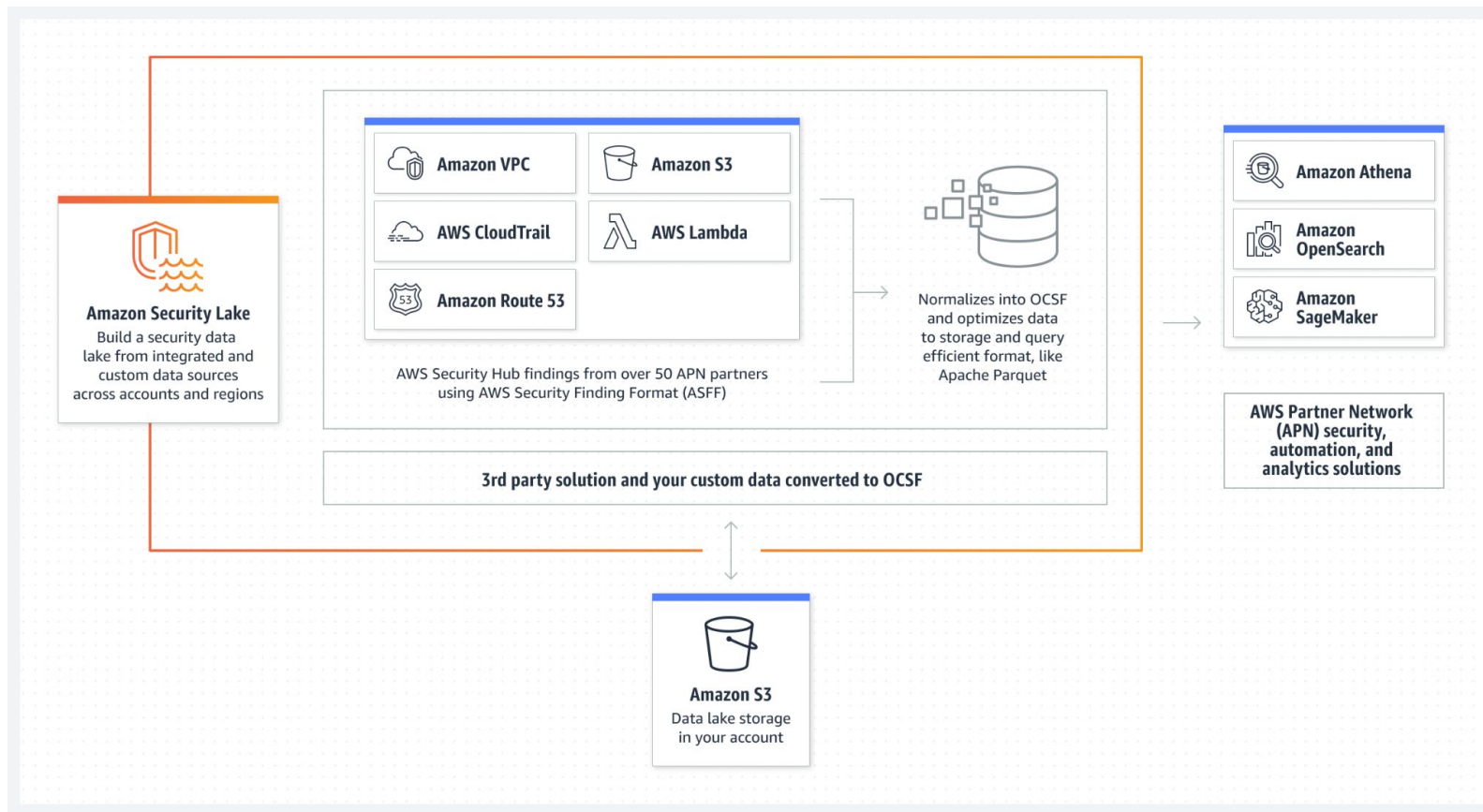


Presentación Técnica: Amazon Security Lake

Febrero 2023
Jorge Barreto

1. Security Lake - ¿Qué es?

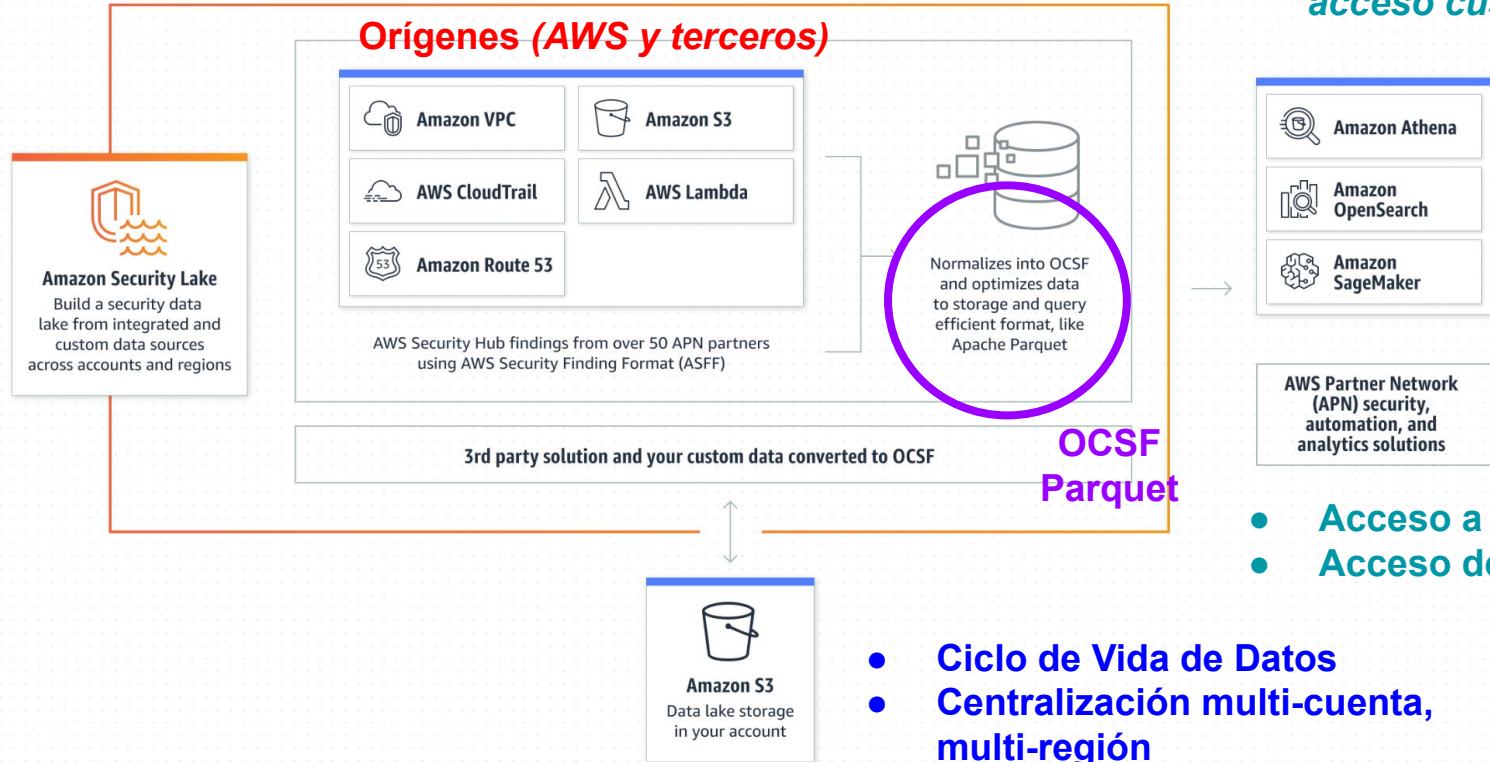




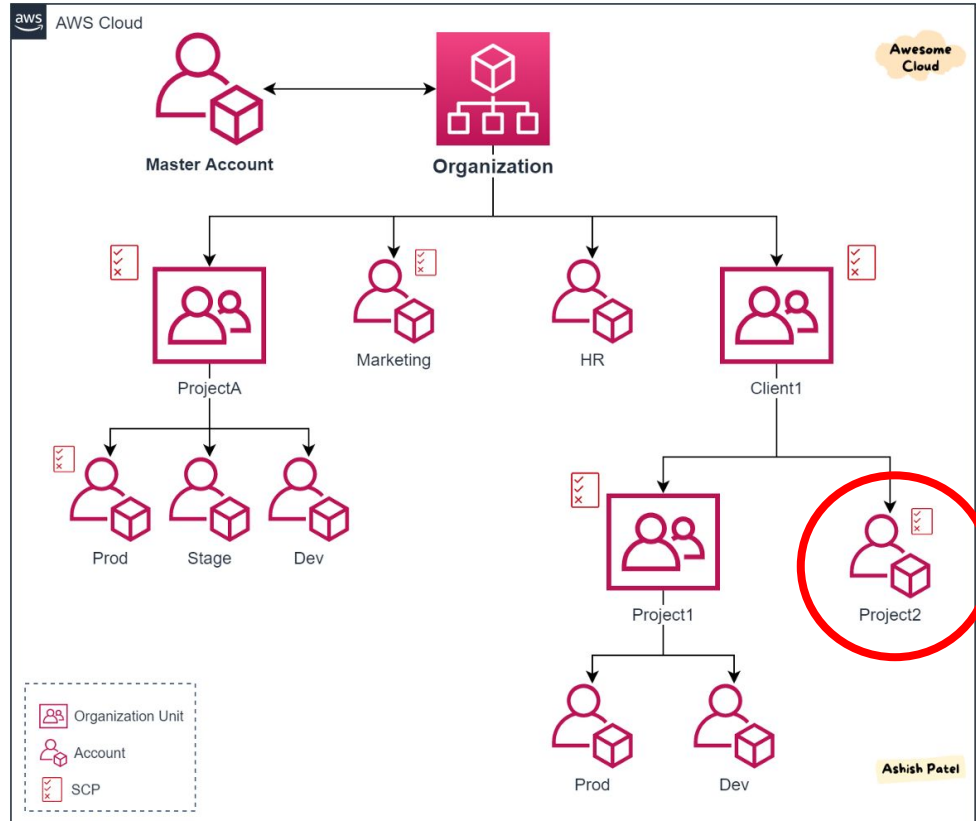
- **Variedad de fuentes de registro y eventos compatibles**, ingiere registros (de AWS y de terceros), independientemente de la fuente, puede acceder a ellos de forma centralizada y administrar su ciclo de vida.
- **Transformación y normalización de datos**, particiona automáticamente los datos entrantes de los servicios de AWS compatibles de forma nativa y los convierte a un formato Parquet eficiente en almacenamiento y consultas. También transforma los datos de los servicios de AWS con soporte nativo al esquema de código abierto Open Cybersecurity Schema Framework (OCSF).
- **Múltiples niveles de acceso para suscriptores**, Los suscriptores consumen datos almacenados en Security Lake. Puede elegir el nivel de acceso de un suscriptor a sus datos. Los suscriptores pueden consumir datos solo de las fuentes y en las regiones de AWS que usted especifique
- **Gestión de datos multicuenta y multiregión**, puede habilitar Security Lake de forma centralizada en todas las regiones donde está disponible y en varias cuentas de AWS. En Security Lake, también puede especificar una región acumulada para consolidar el registro de seguridad y los datos de eventos de varias regiones.
- **Configurable y personalizable**, puede especificar para qué orígenes, cuentas y regiones desea configurar la recopilación de registros. También puede especificar el nivel de acceso de un suscriptor al lago de datos.



Subscriptores (nivel de acceso custom)



2. Security Lake - Delegate Administration





3. Security Lake - Onboarding

Amazon Security Lake

Automatically centralize all
your security data with a few
clicks

Amazon Security Lake automatically centralizes security data from cloud, on-premises, and custom sources into a purpose-built data lake stored in your account. Security Lake makes it easier to analyze security data, so you can get a more complete understanding of your security across the entire organization and improve the protection of your workloads, applications, and data. Security Lake automatically gathers and manages all your security data across accounts and regions, and you can use your preferred analytics tools while retaining control and ownership of your security data. Security Lake has adopted the Open Cybersecurity Schema Framework (OCSF), an open industry standard, making it easier to normalize and combine security data from AWS and a broad range of enterprise security data sources. Now, your analysts and engineers can get broad visibility to investigate and respond to security events and improve your security across the cloud and on-premises.

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](#)



Step 1

Define collection objective

Step 2

Define target objective

Step 3

Review and create

Define collection objective [Info](#)

To enable Amazon Security Lake, first select which data sources, Regions, and accounts you want included in your data lake. Then, you can select a rollup Region and storage classes for your data.

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.

Log and event sources

CloudTrail



User Activity and API usage in AWS services.

VPC flow logs



Details about IP traffic to and from network interfaces in your VPC.

Route 53



DNS queries made by resources within your Amazon Virtual Private Cloud (Amazon VPC).

Security Hub findings



Amazon Security findings from Security Hub.



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

Select Regions

<input type="checkbox"/>	Region Name	Region ID
<input type="checkbox"/>	US East (Ohio)	us-east-2
<input type="checkbox"/>	US West (Oregon)	us-west-2
<input type="checkbox"/>	US East (N. Virginia)	us-east-1
<input type="checkbox"/>	Europe (Frankfurt)	eu-central-1
<input type="checkbox"/>	Asia Pacific (Sydney)	ap-southeast-2
<input type="checkbox"/>	Europe (Ireland)	eu-west-1
<input type="checkbox"/>	Asia Pacific (Tokyo)	ap-northeast-1



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



Execution role required

[Learn more](#)

The execution role authorizes Security Lake to update your Glue Resources. This role must be named:
AmazonSecurityLakeMetaStoreManager

Role ARN

arn:aws:iam::[REDACTED]:role/AmazonSecurityLakeMetaStoreManager

▼ Encryption Settings

- ☒ S3 Managed encryption - *recommended*
S3 will create and manage all encryption keys

Select accounts

Selected accounts will contribute their data to your data lake.



Execution role required

[Learn more](#)

The execution role authorizes Security Lake to update your Glue Resources. This role must be named:
AmazonSecurityLakeMetaStoreManager

Role ARN

arn:aws:iam::[redacted]:role/AmazonSecurityLakeMetaStoreManager

► Encryption Settings

Select accounts

Selected accounts will contribute their data to your data lake.



All accounts

Enable all accounts in my organization.



Specific accounts

Enable specific accounts.



This account

Only enable this account for now.



Enable all new accounts

Cancel

Next



Step 1

Define collection objective

Step 2

Define target objective


Step 3

Review and create

Define target objective [Info](#)

Amazon Security Lake ingests log and event sources from all of your enabled Regions for all accounts in your organization. All of the data can be stored in your preferred rollup Region, and accessed by services that you authorize.

Select Rollup 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. [Learn more](#) 

Add rollup 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. [Learn more](#) 

Add transition

Cancel

Previous

Next



Step 1

Define collection objective

Step 2

Define target objective

Step 3

Review and create

Define target objective [Info](#)

Amazon Security Lake ingests log and event sources from all of your enabled Regions for all accounts in your organization. All of the data can be stored in your preferred rollup Region, and accessed by services that you authorize.

Select Rollup 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. [Learn more](#) [🔗](#)

Rollup region

US East (N. Virginia) ▼

Contributing region

US East (Ohio) ▼

Contributing region replication role

ARN

Remove

US East (N. Virginia) ▼

US West (Oregon) ▼

Remove

Add rollup 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. [Learn more](#) [🔗](#)




Define target objective

Step 3


Review and create

Select Rollup 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. [Learn more](#) 

Add rollup 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. [Learn more](#) 

Choose storage class

Standard-IA



Retention period

30

Remove

One Zone-IA



90

Remove

Glacier Flexible Retrieval(formerly Glacier)



365

Remove

Add transition

Cancel

Previous

Next



Step 1

Define collection objective

Step 2

Define target objective

Step 3

Review and create

Review and create [Info](#)

Review your collection and target objectives below. Once enabled, Amazon Security Lake will begin ingesting your data. You can modify these selections at any time.

Step 1: Collection Objective

Edit

Log and event sources

Log and event sources
All log and event sources

Regions

Contributing Regions
Specify Regions

Regions
(7)

Encryption Settings
S3 Managed encryption

Accounts

[Summary](#)

Sources

Subscribers

Regions

Custom sources

Issues

Accounts

▼ **Settings**

General

Rollup region

Summary

Global Summary for Amazon Security Lake

Overview

Sources

28

Subscribers

+ Create

Region

7

Select Rollup Region

0

Subscribers

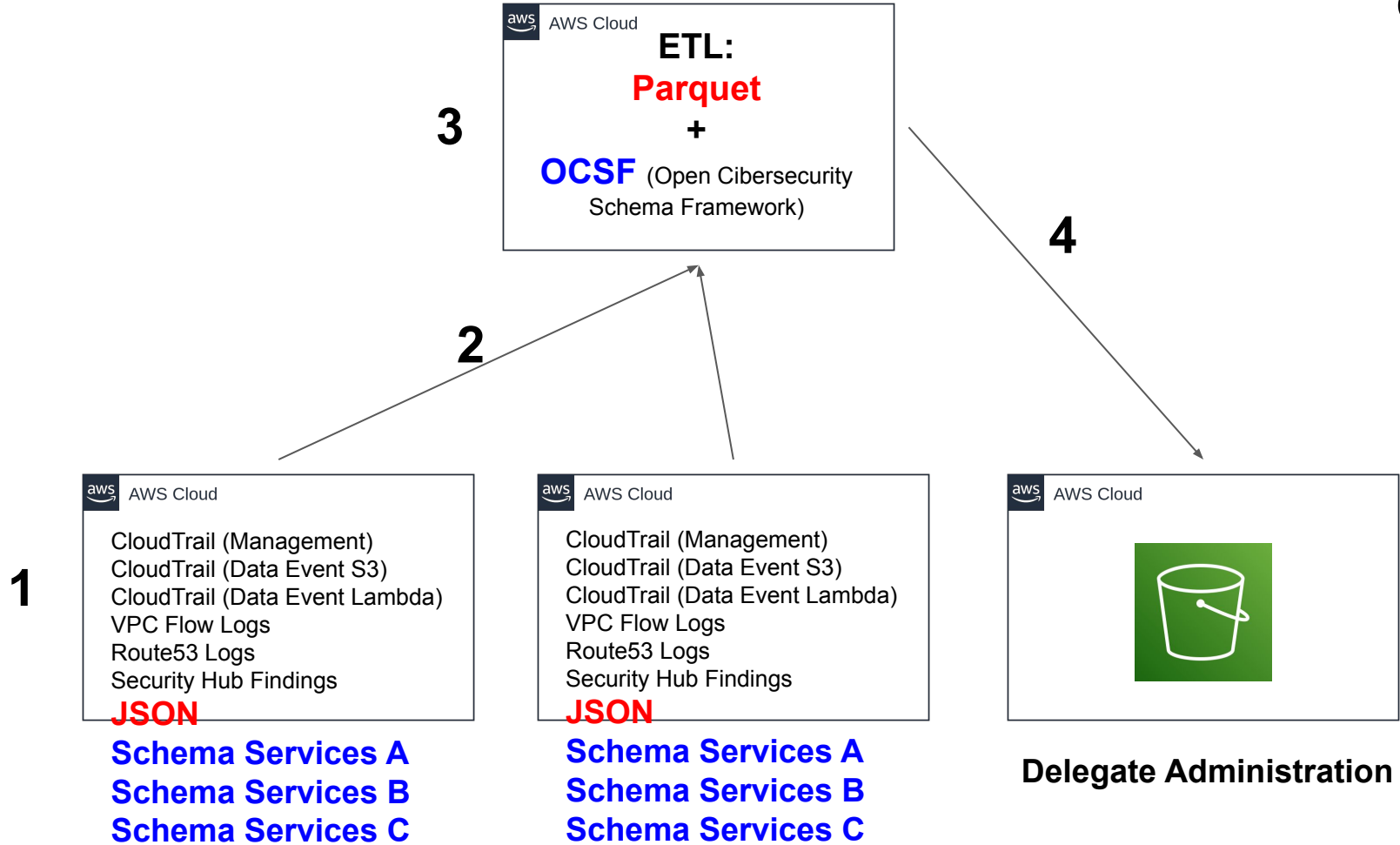
Subscribers are authorized to access data based on your specifications.

No Subscribers

No resources to display

Create subscriber

[View all subscribers](#)





4. Security Lake - Parquet Files

Security Lake - Parquet Files





Amazon S3



Buckets

Access Points

Object Lambda Access Points

Multi-Region Access Points

Batch Operations

IAM Access Analyzer for S3

Block Public Access settings for this account

Storage Lens

Dashboards

AWS Organizations settings

Feature spotlight **3**

AWS Marketplace for S3

Buckets (15) [Info](#)

Buckets are containers for data stored in S3. [Learn more](#)



Copy ARN

Empty

Delete

Create bucket

Find buckets by name

< 1 >



	Name ▲	AWS Region ▼	Access ▼	Creation date ▼
<input type="radio"/>	aws-security-data-lake-ap-northeast-1-qmjgcc2zolxrkvpd7jif3j0li	Asia Pacific (Tokyo) ap-northeast-1	Bucket and objects not public	February 21, 2023, 02:47:13 (UTC-05:00)
<input type="radio"/>	aws-security-data-lake-ap-southeast-2-dvrtcf3eyc5m5hybqc0tddqti	Asia Pacific (Sydney) ap-southeast-2	Bucket and objects not public	February 21, 2023, 02:47:26 (UTC-05:00)
<input type="radio"/>	aws-security-data-lake-eu-central-1-hyusef0bzkbpc0j011sqd9my12	EU (Frankfurt) eu-central-1	Bucket and objects not public	February 21, 2023, 02:47:54 (UTC-05:00)
<input type="radio"/>	aws-security-data-lake-eu-west-1-yjyrit86hgazkapdqdgtkbhgr5tvuy	EU (Ireland) eu-west-1	Bucket and objects not public	February 21, 2023, 02:47:47 (UTC-05:00)
<input type="radio"/>	aws-security-data-lake-us-east-1-zlr1w8gptmqx28jecmzetifuogln93	US East (N. Virginia) us-east-1	Bucket and objects not public	February 21, 2023, 02:45:57 (UTC-05:00)
<input type="radio"/>	aws-security-data-lake-us-east-2-pa1tnzkefbxboajeayk4iz5Gzjbivj	US East (Ohio) us-east-2	Bucket and objects not public	February 21, 2023, 02:48:02 (UTC-05:00)
<input type="radio"/>	aws-security-data-lake-us-west-2-epmexotbgnpwushrudvvbqnfwfumah	US West (Oregon) us-west-2	Bucket and objects not public	February 21, 2023, 02:47:40 (UTC-05:00)



Amazon S3



Buckets

Access Points

Object Lambda Access Points

Multi-Region Access Points

Batch Operations

IAM Access Analyzer for S3

Block Public Access settings for this account

Storage Lens

Dashboards

AWS Organizations settings

Feature spotlight 3

AWS Marketplace for S3

Amazon S3 > Buckets > aws-security-data-lake-us-east-1-zlrw8gptmqx28jecmzetifuogln93 > aws/

aws/

Copy S3 URI

Objects

Properties

Objects (3)

Objects are the fundamental entities stored in Amazon S3. You can use [Amazon S3 inventory](#) to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grant them permissions. [Learn more](#)

Copy S3 URI Copy URL Download Open Delete Actions Create folder Upload

Find objects by prefix

< 1 >

<input type="checkbox"/>	Name	Type	Last modified	Size	Storage class
<input type="checkbox"/>	CLOUD_TRAIL/	Folder	-	-	-
<input type="checkbox"/>	ROUTES3/	Folder	-	-	-
<input type="checkbox"/>	VPC_FLOW/	Folder	-	-	-



Amazon S3



Buckets

Access Points

Object Lambda Access Points

Multi-Region Access Points

Batch Operations

IAM Access Analyzer for S3

Block Public Access settings for this account

Storage Lens

Dashboards

AWS Organizations settings

Feature spotlight 3

AWS Marketplace for S3

Amazon S3 > Buckets > aws-security-data-lake-us-east-1-zlrw8gptmqx28jeczmetifuogln93 > aws/ > CLOUD_TRAIL/ > region=us-east-1/ > accountId=655635095766/ > eventHour=2023022107/

eventHour=2023022107/

Copy S3 URI

Objects

Properties

Objects (3)

Objects are the fundamental entities stored in Amazon S3. You can use [Amazon S3 Inventory](#) to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grant them permissions. [Learn more](#)



Copy S3 URI

Copy URL

Download

Open

Delete

Actions

Create folder

Upload

Find objects by prefix

< 1 > ⚙

<input type="checkbox"/>	Name	Type	Last modified	Size	Storage class
<input type="checkbox"/>	d6c3397b3477b6fcb7c81b1174bea8e9.gz.parquet	parquet	February 21, 2023, 02:53:26 (UTC-05:00)	35.0 KB	Standard
<input type="checkbox"/>	d8c3397fc407c29d77a9a4dca0433102.gz.parquet	parquet	February 21, 2023, 03:03:25 (UTC-05:00)	65.3 KB	Standard
<input type="checkbox"/>	e6c3397d79ab2d5fd49c37a737636a36.gz.parquet	parquet	February 21, 2023, 02:58:48 (UTC-05:00)	75.9 KB	Standard


```
>>> import pandas as pd
>>>
>>> df = pd.read_parquet('d6c3397b3477b6fcb7c81b1174bea8e9.gz.parquet')
>>>
>>> df.head(10)
```



	metadata	time	cloud	...	type_uid	type_name
unmapped						
0	{'product': {'version': '1.08', 'name': 'Cloud...	1676965656000	{'region': 'us-east-1', 'provider': 'AWS'}	...	500103	Cloud API: Operational
	[(eventCategory, Data), (sharedEventID, 3cb9d2...					
1	{'product': {'version': '1.08', 'name': 'Cloud...	1676965659000	{'region': 'us-east-1', 'provider': 'AWS'}	...	500103	Cloud API: Operational
	[(eventCategory, Management), (userIdentity_se...					
2	{'product': {'version': '1.08', 'name': 'Cloud...	1676965674000	{'region': 'us-east-1', 'provider': 'AWS'}	...	500103	Cloud API: Operational
	[(eventCategory, Data), (sharedEventID, ce39a9...					
3	{'product': {'version': '1.08', 'name': 'Cloud...	1676965676000	{'region': 'us-east-1', 'provider': 'AWS'}	...	500103	Cloud API: Operational
	[(eventCategory, Management), (userIdentity_se...					
4	{'product': {'version': '1.08', 'name': 'Cloud...	1676965685000	{'region': 'us-east-1', 'provider': 'AWS'}	...	500103	Cloud API: Operational
	[(eventCategory, Data), (sharedEventID, c4e6e1...					
5	{'product': {'version': '1.08', 'name': 'Cloud...	1676965690000	{'region': 'us-east-1', 'provider': 'AWS'}	...	500103	Cloud API: Operational
	[(eventCategory, Management), (responseElement...					
6	{'product': {'version': '1.08', 'name': 'Cloud...	1676965696000	{'region': 'us-east-1', 'provider': 'AWS'}	...	500103	Cloud API: Operational
	[(eventCategory, Management), (sharedEventID, ...					
7	{'product': {'version': '1.08', 'name': 'Cloud...	1676965696000	{'region': 'us-east-1', 'provider': 'AWS'}	...	500103	Cloud API: Operational
	[(eventCategory, Management), (sharedEventID, ...					
8	{'product': {'version': '1.08', 'name': 'Cloud...	1676965700000	{'region': 'us-east-1', 'provider': 'AWS'}	...	500103	Cloud API: Operational
	[(eventCategory, Data), (sharedEventID, e50c26...					
9	{'product': {'version': '1.08', 'name': 'Cloud...	1676965701000	{'region': 'us-east-1', 'provider': 'AWS'}	...	500103	Cloud API: Operational
	[(eventCategory, Data), (sharedEventID, 992d5f...					

[10 rows x 20 columns]

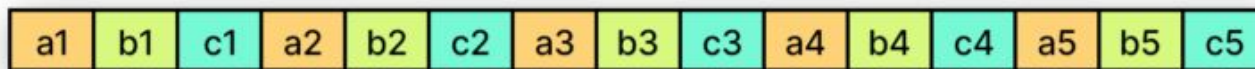
Security Lake - Parquet Files



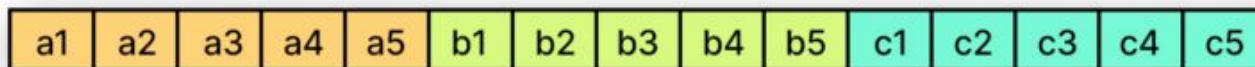
Logical table
representation

a	b	c
a1	b1	c1
a2	b2	c2
a3	b3	c3
a4	b4	c4
a5	b5	c5

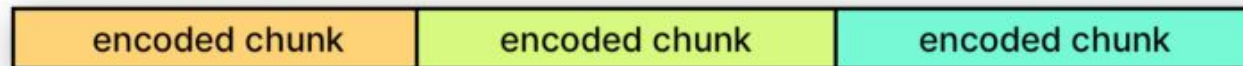
Row Layout



Column Layout



encoding



Security Lake - Parquet Files



Row Store

ProductID	OrderDate	Cost
310	20010701	2171.29
311	20010701	1912.15
312	20010702	2171.29
313	20010702	413.14

data page 1000

ProductID	OrderDate	Cost
314	20010701	333.42
315	20010701	1295.00
316	20010702	4233.14
317	20010702	641.22

data

Column Store

ProductID
310
311
312
313
314
315
316
317
318
319
320
321

data

OrderDate
20010701

20010702

20010703

20010704

data

Cost
2171.29
1912.15
2171.29
413.14
333.42
1295.00
4233.14
641.22
24.95
64.32
1111.25

data

Security Lake - Parquet Files

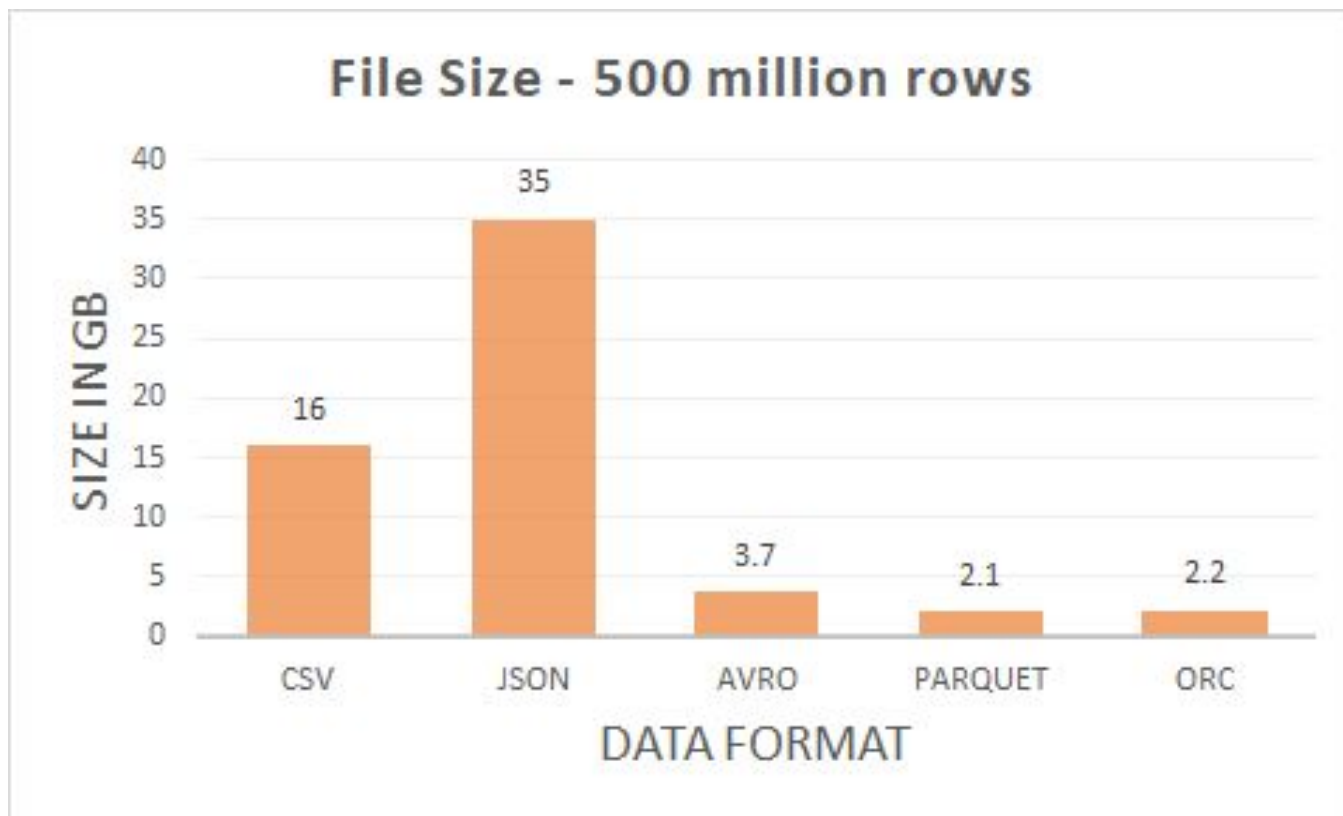


Spark Format Showdown		File Format		
		<u>CSV</u>	<u>JSON</u>	<u>Parquet</u>
A t t r i b u t e	Columnar	No	No	Yes
	Compressable	Yes	Yes	Yes
	Splittable	Yes*	Yes**	Yes
	Human Readable	Yes	Yes	No
	Nestable	No	Yes	Yes
	Complex Data Structures	No	Yes	Yes
	Default Schema: Named columns	Manual	Automatic (full read)	Automatic (instant)
	Default Schema: Data Types	Manual (full read)	Automatic (full read)	Automatic (instant)

Security Lake - Parquet Files



Security Lake - Parquet Files

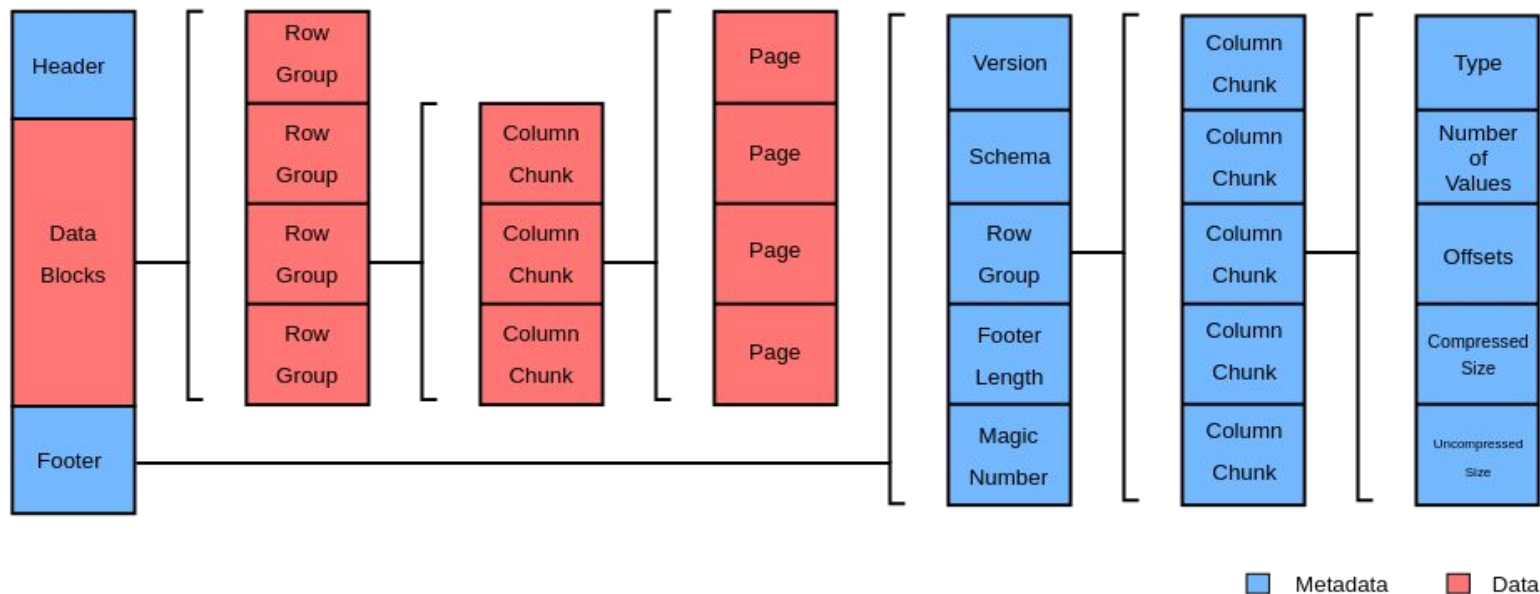


Security Lake - Parquet Files



- High Performance
- Efficient Compression
- Industry Standard
- Binary-Based Files Cannot Be Read by Humans

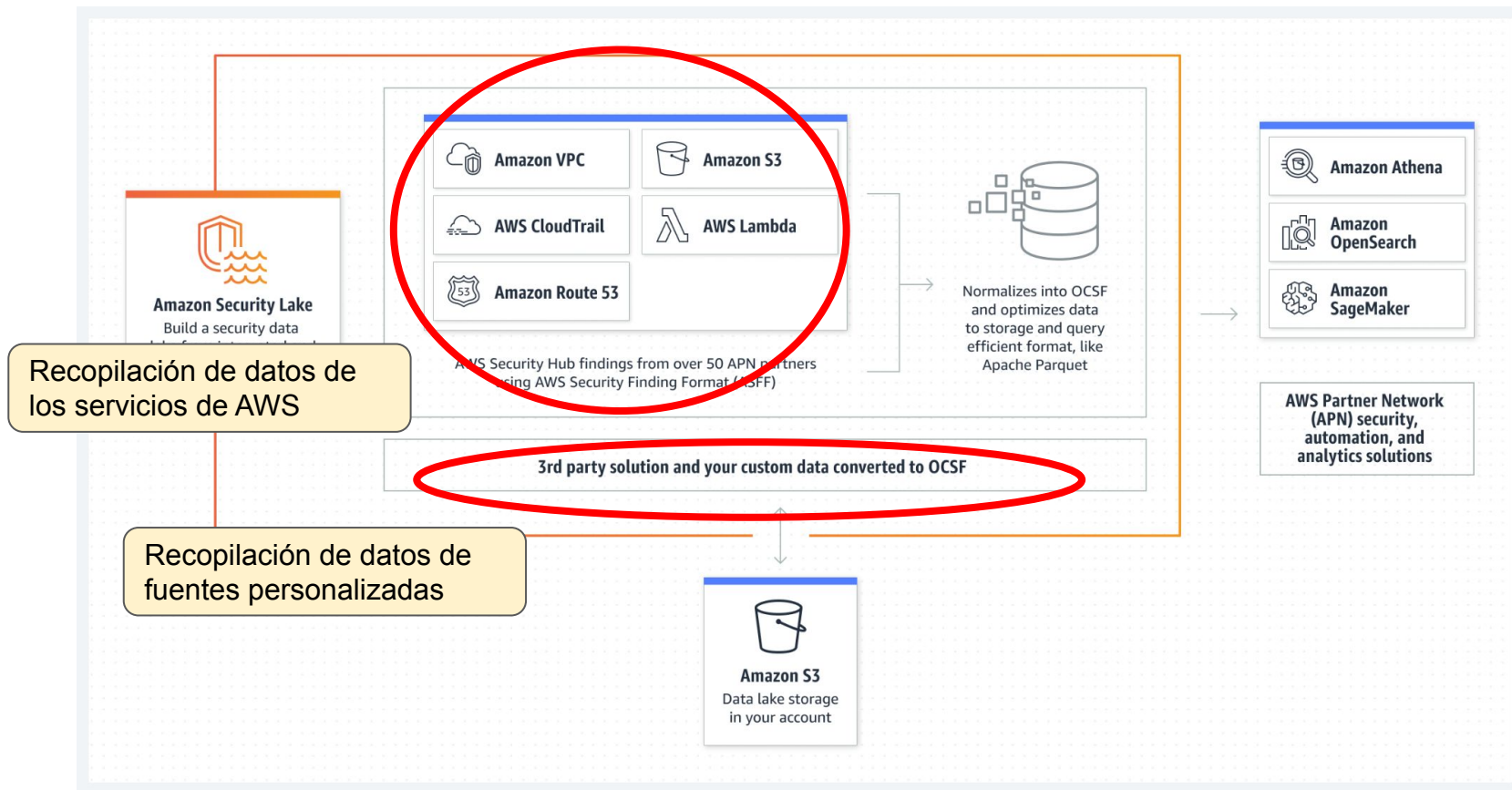
Security Lake - Parquet Files





5. Security Lake - Sources Management

5. Security Lake - Sources Management





Recopilación de datos de los servicios de AWS

- Administración de AWS CloudTrail y eventos de datos (S3, Lambda)
- Registros de consultas de resolución de Amazon Route 53
- Hallazgos del centro de seguridad de AWS
- Registros de flujo de Amazon Virtual Private Cloud (Amazon VPC)

Recopilación de datos de fuentes personalizadas

- Security Lake no administra sus eventos de CloudTrail ni afecta sus configuraciones de **CloudTrail** existentes.
- Security Lake no administra sus registros de **Route 53** ni afecta sus configuraciones de registro de consultas de resolución existentes.
- Cuando agrega hallazgos de **Security Hub** como fuente en Security Lake, Security Lake inmediatamente comienza a recopilar sus hallazgos directamente desde Security Hub a través de un flujo de eventos independiente y duplicado. Security Lake también transforma los hallazgos de ASFF en [Open Cybersecurity Schema Framework \(OCSF\)](#) (OCSF). Security Lake no administra los hallazgos de Security Hub ni afecta la configuración de Security Hub.
- Consume registros de **flujo de VPC** directamente desde la función Registros de flujo de VPC a través de un flujo independiente y duplicado de registros de flujo. Security Lake no administra sus registros de flujo ni afecta sus configuraciones de Amazon VPC.



6. Security Lake - Technical Detail


```
>>> import pandas as pd
>>>
>>> df = pd.read_parquet('d6c3397b3477b6fcb7c81b1174bea8e9.gz.parquet')
>>>
>>> df.head(10)
```



metadata	time	cloud ...	type_uid	type_name
----------	------	-----------	----------	-----------

unmapped

0	{'product': {'version': '1.08', 'name': 'Cloud...	1676965656000	{'region': 'us-east-1', 'provider': 'AWS'}	...	500103	Cloud API: Operational
	[(eventCategory, Data), (sharedEventID, 3cb9d2...					
1	{'product': {'version': '1.08', 'name': 'Cloud...	1676965659000	{'region': 'us-east-1', 'provider': 'AWS'}	...	500103	Cloud API: Operational
	[(eventCategory, Management), (userIdentity_se...					
2	{'product': {'version': '1.08', 'name': 'Cloud...	1676965674000	{'region': 'us-east-1', 'provider': 'AWS'}	...	500103	Cloud API: Operational
	[(eventCategory, Data), (sharedEventID, ce39a9...					
3	{'product': {'version': '1.08', 'name': 'Cloud...	1676965676000	{'region': 'us-east-1', 'provider': 'AWS'}	...	500103	Cloud API: Operational
	[(eventCategory, Management), (userIdentity_se...					
4	{'product': {'version': '1.08', 'name': 'Cloud...	1676965685000	{'region': 'us-east-1', 'provider': 'AWS'}	...	500103	Cloud API: Operational
	[(eventCategory, Data), (sharedEventID, c4e6e1...					
5	{'product': {'version': '1.08', 'name': 'Cloud...	1676965690000	{'region': 'us-east-1', 'provider': 'AWS'}	...	500103	Cloud API: Operational
	[(eventCategory, Management), (responseElement...					
6	{'product': {'version': '1.08', 'name': 'Cloud...	1676965696000	{'region': 'us-east-1', 'provider': 'AWS'}	...	500103	Cloud API: Operational
	[(eventCategory, Management), (sharedEventID, ...					
7	{'product': {'version': '1.08', 'name': 'Cloud...	1676965696000	{'region': 'us-east-1', 'provider': 'AWS'}	...	500103	Cloud API: Operational
	[(eventCategory, Management), (sharedEventID, ...					
8	{'product': {'version': '1.08', 'name': 'Cloud...	1676965700000	{'region': 'us-east-1', 'provider': 'AWS'}	...	500103	Cloud API: Operational
	[(eventCategory, Data), (sharedEventID, e50c26...					
9	{'product': {'version': '1.08', 'name': 'Cloud...	1676965701000	{'region': 'us-east-1', 'provider': 'AWS'}	...	500103	Cloud API: Operational
	[(eventCategory, Data), (sharedEventID, 992d5f...					

[10 rows x 20 columns]

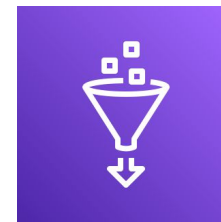
Security Lake - AWS Glue



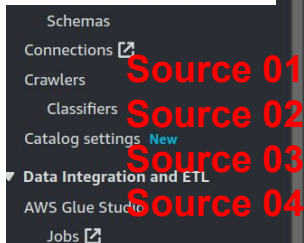
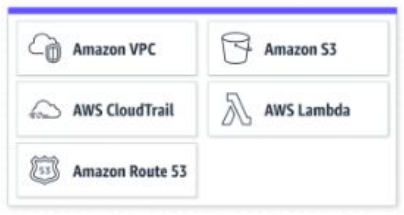
```
>>> import pandas as pd
>>>
>>> df = pd.read_parquet('d6c3397b3477b6fcb7c81b1174bea8e9.gz.parquet')
>>>
>>> df.head(10)
```

	metadata	time	cloud	type_name	unmapped
0	{'product': {'version': '1.08', 'name': 'Cloud...	1676965656000	{'region': 'us-east-1', 'provider': 'AWS'}	Cloud API: Operational	((eventCategory, Data), (sharedEventID, 3cb9d2...
1	{'product': {'version': '1.08', 'name': 'Cloud...	16769656569000	{'region': 'us-east-1', 'provider': 'AWS'}	Cloud API: Operational	((eventCategory, Management), (userIdentity_se...
2	{'product': {'version': '1.08', 'name': 'Cloud...	16769656574000	{'region': 'us-east-1', 'provider': 'AWS'}	Cloud API: Operational	((eventCategory, Data), (sharedEventID, ce39a9...
3	{'product': {'version': '1.08', 'name': 'Cloud...	16769656576000	{'region': 'us-east-1', 'provider': 'AWS'}	Cloud API: Operational	((eventCategory, Management), (userIdentity_se...
4	{'product': {'version': '1.08', 'name': 'Cloud...	16769656585000	{'region': 'us-east-1', 'provider': 'AWS'}	Cloud API: Operational	((eventCategory, Data), (sharedEventID, c4e6e1...
5	{'product': {'version': '1.08', 'name': 'Cloud...	16769656590000	{'region': 'us-east-1', 'provider': 'AWS'}	Cloud API: Operational	((eventCategory, Management),
6	{'product': {'version': '1.08', 'name': 'Cloud...	16769656596000	{'region': 'us-east-1', 'provider': 'AWS'}	Cloud API: Operational	((eventCategory, Management), (sharedEventID, ...
7	{'product': {'version': '1.08', 'name': 'Cloud...	16769656596000	{'region': 'us-east-1', 'provider': 'AWS'}	Cloud API: Operational	((eventCategory, Management), (sharedEventID, ...
8	{'product': {'version': '1.08', 'name': 'Cloud...	16769657000000	{'region': 'us-east-1', 'provider': 'AWS'}	Cloud API: Operational	((eventCategory, Data), (sharedEventID, e50c26...
9	{'product': {'version': '1.08', 'name': 'Cloud...	1676965701000	{'region': 'us-east-1', 'provider': 'AWS'}	Cloud API: Operational	((eventCategory, Data), (sharedEventID, 992d5f...

[10 rows x 20 columns]



Glue



Source 01
Source 02
Source 03
Source 04

AWS Glue > Tables

Tables

A table is the metadata definition that represents your data, including its schema. A table can be used as a source or target in a job definition.

Tables (23) Last updated (UTC) February 21, 2023 at 14:15:20 [Refresh] [Delete] [Data quality] [Add tables using crawler] [Add table]

View and manage all available tables.

Filter tables

<input type="checkbox"/>	Name	Database	Location	Classification	Deprecated	View data
<input type="checkbox"/>	amazon_security_lake_tal	amazon_security_lake_glu	s3://aws-security-data-lak	-	-	Table data
<input type="checkbox"/>	amazon_security_lake_tal	amazon_security_lake_glu	s3://aws-security-data-lak	-	-	Table data
<input type="checkbox"/>	amazon_security_lake_tal	amazon_security_lake_glu	s3://aws-security-data-lak	-	-	Table data
<input type="checkbox"/>	amazon_security_lake_tal	amazon_security_lake_glu	s3://aws-security-data-lak	-	-	Table data

Security Lake - AWS Glue

Source 01

Open
Cybersecurity
Schema
Framework
(OCSF)

#	Column name	Data type
1	metadata	struct
2	cloud	struct
3	src_endpoint	struct
4	time	bigint
5	query	struct
6	rcode	string
7	answers	array
8	connection_info	struct
9	dst_endpoint	struct
10	severity_id	int
11	severity	string
12	class_name	string
13	class_uid	int
14	category_name	string
15	category_uid	int
16	rcode_id	int
17	activity_id	int
18	activity_name	string
19	type_name	string
20	type_uid	int

Schema

Partitions

Indexes

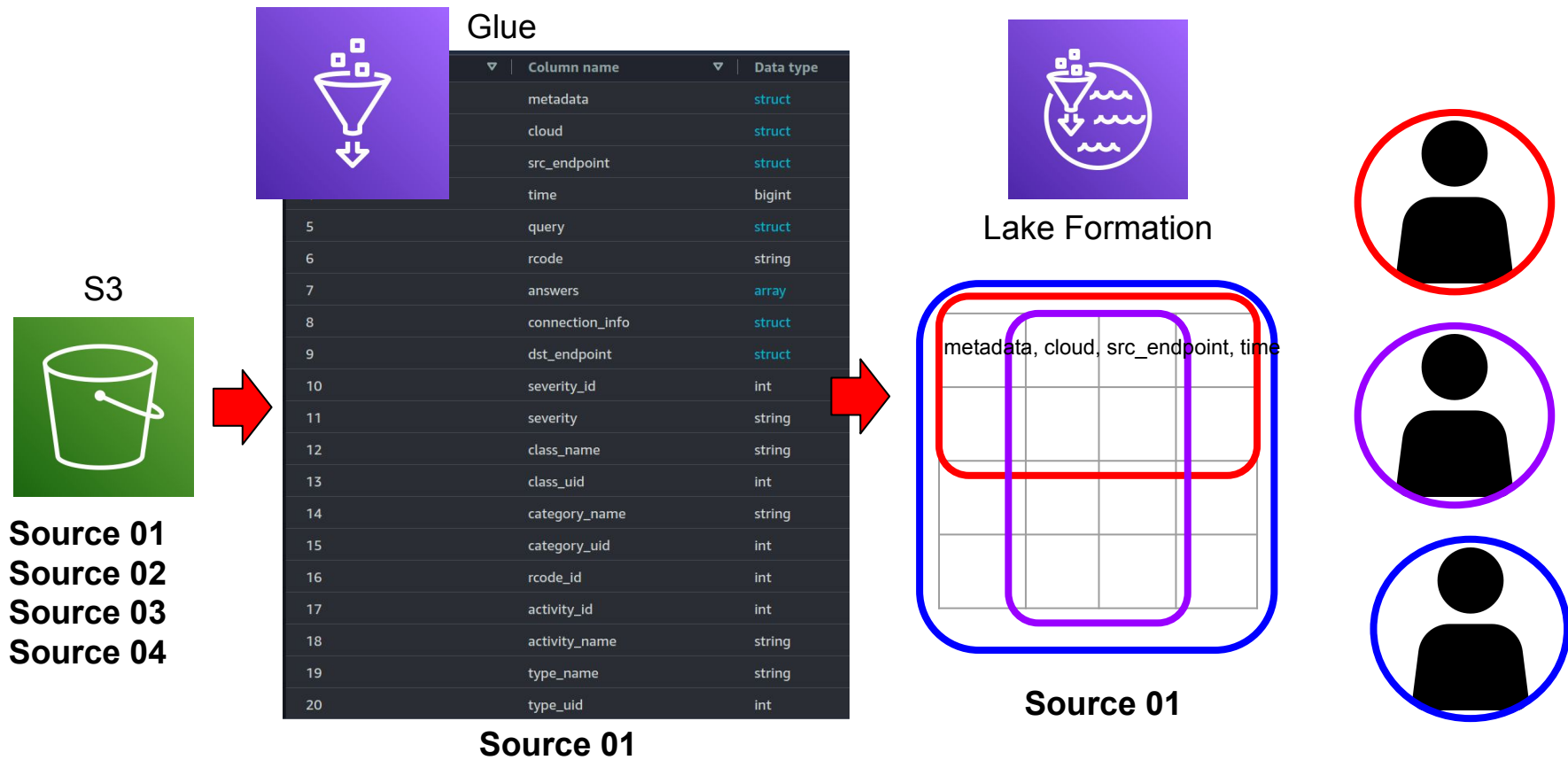
Partitions

Filter partitions

	region	accountid	eventhour
<input type="radio"/>	us-east-1		2023022111
<input type="radio"/>	us-east-1		2023022110
<input type="radio"/>	us-east-1		2023022109
<input type="radio"/>	us-east-1		2023022107
<input type="radio"/>	us-east-1		2023022114
<input type="radio"/>	us-east-1		2023022112
<input type="radio"/>	us-east-1		2023022114
<input type="radio"/>	us-east-1		2023022113
<input type="radio"/>	us-east-1		2023022108
<input type="radio"/>	us-east-1		2023022109
<input type="radio"/>	us-east-1		2023022111
<input type="radio"/>	us-east-1		2023022113
<input type="radio"/>	us-east-1		2023022112
<input type="radio"/>	us-east-1		2023022108
<input type="radio"/>	us-east-1		2023022107
<input type="radio"/>	us-east-1		2023022110



Security Lake - AWS LakeFormation





CloudTrail (Management)

CloudTrail (Data Event S3)

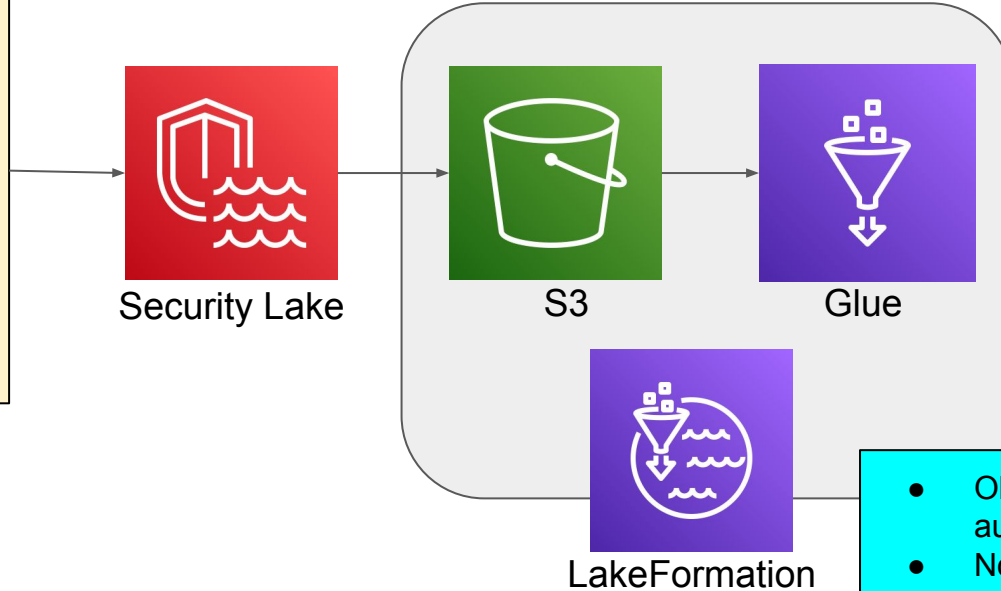
CloudTrail (Data Event Lambda)

VPC Flow Logs

Route53 Logs

Security Hub Findings

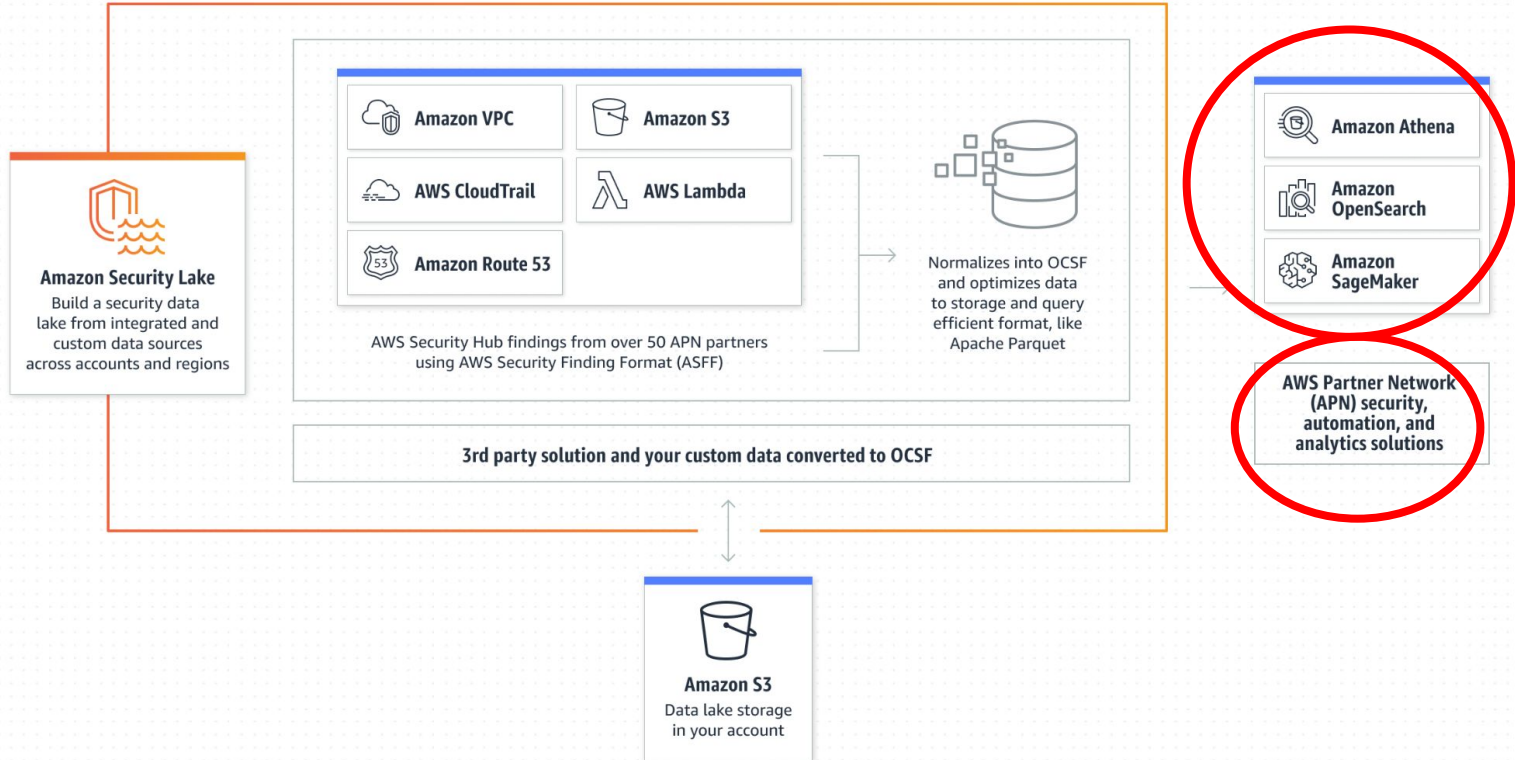
- GuardDuty
- Macie
- Inspector
- Otros



- Obtención de datos automáticos
- Normalización (OCSF y Formato Parquet)
- Implementación de buenas prácticas de Analítica
- Tablas con Particiones
- Seguridad en el acceso a los datos
- Serverless/ Proceso escalable



7. **Security Lake** - Subscriber Management



Security Lake - Amazon Athena



```
SELECT
    time,
    api.service.name,
    api.operation,
    api.response.error,
    api.response.message,
    unmapped['responseElements'],
    cloud.region,
    identity.user.uuid,
    src_endpoint.ip,
    http_request.user_agent
FROM
    "amazon_security_lake_glue_db_us_east_1"."amazon_security_lake_table_us_east_1_c
loud_trail"
```



Data



Data source

AwsDataCatalog

Database

amazon_security_lake_glue_db_us_east_1

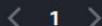
Tables and views

Create



Filter tables and views

Tables (4)



amazon_security_lake_table_us_east_1_cloud_trail

Partitioned

amazon_security_lake_table_us_east_1_route53

Partitioned

amazon_security_lake_table_us_east_1_sh_findings

Partitioned

amazon_security_lake_table_us_east_1_vpc_flow

Partitioned

Query 1

```
1 SELECT
2     time,
3     api.service.name,
4     api.operation,
5     api.response.error,
6     api.response.message,
7     unmapped['responseElements'],
8     cloud.region,
9     identity.user.uuid,
10    src_endpoint.ip,
11    http_request.user_agent
12 FROM "amazon_security_lake_glue_db_us_east_1"."amazon_security_lake_table_us_east_1_cloud_trail"
```

SQL Ln 2, Col 13



Run again

Explain

Cancel

Clear

Create

Reuse query results
*Athena engine version 3 only

Query results

Query stats

Completed

Time in queue: 131 ms

Run time: 3.53 sec

Data scanned: 9.66 MB

Results (100+)

Copy

Download results

Search rows

< 1 ... >

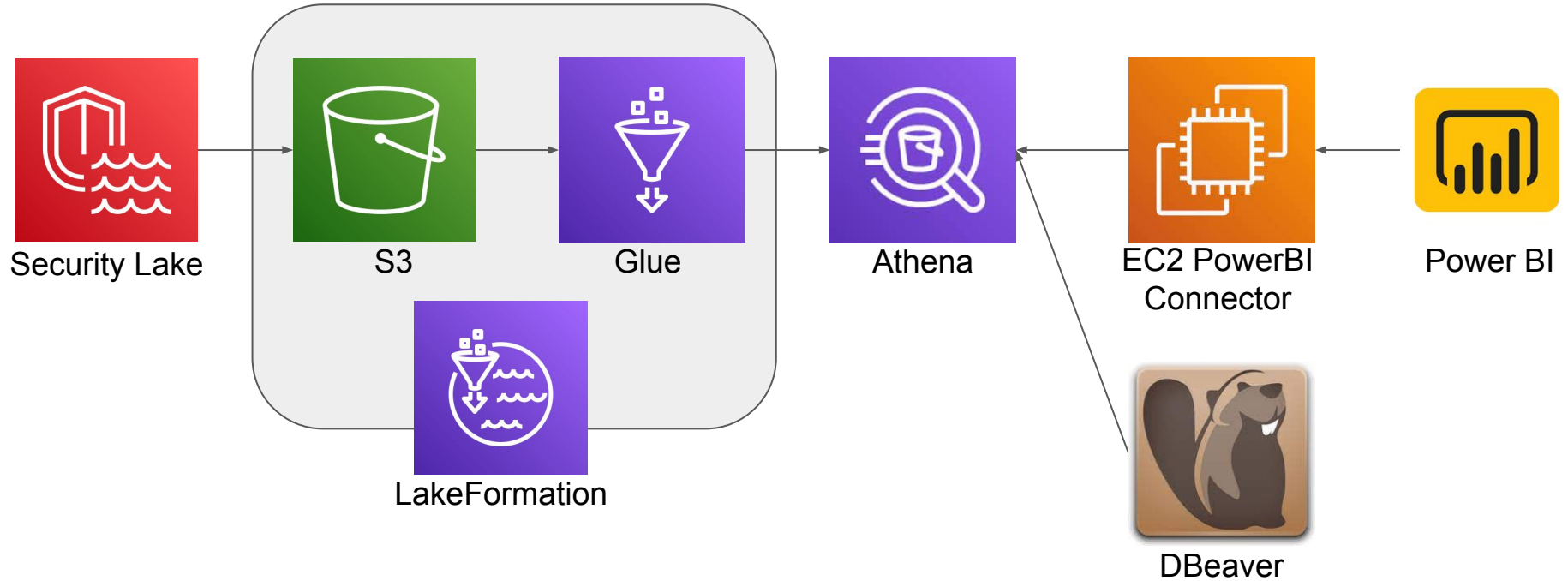




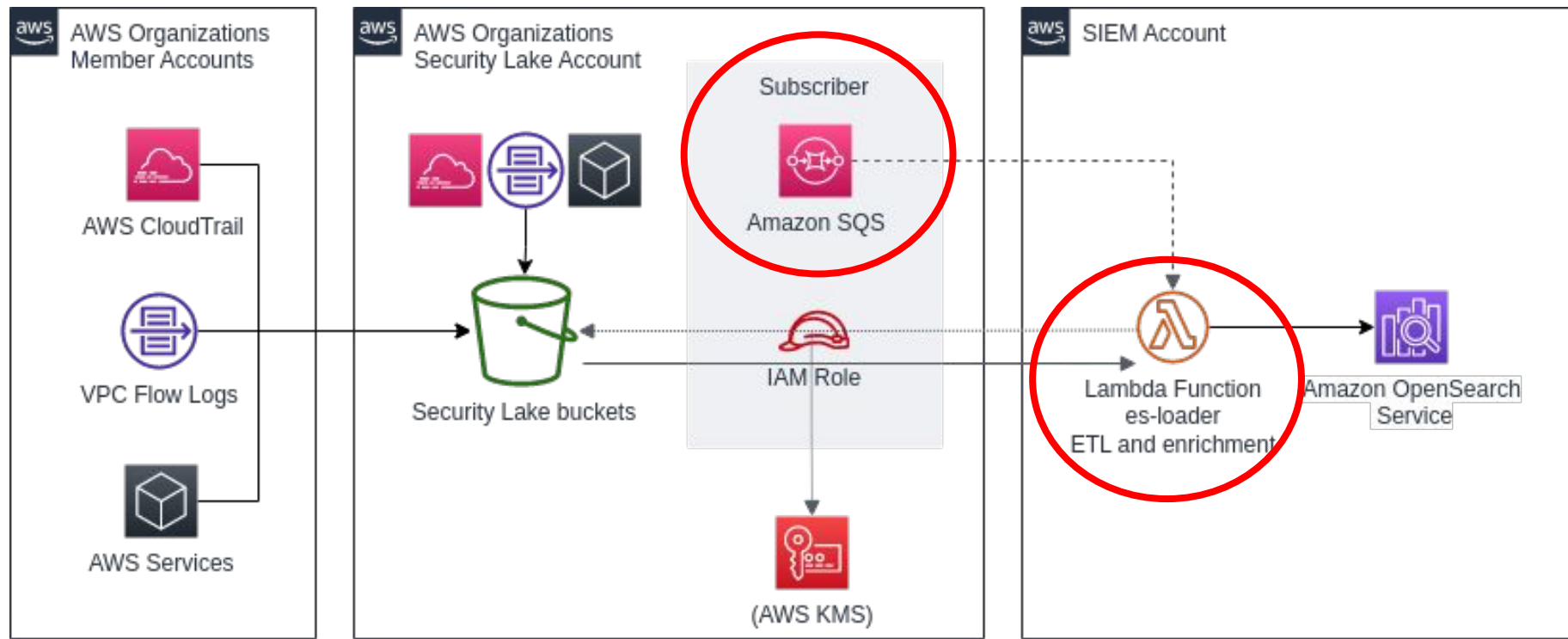
Q Search rows

< 1 ... > ⚙

# ▾	time ▾	name ▾	operation ▾	error ▾
43	1677007601000	s3.amazonaws.com	GetBucketAcl	
44	1677007602000	s3.amazonaws.com	GetBucketAcl	
45	1677007618000	s3.amazonaws.com	GetBucketAcl	
46	1677007657000	s3.amazonaws.com	GetBucketAcl	
47	1677007657000	s3.amazonaws.com	GetBucketAcl	
48	1677007663000	s3.amazonaws.com	GetBucketAcl	
49	1677007663000	s3.amazonaws.com	GetBucketAcl	
50	1677007663000	s3.amazonaws.com	PutObject	
51	1677007663000	s3.amazonaws.com	PutObject	
52	1677007668000	s3.amazonaws.com	GetBucketAcl	
53	1677007668000	s3.amazonaws.com	PutObject	
54	1677007669000	s3.amazonaws.com	GetBucketAcl	
55	1677007669000	s3.amazonaws.com	PutObject	
56	1677007672000	s3.amazonaws.com	PutObject	



Security Lake - Amazon OpenSearch



<https://github.com/aws-samples/siem-on-amazon-opensearch-service/blob/main/docs/securitylake.md>

<https://docs.aws.amazon.com/opensearch-service/latest/developerguide/integrations.html>



8. Security Lake - Pricing



Este de EE. UU. (Norte de Virginia)

Este de EE. UU. (Ohio)

Oeste de EE. UU. (Oregón)

Europa (Irlanda)

Europa (Fráncfort)

Asia-Pacífico (Tokio)

Asia-Pacífico (Sídney)

Región

Este de EE. UU. (Norte de Virginia)

Registros de CloudTrail

0,75 USD por GB

Otros registros

Primero

10

TB

0,25 USD por GB

Siguiente

20

TB

0,15 USD por GB

Siguiente

20

TB

0,075 USD por GB

Más de

50

TB

0,05 USD por GB

Normalización

0,035 USD por GB



CloudTrail (Management)

CloudTrail (Data Event S3)

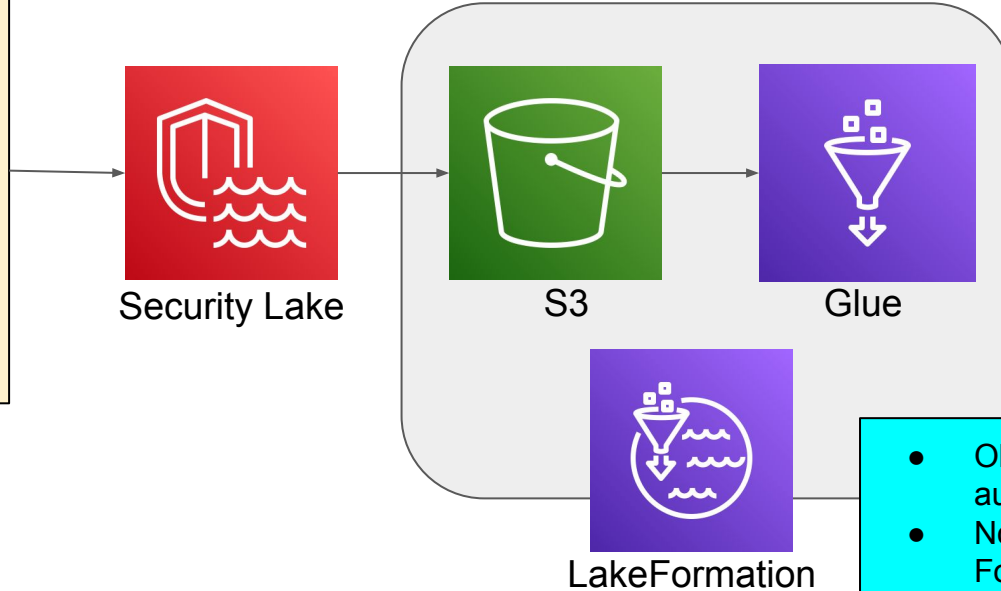
CloudTrail (Data Event Lambda)

VPC Flow Logs

Route53 Logs

Security Hub Findings

- GuardDuty
- Macie
- Inspector
- Otros



- Obtención de datos automáticos
- Normalización (OCSF y Formato Parquet)
- Implementación de buenas prácticas de Analítica
- Tablas con Particiones
- Seguridad en el acceso a los datos
- Serverless/ Proceso escalable
- Bajo Costo

The background is a dark blue gradient with intricate, glowing light blue circuit-like patterns. On the right side, there is a large, circular, futuristic interface element resembling a radar or a data display. In the center of this circle is a glowing, pixelated cloud shape. The text "¡Gracias!" is written in a clean, white, sans-serif font, positioned in the middle of the image, overlapping the circular interface and the cloud.

¡Gracias!

Febrero 2023
Jorge Barreto