
AWS
re:Invent
NOV. 28 – DEC. 2, 2022 | LAS VEGAS, NV

SEC216

Introducing Amazon Security Lake

Rod Wallace

General Manager
AWS

Jonathan Garzon

Product Manager
AWS

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Agenda

Challenges for security teams

The route to modern security analytics

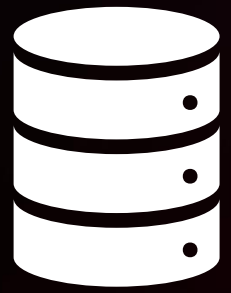
Amazon Security Lake

Conclusion

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

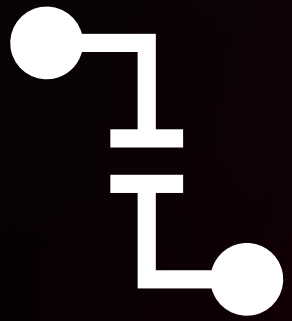
Enterprise-wide security data analysis is challenging

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.



Growing volumes of security data

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.



Inconsistent and incomplete data

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.



Lack of direct ownership of the data

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.



More data wrangling, less analysis

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Imagine if there was a service that . . .



Automatically builds a security lake in your account



Centralizes and normalizes log collection across your entire enterprise



Provides long-term retention and manages storage cost



Gives complete freedom of choice for analytics

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Open Cybersecurity Schema Framework (OCSF)

AN OPEN STANDARD THAT CAN BE ADOPTED BY ANYONE TO SIMPLIFY SECURITY DATA NORMALIZATION



- Open-source project to deliver a simplified and vendor-agnostic taxonomy for security data
- Speed data ingestion and analysis without the time-consuming, up-front normalization tasks
- Combine data from OCSF compliant sources to break down data silos that slow security teams
- Open standard that can be adopted in any environment, application, or solution provider

Over 60 participating organizations across security ISVs, government, education, and enterprise, with many more using OCSF

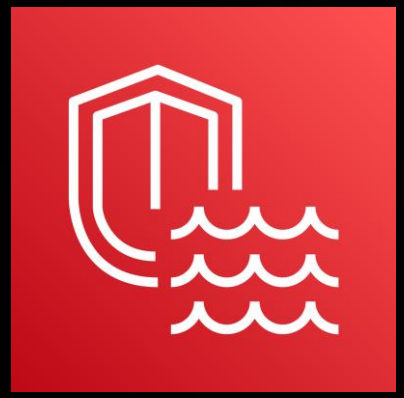
aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Preview

Amazon Security Lake

AUTOMATICALLY CENTRALIZE SECURITY DATA INTO A PURPOSE-BUILT DATA LAKE IN A FEW CLICKS



Centralize data automatically from cloud, on premises, and custom security sources across regions

Optimize and manage security data for more efficient storage and query performance

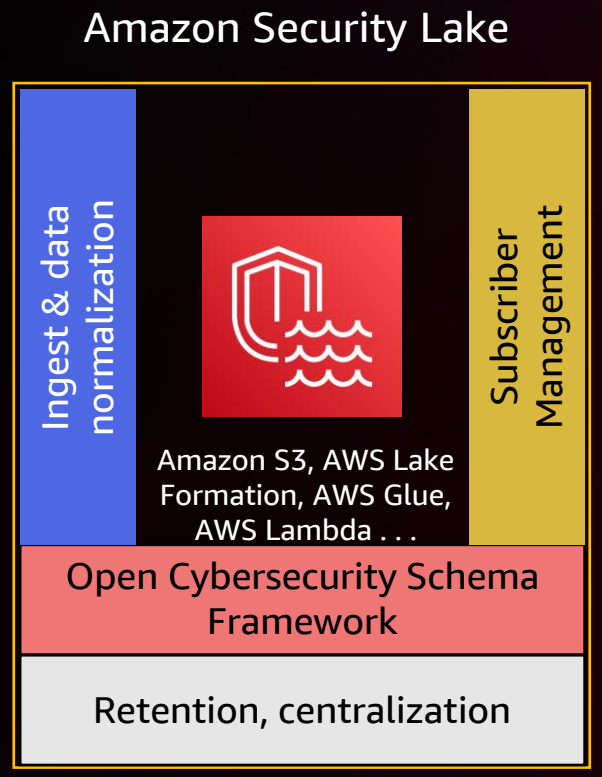
Normalize data to an industry standard to easily share and use with multiple analytics tools

Analyze using your preferred analytics tools while retaining control and ownership of your security data

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

How it works

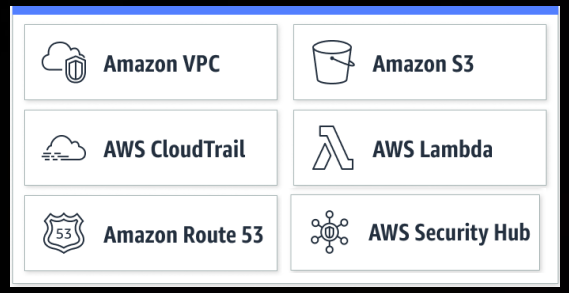


Customer-owned,
managed data lake

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

How it works

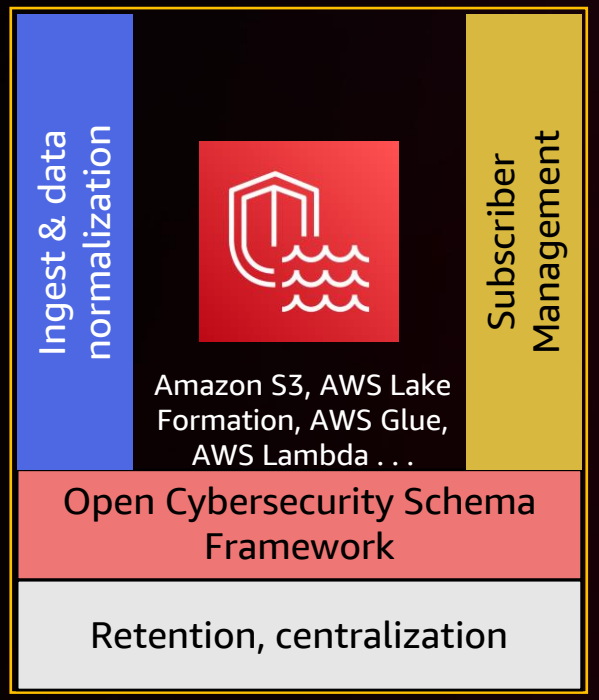
AWS logs sources + findings from over 50 security solutions



AWS Partner enterprise security solutions

Your own data

Amazon Security Lake

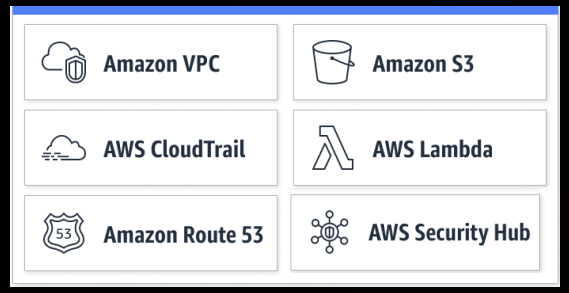


Customer-owned, managed data lake

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

How it works

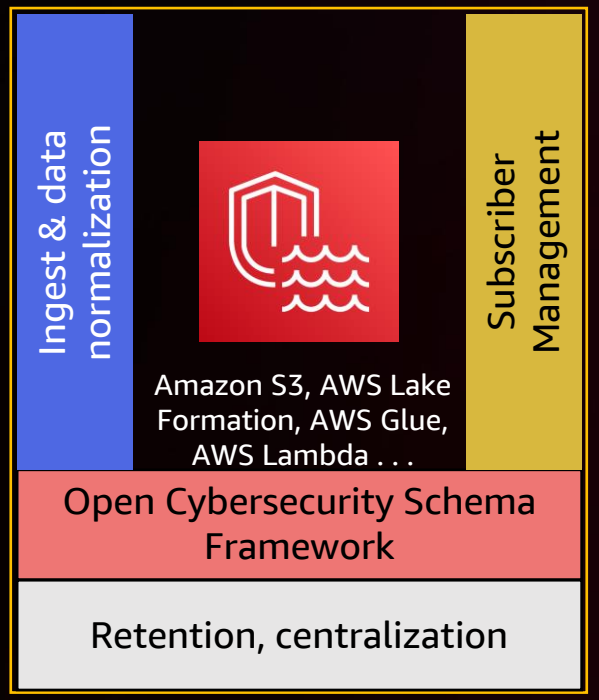
AWS logs sources + findings from over 50 security solutions



AWS Partner enterprise security solutions

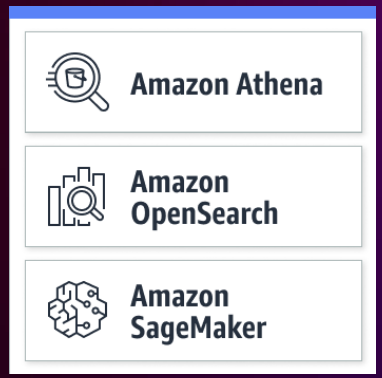
Your own data

Amazon Security Lake



Customer-owned, managed data lake

AWS analytics



AWS Partner analytics & XDR platforms

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Amazon Security Lake Partners

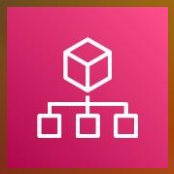


aws

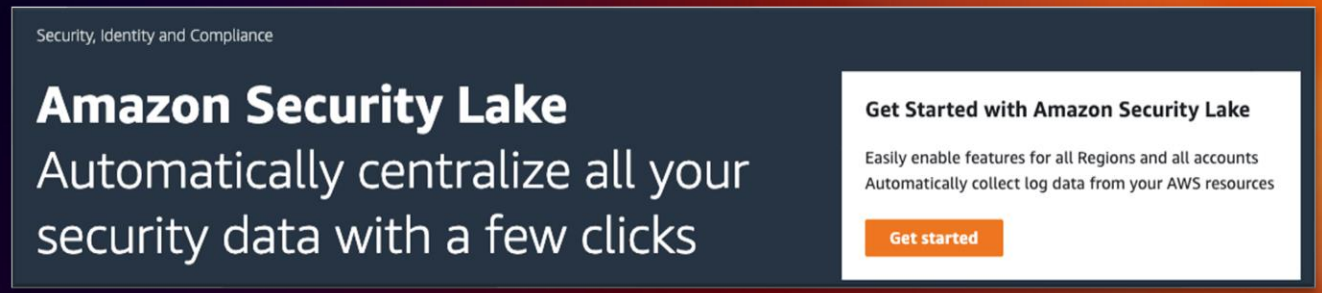
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Getting started – Enterprise-wide enablement

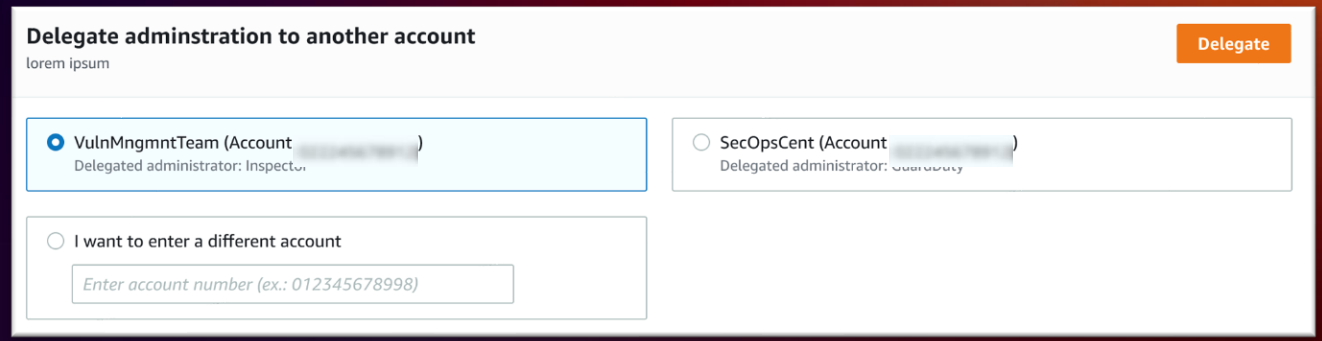
Security Lake works with AWS Organizations



Start from your organization management account



Elected a delegated admin account to manage your security data



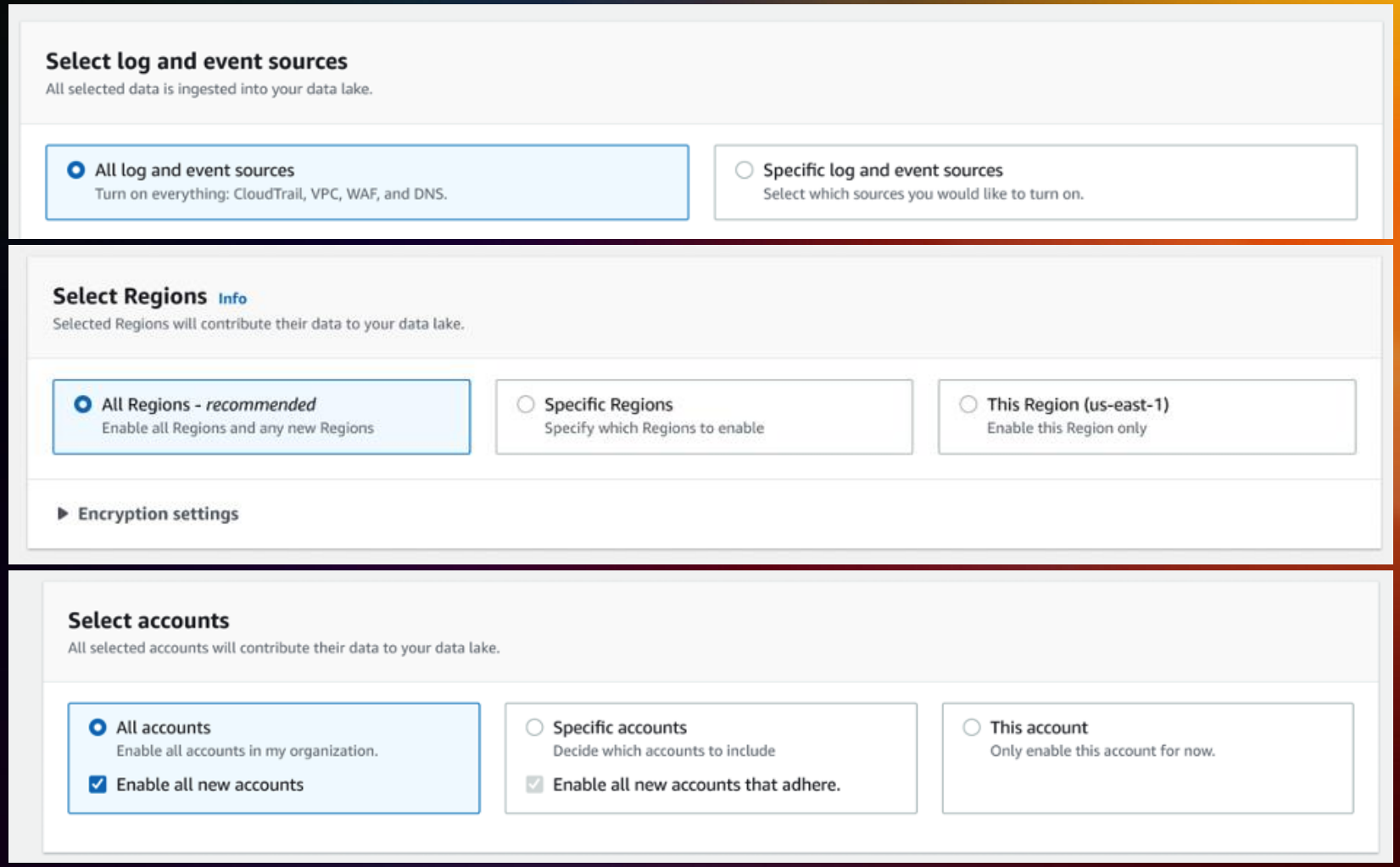
aws
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Getting started – Collect everything

Everything on by default

Multi-Region enablement

All accounts in your organization

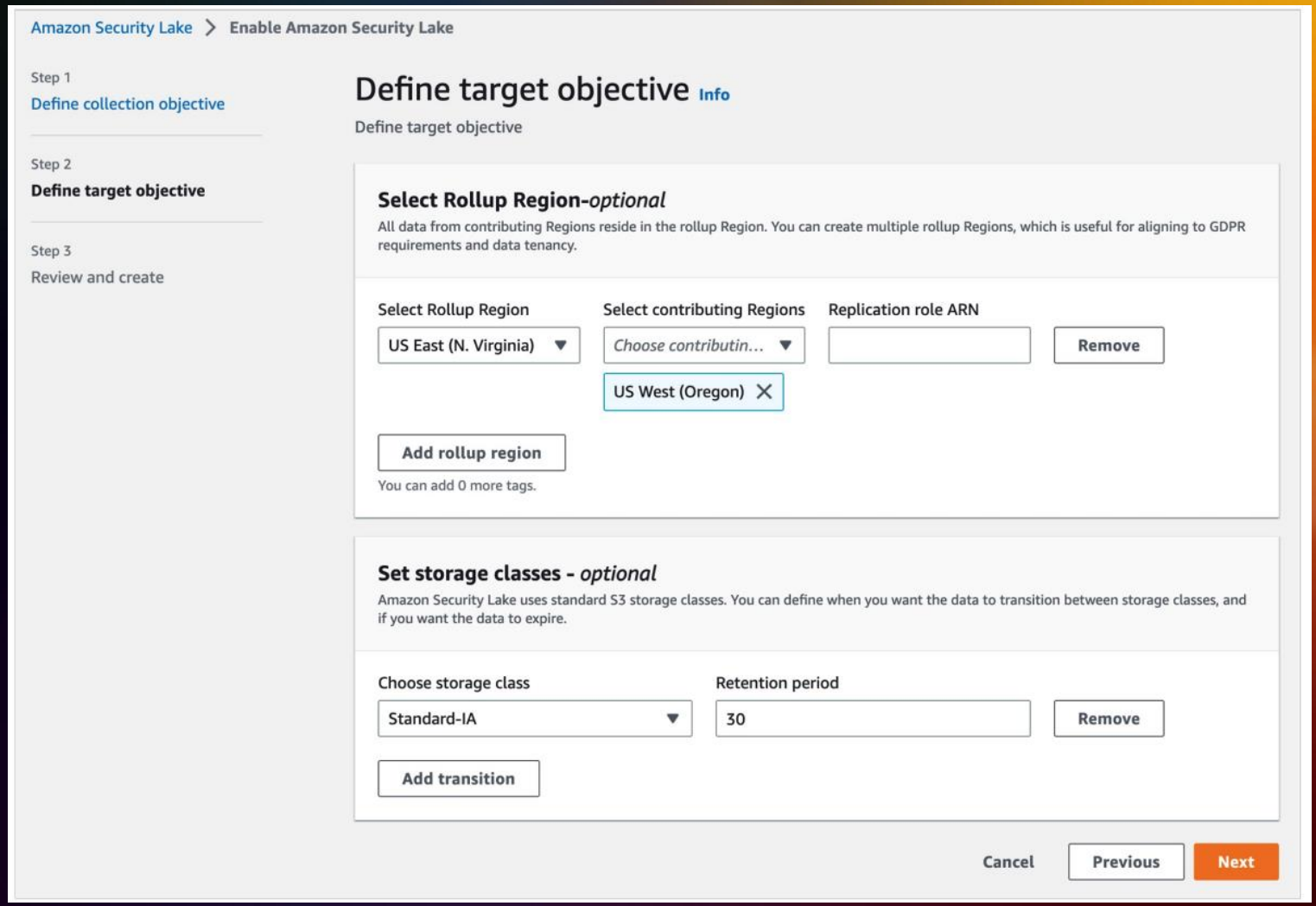


© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Getting started – Centralization and retention

One or multiple central Regions

Define storage class transitions



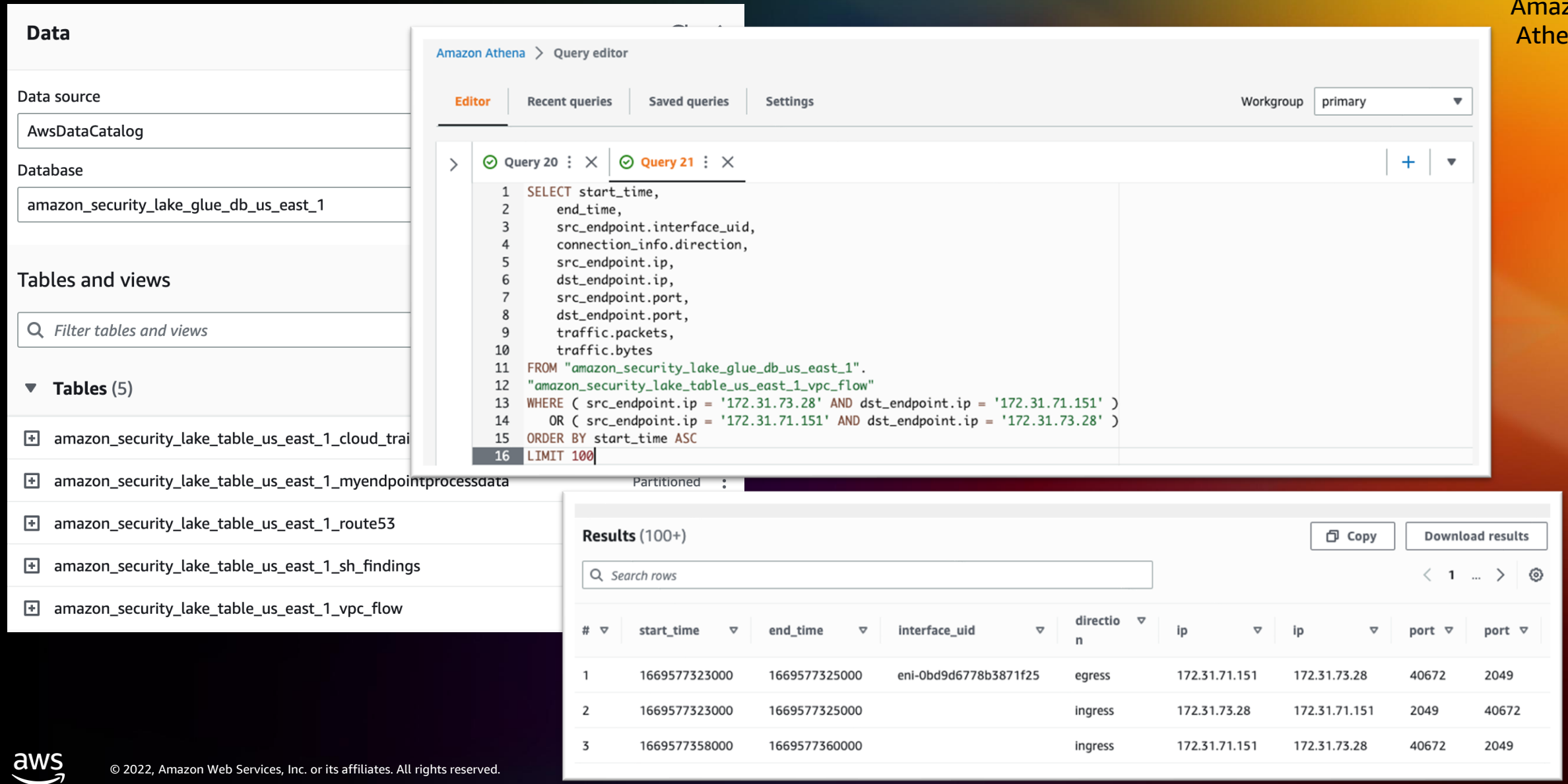
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Done!

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

You can immediately query your data

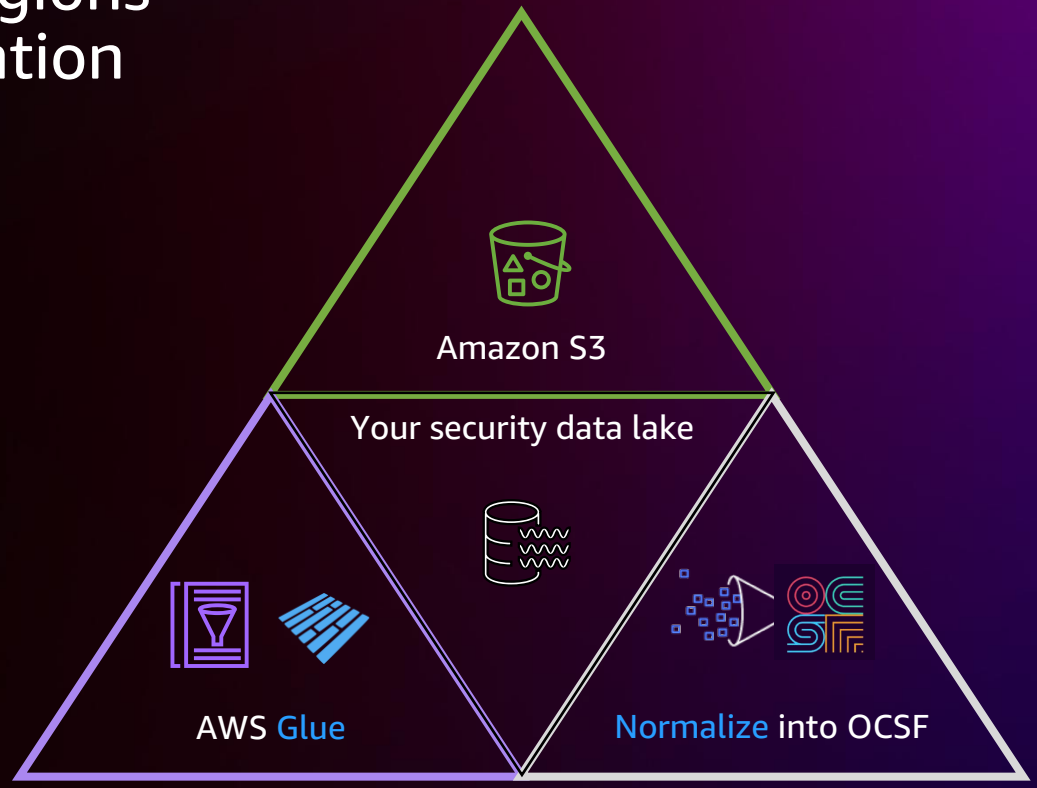
Amazon Athena



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

What's happening under the hood?

- Create encrypted Amazon S3 buckets across regions and configure Amazon S3 retention and replication settings
- Enable logging across all Regions, accounts, and resources
- Transform and partition all incoming data to OCSF and Apache Parquet
- Create and update AWS Glue Tables and partitions



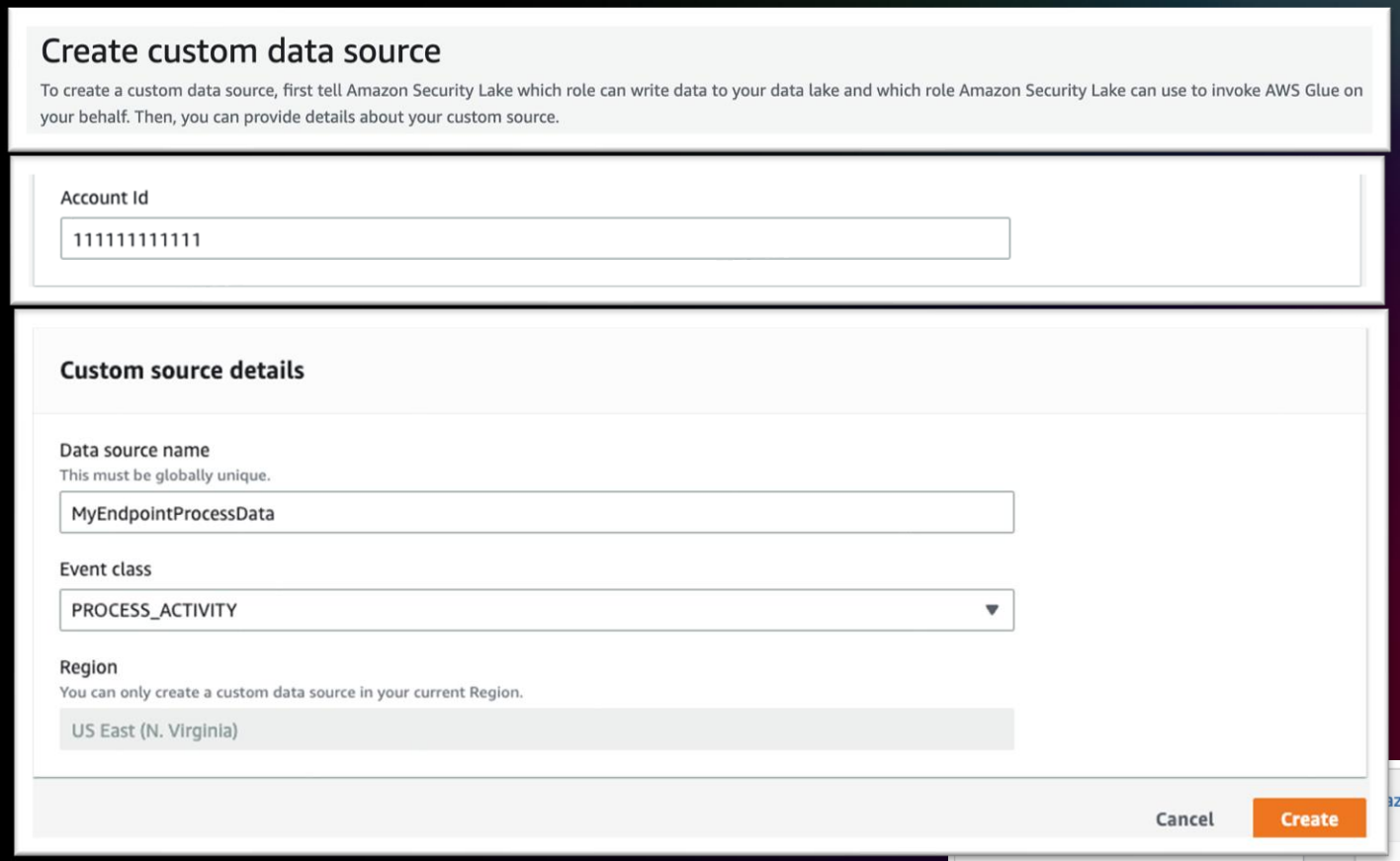
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Bring all your security data

- You can augment your data lake with external OCSF data from partner solutions or your own
- Use the same data lifecycle and access control features as native data
- 20+ partners already provide their data in this format directly to Amazon S3
- Security Lake manages the infrastructure and permissions for you

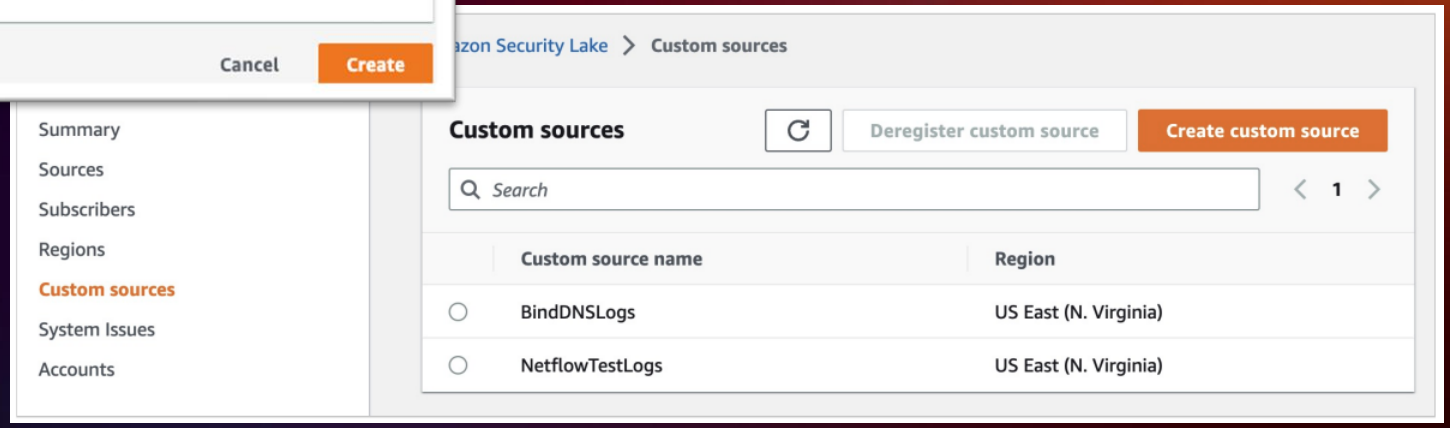
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Bring all your security data



Provide AWS account ID of the source provider

Define name and OCSF event class



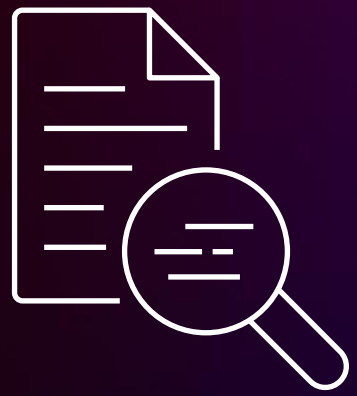
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Share your data with analytics solutions

- Data access
  - Receive a stream of new object notification
  - Direct access to Amazon S3 objects
  - Security Lake manages the infrastructure and permissions



- Query access
  - Query data in place via Athena
  - Cross-account support via Lake Formation
  - No need to move data around



aws

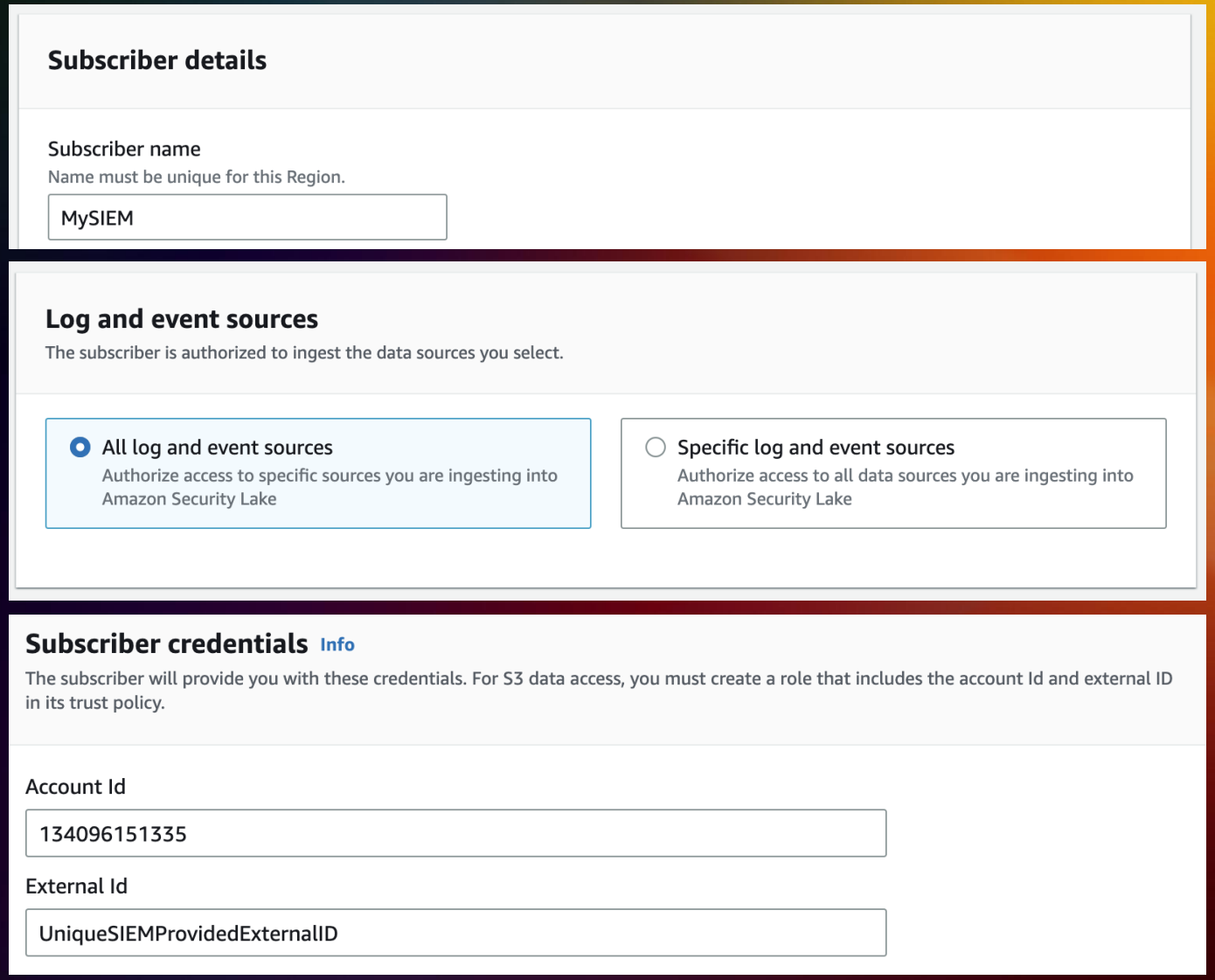
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Configure subscribers

Define name

Select the data sources you want to share

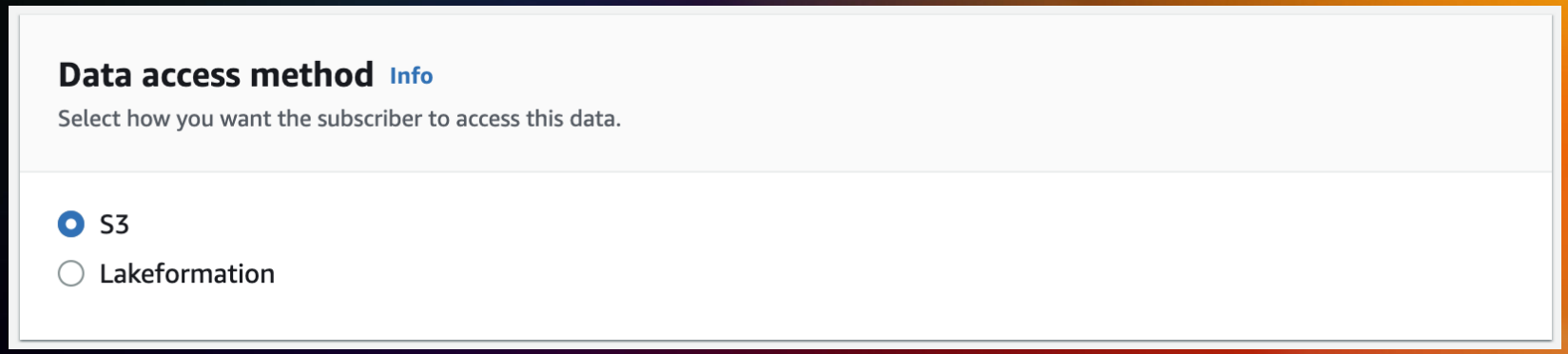
Provide AWS account ID and unique external ID



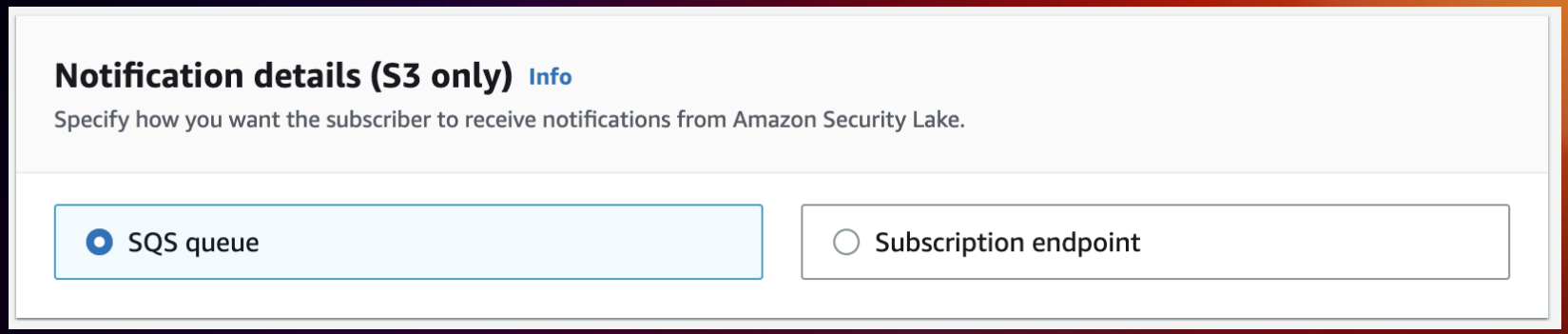
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Configure subscribers

Select a data access method

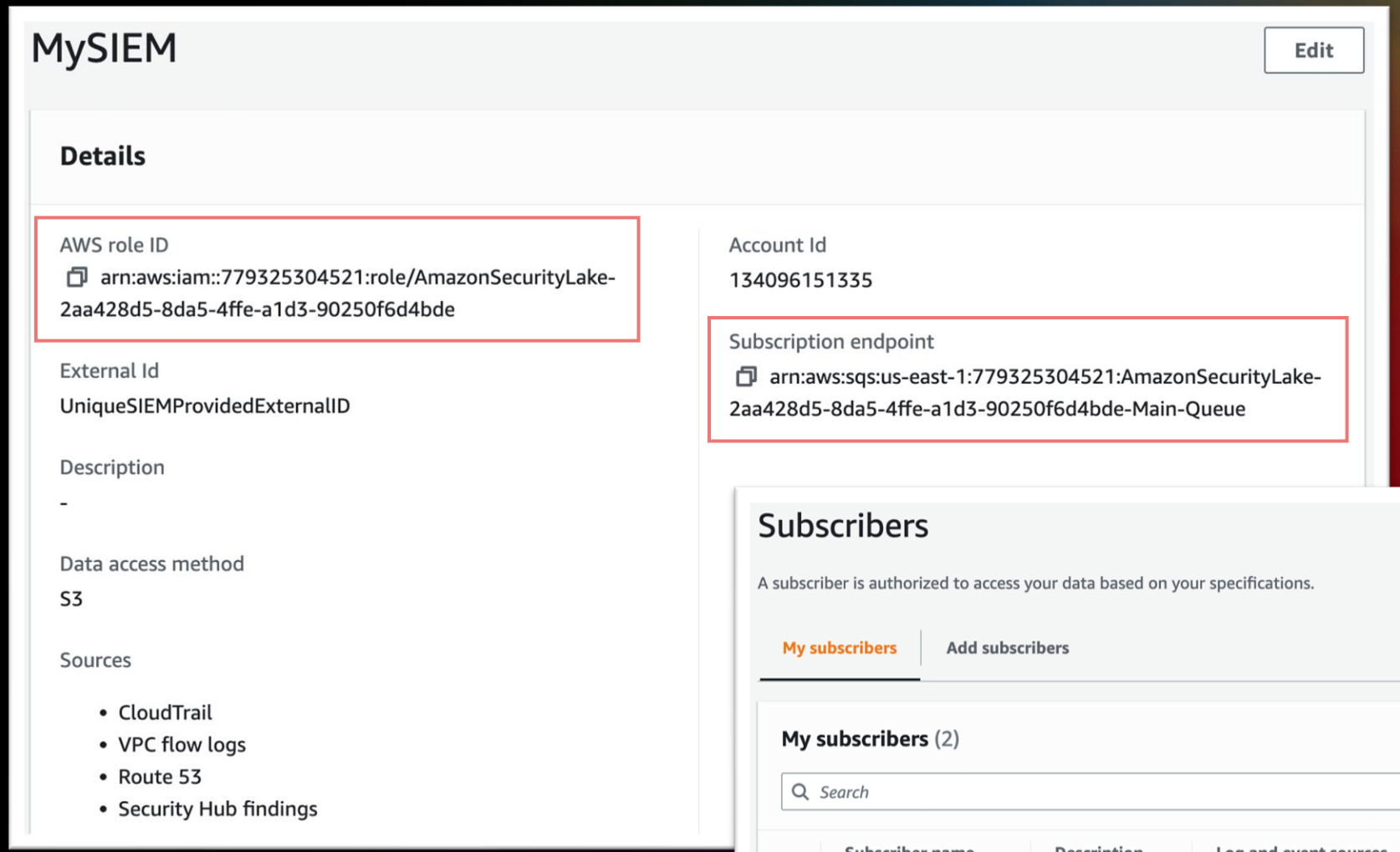


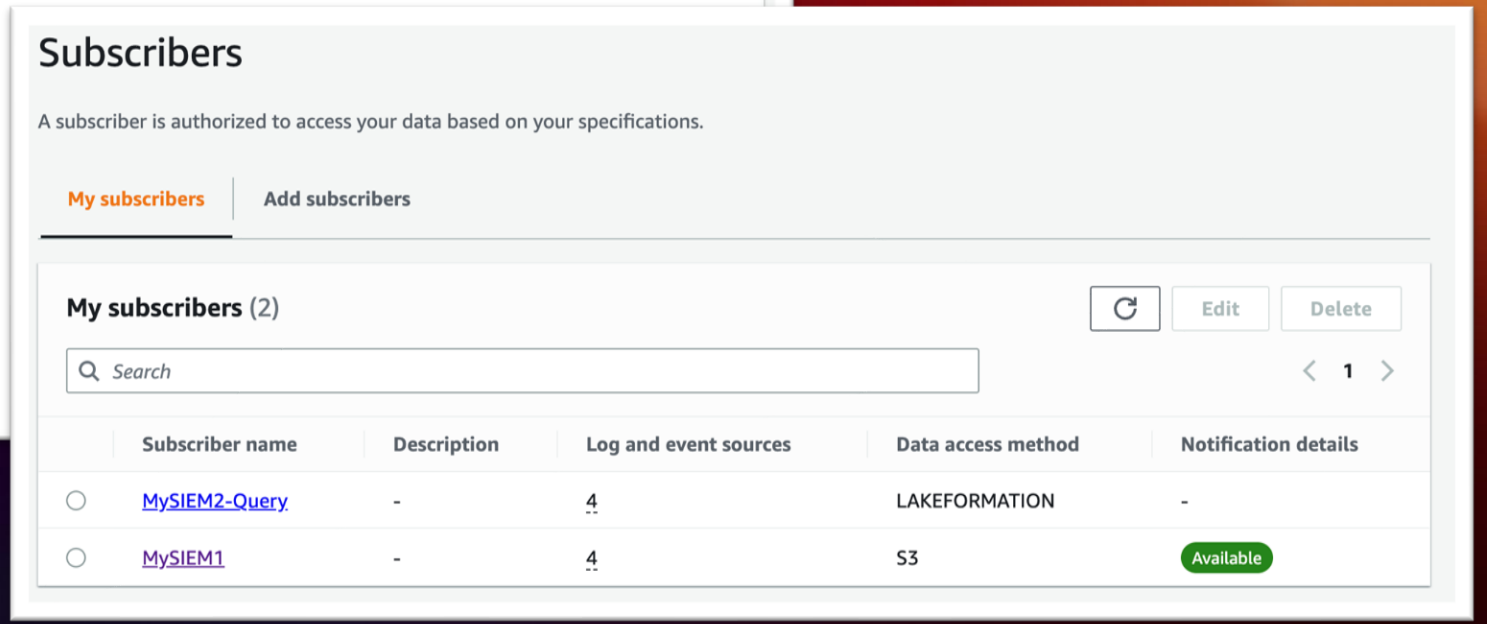
Select the preferred object notification mechanism



aws
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Configure subscribers

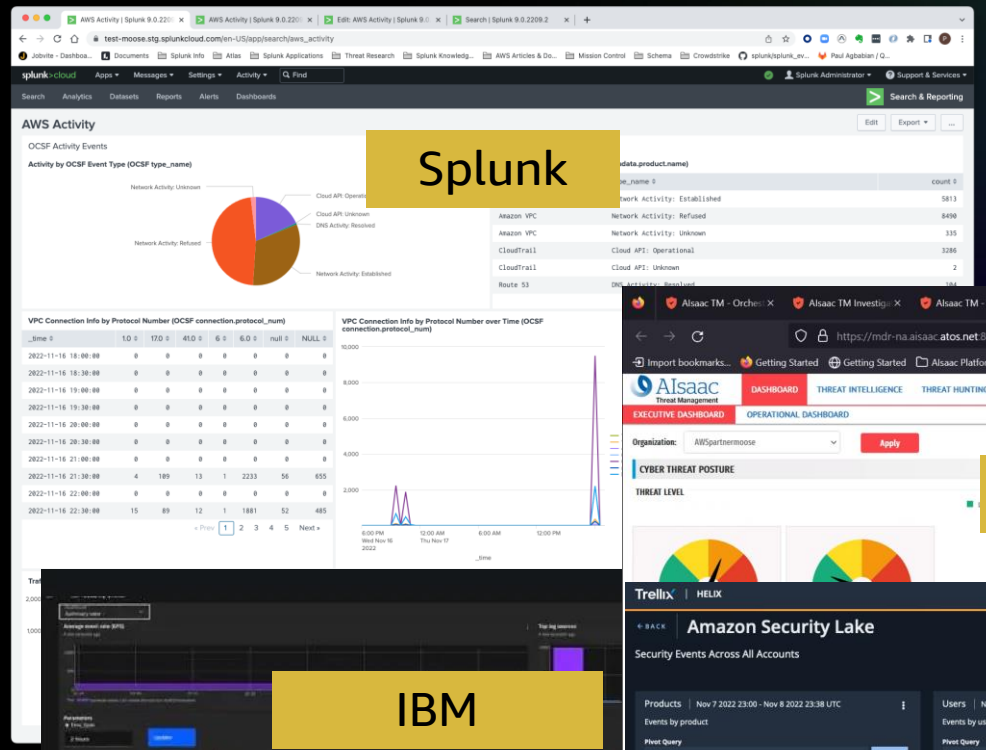


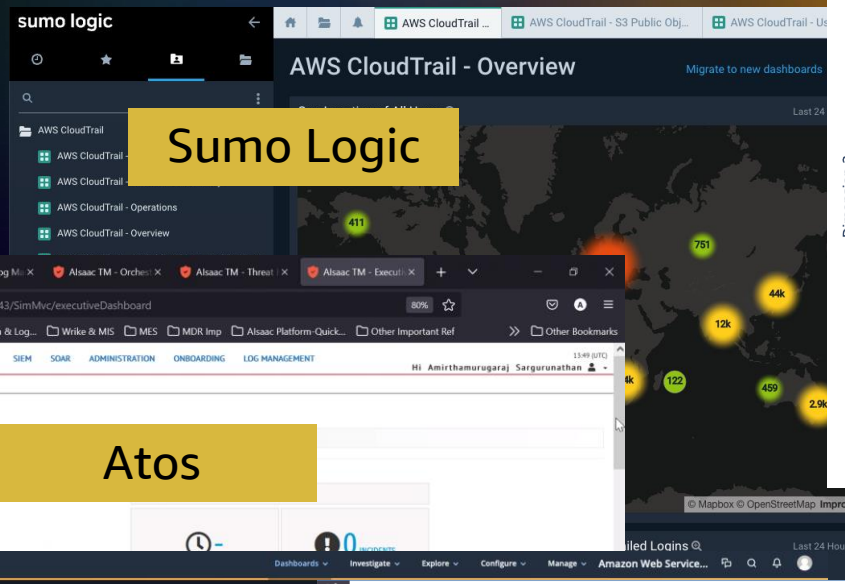


Use Security Lake created resources to configure data access on the subscriber

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

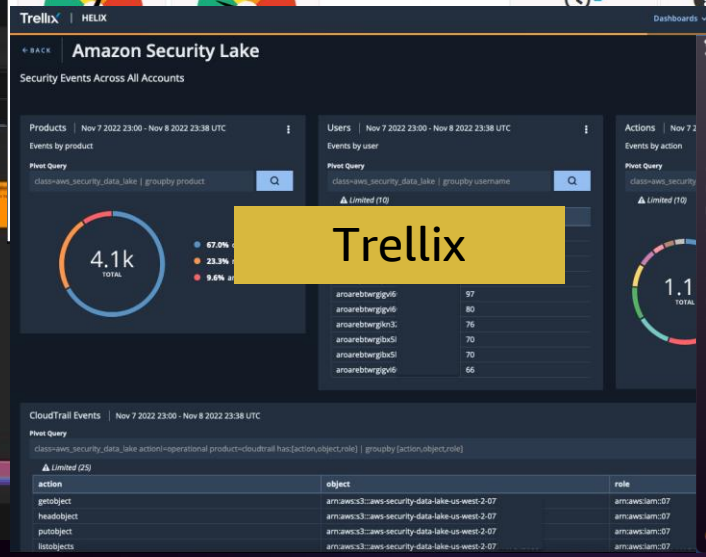
Choose your analytics

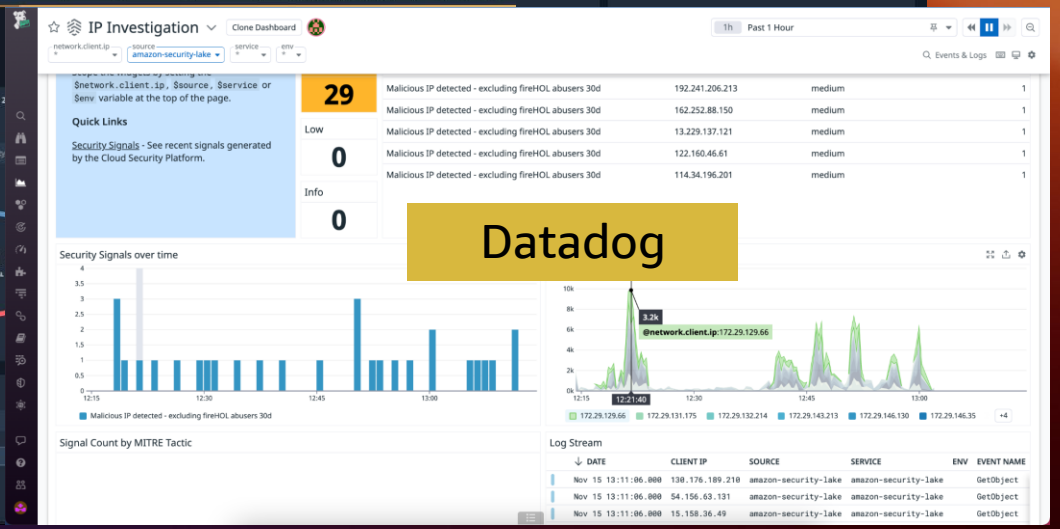












© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Pricing

Priced to allow you to collect and retain everything

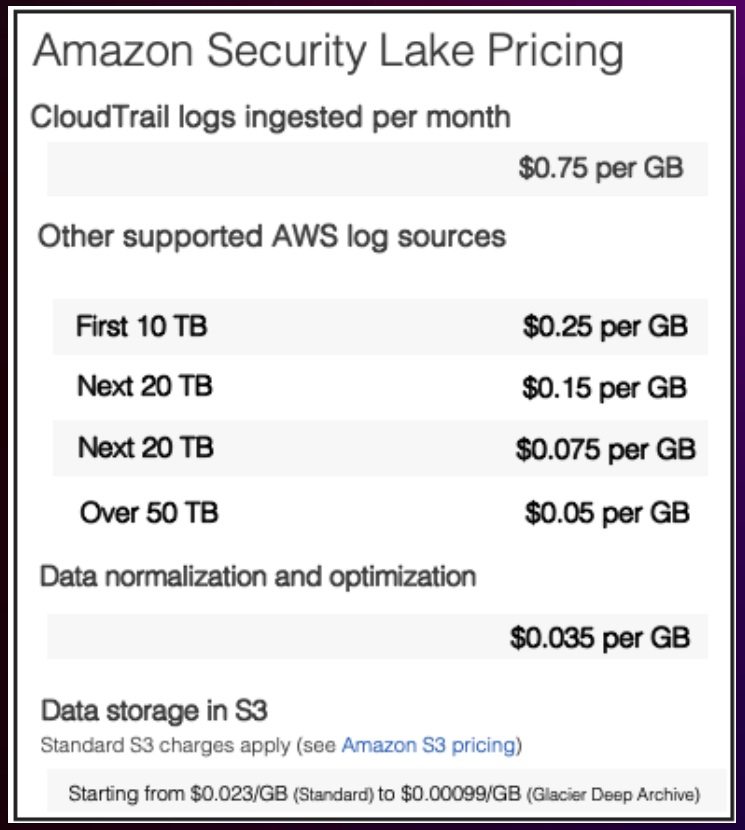
No charge for using your data

No charge for bringing third party or your own data

You only pay per gigabyte of AWS logs ingested and normalized

Standard charges apply for AWS services that Security Lake orchestrates in your account

No cost during preview; 15-day free trial



Amazon Security Lake Pricing

CloudTrail logs ingested per month

	$0.75 per GB

Other supported AWS log sources

First 10 TB	$0.25 per GB
Next 20 TB	$0.15 per GB
Next 20 TB	$0.075 per GB
Over 50 TB	$0.05 per GB

Data normalization and optimization

	$0.035 per GB

Data storage in S3

Standard S3 charges apply (see Amazon S3 pricing)

Starting from $0.023/GB (Standard) to $0.00099/GB (Glacier Deep Archive)

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Conclusion

- AWS is committed to provide security teams with freedom of choice of analytics
- We are working with the community to make it easier than ever
- Security Lake is available in preview today in 7 Regions . . . try it!



Go to Amazon Security Lake product page

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Thank you!

Rod Wallace
rodwall@amazon.com

Jonathan Garzon
jongarzo@amazon.com



Please complete the session survey in the **mobile app**

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.