# AWS Security Hub Automated Response and Remediation

## Implementation Guide

# AWS Security Hub Automated Response and Remediation: Implementation Guide

# Table of Contents

Home ..... 1
Overview ..... 2
    Cost ..... 2
        Small environment ..... 2
        Medium environment ..... 3
        Large environment ..... 4
    Architecture overview ..... 4
        Detect ..... 5
        Ingest ..... 5
        Remediate ..... 5
        Log ..... 6
Solution components ..... 7
    AWS Security Hub integration ..... 7
    Cross-account remediation ..... 7
    Playbooks ..... 7
    Centralized logging ..... 7
    Notifications ..... 7
Design considerations ..... 8
    AWS Security Hub deployment ..... 8
    Solution updates ..... 8
    Regional deployments ..... 8
AWS CloudFormation templates ..... 9
Automated deployment ..... 10
    Prerequisites ..... 10
    Deployment overview ..... 10
    Step 1. Launch the stack ..... 10
    Step 2. Configure service catalog portfolio permissions ..... 11
        Solution IAM groups ..... 11
        User IAM permissions ..... 12
    Step 3: Deploy the playbook(s) ..... 12
        Prerequisite ..... 12
        Deployment ..... 12
    Step 4. Deploy the solution permissions ..... 13
Security ..... 14
    IAM roles ..... 14
Additional resources ..... 15
Appendix A: Deploy the solution playbooks in AWS Regions in China ..... 16
Appendix B: CIS v1.2.0 playbook ..... 17
Appendix C: Customize the playbooks ..... 18
Appendix D: Troubleshooting guide ..... 19
Appendix E: Uninstall the solution ..... 20
    Using the AWS Management Console ..... 20
Appendix F: Collection of operational metrics ..... 21
Source code ..... 22
Contributors ..... 23
Revisions ..... 24
Notices ..... 25

# AWS Security Hub Automated Response and Remediation

**AWS Solution Implementation Guide**

Publication date: **August 2020 (last update (p. 24): November 2020)**

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.

# Overview

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 addresses this challenge by providing predefined response and remediation actions based on industry compliance standards and best practices.

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

Customers choose the individual playbooks they want to deploy in their 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, customers can apply recommendations from the 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.

AWS Security Hub Automated Response and Remediation Version includes the playbook remediations for the security standards defined as part of the Center for Internet Security (CIS) AWS Foundations Benchmark v1.2.0. For more information, refer to Appendix B (p. 17).

# Cost

You are responsible for the cost of the AWS services used to run the AWS Security Hub Automated Response and Remediation solution. Prices are subject to change. For full details, see the pricing page for each AWS service used in this solution.

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-triggered remediations
- The frequency of remediation

The solution uses the following AWS components, which incur a cost based on your configuration. Estimates are provided for small, medium, and large environments.

## Small environment

- 10 accounts
- 15 remediations per day per account (4,500 remediations per month)
- Total cost $5.07 per month / $60.87 per year

| Service | Upfront | Monthly | First 12 months total | Currency | Configuration summary |
|---|---|---|---|---|---|
| AWS Service Catalog | 0 | 5.00 | 60 | USD | One Service Catalog |

| Service | Upfront | Monthly | First 12 months total | Currency | Configuration summary |
|---|---|---|---|---|---|
| | | | | | Portfolio per Security Hub |
| AWS Lambda | 0 | 0.068 | 0.82 | USD | Number of requests (4,500) using 256 MB for 3.6 seconds average |
| Amazon CloudWatch Logs | 0 | 0.0003 | 0.02 | USD | 2,000 per remediation per day<br><br>Retained for 12 months |
| Amazon Simple Notification Service (Amazon SNS) | 0 | 0.0023 | 0.03 | USD | 4,500 notifications<br><br>Outbound < 1,000 per month |

# Medium environment

- 100 accounts
- 15 remediations per day per account (45,000 remediations per month)
- Total cost $5.71 per month / $68.69 per year

| Service | Upfront | Monthly | First 12 months total | Currency | Configuration summary |
|---|---|---|---|---|---|
| AWS Service Catalog | 0 | 5.00 | 60 | USD | One Service Catalog Portfolio per Security Hub |
| AWS Lambda | 0 | 0.68 | 8.21 | USD | Number of requests (45,000) using 256 MB for 3.6 seconds average |
| Amazon CloudWatch Logs | 0 | 0.0027 | 0.21 | USD | 2,000 per remediation per day<br><br>Retained for 12 months |

| Service | Upfront | Monthly | First 12 months total | Currency | Configuration summary |
|---|---|---|---|---|---|
| Amazon Simple Notification Service (Amazon SNS) | 0 | 0.0225 | 0.27 | USD | 45,000 notifications<br><br>Outbound < 1,000 per month |

## Large environment

- 1000 accounts
- 15 remediations per day per account (450,000 remediations per month)
- Total cost $12.09 per month / $146.89 per year

| Service | Upfront | Monthly | First 12 months total | Currency | Configuration summary |
|---|---|---|---|---|---|
| AWS Service Catalog | 0 | 5.00 | 60 | USD | One Service Catalog Portfolio per Security Hub |
| AWS Lambda | 0 | 6.84 | 82.08 | USD | Number of requests (450,000) using 256 MB for 3.6 seconds average |
| Amazon CloudWatch Logs | 0 | 0.0270 | 2.10 | USD | 2,000 per remediation per day<br><br>Retained for 12 months |
| Amazon Simple Notification Service (Amazon SNS) | 0 | 0.2250 | 2.70 | USD | 450,000 notifications<br><br>Outbound < 1,000 per month |

# Architecture overview

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

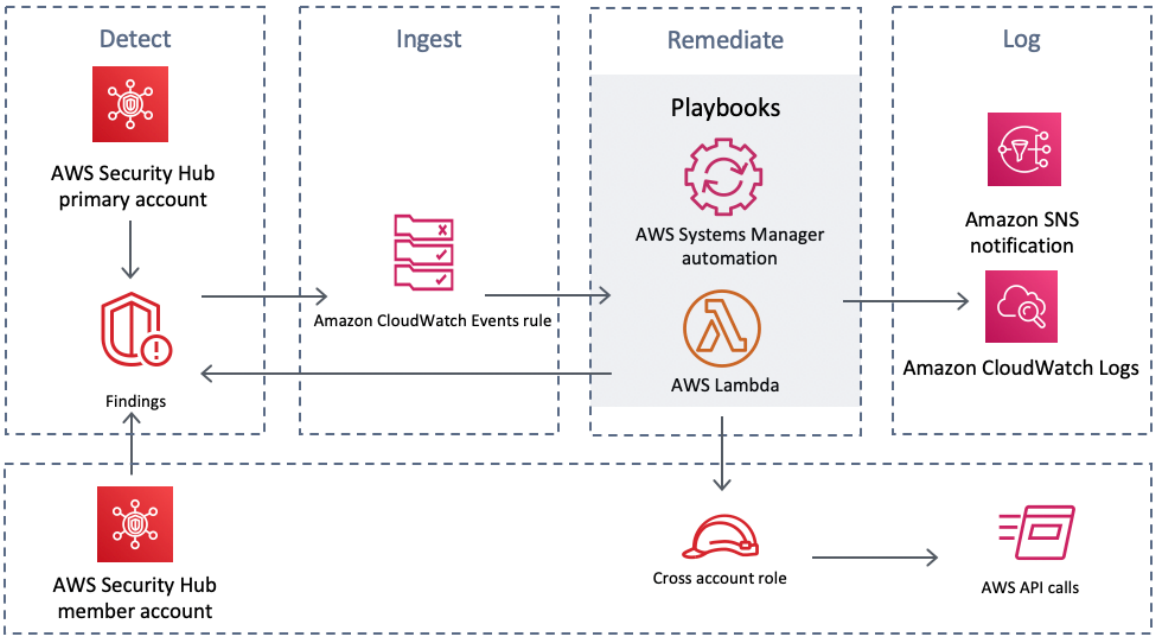


**Figure 1: Security Hub Automatic Response and Remediation architecture**

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

# 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.

# 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.

Customers can use the Security Hub Custom Action menu to initiate automated remediation, or after careful testing in a non-production environment, they can enable automatic triggering for automated remediation. This decision can be made per remediation – it is not necessary to enable automatic triggers on all remediations.

# 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.

# 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

After the solution is deployed successfully, users can install any playbooks from the AWS Service Catalog portfolio. Cross-account permissions for the playbook's functions must be deployed to all AWS Security Hub accounts (primary and member) using the spoke `CISPermissions.template`. Users are then able to initiate remediations for findings using custom actions in the Security Hub console.

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

## 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 Lambda is assigned an individual role. The remediation AWS Lambda function in the primary account is granted permission to assume the corresponding role 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. 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. (See Appendix B: CIS v1.2.0 playbook (p. 17))

## 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. Customers can use subscriptions to this topic to extend the capabilities of the solution. For example, they can send email notifications and update trouble tickets.

# 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 the Setting up AWS Security Hub topic in the *AWS Security Hub User Guide.*

At minimum, customers must have a working Security Hub configured in their primary account. Customers deploy the solution in the same account (and AWS Region) as the Security Hub primary account. In each Security Hub primary and secondary account, users 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 current version, you must delete the existing stack. For deletion instructions, refer to Appendix E: Uninstall the solution (p. 20).

## Regional deployments

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.

# 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:


**aws-sharr-deploy.template**: Use this template to launch the AWS Security Hub Automated Response and Remediation solution. The template creates an AWS Service Catalog product named CIS. You must install the CIS product from AWS Service Catalog before you configure further permissions in the primary member accounts.

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.


**CISPermission.template**: Use this template after you set up the solution and install the CIS product in AWS Service Catalog. After you successfully complete the CIS product installation, install the `CISPermission.template` in the primary account where Security Hub is configured, and in all of the accounts where remediations will be performed.

# Automated deployment

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

> **Important**
> To upgrade this solution to the current version, you must delete the existing stack. For deletion instructions, refer to Appendix E (p. 20).

**Time to deploy:** Approximately 10 minutes

## Prerequisites

Before you deploy this solution, ensure that AWS Security Hub is enabled in the same AWS Region as your primary and secondary accounts.

## Deployment overview

Use the following steps to deploy this solution on AWS.

## Step 1. Launch the stack

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.

> **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 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, see IAM and STS Quotas in the *AWS Identity and Access Management User Guide*.
5. On the **Parameters** page, choose **Next**.
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 10 minutes.

> **Note**
> The solution deploys the `aws-sharr-deploy.template` into your AWS account. The template requires an input to send anonymous data, which is defaulted to **Yes**. The automated deployment creates the foundation components needed for automated response and remediation playbooks in AWS Service Catalog. The playbooks themselves are deployed from an AWS Service Catalog portfolio that is created in your Security Hub primary account after you deploy the template.

# Step 2. Configure service catalog portfolio permissions

> **Note**
> If you are deploying this solution in an AWS Region in China, skip this step and refer to Appendix A (p. 16) to deploy the solution playbooks.

To grant access to IAM users, do one of the following:

- Add them to the default solution IAM groups
- Add IAM users, roles, or groups to the AWS Service Catalog portfolio

For more information, refer Creating IAM Roles in the *AWS Identity and Access Management User Guide.*

With the applicable permissions, users will have access to the **Products** and **Provisioned Products** menu in AWS Service Catalog.

## Solution IAM groups

By default, access to the AWS Security Hub Automated Response and Remediation's Service Catalog portfolio is limited to members of the following IAM groups created by the solution.

**SO0111-SHARR_Catalog_Admin:** This role allows members to have administrative access to the solution's portfolio, *Security Hub Playbooks (SO0111).*

**SO0111-SHARR_Catalog_User:** This role allows members to deploy, update, and terminate playbooks in the solution's portfolio, *Security Hub Playbooks (SO0111).*

Use the following process to grant IAM users access and add them to groups.

1. From the Security Hub primary account, navigate to the IAM console in the AWS Security Hub primary account.
2. From the IAM menu, select **Groups**.

3. Filter the list to solution groups, and then in the search box, enter `SO0111`.
4. Choose **Add users to group**.
5. Choose the IAM users.
6. Choose **Add users**.

## User IAM permissions

Use the following process to add existing IAM users, roles, or groups, and to grant AWS Service Catalog permissions.

1. From the Security Hub primary account, navigate to the AWS Service Catalog console.
2. From the **Administration** menu, choose **Portfolios**.
3. Choose **Security Hub Playbooks** (`SO0111`).
4. Choose the **Groups, roles, and users** tab, and then choose **Add groups, roles, users**.
5. Choose the appropriate IAM entity type.
6. Use the search box to locate the IAM entities to grant access to. Note that the IAM entity selected must have permissions configured to allow AWS Service Catalog access.
7. Choose the entities to add and then choose **Add access**.

# Step 3: Deploy the playbook(s)

> **Note**
> If you are deploying this solution in an AWS Region in China, skip this step and refer to Appendix A (p. 16) to deploy the solution playbooks.

AWS Security Hub Automated Response and Remediation Version currently includes the CIS v1.2.0 playbook. Future releases might include additional playbooks. To install and upgrade playbooks, use AWS Service Catalog.

## Prerequisite

Before you deploy playbooks, verify that you have access to the AWS Service Catalog products:

1. From the Security Hub primary account, navigate to AWS Service Catalog in the AWS Management Console.
2. From the left navigation menu, open **Products**.
3. Confirm that **CIS** appears in the list of product names.

## Deployment

1. From the Security Hub primary account, navigate to the AWS Service Catalog console and choose **CIS**.
2. Choose **Launch Product**.
3. Enter a name for the instance. For example, `CIS-v-1-2-0`.
4. Choose the latest version.
5. Choose **Next.**

   On the **Parameters** page, each individual remediation has the option to be triggered automatically when a matching CloudWatch Logs event occurs for the finding. Use with care. The remediations

cannot be automatically undone. By default, the automatic trigger is disabled for all remediations. Make your selections and then choose **Next**.

# Step 4. Deploy the solution permissions

After you successfully deploy the solution in the primary account, and deploy the CIS playbooks from AWS Service Catalog, you must set up permissions to any secondary member accounts where security findings are to be remediated. This is required for the solution's automation functions.

Use the button below to download the `CISPermission.template` AWS CloudFormation template and then deploy it to the secondary accounts.

You can either use AWS CloudFormation StackSets, or manually sign in to each account and then deploy the permissions template.

# 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 Security Center.

## IAM roles

AWS Identity and Access Management (IAM) roles enable 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 AWS Lambda functions access to create Regional resources.

# Additional resources

**AWS services**

- AWS Security Hub
- AWS CloudFormation
- AWS Lambda
- Amazon CloudWatch Events
- 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

# Appendix A: Deploy the solution playbooks in AWS Regions in China

As of the date of publication, AWS Regions in China do not support AWS Service Catalog for playbook deployment. Therefore, AWS Security Hub Automated Response and Remediation, which includes the CIS v1.2.0 playbook, must be deployed using AWS CloudFormation.

Use the button below to download the `CIS.template` AWS CloudFormation template and then deploy it to the Security Hub primary account.


On the **Specify stack details** page, under **Parameters**, each individual remediation has the option to be triggered automatically when a matching Amazon CloudWatch Logs event occurs for the finding. The remediations cannot be automatically undone. Use these remediation options with caution. By default, the automatic trigger is disabled for all remediations. Make your selections before deploying the template.

# Appendix B: CIS v1.2.0 playbook

The CIS v1.2.0 playbook includes 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 https://www.cisecurity.org/cis-benchmarks/.

- 1.3 – Ensure credentials unused for 90 days or greater are disabled
- 1.4 – Ensure access keys are rotated every 90 days or less
- 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
- 2.2 – Ensure CloudTrail log file validation is enabled
- 2.3 – Ensure the S3 bucket CloudTrail logs to is not publicly accessible
- 2.4 – Ensure CloudTrail trails are integrated with Amazon CloudWatch Logs
- 2.6 – Ensure S3 bucket access logging is enabled on the CloudTrail S3 bucket
- 2.8 – Ensure rotation for customer created CMKs is enabled
- 2.9 – Ensure VPC flow logging is enabled in all VPCs
- 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

# Appendix C: Customize the playbooks

Download the AWS Security Hub Automated Response and Remediation solution playbook 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.

# Appendix D: Troubleshooting guide

**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 and update or delete the log groups that are not created.

**Issue:** The solution deploys successfully in AWS CloudFormation, but the playbook(s) are not visible in the AWS Service Catalog products list.

**Resolution:** Ensure that the user is part of the roles created by the solution: `SO0111-SHARR_Catalog_Admin` and `SO0111_SHARR_Catalog_User`.

**Issue:** After update, the `CISPermissions.template` corrupts the principal with an account key instead of the correct value.

**Resolution:** Remove and reinstall `CISPermissions.template`.

**Issue:** The CIS Permissions template failed to deploy in my Security Hub Member account. The error is `Service: AmazonIdentityManagement; Status Code: 400; Error Code: MalformedPolicyDocument.`

**Resolution:** This error typically occurs when the Lambda role has not been created in the Security Hub primary account. Ensure that the CIS Playbooks are installed in the Security Hub primary account, and that the correct primary account number was used when deploying the CIS Permissions template in the member account.

**Issue:** I run Security Hub in multiple Regions in the same account. I want to deploy this solution in multiple Regions.

**Resolution:** You can enable 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 2 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 remediate actions only for findings within the same Region (you may see findings across other Regions because they are aggregated at account level).

# Appendix E: Uninstall the solution

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

## Using the AWS Management Console

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 primary accounts.
4. 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.

# Appendix F: 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 task.

Modify the AWS CloudFormation template mapping section as follows:

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

to

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

# 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

# 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 |

# 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.