AWS Security Hub Automated Response and Remediation

Implementation Guide

AWS Security Hub Automated Response and Remediation: Implementation Guide

Table of Contents

Automatically address security threats with predefined response and remediation actions in AWS Security Hub

Publication date: **August 2020 (last update (p. 39): August 2021)**

The continued evolution of security threats makes it difficult, expensive, and time-consuming for security teams to react. The AWS Security Hub Automated Response and Remediation solution helps you quickly react to address these threats by providing predefined response and remediation actions based on industry compliance standards and best practices.

This solution is an add-on solution that works with AWS Security Hub to provide a ready-to-deploy architecture and a library of automated playbooks. This solution makes it easier for AWS Security Hub customers to resolve common security findings and to improve their security posture in AWS.

You can select specific playbooks to deploy in your Security Hub primary account. Each playbook contains the necessary custom actions, Identity and Access Management (IAM) roles, Amazon CloudWatch Events, AWS Systems Manager automation documents, AWS Lambda functions, and AWS Step Functions needed to start a remediation workflow within a single AWS account, or across multiple accounts. Remediations work from the Actions menu in AWS Security Hub and allow authorized users to remediate a finding across all of their AWS Security Hub-managed accounts with a single click. For example, you can apply recommendations from the Center for Internet Security (CIS) AWS Foundations Benchmark, a compliance standard for securing AWS resources, to ensure passwords expire within 90 days and enforce encryption of event logs stored in AWS.

> **Note**
> Remediation is intended for emergent situations that require immediate action. This solution makes changes to remediate findings only when initiated by you via the AWS Security Hub Management console. To revert these changes, you must manually put resources back in their original state.
> When remediating AWS resources deployed as a part of the CloudFormation stack, be aware that this might cause a drift. When possible, remediate stack resources by modifying the code that defines the stack resources and updating the stack. For more information, refer to What is drift? in the *AWS CloudFormation User Guide*.

AWS Security Hub Automated Response and Remediation includes the playbook remediations for the security standards defined as part of the Center for Internet Security (CIS) AWS Foundations Benchmark v1.2.0 and AWS Foundational Security Best Practices (AFSBP) v.1.0.0, and Payment Card Industry Data Security Standard (PCI-DSS) v3.2.1. For more information, refer to Playbooks (p. 9).

This implementation guide discusses architectural considerations and configuration steps for deploying the AWS Security Hub Automated Response and Remediation solution in the Amazon Web Services (AWS) Cloud. It includes links to AWS CloudFormation templates that launch, configure, and run the AWS compute, network, storage, and other services required to deploy this solution on AWS, using AWS best practices for security and availability.

The guide is intended for IT infrastructure architects, administrators, and DevOps professionals who have practical experience architecting in the AWS Cloud.

Cost

You are responsible for the cost of the AWS services used to run the AWS Security Hub Automated Response and Remediation solution. As of April 2021, the cost for running this solution with the default settings in the US East (N. Virginia) AWS Region is approximately **$3.33 for 300 remediations/month, $26.83 for 3,000 remediations/month and $261.90 for 30,000 remediations/month**. Prices are subject to change. For full details, see the pricing page for each AWS service used in this solution.

> **Note**
> Many AWS Services include a Free Tier – a baseline amount of the service that customers can use at no charge. Actual costs may be more or less than the pricing examples provided.

The total cost to run this solution depends on the following factors:

- The number of AWS Security Hub member accounts
- The number of active automatically-invoked remediations
- The frequency of remediation

This solution uses the following AWS components, which incur a cost based on your configuration. Pricing examples are provided for small, medium, and large organizations.

Service	Free Tier	Pricing
AWS Systems Manager Automation - Step Count	100,000 steps per account per month	Beyond the free tier, each basic step is charged at $0.002 per step. For multi-account automations, all steps including those run in any child accounts are counted only in the originating account.
AWS Systems Manager Automation - Step Duration	5,000 seconds per month	Beyond the free tier, each `aws:executeScript` action step is charged at $0.00003 for every second after a free tier of 5,000 seconds per month.
AWS Systems Manager Automation - Storage	No free tier	$0.046 per GB per month
AWS Systems Manager Automation - Data Transfer	No free tier	$0.900 per GB transferred (for cross-account or out-of-Region)
AWS Security Hub - Security Checks	No free tier	First 100,000 checks/account/region/month costs $0.0010 per check Next 400,000 checks/account/region/month costs $0.00.0 per check Over 500,000 checks/account/region/month costs $0.0005 per check

Service	Free Tier	Pricing
AWS Security Hub - Finding Ingestion Events	First 10,000 events/account/region/month is free. Finding ingestion events associated with Security Hub's security checks.	Over 10,000 events/account/region/month costs $0.00003 per event
Amazon CloudWatch - Metrics	Basic Monitoring Metrics (at 5-minute frequency) 10 Detailed Monitoring Metrics (at 1-minute frequency) 1 Million API requests (not applicable to GetMetricData and GetMetricWidgetImage)	First 10,000 metrics costs $0.30 metric/month Next 240,000 metrics costs $0.10 metric/month Next 750,000 metrics costs $0.05 metric/month Over 1,000,000 metrics costs $0.02 metric/month
Amazon CloudWatch - Dashboard	3 Dashboards for up to 50 metrics per month	$3.00 per dashboard per month
Amazon CloudWatch - Alarms	10 Alarm metrics (not applicable to high-resolution alarms)	Standard Resolution (60 sec) costs $0.10 per alarm metric High Resolution (10 sec) costs $0.30 per alarm metric Standard Resolution Anomaly Detection costs $0.30 per alarm High Resolution Anomaly Detection costs $0.90 per alarm Composite costs $0.50 per alarm
Amazon CloudWatch - Logs Collection	5GB Data (ingestion, archive storage, and data scanned by Logs Insights queries)	$0.50 per GB
Amazon CloudWatch - Logs Storage	5GB Data (ingestion, archive storage, and data scanned by Logs Insights queries)	$0.005 per GB of data scanned
Amazon CloudWatch - Events	All events except custom events are included	$1.00 per million events for custom events $1.00 per million events for cross-account events
AWS Service Catalog	1,000 API calls per month	Over 1,000 API calls costs $0.0007 (14 calls for 1 cent)
AWS Lambda - Requests	1M free requests per month	$0.20 per 1M requests

Service	Free Tier	Pricing
AWS Lambda - Duration	400,000 GB-seconds of compute time per month	$0.0000166667 for every GB-second. The price for Duration depends on the amount of memory you allocate to your function. You can allocate any amount of memory to your function between 128MB and 10,240MB, in 1MB increments.
AWS Step Functions - State Transitions	4,000 free state transitions per month	$0.025 per 1,000 state transitions thereafter
Amazon EventBridge	All state change events published by AWS services are free	Custom events cost $1.00/ million custom events published Third-party (SaaS) events cost $1.00/million events published Cross-account events cost $1.00/million cross-account events sent
Amazon SNS	First 1 million Amazon SNS requests per month are free	$0.50 per 1 million requests thereafter

Pricing Examples (monthly)

Example 1: 300 remediations per month

- 10 accounts, 1 Region
- 30 remediations per account/region/month
- Total cost $3.33 per month

Service	Assumptions	Monthly Charges
AWS Systems Manager Automation	Steps: ~4 steps * 300 remediations * $0.002 = $2.40 Duration: 10s * 300 remediations * $0.00003 = $0.09	$2.49
AWS Security Hub	No billable services utilized	$0
Amazon CloudWatch Logs	300 remediations * $0.000002 = $0.0006 $0.0006 * 0.03 = $0.000018	< $0.01
AWS Service Catalog	No charge for portfolio	$0
AWS Lambda - Requests	300 remediations * 6 requests = 1,800 requests	$0.20

Service	Assumptions	Monthly Charges
	$0.20 * 1,000,000 requests = $0.20	
AWS Lambda - Duration	256M: 1.875 GB sec * 300 remediations * $0.0000167 = $0.009375	< $0.01
AWS Step Functions	15 state transitions * 300 remediations = 4,500 $0.025 * (4,500/1,000) state transitions = $0.1125	< $0.12
Amazon EventBridge Rules	No charge for rules	$0
Amazon SNS	$0.50 * 1,000,000 notifications = $0.50	$0.50
Total		**$3.33**

Example 2: 3,000 remediations per month

- 100 accounts, 1 Region
- 30 remediations per account/region/month
- Total cost $26.75 per month

Service	Assumptions	Monthly Charges
AWS Systems Manager Automation	Steps: ~4 steps * 3,000 remediations * $0.002 = $24.00 Duration: 10s * 3,000 remediations * $0.00003 = $0.90	$24.90
AWS Security Hub	No billable services utilized	$0
Amazon CloudWatch Logs	3,000 remediations * $0.000002 = $0.006 $0.006 * 0.03 = $0.00018	< $0.01
AWS Service Catalog	No charge for portfolio	$0
AWS Lambda - Requests	3,000 remediations * 6 requests = 18,000 requests $0.20 * 1,000,000 requests = $0.20	$0.20
AWS Lambda - Duration	256M: 1.875 GB sec * 3,000 remediations * $0.000167 = $0.09375	$0.09
AWS Step Functions	15 state transitions * 3,000 remediations = 45,000	$1.13

Service	Assumptions	Monthly Charges
	$0.025 * (45,000/1,000) state transitions = $1.125	
Amazon EventBridge Rules	No charge for rules	$0
Amazon SNS	$0.50 * 1,000,000 notifications = $0.50	$0.50
Total		**$26.83**

Example 3: 30,000 remediations per months

- 1000 accounts, 1 Region
- 30 remediations per account/region/month
- Total cost $261.90 per month

Service	Assumptions	Monthly Charges
AWS Systems Manager Automation	Steps: ~4 steps * 30,000 remediations * $0.002 = $240.00 Duration: 10s * 30,000 remediations * $0.00003 = $9.00	$249.00
AWS Security Hub	No billable services utilized	$0
Amazon CloudWatch Logs	30,000 remediations * $0.000002 = $0.06 $0.06 * 0.03 = $0.0018	< $0.01
AWS Service Catalog	No charge for portfolio	$0
AWS Lambda - Requests	30,000 remediations * 6 requests = 180,000 requests $0.20 * 1,000,000 requests = $0.20	$0.20
AWS Lambda - Duration	256M: 1.875 GB sec * 30,000 remediations * $0.000167 = $0.9375	$0.94
AWS Step Functions	15 state transitions * 30,000 remediations = 450,000 $0.025 * (450,000/1,000) state transitions = $11.25	$11.25
Amazon EventBridge Rules	No charge for rules	$0
Amazon SNS	$0.50 * 1,000,000 notifications = $0.50	$0.50
Total		**261.90**

Architecture overview

Deploying this solution **with the default parameters** builds the following environment in the AWS Cloud.

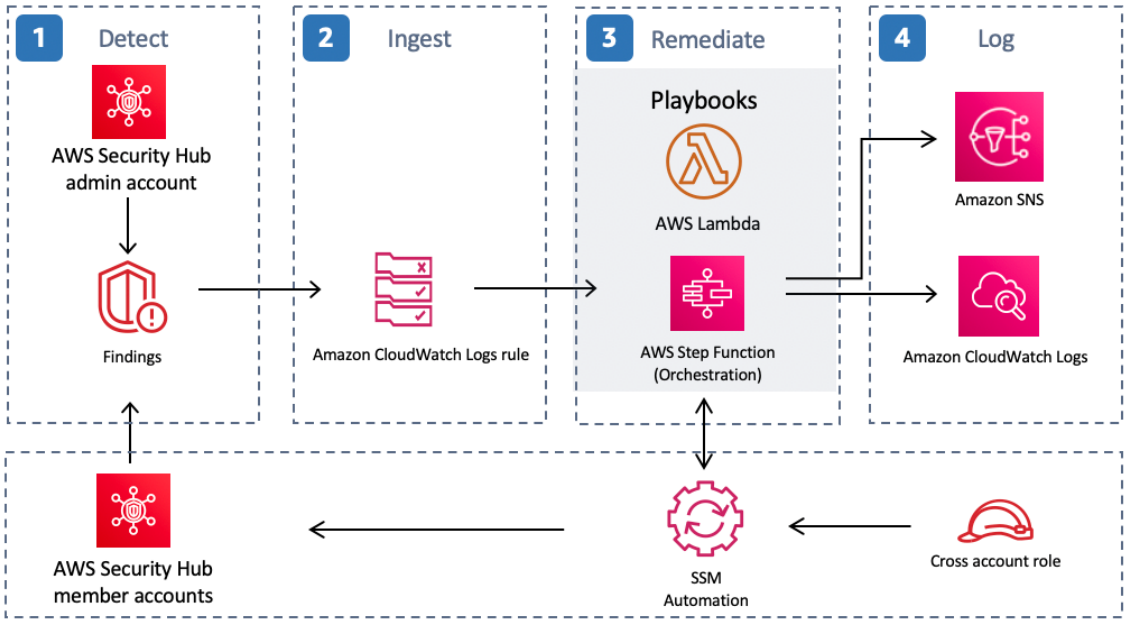

Figure 1: Security Hub Automatic Response and Remediation architecture

The AWS Security Hub Automated Response and Remediation solution contains the following main workflows: detect, ingest, remediate, and log.

1. Detect

AWS Security Hub provides customers with a comprehensive view of their AWS security state. It helps them to measure their environment against security industry standards and best practices. It works by collecting events and data from other AWS services, such as AWS Config, Amazon Guard Duty, and AWS Firewall Manager. These events and data are analyzed against security standards, such as CIS AWS Foundations Benchmark. Exceptions are asserted as *findings* in the AWS Security Hub console. New findings are sent as Amazon CloudWatch Events.

2. Ingest

AWS Security Hub customers can initiate events against findings using custom actions, which result in Amazon CloudWatch Events.

AWS Security Hub Custom Actions and Amazon CloudWatch Event Rules initiate Security Hub Automated Response and Remediation playbooks to address findings. Two CloudWatch Event Rules are deployed for each supported control by the solution: one rule to match the custom action event (user-initiated remediation), and one rule (disabled by default) to match the real-time finding event.

You can use the Security Hub Custom Action menu to initiate automated remediation, or after careful testing in a non-production environment, they can activate automated remediations. This can be activated per remediation – it is not necessary to activate automatic initiations on all remediations.

3. Remediate

Using cross-account Identity and Access Management (IAM) roles, the automated remediation uses the AWS API to perform the tasks needed to remediate findings. All playbooks in this solution call AWS Lambda functions. Some Lambda functions perform remediation directly. Others use AWS Systems Manager automation documents to perform the remediations.

4. Log

The playbook logs the results to the Amazon CloudWatch Log Group for the solution, sends a notification to an Amazon Simple Notification Service (Amazon SNS) topic, and updates the Security Hub finding. An audit trail of actions taken is maintained in the finding notes. On the Security Hub dashboard, the finding workflow status is changed from **NEW** to either **NOTIFIED** or **RESOLVED** on the Security Hub dashboard. The security finding notes are updated to reflect the remediation performed.

Solution components

AWS Security Hub integration

Deploying the `aws-sharr-deploy` stack creates integration with AWS Security Hub's custom action feature. When AWS Security Hub console users select **Findings for remediation**, the solution routes the finding record for remediation using an AWS Step Functions.

Cross-account permissions and AWS Systems Manager runbooks must be deployed to all AWS Security Hub accounts (admin and member) using the `aws-sharr-member.template` CloudFormation template. For more information, refer to Playbooks (p. 9). This template allows automated remediation in the target account.

Users can automatically initiate automated remediations on a per-remediation basis using Amazon CloudWatch Events Rules. This option activates fully automatic remediation of findings as soon as they are reported to AWS Security Hub. By default, automatic initiations are turned off. This option can be changed at any time during or after installation of the playbook.

If you don't want to implement specific remediations within a Playbook, you can deactivate the installation of the remediation runbook in the target account(s) by updating the nested stack under the member stack.

Cross-account remediation

AWS Security Hub Automated Response and Remediation uses cross-account roles to work across primary and secondary accounts using cross-account roles. These roles are deployed to member accounts during solution installation using a spoke template. Each remediation is assigned an individual role. The remediation process in the primary account is granted permission to assume the corresponding role in the account that requires remediation. Remediation is performed by AWS Lambda functions, AWS Lambda Step Functions, or AWS Systems Manager Runbooks.

Playbooks

A set of remediations is grouped into a package called a *playbook*. Playbooks are installed, updated, and removed using AWS Service Catalog. AWS Security Hub Response and Remediation Version currently supports the following playbook:

- Center for Internet Security (CIS) Amazon Web Services Foundations benchmarks, version 1.2.0, published May 18, 2018. For more information, refer to CIS v1.2.0 playbook (p. 22).
- AWS Foundational Security Best Practices (AFSBP) version 1.0.0, published March 2021. For more information, refer to AFSBP v1.0.0 playbook (p. 23).
- Payment Card Industry Data Security Standard (PCI-DSS), version 3.2.1, published May 2018. For more information, refer to PCI-DSS v.3.2.1 playbook (p. 24).

Centralized logging

AWS Security Hub Automated Response and Remediation logs to a single CloudWatch Logs group, SO0111-SHARR. These logs contain detailed logging from the solution for troubleshooting and management of the solution.

Notifications

AWS Security Hub Automated Response and Remediation uses an Amazon Simple Notification Service (Amazon SNS) topic to publish remediation results. You can use subscriptions to this topic to extend the capabilities of the solution. For example, you can send email notifications and update trouble tickets.

Security

When you build systems on AWS infrastructure, security responsibilities are shared between you and AWS. This shared model reduces your operational burden because AWS operates, manages, and controls the components including the host operating system, the virtualization layer, and the physical security of the facilities in which the services operate. For more information about AWS security, visit the AWS Cloud Security.

IAM roles

AWS Identity and Access Management (IAM) roles allow customers to assign granular access policies and permissions to services and users in the AWS Cloud. This solution creates IAM roles that grant the solution's automated functions access to perform remediation actions within a narrow scope set of permissions specific to each remediation.

The Admin account's Step Function is assigned to the `SO0111-SHARR-Orchestrator-Admin_`*`Region_name`* role. Only this role is allowed to assume the `SO0111- Orchestrator-Member_`*`Region_name`* in each member account. The member role is allowed by each remediation role to pass it to the AWS Systems Manager service to run specific remediation runbooks. Remediation role names begin with `SO0111`, followed by a description matching the name of the remediation runbook. For example, `SO0111- RemoveVPCDefaultSecurityGroupRules_`*`us-east-1`* is the role for the `SHARR_ RemoveVPCDefaultSecurityGroupRules` remediation runbook.

Design considerations

AWS Security Hub deployment

AWS Security Hub deployment and configuration is a prerequisite for this solution. For more information about setting up AWS Security Hub, refer to Setting up AWS Security Hub in the *AWS Security Hub User Guide.*

At minimum, you must have a working Security Hub configured in their primary account. You can deploy this solution in the same account (and AWS Region) as the Security Hub primary account. In each Security Hub primary and secondary account, you must also deploy a spoke template that allows `AssumeRule` permissions to the solution's AWS Lambda functions.

Solution updates

To upgrade this solution to the latest version, you must delete the existing stack first and then reinstall the latest version of the stack. For deletion instructions, refer to Uninstall the solution (p. 35).

Regional deployments

This solution uses AWS Service Catalog and Systems Manager, which are currently available in specific AWS Regions only. The solution works in all of the Regions that support these services. For the most current availability by Region, refer to the AWS Regional Services List.

AWS CloudFormation templates

This solution uses AWS CloudFormation to automate the deployment of the AWS Security Hub Automated Response and Remediation solution in your AWS account. It includes the following AWS CloudFormation templates, which you can download before deployment.

Core solution

aws-sharr-deploy.template: Use this template to launch the AWS Security Hub Automated Response and Remediation solution. The template installs the core components of the solution, a nested stack for the AWS Step Functions logs, and one nested stack for each security standard you choose to activate.

Services used include AWS Service Catalog, Amazon Simple Notification Service, AWS Key Management Service, AWS Identity and Access Management, AWS Lambda, Amazon CloudWatch Logs, Amazon S3, and AWS Systems Manager.

Admin account support

The following templates are installed in the AWS Security Hub Admin account to turn on the security standards that you want to support. You can choose which of the following templates to install when installing the `aws-sharr-deploy.template`.

aws-sharr-orchestrator-log.template: Creates a CloudWatch logs group for the Orchestrator Step Function.

AFSBPStack.template: AWS Foundational Security Best Practices v1.0.0 rules.

CIS120Stack.template: CIS Amazon Web Services Foundations benchmarks, v1.2.0 rules.

PCI321Stack.template: PCI-DSS v3.2.1 rules.

Member accounts

aws-sharr-member.template: Use this template after you set up the core solution to install AWS Systems Manager automation runbooks and permissions in each of your AWS Security Hub member accounts (including the Admin account). This template allows you to choose which security standard playbooks to install.

The `aws-sharr-member` template installs the following templates based on your selections:

aws-sharr-remediations.template: Common remediation code used by one or more of the security standards.

AFSBPMemberStack.template: AWS Foundational Security Best Practices v1.0.0 settings, permissions, and remediation runbooks.

CIS120MemberStack.template: CIS Amazon Web Services Foundations benchmarks, version 1.2.0 settings, permissions, and remediation runbooks.

PCI321MemberStack.template: PCI-DSS v3.2.1 settings, permissions, and remediation runbooks.

Automated deployment

Before you launch the solution, review the architecture, solution components, security, and design considerations discussed in this guide. Follow the step-by-step instructions in this section to configure and deploy the solution into your account.

Time to deploy: Approximately 15 minutes

Prerequisites

Before you deploy this solution, ensure that AWS Security Hub is in the same AWS Region as your primary and secondary accounts. If you have previously deployed this solution, you must uninstall the existing solution. For more information, refer to Solution updates (p. 12).

Deployment overview

Use the following steps to deploy this solution on AWS.

Step. 1 Launch the Admin stack (p. 15)

- Launch the `aws-sharr-deploy.template` AWS CloudFormation template into your AWS Security Hub Admin account.
- Choose which Security Standards to install.
- Choose an existing Orchestrator log group to use (select **Yes** if `SO0111-SHARR- Orchestrator` already exists from a previous installation).

Step. 2. Launch the Member stack (p. 17)

- Specify the name of the CloudWatch Logs group to use with CIS 3.1-3.14 remediations. It must be the name of a CloudWatch Logs log group that receives CloudTrail logs.
- Select which Playbooks to install.
- Enter the account ID of the AWS Security Hub Admin account.

Step. 3 (Optional) Adjust the available remediations (p. 19)

- Remove any remediations on a per-member account basis. This is step is optional.

Step 1. Launch the Admin stack

Important
This solution includes an option to send anonymous operational metrics to AWS. We use this data to better understand how customers use this solution and related services and products.

AWS owns the data gathered though this survey. Data collection is subject to the AWS Privacy Policy.
To opt out of this feature, download the template, modify the AWS CloudFormation mapping section, and then use the AWS CloudFormation console to upload your template and deploy the solution. For more information, refer to the Collection of operational metrics (p. 36) section of this guide.

This automated AWS CloudFormation template deploys the AWS Security Hub Automated Response and Remediation solution in the AWS Cloud. Before you launch the stack, you must enable Security Hub and complete the prerequisites (p. 15).

Note
You are responsible for the cost of the AWS services used while running this solution. For more details, visit to the Cost (p. 2) section in this guide, and refer to the pricing webpage for each AWS service used in this solution.

1. Sign in to the AWS Management Console from the account where the AWS Security Hub is currently configured, and use the button below to launch the `aws-sharr-deploy.template` AWS CloudFormation template.

   Launch Solution

   You can also download the template as a starting point for your own implementation.
2. The template launches in the US East (N. Virginia) Region by default. To launch this solution in a different AWS Region, use the Region selector in the AWS Management Console navigation bar.

   Note
   This solution uses AWS Service Catalog, and AWS Systems Manager which are currently available in specific AWS Regions only. The solution works in all of the Regions that support these services. For the most current availability by Region, refer to the AWS Regional Services List.
3. On the **Create stack** page, verify that the correct template URL is in the **Amazon S3 URL** text box and then choose **Next**.
4. On the **Specify stack details** page, assign a name to your solution stack. For information about naming character limitations, refer to IAM and STS limits in the *AWS Identity and Access Management User Guide*.
5. On the **Parameters** page, choose **Next**.

   - For each security standard, specify whether to install the Admin components for automated remediation.
   - Select whether or not to reuse an existing `SO0111-SHARR-Orchestrator` CloudWatch Logs group. This simplifies reinstallation and upgrades without losing log data from a previous version. If you are upgrading from v1.2 or above, choose **Yes**.

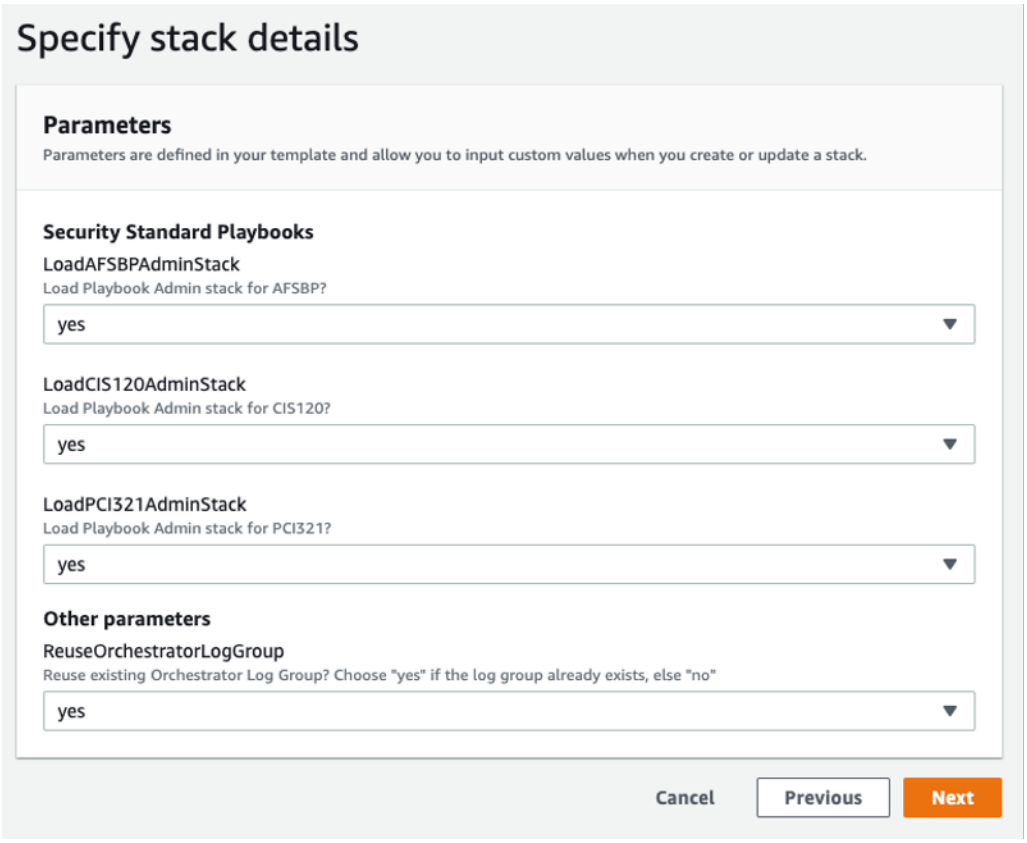

Figure 2: Admin stack details

6. On the **Configure stack options** page, choose **Next**.
7. On the **Review** page, review and confirm the settings. Check the box acknowledging that the template will create AWS Identity and Access Management (IAM) resources.
8. Choose **Create stack** to deploy the stack.

You can view the status of the stack in the AWS CloudFormation console in the **Status** column. You should receive a CREATE_COMPLETE status in approximately 15 minutes.

Step 2. Launch the Member stack

Important
This solution includes an option to send anonymous operational metrics to AWS. We use this data to better understand how customers use this solution and related services and products. AWS owns the data gathered though this survey. Data collection is subject to the AWS Privacy Policy.
To opt out of this feature, download the template, modify the AWS CloudFormation mapping section, and then use the AWS CloudFormation console to upload your template and deploy the solution. For more information, refer to the Collection of operational metrics (p. 36) section of this guide.

The `aws-sharr-member` stack must be installed into each Security Hub member account. This stack defines the permissions and runbooks for automated remediation. The admin for each member account can control what remediations are available via this stack.

1. Sign in to the AWS Management Console from the account where the AWS Security Hub is currently configured, and use the button below to launch the `aws-sharr-member.template` AWS CloudFormation template.

   

   You can also download the template as a starting point for your own implementation.

2. The template launches in the US East (N. Virginia) Region by default. To launch this solution in a different AWS Region, use the Region selector in the AWS Management Console navigation bar.

   Note
   This solution uses AWS Service Catalog, and AWS Systems Manager which are currently available in specific AWS Regions only. The solution works in all of the Regions that support these services. For the most current availability by Region, refer to the AWS Regional Services List.

3. On the **Create stack** page, verify that the correct template URL is in the **Amazon S3 URL** text box and then choose **Next**.
4. On the **Specify stack details** page, assign a name to your solution stack. For information about naming character limitations, refer to IAM and STS limits in the *AWS Identity and Access Management User Guide*.
5. On the **Parameters** page, specify the following parameters and choose **Next**.

   - Specify the name of a AWS CloudFormation Logs group where CloudTrail logs API calls. This is used for CIS 3.1-3.14 remediations.
   - For each security standard, indicate whether to install the member stack components for automated remediation, which includes IAM roles and AWS Systems Manager runbooks..
   - Enter the 12-digit account ID for the AWS Security Hub Admin account. This value grants permissions to the Admin account's solution role.

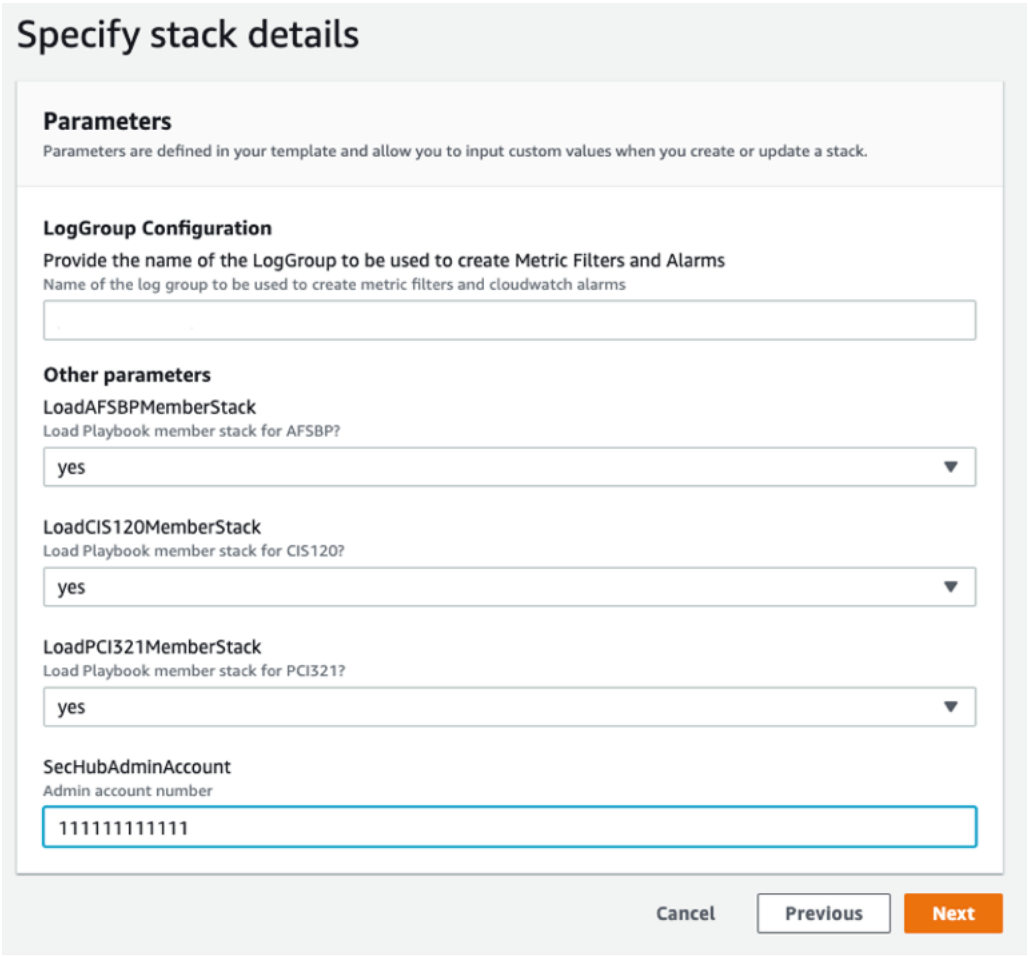

Figure 3: Member stack details

6. On the **Configure stack options** page, choose **Next**.
7. On the **Review** page, review and confirm the settings. Check the box acknowledging that the template will create AWS Identity and Access Management (IAM) resources.
8. Choose **Create stack** to deploy the stack.

You can view the status of the stack in the AWS CloudFormation console in the **Status** column. You should receive a CREATE_COMPLETE status in approximately 15 minutes.

Step 3: (Optional) Adjust the available remediations

If you want to remove specific remediations from a member account, you can do so by updating the nested stack for the security standard. For simplicity, the nested stack options are not propagated to the root stack.

1. Sign in to the AWS CloudFormation console and select the nested stack.
2. Choose **Update**.

3. Select **Update nested stack** and choose **Update stack**.

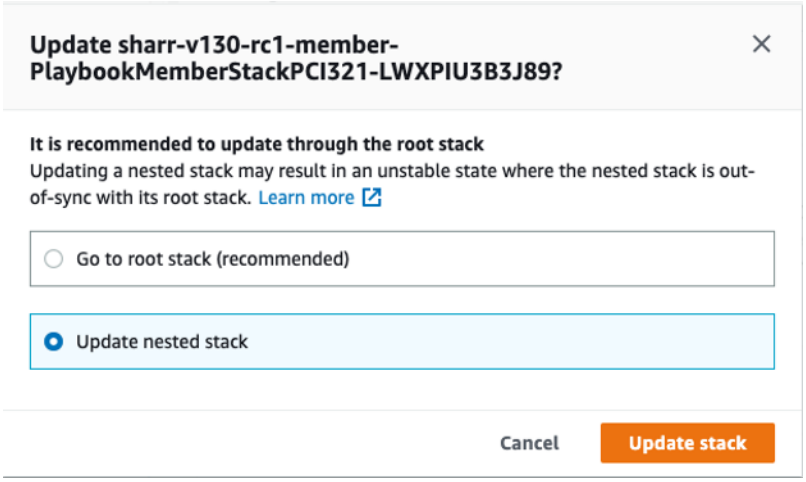

Figure 4: Update nested stack

4. Select **Use current template** and choose **Next**.
5. Adjust the available remediations.

   Note
   Turning off a remediation removes the solutions remediation runbook for the security standard and control.

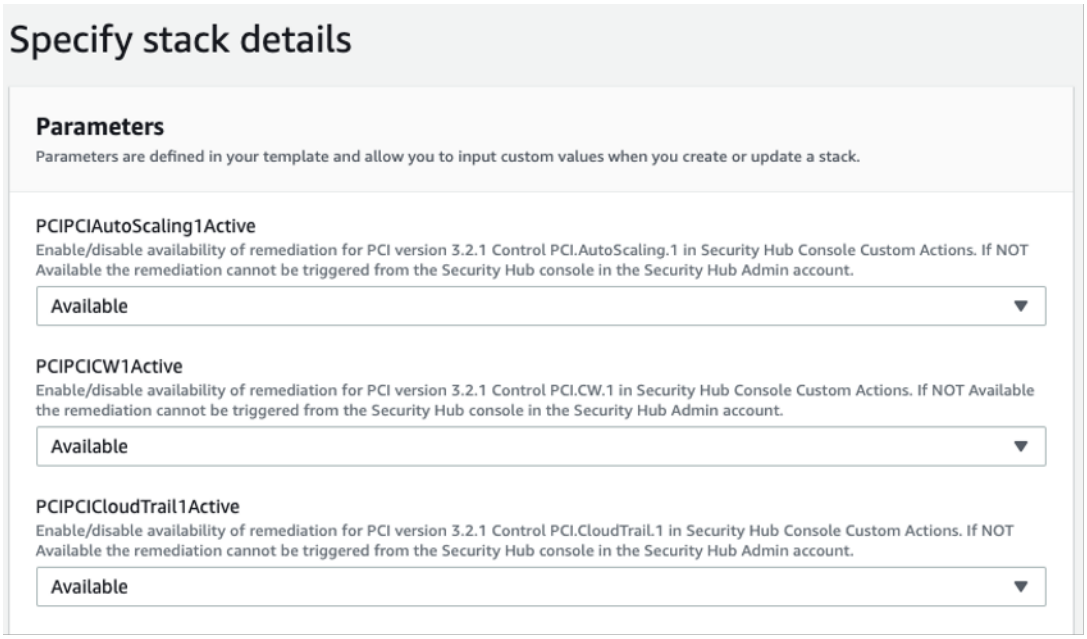

Figure 5: Adjust available remediations

6. On the **Configure stack options** page, choose **Next**.
7. On the **Review** page, review and confirm the settings. Check the box acknowledging that the template will create AWS Identity and Access Management (IAM) resources.
8. Choose **Update stack**.

You can view the status of the stack in the AWS CloudFormation console in the **Status** column. You should receive a CREATE_COMPLETE status in approximately 15 minutes.

Additional resources

AWS services

- AWS Security Hub
- AWS CloudFormation
- AWS Key Management Service
- AWS Lambda
- Amazon CloudWatch Events
- CloudWatch Logs
- AWS Step Functions
- AWS Systems Manager
- Amazon Simple Notification Service
- AWS Identity and Access Management
- AWS CDK

Related Resources

- Automated Response and Remediation with AWS Security Hub
- CIS Amazon Web Services Foundations benchmarks, version 1.2.0
- AWS Foundational Security Best Practices standard
- Payment Card Industry Data Security Standard (PCI DSS)

Playbooks

This solution includes the playbook remediations for the security standards defined as part of the Center for Internet Security (CIS) AWS Foundations Benchmark v1.2.0, AWS Foundation Security Best Practices (AFSBP) v.1.0.0, and Payment Card Industry Data Security Standard (PCI-DSS) v3.2.1. For more details about remediations, review the following list under each playbook.

CIS v1.2.0 playbook

The CIS v1.2.0 playbook includes the following list of remediations for the Center for Internet Security's (CIS) Amazon Web Services Foundations benchmarks, version 1.2.0, published May 18, 2018. For more information, refer to the CIS Benchmarks.

- 1.3 – Ensure credentials unused for 90 days or greater are disabled
- 1.5 – Ensure IAM password policy requires at least one uppercase letter
- 1.6 – Ensure IAM password policy requires at least one lowercase letter
- 1.7 – Ensure IAM password policy requires at least one symbol
- 1.8 – Ensure IAM password policy requires at least one number
- 1.9 – Ensure IAM password policy requires a minimum length of 14 or greater
- 1.10 – Ensure IAM password policy prevents password reuse
- 1.11 – Ensure IAM password policy expires passwords within 90 days or less
- 2.1 – Ensure AWS CloudTrail is enabled in all Regions
- 2.2 – Ensure AWS CloudTrail log file validation is activated
- 2.3 – Ensure the S3 bucket CloudTrail logs to is not publicly accessible
- 2.4 – Ensure CloudTrail trails are integrated with Amazon CloudWatch Logs
- 2.5 – Ensure AWS Config is turned on
- 2.6 – Ensure S3 bucket access logging is activated on the CloudTrail S3 bucket
- 2.7 – Ensure CloudTrail logs are encrypted at rest using AWS AWS KMS CMKs
- 2.8 – Ensure rotation for customer created CMKs is activated
- 2.9 – Ensure VPC flow logging is activated in all VPCs
- 3.1 – Ensure a log metric filter and alarm exist for unauthorized API calls
- 3.2 – Ensure a log metric filter and alarm exist for AWS Management Console sign-in without MFA
- 3.3 – Ensure a log metric filter and alarm exist for usage of "root" account
- 3.4 – Ensure a log metric filter and alarm exist for IAM policy changes
- 3.5 – Ensure a log metric filter and alarm exist for CloudTrail configuration changes
- 3.6 – Ensure a log metric filter and alarm exist for AWS Management Console authentication failures
- 3.7 – Ensure a log metric filter and alarm exist for disabling or scheduled deletion of customer created CMKs
- 3.8 – Ensure a log metric filter and alarm exist for S3 bucket policy changes
- 3.9 – Ensure a log metric filter and alarm exist for AWS Config configuration changes
- 3.10 – Ensure a log metric filter and alarm exist for security group changes
- 3.11 – Ensure a log metric filter and alarm exist for changes to Network Access Control Lists (NACL)
- 3.12 – Ensure a log metric filter and alarm exist for changes to network gateways

- 3.13 – Ensure a log metric filter and alarm exist for route table changes
- 3.14 – Ensure a log metric filter and alarm exist for Amazon VPC changes
- 4.1 – Ensure no security groups allow ingress from 0.0.0.0/0 to port 22
- 4.2 – Ensure no security groups allow ingress from 0.0.0.0/0 to port 3389
- 4.3 – Ensure the default security group of every VPC restricts all traffic

AWS Foundational Security Best Practices v1.0.0 playbook

The AWS Foundational Security Best Practices security standard implements security controls that detect when your AWS accounts and deployed resources do not align with the security best practices defined by AWS security experts, which allows you to monitor your own security posture to ensure that you are using AWS security best practices. These controls closely align to the Top 10 Security Best Practices outlined by AWS Chief Information Security Office, Stephen Schmidt, at AWS re:Invent 2019. For more details, review the following list of remediations.

- Autoscaling.1 - Auto Scaling groups associated with a load balancer should use load balancer health checks

  Actions: Enables ELB Health Checks on the AutoScaling Group that is the subject of the finding
- CloudTrail.1 – CloudTrail should be activated and configured with at least one multi-Region trail

  The CloudTrail.1 remediation creates a new, multi-Region CloudTrail in the Security Hub Admin account's Region. Any existing CloudTrail will not be modified. This might result in duplicate logging, which can drive additional costs in the AWS account. If you have more than one CloudTrail, you should take steps to consolidate them to prevent the additional costs.

  Actions: creates a KMS CMK-encrypted, multi-Region CloudTrail in the Security Hub Admin account's Region. The new trail logs to an encrypted S3 bucket, `so0111-aws-cloudtrail-<accountid>`. Access logs for the CloudTrail bucket are logged to `so0111-access-logs-<region>-<accountid>`. Both buckets have public access blocked.
- CloudTrail.2 – CloudTrail should have encryption at-rest activated

  Actions: Enables KMS CMK encryption on the CloudTrail logs
- Config.1 – AWS Config should be activated

  The Config.1 remediation creates a set of resources using reasonable defaults. The Config.1 remediation uses reasonable defaults and resource names that are logical and can be easily related to the solution. You can also reconfigure AWS Config to your own established buckets.

  Actions: The Config.1 remediation creates a set of resources using reasonable defaults. The Config.1 remediation uses reasonable defaults and resource names that are logical and can be easily related to the solution. You can also reconfigure AWS Config to your own established buckets.

  S3 buckets for AWS Config and access logging to the AWS Config bucket use AES-256 server-side encryption. These buckets are created per Region, per account to avoid inter-Region data transfer. You can also reconfigure AWS Config to use their own centralized logging buckets.
  - AWS Config bucket: `so0111-aws-config-<region>-<accountid>`
  - Access logging bucket: `so0111-access-logs-<region>-<accountid>`
  - Service-linked role: `AWSServiceRoleForConfig`
- EC2.1 - Amazon EBS snapshots should not be public, determined by the ability to be restorable by anyone

Actions: An account-level finding, this runbook will make all EBS snapshots private

- EC2.2 - The VPC default security group should not allow inbound and outbound traffic

  Actions: Removes ALL TRAFFIC inbound and outbound rules on the default Security Group that is the subject of the finding
- EC2.6 - VPC flow logging should be enabled in all VPCs

  Actions: Enables VPC Flow Logs for the Amazon VPC in the finding
- EC2.7 - EBS default encryption should be activated

  Actions: Enables EBS encryption as the account-wide default
- IAM.7 - Password policies for IAM users should have strong configurations

  Actions: Sets default password policy for the account in the finding.
- IAM.8 - Unused IAM user credentials should be removed

  Actions: Disables credentials unused for more than 90 days.
- Lambda.1 - Lambda function policies should prohibit public access

  Actions: Removes any Resource Policy statement with “Principal: *” from the Lambda that is the subject of the finding
- RDS.1 - RDS snapshots should be private

  Actions: Removes public sharing for the RDS snapshot (cluster or database) that is the subject of the finding
- RDS.6 - Enhanced monitoring should be configured for RDS DB instances and clusters

  Actions: Enables enhanced monitoring for the RDS cluster
- RDS.7 - RDS clusters should have deletion protection activated

  Actions: Enables deletion protection for the RDS database
- S3.1 - S3 Block Public Access setting should be turned on

  Actions: Establishes S3 public access blocks by default at the account level
- S3.2 - S3 buckets should prohibit public read access
- S3.3 - S3 buckets should prohibit public write access

  Actions: Blocks public read and write access to the bucket in the finding

Payment Card Industry Data Security Standards (PCI-DSS) v3.2.1 Playbook

The Payment Card Industry Data Security Standard (PCI DSS) v3.2.1 is an information security standard for entities that store, process, and/or transmit cardholder data. This AWS Security Hub standard automatically checks for your compliance readiness against a subset of PCI DSS requirements. The PCI DSS playbook allows you to perform automated remediation of findings for many of the following controls.

- Autoscaling.1 - Auto Scaling groups associated with a load balancer should use load balancer health checks

  Actions: Enables ELB Health Checks on the AutoScaling Group that is the subject of the finding

- CloudTrail.1 – CloudTrail logs should be encrypted at rest using AWS AWS KMS CMKs

  Actions: Applies encryption to the finding's CloudTrail using an AWS KMS customer-managed key. The key ID can be obtained from AWS Systems Manager parameter `/Solutions/SO0111/CMK_REMEDIATION_ARN` (refer to AWS Systems Manager Parameter Store). This key is unique for each Member account.
- CloudTrail.2 – CloudTrail should be enabled

  The CloudTrail.1 remediation creates a new, multi-Region CloudTrail in the Security Hub Admin account's Region. Any existing CloudTrail will not be modified. This might result in duplicate logging, which can drive additional costs in the AWS account. If you have more than one CloudTrail, you should take steps to consolidate them to prevent the additional costs.

  Actions: Creates a KMS CMK-encrypted, multi-Region CloudTrail in the Security Hub Admin account's Region. The new trail logs to an encrypted S3 bucket, `so0111-aws-cloudtrail-<accountid>`. Access logs for the CloudTrail bucket are logged to `so0111-access-logs-<region>-<accountid>`. Both buckets have public access blocked.
- CloudTrail.3 – CloudTrail log file validation should be enabled

  Actions: Enables CloudTrail log file validation for the CloudTrail in the finding
- CloudTrail.4 – CloudTrail trails should be integrated with CloudWatch Logs

  Actions: Configures CloudTrail to write logs to CloudWatch Logs
- Config.1 – AWS Config should be activated

  The Config.1 remediation creates a set of resources using reasonable defaults. The Config.1 remediation uses reasonable defaults and resource names that are logical and can be easily related to the solution. You can also reconfigure AWS Config to your own established buckets.

  Actions: The Config.1 remediation creates a set of resources using reasonable defaults. The Config.1 remediation uses reasonable defaults and resource names that are logical and can be easily related to the solution. You can also reconfigure AWS Config to your own established buckets.

  S3 buckets for AWS Config and access logging to the AWS Config bucket use AES-256 server-side encryption. These buckets are created per Region, per account to avoid inter-Region data transfer. You can also reconfigure AWS Config to use their own centralized logging buckets.
  - AWS Config bucket: `so0111-aws-config-<region>-<accountid>`
  - Access logging bucket: `so0111-access-logs-<region>-<accountid>`
  - Service-linked role: `AWSServiceRoleForConfig`
- CW.1 – A log metric filter and alarm should exist for usage of the "root" user

  Actions: Creates a log metric that counts and alarms on use of the "root" IAM account
- EC2.1 - Amazon EBS snapshots should not be publicly restorable

  Actions: An account-level finding, this runbook will make all EBS snapshots private
- EC2.2 - VPC default security group should prohibit inbound and outbound traffic

  Actions: Removes ALL TRAFFIC inbound and outbound rules on the default Security Group that is the subject of the finding
- EC2.6 - VPC flow logging should be enabled in all VPCs

  Actions: Enables VPC Flow Logs for the Amazon VPC in the finding
- IAM.7 - IAM user credentials should be disabled if not used within a predefined number of days

  Actions: Disables credentials unused for more than 90 days.
- IAM.8 - Password policies for IAM users should have strong configurations

Actions: Sets default password policy for the account in the finding.

- Lambda.1 - Lambda functions should prohibit public access

  Actions: Removes any Resource Policy statement with “Principal: *” from the Lambda that is the subject of the finding

- RDS.1 - RDS snapshots should prohibit public access

  Actions: Removes public sharing for the RDS snapshot (cluster or database) that is the subject of the finding

- S3.1 - S3 buckets should prohibit public write access
- S3.2 - S3 buckets should prohibit public read access

  Actions: Blocks public read and write access to the bucket in the finding

- S3.6 - S3 Block Public Access setting should be turned on

  Actions: Establishes S3 public access blocks by default at the account level

Adding new remediations

Adding a new remediation to an existing Playbook does not require modification to the solution itself.

> **Note**
> The instructions that follow leverage resources installed by the solution as a starting point. By convention, most solution resource names contain **SHARR** and/or **SO0111** to make it easy to locate and identify them.

Overview

AWS Security Hub Response and Remediation (SHARR) runbooks must follow the following standard naming:

`SHARR-<standard>-<version>-<control>`

Standard: The abbreviation for the security standard. This must match standards supported by SHARR. It must be one of “CIS”, “AFSBP”, or “PCI”.

Version: The version of the standard. Again, this must match the version supported by SHARR and the version in the finding data.

Control: The control ID of the control to be remediated. This must match the finding data.

1. Create a runbook in the member account(s).
2. Create an IAM role in the member account(s).
3. (Optional) Create an automatic remediation rule in the Admin account.

Step 1. Create a runbook in the member account(s)

1. Sign in to the AWS Systems Manager console and obtain an example of the finding JSON.
2. Create an automation runbook that remediates the finding. In the **Owned by me** tab, use any of the `SHARR-` documents under the **Documents** tab as a starting point.
3. The AWS Step Functions in the Admin account will run your runbook. Your runbook must specify the remediation role in order to be passed when calling the runbook.

Step 2. Create an IAM role in the member account(s)

1. Sign in to the AWS Identity and Access Management console.
2. Obtain an example from the IAM **SO0111** roles and create a new role. The role name must start with `SO0111-Remediate-<standard>-<version>-<control>`. For example, if adding CIS v1.2.0 control 5.6 the role must be `SO0111-Remediate-CIS-1.2.0-5.6`.
3. Using the example, create a properly scoped role that allows only the necessary API calls to perform remediation.

At this point, your remediation is active and available for automated remediation from the SHARR Custom Action in AWS Security Hub.

Step 3: (Optional) Create an automatic remediation rule in the admin account

Automatic (not "automated") remediation is the immediate execution of the remediation as soon as the finding is received by AWS Security Hub. Carefully consider the risks before using this option.

1. View an example rule for the same Security Standard in CloudWatch Events. The naming standard for rules is `standard_control_`**`AutoTrigger`**.
2. Copy the event pattern from the example to be used.
3. Change the `GeneratorId` value to match the `GeneratorId` in your Finding JSON.
4. Save and enable the rule.

Adding a new playbook

Download the AWS Security Hub Automated Response and Remediation solution playbooks and deployment source code from the GitHub repository.

The CloudFormation resources are created from AWS CDK components, and the resources contain the playbook template code that you can use to create and configure new playbooks. For more information about setting up your project and customizing your playbooks, refer to the README.md file in GitHub.

AWS Systems Manager Parameter Store

AWS Security Hub Automated Response and Remediation uses AWS Systems Manager Parameter Store for storage of operational data. The following parameters are stored in Parameter Store:

Name	Value	Use
`/Solutions/SO0111/CMK_REMEDIATION_ARN`	AWS KMS Customer Managed Key that will encrypt data for AFSBP remediations	Encryption of customer data, such as CloudTrail logs, as part of remediations
`/Solutions/SO0111/CMK_ARN`	AWS KMS Customer Managed Key that SHARR will use to encrypt data	Encryption of solution data
`/Solutions/SO0111/SNS_Topic_ARN`	ARN of the Amazon SNS topic for the solution	Notification of remediation events
`/Solutions/SO0111/SNS_Topic_Config.1`	SNS Topic for AWS Config updates	Config.1 remediation
`/Solutions/SO0111/sendAnonymousMetrics`	Yes	Anonymous metrics collection
`/Solutions/SO0111/version`	Solution version	
`/Solutions/SO0111/<security standard long name>/<version>/status`	enabled	Indicates whether the standard is active in the solution. A standard can be disabled for automated remediation by changing this to **disabled**
`/Solutions/SO0111/<security standard long name>/shortname`	String	Short name for the security standard. For example: 'CIS', 'AFSBP', 'PCI'
`/Solutions/SO0111/<security standard long name>/<version>/<control>/remap`	String	When one control uses the same remediation as another, these parameters accomplish the remap

Troubleshooting

Solution logs

AWS Security Hub Automated Response and Remediation (SHARR) collects output from remediation runbooks, which run under AWS Systems Manager, and logs the result to CloudWatch Logs group `SO0111-SHARR` in the AWS Security Hub Admin account. There is one stream per control per day.

The Orchestrator Step Function logs all step transitions to the `SO0111-SHARR-Orchestrator` CloudWatch Logs Group in the AWS Security Hub Admin account. This log is an audit trail to record state transitions for each instance of the Step Function. There is one log stream per Step Function execution.

Both log groups are encrypted using an AWS KMS Customer-Manager Key (CMK).

The following troubleshooting information uses the `SO0111-SHARR` log group. Use this log, as well as AWS Systems Manager Automation console, Automation Executions logs, Step Function console, and Lambda logs to troubleshoot problems.

If a remediation fails, a message similar to the following will be logged to `SO0111-SHARR` in the log stream for the standard, control, and date. For example: **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)
```

The following messages provide additional detail. This output is from the SHARR runbook for the security standard and control. For example: **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.
```

This information points you to the failure, which in this case was a child automation running in the member account. To troubleshoot this issue, you must log in to the AWS Management Console in the member account (from the message above), go to AWS Systems Manager, navigate to **Automation**, and examine the log output for Execution ID `eecdef79-9111-4532-921a-e098549f525`.

Issues and resolutions

- **Issue:** The solution deployment fails with an error stating that the resources are already available in Amazon CloudWatch.

  Resolution: Check for an error message in the CloudFormation resources/events section indicating log groups already exist. The SHARR deployment templates allow reuse of existing log groups. Verify that you have selected reuse.
- **Issue:** I run Security Hub in multiple Regions in the same account. I want to deploy this solution in multiple Regions.

Resolution: You can activate multi-Region deployment by deploying multiple instances of the solution in the same account across different Regions. Multi-Region deployment is supported, but Cross-Region remediation is not because AWS Security Hub is a Regional service.

- **Issue:** After completing cross account deployment in two Regions (us-east-1 and ap-southeast-2), I see that security findings from both Regions are displayed in AWS Security Hub in us-east-1 and ap-southeast-2. However, I am not able to remediate findings in ap-southeast-2 from AWS Security Hub in us-east-1 (not able to run cross Region remediation).

  Resolution: Because AWS Security Hub is a Regional service, you can run remediation actions only for findings within the same Region (you may see findings across other Regions because they are aggregated at the account level by other services).

- **Issue:** Immediately after deploying, the **SO0111-SHARR-Orchestrator** is failing in the Get Automation Document State with a 502 error: *"Lambda was unable to decrypt the environment variables because KMS access was denied. Please check the function's KMS key settings. KMS Exception: UnrecognizedClientExceptionKMS Message: The security token included in the request is invalid. (Service: AWSLambda; Status Code: 502; Error Code: KMSAccessDeniedException; Request ID: …"*

  Resolution: Allow the solution about 10 minutes to stabilize before running remediations. If the problem continues, open a support ticket or GitHub issue.

- **Issue**: I attempted to remediate a finding but nothing happened.

  Resolution: Check the notes of the finding for reasons why it was not remediated. A common cause is that the finding has no automated remediation. At this time there is no way to provide direct feedback to the user when no remediation exists other than via the notes.

  A second common cause is that the finding has already been remediated. If the finding state is not **NEW** then the remediation will not run.

  Review the solution logs. Open CloudWatch Logs in the console. Find the SO0111-SHARR CloudWatch Logs Group. Sort the list so the most-recently updated streams appear first. Select the log stream for the finding you attempted to run. You should find any errors there. Some reasons for the failure could be: mismatch between finding control and remediation control, cross-account remediation (not yet supported), or that the finding has already been remediated. If unable to determine the reason for the failure, please collect the logs and open a support ticket.

- **Issue:** After starting a remediation, the status in the Security Hub console has not updated.

  Resolution: The Security Hub console does not update automatically. Refresh the current view. The status of the finding should update.

  It might take several hours for the finding to transition from **Failed** to **Passed**. Findings are created from event data sent by other services, such as AWS Config, to AWS Security Hub. The time before a rule is reevaluated depends on the underlying service.

  If this does not resolve the issue, refer to the resolution above for *"I attempted to remediate a finding but nothing happened."*

- **Issue**: Orchestrator step function fails in **Get Automation Document State**: *An error occurred (AccessDenied) when calling the AssumeRole operation*.

  Resolution: The member template has not been installed in the member account where SHARR is attempting to remediate a finding. Follow instructions for deployment of the member template.

- **Issue**: Config.1 runbook fails because Recorder or Delivery Channel already exists.

  Resolution: Inspect your AWS Config settings carefully to ensure Config is properly set up. The automated remediation is not able to fix existing AWS Config settings in some cases.

- **Issue**: Remediation is successful but returns the message `"No output available yet because the step is not successfully executed."`

Resolution: This is a known issue in this release where certain remediation runbooks do not return a response. The remediation runbooks will properly fail and signal the solution if they do not work.

- **Issue**: The resolution failed and sent a stack trace.

  Resolution: Occasionally, we miss the opportunity to handle an error condition that results in a stack trace rather than an error message. Attempt to troubleshoot the problem from the trace data. Open a support ticket if you need assistance.

- **Issue**: Removal of the v1.3.0 stack failed on the Custom Action resource.

  Resolution: Removal of the admin template may fail on the Custom Action removal. This is a known issue that will be fixed in the next release. If this occurs:

  1. Sign in to AWS Security Hub management console.
  2. In the Admin account, go to **Settings**.
  3. Select the **Custom actions** tab
  4. Manually delete the entry **Remediate with SHARR**.
  5. Delete the stack again.

Update the solution

If you have previously deployed the solution, use the following instructions to upgrade your solution to the latest version:.

1. Uninstall the previously deployed solution. Refer to Uninstall the solution (p. 35).
2. Launch the latest template. Refer to Automated deployment (p. 15).

   Note
   If you are upgrading from v1.2.1 or earlier to v1.3.0, set **Use existing Orchestrator Log Group** to **No**. If you are reinstalling v1.3.0 you can select **Yes** for this option. This option allows you to continue to log to the same Log Group for the Orchestrator Step Function.

Uninstall the solution

Use the following procedure to uninstall the solution with the AWS Management Console.

V1.0.0-V1.2.1

For releases v1.0.0 to v1.2.1, use Service Catalog to uninstall the CIS and/or AFSBP Playbooks. With v1.3.0 Service Catalog is no longer used.

1. Sign in to the AWS CloudFormation console and navigate to the Security Hub primary account.
2. Choose **Service Catalog** to terminate any provisioned playbooks, remove any security groups, roles, or users.
3. Remove the spoke `CISPermissions.template` template form the Security Hub member accounts.
4. Remove the spoke `AFSBPMemberStack.template` template form the Security Hub admin and member accounts.
5. Navigate to the Security Hub primary account, select the solution's installation stack, and then choose **Delete**.

Note
CloudWatch Logs group logs are retained. We recommend retaining these logs as required by your organization's log retention policy.

V1.3.0

1. Remove the `aws-sharr-member.template` from each member account.
2. Remove the `aws-sharr-admin.template` from the admin account.

Note
Removal of the admin template might fail on the Custom Action removal. This is a known issue that will be fixed in the next release. Use the following instructions to fix this issue:

1. Sign in to the AWS Security Hub management console.
2. In the Admin account, go to **Settings**.
3. Select the **Custom actions** tab.
4. Manually delete the entry **Remediate with SHARR**.
5. Delete the stack again.

Collection of operational metrics

This solution includes an option to send anonymous operational metrics to AWS. We use this data to better understand how customers use this solution and related services and products. When enabled, the following information is collected and sent to AWS:

- **Solution ID:** The AWS solution identifier
- **Unique ID (UUID):** Randomly generated, unique identifier for each AWS Security Hub Response and Remediation deployment
- **Timestamp:** Data collection timestamp
- **Instance Data:** Information about this stack deployment
- **Status**: Deployment status (passed or failed solution) or (passed or failed remediation)
- **Error message**: The generic error message in the status field
- **Generator_id**: Security Hub rule information
- **Type**: Remediation type and name
- **productArn**: The Region where Security Hub is deployed
- **finding_triggered_by**: The type of remediation performed (custom action or automated trigger)

AWS owns the data gathered though this survey. Data collection is subject to the AWS Privacy Policy. To opt out of this feature, complete the following steps before launching the AWS CloudFormation template.

1. Download the AWS CloudFormation template to your local hard drive.
2. Open the AWS CloudFormation template with a text editor.
3. Modify the AWS CloudFormation template mapping section from:

```
Mappings:
  Solution:
    Data:
      SendAnonymousUsageData: 'Yes'
```

   to

```
  Mappings:
    Solution:
      Data:
        SendAnonymousUsageData: 'No'
```

4. Sign in to the AWS CloudFormation console.
5. Select **Create stack**.
6. On the **Create stack** page, **Specify template section**, select **Upload a template file**.
7. Under **Upload a template file**, choose **Choose file** and select the edited template from your local drive.
8. Choose **Next** and follow the steps in Launch the stack (p. 15) in the Automated Deployment section of this guide.

Source code

Visit the GitHub repository to download the templates and scripts for this solution, and to share your customizations with others.

Contributors

The following individuals contributed to this document:

- Mike O'Brien
- Nikhil Reddy
- Chandini Penmetsa
- Chaitanya Deolankar

Revisions

Date	Change
August 2020	Initial release
October 2020	Added additional troubleshooting information to Appendix C
November 2020	Added deployment instructions for China regions; updated solution deployment instructions for the Security Hub admin account; for more information, refer to the CHANGELOG.md file in the GitHub repository
April 2021	Release v1.2.0: Added new playbook architecture and new AFSBP remediations. For more information, refer to the CHANGELOG.md file in the GitHub repository
May 2021	Release v1.2.1: Bugfix for an issue affecting EC2.2 and EC2.7. For more information, refer to the CHANGELOG.md file in the GitHub repository
August 2021	Release v1.3.0: Added PCI DSS v3.2.1 Playbook. Added 17 new remediations to CIS v1.2.0. Added four new remediations to AFSBP. Converted CIS to use new playbook architecture based on SSM runbooks. Added instructions to extend existing Playbooks with customer-defined remediations. For more information, refer to the CHANGELOG.md file in the GitHub repository

Notices

Customers are responsible for making their own independent assessment of the information in this document. This document: (a) is for informational purposes only, (b) represents AWS current product offerings and practices, which are subject to change without notice, and (c) does not create any commitments or assurances from AWS and its affiliates, suppliers or licensors. AWS products or services are provided “as is” without warranties, representations, or conditions of any kind, whether express or implied. AWS responsibilities and liabilities to its customers are controlled by AWS agreements, and this document is not part of, nor does it modify, any agreement between AWS and its customers.

AWS Security Hub Automated Response and Remediation is licensed under the terms of the of the Apache License Version 2.0 available at The Apache Software Foundation.