

AWS re:Inforce

JUNE 13 - 14, 2023 | ANAHEIM, CA

TDR341

Investigating incidents with Amazon Security Lake & Jupyter notebooks

Anna McAbee

Senior Security Specialist SA (TD/IR)
AWS

Shannon Brazil

Incident Responder (CIRT)
AWS

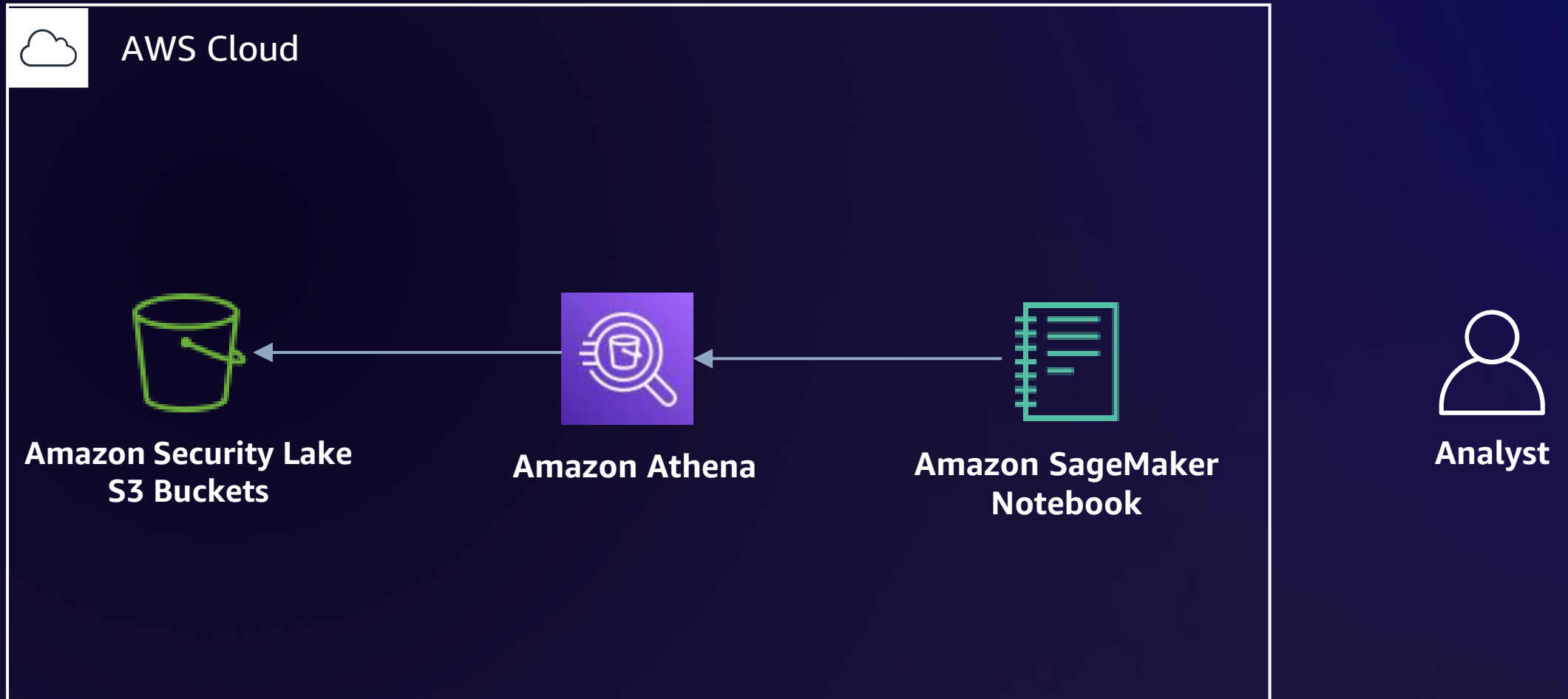


Agenda

- Incident response tools
- Live incident response
- Summary and Q&A

Architecture and incident response tools

Analysis architecture



Amazon Security Lake basics



Amazon Security Lake setup

Security, Identity and Compliance

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,

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

 CloudShell [Feedback](#) [Language](#)

[Privacy](#) [Terms](#) [Cookie preferences](#)


Waiting for us-east-1.console.aws.amazon.com...

© 2023, Amazon Web Services, Inc. or its affiliates.



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

Amazon Security Lake: Provisioned Amazon S3 buckets

Buckets (11) Info			
Buckets are containers for data stored in S3. Learn more			
<input type="text" value="Find buckets by name"/>			
	Name	AWS Region	
<input type="radio"/>	aws-security-data-lake-ap-northeast-1-nqvgehyoblhoidp46ozlulkul	Asia Pacific (Tokyo) ap-northeast-1	
<input type="radio"/>	aws-security-data-lake-ap-southeast-1-p6h2qagjxaupvbpzkubvcd1vv	Asia Pacific (Singapore) ap-southeast-1	
<input type="radio"/>	aws-security-data-lake-ap-southeast-2-ktlegemimkk0srvglmowqy7gb	Asia Pacific (Sydney) ap-southeast-2	
<input type="radio"/>	aws-security-data-lake-eu-central-1-3hqlrholt6dooknqrpc1kminznx	EU (Frankfurt) eu-central-1	
<input type="radio"/>	aws-security-data-lake-eu-west-1-sbv4kvad1h663frgo1m6s1qraq1ttm	EU (Ireland) eu-west-1	
<input type="radio"/>	aws-security-data-lake-eu-west-2-hb8grf56h3ryjqmxirpsoqi4zmagty	EU (London) eu-west-2	
<input type="radio"/>	aws-security-data-lake-sa-east-1-kptfqg2bhvzp7ajvhzvfpsy2ssyrr	South America (São Paulo) sa-east-1	
<input type="radio"/>	aws-security-data-lake-us-east-1-jhzx13b9mjya9lvn94fifa5waqtewo	US East (N. Virginia) us-east-1	
<input type="radio"/>	aws-security-data-lake-us-east-2-dp4aydmvciafinnn7z1tqewyzvb9zi	US East (Ohio) us-east-2	
<input type="radio"/>	aws-security-data-lake-us-west-2-y2ooyzrklg9ccjouczjjpgqmjohiw	US West (Oregon) us-west-2	

Amazon Security Lake: AWS Glue tables

AWS Glue×

Getting started

ETL jobs

Visual ETL

Notebooks

Job run monitoring

Data Catalog tables

Data connections

Workflows (orchestration)

▼ **Data Catalog**

Databases

Tables

Stream schema registries

Schemas

Connections

Crawlers

Classifiers

Catalog settings

► **Data Integration and ETL**

► **Legacy pages**

Use AWS Glue to move and prepare data for analytics and machine learning

Get started

What's new in Glue [↗](#)

[AWS Glue Crawlers now support creating partition indexes](#)

Apr 24, 2023

[AWS Lake Formation and Glue Data Catalog now manage Apache Hive Metastore resources](#)

Apr 19, 2023

[AWS Glue launches new capability to monitor usage of Glue resources](#)

Apr 17, 2023

[View more](#) [↗](#)


Benefits and features

AWS Glue Data Catalog

Track your data assets and make them accessible from your analytics tools of choice.

Crawlers for data discovery

Automatically detect the schema and structure of your data and add it to the AWS Glue Data Catalog.





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

Amazon Security Lake: Amazon Athena queries



The screenshot displays the Amazon Athena console's Editor interface. At the top, there are tabs for 'Editor', 'Recent queries', 'Saved queries', and 'Settings'. A 'Workgroup' dropdown menu is set to 'primary'. The left sidebar contains a 'Data' section with a refresh icon and a list of tables. The 'Data source' is set to 'AwsDataCatalog' and the 'Database' is 'amazon_security_lake_glue_db_us_east_1'. Under 'Tables and views', there is a search bar and a list of four tables: 'amazon_security_lake_table_us_east_1_c_loud_trail', 'amazon_security_lake_table_us_east_1_r_oute53', 'amazon_security_lake_table_us_east_1_s_h_findings', and 'amazon_security_lake_table_us_east_1_s_h_findings'. The main area shows 'Query 2' and 'Query 3' tabs. The 'Query 3' tab is active, displaying a large empty space for the query. At the bottom, there are buttons for 'Run', 'Explain', 'Cancel', 'Clear', and 'Create'. A 'Reuse query results' toggle is also present, with a note that it is only available for Athena engine version 3.


Editor | Recent queries | Saved queries | Settings | Workgroup: primary



Data  







Data source: AwsDataCatalog





Database: amazon_security_lake_glue_db_us_east_1

Tables and views  




 Filter tables and views






▼ **Tables (4)**  **1** 

-  amazon_security_lake_table_us_east_1_c_loud_trail 
Partitioned
-  amazon_security_lake_table_us_east_1_r_oute53 
Partitioned
-  amazon_security_lake_table_us_east_1_s_h_findings 

Query 2  | Query 3  |  | 

1

SQL Ln 1, Col 1   



☐ Reuse query results
*Athena engine version 3 only

[Query results](#) | [Query stats](#)

Jupyter Notebooks

Open source web application for sharing live code and analysis

- **Benefits**
 - Standardize techniques
 - Reduce silos
 - Team collaboration
- **Functions**
 - IR notebook
 - Code execution
- **Impact: Enhanced incident response**

 **Jupyter Notebook template** 

This skeleton notebook showcases a basic structure including ToC and imports

Table of Contents


- [1 Load data](#)
- [2 Analysis](#)
- [3 Modelling](#)
- [4 Evaluate results](#)

```
In [1]: %load_ext autoreload

import pandas as pd
import numpy as np
import matplotlib as mpl
import matplotlib.pyplot as plt

# Pandas Dataframe display options
pd.set_option('display.max_rows', 8)
pd.set_option('display.max_columns', 200)

# Plotting style
plt.style.use('seaborn-darkgrid')
mpl.rcParams['figure.dpi'] = 100
```

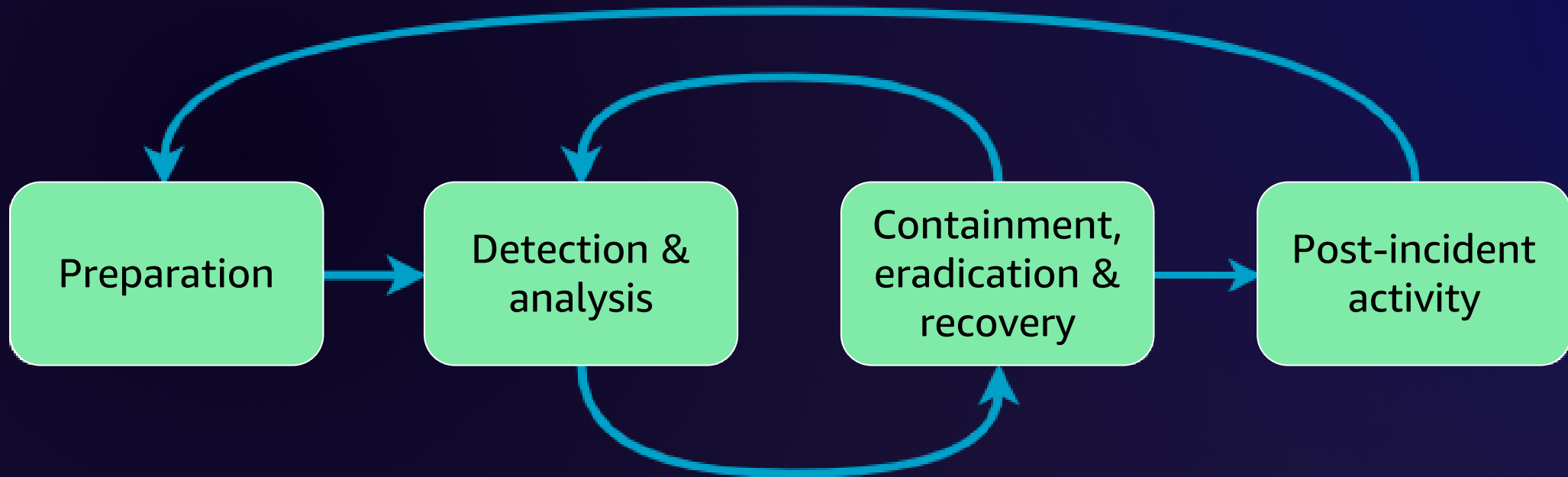
 **1 Load data**

```
In [ ]: # pd.read_ ...
```

 **2 Analysis**

```
In [ ]: # df = ...
```

Incident response lifecycle



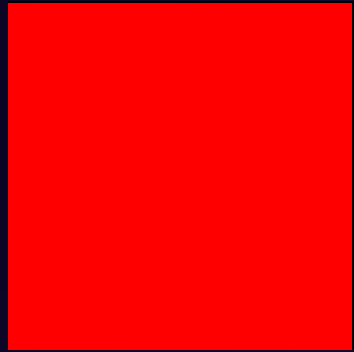
Source: NIST 800-61 Incident Response Lifecycle

Live incident response

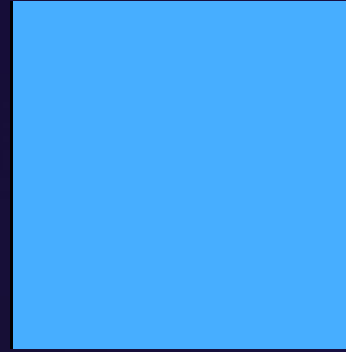


Session details

Incident response requires **teamwork!**



OR



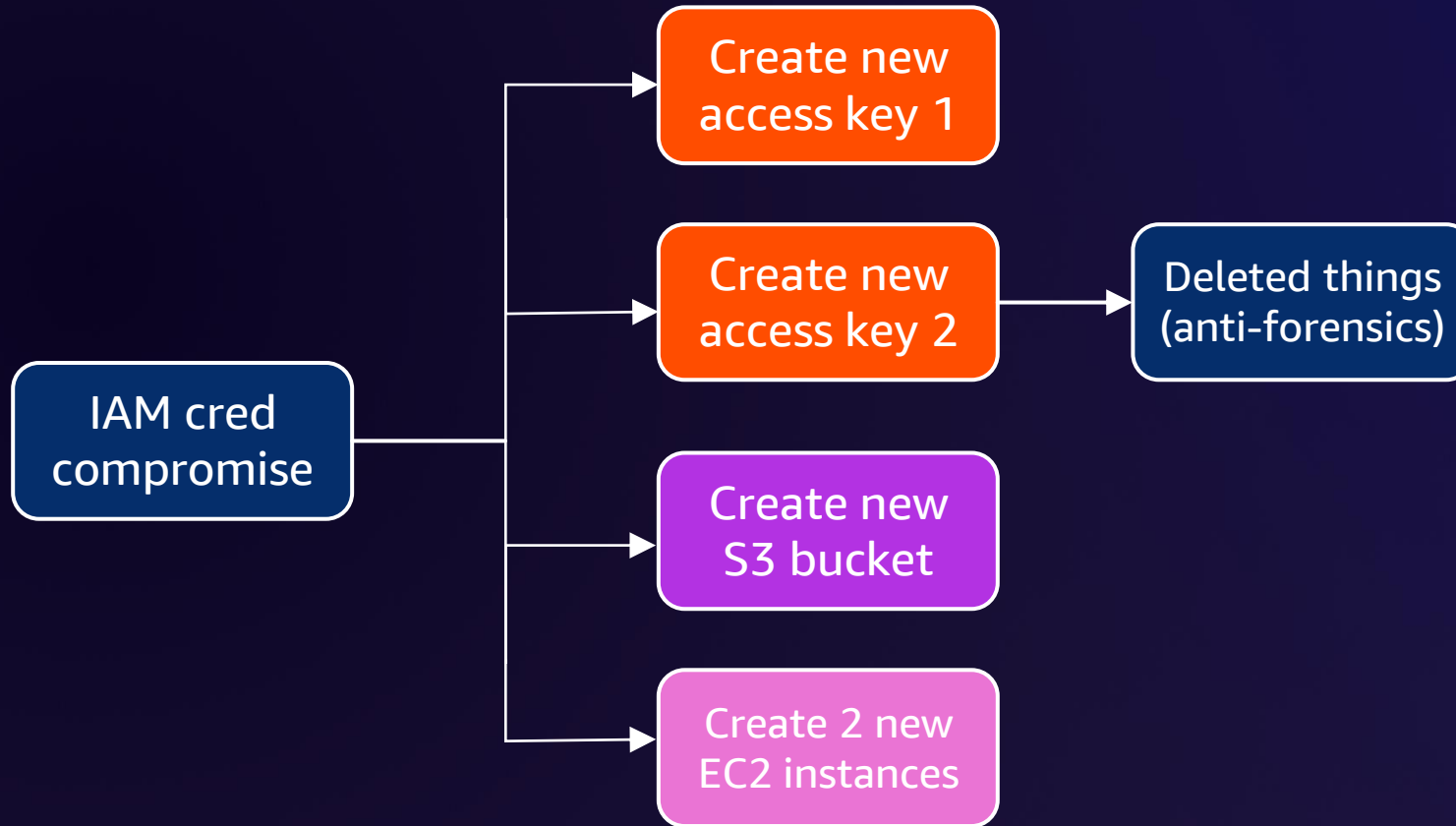
The **most popular** vote will be chosen as the action.

Game time

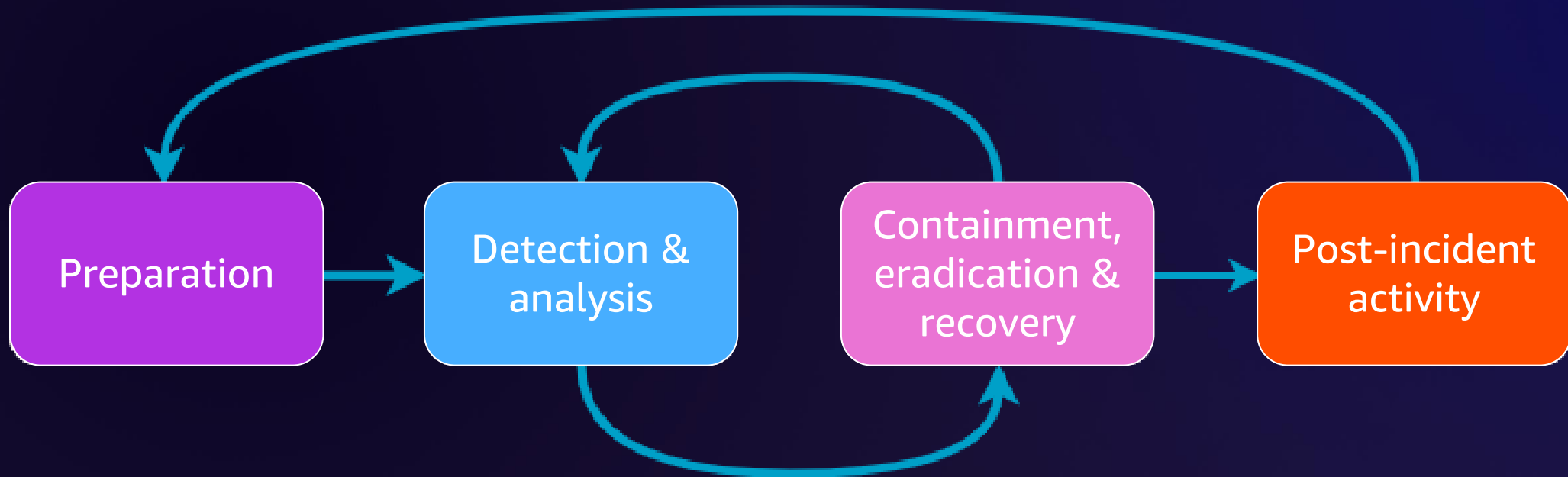


Summary and Q&A

Complete scenario

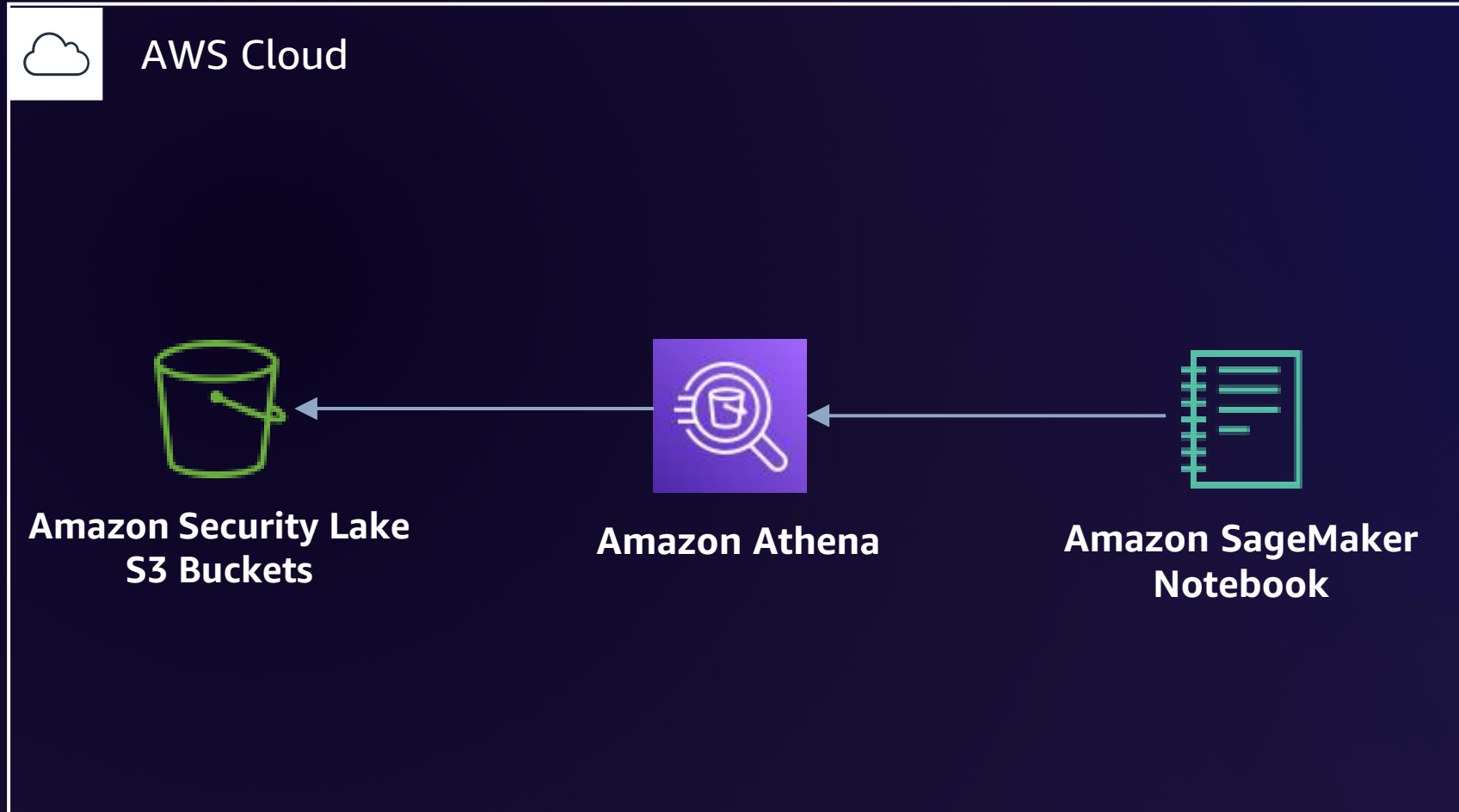


Enhanced incident response lifecycle



Source: NIST 800-61 Incident Response Lifecycle

Lessons learned



Additional resources

AWS Security incident Response Guide

<https://docs.aws.amazon.com/whitepapers/latest/aws-security-incident-response-guide/aws-security-incident-response-guide.html>

Logging strategies for security incident response

<https://aws.amazon.com/blogs/security/logging-strategies-for-security-incident-response/>

Incident Response with Jupyter Workshop

<https://catalog.workshops.aws/incident-response-jupyter/en-US>

New AWS CIRT workshops

<https://aws.amazon.com/blogs/security/aws-cirt-announces-the-release-of-five-publicly-available-workshops/>

AWS Customer Playbook Framework

<https://github.com/aws-samples/aws-customer-playbook-framework>

Amazon Security Lake Machine Learning Solution

<https://github.com/aws-samples/amazon-security-lake-machine-learning>



Related sessions

- [TDR333](#) | [Chalk talk](#) | Gaining insights from Amazon Security Lake
- [TDR432](#) | [Chalk talk](#) | Deep dive into exposed credentials and how to investigate them
- [TDR221](#) | [Lightning talk](#) | Streamline security operations and improve threat detection with OCSF

Thank you!



Please complete
the session survey
in the mobile app

Anna McAbee


annaaws@amazon.com

 @amcabee13

 linkedin.com/in/anna-mcabee

Shannon Brazil

awslady@amazon.com

 @4n6lady

 linkedin.com/in/shannonbrazil