

AWS re:Inforce

JUNE 13 - 14, 2023 | ANAHEIM, CA

TDR333

Gaining insights from Amazon Security Lake

Mark Keating (he/him)

Principal Security Solutions Architect
AWS

Keith Gilbert (he/him)

Security Engineering Manager, Amazon
Security Lake
AWS



Agenda

- Service overview
- Amazon Security Lake architecture
- How to access your data
- Example use cases and queries

What is Amazon Security Lake?

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



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

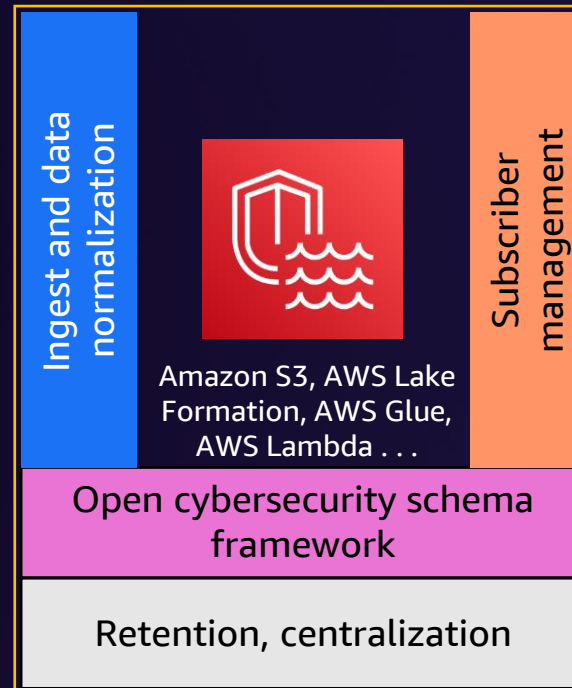
Optimize and manage security data for more efficient storage and query performance

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

How it works

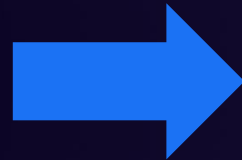
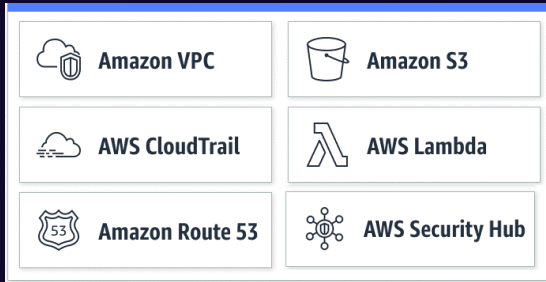
Amazon Security Lake



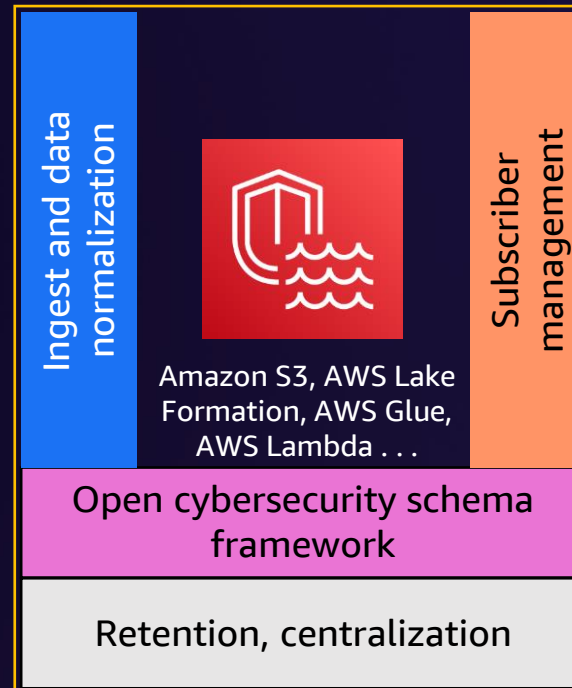
Customer-owned,
managed data lake

How it works

AWS logs sources and findings from over 50 security solutions



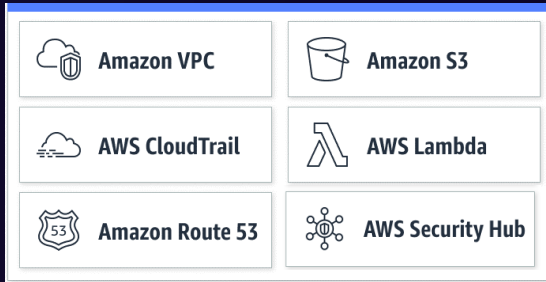
Amazon Security Lake



Customer-owned,
managed data lake

How it works

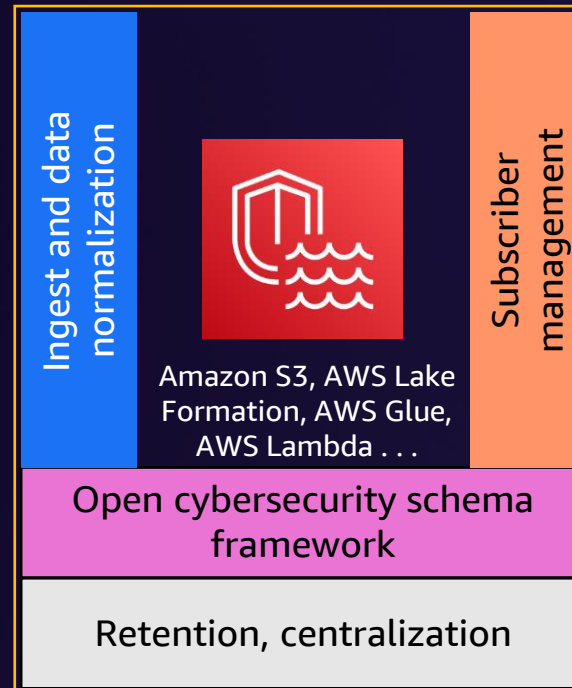
AWS logs sources and findings from over 50 security solutions



AWS Partner enterprise security solutions

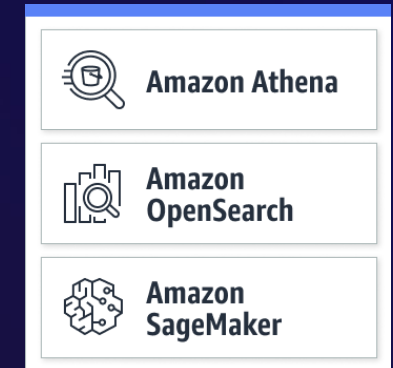
Your own data

Amazon Security Lake



Customer-owned, managed data lake

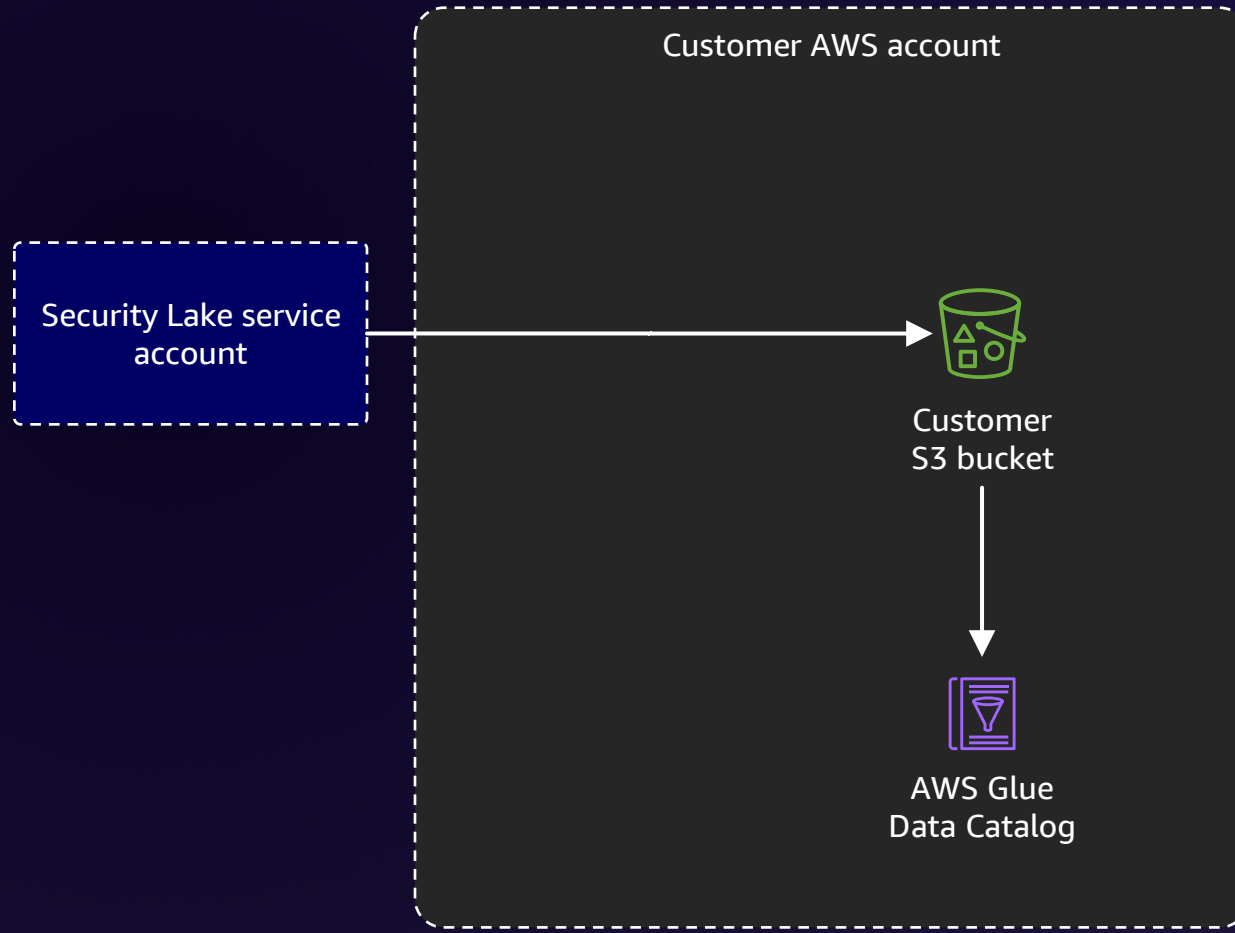
AWS analytics



AWS Partner analytics and XDR platforms

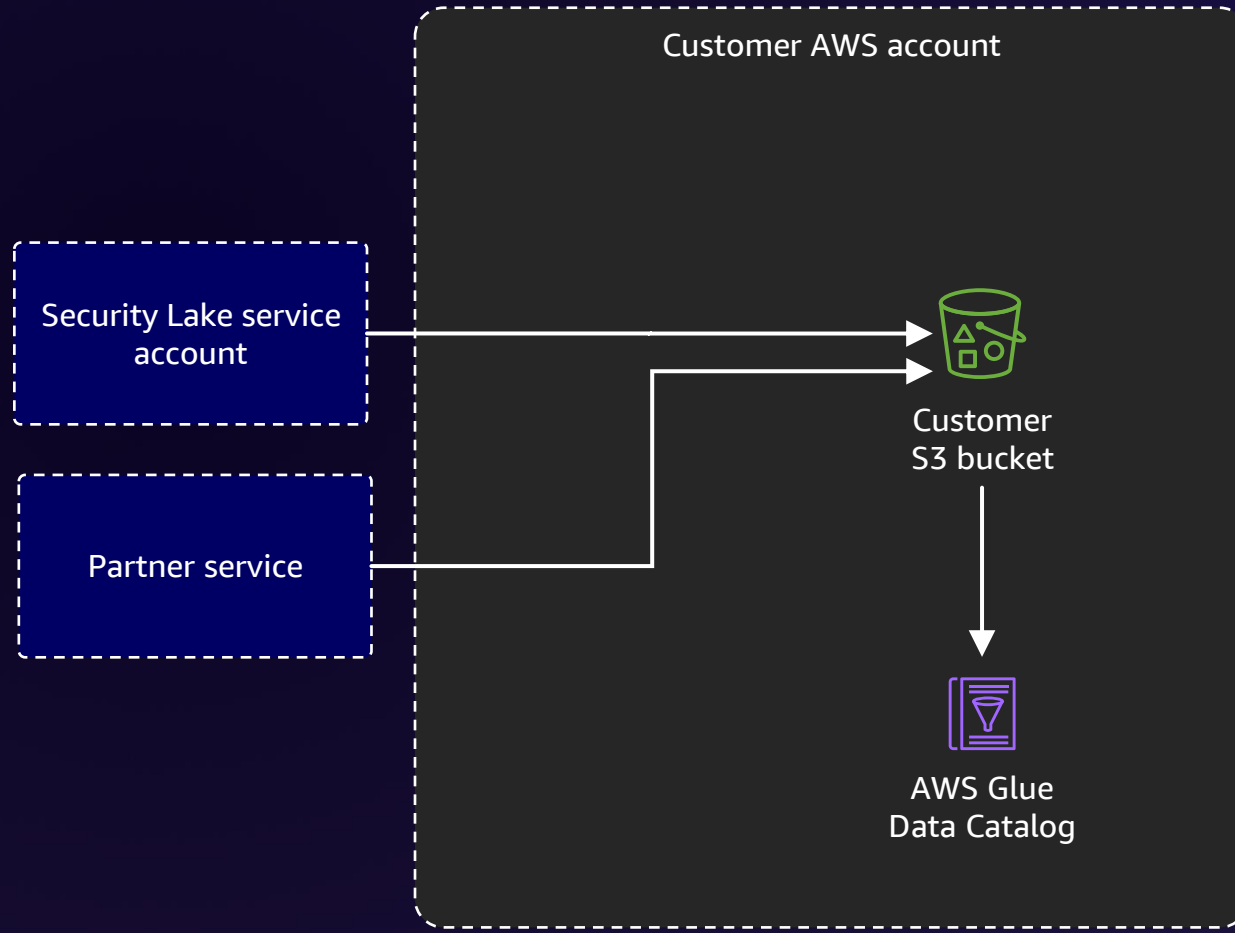
Amazon Security Lake

ARCHITECTURE OVERVIEW



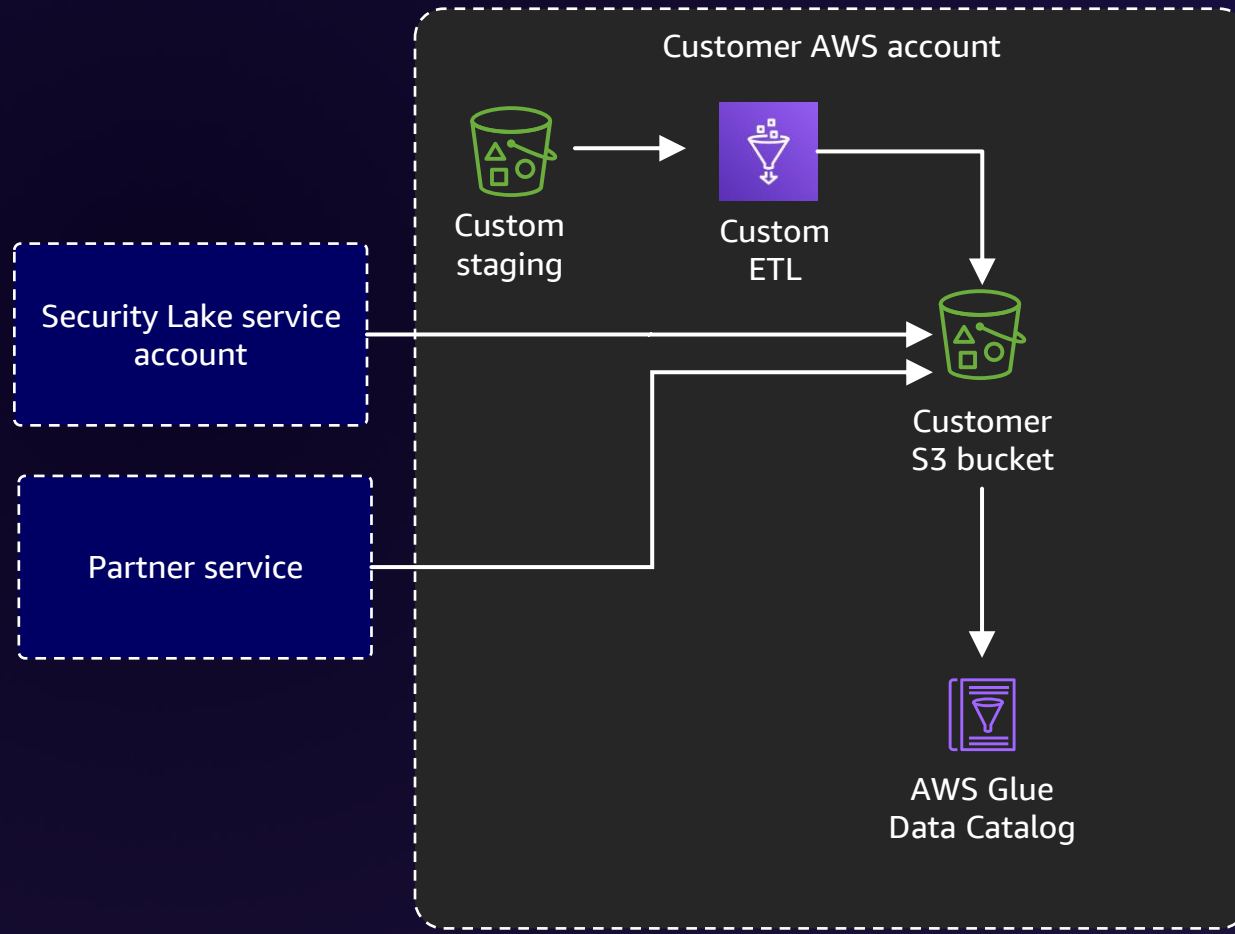
Amazon Security Lake

ARCHITECTURE OVERVIEW



Amazon Security Lake

ARCHITECTURE OVERVIEW



Amazon Security Lake

CENTRALIZED SECURITY DATA

Now what?



Amazon Security Lake

CENTRALIZED SECURITY DATA

Now what?

How do I get access to the data?



Amazon Security Lake

CENTRALIZED SECURITY DATA

Now what?

How do I get access to the data?

What tools can/should I use?

Amazon Security Lake

CENTRALIZED SECURITY DATA

Now what?

How do I get access to the data?

What tools can/should I use?

How do I visualize the information?

Amazon Security Lake

ACCESS TYPES

Query access

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



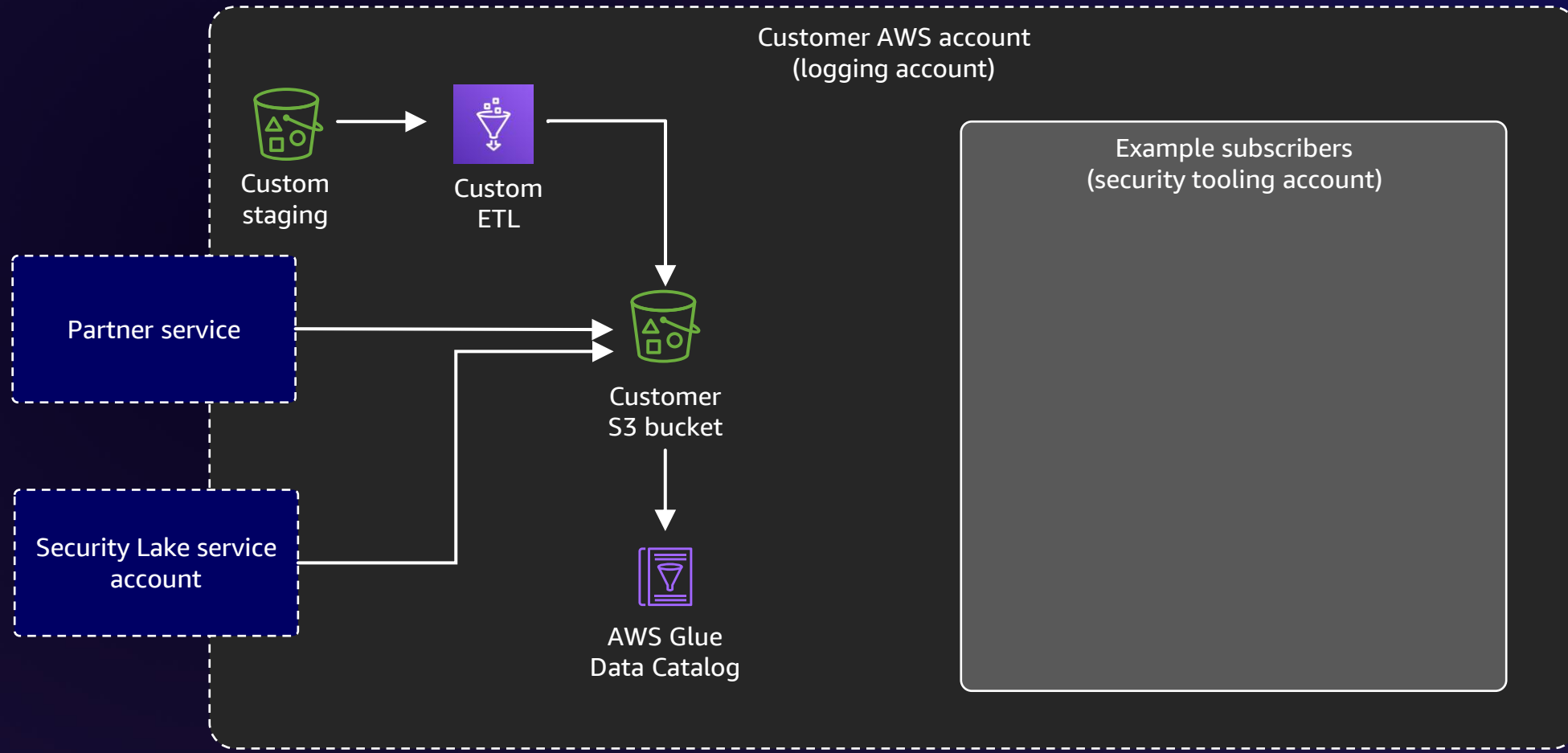
Data access

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



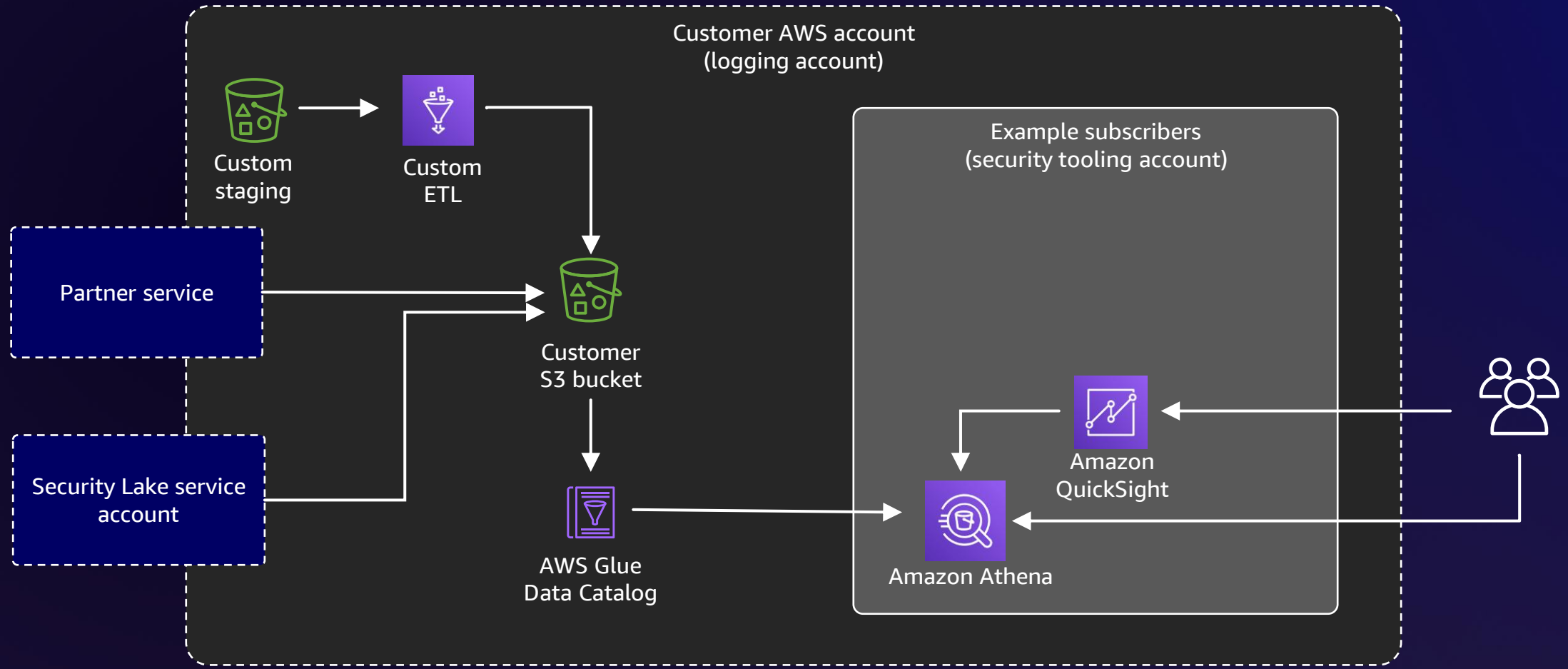
Amazon Security Lake

ARCHITECTURE OVERVIEW



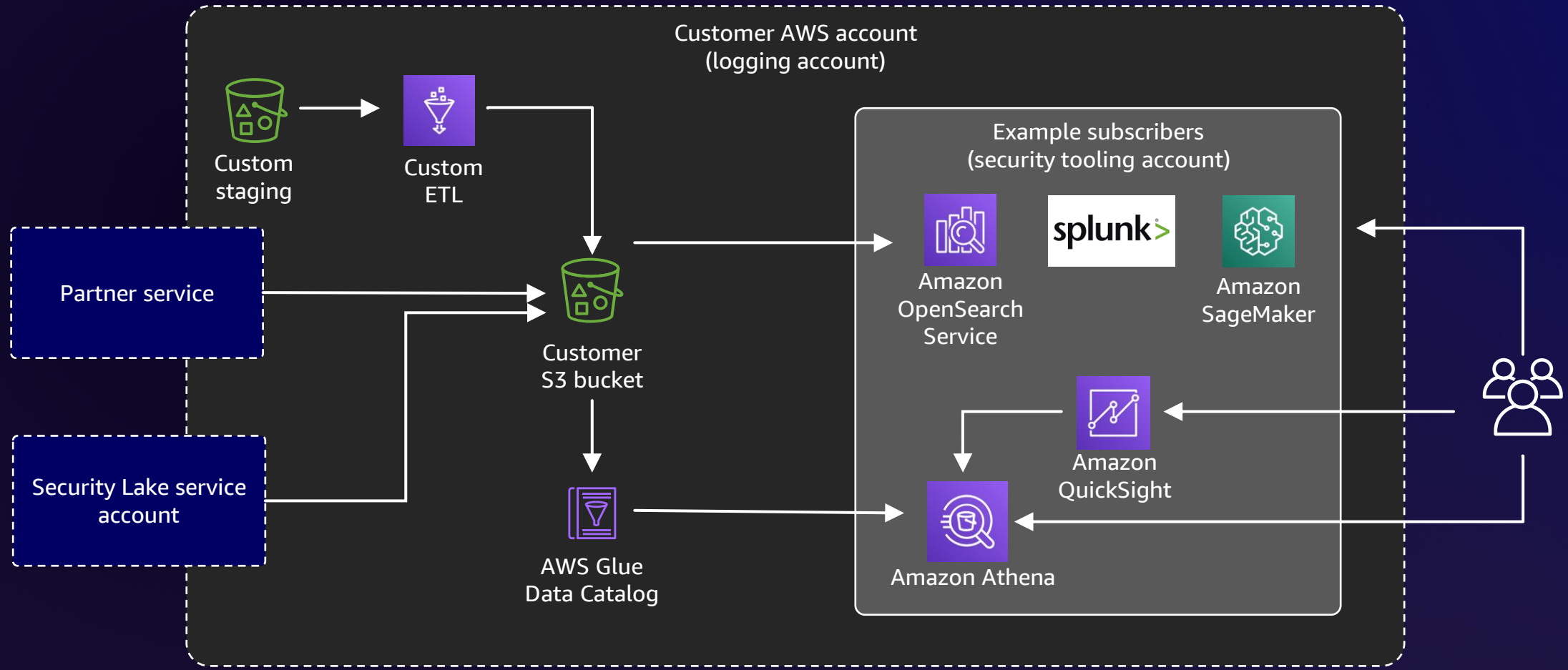
Amazon Security Lake

ARCHITECTURE OVERVIEW



Amazon Security Lake

ARCHITECTURE OVERVIEW



Directly querying your data

Data

Data source

AwsDataCatalog

Database

amazon_security_lake_glue_db_us_east_1

Tables and views

Filter tables and views

▼ Tables (5)

amazon_security_lake_table_us_east_1_cloud_trai

amazon_security_lake_table_us_east_1_myendpointprocessdata

amazon_security_lake_table_us_east_1_route53

amazon_security_lake_table_us_east_1_sh_findings

amazon_security_lake_table_us_east_1_vpc_flow

Amazon Athena > Query editor

Editor

Recent queries

Saved queries

Settings

Workgroup primary

>

Query 20 : X

Query 21 : X

+ ▼

```
1 SELECT start_time,
2     end_time,
3     src_endpoint.interface_uid,
4     connection_info.direction,
5     src_endpoint.ip,
6     dst_endpoint.ip,
7     src_endpoint.port,
8     dst_endpoint.port,
9     traffic.packets,
10    traffic.bytes
11 FROM "amazon_security_lake_glue_db_us_east_1".
12      "amazon_security_lake_table_us_east_1_vpc_flow"
13 WHERE ( src_endpoint.ip = '172.31.73.28' AND dst_endpoint.ip = '172.31.71.151' )
14        OR ( src_endpoint.ip = '172.31.71.151' AND dst_endpoint.ip = '172.31.73.28' )
15 ORDER BY start_time ASC
16 LIMIT 100
```

Partitioned :


Results (100+)

Copy Download results

Search rows

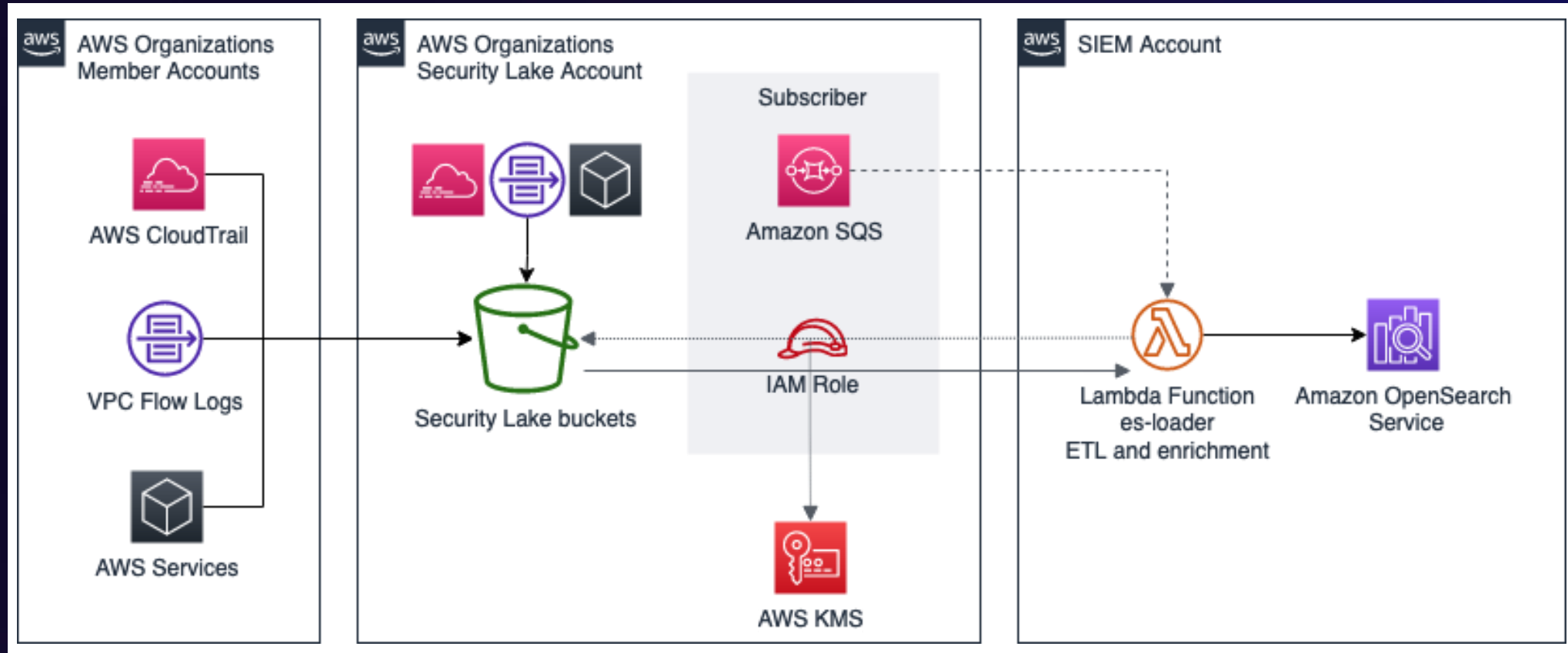
< 1 ... > ⚙

# ▼	start_time ▼	end_time ▼	interface_uid ▼	direction ▼	ip ▼	ip ▼	port ▼	port ▼
1	1669577323000	1669577325000	eni-0bd9d6778b3871f25	egress	172.31.71.151	172.31.73.28	40672	2049
2	1669577323000	1669577325000		ingress	172.31.73.28	172.31.71.151	2049	40672
3	1669577358000	1669577360000		ingress	172.31.71.151	172.31.73.28	40672	2049



© 2023, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Architecture example – OpenSearch Service



Amazon OpenSearch Service SIEM solution

(<https://github.com/aws-samples/siem-on-amazon-opensearch-service>)

Thank you!

Mark Keating

markkeat@amazon.com

 [linkedin.com/in/mkeat](https://www.linkedin.com/in/mkeat)

Keith Gilbert

gilbert@amazon.com



Please complete
the session survey
in the mobile app