sysdig | aws

Forwarding Sysdig Events to Amazon Security Lake

In the vast realm of cloud-native security, understanding and analyzing your security data is paramount. Sysdig has emerged as a comprehensive security platform that provides detailed Runtime Insights into your systems. When integrated with Amazon Security Lake, you unlock a powerful centralized platform for your security data analytics. This guide offers a step-by-step walkthrough to seamlessly integrate Sysdig with Amazon Security Lake.

Table of Contents

Concepts

OCSF

The Open Cybersecurity Schema Framework (OCSF) is a collaborative open source schema framework. The OCSF provides a standard schema for many event types. Amazon Web Services (AWS) has adopted this schema type for Amazon Security Lake data. Please see the links below for more information.

- Open Cybersecurity Schema Framework (OCSF)
- OCSF Schema

Parquet

This is an open source file format that is used for storing flat columnar data in an efficient manner that optimizes query performance.

- Parquet Documentation

Sysdig Events/Logs

The Sysdig event forwarding feature allows you to send Policy events, Sysdig platform audit, Benchmarks (legacy), and host scanning.

Policy events
These are Sysdig runtime insights events that are based on various policies/rules.

- Event Forwarding

Sysdig Platform audit
These are Sysdig platform events. This would include policy modifications, user addition, what alert modifications were made, etc.

- Sysdig Platform Audit

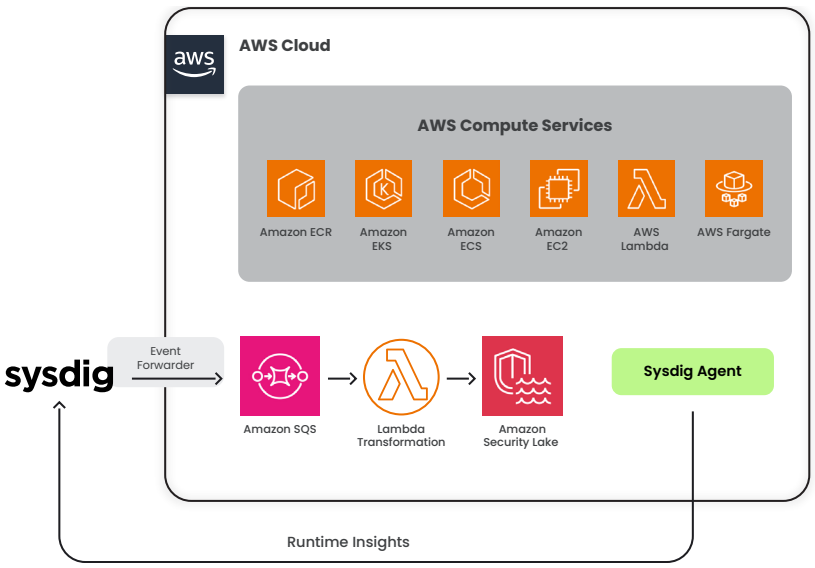
Benchmarks (legacy)
These are drift events related to various compliance frameworks.

- Compliance Legacy Versions

Host Scanning
These are events related to host vulnerability automated and manual scans.

- Host Scanning

Figure 1:
Sysdig Security Lake Architecture



Prerequisites

- **AWS Account(s):** With roles setup with permissions for AWS Lambda, Amazon SQS, and AWS CloudFormation. (You will need an AWS account with Amazon Security Lake enabled. You will also need access to any AWS accounts you want to forward events to Amazon Security Lake from).
- **Sysdig Account:** With event forwarding capabilities.
- **Sysdig ExternalID:** If you have deployed the Sysdig AWS CloudFormation template, you can find this in the AWS CloudFormation parameters tab. Otherwise, you can navigate in the Sysdig UI and go to Integrations -> Cloud Accounts -> Add an AWS single account -> click on the launch stack -> locate your External ID.
- **AWS IAM User:** An AWS IAM user that has been created in the AWS account that you will be forwarding events to that has Amazon SQS permissions to the event forwarding queue that will hold the Sysdig events for Amazon Security Lake.
- **Amazon Security Lake Custom Source:** Custom source configured with Sysdig external ID.
- **Knowledge:** A basic understanding of AWS Lambda, Amazon SQS, Amazon S3, and AWS CloudFormation.

Create a Custom Source in Amazon Security Lake for Sysdig

Amazon Security Lake is a landing spot for events from both AWS services and external partners alike. Amazon Security Lake uses the custom source construct to allow partners to send events. You will need to create a custom source in Amazon Security Lake for Sysdig. This will create both the IAM role and Amazon S3 bucket needed for Amazon Security Lake. During the creation process, you will be asked for your Sysdig External ID. You can find more details on creating the custom source below:

- Collecting data from custom sources

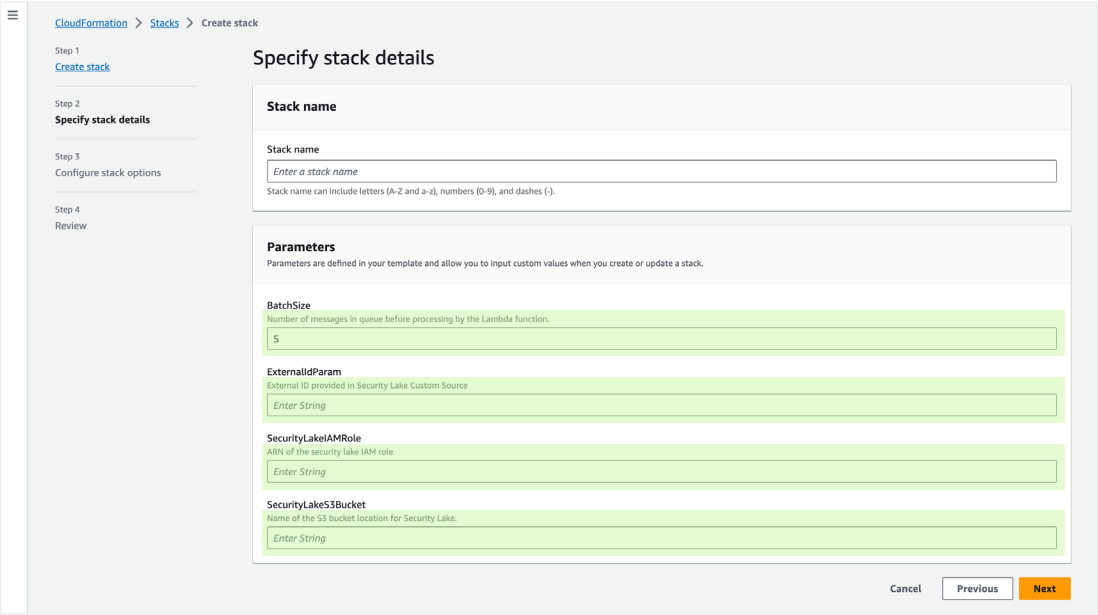
Deploying AWS Resources

01

AWS CloudFormation Stack Deployment:

1. Access AWS CloudFormation via AWS Console.
2. Start a new stack creation process.
   a. If you don't already have the Sysdig event forwarding to Amazon SQS feature setup (this will create a Sysdig eventforwarding queue/DLQ, execution role, as well as deploy the lambda function as a trigger):
      - https://sysdig-securitylake-lambda.s3.amazonaws.com/SecurityLake.yaml
   b. If you already have the Sysdig event forwarding to Amazon SQS feature setup, deploy the following cloudformation and configure the lambda function as an Amazon SQS trigger (use this if you already have the Amazon SQS queues setup and the event forwarding from Sysdig setup. This will just deploy the lambda function for the trigger):
      - https://sysdig-securitylake-lambda.s3.amazonaws.com/SysdigSecurityLake.yaml

Figure 2: AWS CloudFormation Stack Parameters



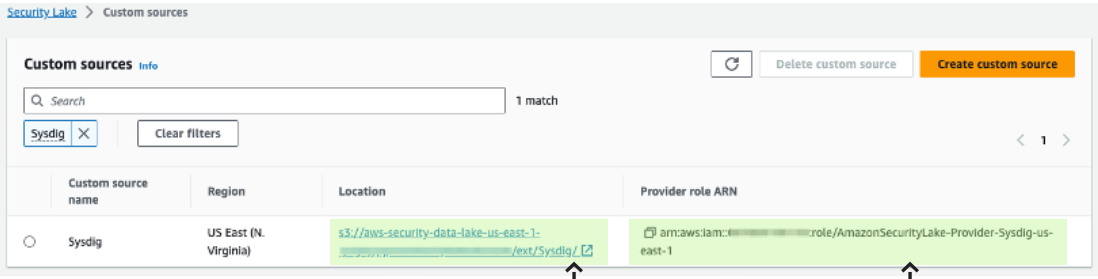
c. Specify message batch size.

d. Specify ExternalID.

e. Specify Amazon Security Lake IAM Role ARN (IAM role that's created as part of custom source creation in Amazon Security Lake).

f. Specify Amazon Security Lake S3 bucket location (S3 bucket that's created as part of the custom source creation in Amazon Security Lake).

Figure 3: Security Custom Source Resources



g. Click Next.

h. Review configurations and click "Create Stack."

02

AWS CloudFormation Outputs Review:

1. If you deployed the Amazon SQS queues as part of this.

   a. Post stack creation, verify the outputs tab for the Amazon SQS arn.

Sysdig Configuration for Event Forwarding

01

IAM User Set Up:

1. Create a dedicated IAM user for Sysdig or identify a pre-existing one.
2. Generate an access key for third-party service use.
3. Adjust the access policy to empower the user to access Amazon SQS.

02

Integrating with Amazon SQS:

1. Use Sysdig Secure with admin privileges.
2. Head to the Settings > Events Forwarding.

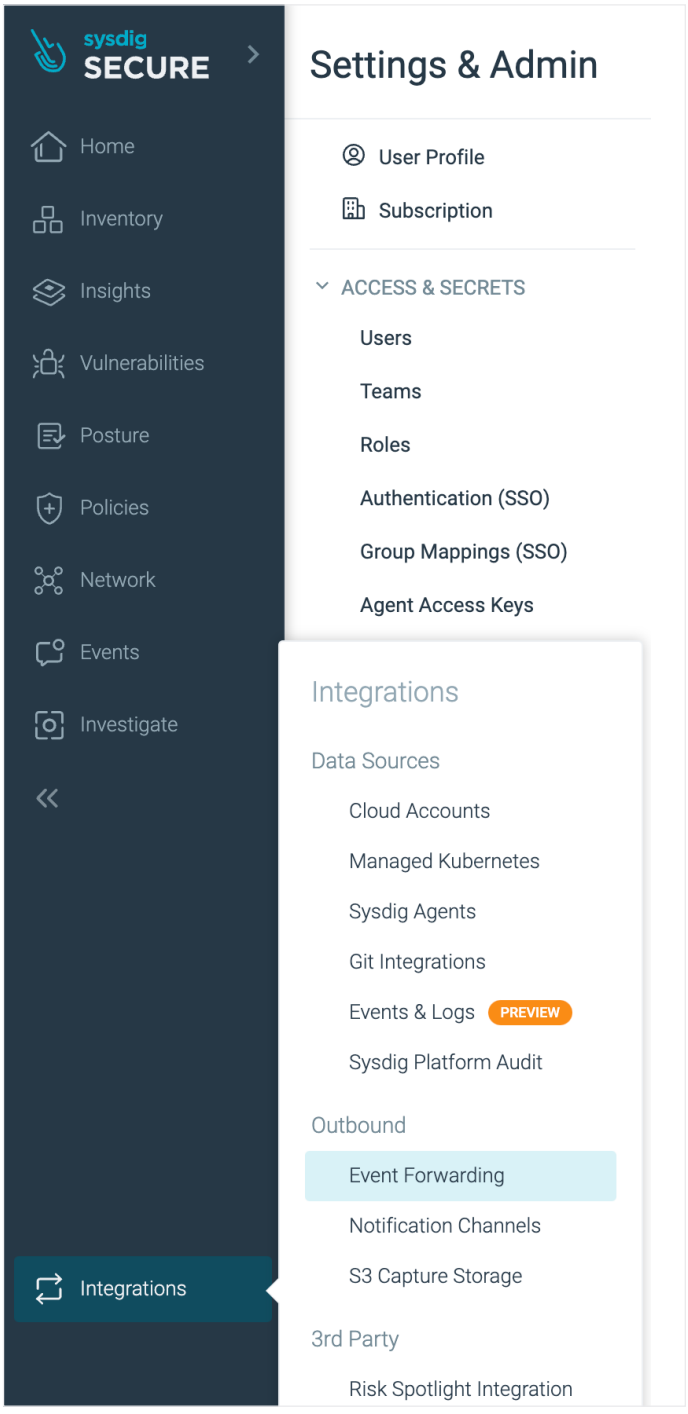
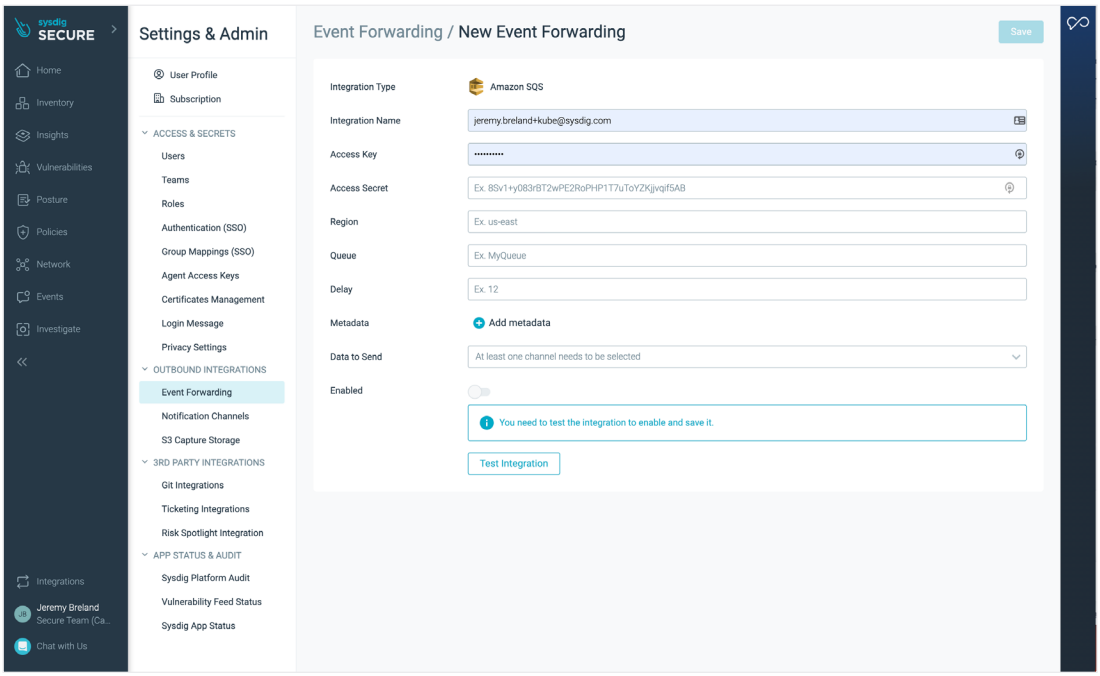


Figure 4:
Accessing Sysdig's event forwarding feature

3. Add new integration and pick Amazon SQS.

Figure 5:

Creating a new event forwarding integration



4. Choose which data you would like to send to Amazon Security Lake.
5. Click on the Test integration button.
6. Set up and save the integration.

AWS Lambda Function Operations

Amazon SQS Event Activation:
AWS Lambda responds automatically to Amazon SQS messages.

Event Transformation:

- AWS Lambda decodes incoming events.
- Adjusts them for the Open Cybersecurity Standards Framework (OCSF).

Parquet Format Conversion
Transforms the OCSF events to Parquet for efficient storage.

Transferring Data to Amazon S3
Parquet files are stored in the specified Amazon Security Lake S3 bucket.

Testing & Validation

Sysdig Event Generation
Simulate an event or await a real-time one.

Event Handling
AWS Lambda should interpret and store the event autonomously.

Verifying Amazon S3
The Amazon S3 bucket should now house a Parquet file with event specifics. The partitioning scheme for the parquet objects should conform to *<custom source S3 location>/region=<region>/accountId=<accountId>/eventDay=<yyyyMMdd>/parquet files.*"

Monitoring & Debugging

Overseeing AWS Lambda
Visit the AWS Lambda section in AWS Console for the "Monitoring" tab.

Integration with Amazon CloudWatch
AWS Lambda logs any errors and they will appear in corresponding AWS Lambda CloudWatch logs for easy troubleshooting.

Conclusion

In the dynamic landscape of the cloud, having a robust solution for security data analytics is key to improving the protection of your workloads, applications, and data. Sysdig and Amazon Security Lake provide a modern foundation for securing your cloud estate. By bringing together Sysdig's powerful runtime security capabilities with a scalable and cost-effective data lake, you gain a more complete view of security data across your entire organization for more effective risk management.

Support

You can find the source code for this integration here:

SOURCE CODE →

If you have additional questions or comments, please reach out to Sysdig support

SYSDIG SUPPORT →

GUIDE-020 REV. B 01/24