Automated Security Response on AWS

Implementation Guide

Automated Security Response on AWS: 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. 49): June 2022)*

The continued evolution of security threats makes it difficult, expensive, and time-consuming for security teams to react. The Automated Security Response on AWS 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*.

Automated Security Response on AWS 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 Automated Security Response on AWS 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 this solution. As of June 2022, 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 Lambda - Requests	1M free requests per month	$0.20 per 1M requests
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.

Service	Free Tier	Pricing
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 Lambda - Requests	300 remediations * 6 requests = 1,800 requests $0.20 * 1,000,000 requests = $0.20	$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	< $0.12

Service	Assumptions	Monthly Charges
	$0.025 * (4,500/1,000) state transitions = $0.1125	
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 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 $0.025 * (45,000/1,000) state transitions = $1.125	$1.13
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 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.

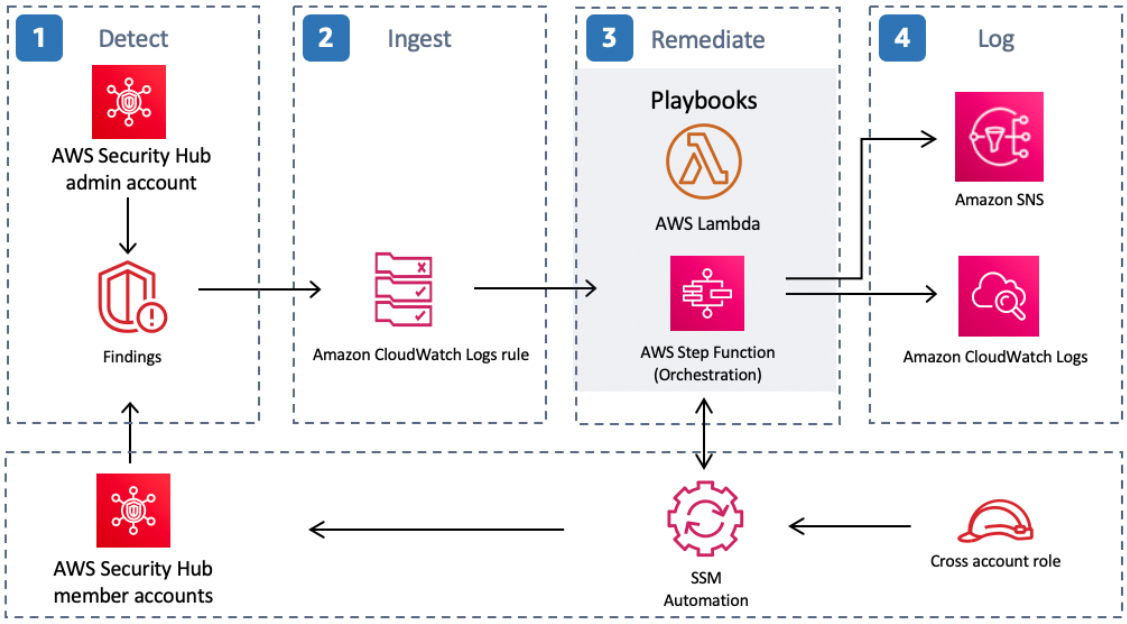

Figure 1: Automated Security Response on AWS architecture

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

You 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` and `aws-sharr-member-roles.template` CloudFormation templates. 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 by turning on the CloudWatch Events rules in the AWS Security Hub admin account.

Cross-account remediation

Automated Security Response on AWS 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. Each remediation is assigned an individual role. The remediation process in the primary account is granted permission to assume the remediation role in the account that requires remediation. Remediation is performed by AWS Systems Manager runbooks running in the account that requires remediation.

Playbooks

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

- Center for Internet Security (CIS) Amazon Web Services Foundations benchmarks, version 1.2.0, published May 18, 2018.
- AWS Foundational Security Best Practices (AFSBP) version 1.0.0, published March 2021.
- Payment Card Industry Data Security Standard (PCI-DSS), version 3.2.1, published May 2018.

Centralized logging

Automated Security Response on AWS 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

This solution 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` role. Only this role is allowed to assume the `SO0111- Orchestrator-Member` 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` 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 `AssumeRole` permissions to the solution's AWS Lambda functions.

Solution updates

To upgrade this solution from v1.3.x or earlier 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. 44). Note that any log data is retained and there is no loss of operational data. If upgrading from v1.4.x, refer to Update the solution (p. 43).

Stack vs StackSets deployment

A *stack set* lets you create stacks in AWS accounts across AWS Regions by using a single AWS CloudFormation template. Starting with verson 1.4, this solution supports stack set deployment by splitting resources based on where and how they are deployed. Multi-account customers, particularly those using AWS Organizations, can benefit from using stack sets for deployment across many accounts. It reduces the effort needed to install and maintain the solution. For more information about StackSets, refer to Using AWS CloudFormation StackSets.

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 Automated Security Response on AWS 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 Automated Security Response on AWS 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 Amazon Simple Notification Service, AWS Key Management Service, AWS Identity and Access Management, AWS Lambda, AWS Step Functions, 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.

Member roles

View template **aws-sharr-member-roles.template** - Defines the remediation roles needed in each AWS Security Hub member account.

Automated deployment - StackSets

> **Note**
> We recommend deploying with StackSets. However, for single account deployments or for testing or evaluation purposes, consider the stacks deployment (p. 20) option.

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 AWS Organizations.

Time to deploy: Approximately 15 minutes per account, depending upon StackSet parameters.

Prerequisites

AWS Organizations helps you centrally manage and govern your multi-account AWS environment and resources. StackSets work best with AWS Organizations.

If you have previously deployed v1.3.x or earlier of this solution, you must uninstall the existing solution. For more information, refer to Solution updates (p. 12).

Before you deploy this solution, review your AWS Security Hub deployment:

- There must be a delegated Security Hub admin account in your AWS Organization.
- Security Hub should be configured to aggregate findings across Regions. For more information, refer to Aggregating findings across Regions in the AWS Security Hub User Guide.
- You should activate Security Hub for your organization in each Region where you have AWS usage.

This procedure assumes that you have multiple accounts using AWS Organizations, and have delegated an AWS Organizations admin account and an AWS Security Hub admin account.

Deployment overview

> **Note**
> StackSet deployment for this solution uses a combination of service-managed and self-managed StackSets. Self-Managed StackSets must be used currently as they use nested StackSets, which are not yet supported with service-managed StackSets.

Deploy the StackSets from a delegated administrator account in your AWS Organizations.

Planning

Use the following form to help with StackSet deployment. Prepare your data, then copy and paste the values during deployment.

```
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):
_____________________,
_____________________,
_____________________,
_____________________,
_____________________
```

Step. 1: Launch the admin stack in the delegated Security Hub admin account (p. 17)

- Using a self-managed StackSet, launch the `aws-sharr-deploy.template` AWS CloudFormation template into your AWS Security Hub admin account in the same Region as your Security Hub admin. This template uses nested stacks.
- Choose which Security Standards to install. By default, all are selected (Recommended)
- Choose an existing Orchestrator log group to use. Select `Yes` if `SO0111-SHARR- Orchestrator` already exists from a previous installation.

For more information on self-managed StackSets, refer to Grant self-managed permissions in the *AWS CloudFormation User Guide*.

Step 2: Install the remediation roles into each AWS Security Hub member account (p. 17)

Wait for Step 1 to complete deployment, because the template in Step 2 references IAM roles created by Step 1.

- Using a service-managed StackSet, launch the `aws-sharr-member-roles.template` AWS CloudFormation template into a single Region in each account in your AWS Organizations.
- Choose to install this template automatically when a new account joins the organization.
- Enter the account ID of your AWS Security Hub admin account.

Step. 3: Launch the member stack into each AWS Security Hub member account and Region (p. 18)

- Using a self-managed StackSet, launch the `aws-sharr-member.template` AWS CloudFormation template into all Regions where you have AWS resources in every account in your AWS Organization managed by the same Security Hub admin.

  Note
  Until service-managed StackSets support nested stacks, you must do this step for any new accounts that join the organization.
- Choose which Security Standard playbooks to install.
- Provide the name of a CloudTrail logs group (used by some remediations).
- Enter the account ID of your AWS Security Hub admin account.

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. 46) section of this guide.

Step 1. Launch the admin stack in the delegated Security Hub admin account

1. Launch the admin stack, `aws-sharr-deploy.template`, with your Security Hub admin account. Typically, one per organization in a single Region. Because this stack uses nested stacks, you must deploy this template as a self-managed StackSet.

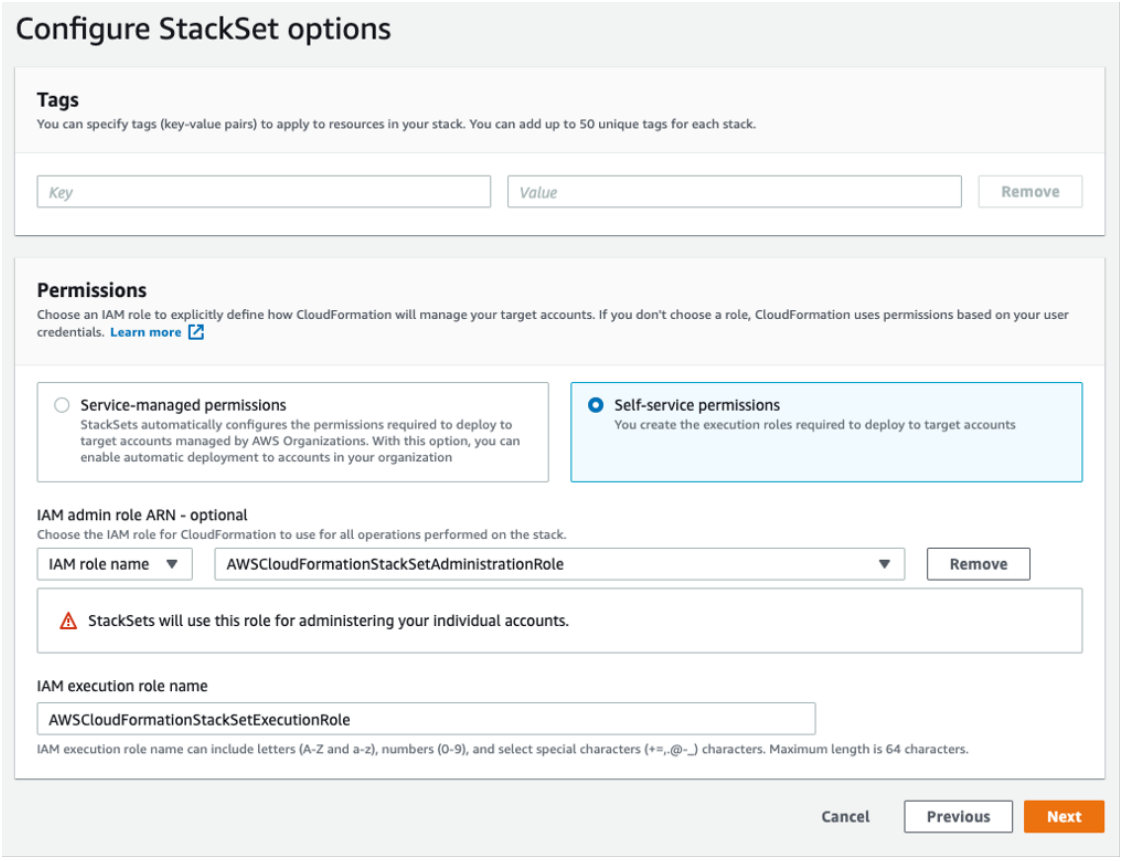

Figure 2: Configure StackSet options

2. For the **Account numbers** parameter, enter the account ID of the AWS Security Hub admin account.
3. For the **Specify regions** parameter, select only the Region where Security Hub admin is turned on. Wait for this step to complete before going on to Step 2.

Step 2. Install the remediation roles into each AWS Security Hub member account

Use a service-managed StackSet to deploy the member roles template, aws-sharr-member-roles.template. This StackSet must be deployed in one Region per member account. It defines the global roles that allow cross-account API calls from the SHARR Orchestrator step function.

1. Deploy to the entire organization (typical) or to organizational units, as per your organizations policies.
2. Turn on automatic deployment so new accounts in the AWS Organizations receive these permissions.
3. For the **Specify regions** parameter, select a single Region. IAM roles are global. You can continue to Step 3 while this StackSet deploys.

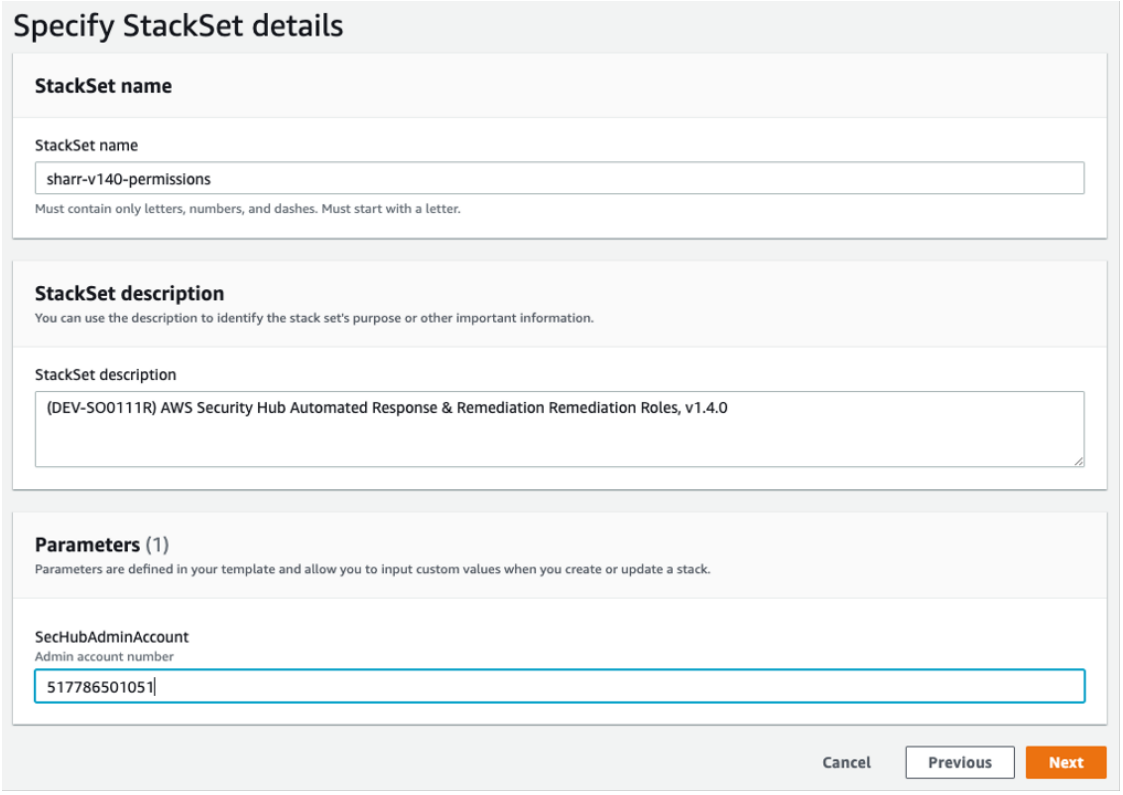

Figure 3: Specify StackSet details

Step 3. Launch the member stack into each AWS Security Hub member account and Region

Because this stack uses nested stacks, you must deploy as a self-managed StackSet. This does not support automatic deployment to new accounts in the AWS Organization.

Parameters

LogGroup Configuration: Choose the log group that receives CloudTrail logs. If none exists, or if the log group is different for each account, choose a convenient value. Account administrators must update the Systems Manager – Parameter Store /Solutions/SO0111/Metrics_LogGroupName parameter after creating a CloudWatch Logs Group for CloudTrail logs. This is required for remediations that create metrics alarms on API calls.

Standards: Choose the standards to load in the member account. This only installs the AWS Systems Manager runbooks – it does not enable the Security Standard.

SecHubAdminAccount: Enter the account ID of the AWS Security Hub Admin account where you installed the solution's admin template.

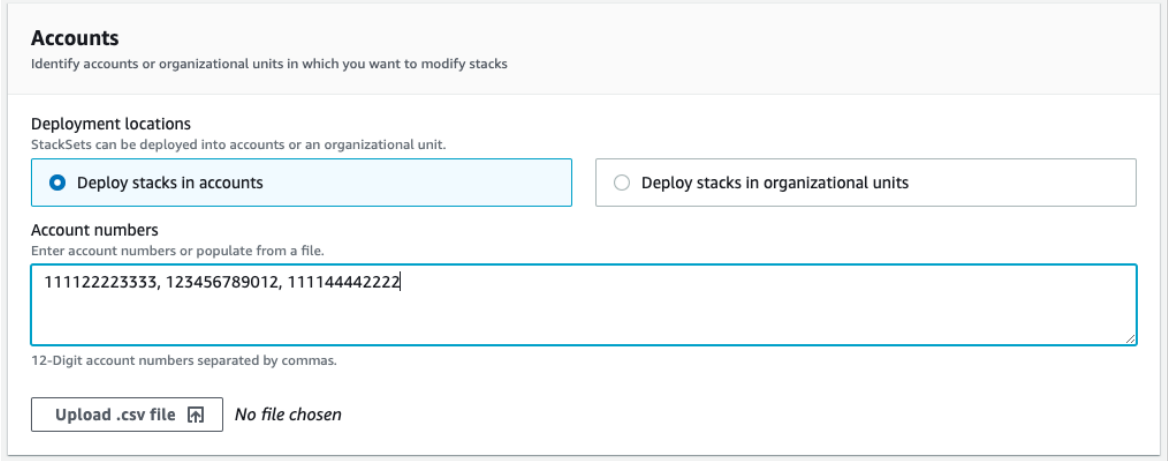

Figure 4: Accounts

Deployment locations: You may specify a list of account numbers or organizational units.

Specify regions: Select all of the Regions where you want to remediate findings. You can adjust Deployment options as appropriate for the number of accounts and Regions. Region Concurrency can be parallel.

Automated deployment - Stacks

Note
For Multi-account customers, we strongly recommend deployment with StackSets (p. 15).

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. 20)

- 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. 22)

- 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.
- Choose whether to install the remediation roles. Install these roles only once per account.
- Select which playbooks to install.
- Enter the account ID of the AWS Security Hub admin account.

Step. 3 (Optional) Adjust the available remediations (p. 23)

- Remove any remediations on a per-member account basis. This 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. 46) section of this guide.

This automated AWS CloudFormation template deploys the Automated Security Response on AWS solution in the AWS Cloud. Before you launch the stack, you must enable Security Hub and complete the prerequisites (p. 20).

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.

   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 Systems Manager which is currently available in specific AWS Regions only. The solution works in all of the Regions that support this service. 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**.

Parameter	Default	Description
Load AFSBP Admin Stack	`yes`	Specify whether to install the admin components for automated remediation of AFSBP controls.
Load CIS120 Admin Stack	`yes`	Specify whether to install the admin components for automated remediation of CIS120 controls.
Load PC1321Admin Stack	`yes`	Specify whether to install the admin components for automated remediation of CIS120 controls.
Reuse Orchestrator Log Group	`no`	Select whether or not to reuse an existing `SO0111-SHARR-Orchestrator` CloudWatch

Parameter	Default	Description
		Logs group. This simplifies reinstallation and upgrades without losing log data from a previous version. If you are upgrading from v1.2 or above, select `yes`.

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. Install the remediation roles into each AWS Security Hub member account

The `aws-sharr-member-roles.template` StackSet must be deployed in only one Region per member account. It defines the global roles that allow cross-account API calls from the SHARR Orchestrator step function.

1. Sign in to the AWS Management Console for each AWS Security Hub member account (including the admin account, which is also a member). Select the button to launch the `aws-sharr-member-roles.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.
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.

Parameter	Default	Description
Sec Hub Account Admin	*<Requires input>*	Enter the 12-digit account ID for the AWS Security Hub admin account. This value grants permissions to the admin account's solution role.

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 5 minutes. You may continue with the next step while this stack loads.

Step 3. 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. 46) section of this guide.

The `aws-sharr-member` stack must be installed into each Security Hub member account. This stack defines the 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 for each AWS Security Hub member account (including the admin account, which is also a member). Select the button 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 Systems Manager, which is currently available in the majority of AWS Regions. 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**.

Parameter	Default	Description
Provide the name of the LogGroup to be used to create Metric Filters and Alarms	*<Requires input>*	Specify the name of a CloudWatch Logs group where CloudTrail logs API calls.

Parameter	Default	Description
		This is used for CIS 3.1-3.14 remediations.
Load AFSBP Admin Stack	`yes`	Specify whether to install the admin components for automated remediation of AFSBP controls.
Load CIS120 Admin Stack	`yes`	Specify whether to install the admin components for automated remediation of CIS120 controls.
Load PC1321Admin Stack	`yes`	Specify whether to install the admin components for automated remediation of CIS120 controls.
Create S3 Bucket For Redshift Audit Logging	`no`	Select `yes` if the S3 bucket should be created for the AFSBP RedShift.4 remediation. For details of the S3 bucket and the remediation, review the Redshift.4 remediation in the *AWS Security Hub User Guide*.
Sec Hub Admin Account	*`<Requires input>`*	Enter the 12-digit account ID for the AWS Security Hub a dmin account.

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 4: (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**.

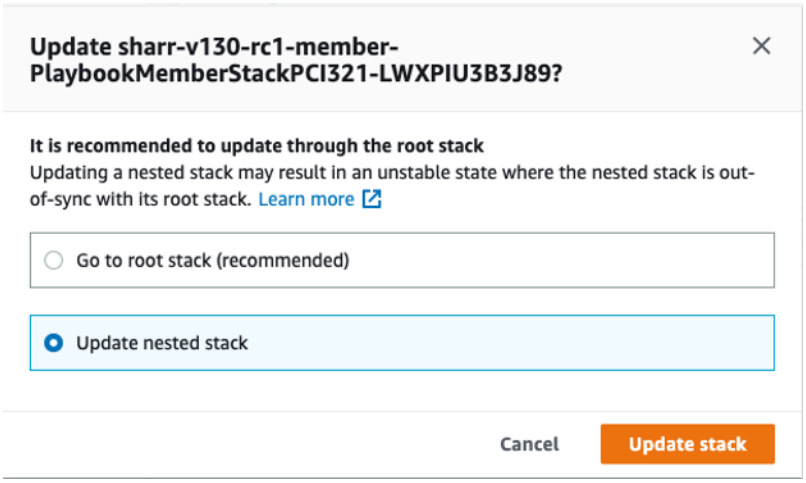

Figure 5: Update nested stack

4. Select **Use current template** and choose **Next**.
5. Adjust the available remediations. Change the values for desired controls to `Available` and undesired controls to `Not available`.

   Note
   Turning off a remediation removes the solutions remediation runbook for the security standard and control.
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 Step Functions
• AWS CloudFormation	• AWS Systems Manager
• AWS Key Management Service	• Amazon Simple Notification Service
• AWS Lambda	• AWS Identity and Access Management (IAM)
• Amazon CloudWatch Events	• AWS CDK
• CloudWatch Logs	

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 details on a specific remediation, refer to the Systems Manager automation document with the name deployed by the solution in your account. Go to the AWS Systems Manager console, then in the navigation pane choose **Documents**.

Description	AWS FSBP	CIS v1.2.0	PCI v3.2.1
SHARR-EnableAutoScalingGroupELBHealthCheck Auto Scaling groups associated with a load balancer should use load balancer health checks	Autoscaling.1		Autoscaling.1
SHARR-CreateCloudTrailMultiRegionTrail CloudTrail should be activated and configured with at least one multi-Region trail	CloudTrail.1	2.1	CloudTrail.2
SHARR-EnableCloudTrailEncryption CloudTrail should have encryption at rest activated	CloudTrail.2	2.7	CloudTrail.1
SHARR-EnableCloudTrailLogFileValidation Ensure CloudTrail log file validation is activated	CloudTrail.4	2.2	CloudTrail.3
SHARR-EnableCloudTrailToCloudWatchLogging Ensure CloudTrail trails are integrated with Amazon CloudWatch Logs	CloudTrail.5	2.4	CloudTrail.4
SHARR-ReplaceCodeBuildClearTextCredentials CodeBuild project environment variables	CodeBuild.2		CodeBuild.2

should not contain clear text credentials			
SHARR-EnableAWSConfig Ensure AWS Config is activated	Config.1	2.5	Config.1
SHARR-MakeEBSSnapshotsPrivate Amazon EBS snapshots should not be publicly restorable	EC2.1		EC2.1
SHARR-RemoveVPCDefaultSecurityGroupRules VPC default security group should prohibit inbound and outbound traffic	EC2.2	4.3	EC2.2
SHARR-EnableVPCFlowLogs VPC flow logging should be enabled in all VPCs	EC2.6	2.9	EC2.6
SHARR-EnableEbsEncryptionByDefault EBS default encryption should be activated	EC2.7		
SHARR-RevokeUnrotatedKeys IAM users' access keys should be rotated every 90 days or less	IAM.3	1.4	
SHARR-SetIAMPasswordPolicy IAM default password policy	IAM.7	1.5-1.11	IAM.8
SHARR-RevokeUnusedIAMUserCredentials IAM user credentials should be turned off if not used within a pre-defined number of days	IAM.8	1.3	IAM.7

SHARR-RemoveLambdaPublicAccess Lambda functions should prohibit public access	Lambda.1		Lambda.1
SHARR-MakeRDSSnapshotPrivate RDS snapshots should prohibit public access	RDS.1		RDS.1
SHARR-DisablePublicAccessToRDSInstance RDS DB Instances should prohibit public access	RDS.2		RDS.2
SHARR-EncryptRDSSnapshot RDS cluster snapshots and database snapshots should be encrypted at rest	RDS.4		
SHARR-EnableMultiAZOnRDSInstance RDS DB instances should be configured with multiple Availability Zones	RDS.5		
SHARR-EnableEnhancedMonitoringOnRDSInstance Enhanced monitoring should be configured for RDS DB instances and clusters	RDS.6		
SHARR-EnableRDSClusterDeletionProtection RDS clusters should have deletion protection activated	RDS.7		
SHARR-EnableRDSInstanceDeletionProtection RDS DB instances should have deletion protection activated	RDS.8		

SHARR-EnablMinorVersionUpgradeOnRDSDBInstance RDS automatic minor version upgrades should be activated	RDS.13		
SHARR-EnableCopyTagsToSnapshotOnRDSCluster RDS DB clusters should be configured to copy tags to snapshots	RDS.16		
SHARR-DisablePublicAccessToRedshiftCluster Amazon Redshift clusters should prohibit public access	Redshift.1		Redshift.1
SHARR-EnableAutomaticSnapshotsOnRedshiftCluster Amazon Redshift clusters should have automatic snapshots activated	Redshift.3		
SHARR-EnableRedshiftClusterAuditLogging Amazon Redshift clusters should have audit logging activated	Redshift.4		
SHARR-EnableAutomaticVersionUpgradeOnRedshiftCluster Amazon Redshift should have automatic upgrades to major versions activated	Redshift.6		
SHARR-ConfigureS3PublicAccessBlock S3 Block Public Access setting should be activated	S3.1		S3.6
SHARR-ConfigureS3BucketPublicAccessBlock S3 buckets should prohibit public read access	S3.2		S3.2

S3 buckets should prohibit public write access	S3.3		S3.1
SHARR-EnableDefaultEncryptionS3 S3 buckets should have server-side encryption activated	S3.4		S3.4
SHARR-SetSSLBucketPolicy S3 buckets should require requests to use SSL	S3.5		S3.5
SHARR-S3BlockDenylist Amazon S3 permissions granted to other AWS accounts in bucket policies should be restricted	S3.6		
S3 Block Public Access setting should be activated at the bucket level	S3.8		
SHARR-ConfigureS3BucketPublicAccessBlock Ensure the S3 bucket CloudTrail logs to is not publicly accessible		2.3	
SHARR-CreateAccessLoggingBucket Ensure S3 bucket access logging is activated on the CloudTrail S3 bucket		2.6	
SHARR-EnableKeyRotation Ensure rotation for customer-created CMKs is activated		2.8	KMS.1

SHARR-CreateLogMetricFilterAndAlarm Ensure a log metric filter and alarm exist for unauthorized API calls		3.1	
SHARR-CreateLogMetricFilterAndAlarm Ensure a log metric filter and alarm exist for AWS Management Console sign-in without MFA		3.2	
SHARR-CreateLogMetricFilterAndAlarm Ensure a log metric filter and alarm exist for usage of the "root" user		3.3	CW.1
SHARR-CreateLogMetricFilterAndAlarm Ensure a log metric filter and alarm exist for IAM policy changes		3.4	
SHARR-CreateLogMetricFilterAndAlarm Ensure a log metric filter and alarm exist for CloudTrail configuration changes		3.5	
SHARR-CreateLogMetricFilterAndAlarm Ensure a log metric filter and alarm exist for AWS Management Console authentication failures		3.6	
SHARR-CreateLogMetricFilterAndAlarm Ensure a log metric filter and alarm exist for disabling or scheduled deletion of customer created CMKs		3.7	

SHARR-CreateLogMetricFilterAndAlarm Ensure a log metric filter and alarm exist for S3 bucket policy changes		3.8	
SHARR-CreateLogMetricFilterAndAlarm Ensure a log metric filter and alarm exist for AWS Config configuration changes		3.9	
SHARR-CreateLogMetricFilterAndAlarm Ensure a log metric filter and alarm exist for security group changes		3.10	
SHARR-CreateLogMetricFilterAndAlarm Ensure a log metric filter and alarm exist for changes to Network Access Control Lists (NACL)		3.11	
SHARR-CreateLogMetricFilterAndAlarm Ensure a log metric filter and alarm exist for changes to network gateways		3.12	
SHARR-CreateLogMetricFilterAndAlarm Ensure a log metric filter and alarm exist for route table changes		3.13	
SHARR-CreateLogMetricFilterAndAlarm Ensure a log metric filter and alarm exist for VPC changes		3.14	

AWS-DisablePublicAccessForSecurityGroup Ensure no security groups allow ingress from 0.0.0.0/0 to port 22		4.1	EC2.5
AWS-DisablePublicAccessForSecurityGroup Ensure no security groups allow ingress from 0.0.0.0/0 to port 3389		4.2	

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

Automated Security Response on AWS 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 activate the rule.

Adding a new playbook

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

The AWS 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

Automated Security Response on AWS 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 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 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

Amazon SNS topic

Automated Security Response on AWS creates an Amazon SNS topic, SO0111-SHARR_Topic. This topic is used to post updates about remediation progress. Following are the three possible notifications sent to this topic.

```
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>
```

This is the completion message. It indicates that the remediation completed without error; however, the definitive test for successful remediation is the AWS Config check and/or manual validation.

Troubleshooting

Solution logs

This solution 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 must deploy the admin stack in the same account and Region as your Security Hub admin. Install the member template into each account and Region where you have a Security Hub member configured. Enable aggregation in Security Hub.
- **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.

  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.

- **Issue**: After redeploying the admin stack the step function is failing on `AssumeRole`.

  Resolution: Redeploying the admin stack breaks the trust connection between the admin role in the admin account and the member role in the member accounts. You must redeploy the member roles stack in all member accounts.
- **Issue**: CIS 3.x remediations are not showing `PASSED` after more than 24 hours.

  Resolution: This is a common occurrence if you have no subscriptions to the `SO0111-SHARR_LocalAlarmNotification` SNS topic in the member account.

Update the solution

Upgrading from versions prior to v1.4

If you have previously deployed the solution prior to v1.4.x, uninstall, then install the latest version:

1. Uninstall the previously deployed solution. Refer to Uninstall the solution (p. 44).
2. Launch the latest template. Refer to Automated deployment (p. 20).

   Note
   If you are upgrading from v1.2.1 or earlier to v1.3.0 or later, set **Use existing Orchestrator Log Group** to `No`. If you are reinstalling v1.3.0 or later, 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.

Upgrading from v1.4 and later

If you are upgrading from v1.4.x, update all stacks or StackSets as follows:

1. Update the stack in the Security Hub admin account using the latest template.
2. In each member account, update the permissions from the latest template.
3. In each member account in all Regions where currently deployed, update the member stack from the latest template.

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.x

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 in v1.3.0 will likely 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.

V1.4.0 and later

Stack deployment

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

StackSet deployment

For each StackSet, remove stacks, then remove the StackSet in the reverse order of deployment.

Note that IAM roles from the `aws-sharr-member-roles.template` are retained even if the template is removed. This is so that remediations using these roles continue to function. These SO0111-* roles can be manually removed after verifying that they are no longer in use by active remediations, such as CloudTrail to CloudWatch logging, or RDS Enhanced Monitoring.

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. 20) 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
September 2021	Release v1.3.1: `CreateLogMetricFilterAndAlarm.py` changed to make Actions active, add SNS notification to `SO0111-SHARR-LocalAlarmNotification`. Changed CIS 2.8 remediation to match new finding data format. For more information, refer to the CHANGELOG.md file in the GitHub repository
November 2021	Release v1.3.2: Bug fixes for CIS v1.2.0 controls 3.1 - 3.14. For more information, refer to the CHANGELOG.md file in the GitHub repository
December 2021	Release v1.4.0: The solution can now be deployed using StackSets. Cross-Region remediation is now supported in addition to cross-account. Member account IAM roles are now retained when the stack is removed. For more information, refer to the CHANGELOG.md file in the GitHub repository
January 2022	Release v1.4.1: Bug fixes. For more information, refer to the CHANGELOG.md file in the GitHub repository

Date	Change
January 2022	Release v1.4.2: Bug fixes. For more information, refer to the CHANGELOG.md file in the GitHub repository
June 2022	Release v1.5.0: Additional 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.

AWS glossary

For the latest AWS terminology, see the AWS glossary in the *AWS General Reference*.