aws

Implementation Guide

Security Insights on AWS

Security Insights on AWS: Implementation Guide

Table of Contents

Create an automated, centralized security dashboard with pre-built widgets

Publication date: *March 2024*

The Security Insights on AWS solution helps analyze the data within your [Amazon Security Lake](#). Amazon Security Lake is a data lake service that's designed to collect security-related logs and events. It automatically centralizes security data from AWS environments, software as a service (SaaS) providers, and on-premises and cloud sources into a purpose-built data lake stored in your AWS account.

This solution provides a single pane view for your security data by creating an automated [Amazon QuickSight](#) dashboard. The dashboard's 20+ pre-built widgets show critical insights for data sources such as:

- [Amazon Virtual Private Cloud](#) (Amazon VPC)
- [AWS Security Hub](#)
- [AWS CloudTrail](#)
- [AWS AppFabric](#)

You can opt into the data sources that you're interested in and configure the insights' duration. You can use this dashboard to derive actionable insights and improve your security posture. You can visualize security key performance indicators (KPIs) and take action to enhance security across your cloud, on-premises, or hybrid environments.

> ⚠️ **Important**
>
> To use this solution, you must set up and configure a Security Lake and a QuickSight admin account. In addition, your Security Lake queries must use source version 2. For more details, see [Prerequisites](#).

This implementation guide provides an overview of the Security Insights on AWS solution, its reference architecture and components, considerations for planning the deployment, and configuration steps for deploying the solution to the Amazon Web Services (AWS) Cloud.

The intended audience for using this solution's features and capabilities in their environment includes IT security teams, solutions architects, business decision makers, and cloud professionals. To deploy this solution, you should have an understanding of your Security Lake.

Use this navigation table to quickly find answers to these questions:

If you want to . . .	Read . . .
Know the cost for running this solution. The estimated cost for running this solution in the US East (N. Virginia) Region is USD $620.86 a month for AWS resources to scan 100 GB of data. This doesn't include the cost of your existing Security Lake.	Cost
Understand the security considerations for this solution.	Security
Know how to plan for quotas for this solution.	Quotas
Know which AWS Regions support this solution.	Supported AWS Regions
View or download the AWS CloudFormation template included in this solution to automatically deploy the infrastructure resources (the "stack") for this solution.	AWS CloudFormation template
Access the source code and optionally use the AWS Cloud Development Kit (AWS CDK) to deploy the solution.	GitHub repository

Features and benefits

The solution provides the following features:

Visualize data from multiple sources

Security Lake supports many data sources for data aggregation. This solution supports four data sources for QuickSight analysis:

- VPC Flow Logs

- Security Hub findings

- CloudTrail management events

- AWS AppFabric audit log data

You can customize your QuickSight dashboard to display only the data sources you choose. To see widgets for a data source, enable the data source in your Security Lake.

Schedule your dataset refresh

You can configure the refresh frequency of the datasets that this solution creates by providing the input parameters to the CloudFormation template. The solution supports creating daily, weekly, and monthly refresh periods. This helps customize your experience to view the most recent and relevant data, as it fits your use case and budget. The default refresh period is set to weekly.

Assign permissions with user groups

This solution provisions two QuickSight user groups with read and admin permissions, respectively. You can use these groups to give access to the QuickSight analysis and dashboard. The read group provides access to the dashboard, and the admin group provides access to both the analysis and dashboard.

Receive alarms for excessive Athena usage and errors

The solution creates an Amazon Athena workgroup to run all the queries for creating QuickSight datasets. To monitor the data scanned as part of this workgroup, the solution creates an Amazon CloudWatch alarm. This alarm is set off when the data scanned by the solution exceeds a certain threshold.

You can configure this threshold when deploying the CloudFormation template for this solution. The default threshold is set to 100 GB per day. If the alarm is set off, you receive an Amazon Simple Notification Service (Amazon SNS) notification to the email address provided during the solution deployment. Customizing your threshold can help you manage your Athena usage to fit your use case and budget.

The solution also provisions an Amazon EventBridge rule to filter failure events for the Athena workgroup. If an Athena query run fails when updating the dataset, Amazon SNS sends failure notifications to the email address provided during the solution deployment.

Integration with Service Catalog AppRegistry and Application Manager, a capability of AWS Systems Manager

This solution includes a Service Catalog AppRegistry resource to register the solution's CloudFormation template and its underlying resources as an application in both Service Catalog AppRegistry and Application Manager. With this integration, centrally manage the solution's resources and enable application search, reporting, and management actions.

Use cases

This solution consolidates security findings into a dashboard with more than 20 widgets. The widgets display these findings both graphically and in a detailed table to help you simultaneously achieve a high-level overview and a detailed list for investigation. The following are example use cases.

Investigate security findings

You can use the pre-built widgets of this solution to identify findings such as:

- Unresolved security findings, such as failure to follow best practices or align with security standards and frameworks.
- Threat detection findings, such as unusual API calls or compromised compute resources.
- Suspicious login activity, such as 3 failed login attempts within a 30-minute window.

With these findings, you can focus on the security topics that matter most to your organization.

Investigate network traffic

You can use the pre-built widgets of this solution to identify findings such as:

- The top destination and source IPs for inbound and outbound network traffic.
- Which IPs were blocked.

You can use this information to help you diagnose overly restrictive security group rules and detect anomalies.

Investigate changes to your environment

You can use the pre-built widgets of this solution to identify findings such as:

- Your organization's top operational events.
- Your organization's top failed events.
- Accounts with the most failed events.
- Changes to your VPC security groups or network access control lists (NACLs).
- Changes to AWS Identity and Access Management (IAM) access keys.
- Changes to your AWS Key Management Service (AWS KMS) keys and policies.

You can use this information to help you detect anomalies and unwanted changes to your environment.

Concepts and definitions

This section describes key concepts and defines terminology specific to this solution:

contributing Region

One or more AWS Regions that contribute data to a rollup Region.

rollup Region

An AWS Region that consolidates security logs and events from one or more contributing Regions. Specifying one or more rollup Regions can help you comply with regional compliance requirements.

QuickSight analysis

The basic workspace for creating data visualizations, which are graphical representations of your data. Each analysis contains a collection of visualizations that you arrange and customize.

QuickSight dashboard

The published version of a QuickSight analysis. You can share with other users of QuickSight for reporting purposes. You specify who has access and what they can do with the dashboard.

For a general reference of AWS terms, see the AWS glossary.

Architecture overview

This section provides a reference implementation architecture diagram for the components deployed with this solution, as well as Well-Architected considerations.

Architecture diagram

Deploying this solution with the default parameters deploys the following components in your AWS account. The left side of the diagram shows the Security Lake account that you set up before deploying this solution. The right side of the diagram shows the solution deployed in a shared account with a QuickSight admin user.
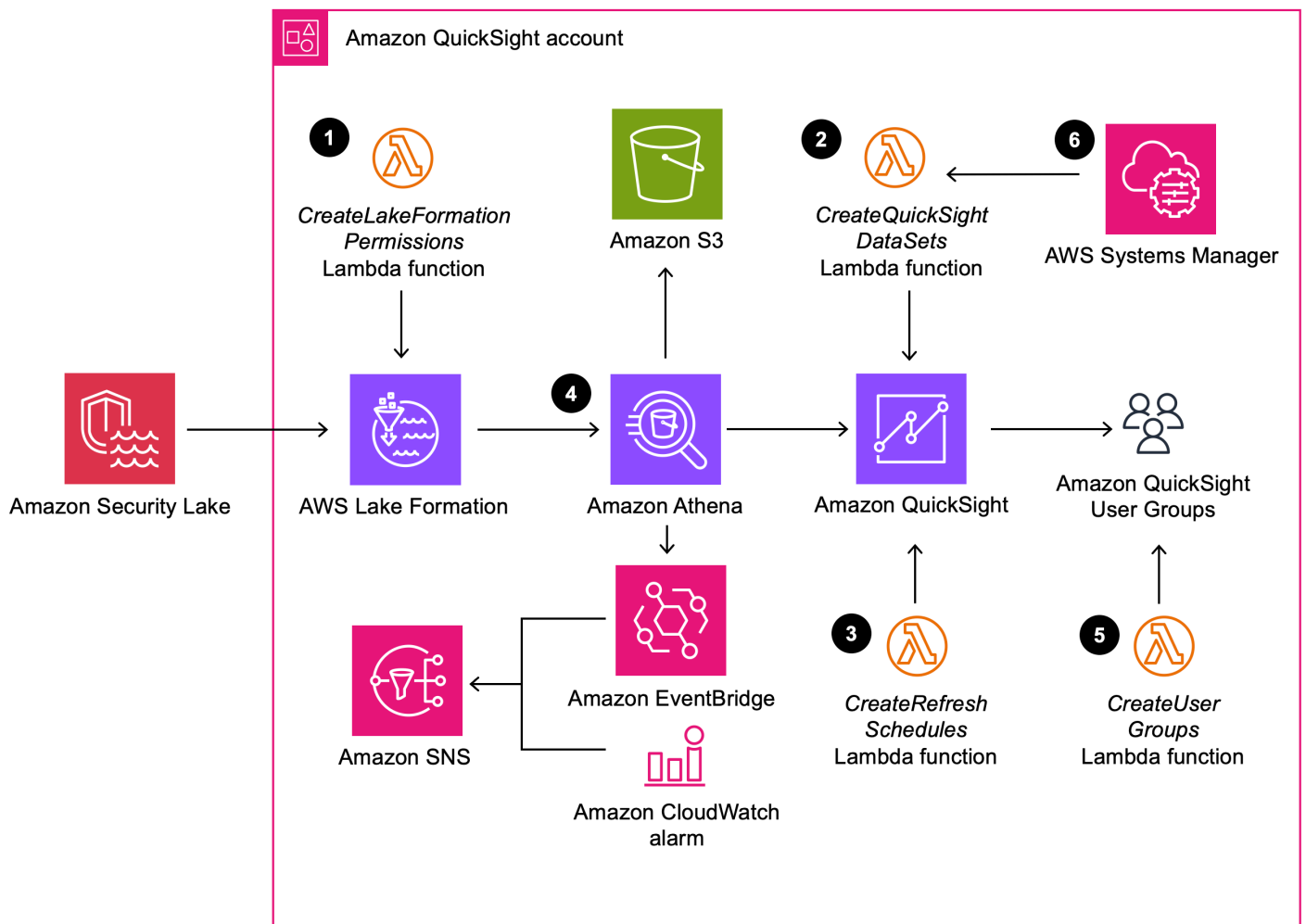
Security Insights on AWS architecture on AWS

> **ⓘ Note**
>
> AWS CloudFormation resources are created from AWS CDK constructs.

The high-level process flow for the solution components deployed with the AWS CloudFormation template is as follows:

1. **Create permissions** – The solution sets up the permissions needed to visualize the data from your Amazon Security Lake. As part of this setup, the solution:

   a. Adds the [AWS Identity and Access Management](#) (IAM) role for the `CreateLakeFormationPermissions` [AWS Lambda](#) function as one of the admins for the Security Lake.

   b. Grants `Describe` and `Select` permissions on the Security Lake database and [AWS Lake Formation](#) data tables to the following principals:

      - Service-linked role for QuickSight

      - QuickSight admin user provided in the input parameters to the solution's CloudFormation template

      - QuickSight user groups created by the solution

2. **Create datasets** – The solution provisions QuickSight datasets that are required for the QuickSight widgets.

3. **Create refresh schedules** – The solution provisions the QuickSight datasets with the refresh schedule provided as an input to the solution's CloudFormation template.

4. **Create Athena workgroup** – The solution creates an Athena workgroup and runs all the queries for the QuickSight datasets as part of this workgroup. As part of this setup, the solution:

   a. Creates an [Amazon Simple Storage Service](#) (Amazon S3) bucket to store Athena results.

   b. Creates a CloudWatch alarm for the Athena workgroup. You can set this threshold when deploying the solution's CloudFormation template. If the solution exceeds the threshold, the CloudWatch alarm invokes an action to send an Amazon SNS notification to the provided email address.

5. **Manage QuickSight users** – The solution provisions three QuickSight user groups with read, write, and admin permissions. You can use these groups to give different levels of access to the QuickSight analysis and dashboard.

6. **AWS Systems Manager parameters to configure QuickSight dashboards** – After launching the solution, you must enable the data sources for which you want to see the QuickSight analysis and dashboard insights.

AWS Well-Architected design considerations

This solution uses the best practices from the [AWS Well-Architected Framework](#), which helps customers design and operate reliable, secure, efficient, and cost-effective workloads in the cloud.

This section describes how the design principles and best practices of the Well-Architected Framework benefit this solution.

Operational excellence

This section describes how we architected this solution using the principles and best practices of the [operational excellence pillar](#).

1. The Lambda functions in the solution store the processing logs in the CloudWatch Logs. You can use these logs to debug and troubleshoot any errors.

2. The solution also sends Amazon SNS notifications for Athena query run failures.

Security

This section describes how we architected this solution using the principles and best practices of the [security pillar](#).

1. All roles used by the solution follow [least-privilege](#) access. The solution uses roles with only the necessary permissions to:
   - Limit the actions that can be performed
   - Restrict the actions to only the resources provisioned by the solution

2. The solution configures the S3 bucket created with [server-side encryption with Amazon S3 managed keys](#) (SSE-S3) and [Block Public Access](#) enabled.

3. The solution configures the Amazon SNS topic with encryption enabled.

4. The Athena workgroup provisioned by the solution has a security setting enabled to validate the account owner when making requests to the S3 bucket.

5. The solution provisions QuickSight user groups, which provide a way to restrict and manage access to the QuickSight analysis and dashboard.

Reliability

This section describes how we architected this solution using the principles and best practices of the reliability pillar.

1. The solution deploys a serverless architecture with Lambda functions for compute. Each Lambda function performs one independent function.

2. Every data source has its own Systems Manager parameters used to enable or disable data sources.

3. The solution creates an S3 bucket to store Athena results, providing high availability.

Performance efficiency

This section describes how we architected this solution using the principles and best practices of the performance efficiency pillar.

1. The solution runs Athena queries on Security Lake data, which is partitioned and compressed using Parquet columnar format.

2. You can configure the duration for insights, which reduces the data scanned by the Athena queries.

3. You can configure the refresh cycles for the data sources to reduce the number of times the Athena queries are run.

Cost optimization

This section describes how we architected this solution using the principles and best practices of the cost optimization pillar.

1. The solution uses serverless architecture, and you pay only for what you use.

2. The solution helps you save costs by providing option to choose which data sources you want to use for the QuickSight analysis.

3. The solution uses a lifecycle policy for the S3 bucket to delete objects after a year to help reduce the storage cost.

Sustainability

This section describes how we architected this solution using the principles and best practices of the [sustainability pillar](#).

The solution uses serverless architecture to minimize the environmental impact of the backend services. This design helps reduce the carbon footprint compared to the footprint of continually operating on-premises servers.

Architecture details

This section describes the components and AWS services that make up this solution and the architecture details on how these components work together.

QuickSight components

This section describes the QuickSight components of this solution.

QuickSight analysis

The solution creates a QuickSight analysis comprising multiple sheets. Each sheet displays relevant data visualizations to the following AWS service integrations in Security Lake: Amazon VPC, Security Hub, CloudTrail, and AppFabric.

Users can interact with the widgets, such as by selecting fields or filtering by specific parameters of the data visualizations.

See Working with an analysis in Amazon QuickSight for more information about how to use this feature of QuickSight.

QuickSight datasets

The QuickSight datasets are queried Athena results on relevant AWS Glue tables. The solution stores these datasets in Super-fast, Parallel, In-memory Calculation Engine (SPICE) as precomputed cache to optimize for quick reads.

Each widget presents its respective dataset graphically for the user, with the option to view more data in a table. Consequently, if there's an error with the dataset or it shows as empty, the widget won't show data.

QuickSight user groups

The solution provisions two QuickSight user groups with read and admin permissions, respectively. You can use these groups to give different levels of access to the QuickSight analysis and dashboard. The read group provides access to the dashboard, and the admin group provides access to both the analysis and dashboard.

Refresh schedules

The solution creates one dataset per widget in the QuickSight analysis. You can refresh the datasets so that the widgets show the latest data from the data tables. You can do this by setting the refresh frequency to daily, weekly, or monthly. The default refresh frequency is set to weekly.

The dataset refresh supported by the solution is FULL_REFRESH. With the weekly configuration, you can select which day of the week to refresh the dataset on. Similarly, with the monthly refresh option, you can select the day of the month to refresh the dataset on.

Systems Manager parameters

The solution creates Systems Manager parameters to help configure the data sources for the QuickSight analysis and dashboard. The solution supports four data sources and creates one Systems Manager parameter for each. The parameters created are:

- `/solutions/securityInsights/vpcFlowLogs`
- `/solutions/securityInsights/securityHub`
- `/solutions/securityInsights/cloudtrail`
- `/solutions/securityInsights/appFabric`

You can use these Systems Manager parameter to enable or disable the data source and to configure the duration for which you want to see the insights.

This solution also creates a `/solutions/securityInsights/updatePermissions` Systems Manager parameter for updating permissions to new data sources.

See Adjust Systems Manager parameters to learn how to adjust these parameters after deploying the solution.

Athena components

This section describes the Athena components of this solution.

Athena workgroup settings

The solution creates an Athena workgroup to run the Athena SQL queries for QuickSight datasets. The workgroup stores the results in an S3 bucket. This S3 bucket has SSE-S3 encryption enabled.

The workgroup's **Expected bucket owner** property is set to the AWS account ID of the deployment account.

Athena data usage alarm

The solution creates a CloudWatch alarm to monitor the amount of data scanned within the Athena workgroup. The default threshold for this alarm is 10GB/day. You can change the threshold value during the solution deployment by using the input parameters to the CloudFormation template.

If the amount of data scanned exceeds this threshold value, the solution changes the state of the alarm to **In Alarm**. We configured the alarm to send an SNS notification when this state changes. You will receive an email at the email address provided during the solution deployment.

> ⓘ **Note**
>
> If the CloudWatch alarm is active, you can disable the Athena quries by updating the Systems Manager parameters created by the solution. Disabling the Systems Manager parameters stops Athena from perfoming data scans on the Security Lake database.

SNS notifications

The SNS topic sends an email upon a failed Athena query from the relevant Athena workgroup. You can configure this failure notification email in the CloudFormation template parameter.

Lambda functions

This section describes the solution's Lambda functions.

CreateQuickSightDataSets

This Lambda function creates the QuickSight datasets that are necessary for the QuickSight analysis. When you deploy the solution, the datasets read data from the placeholder Glue data tables. You can enable or disable a data source by using the Systems Manager parameter created for the data source.

When the Systems Manager parameter for data source is enabled, the Lambda function updates the dataset SQL query to read from the Security Lake table. When the source is disabled, this Lambda function updates the dataset SQL query to read from the placeholder data tables.

CreateLakeFormationPermissions

This Lambda function sets up the permissions necessary for visualizing the data from your Security Lake. The solution invokes this Lambda function during the **Create** and **Delete** workflows for CloudFormation template by using a custom resource. The Lambda function adds its IAM role to the list of Security Lake administrators. This Lambda function also grants `Describe` and `Select` permissions on the Security Lake database and data tables in the Lake Formation service to the following principals:

- Service-linked role for QuickSight
- QuickSight admin user provided in the input parameters to the template
- QuickSight user groups created by the solution

As part of the **Delete** workflow, the Lambda function removes all the permissions that it created for showing the insights using a QuickSight dashboard.

CreateRefreshSchedules

This Lambda function creates the refresh schedules for QuickSight datasets. You can configure the refresh schedule by using the input parameters to the solution template. The default frequency is set to weekly.

CreateUserGroups

This Lambda function manages the creation and deletion of default user groups for QuickSight. This helps users to access the analysis and dashboard. The default user groups have admin and read only permissions, respectively. QuickSight admins have the permissions to add users to the newly created user groups.

AWS services in this solution

The solution uses the following services. Core services are required to use the solution, and supporting services connect the core services.

AWS service	Description
[Amazon Athena](#)	**Core.** The solution uses Amazon Athena to run queries against the data in your Security Lake.

AWS service	Description
AWS CloudFormation	**Core.** The solution uses AWS CloudFormation to deploy the infrastructure needed to set up the resources in the solution.
AWS Lake Formation	**Core.** The solution creates Lake Formation resource links to run Athena queries and retrieve insights from Lake Formation data.
AWS Lambda	**Core.** The solution provisions six Lambda functions for tasks like creating and updating datasets, setting up Lake Formation permissions, and creating user groups.
Amazon QuickSight	**Core.** The solution uses QuickSight to create analysis and a dashboard to show insights for data in your Security Lake.
Amazon S3	**Core.** The solution uses Amazon S3 to store query results for Athena**.**
Amazon SNS	**Core.** The solution uses Amazon SNS to send notifications for errors occurring when running Athena queries.
AWS Systems Manager	**Core.** The solution creates Systems Manager parameters to enable or disable data sources for analysis.
Amazon CloudWatch	**Supporting.** The solution uses CloudWatch Logs to store information about Lambda runs.
Amazon EventBridge	**Supporting.** The solution uses an EventBridge rule to filter error events during Athena query runs and send the event to the SNS topic.

AWS service	Description
AWS Glue	**Supporting.** The solution uses AWS Glue to set up placeholder data tables needed for the solution deployment. These tables store placeholder data for QuickSight analysis for the initial deployment.

Plan your deployment

This section describes the cost, security, Regions, and other considerations before deploying the solution.

> ⚠️ **Important**
>
> Modifying or making changes to the solution outside of AWS instructions and parameters cause the solution to fail. To customize the solution, use the parameters when deploying the solution and follow the instructions in the Developer guide.

Cost

You are responsible for the cost of the AWS services used while running this solution. The total cost for running this solution depends on the amount of data ingested, stored, and processed, the amount of data scanned by Amazon Athena queries, and the number of Amazon QuickSight readers and authors, along with their access time to the dashboard. As of this revision, the cost for running this solution with the default settings in the US East (N. Virginia) Region is approximately **$620.86 a month** to scan 100 GB of data. This cost is for the resources shown in the Sample cost tables. This doesn't include the cost of your exisiting Security Lake.

We recommend creating a budget through AWS Cost Explorer to help manage costs. Prices are subject to change. For full details, see the pricing webpage for each AWS service used in this solution.

Sample cost tables

The following table provides a sample cost breakdown for deploying this solution with the default parameters in the US East (N. Virginia) Region for one month.

	Small organization		Medium organization		Large organization	
AWS Service (example	**Dimensions/Month**	**Estimated Cost/Month [USD]**	**Dimensions/Month**	**Estimated Cost/Month [USD]**	**Dimensions/Month**	**Estimated Cost/Month [USD]**

	Small organization		Medium organization		Large organization	
region: us-east-1)						
QuickSight	5 Authors 20 Readers SPICE 10 GB free per Author	$122.00	5 Authors 50 Readers SPICE 10 GB free per Author	$172.80	10 Authors 100 Readers SPICE 10 GB free per Author	$340.00
QuickSight SPICE capacity	1 GB	$0.38	5 GB	$1.90	10 GB	$3.80
Lambda	512 MB 5 functions 1,000 invocations Average 1,500 millisecond duration per Lambda run	$0.01	512 MB 5 functions 10,000 invocations Average 1,500 millisecond duration per Lambda run	$0.13	512 MB 5 functions 1M invocations Average 1,500 millisecond duration per Lambda run	$12.70
Athena	30 queries, each scans 10 GB of data	$44.58	30 queries, each scans 100 GB of data	$445.80	30 queries, each scans 500 GB of data	$2,229.00

	Small organization		Medium organization		Large organization	
Amazon S3	1 GB	$0.02	10 GB	$0.23	100 GB	$2.30
Total Estimated Monthly Costs		$166.99		$620.86		$2,587.80

> ⓘ **Note**
>
> We optimized this solution so that Athena only scans certain fields, not your entire dataset. You can further reduce the amount of data scanned by the Athena queries by reducing the duration for which the queries are run from the Systems Manager parameters. For example, if you change the `queryWindowDuration` value from 7 to 2, the Athena queries scan the last 2 days of data, which reduces the amount of data scanned and helps reduce the cost for Athena queries.

Security

When you build systems on AWS infrastructure, security responsibilities are shared between you and AWS. This shared responsibility 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 AWS Cloud Security.

IAM roles

IAM roles allow customers to assign granular access policies and permissions to services and users on the AWS Cloud. This solution creates IAM roles that grant the solution's Lambda functions access to create Regional resources.

Supported AWS Regions

This solution requires the Security Lake service, which is not currently available in all AWS Regions. For the most current availability of AWS services by Region, see the AWS Regional Services List.

Security Insights on AWS is available in the following AWS Regions:

Region name	
US East (Ohio)	Asia Pacific (Sydney)
US East (N. Virginia)	Asia Pacific (Tokyo)
US West (Northern California)	Canada (Central)
US West (Oregon)	Europe (Frankfurt)
Asia Pacific (Mumbai)	Europe (Ireland)
Asia Pacific (Osaka)	Europe (London)
Asia Pacific (Seoul)	Europe (Paris)
Asia Pacific (Singapore)	South America (São Paulo)

Quotas

Service quotas, also referred to as limits, are the maximum number of service resources or operations for your AWS account.

Quotas for AWS services in this solution

Make sure you have sufficient quota for each of the services implemented in this solution. For more information, see AWS service quotas.

Use the following links to go to the page for that service. To view the service quotas for all AWS services in the documentation without switching pages, view the information in the Service endpoints and quotas page in the PDF instead.

AWS CloudFormation quotas

Your AWS account has AWS CloudFormation quotas that you should be aware of when launching the stack in this solution. By understanding these quotas, you can avoid limitation errors that would prevent you from deploying this solution successfully. For more information, see AWS CloudFormation quotas in the *AWS CloudFormation User's Guide*.

QuickSight quotas

Your AWS account has QuickSight quotas that you should be aware of when using this solution. In particular, there is a maximum number of fields that datasets can contain, and a maximum number of distinct items that a sheet control can display. We built this solution to function within these quotas. However, by understanding these quotas, you can avoid limitation errors that would prevent you from deploying this solution successfully. For more information, see Amazon QuickSight service quotas in the in the *AWS General Reference Guide*.

Deploy the solution

This solution uses AWS CloudFormation templates and stacks to automate its deployment. The CloudFormation template specifies the AWS resources included in this solution and their properties. The CloudFormation stack provisions the resources that are described in the template.

Deployment process overview

Follow the step-by-step instructions in this section to configure and deploy the solution into your account.

Before you launch the solution, review the cost, architecture, network security, and other considerations discussed earlier in this guide.

Time to deploy: Approximately five to ten minutes

Step 1: Launch the stack

Step 2: Enable Systems Manager parameters

> ⚠️ **Important**
>
> This solution includes an option to send anonymized 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 through this survey. Data collection is subject to the AWS Privacy Notice.
>
> 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 updated template and deploy the solution. For more information, see the Anonymized data collection section of this guide.

AWS CloudFormation template

You can download the CloudFormation template for this solution before deploying it.

View template

_____**securit**

insights-on-aws.template – Use this template to launch the solution and all associated components. The default configuration deploys the core and supporting services found in the [AWS services in this solution](#) section, but you can customize the template to meet your specific needs.

> ℹ️ **Note**
>
> AWS CloudFormation resources are created from AWS CDK constructs.

This AWS CloudFormation template deploys this solution in the AWS Cloud.

Prerequisites

You must meet the following prerequisites before launching the stack.

Security Lake setup

The Amazon Security Lake centralizes your security data using Lake Formation and Amazon S3 buckets. Before deploying this solution, enable and configure your Security Lake. For more information about Security Lake, see the [Getting started with Amazon Security Lake](#) in the *Amazon Security Lake User Guide*.

Security Lake table sharing

If you're deploying the solution in the **delegated admin account** for the Security Lake, you don't need additional setup.

If you're deploying this solution in **any other account**, share the Security Lake tables with the deployment account using the Security Lake service console. You can create a [subscriber](#) from the Security Lake console, and then Security Lake shares the data tables with another account. This creates an [AWS Resource Access Manager](#) (AWS RAM) resource share with the subscriber account. You can accept this share from AWS RAM, which sets up the required tables in this account. For more information, see [Accepting a resource share invitation from AWS RAM](#) in the *AWS Lake Formation Developer Guide*.

Rollup Region

If you want the solution to show security insights for your entire AWS Organization, deploy the solution in the rollup Region selected when you set up your Security Lake. The rollup Region has centralized data for your entire AWS Organization. The solution uses the Lake Formation database that your Security Lake created in this rollup Region to query and get data. If you don't deploy the solution in the rollup Region, the solution only generates insights from the data within the deployed Region. For more information, see [Step 2: Define storage settings and rollup Regions (optional)](#) and [Managing multiple accounts with AWS Organizations](#) in the *Amazon Security Lake User Guide*.

QuickSight admin account

The solution uses QuickSight to show insights for data within your Security Lake. You must have a QuickSight admin account to deploy the solution and provide the Amazon Resource Name (ARN) for the admin user as one of the parameters to the solution. For more information, see [Create an administrative user](#) and [Managing user access inside Amazon QuickSight](#) in the *Amazon QuickSight User Guide*.

QuickSight uses a service role to access data from Athena and Amazon S3. This solution adds QuickSight as the one of the principals for the Lake Formation database and tables. The solution only provides SELECT and DESCRIBE access to this role. This is required so that:

- The solution can refresh the QuickSight datasets
- QuickSight can run Athena queries on the data in the Lake Formation database

For more information, see [Lake Formation permissions reference](#) in the *AWS Lake Formation Developer Guide* and [Authorizing connections to Amazon Athena](#) in the *Amazon QuickSight User Guide*.

Data sources

The solution creates a QuickSight analysis and dashboard to show insights from four supported data sources.

> ⚠️ **Important**
>
> For this solution to work properly, your Security Lake queries must use source version 2. For more information, see [Security Lake queries for source version 2](#) and [Source management in Amazon Security Lake](#).

To see these visualizations and insights, enable the data sources in Security Lake. If the data source isn't enabled, QuickSight won't show data for the corresponding sheet in the analysis. For example, If the VPC Flow Logs data source is not enabled in the Security Lake, the **VPC Flow Logs** sheet won't show data in the analysis. For more information, see [Source management in Amazon Security Lake](#) in the *Amazon Security Lake User Guide*.

AWS AppFabric setup

AWS AppFabric connects software as a service (SaaS) applications across your organization. You can get your SaaS audit logs into Amazon Security Lake in your AWS account by adding a custom source to Security Lake.

To set up AWS AppFabric, see [Getting started with AWS AppFabric for security](#).

To use AWS AppFabric with your Security Lake, see [AppFabric audit log ingestion considerations](#).

Step 1: Launch the stack

Follow the step-by-step instructions in this section to configure and deploy the solution into your account.

Time to deploy: Approximately five to ten minutes.

1.

    [**Launch solution**] Sign in to the [AWS Management Console](#) and select the button to launch the `security-insights-on-aws.template` AWS CloudFormation template.

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

> ⓘ **Note**
>
> This solution requires the Security Lake service, which is not currently available in all AWS Regions. For the most current availability by Region, see 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 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 AWS STS quotas, name requirements, and character limits](#) in the *AWS Identity and Access Management User Guide*.

5. Under **Parameters**, review the parameters for this solution template and modify them as necessary. This solution uses the following default values.

Parameter	Default	Description
Account ID where Security Lake is created	*<Requires input>*	Account ID in which you created your Security Lake. > ⓘ **Note** > You can't update this parameter after you deploy the solution. If you need to change it, see [Problem: Change your account ID](#).
ARN for QuickSight admin user	*<Requires input>*	QuickSight ARN for admin. To retrieve this ARN, you must have access to a shell or terminal with the AWS CLI installed. For installation instructions, refer to [What](#)

Parameter	Default	Description
		Is the AWS Command Line Interface in the *AWS CLI User Guide*. Optionally, you can use the AWS CloudShell service to run AWS CLI commands. Running the following command returns the list of users with their corresponding QuickSight User ARNs. `aws quicksight list-users --region` *`<aws-region>`* `--aws-account-id` *`<account-id>`* `--namespace` *`<namespace-name>`* The *`<namespace-name>`* is `default`, unless explicitly created in Amazon QuickSight. Choose an **Admin** user, or a user who has permissions to create QuickSight resources in that account and AWS Region.
Frequency for QuickSight Dataset refresh	`Weekly`	Dataset refresh frequency. The options are DAILY, WEEKLY, and MONTHLY.

Parameter	Default	Description
Day of the week for weekly refresh of QuickSight Dataset	Monday	The day of the week on which the dataset refreshes for a WEEKLY frequency. If the frequency is set to DAILY or MONTHLY, this parameter has no impact.
Day of the month for monthly refresh of QuickSight Dataset	1	The day of the month on which the dataset refreshes for a MONTHLY frequency. If the frequency is set to DAILY or WEEKLY, this parameter has no impact.
Log level for the Lambda functions	Info	Log level for Lambda function logs.
Email ID to receive QuickSight Dataset refresh alerts	*<Requires input>*	Email address where you want to receive alerts for error notifications.
Threshold value in GB for Alarm on Athena Workgroup	100	Threshold value for the alarm on the Athena workgroup. The default measurement is GB, which you can adjust in the unit parameter.
Unit for threshold value for Athena Alarm	GB	Unit for the threshold value for the Athena alarm.

6. Select **Next**.

7. On the **Configure stack options** page, choose **Next**.

8. On the **Review** page, review and confirm the settings. Select the box acknowledging that the template will create IAM resources.

9. 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 five to ten minutes.

Step 2: Enable Systems Manager parameters

The solution creates one Systems Manager parameter per data source. By default, all the parameters are disabled. Enable each parameter to see the corresponding QuickSight widgets for the data source:

1. Sign in to the [Systems Manager console](#).

2. In the navigation pane, choose **Parameter Store**.

3. Select the parameter for the data source.

4. Choose **Edit**.

5. Under **Value**:

   a. Change the `status` from `Disabled` to `Enabled`.

   b. If desired, change the `queryWindowDuration`. See [Adjust Systems Manager parameters](#) for instructions.

6. Choose **Save changes**.

Monitoring the solution with Service Catalog AppRegistry

The solution includes a Service Catalog AppRegistry resource to register the CloudFormation template and underlying resources as an application in both Service Catalog AppRegistry and AWS Systems Manager Application Manager.

AWS Systems Manager Application Manager gives you an application-level view into this solution and its resources so that you can:

- Monitor its resources, costs for the deployed resources across stacks and AWS accounts, and logs associated with this solution from a central location.

- View operations data for the solution's AWS resources (such as deployment status, Amazon CloudWatch alarms, resource configurations, and operational issues) in the context of an application.

The following figure depicts an example of the application view for this solution stack in Application Manager.

Security Insights on AWS stack in Application Manager

> **ⓘ Note**
>
> You must activate CloudWatch Application Insights, AWS Cost Explorer, and cost allocation tags associated with this solution. They are not activated by default.

Activate CloudWatch Application Insights

1. Sign in to the Systems Manager console.

2. In the navigation pane, choose **Application Manager**.

3. In **Applications**, choose **AppRegistry applications**.

4. In **AppRegistry applications**, search for the application name for this solution and select it.

   The next time you open Application Manager, you can find the new application for your solution in the **AppRegistry application** category.

5. In the **Components** tree, choose the application stack you want to activate.

6. In the **Monitoring** tab, in **Application Insights**, select **Auto-configure Application Monitoring**.
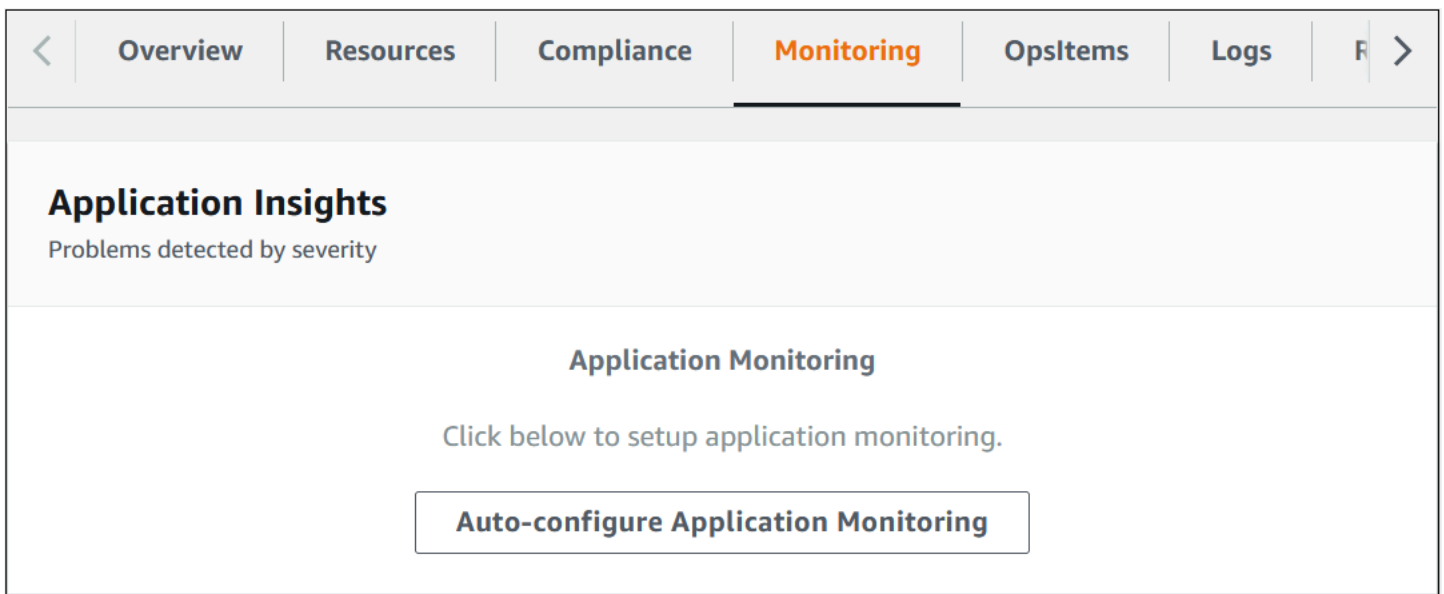
Monitoring for your applications is now activated and the following status box appears:
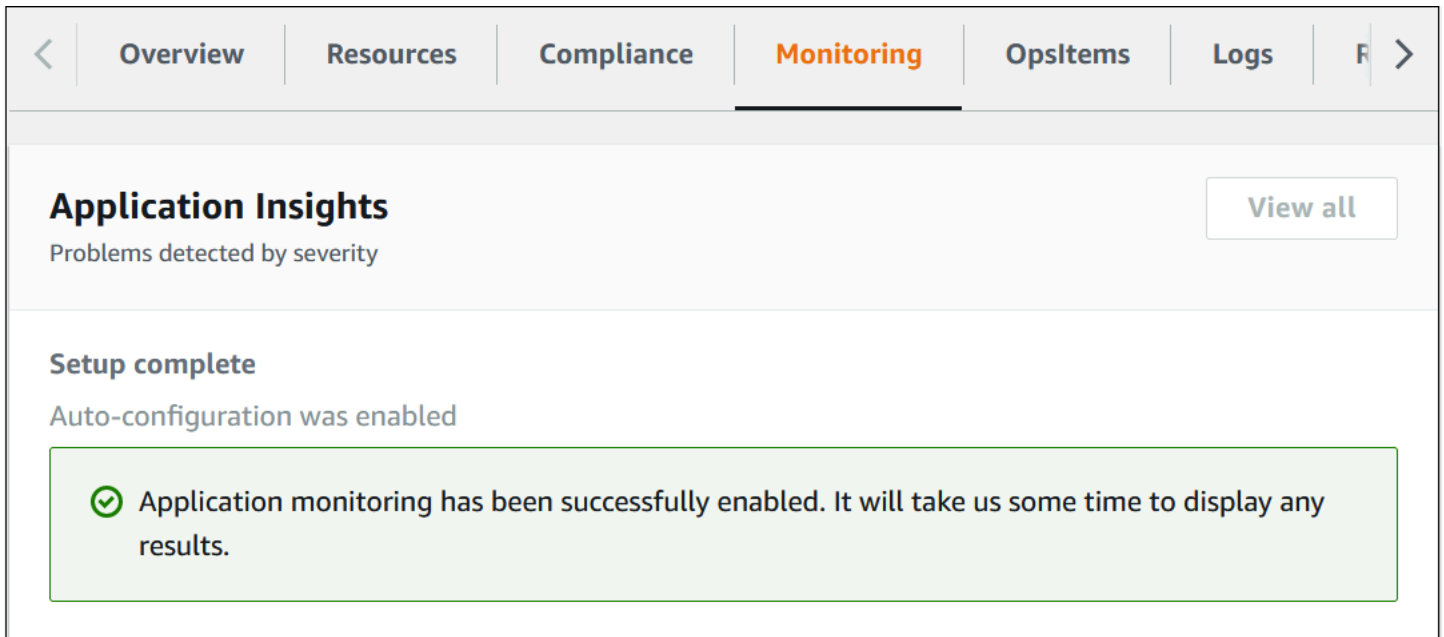
Activate AWS Cost Explorer

You can see the overview of the costs associated with the application and application components within the Application Manager console through integration with AWS Cost Explorer which must be first activated. Cost Explorer helps you manage costs by providing a view of your AWS resource costs and usage over time. To activate Cost Explorer for the solution:

1. Sign in to the [AWS Billing and Cost Management console](#).

2. In the navigation pane, select **Cost Explorer**.

3. On the **Welcome to Cost Explorer** page, choose **Launch Cost Explorer**.

The activation process can take up to 24 hours to complete. Once activated, you can open the Cost Explorer user interface to further analyze cost data for the solution.

Confirm cost tags associated with the solution

After you activate cost allocation tags associated with the solution, you must confirm the cost allocation tags to see the costs for this solution. To confirm cost allocation tags:

1. Sign in to the [Systems Manager console](#).

2. In the navigation pane, choose **Application Manager**.

3. In **Applications**, choose the application name for this solution and select it.

4. In the **Overview** tab, in **Cost**, select **Add user tag**.

Cost   View all

View resource costs per application using AWS Cost Explorer.

To enable cost tracking, add the "AppManagerCFNStackKey" user tag to your CloudFormation stack.

Adding the user tag will require redeployment of the stack.
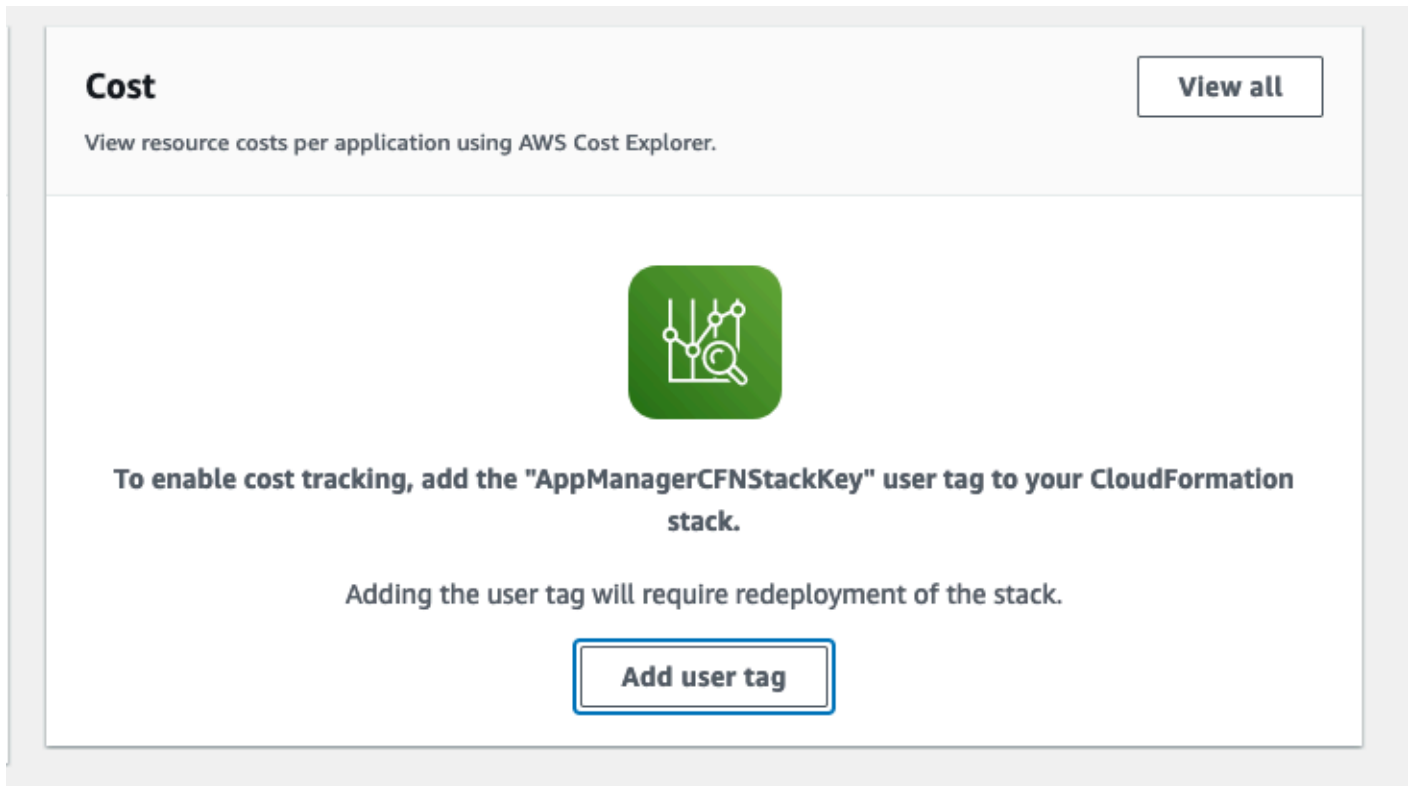
Add user tag

5. On the **Add user tag** page, enter `confirm`, then select **Add user tag**.

The activation process can take up to 24 hours to complete and the tag data to appear.

Activate cost allocation tags associated with the solution

After you activate Cost Explorer, you must activate the cost allocation tags associated with this solution to see the costs for this solution. The cost allocation tags can only be activated from the management account for the organization.

> ⓘ **Note**
>
> The activation process can take up to 24 hours to complete and the tag data to appear.

To activate cost allocation tags:

1. Sign in to the AWS Billing and Cost Management and Cost Management console.

2. In the navigation pane, select **Cost Allocation Tags**.

3. On the **Cost allocation tags** page, filter for the `AppManagerCFNStackKey` tag, then select the tag from the results shown.

4. Choose **Activate**.

Troubleshooting

This section provides troubleshooting instructions for deploying and using the solution.

Problem: Changing your account ID

You can't change your input to the **Account ID where Security Lake is created** parameter after you deploy this solution.

Resolution

If your Security Lake account ID changes, [uninstall the solution](#) and then [re-deploy](#) it with the new account ID.

Problem: QuickSight widgets don't show data

There could be several reasons why your QuickSight widgets aren't showing data.

Resolution 1: Enable the Systems Manager parameter data source

This error might happen if the value to enable the data source isn't set to `Enabled`. For example, a typo can result in errors and data not being shown in the widgets.

To resolve this issue, correct the value and save the parameter again. See [Enable data and insights](#) for more detailed instructions.

Resolution 2: Enable the data source in Security Lake

This error can also happen if the data source isn't enabled in Security Lake. To resolve this issue:

1. Enable the data source in Security Lake. See [Data sources](#) for more detailed instructions.
2. Update the `/solutions/securityInsights/region/updatePermissions` Systems Manager parameter by increasing the version number and saving the parameter. This adds the required permissions to the new data source. See [Update permissions to new data sources](#) for more detailed instructions.
3. [Disable](#) and [enable](#) the Systems Manager parameter again for the data source.

Resolution 3: Increase the query window duration

If a particular widget isn't showing data, the data for those events might not have been generated in the configured `queryWindowDuration` parameter.

To resolve this issue, increase the number for this parameter. This results in Athena scanning data for more days. If the corresponding events occurred in that period, then the data will show in the widgets. See Change the duration for more detailed instructions.

Uninstall the solution

You can uninstall the Security Insights on AWS solution from the AWS Management Console or by using the AWS Command Line Interface (AWS CLI). You must manually delete the CloudWatch Logs and S3 bucket created by this solution. AWS Solutions do not automatically delete these resources in case you have stored data to retain.

Using the AWS Management Console

1. Sign in to the CloudFormation console.

2. On the **Stacks** page, select this solution's installation stack.

3. Choose **Delete**.

Using AWS Command Line Interface

Determine whether the AWS CLI is available in your environment. For installation instructions, see What Is the AWS Command Line Interface in the *AWS CLI User Guide*. After confirming that the AWS CLI is available, run the following command.

```
$ aws cloudformation delete-stack --stack-name <installation-stack-name>
```

Deleting the CloudWatch Logs

The solution configures all the Lambda functions with a log retention period of 365 days. These logs are retained and not deleted when solution template is deleted. Follow these steps to delete the CloudWatch Logs.

1. Sign in to the CloudWatch console.

2. Choose **Log groups** from the left navigation pane.

3. Locate the *<stack-name>* CloudWatch Logs.

4. Select each CloudWatch Log and choose **Actions**, then **Delete log groups.**

5. Confirm the deletion.

To delete the CloudWatch Logs using the AWS CLI, run the following command:

```
$ aws logs delete-log-group --log-group-name <log-group-name>
```

Deleting the Amazon S3 bucket

This solution is configured to retain the solution-created S3 bucket to store Athena query results if you decide to delete the AWS CloudFormation stack, to prevent accidental data loss. After uninstalling the solution, you can manually delete this S3 bucket if you don't need to retain the data. Follow these steps to delete the Amazon S3 bucket.

1. Sign in to the [Amazon S3 console](#).
2. Choose **Buckets** from the left navigation pane.
3. Locate the *<stack-name>* S3 buckets.
4. Select the S3 bucket and choose **Delete**.

To delete the S3 bucket using AWS CLI, run the following command:

```
$ aws s3 rb s3://<bucket-name> --force
```

Use the solution

This section provides a user guide for using the AWS solution.

Access and use the solution

This solution creates a QuickSight dashboard with widgets for all four data sources. To access the QuickSight dashboard, follow these steps:

1. Sign in to the [QuickSight console](#).
2. Choose this solution's QuickSight dashboard.

The dashboard provides one tab for each data source: **VPC Flow Logs**, **AWS Security Hub**, **CloudTrail**, and **AWS AppFabric**. These tabs include the following widgets, plus detailed tables. By default, each widget scans the previous seven days of data.

VPC Flow Logs	AWS Security Hub	CloudTrail	AWS AppFabric
Top 25 Destinati on IPs for Inbound Network Traffic (Separated by Disposition)	Security Hub Findings by Severity and WorkFlow Status	Top 10 API Events by Status	User Logins By SaaS Apps
Top 25 Destination IPs for Outbound Network Traffic (Separated by Disposition)	Security Hub Findings by Severity and WorkFlow Status Details	Distribution of API Events	Top 25 Apps With Most Failed Logins
Top 25 Source IPs for Inbound Network Traffic (separated by Disposition)	Top 25 Unresolved Findings by Time	Top 25 APIs with most failures	Suspicious Login Activities (3 consecuti ve failed logins in 30 mins)

VPC Flow Logs	AWS Security Hub	CloudTrail	AWS AppFabric
Top 25 Source IPs for Outbound Network Traffic (separated by Disposition)	Summary Status for Resolved vs New GuardDuty Findings	Top 25 UIDs for API Failures	Top 25 IP Addresses By SaaS Login Activity
Network Traffic By Region	Summary Status of Resolved vs New Findings	Top Regions with Most API Failures	
		Top 25 Accounts with Most API Failures	
		VPC Security Group Rule Changes by Type	
		VPC Network Access Control List (NACL) Changes by Type	
		Route Table Changes by Type	
		IAM Access Key Related Changes	
		KMS Key Policy Changes	
		KMS Keys Set for Deletion	
		Total Number of Failed and Successful IAM Logins	

VPC Flow Logs	AWS Security Hub	CloudTrail	AWS AppFabric
		Total Number of Root User Login Attempts by Success Rate and MFA Usage	

The dashboard also has widgets that show details, such as user IDs, account IDs, and Regions for events. These widgets only show 25 rows per category to avoid creating a large dataset which might use a large SPICE capacity. For example, **Details for Destination IPs for Inbound Traffic Network** only shows 25 rows per IP address.

Adjust Systems Manager parameters

The solution supports four data sources and creates one Systems Manager parameter for each. The parameters created are:

- `/solutions/securityInsights/vpcFlowLogs`
- `/solutions/securityInsights/securityHub`
- `/solutions/securityInsights/cloudtrail`
- `/solutions/securityInsights/appFabric`

You can use these Systems Manager parameters to enable or disable the data source and to configure the duration for which you want to see your insights. The default Systems Manager parameter has the following value:

```
{"status":"Disabled","queryWindowDuration":"7"}
```

Enable data and insights

To see the data and insights in the QuickSight analysis:

1. Sign in to the Systems Manager console.

2. In the navigation pane, choose **Parameter Store**.

3. Select the parameter for the data source.

4. Choose **Edit**.

5. Under **Value**, change the `status` from `Disabled` to `Enabled`.

6. Choose **Save changes**.

Disable data and insights

If you no longer want to see the insights for the data source of VPC Flow Logs:

1. Sign in to the [Systems Manager console](#).

2. In the navigation pane, choose **Parameter Store**.

3. Select the parameter for the data source.

4. Choose **Edit**.

5. Under **Value**, change the `status` from `Enabled` to `Disabled`.

6. Choose **Save changes**.

Change the duration

You can use the `queryWindowDuration` field to configure the duration in days for which you want to see the results.

1. Sign in to the [Systems Manager console](#).

2. In the navigation pane, choose **Parameter Store**.

3. Select the parameter for the data source.

4. Choose **Edit**.

5. Under **Value**, change the "`queryWindowDuration`" to your desired number of days.

6. Choose **Save changes**.

For example, if you need to see the analysis for VPC Flow Logs for the past 30 days, change the value of the `/solutions/securityInsights/vpcFlowLogs` parameter to the following value:

```
{"status":"Enabled","queryWindowDuration":"30"}
```

> ⓘ **Note**
>
> We recommend minimizing this duration as much as possible to avoid large data scans. A shorter duration lessens the amount of data scanned by Athena queries, which in turn helps minimize cost.

Update permissions to new data sources

This solution creates a /solutions/securityInsights/updatePermissions Systems Manager parameter for updating permissions to new data sources.

When you deploy the solution, it creates the permissions needed to visualize your data. The solution only creates these permissions for the data sources that you enable when you deploy the solution. If you enable a data source after deployment:

1. Sign in to the Systems Manager console.

2. In the navigation pane, choose **Parameter Store**.

3. Select the **/solutions/securityInsights/updatePermissions** parameter.

4. Choose **Edit**.

5. Under **Version**, update the version number.

6. Choose **Save changes**.

This invokes the Lambda function to update the permissions for the new data source.

Change the CloudWatch log group retention period

The solution's Lambda functions create CloudWatch log groups. These log groups have a retention period of one year and record information about how the Lambda functions run. To change the retention period, follow these steps:

1. Sign in to the CloudFormation console.

2. Choose this solution's stack.

3. Select the **Resources** tab, and choose **Flat view**.

4. Enter logs in the **Search resources** box.

5. Choose the log group that you want to edit.

6. Choose **Actions**. Select **Edit retention setting(s)**, then select the option that you want for the retention period of the log group.

If you want to change the retention period for multiple functions using the same log group, you can update the retention period in CloudWatch Logs. For more information, see Change log data retention in CloudWatch Logs in the *Amazon CloudWatch Logs User Guide*.

Developer guide

This section provides the source code for the solution and an API reference.

Source code

Visit our GitHub repository to download the source files for this solution and to share your customizations with others.

The AWS CDK generates the solution templates. See the README.md file for additional information.

Customization guide

This section provides a guide for customizing the solution.

Customize widgets

You can customize the solution's widgets and add more columns from the data source tables created by the Security Lake service. However, these updates will be overwritten if you upgrade the solution to a newer version. For more information, see Working with an analysis in Amazon QuickSight.

Build new widgets

To build your own widgets, follow these steps:

1. Create a duplicate of the dataset that you want to customize from the QuickSight service console. For instructions, see Duplicating datasets in the *Amazon QuickSight User Guide*.
2. Edit the dataset to add or remove columns.
3. Use the updated dataset and create your own analysis. For more information, see Starting an analysis in Amazon QuickSight.

> **ⓘ Note**
>
> The custom analysis that you create won't update when the solution receives updates.

API reference

You can use the following API operations to control the solution's pipelines. The following is a description of all attributes with examples of required attributes per pipeline type.

- `/inference`
  - Method: POST
  - Body
    - `Payload`: The data to be sent for inference.
    - `ContentType`: MIME content type for the payload.

      ```
      {
        "payload": "1.0, 2.0, 3.2",
        "content_type": "text/csv"
      }
      ```

  - Expected responses of APIs requests to `/inference`:
    - If one data point was in the request, the request returns a single prediction value.
    - If multiple data points were in the request, the request returns multiple prediction values (separated by a `,`).

Reference

This section includes information about an optional feature for collecting unique metrics for this solution, pointers to related resources, and a list of builders who contributed to this solution.

Anonymized data collection

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

- **Solution ID** - The AWS solution identifier
- **Unique ID (UUID)** - Randomly generated, unique identifier for each Security Insights on AWS deployment
- **Timestamp** - Data-collection timestamp

AWS owns the data gathered through this survey. Data collection is subject to the [Privacy Notice](). To opt out of this feature, complete the following steps before launching the AWS CloudFormation template.

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

```
AnonymizedData:
    SendAnonymizedData:
      Data: Yes
```

to:

```
AnonymizedData:
    SendAnonymizedData:
      Data: 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](#) in the Deploy the solution section of this guide.

Contributors

- Chaitanya Deolankar

- William Quan

Revisions

For more information, see the CHANGELOG.md file in the GitHub repository.

Date	Change
March 2024	Initial release.

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.

Security Insights on AWS is licensed under the terms of the Apache License Version 2.0 available at [The Apache Software Foundation](#).