aws

COMMUNITY DAY

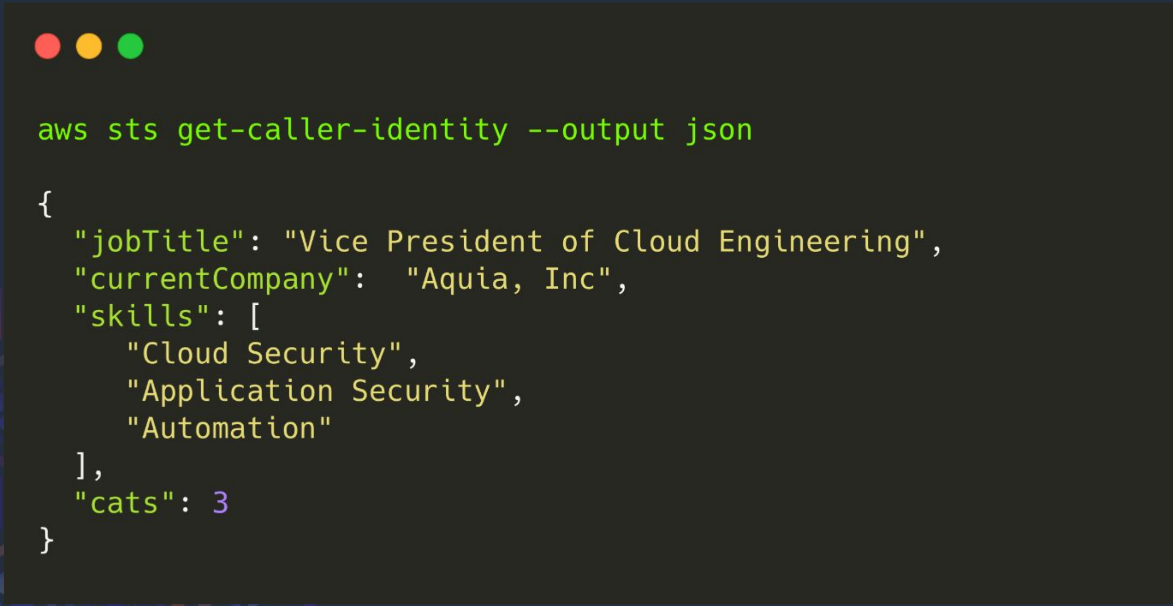
MIDWEST | OHIO

COMMUNITY DAY

Exploring Amazon Security Lake!!!!

Dakota Riley | Aquia, Inc

COMMUNITY DAY



```
aws sts get-caller-identity --output json

{
  "jobTitle": "Vice President of Cloud Engineering",
  "currentCompany":  "Aquia, Inc",
  "skills": [
     "Cloud Security",
     "Application Security",
     "Automation"
  ],
  "cats": 3
}
```

AWS community builders

Aq

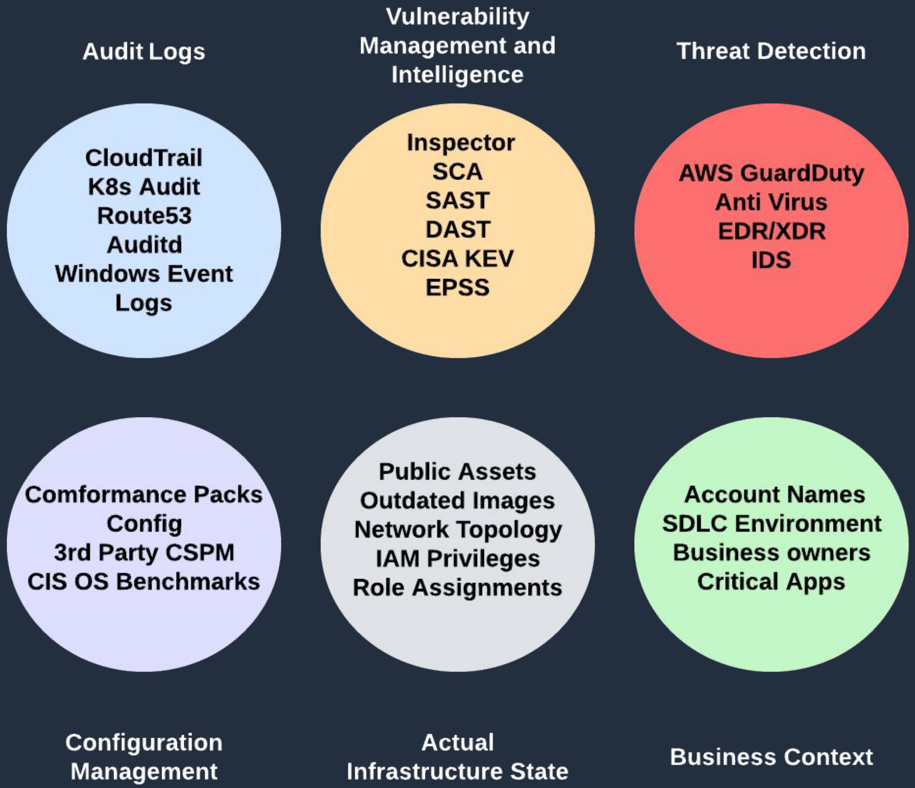
Agenda

- Overview
- Security Data Lakes and Amazon Security Lake
- OCSF
- First Steps
- Jupyter Notebook Demo

Security is a data problem…..

aws

COMMUNITY DAY



Audit Logs

CloudTrail
K8s Audit
Route53
Auditd
Windows Event Logs

Vulnerability Management and Intelligence

Inspector
SCA
SAST
DAST
CISA KEV
EPSS

Threat Detection

AWS GuardDuty
Anti Virus
EDR/XDR
IDS

Configuration Management

Comformance Packs
Config
3rd Party CSPM
CIS OS Benchmarks

Actual Infrastructure State

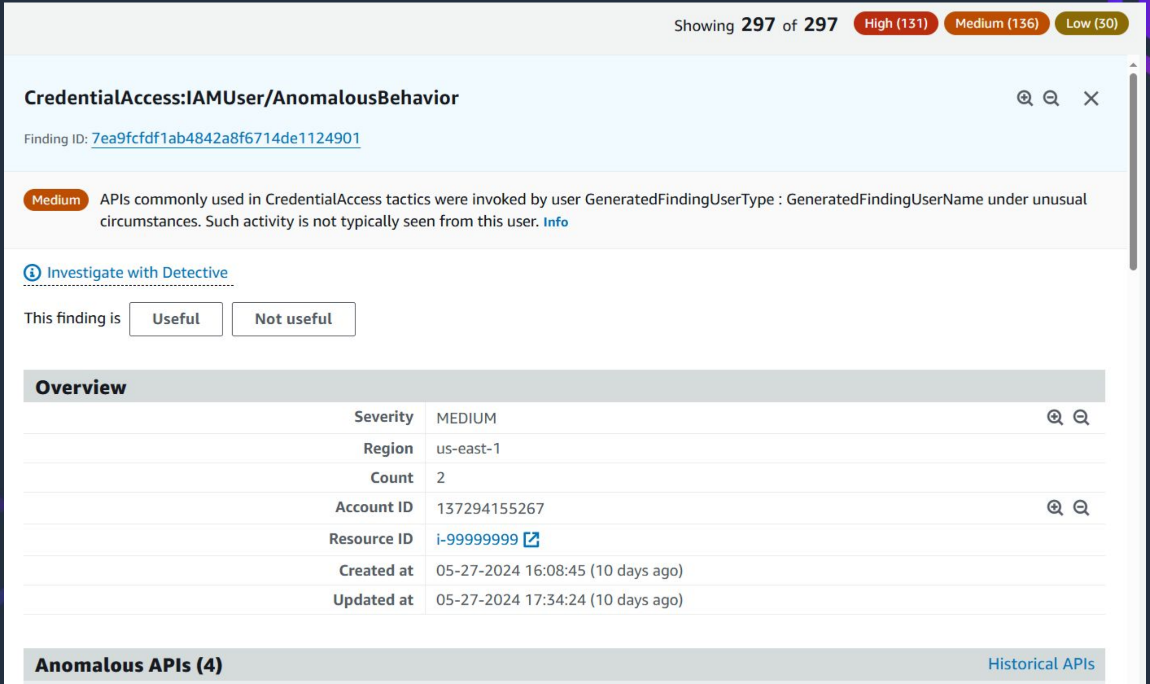
Public Assets
Outdated Images
Network Topology
IAM Privileges
Role Assignments

Business Context

Account Names
SDLC Environment
Business owners
Critical Apps

aws

COMMUNITY DAY



Showing **297** of **297** High (131) Medium (136) Low (30)

CredentialAccess:IAMUser/AnomalousBehavior

Finding ID: 7ea9fcfdf1ab4842a8f6714de1124901

Medium APIs commonly used in CredentialAccess tactics were invoked by user GeneratedFindingUserType : GeneratedFindingUserName under unusual circumstances. Such activity is not typically seen from this user. Info

Overview

Severity	MEDIUM
Region	us-east-1
Count	2
Account ID	137294155267
Resource ID	i-99999999
Created at	05-27-2024 16:08:45 (10 days ago)
Updated at	05-27-2024 17:34:24 (10 days ago)

Anomalous APIs (4) Historical APIs

aws

COMMUNITY DAY

Supply Chain Compromise

Development Team accidentally installs a **malicious PyPI Package**

Initial Access

Credentials on Developer workstation

Malicious entity discovers **~/aws/config** file with existing AWS credentials

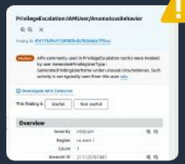
Credential Access

AWS Identity Enumeration and Access

Malicious entity attempts lateral movement via APIs

Lateral Movement

GuardDuty Finding triggered



PrivilegeEscalation:IAMUser/AnomalousBehavior

Finding ID: [illegible]

Medium APIs commonly used in PrivilegeEscalation tactics were invoked by user GeneratedFindingUserType : GeneratedFindingUserName under unusual circumstances. Such activity is not typically seen from this user. Info

Investigate with Detective

This finding is Useful Not useful

Overview

Severity	MEDIUM
Region	us-east-1
Count	1
Account ID	[illegible]

PrivilegeEscalation: AnomalousBehvaior GuardDuty Finding triggered by malicious entity

GuardDuty Alert

1. GuardDuty Finding(s)
2. CloudTrail
3. AWS Account Business Context
4. Developer and User Identity Information
5. Company Asset Information
6. OS Logs - developer endpoint

aws

COMMUNITY DAY

Security Data Lake

It is:

Cheap storage for (security) data with varying use cases!

Alternative to sending ALL data to SIEM

Staging point for different tools!

Break down data silos across your security org!

It isn't:

Replacement for SIEM or other security tools

Magic fix to your security org problems

Easy or free

aws

COMMUNITY DAY

Enter Amazon Security Lake!

S3 Backed Data lake

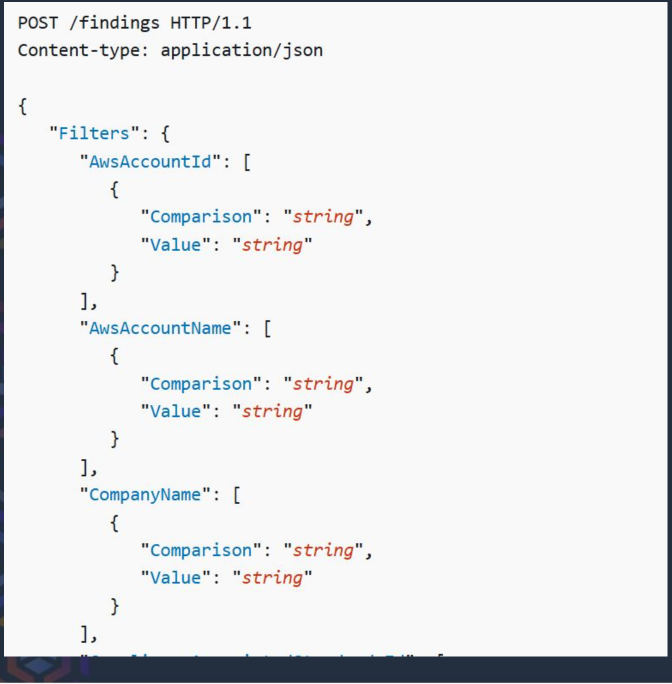
OOB Integrations with AWS and Third Party Security Services

OCSF and Parquet transformation!

aws

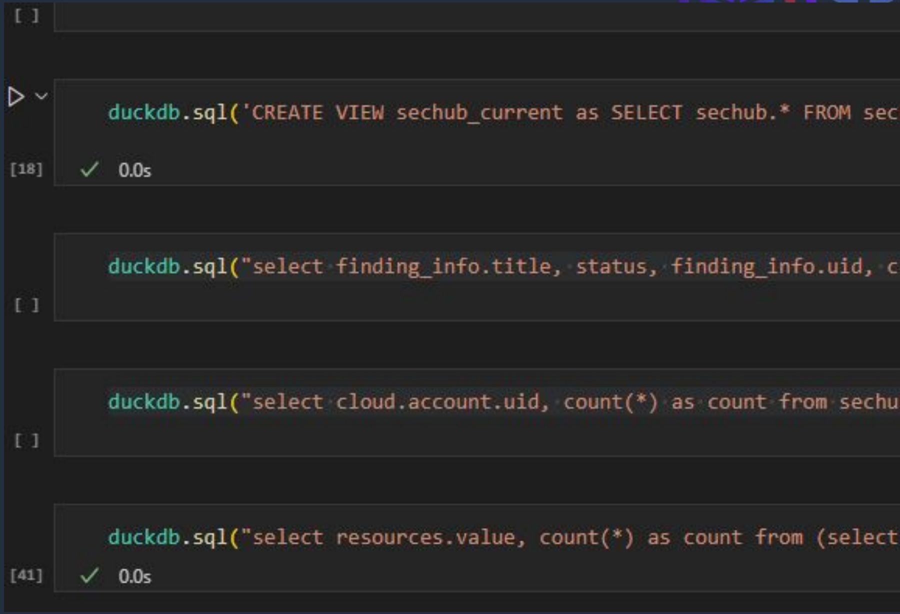
COMMUNITY DAY

How is this different from Security Hub!?



```
POST /findings HTTP/1.1
Content-type: application/json

{
   "Filters": {
      "AwsAccountId": [
         {
            "Comparison": "string",
            "Value": "string"
         }
      ],
      "AwsAccountName": [
         {
            "Comparison": "string",
            "Value": "string"
         }
      ],
      "CompanyName": [
         {
            "Comparison": "string",
            "Value": "string"
         }
      ],
```

VS



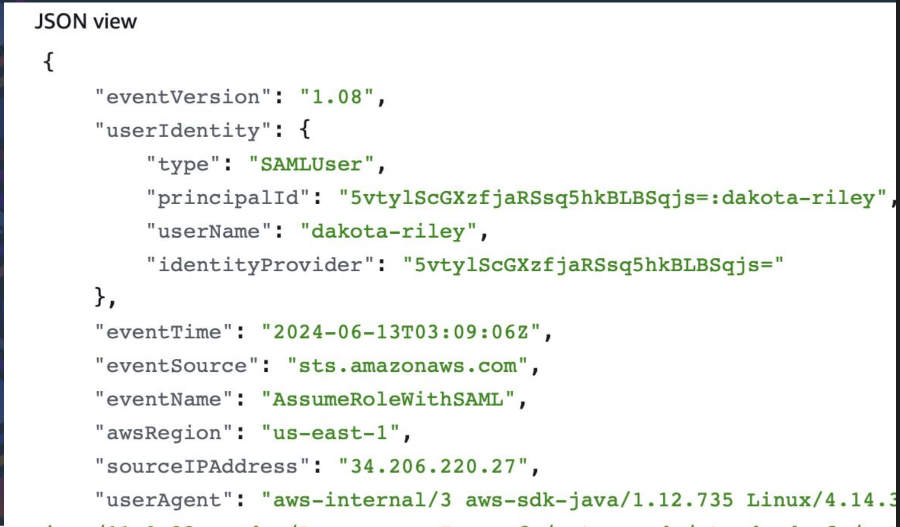
```
[ ]

duckdb.sql('CREATE VIEW sechub_current as SELECT sechub.* FROM sec
[18]  ✓ 0.0s

duckdb.sql("select finding_info.title, status, finding_info.uid, c
[ ]

duckdb.sql("select cloud.account.uid, count(*) as count from sechu
[ ]

duckdb.sql("select resources.value, count(*) as count from (select
[41]  ✓ 0.0s
```

aws

COMMUNITY DAY

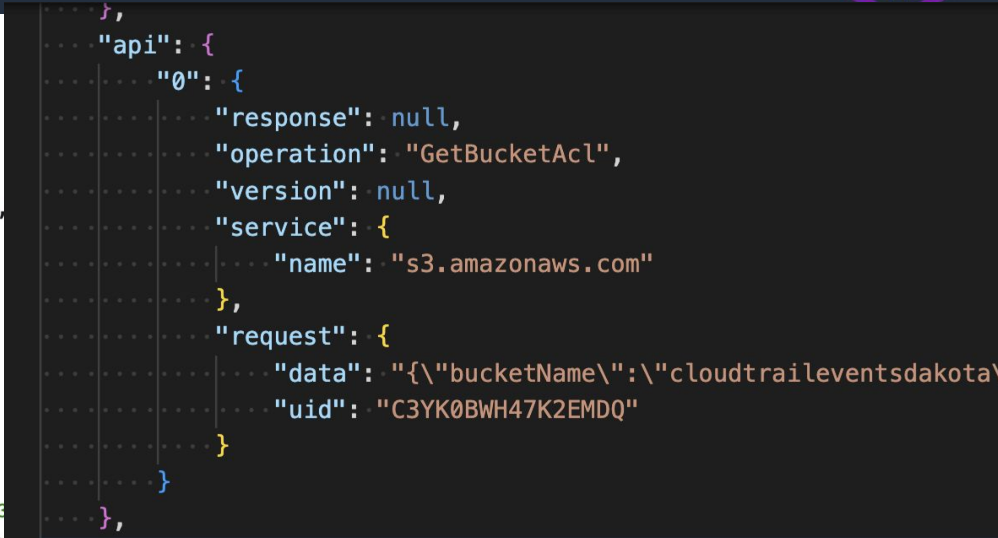
Open Cybersecurity Schema Framework (OCSF)

- Vendor-agnostic security event schema
- “Common language for threat detection and investigation”



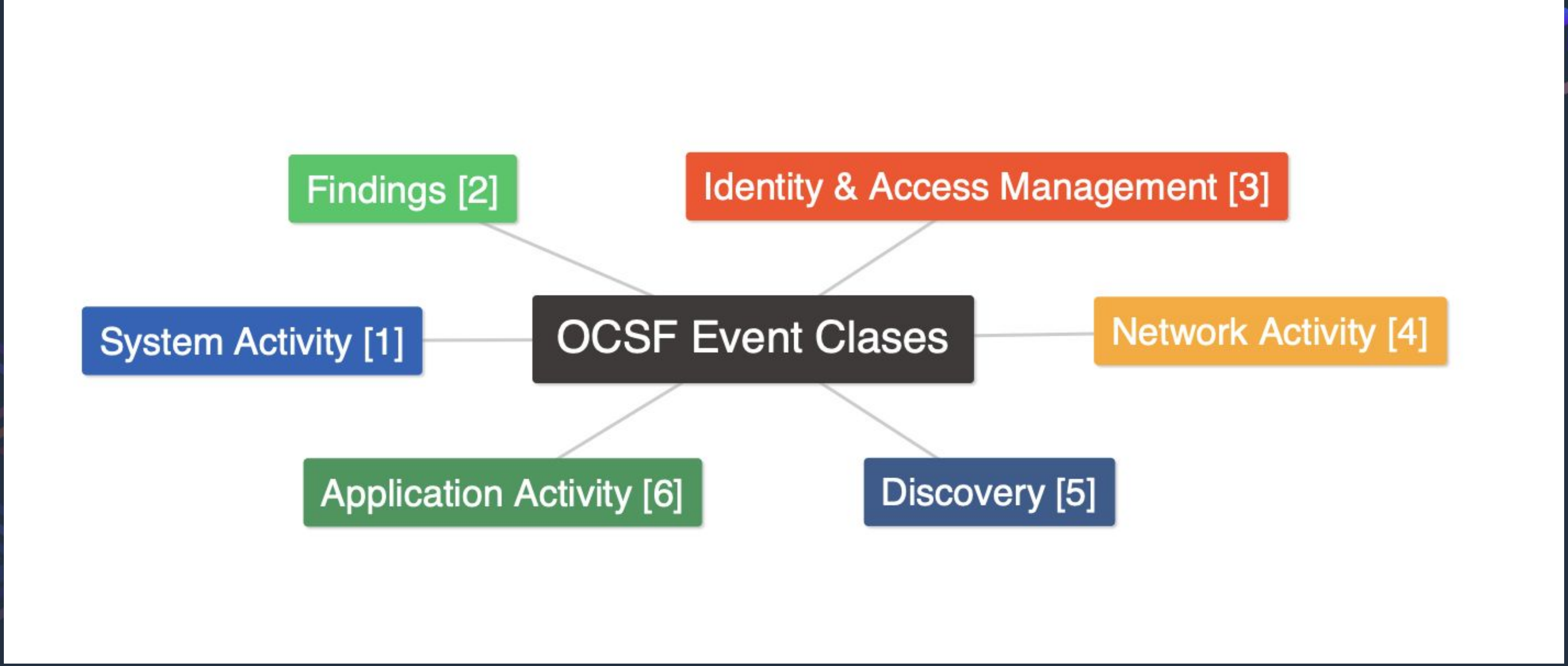
JSON view

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "SAMLUser",
        "principalId": "5vtylScGXzfjaRSsq5hkBLBSqjs=:dakota-riley",
        "userName": "dakota-riley",
        "identityProvider": "5vtylScGXzfjaRSsq5hkBLBSqjs="
    },
    "eventTime": "2024-06-13T03:09:06Z",
    "eventSource": "sts.amazonaws.com",
    "eventName": "AssumeRoleWithSAML",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "34.206.220.27",
    "userAgent": "aws-internal/3 aws-sdk-java/1.12.735 Linux/4.14.3
```



```
    },
    "api": {
        "0": {
            "response": null,
            "operation": "GetBucketAcl",
            "version": null,
            "service": {
                "name": "s3.amazonaws.com"
            },
            "request": {
                "data": "{\"bucketName\":\"cloudtraileventsdakota\
                "uid": "C3YK0BWH47K2EMDQ"
            }
        }
    },
```

OCSF Classification



Findings [2]

Identity & Access Management [3]

System Activity [1]

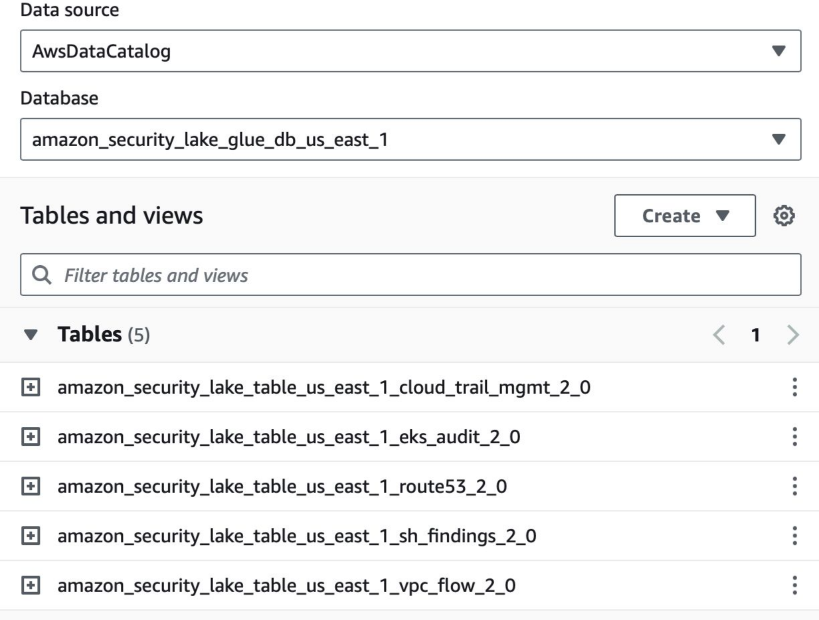
OCSF Event Clases

Network Activity [4]

Application Activity [6]

Discovery [5]

How do we get started!?



Data source

AwsDataCatalog

Database

amazon_security_lake_glue_db_us_east_1

Tables and views

Tables (5)

- amazon_security_lake_table_us_east_1_cloud_trail_mgmt_2_0
- amazon_security_lake_table_us_east_1_eks_audit_2_0
- amazon_security_lake_table_us_east_1_route53_2_0
- amazon_security_lake_table_us_east_1_sh_findings_2_0
- amazon_security_lake_table_us_east_1_vpc_flow_2_0

aws

COMMUNITY DAY

How do we get started!?

Assess Log Volumes and Costs

Create views for use cases

Onboard helpful metadata sources

Open Cybersecurity Schema Framework

Get comfortable with OCSF

aws

COMMUNITY DAY

Jupyter Notebook Time!