Centralize Your Security Data with Amazon Security Lake

Harrison Holstein – Partner Solutions Architect (AWS)

Trellix & aws

Trellix and AWS

Trellix and Amazon Web Services (AWS) have come together to expand security capabilities on the cloud and uncover cloud-specific threats.

AWS Network Firewall

Amazon Route 53 Resolver DNS Firewall

Amazon Virtual Private Cloud (Amazon VPC) Flow Logs

AWS Verified Access

Amazon Simple Storage Service (Amazon S3)

Amazon CloudWatch

AWS CloudTrail

Amazon Inspector

Amazon Guard Duty

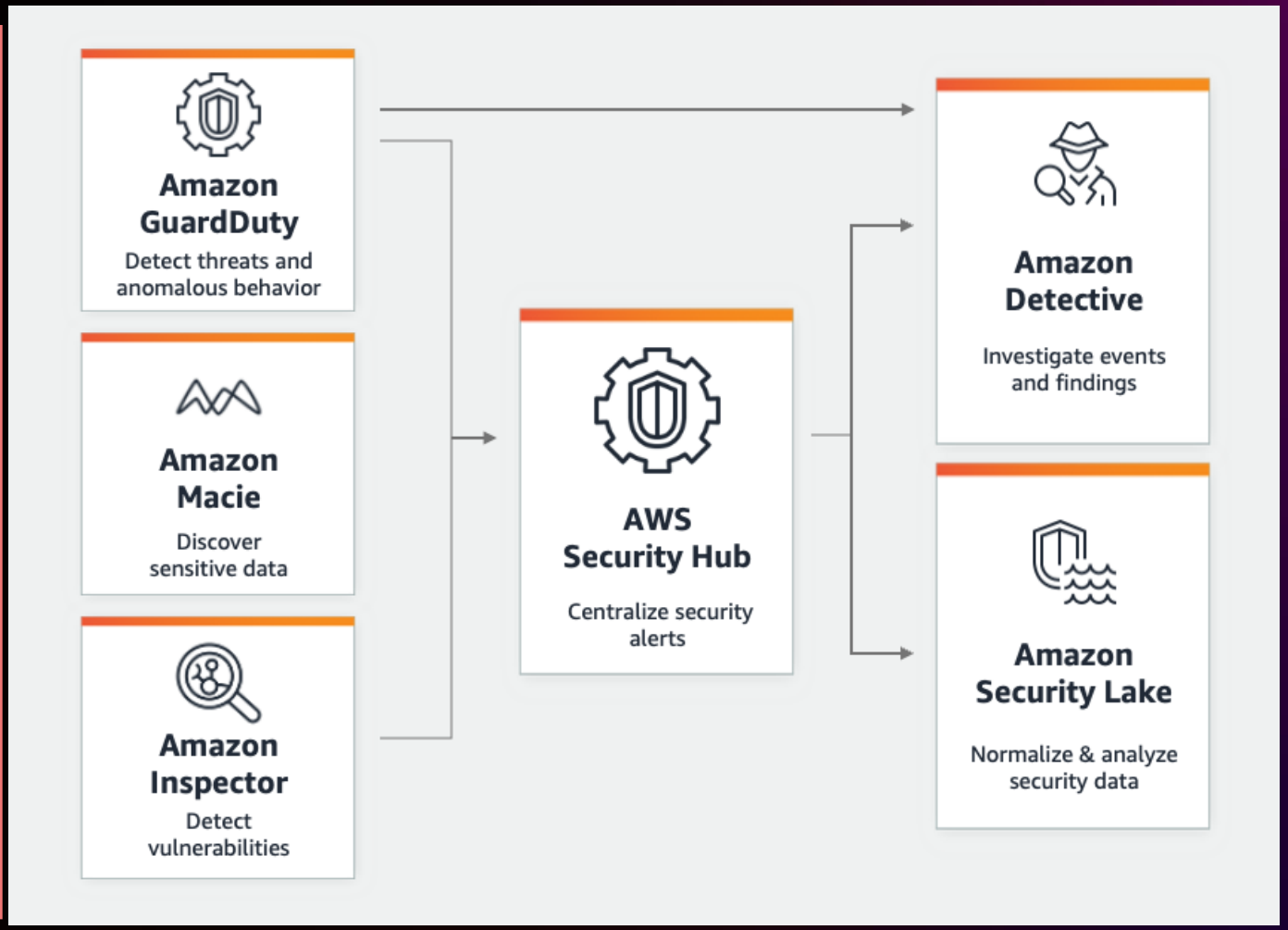
AWS Security Hub

Amazon Security Lake

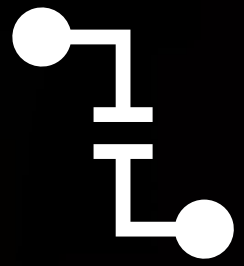
Cloud Native Detection & Response with AWS

Security Monitoring and Threat Detection

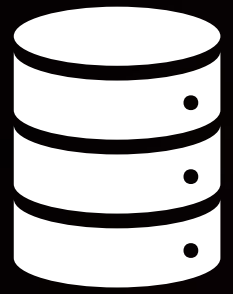
Integrated with AWS Workloads in an AWS Account, along with identities and network activity



Data Wrangling Challenges



Inconsistent and incomplete data



Growing volumes of security data

Inefficient use of data across use cases

Lack of direct control over processed data

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

What is Security Lake?

AUTOMATICALLY CENTRALIZE SECURITY DATA INTO A PURPOSE-BUILT DATA LAKE

Automatically centralize data from AWS environments, SaaS providers, on premises, and cloud sources across AWS Regions

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

Normalize data to an open standard to streamline security data management across multicloud and hybrid environments

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

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 500+ participating organizations across security ISVs, government, education, and enterprise,

with many more using OCSF

Security Lake Partners: Data Sources

OVER 100 SOURCES PROVIDING DATA TO SECURITY LAKE

aws

Amazon S3 | Amazon VPC | AWS CloudTrail | Amazon Route 53 | AWS Security Hub | AWS Lambda

Partner Sources

aqua | Barracuda | cisco SECURE | CLAROTY | CONFLUENT | Cribl

CROWDSTRIKE | CYBERARK | DARKTRACE | ExtraHop | Falco | Gigamon

LACEWORK | Laminar | monad | NETSCOUT | netskope | okta | orca security

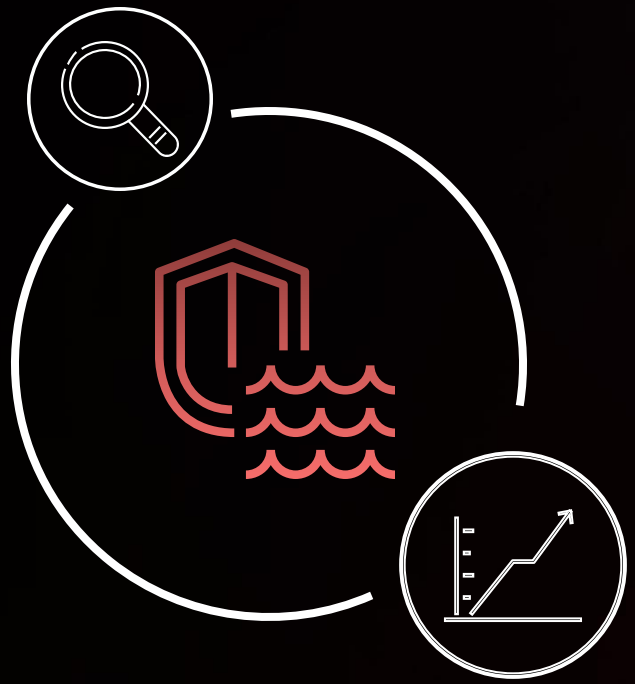
paloalto NETWORKS | PingIdentity | sentra | TANIUM | torq | TALON

Trellix | TREND MICRO | uptycs | VECTRA | vmware | WIZ | zscaler

This list of partners is current as of August 2023.

Security Lake Partners: Analytics Tools & Service Partners

OVER 30 ANALYTICS AND SERVICES PARTNERS



aws

Amazon Athena

Amazon OpenSearch

Amazon SageMaker

Partner Analytics

CHAOSSEARCH, DATADOG, DEVO, IBM, new relic., RAPID7, RIPJAR, securonix, SentinelOne, SOC PRIME, splunk>, STELLAR CYBER, sumo logic, SWIMLANE, tines, torq, Trellix, wazuh.

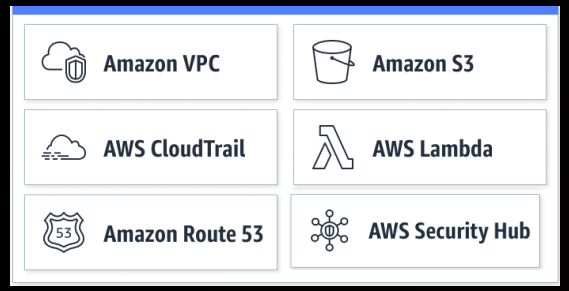
Service Partners

accenture, Booz Allen, CMD, Deloitte., DXC TECHNOLOGY, insbuild., kyndryl, EVIDEN, HCOOP, IBM, Infosys, leidos, MEGAZONE CLOUD, pwc, SOC PRIME, tcs TATA CONSULTANCY SERVICES, wipro

This list of partners is current as of August 2023.

Sources & Subscribers

Source → Amazon Security Lake → Subscribe



Trellix

Other Partners/Custom Sources

Amazon Security Lake

Ingest & Normalization

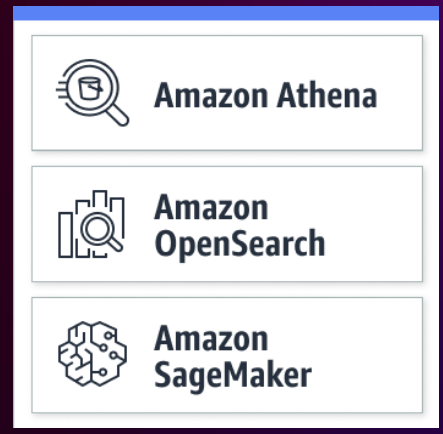
Manage Lifecycle

Manage Subscribers

Orchestration

S3 SQS Lambda EventBridge

Glue Athena Lake Formation



Trellix

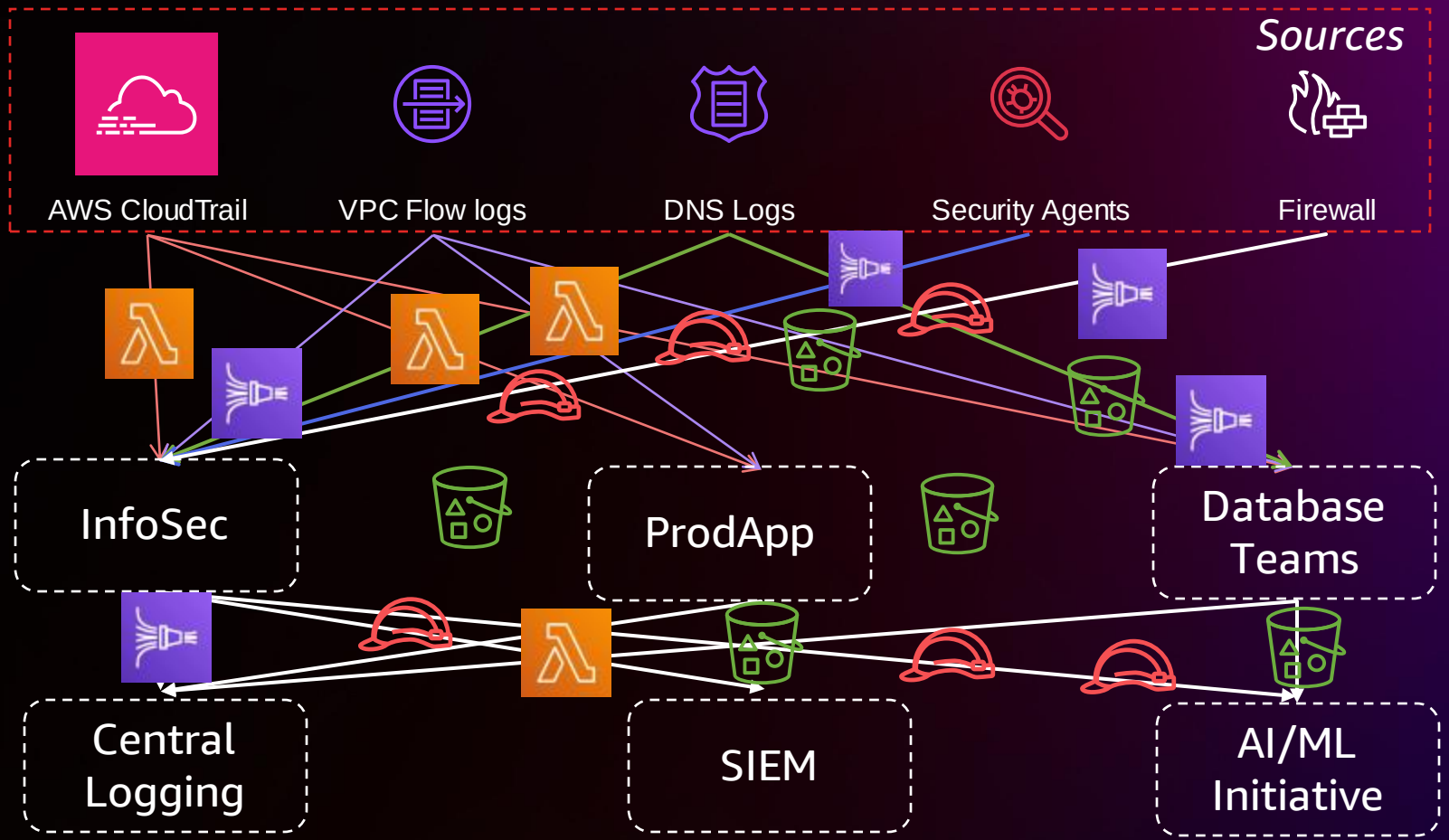
Before Security Lake – Resource based logging

Duplication of data

Multiple integrations

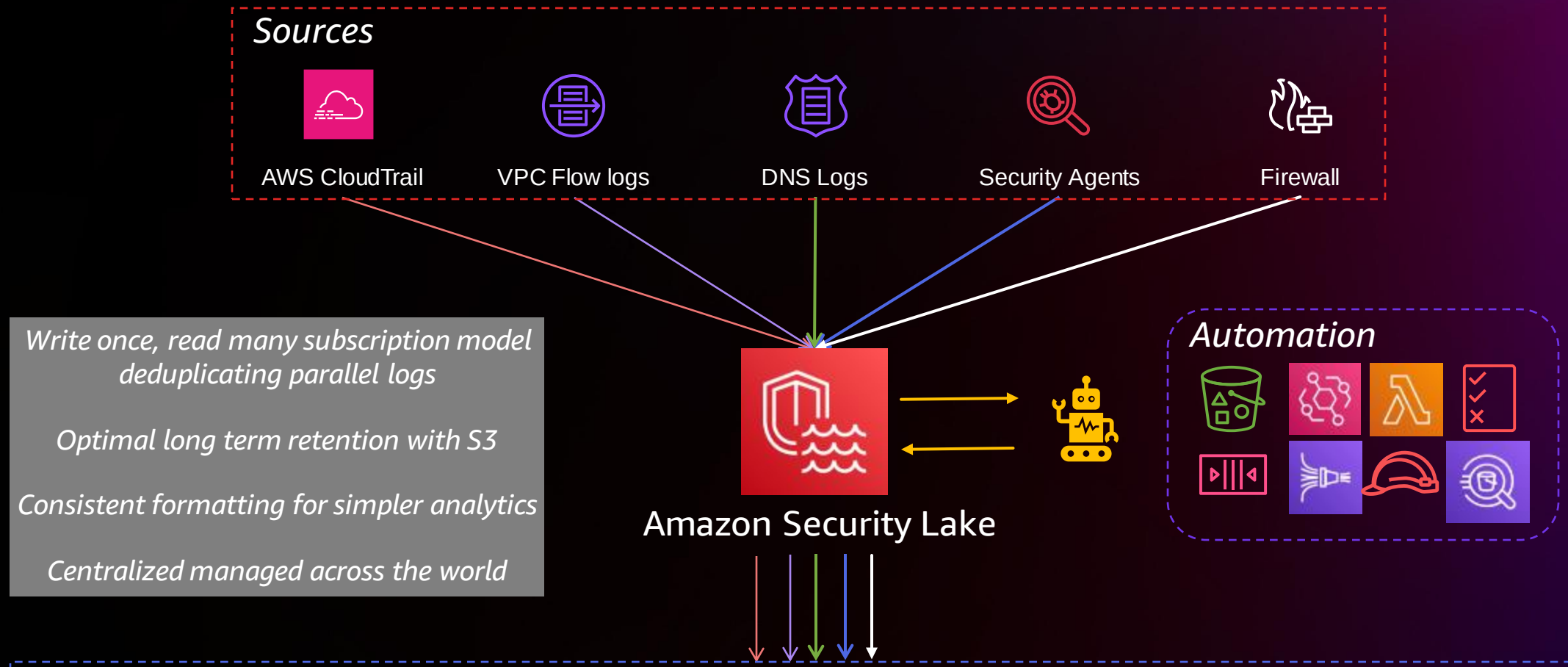
Data in different formats

Multiple long term storage options

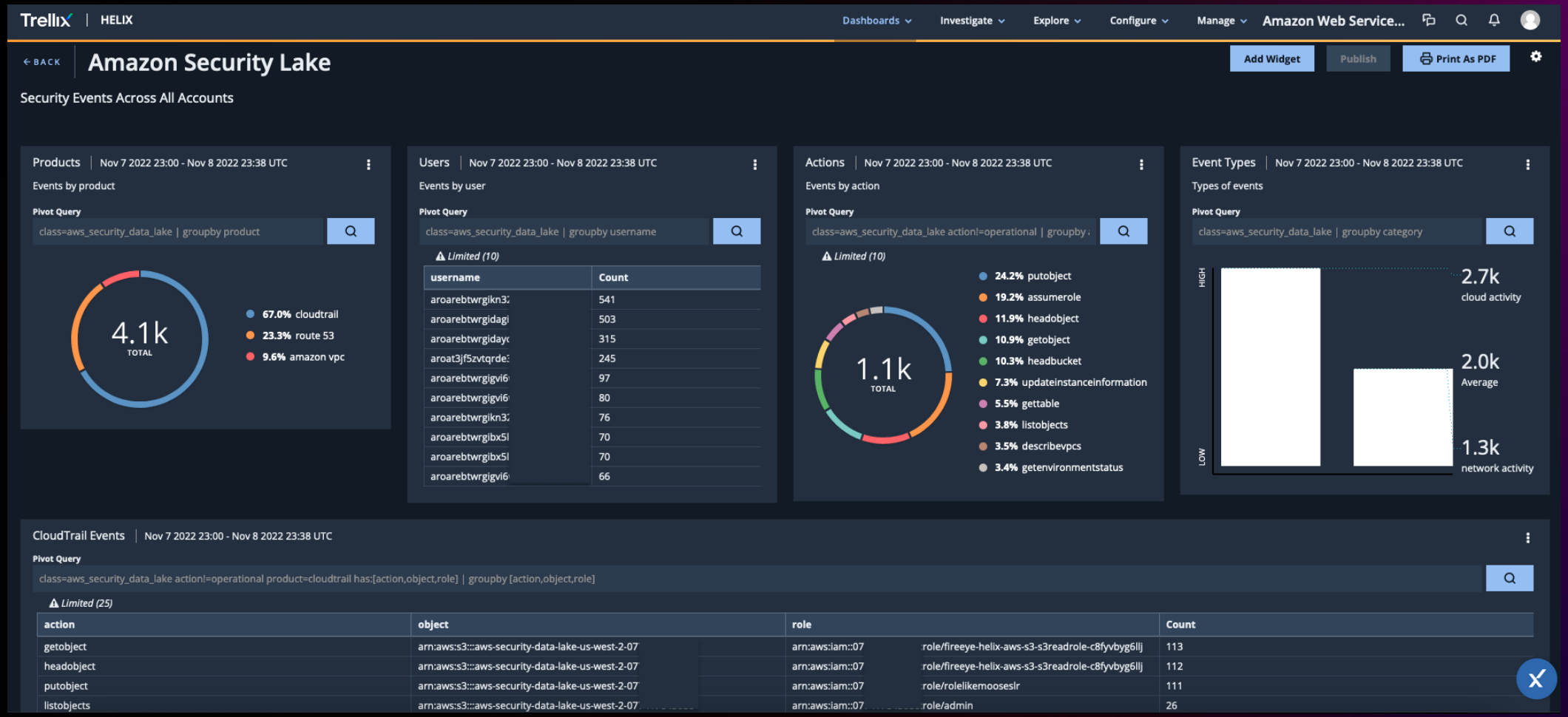


Plus many more..

After Security Lake – the data lake model

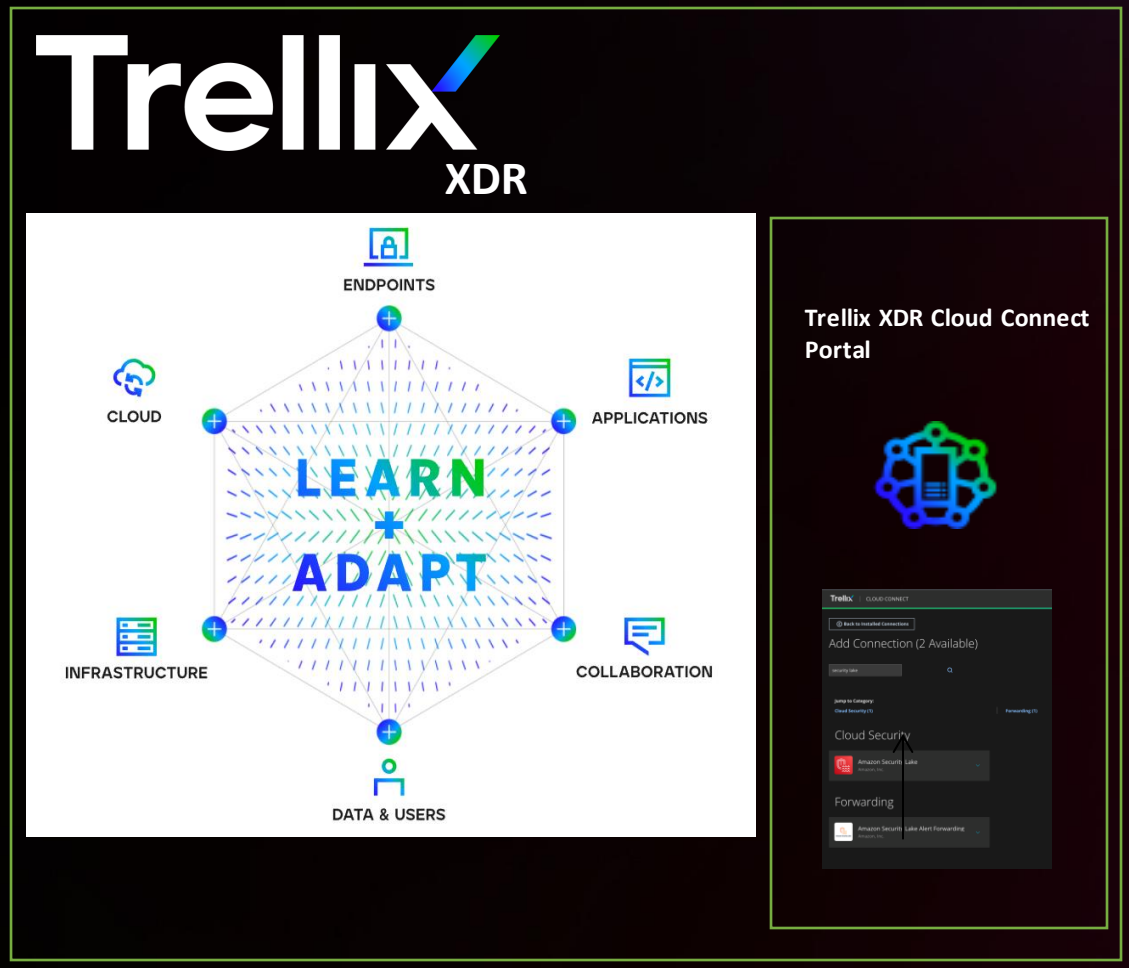


Analyze with Trellix



Trellix + Security Lake

1000+ third-party connectors and data sources



Security Events (in OCSF)

Figure 1: Joint customers can share security events across Trellix XDR and with Amazon Security Lake, getting complete detection and response capabilities for their AWS environments.

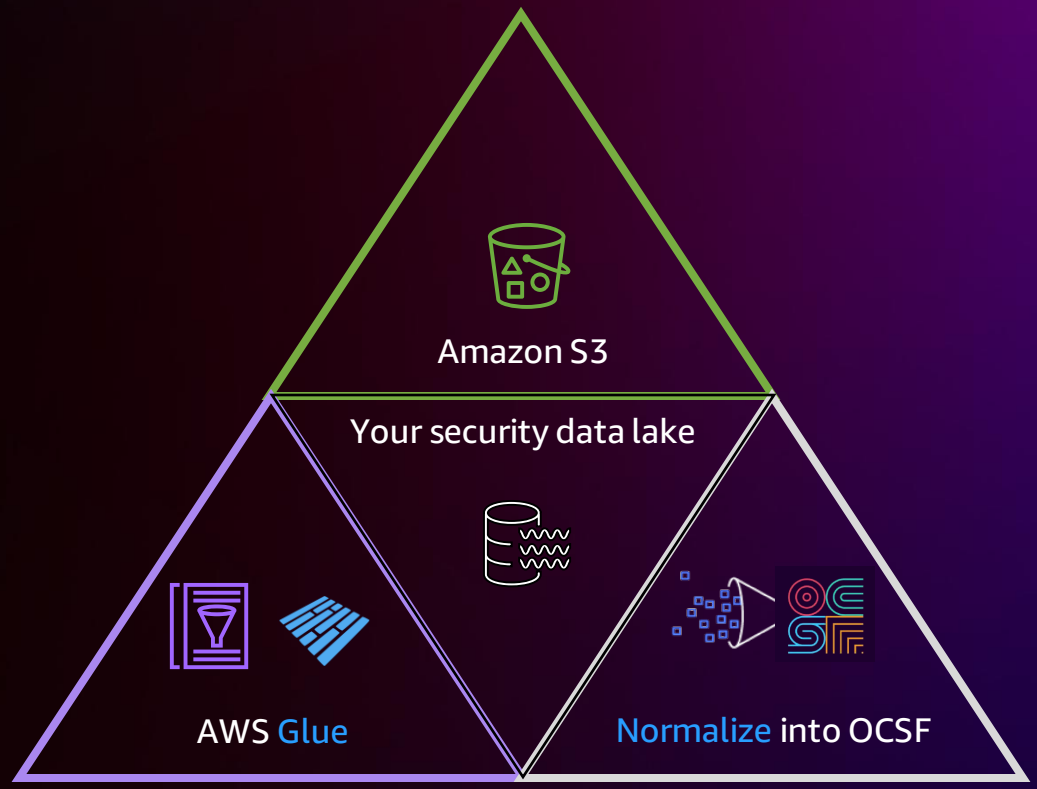
What's happening under the hood?

Create encrypted Amazon S3 buckets across regions and configure Amazon S3 retention and replication settings

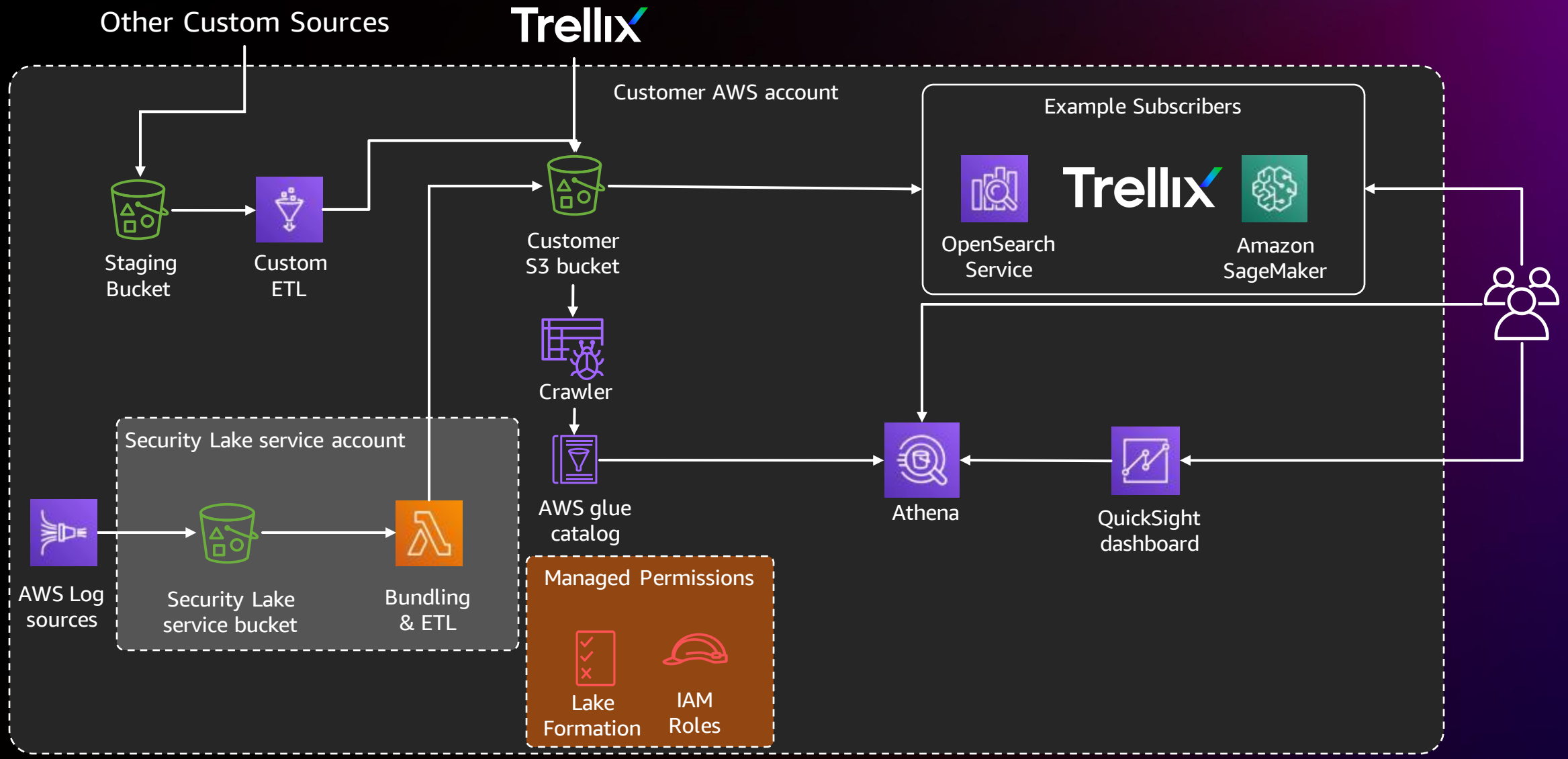
Enable logging across all Regions, accounts, and resources

Transform and partition all incoming data to OCSF and Apache Parquet

Create and update AWS Glue Tables and partitions



Amazon Security Lake Architecture



Share your data with analytics solutions

Data access

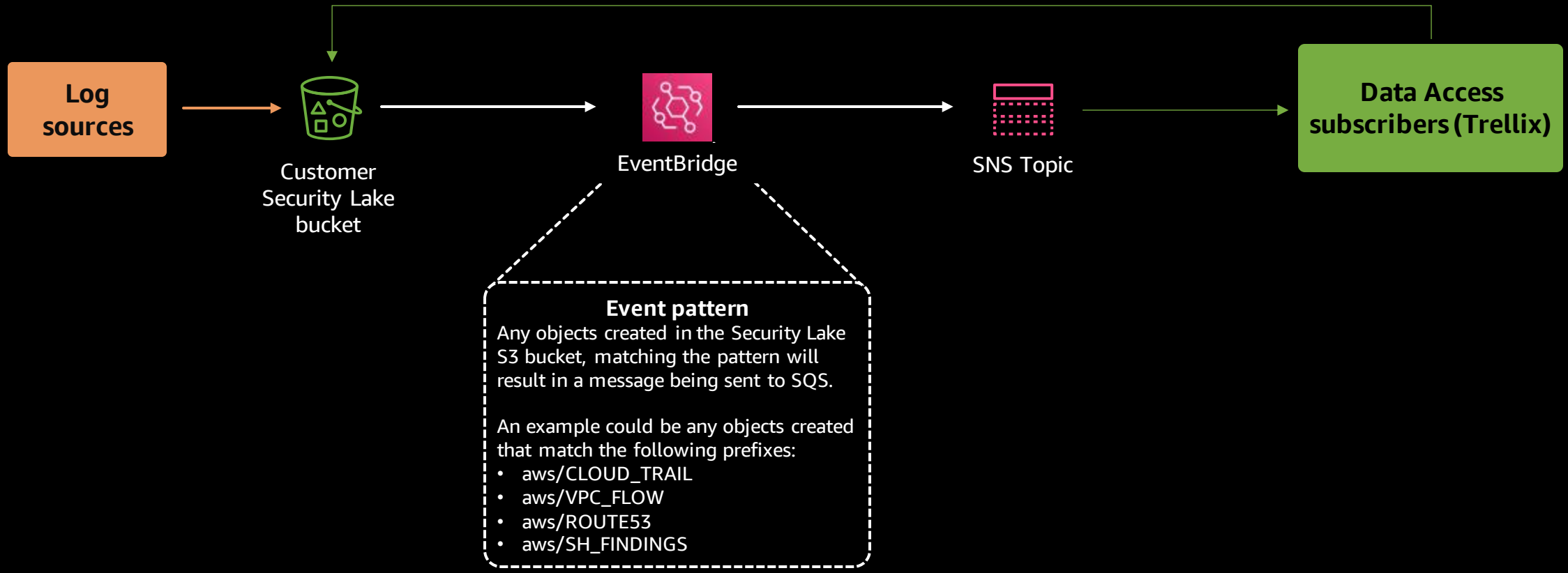
- Receive a stream of new object notification
- Direct access to Amazon S3 objects
- Security Lake manages the infrastructure and permissions

Query access

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

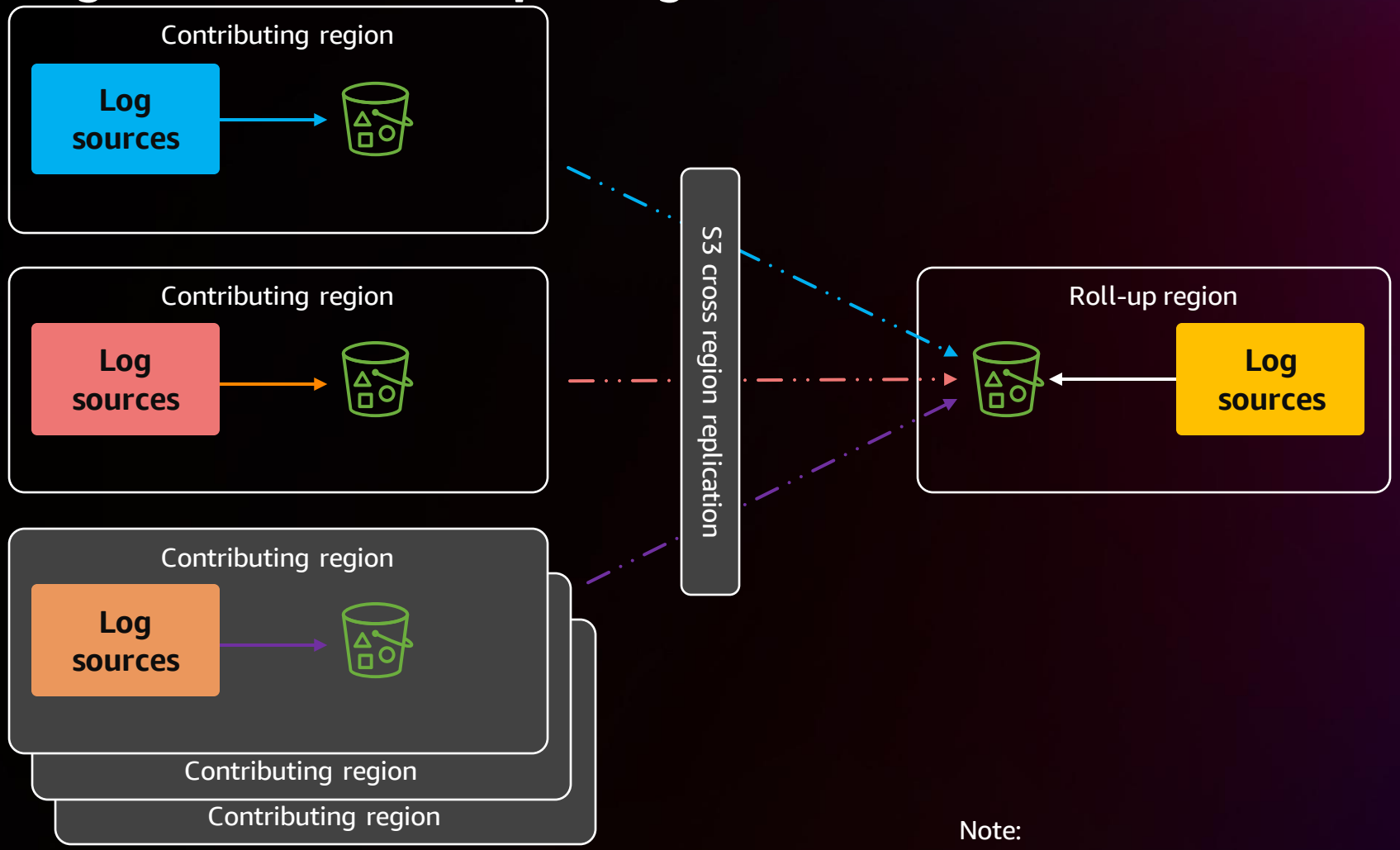
Data Access Subscriber flow

Sending events to Data Access Subscribers via SNS



Roll-up regions overview

Centralizing data from multiple regions

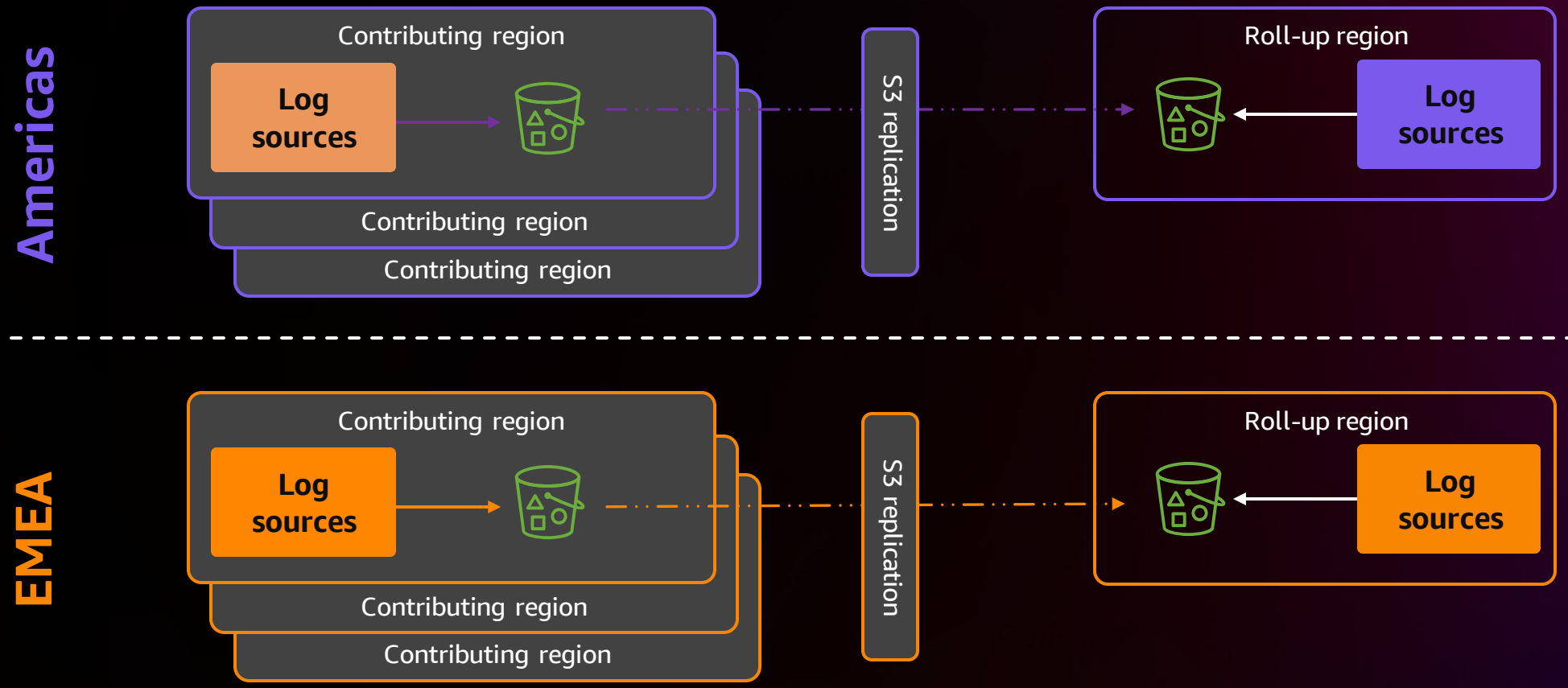


Note:

- S3 replication is configured automatically during roll-up region setup

Multiple roll-up regions

Keeping data within geographic areas to help with data residency

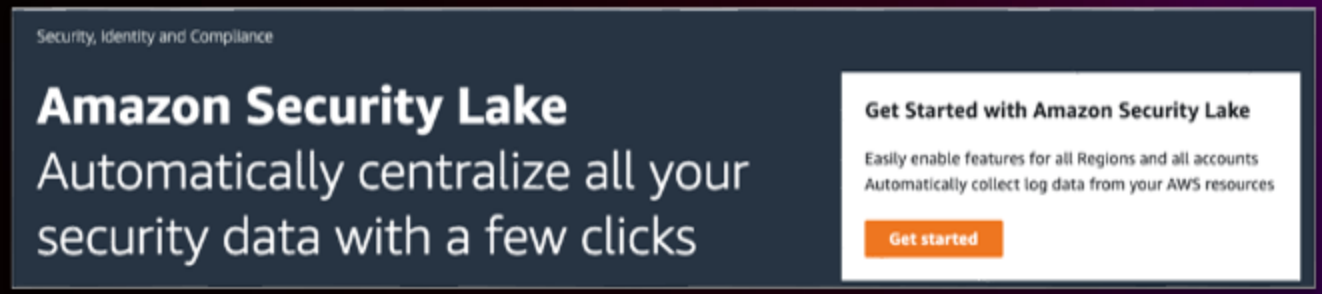


Note:

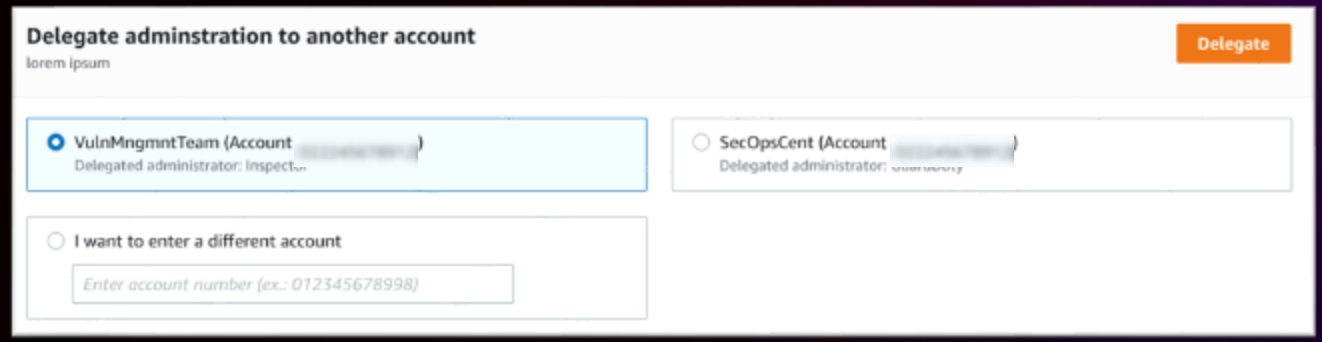
- S3 replication is configured automatically during roll-up region setup

Getting started – Enterprise-wide enablement

Security Lake works with AWS Organizations



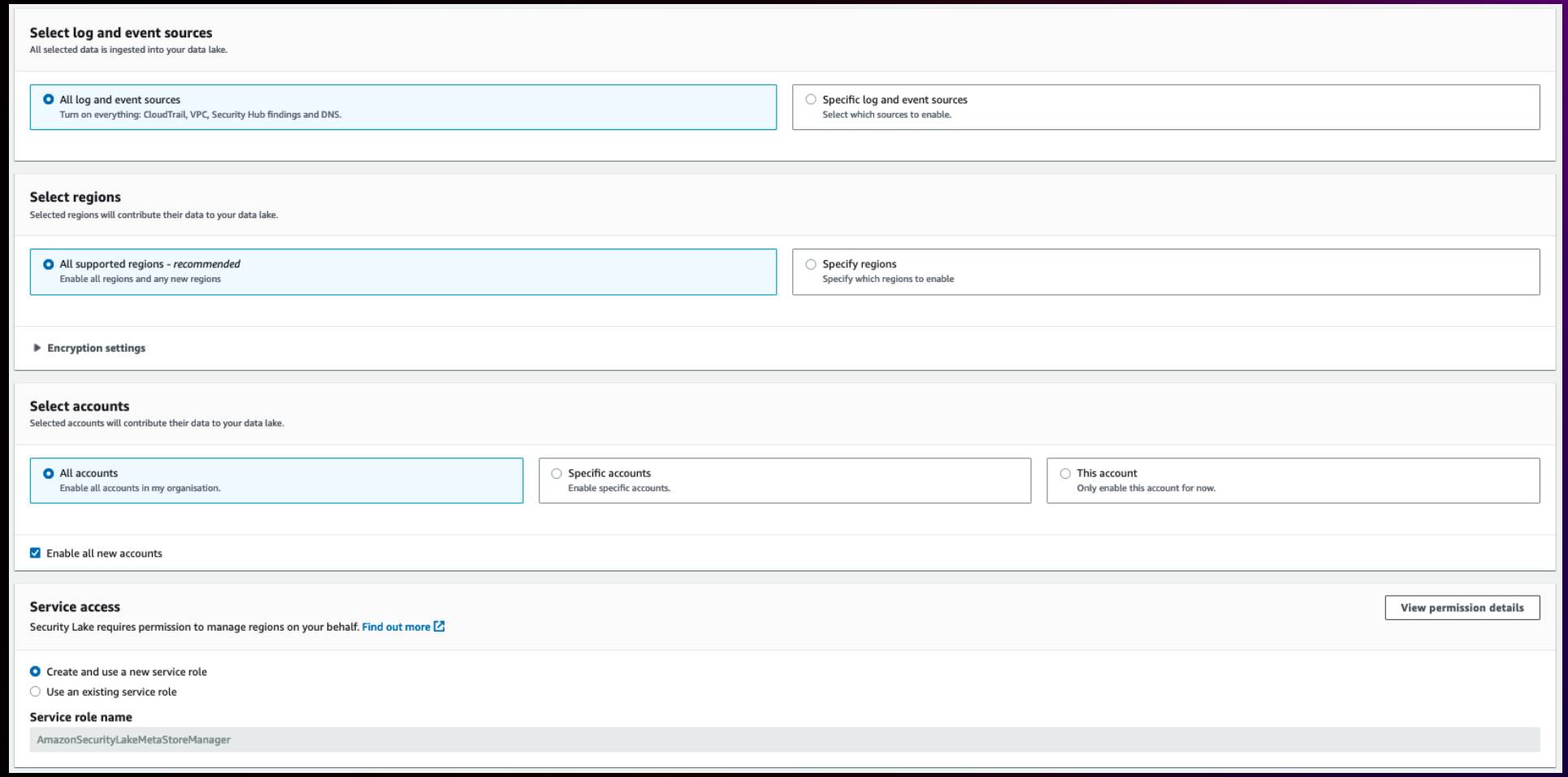
Start from your organization management account



Elected a delegated admin account to manage your security data

Getting started – Collect everything

- Everything on by default
- Multi-Region enablement
- All accounts in your organization
- Service role creation

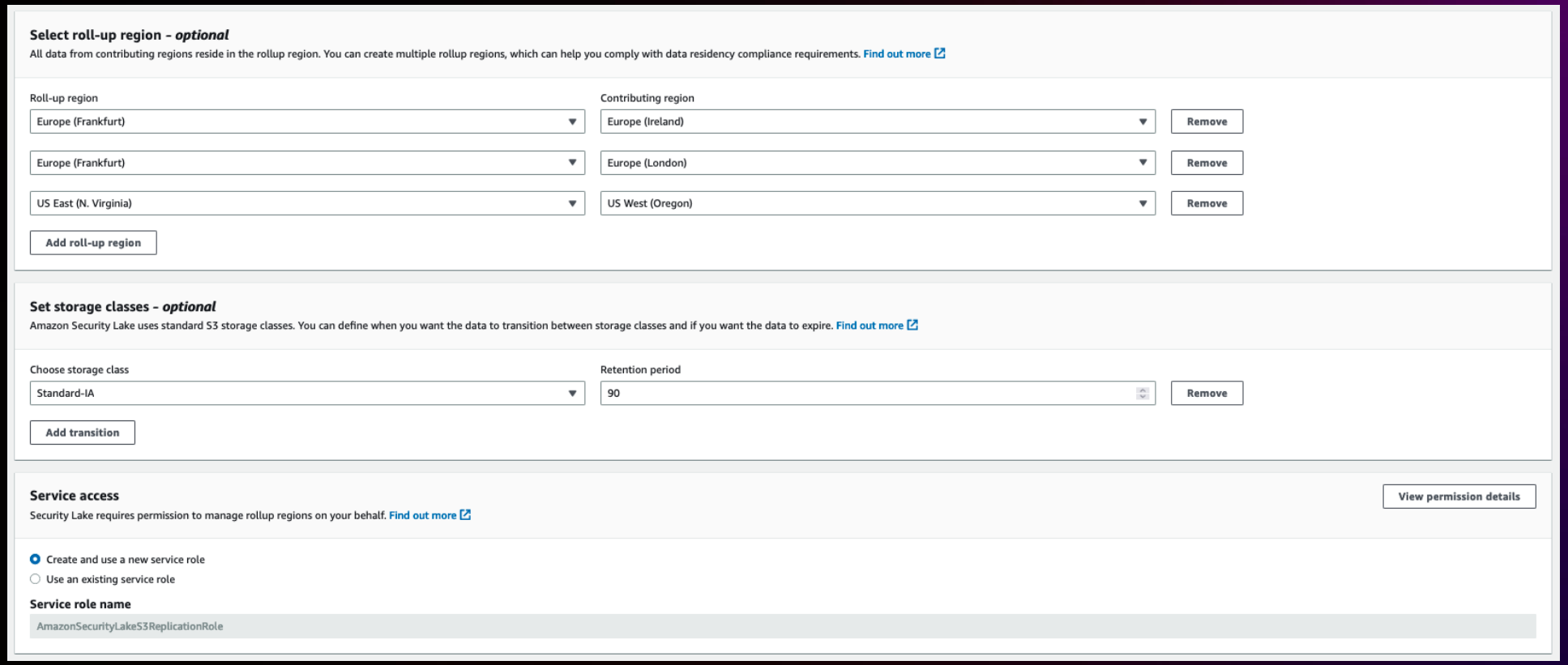


Getting started – Centralization and retention

One or multiple central Regions

Define storage class transitions

S3 replication role

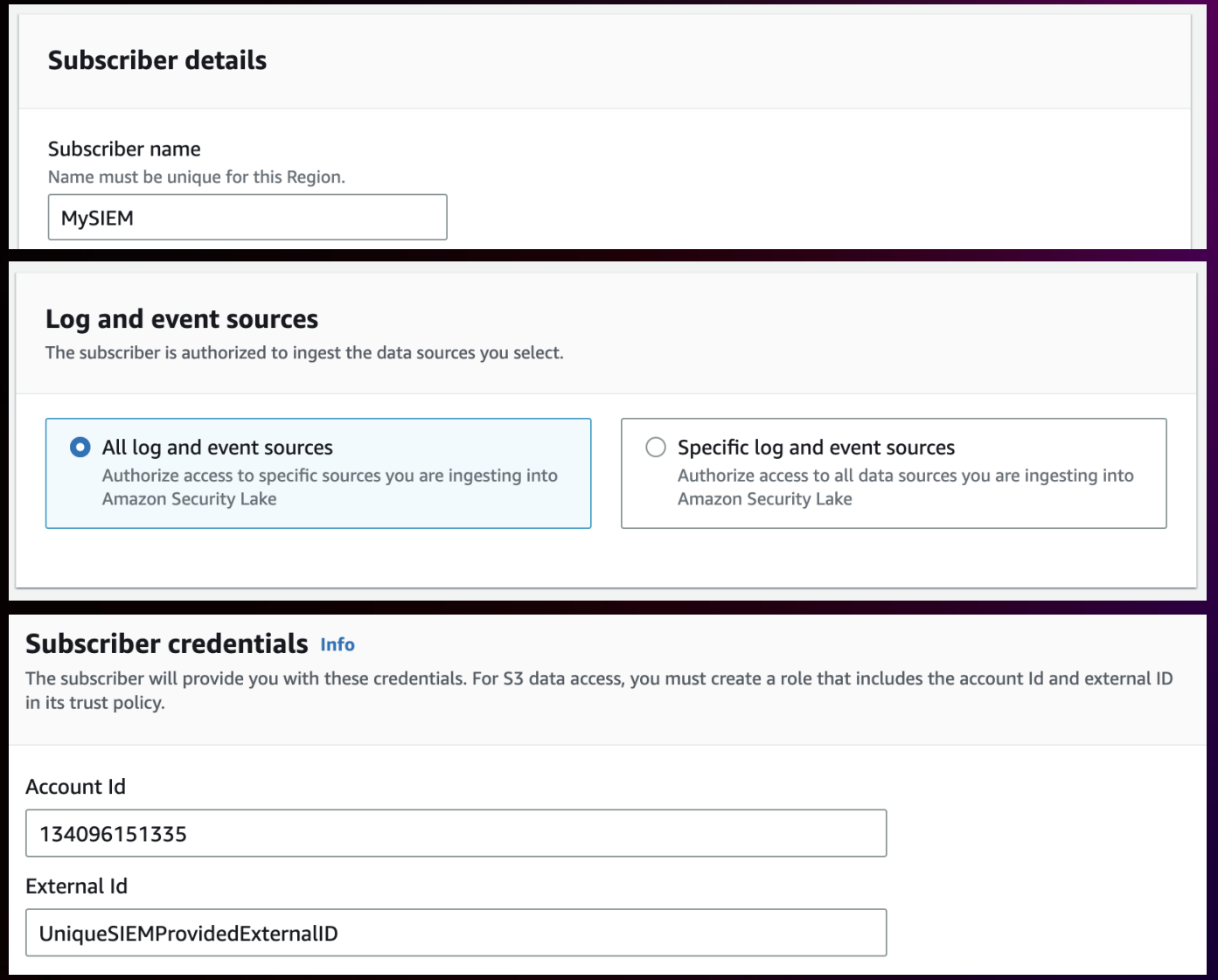


Configure subscribers

Define name

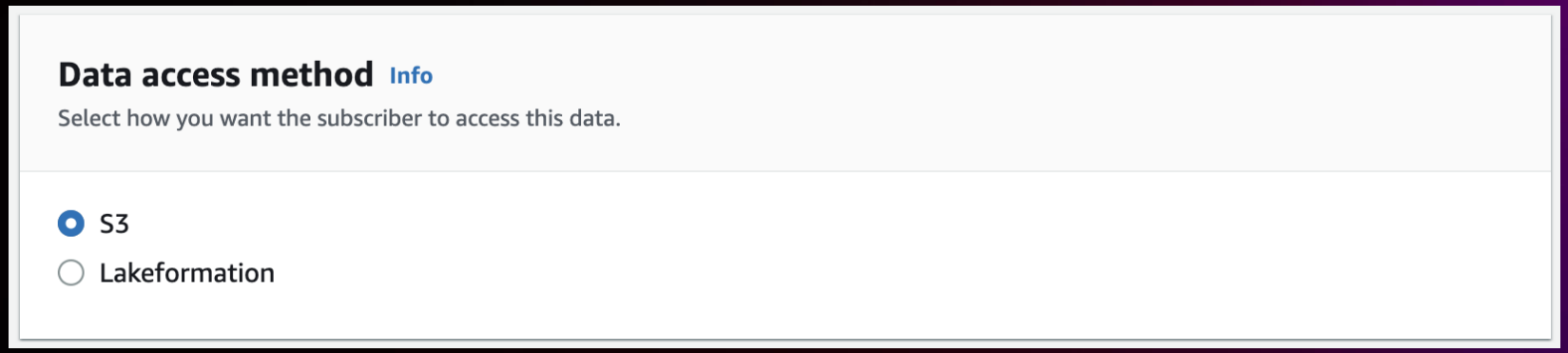
Select the data sources you want to share

Provide AWS account ID and unique external ID

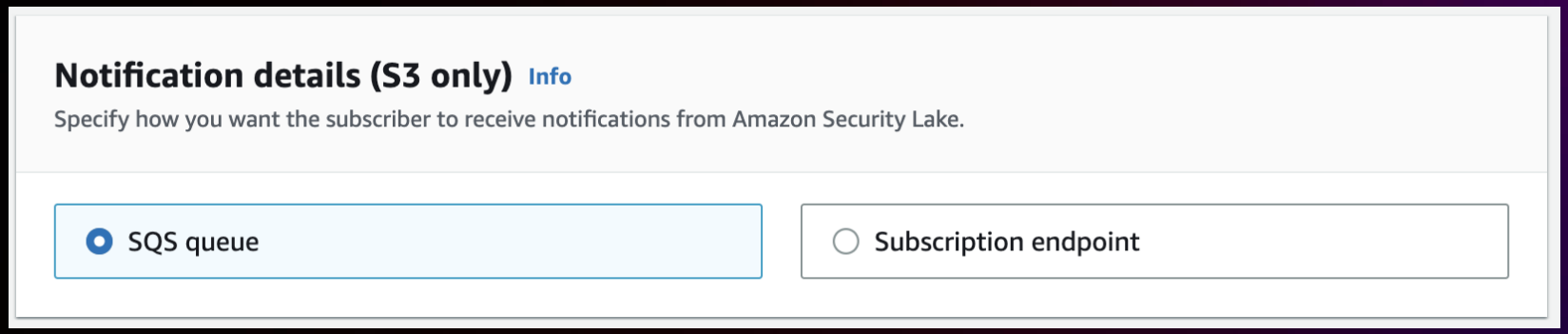


Configure subscribers

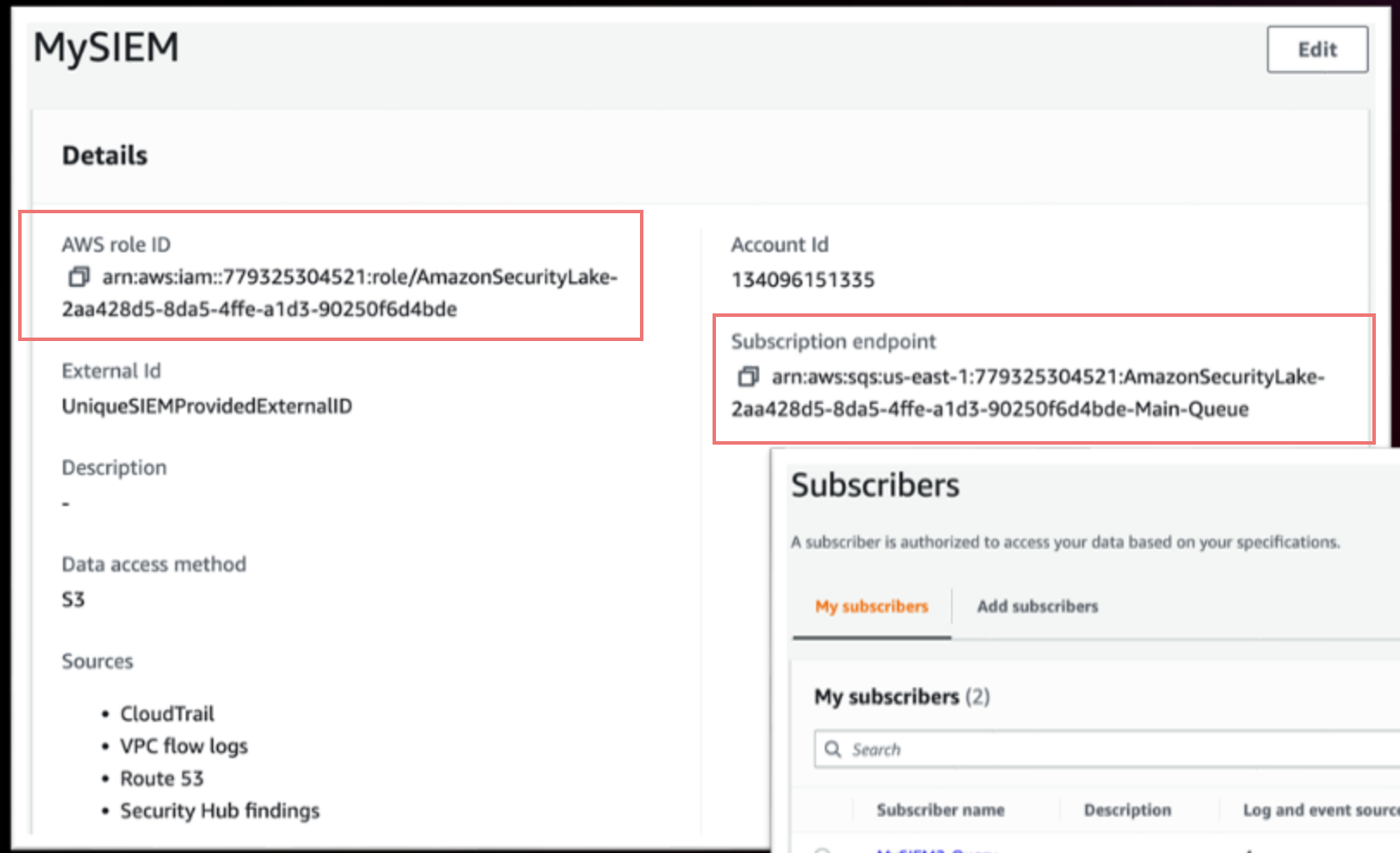
Select a data access method

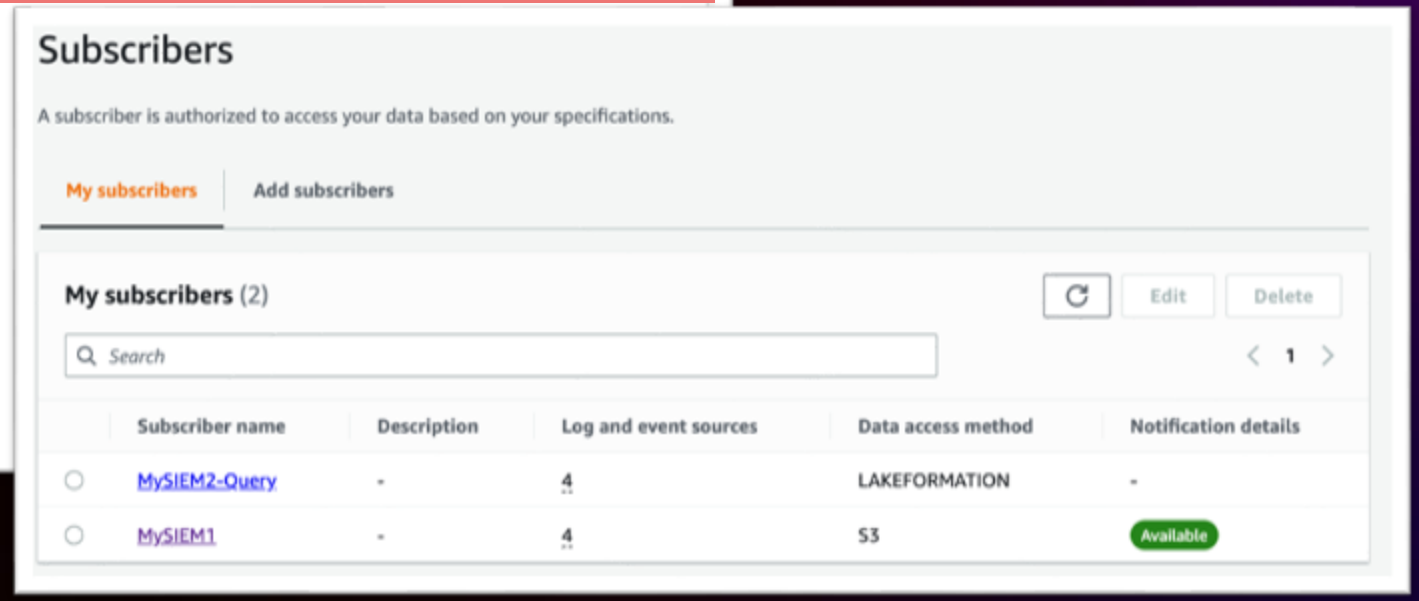


Select preferred object notification mechanism



Configure subscribers





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

Get started

Go to the Security Lake product page to learn more

Trellix XDR in the AWS Marketplace

Get Started with Trellix and Amazon Security Lake

Thank you!