funções de membros nessas contas ou regiões.

Configuração de agregação de localização de conta e região no Security Hub:

- A pilha administrativa só poderá iniciar correções (por meio de ações personalizadas ou EventBridge regras totalmente automatizadas) para descobertas que chegarem à conta do administrador e à região.
- Para isentar completamente as contas ou regiões do controle da solução, não inclua essas contas ou regiões para enviar descobertas para a mesma conta de administrador e região em que a pilha administrativa está implantada.

Quais pilhas aninhadas padrão são implantadas:

- A pilha de administração só poderá iniciar correções (por meio de ações personalizadas ou EventBridge regras totalmente automatizadas) para controles que tenham um runbook de controle implantado na conta e região do membro de destino. Eles são implantados pela pilha de membros para cada padrão.
- A pilha de administração só poderá iniciar correções totalmente automatizadas usando EventBridge regras para controles que tenham as regras implantadas pela pilha de administração para esse padrão. Eles são implantados na conta do administrador.
- Para simplificar, recomendamos a implantação consistente de padrões em suas contas de administrador e de membros. Se você se importa AWS FSBP com a CIS versão 1.2.0, implante

essas duas pilhas de administração aninhadas na conta de administrador e implante essas duas pilhas de membros aninhadas em cada conta de membro e região.

Quais runbooks de controle são implantados em cada pilha de membros aninhada:

- A pilha de administração só poderá iniciar correções (por meio de ações personalizadas ou EventBridge regras totalmente automatizadas) para controles que tenham um runbook de controle implantado na conta do membro alvo e na região pela pilha de membros para cada padrão.
- Para exercer um controle mais refinado sobre quais controles estão habilitados para um determinado padrão, cada pilha aninhada de um padrão tem parâmetros para os quais os runbooks de controle são implantados. Defina o parâmetro de um controle com o valor “NOTDisponível” para desimplantar esse runbook de controle.

SSMParâmetros para habilitar e desabilitar padrões:

- A pilha de administração só poderá iniciar correções (por meio de ações personalizadas ou EventBridge regras totalmente automatizadas) para padrões habilitados por meio do SSM parâmetro implantado pela pilha de administração padrão.
- <standard_name><standard_version>Para desativar um padrão, defina o valor do SSM Parâmetro com o caminho “/Solutions/SO0111///status” como “Não”.

SNSNotificações de exemplo

Quando uma remediação é iniciada


```
{
  "severity": "INFO",
  "message": "00000000-0000-0000-0000-000000000000: Remediation queued for SC control
 RDS.13 in account 111111111111",
  "finding": {
    "finding_id": "22222222-2222-2222-2222-222222222222",
    "finding_description": "This control checks if automatic minor version upgrades are
 enabled for the Amazon RDS database instance.",
    "standard_name": "security-control",
    "standard_version": "2.0.0",
    "standard_control": "RDS.13",
    "title": "RDS automatic minor version upgrades should be enabled",
```

```
    "region": "us-east-1",
    "account": "111111111111",
    "finding_arn": "arn:aws:securityhub:us-east-1:111111111111:security-control/RDS.13/
finding/22222222-2222-2222-2222-222222222222"
  }
}
```

Quando uma remediação é bem-sucedida

```
{
  "severity": "INFO",
  "message": "00000000-0000-0000-0000-000000000000: Remediation succeeded for SC
 control RDS.13 in account 111111111111: See Automation Execution output for details
 (AwsRdsDbInstance arn:aws:rds:us-east-1:111111111111:db:database-1)",
  "finding": {
    "finding_id": "22222222-2222-2222-2222-222222222222",
    "finding_description": "This control checks if automatic minor version upgrades are
 enabled for the Amazon RDS database instance.",
    "standard_name": "security-control",
    "standard_version": "2.0.0",
    "standard_control": "RDS.13",
    "title": "RDS automatic minor version upgrades should be enabled",
    "region": "us-east-1",
    "account": "111111111111",
    "finding_arn": "arn:aws:securityhub:us-east-1:111111111111:security-control/RDS.13/
finding/22222222-2222-2222-2222-222222222222"
  }
}
```

Quando uma remediação falha

```
{
  "severity": "ERROR",
  "message": "00000000-0000-0000-0000-000000000000: Remediation failed for SC
 control RDS.13 in account 111111111111: See Automation Execution output for details
 (AwsRdsDbInstance arn:aws:rds:us-east-1:111111111111:db:database-1)",
  "finding": {
    "finding_id": "22222222-2222-2222-2222-222222222222",
```

```
    "finding_description": "This control checks if automatic minor version upgrades are
 enabled for the Amazon RDS database instance.",
    "standard_name": "security-control",
    "standard_version": "2.0.0",
    "standard_control": "RDS.13",
    "title": "RDS automatic minor version upgrades should be enabled",
    "region": "us-east-1",
    "account": "111111111111",
    "finding_arn": "arn:aws:securityhub:us-east-1:111111111111:security-control/RDS.13/
finding/22222222-2222-2222-2222-222222222222"
  }
}
```

Use a solução

Este é um tutorial que o guiará em sua primeira implantação doASR. Começará com os pré-requisitos para implantar a solução e terminará com você corrigindo exemplos de descobertas em uma conta de membro.

Tutorial: Introdução ao Automated Security Response em AWS

Este é um tutorial que o guiará em sua primeira implantação. Começará com os pré-requisitos para implantar a solução e terminará com você corrigindo exemplos de descobertas em uma conta de membro.

Prepare as contas

Para demonstrar os recursos de remediação entre contas e regiões da solução, este tutorial usará duas contas. Você também pode implantar a solução em uma única conta.

Os exemplos a seguir usam contas `111111111111` e demonstram `222222222222` a solução. `111111111111`será a conta do administrador e `222222222222` será a conta do membro. Vamos configurar a solução para remediar as descobertas de recursos nas regiões `us-east-1` e. `us-west-2`

A tabela abaixo é um exemplo para ilustrar as ações que tomaremos em cada etapa em cada conta e região.

Conta	Finalidade	Ação em us-east-1	Ação em us-west-2
`111111111111`	Administrador	Nenhum	Nenhum
`222222222222`	Membro	Nenhum	Nenhum

A conta de administrador é a conta que executará as ações administrativas da solução, ou seja, iniciar as remediações manualmente ou ativar a remediação totalmente automatizada com regras. EventBridge Essa conta também deve ser a conta de administrador delegado do Security Hub para todas as contas nas quais você deseja corrigir as descobertas, mas não precisa ser nem deve ser a conta de administrador do AWS Organizations da AWS organização à qual suas contas pertencem.

Habilitar AWS Config

Analise a seguinte documentação:

- AWSDocumentação de configuração
- AWSConfig preços
- Ativando o AWS Config

Ative o AWS Config nas duas contas e nas duas regiões. Isso incorrerá em cobranças.

> **Important**
>
> Certifique-se de selecionar a opção “Incluir recursos globais (por exemplo, AWS IAM recursos)”. Se você não selecionar essa opção ao ativar o AWS Config, não verá descobertas relacionadas a recursos globais (por exemplo AWSIAM, recursos)

Conta	Finalidade	Ação em us-east-1	Ação em us-west-2
111111111111	Administrador	Habilitar AWS Config	Habilitar AWS Config
222222222222	Membro	Habilitar AWS Config	Habilitar AWS Config

Ativar hub AWS de segurança

Analise a seguinte documentação:

- AWSDocumentação do Security Hub
- AWSPreços do Security Hub
- Habilitando o AWS Security Hub

Ative o AWS Security Hub nas duas contas e nas duas regiões. Isso incorrerá em cobranças.

Conta	Finalidade	Ação em us-east-1	Ação em us-west-2
111111111111	Administrador	Ativar o AWS Security Hub	Ativar o AWS Security Hub
222222222222	Membro	Ativar o AWS Security Hub	Ativar o AWS Security Hub

Possibilite descobertas consolidadas de controle

Analise a seguinte documentação:

- Gerando e atualizando descobertas de controle

Para os fins deste tutorial, demonstraremos o uso da solução com o recurso consolidado de descobertas de controle do AWS Security Hub ativado, que é a configuração recomendada. Em partições que não oferecem suporte a esse recurso no momento em que este artigo foi escrito, você precisará implantar os manuais específicos do padrão em vez do SC (Controle de Segurança).

Possibilite descobertas de controle consolidadas em ambas as contas e em ambas as regiões.

Conta	Finalidade	Ação em us-east-1	Ação em us-west-2
111111111111	Administrador	Possibilite descobertas consolidadas de controle	Possibilite descobertas consolidadas de controle
222222222222	Membro	Possibilite descobertas consolidadas de controle	Possibilite descobertas consolidadas de controle

Pode levar algum tempo para que as descobertas sejam geradas com o novo recurso. Você pode continuar com o tutorial, mas não conseguirá corrigir as descobertas geradas sem o novo recurso. As descobertas geradas com o novo recurso podem ser identificadas pelo valor do `GeneratorId` campo`security-control/<control_id>`.

Configurar a agregação de localização entre regiões

Analise a seguinte documentação:

- Agregação entre regiões
- Habilitando a agregação entre regiões

Configure a agregação de localização de us-west-2 a us-east-1 em ambas as contas.

Conta	Finalidade	Ação em us-east-1	Ação em us-west-2
111111111111	Administrador	Configurar a agregação de us-west-2	Nenhum
222222222222	Membro	Configurar a agregação de us-west-2	Nenhum

Pode levar algum tempo para que as descobertas se propaguem para a região de agregação. Você pode continuar com o tutorial, mas não poderá corrigir descobertas de outras regiões até que elas comecem a aparecer na região de agregação.

Designar uma conta de administrador do Security Hub

Analise a seguinte documentação:

- Gerenciando contas no AWS Security Hub
- Gerenciando contas de membros da organização
- Gerenciando contas de membros por convite

No exemplo a seguir, usaremos o método de convite manual. Para um conjunto de contas de produção, recomendamos gerenciar a administração delegada do Security Hub por meio de Organizations. AWS

No console do AWS Security Hub na conta de administrador (111111111111), convide a conta de membro (222222222222) para aceitar a conta de administrador como administrador delegado do Security Hub. Na conta do membro, aceite o convite.

Conta	Finalidade	Ação em us-east-1	Ação em us-west-2
111111111111	Administrador	Convide a conta do membro	Nenhum
222222222222	Membro	Aceite o convite	Nenhum

Pode levar algum tempo para que as descobertas se propaguem para a conta do administrador. Você pode continuar com o tutorial, mas não poderá corrigir as descobertas das contas dos membros até que elas comecem a aparecer na conta do administrador.

Crie as funções para permissões autogerenciadas StackSets

Analise a seguinte documentação:

- AWS CloudFormation StackSets
- Conceda permissões autogerenciadas

Vamos implantar CloudFormation pilhas em várias contas, então usaremos. StackSets Não podemos usar permissões gerenciadas pelo serviço porque a pilha de administradores e a pilha de membros têm pilhas aninhadas, que não são suportadas pelo serviço, portanto, devemos usar permissões autogerenciadas.

Implante as pilhas para obter permissões básicas para StackSet operações. Para contas de produção, talvez você queira restringir as permissões de acordo com a documentação de “opções de permissões avançadas”.

Conta	Finalidade	Ação em us-east-1	Ação em us-west-2
111111111111	Administrador	Implantar a pilha de funções de StackSet administrador	Nenhum

Conta	Finalidade	Ação em us-east-1	Ação em us-west-2
		Implante a pilha StackSet de funções de execução	
222222222222	Membro	Implante a pilha StackSet de funções de execução	Nenhum

Crie os recursos inseguros que gerarão exemplos de descobertas

Analise a seguinte documentação:

- Referência de controles do Security Hub
- AWSControles Lambda

O exemplo a seguir é um recurso com uma configuração insegura para demonstrar uma remediação. O exemplo de controle é o Lambda.1: As políticas da função Lambda devem proibir o acesso público.

> **Important**
>
> Estaremos criando intencionalmente um recurso com uma configuração insegura. Analise a natureza do controle e avalie por si mesmo o risco de criar esse recurso em seu ambiente. Esteja ciente de qualquer ferramenta que sua organização possa ter para detectar e relatar esses recursos e solicite uma exceção, se apropriado. Se o controle de exemplo que selecionamos não for adequado para você, selecione outro controle compatível com a solução.

Na segunda região da conta do membro, navegue até o console AWS Lambda e crie uma função no tempo de execução mais recente do Python. Em Configuração -> Permissões, adicione uma declaração de política para permitir a invocação da função a partir do URL sem autenticação.

Confirme na página do console se a função permite acesso público. Depois que a solução corrigir esse problema, compare as permissões para confirmar que o acesso público foi revogado.

Conta	Finalidade	Ação em us-east-1	Ação em us-west-2
111111111111	Administrador	Nenhum	Nenhum
222222222222	Membro	Nenhum	Crie uma função Lambda com uma configuração insegura

Pode levar algum tempo para que o AWS Config detecte a configuração insegura. Você pode continuar com o tutorial, mas não conseguirá corrigir a descoberta até que o Config a detecte.

Crie grupos de CloudWatch registros para controles relacionados

Analise a seguinte documentação:

- Monitoramento CloudTrail de arquivos de log com o Amazon CloudWatch Logs
- CloudTrail controles

Vários CloudTrail controles suportados pela solução exigem que haja um grupo de CloudWatch registros que seja o destino de uma multirregião CloudTrail. No exemplo a seguir, criaremos um grupo de registros de espaço reservado. Para contas de produção, você deve configurar adequadamente a CloudTrail integração com o CloudWatch Logs.

Crie um grupo de registros em cada conta e região com o mesmo nome, por exemplo:`asr-log-group`.

Conta	Finalidade	Ação em us-east-1	Ação em us-west-2
111111111111	Administrador	Criar um grupo de logs	Criar um grupo de logs
222222222222	Membro	Criar um grupo de logs	Criar um grupo de logs

Implemente a solução em contas de tutoriais

Reúna os três Amazon S3 URLs para a pilha de funções de administrador, membro e membro.

Implante a pilha de administração

View template

aws-sharr-deploy.modelo

Na conta de administrador, navegue até o CloudFormation console e implante a pilha administrativa na região de agregação de localização do Security Hub.

Escolha No o valor de todos os parâmetros para carregar pilhas administrativas aninhadas, exceto a pilha “SC” ou “Security Control”. Essa pilha contém os recursos para as descobertas de controle consolidadas que configuramos em nossas contas.

Opte No por reutilizar o grupo de registros do orquestrador, a menos que você tenha implantado essa solução nessa conta e região antes.

Conta	Finalidade	Ação em us-east-1	Ação em us-west-2
111111111111	Administrador	Implante a pilha de administração	Nenhum
222222222222	Membro	Nenhum	Nenhum

Espere até que a pilha administrativa conclua a implantação antes de continuar para que uma relação de confiança possa ser criada das contas dos membros para a conta do administrador.

Implante a pilha de membros

View template

aws-sharr-member.modelo

Na conta de administrador, navegue até o CloudFormation StackSets console e implante a pilha de membros em cada conta e região. Use as funções de StackSets administração e execução criadas neste tutorial.

Insira o nome do grupo de registros que você criou como o valor do parâmetro para o nome do grupo de registros.

Escolha No o valor de todos os parâmetros para carregar pilhas de membros aninhadas, exceto a pilha “SC” ou “controle de segurança”. Essa pilha contém os recursos para as descobertas de controle consolidadas que configuramos em nossas contas.

Insira o ID da conta do administrador como o valor do parâmetro para o número da conta do administrador. Em nosso exemplo, isso é111111111111.

Conta	Finalidade	Ação em us-east-1	Ação em us-west-2
111111111111	Administrador	Implantar o membro StackSet //Confirmar a pilha de membros implantada	Confirme se a pilha de membros foi implantada
222222222222	Membro	Confirme se a pilha de membros foi implantada	Confirme se a pilha de membros foi implantada

Implante a pilha de funções de membros

View template

aws-sharr-member-roles.modelo

Na conta de administrador, navegue até o CloudFormation StackSets console e implante a pilha de membros em cada conta. Use as funções de StackSets administração e execução criadas neste tutorial. Insira o ID da conta do administrador como o valor do parâmetro para o número da conta do administrador. Em nosso exemplo, isso é111111111111.

Conta	Finalidade	Ação em us-east-1	Ação em us-west-2
111111111111	Administrador	Implantar o membro StackSet //Confirmar	Nenhum

Conta	Finalidade	Ação em us-east-1	Ação em us-west-2
		a pilha de membros implantada	
222222222222	Membro	Confirme se a pilha de membros foi implantada	Nenhum

Você pode continuar, mas não poderá corrigir as descobertas até que a implantação seja CloudFormation StackSets concluída.

Inscreva-se no SNS tópico

Atualizações de remediação

Tópico - SO0111 - _Tópico SHARR

Na conta de administrador, assine o SNS tópico da Amazon criado pela pilha de administradores. Isso o notificará quando as remediações forem iniciadas e quando elas forem bem-sucedidas ou falharem.

Alarmes

Tópico - SO0111 - _Alarm_Topic ASR

Na conta de administrador, assine o SNS tópico da Amazon criado pela pilha de administradores. Isso o notificará quando os alarmes métricos forem iniciados.

Corrija exemplos de descobertas

Na conta de administrador, navegue até o console do Security Hub e localize a descoberta do recurso com uma configuração insegura que você criou como parte deste tutorial.

Isso pode ser feito de diversas formas:

1. Em partições que suportam o recurso de descobertas de controle consolidado, uma página chamada “Controles” permite localizar a descoberta pelo ID de controle consolidado.

2. Na página “Padrões de segurança”, você pode localizar o controle de acordo com o padrão ao qual ele pertence.
3. Você pode ver todas as descobertas na página “Descobertas” e pesquisar por atributo.

O ID de controle consolidado para a função pública do Lambda que criamos é Lambda.1.

Inicie a remediação

Marque a caixa de seleção à esquerda da descoberta relacionada ao recurso que criamos. No menu suspenso “Ações”, selecione “Remediar com”. ASR Você verá uma notificação de que a descoberta foi enviada para a Amazon EventBridge.

Conta	Finalidade	Ação em us-east-1	Ação em us-west-2
111111111111	Administrador	Inicie a remediação	Nenhum
222222222222	Membro	Nenhum	Nenhum

Confirme se a remediação resolveu a descoberta

Você deve receber duas SNS notificações. O primeiro indicará que uma remediação foi iniciada e o segundo indicará que a remediação foi bem-sucedida. Depois de receber a segunda notificação, navegue até o console Lambda na conta do membro e confirme se o acesso público foi revogado.

Conta	Finalidade	Ação em us-east-1	Ação em us-west-2
111111111111	Administrador	Nenhum	Nenhum
222222222222	Membro	Nenhum	Confirme se a correção foi bem-sucedida

Rastreie a execução da remediação

Para entender melhor como a solução funciona, você pode rastrear a execução da remediação.

EventBridge regra

Na conta do administrador, localize uma EventBridge regra chamada SHARRRemediate_with_ _. CustomAction Essa regra corresponde à descoberta que você enviou do Security Hub e a envia para o Orchestrator Step Functions.

Execução de Step Functions

Na conta de administrador, localize o AWS Step Functions chamado "SO0111- SHARR - Orchestrator". Essa função de etapa chama o documento de SSM automação na conta e região de destino. Você pode rastrear a execução da remediação no histórico de execução deste AWS Step Functions.

Automação do SSM

Na conta do membro, navegue até o console SSM de automação. Você encontrará duas execuções de um documento chamado "ASR-SC_2.0.0_Lambda.1" e uma execução de um documento chamado" -". ASR RemoveLambdaPublicAccess

A primeira execução é a partir da função de etapa do orquestrador na conta de destino. A segunda execução ocorre na região alvo, que pode não ser a região da qual a descoberta se originou. A execução final é a remediação que revoga a política de acesso público da Função Lambda.

CloudWatch Grupo de registros

Na conta de administrador, navegue até o console de CloudWatch registros e localize um grupo de registros chamado "SO0111- SHARR". Esse grupo de registros é o destino dos registros de alto nível do Orchestrator Step Functions.

Permita remediações totalmente automatizadas

O outro modo de operação da solução é corrigir automaticamente as descobertas à medida que elas chegam ao Security Hub.

Confirme se você não tem recursos aos quais essa descoberta pode ser aplicada acidentalmente

A ativação de remediações automáticas iniciará as remediações em todos os recursos correspondentes ao controle que você habilita (Lambda.1).

> **Important**
>
> Confirme que você deseja que todas as Funções Lambda públicas dentro do escopo da solução tenham essa permissão revogada. As remediações totalmente automatizadas não serão limitadas em escopo à Função que você criou. A solução remediará esse controle se ele for detectado em qualquer uma das contas e regiões nas quais está instalado.

Conta	Finalidade	Ação em us-east-1	Ação em us-west-2
111111111111	Administrador	Confirme se não há funções públicas desejadas	Confirme se não há funções públicas desejadas
222222222222	Membro	Confirme se não há funções públicas desejadas	Confirme se não há funções públicas desejadas

Ativar a regra

Na conta Admin, localize uma EventBridge regra chamada AutoTriggerSC_2.0.0_Lambda.1_ e ative-a.

Conta	Finalidade	Ação em us-east-1	Ação em us-west-2
111111111111	Administrador	Ative as regras de remediação automatizadas	Nenhum
222222222222	Membro	Nenhum	Nenhum

Configurar o recurso

Na conta do membro, reconfigure a Função Lambda para permitir o acesso público.

Conta	Finalidade	Ação em us-east-1	Ação em us-west-2
111111111111	Administrador	Nenhum	Nenhum
222222222222	Membro	Nenhum	Configurar a função Lambda para permitir o acesso público

Confirme se a remediação resolveu a descoberta

Pode levar algum tempo para que o Config detecte a configuração insegura novamente. Você deve receber duas SNS notificações. O primeiro indicará que uma remediação foi iniciada. O segundo indicará que a remediação foi bem-sucedida. Depois de receber a segunda notificação, navegue até o console Lambda na conta do membro e confirme se o acesso público foi revogado.

Conta	Finalidade	Ação em us-east-1	Ação em us-west-2
111111111111	Administrador	Ative as regras de remediação automatizadas	Nenhum
222222222222	Membro	Nenhum	Confirme se a correção foi bem-sucedida

Limpeza

Exclua os recursos de exemplo

Na conta do membro, exclua o exemplo de função Lambda que você criou.

Conta	Finalidade	Ação em us-east-1	Ação em us-west-2
111111111111	Administrador	Nenhum	Nenhum

Conta	Finalidade	Ação em us-east-1	Ação em us-west-2
222222222222	Membro	Nenhum	Exclua o exemplo da função Lambda

Exclua a pilha de administração

Na conta de administrador, exclua a pilha de administração.

Conta	Finalidade	Ação em us-east-1	Ação em us-west-2
111111111111	Administrador	Exclua a pilha de administração	Nenhum
222222222222	Membro	Nenhum	Nenhum

Excluir a pilha de membros

Na conta de administrador, exclua o membro StackSet.

Conta	Finalidade	Ação em us-east-1	Ação em us-west-2
111111111111	Administrador	Excluir o membro StackSet Confirme se a pilha de membros foi excluída	Confirme se a pilha de membros foi excluída
222222222222	Membro	Confirme se a pilha de membros foi excluída	Confirme se a pilha de membros foi excluída

Exclua a pilha de funções dos membros

Na conta de administrador, exclua as funções dos membros StackSet.

Conta	Finalidade	Ação em us-east-1	Ação em us-west-2
111111111111	Administrador	Exclua as funções dos membros StackSet Confirme se a pilha de funções de lembrete foi excluída	Nenhum
222222222222	Membro	Confirme se a pilha de funções dos membros foi excluída	Nenhum

Excluir as funções retidas

Em cada conta, exclua as IAM funções retidas.

Importante: essas funções são mantidas para remediações que exigem uma função para que a remediação continue funcionando (por exemplo, registro de VPC fluxo). Confirme que você não precisa da função contínua de nenhuma dessas funções antes de excluí-las.

Exclua todas as funções prefixadas com SO0111-.

Conta	Finalidade	Ação em us-east-1	Ação em us-west-2
111111111111	Administrador	Excluir funções retidas	Nenhum
222222222222	Membro	Excluir funções retidas	Nenhum

Programe as KMS chaves retidas para exclusão

As pilhas de administradores e membros criam e retêm uma KMS chave. Você incorrerá em cobranças se guardar essas chaves.

Essas chaves são retidas para que você tenha acesso a quaisquer recursos criptografados pela solução. Confirme que você não precisa deles antes de programá-los para exclusão.

Identifique as chaves implantadas pela solução usando os aliases criados pela solução ou a partir do CloudFormation histórico. Agende-os para exclusão.

Conta	Finalidade	Ação em us-east-1	Ação em us-west-2
111111111111	Administrador	Identifique e agende a chave do administrador para exclusão Identifique e agende a chave do membro para exclusão	Identifique e agende a chave do membro para exclusão
222222222222	Membro	Identifique e agende a chave do membro para exclusão	Identifique e agende a chave do membro para exclusão

Exclua as pilhas para obter permissões StackSets autogerenciadas

Exclua as pilhas criadas para permitir permissões StackSets autogerenciadas

Conta	Finalidade	Ação em us-east-1	Ação em us-west-2
111111111111	Administrador	Excluir a pilha de funções de StackSet administrador	Nenhum
222222222222	Membro	Excluir a pilha StackSet de funções de execução	Nenhum

Guia do desenvolvedor

Esta seção fornece o código-fonte da solução e personalizações adicionais.

Código-fonte

Visite nosso GitHub repositório para baixar os modelos e scripts dessa solução e compartilhar suas personalizações com outras pessoas.

Manuais

Essa solução inclui as correções manuais para os padrões de segurança definidos como parte do Center for Internet Security (CIS) Foundations Benchmark v1.2.0, AWS Foundations Benchmark v1.4.0, CIS AWS Foundations Benchmark v3.0.0, AWS Foundational Security Best Practices (FSBP) v.1.0.0, Payment Card Industry Data Security Standard (-) v3.2.1 e National Institute of Standards CIS AWS PCI DSS e Tecnologia (NIST).

Se você tiver as descobertas de controle consolidadas habilitadas, esses controles serão suportados em todos os padrões. Se esse recurso estiver ativado, somente o manual do SC precisará ser implantado. Caso contrário, os manuais são compatíveis com os padrões listados anteriormente.

> **Important**
>
> Somente implante os manuais de acordo com os padrões habilitados para evitar atingir as cotas de serviço.

Para obter detalhes sobre uma remediação específica, consulte o documento de automação do Systems Manager com o nome implantado pela solução em sua conta. Vá para o console do AWS Systems Manager e, no painel de navegação, escolha Documents.

Descrição	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISv1.4.0	NIST	CISv3.0.0	ID de controle de segurança
Total de remediações	63	34	29	33	65	19	90
ASR-EnableAutoScalingGroupELBHealthCheck Grupos de Auto Scaling associados a um balanceador de carga devem usar verificações de integridade do balanceador de carga	Escalonamento automático.1		Escalonamento automático.1		Escalonamento automático.1		Escalonamento automático.1
ASR-Creat	CloudTrail1.	2.1	CloudTrail2.	3.1	CloudTrail1.	3.1	CloudTrail1.

Descrição	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISv1.4.0	NIST	CISv3.0.0	ID de controle de segurança
eMultiRegionTrail CloudTrail deve ser ativada e configurada com pelo menos uma trilha multirregional							
ASR-EnableEncryption CloudTrail deve ter a criptografia em repouso ativada	CloudTrail2.	2.7	CloudTrail1.	3.7	CloudTrail2.	3.5	CloudTrail2.

Descrição	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISv1.4.0	NIST	CISv3.0.0	ID de controle de segurança
ASR-EnablLogFileValidation Certifique-se de que a validação do arquivo de CloudTrail log esteja ativada	CloudTrail4.	2.2	CloudTrail3.	3.2	CloudTrail4.		CloudTrail4.

Descrição	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISv1.4.0	NIST	CISv3.0.0	ID de controle de segurança
ASR-EnableCloudTrailToCloudWatchLogging Garanta que as CloudTrail trilhas estejam integradas com o Amazon CloudWatch Logs	CloudTrail5.	2.4	CloudTrail4.	3.4	CloudTrail5.		CloudTrail5.

Descrição	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISv1.4.0	NIST	CISv3.0.0	ID de controle de segurança
ASR-Configura S3 BucketLogging Certifiqu e-se de que o registro de acesso ao bucket do S3 esteja ativado no bucket do CloudTrai l S3		2.6		3.6		3.4	CloudTrai l7.

Descrição	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISv1.4.0	NIST	CISv3.0.0	ID de controle de segurança
ASR-ReplaceCodeBuildClearTextCredentials CodeBuild as variáveis de ambiente do projeto não devem conter credenciais de texto não criptografado	CodeBuild 2.		CodeBuild 2.		CodeBuild 2.		CodeBuild 2.

Descrição	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISv1.4.0	NIST	CISv3.0.0	ID de controle de segurança
ASR-EnableAWSConfig Certifique-se de AWS Config que está ativado	Config.1	2,5	Config.1	3.5	Config.1	3.3	Config.1
ASR-MakeEBSSnapshotsPrivado Os EBS snapshots da Amazon não devem ser restauráveis publicamente	EC21.		EC21.		EC21.		EC21.

Descrição	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISv1.4.0	NIST	CISv3.0.0	ID de controle de segurança
ASR-RemoveVPCefaultSecurityGroupRules VPCo grupo de segurança padrão deve proibir o tráfego de entrada e saída	EC22.	4.3	EC22.	5.3	EC22.	5.4	EC22.
ASRRegistros -EnableVPCFlow VPCo registro de fluxo deve ser ativado em todos VPCs	EC2.6	2.9	EC2.6	3.9	EC2.6	3.7	EC2.6

Descrição	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISv1.4.0	NIST	CISv3.0.0	ID de controle de segurança
ASR-EnablEbsEncryptionByDefault EBSa criptografia padrão deve ser ativada	EC27.	2.2.1			EC27.	2.2.1	EC27.
ASR-RevokeUnrotatedKeys As chaves de acesso dos usuários devem ser trocadas a cada 90 dias ou menos	IAM3.	1.4		1.14	IAM3.	1.14	IAM3.

Descrição	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISv1.4.0	NIST	CISv3.0.0	ID de controle de segurança
ASRPolítica -SetIAMPassword IAMpolítica de senha padrão	IAM7.	1,5-1,11	IAM8.	1.8	IAM7.	1.8	IAM7.
ASR-RevokeUnusedIAMUserCredentials As credenciais do usuário devem ser desativadas se não forem usadas dentro de 90 dias	IAM8.	1.3	IAM7.		IAM8.		IAM8.

Descrição	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISv1.4.0	NIST	CISv3.0.0	ID de controle de segurança
ASR-RevokeUnusedIAMUserCredentials As credenciais do usuário devem ser desativadas se não forem usadas dentro de 45 dias				1.12		1.12	IAM2.2

Descrição	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISv1.4.0	NIST	CISv3.0.0	ID de controle de segurança
ASR-RemoveLambdaPublicAccess As funções Lambda devem proibir o acesso público	Lambda.1		Lambda.1		Lambda.1		Lambda.1
ASR-MakeRDSSnapshotPrivado RDSos instantâneos devem proibir o acesso público	RDS1.		RDS1.		RDS1.		RDS1.

Descrição	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISv1.4.0	NIST	CISv3.0.0	ID de controle de segurança
ASR-DisablePublicAccessToRDSInstance RDSAs instâncias de banco de dados devem proibir o acesso público	RDS2.		RDS2.		RDS2.	2.3.3	RDS2.

Descrição	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISv1.4.0	NIST	CISv3.0.0	ID de controle de segurança
ASR-EncryptRDSSnapshot RDSos instantâneos do cluster e os instantâneos do banco de dados devem ser criptografados em repouso	RDS4.				RDS4.		RDS4.

Descrição	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISv1.4.0	NIST	CISv3.0.0	ID de controle de segurança
ASR-EnableMultiAZOnRDSInstance RDSAs instâncias de banco de dados devem ser configuradas com várias zonas de disponibilidade	RDS5.				RDS5.		RDS5.

Descrição	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISv1.4.0	NIST	CISv3.0.0	ID de controle de segurança
ASR-EnableEnhancedMonitoringOnRDSInstance O monitoramento aprimorado deve ser configurado para instâncias e clusters de RDS banco de dados	RDS.6				RDS.6		RDS.6

Descrição	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISv1.4.0	NIST	CISv3.0.0	ID de controle de segurança
ASR-EnableRDSCluster DeletionProtection RDSos clusters devem ter a proteção de exclusão ativada	RDS7.				RDS7.		RDS7.
ASR-EnableRDSInstance DeletionProtection RDSAs instâncias de banco de dados devem ter a proteção de exclusão ativada	RDS8.				RDS8.		RDS8.

Descrição	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISv1.4.0	NIST	CISv3.0.0	ID de controle de segurança
ASR-EnableMinorVersionUpgradeOnRDSDBInstance RDSatualizações automáticas de versões secundárias devem ser ativadas	RDS1.3				RDS1.3	2.3.2	RDS1.3

Descrição	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISv1.4.0	NIST	CISv3.0.0	ID de controle de segurança
ASR-EnableCopyTagsToSnapshotOnRDSCluster RDSOs clusters de banco de dados devem ser configurados para copiar tags para snapshots	RDS1.6				RDS1.6		RDS1.6

Descrição	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISv1.4.0	NIST	CISv3.0.0	ID de controle de segurança
ASR-DisablePublicAccessToRedshiftCluster Os clusters do Amazon Redshift devem proibir o acesso público	Redshift.1		Redshift.1		Redshift.1		Redshift.1

Descrição	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISv1.4.0	NIST	CISv3.0.0	ID de controle de segurança
ASR-EnableAutomaticSnapshotsOnRedshiftCluster Os clusters do Amazon Redshift devem ter snapshots automáticos ativados	Redshift.3				Redshift.3		Redshift.3

Descrição	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISv1.4.0	NIST	CISv3.0.0	ID de controle de segurança
ASR-EnableRedshiftClusterAuditLogging Os clusters do Amazon Redshift devem ter o registro de auditoria ativado	Redshift.4				Redshift.4		Redshift.4

Descrição	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISv1.4.0	NIST	CISv3.0.0	ID de controle de segurança
ASR-EnableAutomaticVersionUpgradeOnRedshiftCluster O Amazon Redshift deve ter as atualizações automáticas para as versões principais ativadas	Redshift.6				Redshift.6		Redshift.6

Descrição	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISv1.4.0	NIST	CISv3.0.0	ID de controle de segurança
ASR-Configura S3 PublicAccessBlock A configuração do S3 Block Public Access deve ser ativada	S3.1	2.3	S3.6	2.1.5.1	S3.1	2.1.4	S3.1
ASR-Configura S3 BucketPublicAccessBlock Os buckets do S3 devem proibir o acesso público à leitura	S3.2		S3.2	2.1.5.2	S3.2		S3.2

Descrição	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISv1.4.0	NIST	CISv3.0.0	ID de controle de segurança
ASR-ConfigureS3BucketPublicAccessBlock Os buckets do S3 devem proibir o acesso público à gravação		S3.3					S3.3
ASR-EnableDefaultEncryption S3 Os buckets S3 devem ter a criptografia do lado do servidor ativada	S3.4		S3.4	2.1.1	S3.4		S3.4

Descrição	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISv1.4.0	NIST	CISv3.0.0	ID de controle de segurança
ASRPolítica -SetSSLBucket Os buckets S3 devem exigir solicitações de uso SSL	S3.5		S3.5	2.1.2	S3.5	2.1.1	S3.5

Descrição	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISv1.4.0	NIST	CISv3.0.0	ID de controle de segurança
ASR-S3 BlockDenylist As permissões do Amazon S3 concedidas a outras políticas Contas da AWS no bucket devem ser restritas	3.6				S3.6		S3.6
A configuração do S3 Block Public Access deve ser ativada no nível do bucket	S3.8				S3.8		S3.8

Descrição	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISv1.4.0	NIST	CISv3.0.0	ID de controle de segurança
ASR-Configura S3 BucketPublicAccessBlock Certifique-se de que os CloudTrail registros do bucket do S3 não estejam acessíveis publicamente		2.3					CloudTrail.6

Descrição	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISv1.4.0	NIST	CISv3.0.0	ID de controle de segurança
ASR-CreateAccessLoggingBucket Certifique-se de que o registro de acesso ao bucket do S3 esteja ativado no bucket do CloudTrail S3		2.6					CloudTrail7.

Descrição	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISv1.4.0	NIST	CISv3.0.0	ID de controle de segurança
ASR-EnableKeyRotation Garanta que a rotação criada pelo cliente CMKs esteja ativada		2.8	KMS1.	3.8	KMS4.	3.6	KMS4.

Descrição	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISv1.4.0	NIST	CISv3.0.0	ID de controle de segurança
ASR-CreateLogMetricFilterAndAlarm Certifique-se de que exista um filtro métrico de registro e um alarme para chamadas não autorizadas API		3.1		4.1			Cloudwatch.1

Descrição	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISv1.4.0	NIST	CISv3.0.0	ID de controle de segurança
ASR-CreateLogMetricFilterAndAlarm Certifique-se de que exista um filtro métrico de registro e um alarme para fazer AWS Management Console login sem MFA		3.2		4.2			Cloudwatch.2

Descrição	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISv1.4.0	NIST	CISv3.0.0	ID de controle de segurança
ASR-CreateLogMetricFilterAndAlarm Certifique-se de que exista um filtro métrico de log e um alarme para uso do usuário “root”		3.3	VACA.1	4.3			Cloudwatch.3

Descrição	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISv1.4.0	NIST	CISv3.0.0	ID de controle de segurança
ASR-CreateLogMetricFilterAndAlarm Certifique-se de que exista um filtro métrico de log e um alarme para mudanças na IAM política		3.4		4.4			Cloudwatch.4

Descrição	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISv1.4.0	NIST	CISv3.0.0	ID de controle de segurança
ASR-CreateLogMetricFilterAndAlarm Certifique-se de que exista um filtro métrico de registro e um alarme para alterações CloudTrail de configuração		3.5		4.5			Cloudwatch.5

Descrição	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISv1.4.0	NIST	CISv3.0.0	ID de controle de segurança
ASR-CreateLogMetricFilterAndAlarm Certifique-se de que exista um filtro métrico de registro e um alarme para falhas AWS Management Console de autenticação		3.6		4.6			Cloudwatch.6

Descrição	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISv1.4.0	NIST	CISv3.0.0	ID de controle de segurança
ASR-CreateLogMetricFilterAndAlarm Certifique-se de que exista um filtro métrico de registro e um alarme para desativação ou exclusão programada do cliente criado CMKs		3.7		4.7			Cloudwatch.7

Descrição	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISv1.4.0	NIST	CISv3.0.0	ID de controle de segurança
ASR-CreateLogMetricFilterAndAlarm Verificar se existe um alarme e um filtro de métrica de log para alterações de política do bucket do S3		3.8		4.8			Cloudwatch.8

Descrição	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISv1.4.0	NIST	CISv3.0.0	ID de controle de segurança
ASR-CreateLogMetricFilterAndAlarm Certifique-se de que exista um filtro métrico de registro e um alarme para alterações AWS Config de configuração		3.9		4,9			Cloudwatch.9

Descrição	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISv1.4.0	NIST	CISv3.0.0	ID de controle de segurança
ASR-CreateLogMetricFilterAndAlarm Verificar se existe um alarme e um filtro de métrica de log para alterações do grupo de segurança		3.10		4.10			Cloudwatch.10

Descrição	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISv1.4.0	NIST	CISv3.0.0	ID de controle de segurança
ASR-CreateLogMetricFilterAndAlarm Verifique se existe um filtro métrico de registro e um alarme para alterações nas listas de controle de acesso à rede (NACL)		3.11		4.11			Cloudwatch.11

Descrição	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISv1.4.0	NIST	CISv3.0.0	ID de controle de segurança
ASR-CreateLogMetricFilterAndAlarm Verificar se existe um alarme e um filtro de métrica de log para alterações nos gateways de rede		3.12		4.12			Cloudwatch.12

Descrição	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISv1.4.0	NIST	CISv3.0.0	ID de controle de segurança
ASR-CreateLogMetricFilterAndAlarm Verificar se existe um alarme e um filtro de métrica de log para alterações da tabela de rotas		3.13		4.13			Cloudwatch.13

Descrição	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISv1.4.0	NIST	CISv3.0.0	ID de controle de segurança
ASR-CreateLogMetricFilterAndAlarm Certifique-se de que exista um filtro métrico de registro e um alarme para VPC alterações		3,14		4.14			Cloudwatch.14

Descrição	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISv1.4.0	NIST	CISv3.0.0	ID de controle de segurança
AWS-DisablePublicAccessForSecurityGroup Certifique-se de nenhum grupo de segurança permita a entrada de 0.0.0.0/0 na porta 22		4.1	EC25.		EC21.3		EC21.3

Descrição	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISv1.4.0	NIST	CISv3.0.0	ID de controle de segurança
AWS-DisablePublicAccessForSecurityGroup 4.2 Certifique-se de que nenhum grupo de segurança permita a entrada de 0.0.0.0/0 na porta 3389		4.2			EC21.4		EC21.4
ASR-ConfigureSNSTopicForStack	CloudFormation1.				CloudFormation1.		CloudFormation1.
ASRFunção-CreateIAMSupport		1,20		1.17		1.17	IAM1.8

Descrição	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISv1.4.0	NIST	CISv3.0.0	ID de controle de segurança
ASR-DisablePublicIPAutoAssign EC2As sub-redes da Amazon não devem atribuir automaticamente endereços IP públicos	EC2.15				EC2.15		EC2.15
ASR-EnableCloudTrailLogFileValidation	CloudTrail.4	2.2	CloudTrail.3	3.2			CloudTrail.4
ASR-EnableEncryptionForSNSTopic	SNS.1				SNS.1		SNS.1

Descrição	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISv1.4.0	NIST	CISv3.0.0	ID de controle de segurança
ASR-EnableDeliveryStatusLoggingForSNSTopic O registro do status de entrega deve ser ativado para mensagens de notificação enviadas para um tópico	SNS2.				SNS2.		SNS2.
ASR-EnableEncryptionForSQSQueue	SQS1.				SQS1.		SQS1.

Descrição	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISv1.4.0	NIST	CISv3.0.0	ID de controle de segurança
ASR-MakeRDSSnapshotPrivado RDSo instantâneo deve ser privado	RDS1.		RDS1.				RDS1.
ASR-BlockSSMDocumentPublicAccess SSMOs documentos não devem ser públicos	SSM4.				SSM4.		SSM4.

Descrição	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISv1.4.0	NIST	CISv3.0.0	ID de controle de segurança
ASR-EnableCloudFrontDefaultRootObject CloudFront as distribuições devem ter um objeto raiz padrão configurado	CloudFront1.				CloudFront1.		CloudFront1.

Descrição	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISv1.4.0	NIST	CISv3.0.0	ID de controle de segurança
ASR-SetCloudFrontOriginDomain CloudFront distribuições não devem apontar para origens inexistentes do S3	CloudFront.2				CloudFront.2		CloudFront.2

Descrição	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISv1.4.0	NIST	CISv3.0.0	ID de controle de segurança
ASR-RemoveCodeBuildPrivilegedMode CodeBuild ambientes de projeto devem ter uma duração de registro AWS Config	CodeBuild 5.				CodeBuild 5.		CodeBuild 5.

Descrição	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISv1.4.0	NIST	CISv3.0.0	ID de controle de segurança
ASR-EncerrarEC2Instance EC2As instâncias interrompidas devem ser removidas após um período de tempo especificado	EC24.				EC24.		EC24.

Descrição	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISv1.4.0	NIST	CISv3.0.0	ID de controle de segurança
ASR-Habilitar IMDSV2Onnstance EC2as instâncias devem usar o Instance Metadata Service versão 2 () IMDSv2	EC28.				EC28.	5.6	EC28.

Descrição	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISv1.4.0	NIST	CISv3.0.0	ID de controle de segurança
ASR-RevokeUnauthorizedInboundRules Os grupos de segurança só devem permitir tráfego de entrada irrestrito para portas autorizadas	EC21.8				EC21.8		EC21.8

Descrição	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISv1.4.0	NIST	CISv3.0.0	ID de controle de segurança
ASR-DisableUnres t rictedAccessTo HighRiskPorts Grupos de segurança não devem permitir acesso irrestrito a portas com alto risco	EC21.9				EC21.9		EC21.9

Descrição	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISv1.4.0	NIST	CISv3.0.0	ID de controle de segurança
ASR-DisableTGWAutoAcceptSharedAttachments O Amazon EC2 Transit Gateways não deve aceitar automaticamente solicitações de VPC anexos	EC22.3				EC22.3		EC22.3

Descrição	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISv1.4.0	NIST	CISv3.0.0	ID de controle de segurança
ASR-EnablePrivateRepositoryScanning ECRrepositórios privados devem ter a digitalização de imagens configurada	ECR1.				ECR1.		ECR1.
ASR-EnableGuardDuty GuardDuty deve ser habilitado	GuardDuty 1.		GuardDuty 1.		GuardDuty 1.		GuardDuty 1.

Descrição	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISv1.4.0	NIST	CISv3.0.0	ID de controle de segurança
ASR-Configura S3 BucketLogging O registro em log de acesso ao servidor para bucket do S3 deve estar habilitado	S3.9				S3.9		S3.9

Descrição	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISv1.4.0	NIST	CISv3.0.0	ID de controle de segurança
ASR-EnablBucketEventNotifications Os buckets do S3 devem ter as notificações de eventos ativadas	S3.11				S3.11		S3.11
ASR-Conjuntos3LifecyclePolicy Os buckets do S3 devem ter políticas de ciclo de vida configuradas	S3.13				S3.13		S3.13

Descrição	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISv1.4.0	NIST	CISv3.0.0	ID de controle de segurança
ASR-EnableAutoSecretRotation Os segredos do Secrets Manager devem ter a alternância automática ativada	SecretsManager1.				SecretsManager1.		SecretsManager1.
ASR-RemoveUnusedSecret Remover segredos do Secrets Manager não utilizados	SecretsManager3.				SecretsManager3.		SecretsManager3.

Descrição	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISv1.4.0	NIST	CISv3.0.0	ID de controle de segurança
ASR-UpdateSecretRotationPeriod Os segredos do Secrets Manager devem ser alternados dentro de um determinado número de dias	SecretsManager4.				SecretsManager4.		SecretsManager4.

Descrição	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISv1.4.0	NIST	CISv3.0.0	ID de controle de segurança
ASR-EnableAPIGatewayCacheDataEncryption APIOs dados REST API do cache do gateway devem ser criptografados em repouso					APIGateway5.		APIGateway5.

Descrição	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISv1.4.0	NIST	CISv3.0.0	ID de controle de segurança
ASR-SetLogGroupRetentionDays CloudWatch os grupos de registros devem ser mantidos por um período de tempo especificado					CloudWatch1.6		CloudWatch1.6

Descrição	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISv1.4.0	NIST	CISv3.0.0	ID de controle de segurança
ASR-AttachServiceVPCEndpoint A Amazon EC2 deve ser configurada para usar VPC endpoints criados para o serviço Amazon EC2	EC2.10				EC2.10		EC2.10
ASR-TagGuardDutyResource GuardDuty os filtros devem ser marcados							GuardDuty 2.

Descrição	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISv1.4.0	NIST	CISv3.0.0	ID de controle de segurança
ASR-TagGuardDutyResource GuardDuty detectores devem ser marcados							GuardDuty 4.
ASR-UmttachSSMPermissions brinquedo EC2 EC2As instâncias da Amazon devem ser gerenciadas pelo Systems Manager	SSM1.		SSM3.				SSM1.

Descrição	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISv1.4.0	NIST	CISv3.0.0	ID de controle de segurança
ASR-ConfigureLaunchConfigNoPublicIPDocument EC2As instâncias da Amazon lançadas usando as configurações de lançamento em grupo do Auto Scaling não devem ter endereços IP públicos					Autoscaling.5		Autoscaling.5

Descrição	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISv1.4.0	NIST	CISv3.0.0	ID de controle de segurança
ASR-EnableAPIGateway Execution Logs	APIGateway1.						APIGateway1.
ASR-EnablEMacie O Amazon Macie deve ser habilitado	Macie.1				Macie.1		Macie.1

Descrição	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISv1.4.0	NIST	CISv3.0.0	ID de controle de segurança
ASR-EnablAthenaWorkGroupLogging Os grupos de trabalho do Athena devem ter o registro em log habilitado	Athena.4						Athena.4

Adicionando novas remediações

Adicionar uma nova remediação a um manual existente não exige modificações na solução em si.

> **Note**
>
> As instruções a seguir utilizam os recursos instalados pela solução como ponto de partida. Por convenção, a maioria dos nomes de recursos da solução contém SHARRe/ou SO0111 para facilitar sua localização e identificação.

Visão geral

A resposta de segurança automatizada em AWS runbooks deve seguir a seguinte nomenclatura padrão:

`ASR-<standard>-<version>-<control>`

Padrão: a abreviatura do padrão de segurança. Isso deve corresponder aos padrões suportados peloSHARR. Deve ser “CIS”, “AFSBP”, “PCI”, "NIST“ou “SC”.

Versão: A versão do padrão. Novamente, isso deve corresponder à versão suportada por SHARR e à versão nos dados de busca.

Controle: O ID de controle do controle a ser remediado. Isso deve corresponder aos dados de descoberta.

1. Crie um runbook na (s) conta (s) do membro.
2. Crie uma IAM função na (s) conta (s) do membro.
3. (Opcional) Crie uma regra de remediação automática na conta do administrador.

Etapa 1. Crie um runbook na (s) conta (s) do membro

1. Faça login no AWS Systems Manager console e obtenha um exemplo da descobertaJSON.
2. Crie um runbook de automação que corrija a descoberta. Na guia Propriedade minha, use qualquer um dos `ASR-` documentos na guia Documentos como ponto de partida.
3. AWS Step Functions Na conta de administrador, seu runbook será executado. Seu runbook deve especificar a função de remediação para ser aprovado ao chamar o runbook.

Etapa 2. Crie uma IAM função na (s) conta (s) do membro

1. Faça login no console do AWS Identity and Access Management.
2. Obtenha um exemplo das funções IAM SO0111 e crie uma nova função. O nome da função deve começar com `SO0111-Remediate-<standard>-<version>-<control>`. Por exemplo, se adicionar o controle 5.6 CIS v1.2.0, a função deve ser. `SO0111-Remediate-CIS-1.2.0-5.6`
3. Usando o exemplo, crie uma função com escopo adequado que permita somente as API chamadas necessárias para realizar a correção.

Neste momento, sua remediação está ativa e disponível para correção automatizada a partir da Ação SHARR Personalizada no AWS Security Hub.

Etapa 3: (Opcional) Crie uma regra de remediação automática na conta do administrador

A remediação automática (não “automatizada”) é a execução imediata da remediação assim que a descoberta é recebida pelo AWS Security Hub. Considere cuidadosamente os riscos antes de usar essa opção.

1. Veja um exemplo de regra para o mesmo padrão de segurança em CloudWatch Eventos. O padrão de nomenclatura para regras `éstandard_control_AutoTrigger`.
2. Copie o padrão de evento do exemplo a ser usado.
3. Altere o `GeneratorId` valor para corresponder ao `GeneratorId` da sua descobertaJSON.
4. Salve e ative a regra.

Adicionar um novo manual

Faça o download do Automated Security Response sobre os manuais da AWS solução e o código-fonte de implantação do GitHub repositório.

Os AWS CloudFormation recursos são criados a partir de AWS CDKcomponentes e contêm o código do modelo de manual que você pode usar para criar e configurar novos manuais. Para obter mais informações sobre como configurar seu projeto e personalizar seus playbooks, consulte o READMEarquivo.md em. GitHub

AWS Systems Manager Armazenamento de parâmetros

O Automated Security AWS Response on usa o AWS Systems Manager Parameter Store para armazenamento de dados operacionais. Os seguintes parâmetros são armazenados no Parameter Store:

Nome	Valor	Use
`/Solutions/SO0111/CMK_REMEDIATION_ARN`	AWS KMS chave que criptografará dados para remediações FSBP	Criptografia dos dados do cliente, como CloudTrail

Nome	Valor	Use
		registros, como parte das correções
/Solutions/SO0111/CMK_ARN	AWS KMS chave que SHARR será usada para criptografar dados	Criptografia dos dados da solução
/Solutions/SO0111/SNS_Topic_ARN	ARNdo SNS tópico Amazon para a solução	Notificação de eventos de remediação
/Solutions/SO0111/SNS_Topic_Config.1	SNStópico para AWS Config atualizações	Remediação do Config.1
/Solutions/SO0111/sendAnonymousMetrics	Yes	Coleção de métricas anônimas
/Solutions/SO0111/version	Versão da solução	
/Solutions/SO0111/ *<security standard long name>*/*<version>* /status	enabled	Indica se o padrão está ativo na solução. Um padrão pode ser desativado para remediação automatizada alterando-o para disabled
/Solutions/SO0111/ *<security standard long name>*/shortname	String	Nome abreviado do padrão de segurança. Por exemplo: 'CIS', 'AFSBP', 'PCI'
/Solutions/SO0111/ *<security standard long name>*/*<version>* /*<control>* /remap	String	Quando um controle usa a mesma remediação que outro, esses parâmetros realizam o remapeamento

SNSTópico da Amazon - Progresso da remediação

O Automated Security Response on AWS cria um SNS tópico da Amazon, SO0111- SHARR _Topic. Este tópico é usado para publicar atualizações sobre o progresso da remediação. A seguir estão as três possíveis notificações enviadas para esse tópico.

```
Remediation queued for <standard> control <control_ID> in account <account_ID>
```

```
Remediation failed for <standard> control <control_ID> in account <account_ID>
```

```
<control_ID> remediation was successfully invoke via AWS Systems Manager in
 account <account_ID>
```

Essa é a mensagem de conclusão. Isso indica que a remediação foi concluída sem erros; no entanto, o teste definitivo para uma remediação bem-sucedida é a verificação do AWS Config e/ou a validação manual.

Filtrando uma assinatura de SNS tópico

Políticas SNS de filtro de assinatura da Amazon:

1. Navegue até a assinatura do SNS tópico.
2. Em Política de filtro de assinatura, selecione “Editar”.
3. Expanda “Política de filtro de assinatura” e alterne a opção “Política de filtro de assinatura” para ativar os filtros.
4. Selecione o escopo “Corpo da mensagem”.
5. Adicione sua política ao JSON editor.
6. Salve as alterações.

Políticas de exemplo:

Filtrar por conta

```
{
    "finding": {
```

```
        "account": [
          "111111111111",
          "222222222222"
        ]
      }
```

Filtrar por erros

```
{
    "severity": ["ERROR"]
    }
```

Filtrar por controles

```
{
    "finding": {
       "standard_control": ["S3.9","S3.6"]
      }
   }
```

SNSTópico da Amazon — CloudWatch Alarmes

Essa solução cria um SNS tópico da Amazon,`SO0111-ASR_Alarm_Topic`. Este tópico é usado para publicar alertas de alarme.

Os detalhes de todos os alarmes que entrarem no ALARM estado serão enviados para este tópico.

Inicie o Runbook on Config Findings

Essa solução pode iniciar runbooks com base em descobertas personalizadas AWS Config . Para fazer isso, você precisará:

1. Encontre o nome da AWS Config regra que você gostaria de corrigir. Isso pode ser encontrado em uma AWS Config ou na descoberta que o Security Hub gera para essa regra.
2. Navegue até AWS Systems Manager Parameter Store e selecione Create Parameter.
3. O nome da sua regra deve ser `/Solutions/SO0111/`*`Rule name from Step 1`*
4. O valor deve ser formatado da seguinte forma:

```
{

"RunbookName":"Name of SSM runbook",

"RunbookRole": "Role that Orchestrator will assume"

}
```

5. RunbookName é um campo obrigatório e será o runbook executado quando você corrigir essa regra de Config. RunbookRole é a função que o orquestrador assumirá ao executar essa função. Não é um campo obrigatório e, se deixado de fora, o orquestrador usará como padrão a função de membro da conta.
6. Depois que isso estiver pronto, você poderá corrigir sua regra de Config usando a ação personalizada “Remediar ASR com” encontrada no Security Hub.

Referência

Esta seção inclui informações sobre um recurso opcional para coletar métricas exclusivas para essa solução, indicadores para recursos relacionados e uma lista dos criadores que contribuíram para essa solução.

Coleta de dados anônima

Essa solução inclui uma opção para enviar métricas operacionais anônimas para a AWS. Usamos esses dados para entender melhor como os clientes usam essa solução e os serviços e produtos relacionados. Quando ativada, as seguintes informações são coletadas e enviadas paraAWS:

- ID da solução - O identificador da AWS solução
- ID exclusivo (UUID) - Identificador exclusivo gerado aleatoriamente para cada implantação de AWS Security Hub resposta e remediação
- Timestamp - Timestamp de coleta de dados
- Dados da instância - Informações sobre a implantação dessa pilha
- CloudWatchMetricsDashboardEnabled- `"Yes"` se CloudWatch as métricas e o painel estiverem habilitados durante a implantação
- Status - Status da implantação (solução aprovada ou reprovada) ou (correção aprovada ou reprovada)
- Mensagem de erro - A mensagem de erro genérica no campo de status
- Generator_id - Informações sobre as regras do Security Hub
- Tipo - Tipo e nome da remediação
- productArn- A região onde o Security Hub está implantado
- finding_trigger _ by - O tipo de remediação realizada (ação personalizada ou gatilho automático)

AWSpossui os dados coletados por meio desta pesquisa. A coleta de dados está sujeita ao AWS Aviso de Privacidade. Para desativar esse recurso, conclua as etapas a seguir antes de iniciar o AWS CloudFormation modelo.

1. Baixe o modelo do AWS CloudFormation em seu disco rígido local.
2. Abra o AWS CloudFormation modelo com um editor de texto.

3. Modifique a seção AWS CloudFormation de mapeamento de modelos a partir de:

```
Mappings:
  Solution:
    Data:
      SendAnonymizedUsageData: 'Yes'
```

para:

```
  Mappings:
    Solution:
      Data:
        SendAnonymizedUsageData: 'No'
```

4. Faça login no console do AWS CloudFormation .
5. Selecione Criar pilha.
6. Na página Criar pilha, seção Especificar modelo, selecione Carregar um arquivo de modelo.
7. Em Carregar um arquivo de modelo, escolha Escolher arquivo e selecione o modelo editado em sua unidade local.
8. Escolha Avançar e siga as etapas em Iniciar a pilha na seção Implantação automatizada deste guia.

Recursos relacionados

- Resposta e remediação automatizadas com AWS Security Hub
- CISBenchmarks do Amazon Web Services Foundations, versão 1.2.0
- Padrão de práticas recomendas de segurança básica da AWS
- Padrão de segurança de dados do setor de cartões de pagamento (PCIDSS)
- Instituto Nacional de Padrões e Tecnologia (NIST) SP 800-53 Rev. 5

Colaboradores

As pessoas a seguir contribuíram na elaboração deste documento:

- Mike O'Brien
- Nikhil Reddy
- Chandini Penmetsa
- Chaitanya Deolankar
- Max Granat
- Tim Mekari
- Aaron Schuetter
- Andrew Yankowsky
- Josh Moss
- Ryan Garay
- Thiemo Belmega

Revisões

Data	Alteração
agosto de 2020	Lançamento inicial
Outubro de 2020	Informações adicionais sobre solução de problemas foram adicionadas ao Apêndice C.
Novembro de 2020	Instruções de implantação adicionadas para regiões da China; instruções atualizadas de implantação da solução para a conta de administrador do Security Hub; para obter mais informações, consulte o CHANGELOG arquivo.md no GitHub repositório.
abril de 2021	Versão v1.2.0: nova arquitetura de manual e novas correções foram adicionadas. FSBP Para obter mais informações, consulte o CHANGELOGarquivo.md no GitHub repositór io.
Maio de 2021	Versão v1.2.1: correção de um problema que afeta EC2 .2 e .7. EC2 Para obter mais informações, consulte o CHANGELOG arquivo.md no GitHub repositório.
Agosto de 2021	Versão v1.3.0: foi adicionado o manual PCI DSS v3.2.1. Foram adicionadas 17 novas remediações à CIS v1.2.0. Foram adicionad as quatro novas remediações aoFSBP. Convertido CIS para usar a nova arquitetu ra de playbook baseada em SSM runbooks. Instruções adicionadas para ampliar os Playbooks existentes com correções definidas pelo cliente. Para obter mais informações,

Data	Alteração
	consulte o CHANGELOGarquivo.md no GitHub repositório.
Setembro de 2021	Versão v1.3.1: `CreateLogMetricFilterAndAlarm.py` alterada para tornar as ações ativas, adicionar SNS notificação a. `SO0111-SHARR-LocalAlarmNotification` Alterou a correção CIS 2.8 para corresponder ao novo formato de dados de descoberta. Para obter mais informações, consulte o CHANGELOGarquivo.md no GitHub repositório.
Novembro de 2021	Versão v1.3.2: correções de bugs para os controles 3.1 a 3.14 da CIS v1.2.0. Para obter mais informações, consulte o CHANGELOG arquivo.md no GitHub repositório.
Dezembro de 2021	Versão v1.4.0: A solução agora pode ser implantada usando o. StackSets Agora há suporte para remediação entre regiões, além da entre contas. As IAM funções da conta do membro agora são mantidas quando a pilha é removida. Para obter mais informações, consulte o CHANGELOGarquivo.md no GitHub repositório.
Janeiro de 2022	Versão v1.4.1: correções de bugs. Para obter mais informações, consulte o CHANGELOG arquivo.md no GitHub repositório.
Janeiro de 2022	Versão v1.4.2: correções de bugs. Para obter mais informações, consulte o CHANGELOG arquivo.md no GitHub repositório.

Data	Alteração
Junho de 2022	Versão v1.5.0: correções adicionais. Para obter mais informações, consulte o CHANGELOG arquivo.md no GitHub repositório.
Dezembro de 2022	Versão 1.5.1 Alterações para mudar a criação de SSM documentos do recurso personali zado `CfnDocument` Lambda para o. Os prefixos dos nomes dos SSM documentos são atualizados para começar com ASR em vez deSHARR. Para obter mais informações, consulte o CHANGELOGarquivo.md no GitHub repositório.
Março de 2023	Versão 2.0.0: Foi adicionado suporte para controles de segurança e padrões CIS v1.4.0, cinco novas correções nos padrões, uma nova correção nos FSBP padrões CIS v1.2.0, a AppRegistry integração do catálogo de serviços e proteções adicionais para evitar falhas na implantação devido à limitação de documento s. SSM Para obter mais informações, consulte o CHANGELOGarquivo.md no GitHub repositór io.
Abril de 2023	Versão 2.0.1: Impacto mitigado causado pelas novas configurações padrão de propriedade de objetos do S3 (ACLsdesativadas) para todos os novos buckets do S3. Para obter mais informações, consulte o CHANGELOG arquivo.md no GitHub repositório.

Data	Alteração
Maio de 2023	Atualização da documentação: definições atualizadas do Well-Architected, orientaçã o adicional sobre onde implantar cada pilha, edição adicional de solução de problemas com remediação específica e exemplos de código atualizados na notificação. SNS
Julho de 2023	Atualização da documentação: atualizou o diagrama de arquitetura e os componentes da solução no fluxo de trabalho.
Outubro de 2023	Versão 2.0.2: versões atualizadas do pacote para resolver vulnerabilidades de segurança . Para obter mais informações, consulte o CHANGELOGarquivo.md no GitHub repositór io.
Novembro de 2023	Atualização da documentação: foi adicionad a a seção Confirmar as etiquetas de custo associadas à solução na AppRegistry seção Monitorando a solução com o AWS Service Catalog.
Março de 2024	Versão 2.1.0: foi adicionado suporte para o NIST padrão, adicionou 17 novas correções aos FSBP padrões, adicionou CloudWatc h painel para solução de monitoramento, adicionou manipulador de limitação à arquitetu ra, adicionou suporte aos parâmetros de entrada personalizáveis do Security Hub e adicionou suporte para remediar descobert as do Config. Para obter mais informações, consulte o CHANGELOGarquivo.md no GitHub repositório.

Data	Alteração
Abril de 2024	Versão 2.1.1: Atualizado para a ordem dos CloudFormation parâmetros e valores padrão Atualização da documentação. Referências adicionadas ao NIST padrão. Foram adicionad as informações sobre cotas de serviços de EventBridge regras. Para obter mais informaçõ es, consulte o CHANGELOGarquivo.md no GitHub repositório.
Junho de 2024	Versão 2.1.2: desativada AppRegistry em determinados manuais para evitar erros ao atualizar a solução. Para obter mais informaçõ es, consulte o CHANGELOGarquivo.md no GitHub repositório.
Setembro de 2024	Versão 2.1.3: Resolveu um problema nos scripts de remediação para EC2 .18 e EC2 .19 em que as regras do grupo de segurança IpProtocol definidas como -1 estavam sendo ignoradas incorretamente. Atualizou todos os tempos de execução do Python nos documento s de SSM remediação do Python 3.8 para o Python 3.11. Para obter mais informações, consulte o CHANGELOGarquivo.md no GitHub repositório.
Novembro de 2024	Versão 2.1.4: tempos de execução do Python atualizados em todos os runbooks de controle do Python 3.8 para o Python 3.11. Para obter mais informações, consulte o CHANGELOG arquivo.md no GitHub repositório.

Data	Alteração
Dezembro de 2024	Versão 2.2.0: Foi adicionada a integração do sistema de emissão de bilhetes, o CloudTrai l Action Log e o Playbook CIS 3.0.0. Painel e notificações aprimorados. Para obter mais informações, consulte o CHANGELOG arquivo.md no GitHub repositório.

Avisos

Os clientes são responsáveis por fazer uma avaliação independente das informações contidas neste documento. Este documento: (a) é apenas para fins informativos, (b) representa ofertas e práticas AWS atuais de produtos, que estão sujeitas a alterações sem aviso prévio, e (c) não cria nenhum compromisso ou garantia de AWS suas afiliadas, fornecedores ou licenciadores. AWS os produtos ou serviços são fornecidos “no estado em que se encontram”, sem garantias, representações ou condições de qualquer tipo, expressas ou implícitas. AWS as responsabilidades e obrigações para com seus clientes são controladas por AWS contratos, e este documento não faz parte nem modifica nenhum acordo entre AWS e seus clientes.

O Automated Security Response on AWS é licenciado sob os termos da Licença Apache Versão 2.0, disponível na The Apache Software Foundation.

As traduções são geradas por tradução automática. Em caso de conflito entre o conteúdo da tradução e da versão original em inglês, a versão em inglês prevalecerá.