

# 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.



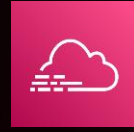
AWS Network Firewall



Amazon CloudWatch



Amazon Route 53 Resolver  
DNS Firewall



AWS CloudTrail



Amazon Virtual Private Cloud  
(Amazon VPC) Flow Logs



Amazon Inspector



AWS Verified Access



Amazon Guard Duty



Amazon Simple Storage Service  
(Amazon S3)



AWS Security Hub



Amazon Security Lake

# Cloud Native Detection & Response with AWS



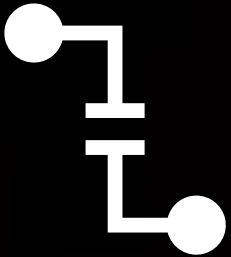
## Security Monitoring and Threat Detection



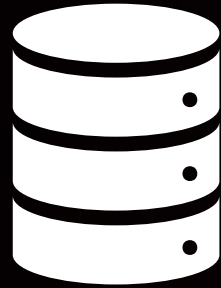
Integrated with AWS Workloads in an AWS Account, along with identities and network activity



# 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



Amazon S3



Amazon VPC



AWS CloudTrail



Amazon Route 53

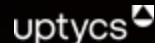
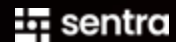
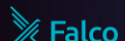
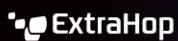


AWS Security Hub



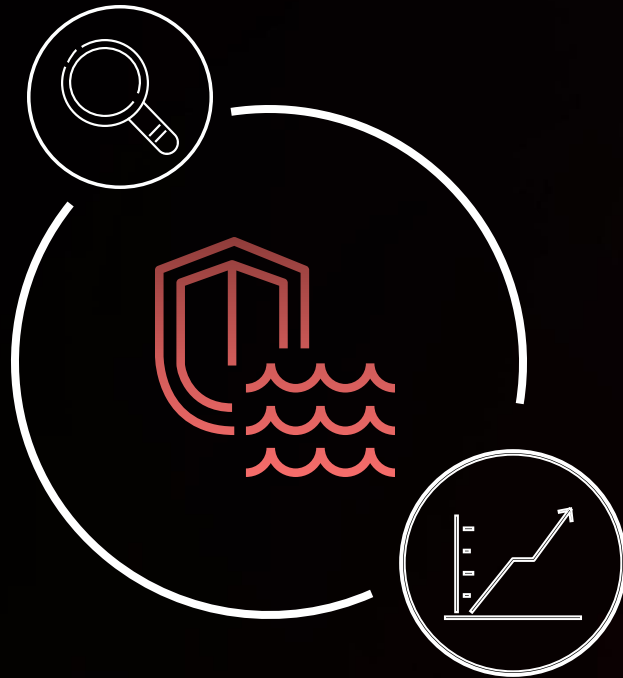
AWS Lambda

## Partner Sources



# Security Lake Partners: Analytics Tools & Service Partners

OVER 30 ANALYTICS AND SERVICES PARTNERS



Amazon Athena



Amazon OpenSearch



Amazon SageMaker

## Partner Analytics

CHAOSSEARCH



DEVO

IBM

new relic. **RAPID7**



securonix

SentinelOne

SQC PRIME

splunk>

STELLAR CYBER

sumo logic

SWIMLANE

tines

torq=

Trellix

wazuh.

## Service Partners

accenture

Booz Allen

CMD

Deloitte.

DXC TECHNOLOGY

insbuilt:  
Driving with the cloud

kyndryl.

EVIDEN

HCOP

IBM

Infosys

leidos

MEGAZONE CLOUD

pwc

SQC PRIME

tcs TATA CONSULTANCY SERVICES

wipro



# Sources & Subscribers

Source



Subscribe

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

Amazon Security Lake

Ingest & Normalization

Manage Lifecycle

Manage Subscribers

Orchestration

S3 SQS Lambda EventBridge  
Glue Athena Lake Formation

Amazon Athena
Amazon OpenSearch
Amazon SageMaker

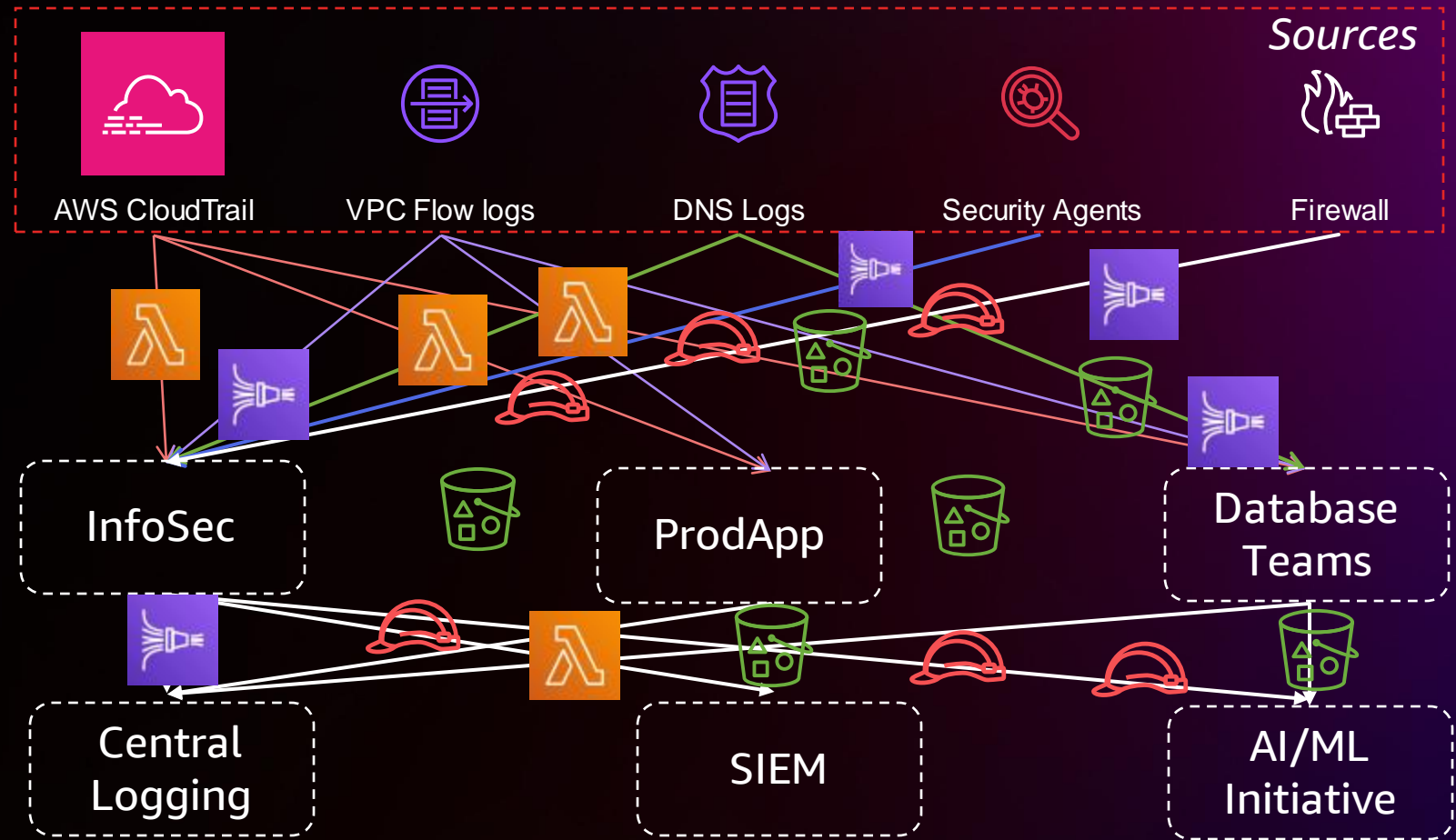
Trellix

Other Partners/Custom Sources

Trellix



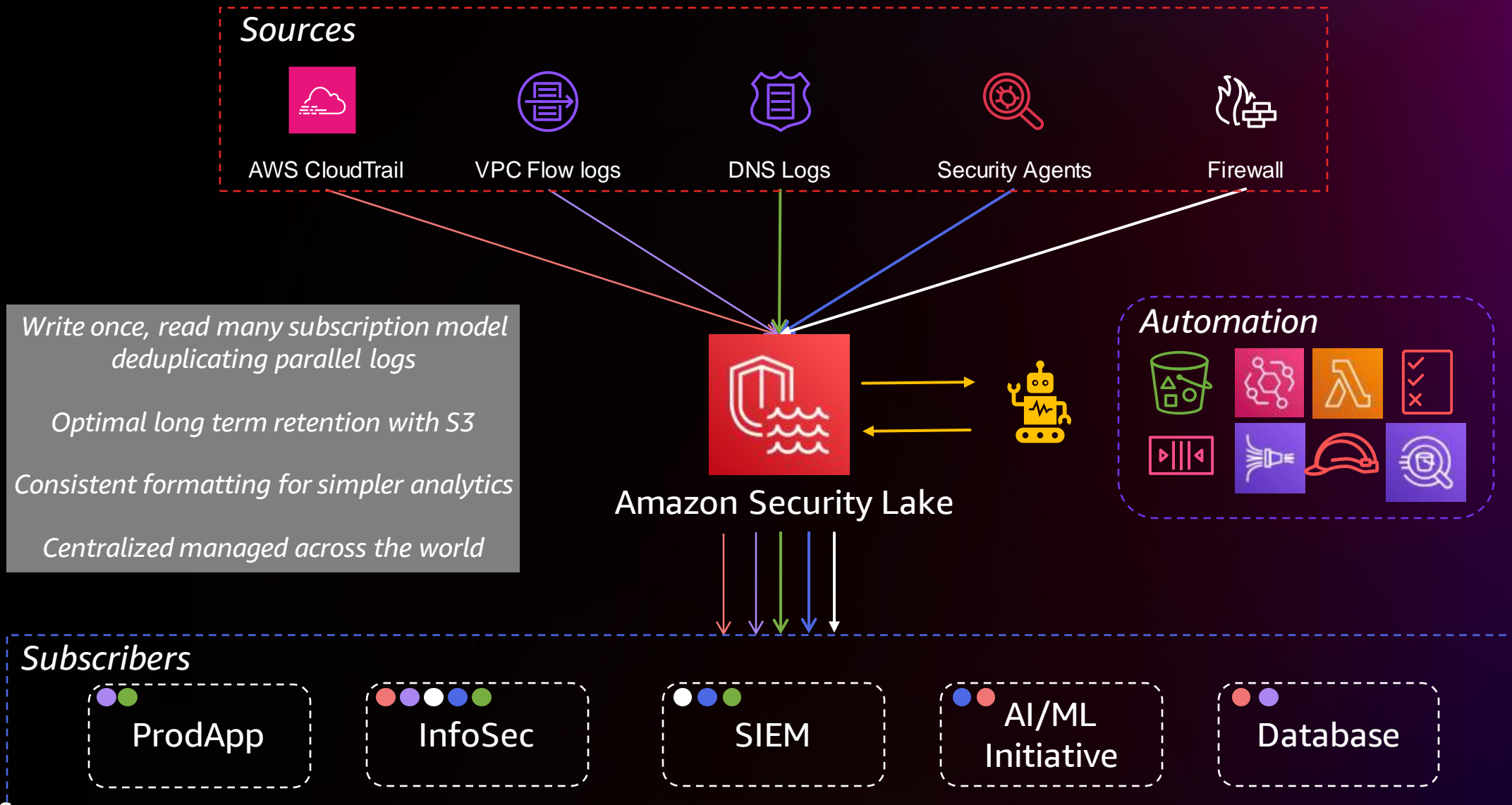
# Before Security Lake – Resource based logging



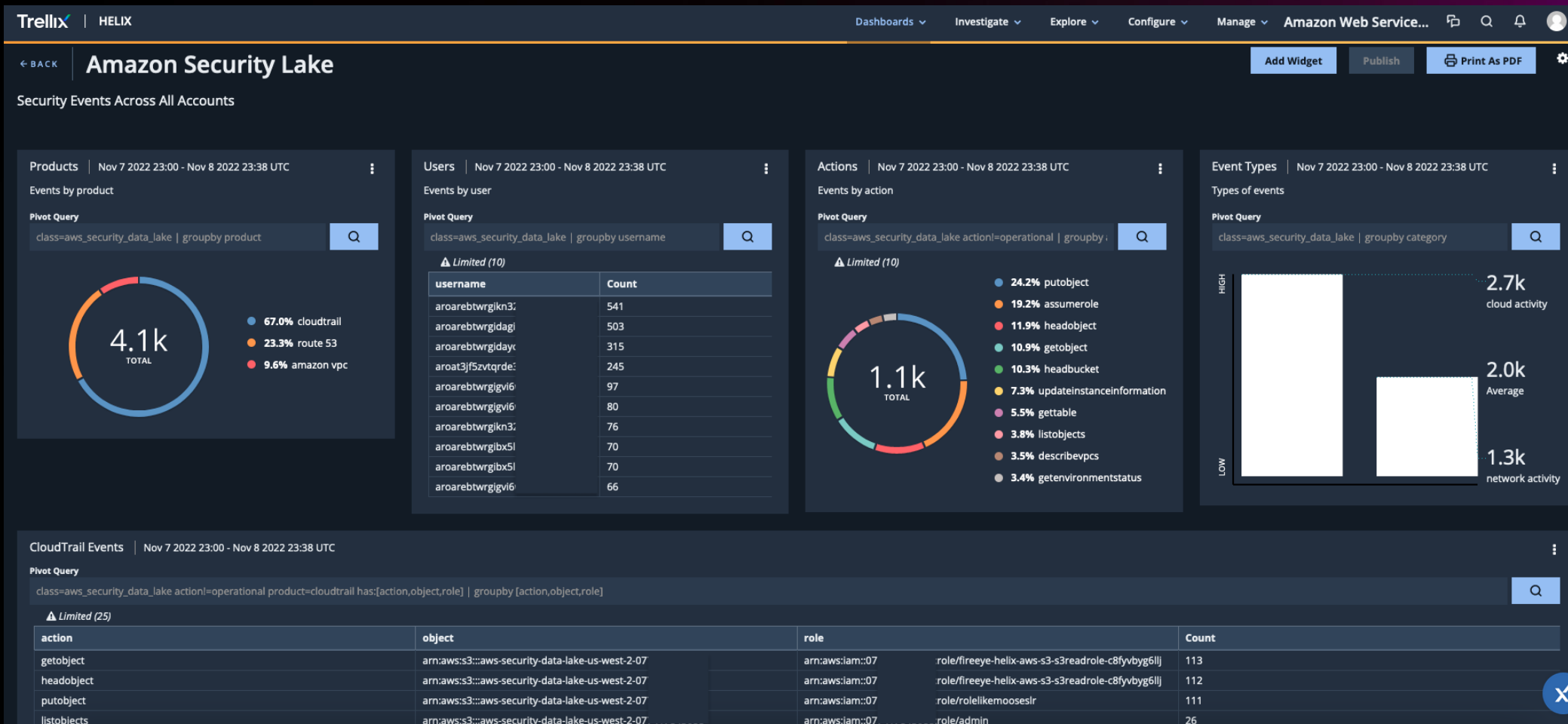
*Duplication of data*  
*Multiple integrations*  
*Data in different formats*  
*Multiple long term storage options*



# After Security Lake – the data lake model

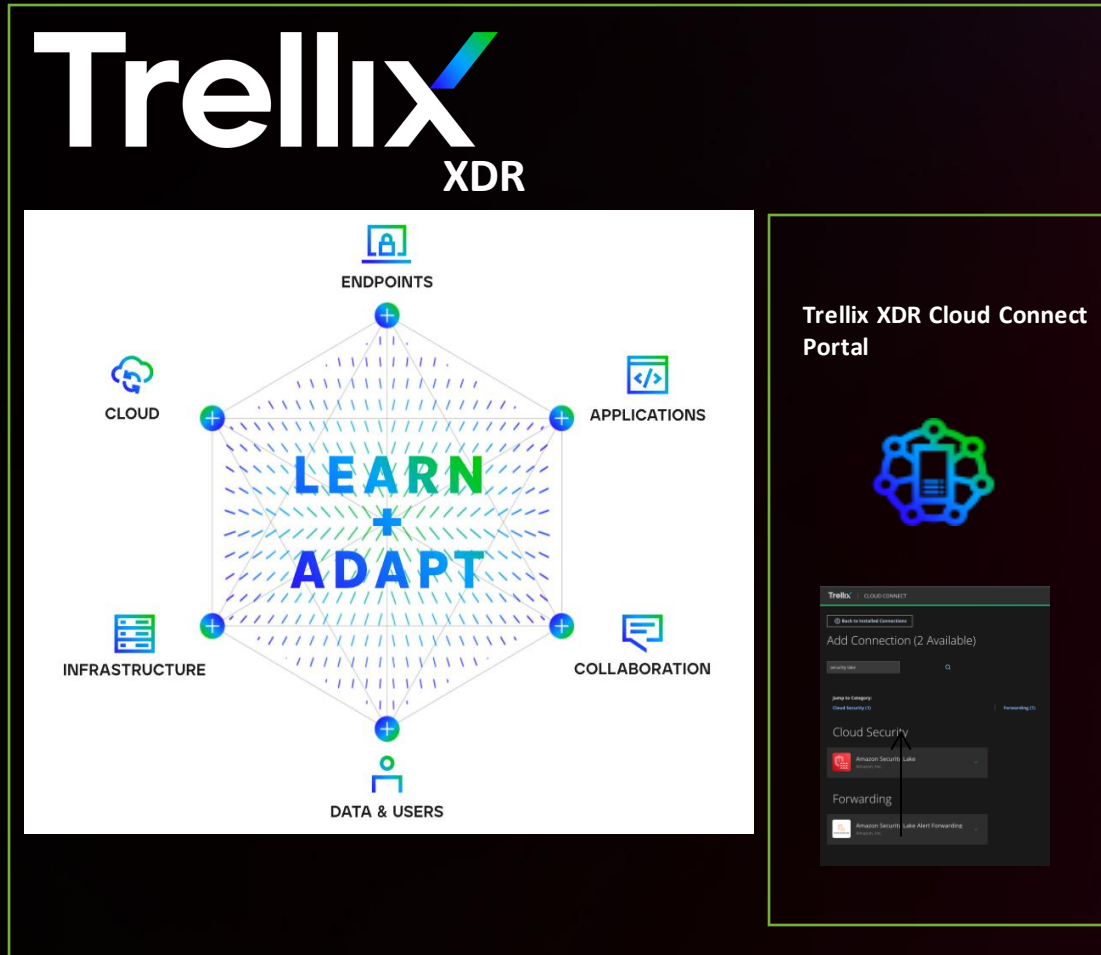


# Analyze with Trellix



# 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.

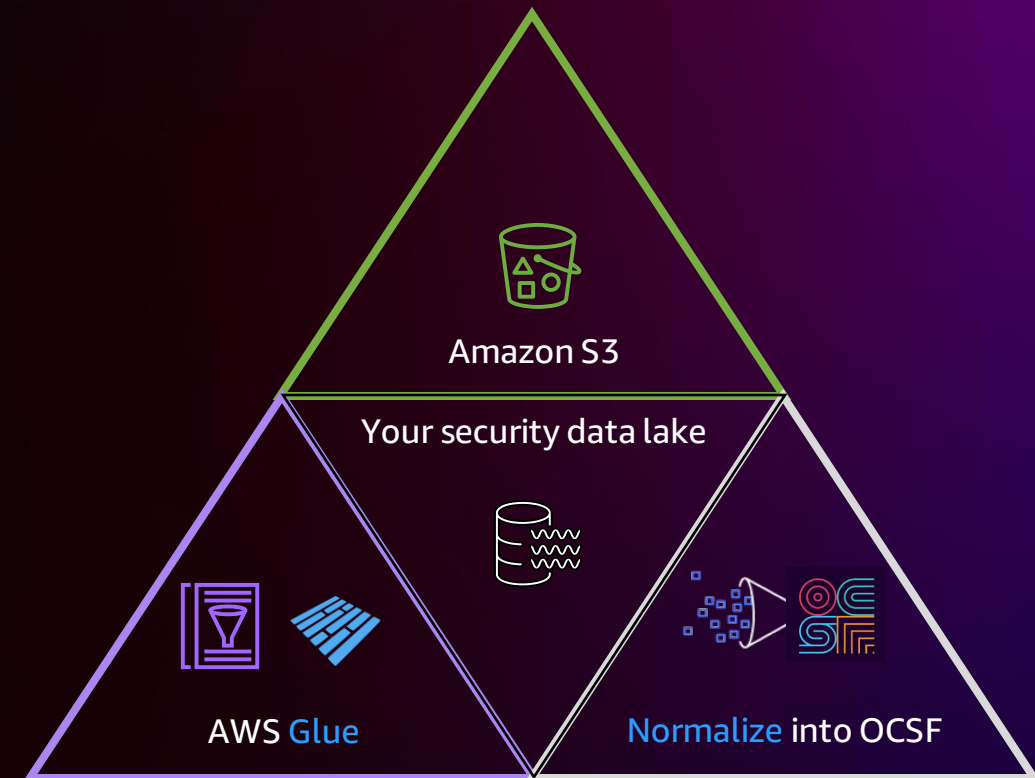
# What's happening under the hood?

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

Enable logging across all Regions, accounts, and resources

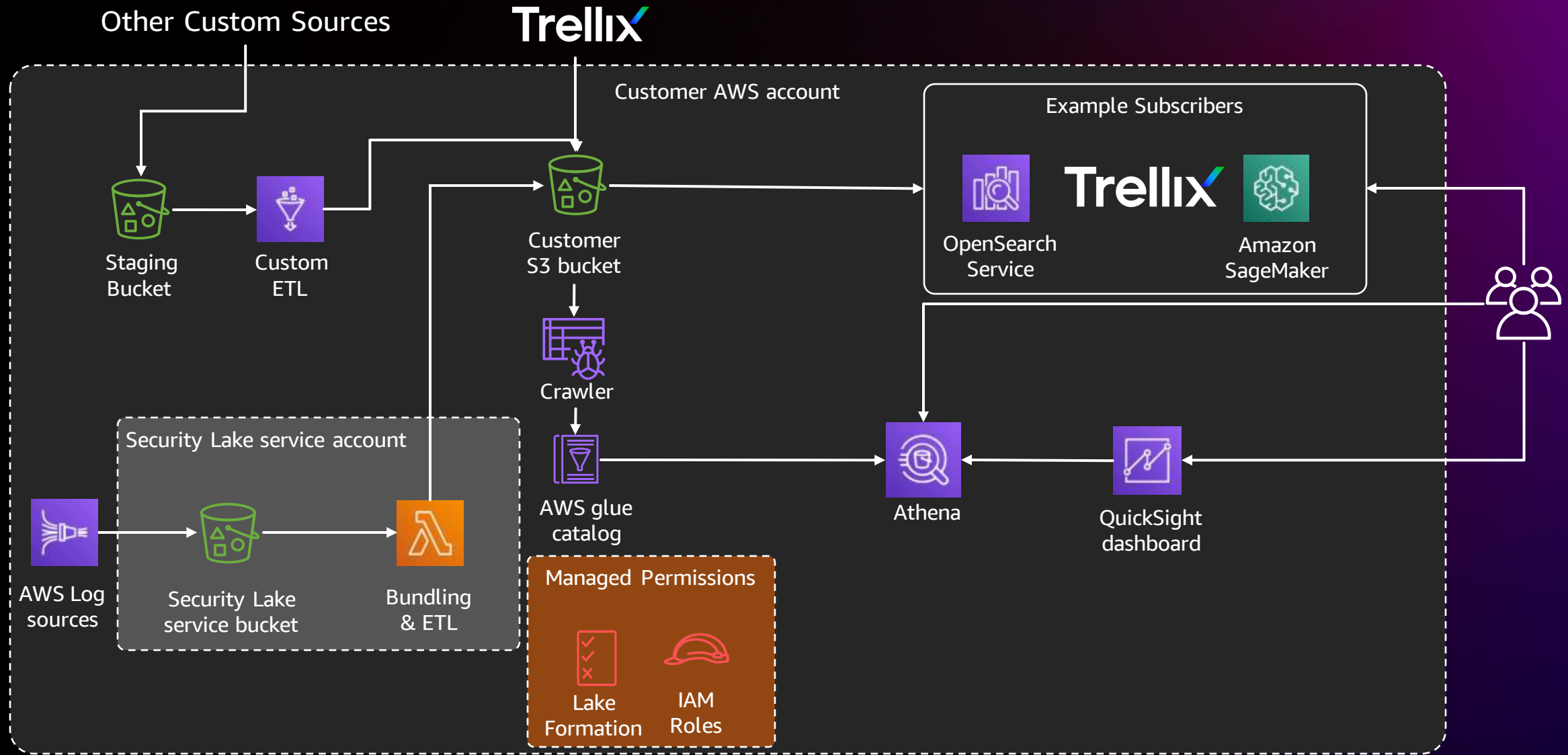
Transform and partition all incoming data to OCSF and Apache Parquet

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

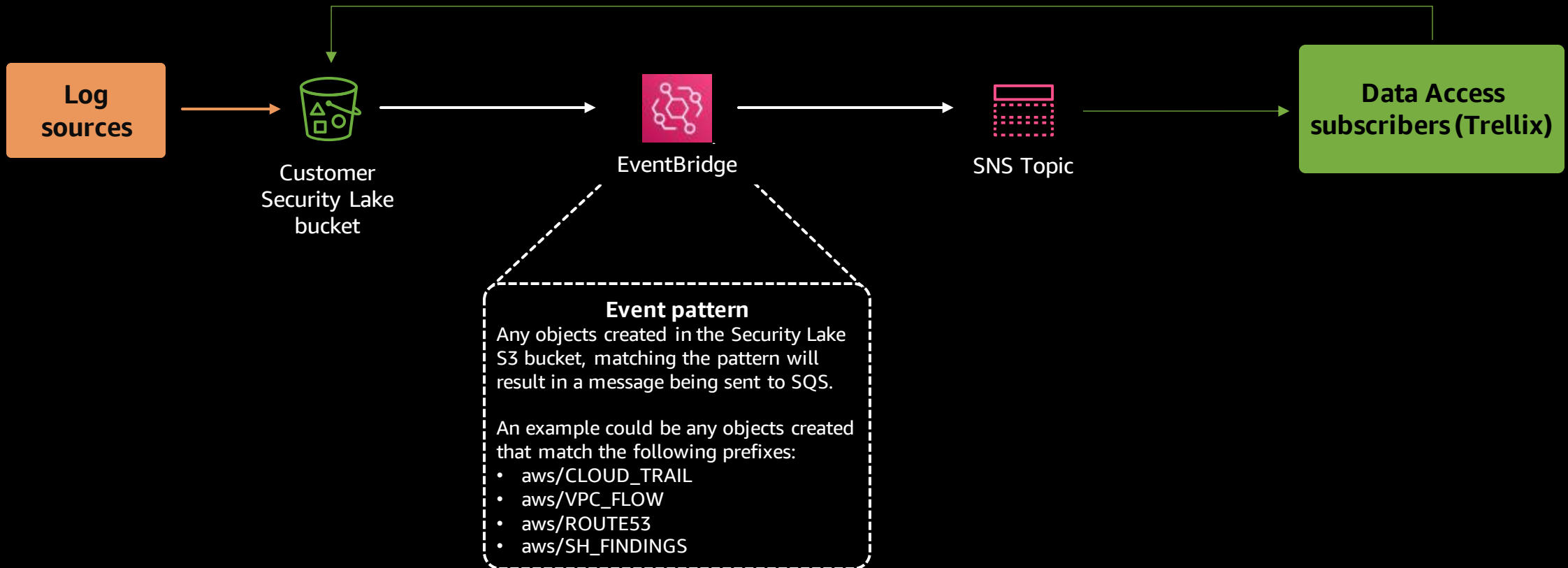
Cross-account support via Lake Formation

No need to move data around



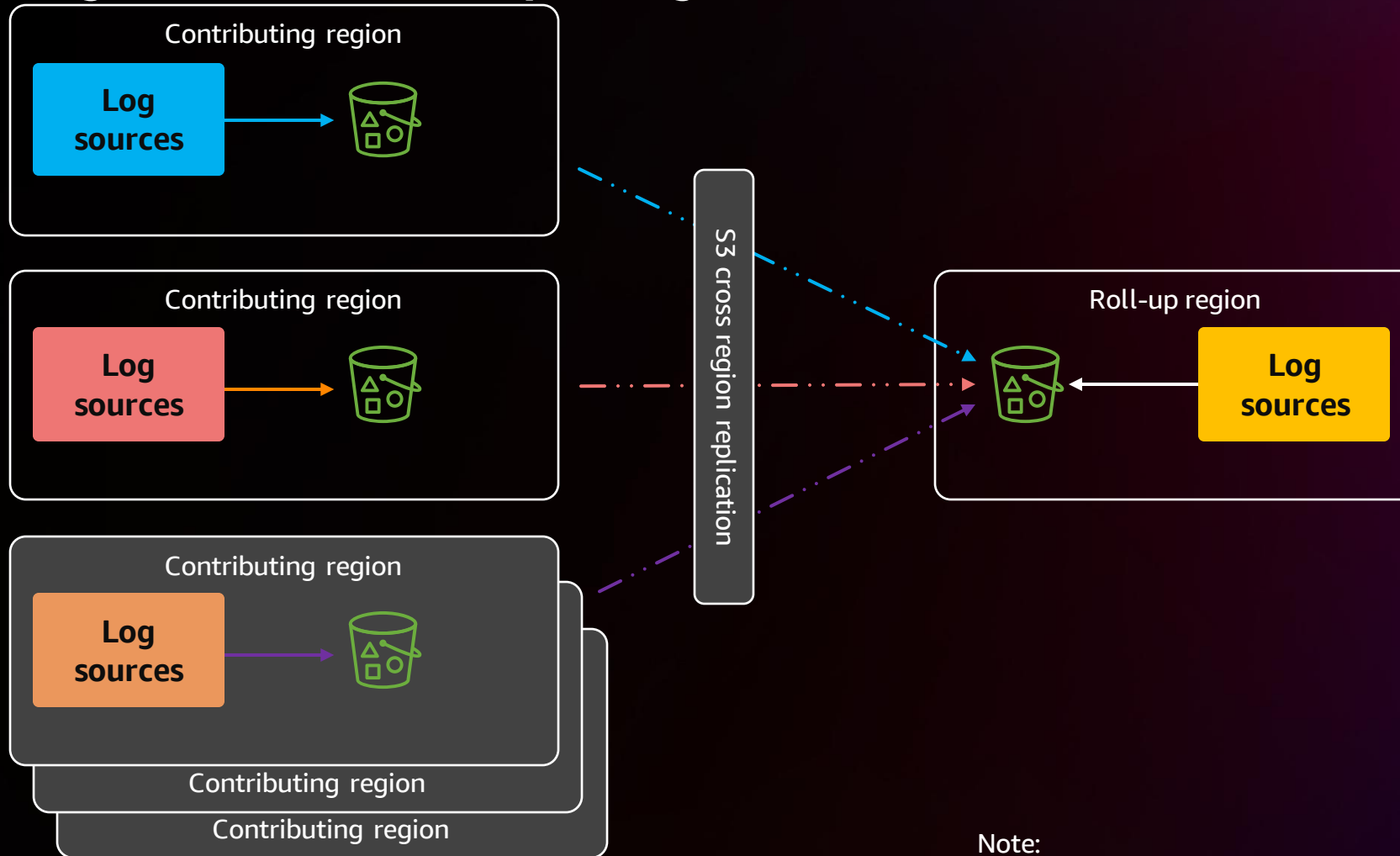
# Data Access Subscriber flow

## Sending events to Data Access Subscribers via SNS



# Roll-up regions overview

## Centralizing data from multiple regions



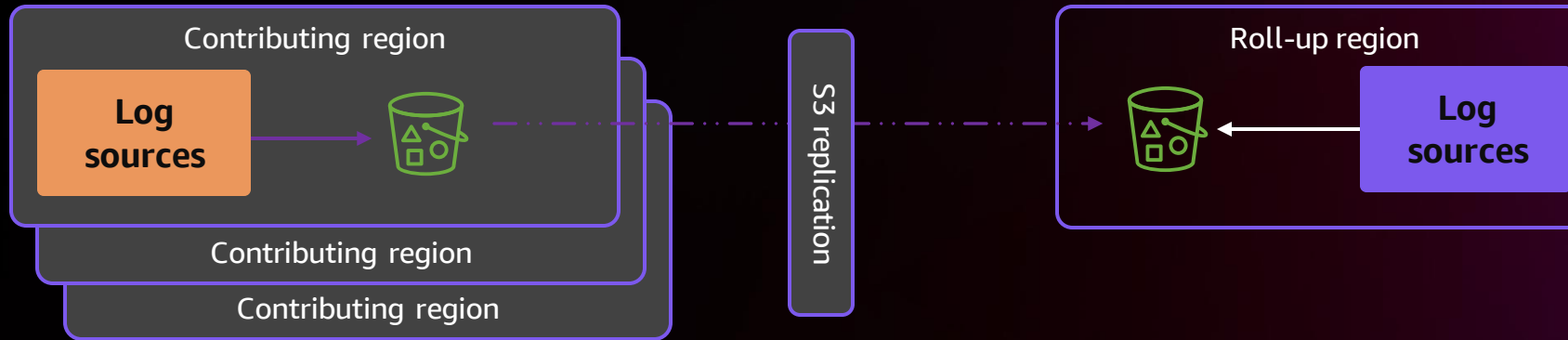
Note:

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

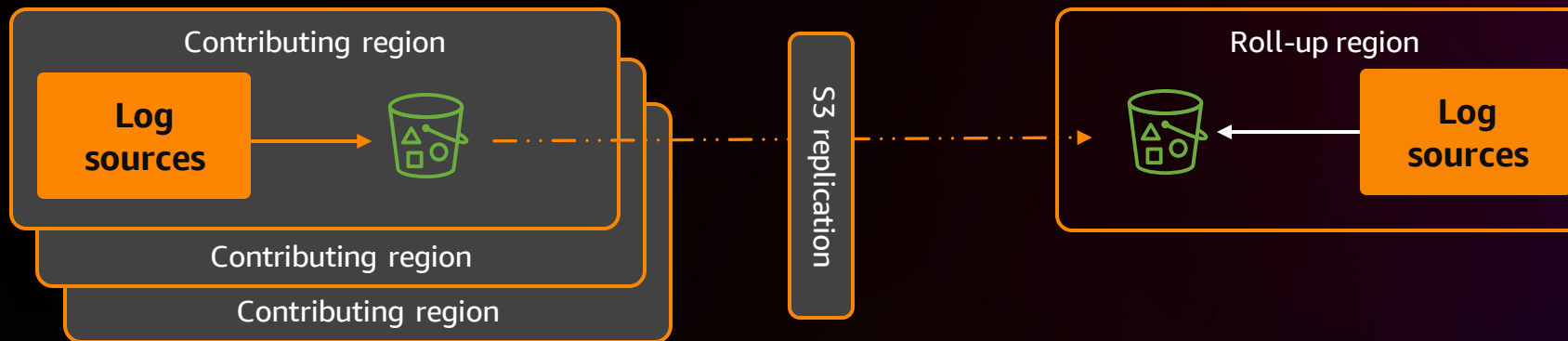
# Multiple roll-up regions

Keeping data within geographic areas to help with data residency

Americas



EMEA

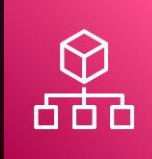


Note:

- 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

Security, Identity and Compliance

## Amazon Security Lake

Automatically centralize all your security data with a few clicks

**Get Started with Amazon Security Lake**

Easily enable features for all Regions and all accounts  
Automatically collect log data from your AWS resources

[Get started](#)

Elected a delegated admin account to manage your security data

### Delegate administration to another account

lore ipsum [Delegate](#)

VulnMngmntTeam (Account [redacted])  
Delegated administrator: Inspect...

SecOpsCent (Account [redacted])  
Delegated administrator: [redacted]

I want to enter a different account

# Getting started – Collect everything

Everything on by default

Multi-Region enablement

All accounts in your organization

Service role creation

**Select log and event sources**  
All selected data is ingested into your data lake.

All log and event sources  
Turn on everything: CloudTrail, VPC, Security Hub findings and DNS.

Specific log and event sources  
Select which sources to enable.

**Select regions**  
Selected regions will contribute their data to your data lake.

All supported regions - *recommended*  
Enable all regions and any new regions

Specify regions  
Specify which regions to enable.

► Encryption settings

**Select accounts**  
Selected accounts will contribute their data to your data lake.

All accounts  
Enable all accounts in my organisation.

Specific accounts  
Enable specific accounts.

This account  
Only enable this account for now.

Enable all new accounts

**Service access**  
Security Lake requires permission to manage regions on your behalf. [Find out more](#)

Create and use a new service role

Use an existing service role

**Service role name**  
AmazonSecurityLakeMetaStoreManager

[View permission details](#)



# Getting started – Centralization and retention

One or multiple central Regions

Define storage class transitions

S3 replication role

### Select roll-up region - *optional*

All data from contributing regions reside in the rollup region. You can create multiple rollup regions, which can help you comply with data residency compliance requirements. [Find out more](#)

Roll-up region	Contributing region	
Europe (Frankfurt)	Europe (Ireland)	<button>Remove</button>
Europe (Frankfurt)	Europe (London)	<button>Remove</button>
US East (N. Virginia)	US West (Oregon)	<button>Remove</button>

Add roll-up region

### Set storage classes - *optional*

Amazon Security Lake uses standard S3 storage classes. You can define when you want the data to transition between storage classes and if you want the data to expire. [Find out more](#)

Choose storage class	Retention period	
Standard-IA	90	<button>Remove</button>

Add transition

### Service access

Security Lake requires permission to manage rollup regions on your behalf. [Find out more](#)

Create and use a new service role  
 Use an existing service role

**Service role name**

AmazonSecurityLakeS3ReplicationRole

[View permission details](#)



# Configure subscribers

Define name

Select the data sources  
you want to share

Provide AWS account ID  
and unique external ID

## Subscriber details

### Subscriber name

Name must be unique for this Region.

## Log and event sources

The subscriber is authorized to ingest the data sources you select.

All log and event sources

Authorize access to specific sources you are ingesting into Amazon Security Lake

Specific log and event sources

Authorize access to all data sources you are ingesting into Amazon Security Lake

## Subscriber credentials [Info](#)

The subscriber will provide you with these credentials. For S3 data access, you must create a role that includes the account ID and external ID in its trust policy.

### Account Id

### External Id



# Configure subscribers

Select a data access method

## Data access method [Info](#)

Select how you want the subscriber to access this data.

- S3
- Lakeformation

Select preferred object notification mechanism

## Notification details (S3 only) [Info](#)

Specify how you want the subscriber to receive notifications from Amazon Security Lake.

SQS queue

Subscription endpoint

# Configure subscribers

**MySIEM** Edit

**Details**

**AWS role ID**  
arn:aws:iam::779325304521:role/AmazonSecurityLake-2aa428d5-8da5-4ffe-a1d3-90250f6d4bde

**Account Id**  
134096151335

**Subscription endpoint**  
arn:aws:sqs:us-east-1:779325304521:AmazonSecurityLake-2aa428d5-8da5-4ffe-a1d3-90250f6d4bde-Main-Queue

**External Id**  
UniqueSIEMProvidedExternalID

**Description**  
-

**Data access method**  
S3

**Sources**

- CloudTrail
- VPC flow logs
- Route 53
- Security Hub findings

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

**Subscribers**

A subscriber is authorized to access your data based on your specifications.

[My subscribers](#) [Add subscribers](#)

**My subscribers (2)** Refresh Edit Delete

Search

	Subscriber name	Description	Log and event sources	Data access method	Notification details
<input type="radio"/>	<a href="#">MySIEM2-Query</a>	-	4	LAKEFORMATION	-
<input type="radio"/>	<a href="#">MySIEM1</a>	-	4	S3	<span>Available</span>

# 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!

