

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

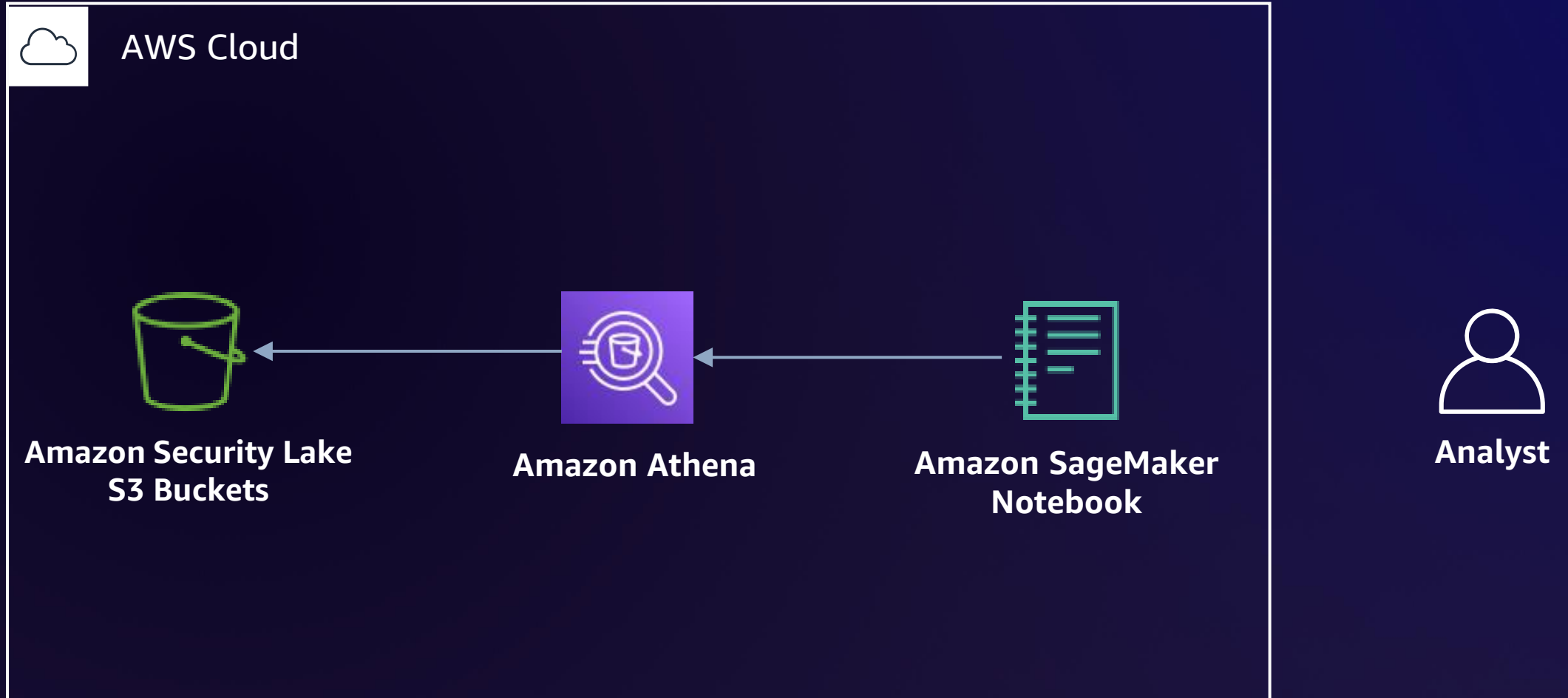


Agenda

- 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.



Amazon Security Lake: Provisioned Amazon S3 buckets

Buckets (11) [Info](#) 🔄

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

Name	AWS Region
aws-security-data-lake-ap-northeast-1-nqvgehyoblhoidp46ozlulkul	Asia Pacific (Tokyo) ap-northeast-1
aws-security-data-lake-ap-southeast-1-p6h2qagjxaupvbpzkubvcd1vv	Asia Pacific (Singapore) ap-southeast-1
aws-security-data-lake-ap-southeast-2-ktlegemimkk0srvglmowqy7gb	Asia Pacific (Sydney) ap-southeast-2
aws-security-data-lake-eu-central-1-3hqlrholt6dooknqrpc1kminzrx	EU (Frankfurt) eu-central-1
aws-security-data-lake-eu-west-1-sbv4kvad1h663frgo1m6s1qraq1ttm	EU (Ireland) eu-west-1
aws-security-data-lake-eu-west-2-hb8grf56h3ryjqmxirpsoqi4zmagty	EU (London) eu-west-2
aws-security-data-lake-sa-east-1-kptfqg2bhvzp7ajvhzvfpsy2ssyrr	South America (São Paulo) sa-east-1
aws-security-data-lake-us-east-1-jhzx13b9mjya9lvn94fifa5waqtewo	US East (N. Virginia) us-east-1
aws-security-data-lake-us-east-2-dp4aydmvciafinnn7z1tqewyzvb9zi	US East (Ohio) us-east-2
aws-security-data-lake-us-west-2-y2ooyzrklg9ccjouczjjpgqmjohiw	US West (Oregon) us-west-2

Amazon Security Lake: AWS Glue tables

The screenshot displays the AWS Glue console interface. On the left is a navigation menu with the following items: Getting started, ETL jobs (with sub-items Visual ETL, Notebooks, and Job run monitoring), Data Catalog tables, Data connections, Workflows (orchestration), **Data Catalog** (expanded), Databases (with sub-item Tables), Stream schema registries (with sub-item Schemas), Connections, Crawlers (with sub-item Classifiers), Catalog settings, **Data Integration and ETL**, and Legacy pages. The main content area features a dark header with the text 'Use AWS Glue to move and prepare data for analytics and machine learning' and an orange 'Get started' button. Below this is a 'What's new in Glue' section with three news items: 'AWS Glue Crawlers now support creating partition indexes' (dated Apr 24, 2023), 'AWS Lake Formation and Glue Data Catalog now manage Apache Hive Metastore resources' (dated Apr 19, 2023), and 'AWS Glue launches new capability to monitor usage of Glue resources' (dated Apr 17, 2023). A 'View more' link is also present. At the bottom of the main content area is a 'Benefits and features' section with two columns: 'AWS Glue Data Catalog' (describing tracking data assets) and 'Crawlers for data discovery' (describing automatic schema detection).

Amazon Security Lake: Amazon Athena queries

The screenshot displays the Amazon Athena console interface. At the top, there are tabs for 'Editor', 'Recent queries', 'Saved queries', and 'Settings'. The 'Workgroup' is set to 'primary'. The main area is divided into a left sidebar and a main editor pane. The sidebar contains a 'Data' section with a refresh icon and a 'Data source' dropdown set to 'AwsDataCatalog'. Below that is the 'Database' dropdown set to 'amazon_security_lake_glue_db_us_east_1'. The 'Tables and views' section includes a 'Create' button and a search bar with the placeholder text 'Filter tables and views'. A list of tables is shown, including 'amazon_security_lake_table_us_east_1_c_loud_trail', 'amazon_security_lake_table_us_east_1_r_oute53', and 'amazon_security_lake_table_us_east_1_s_h_findings'. The main editor pane shows 'Query 3' with a single line of SQL code. Below the editor, there are buttons for 'Run', 'Explain', 'Cancel', and 'Clear', along with a 'Reuse query results' toggle and a note '*Athena engine version 3 only'. At the bottom, there are tabs for 'Query results' and '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
```

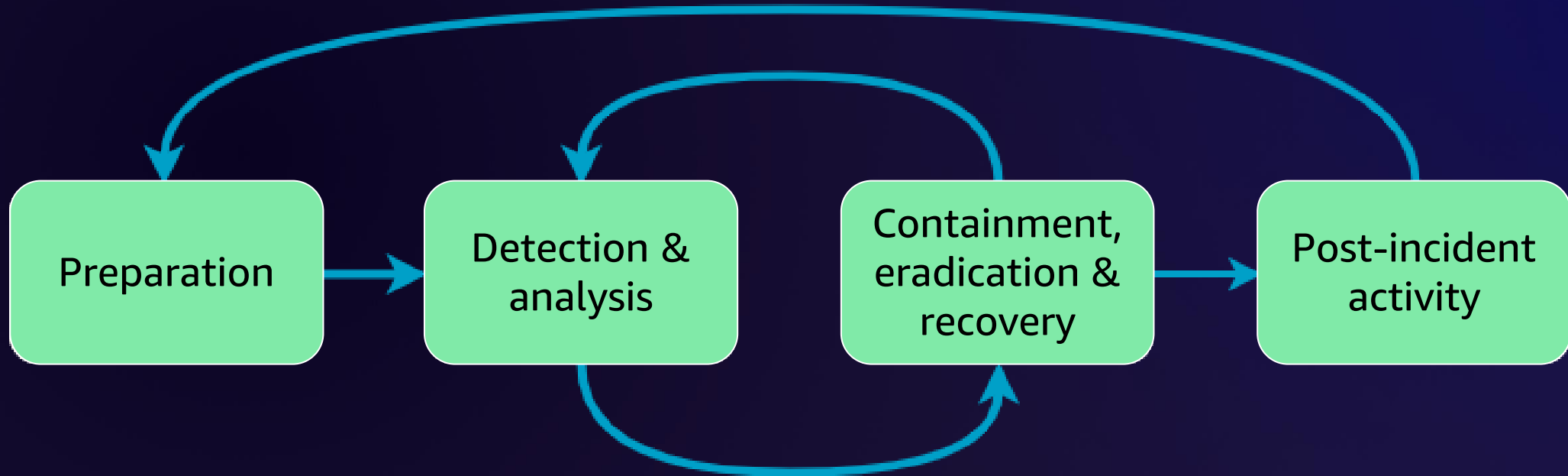
▼ **1 Load data**

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

▼ **2 Analysis**

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

Incident response lifecycle



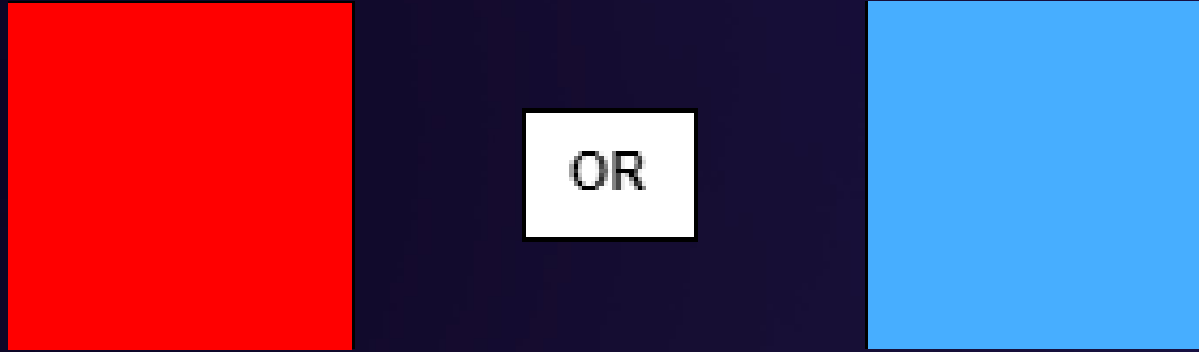
Source: NIST 800-61 Incident Response Lifecycle

Live incident response



Session details

Incident response requires **teamwork!**



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

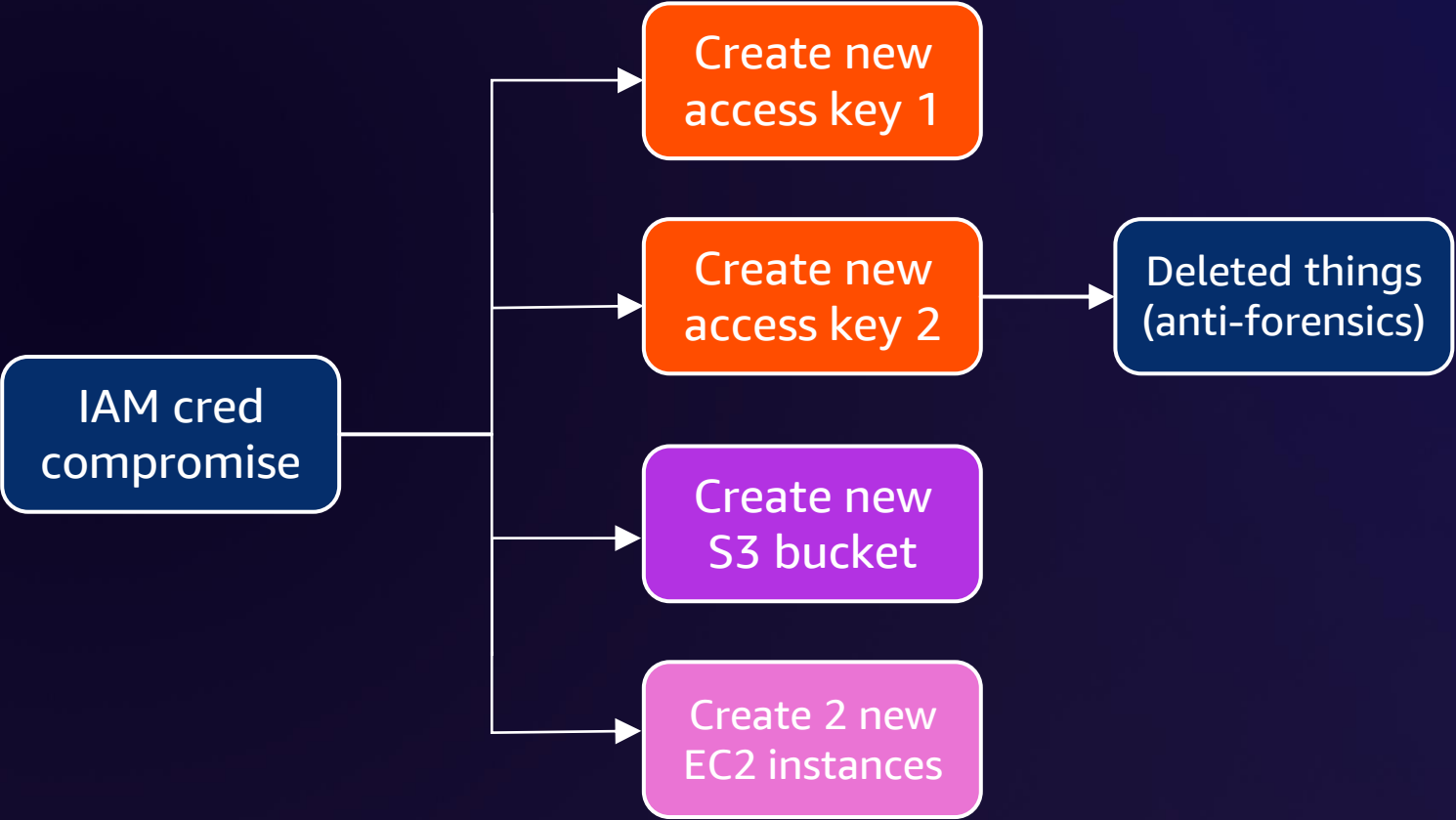
Game time



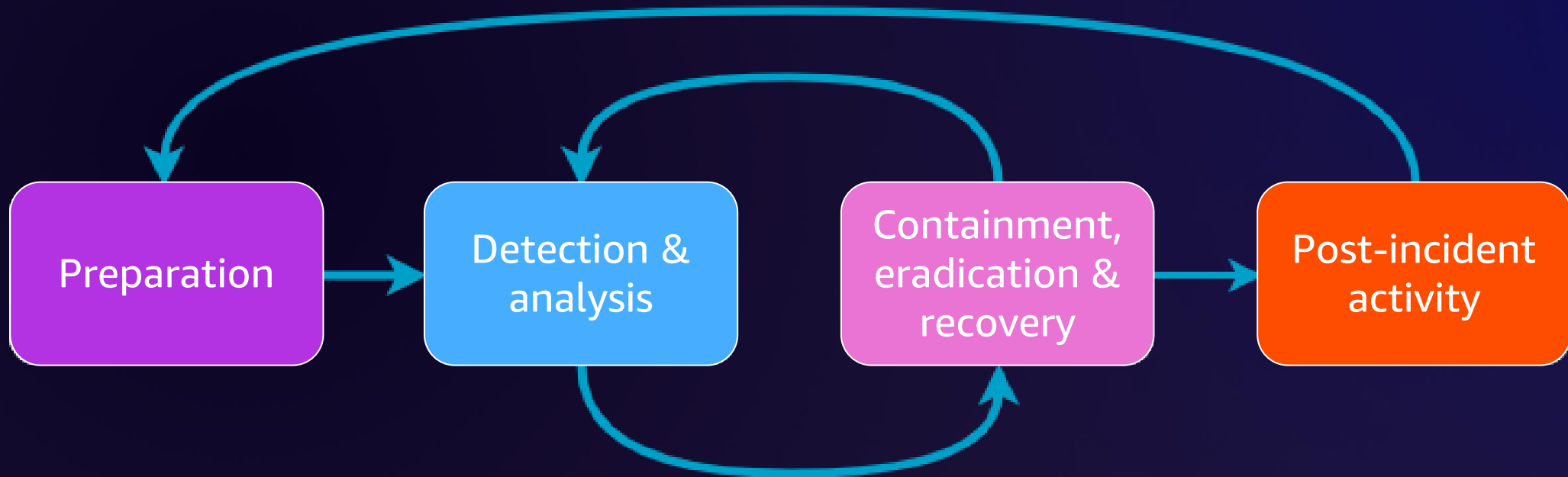
Summary and Q&A



Complete scenario

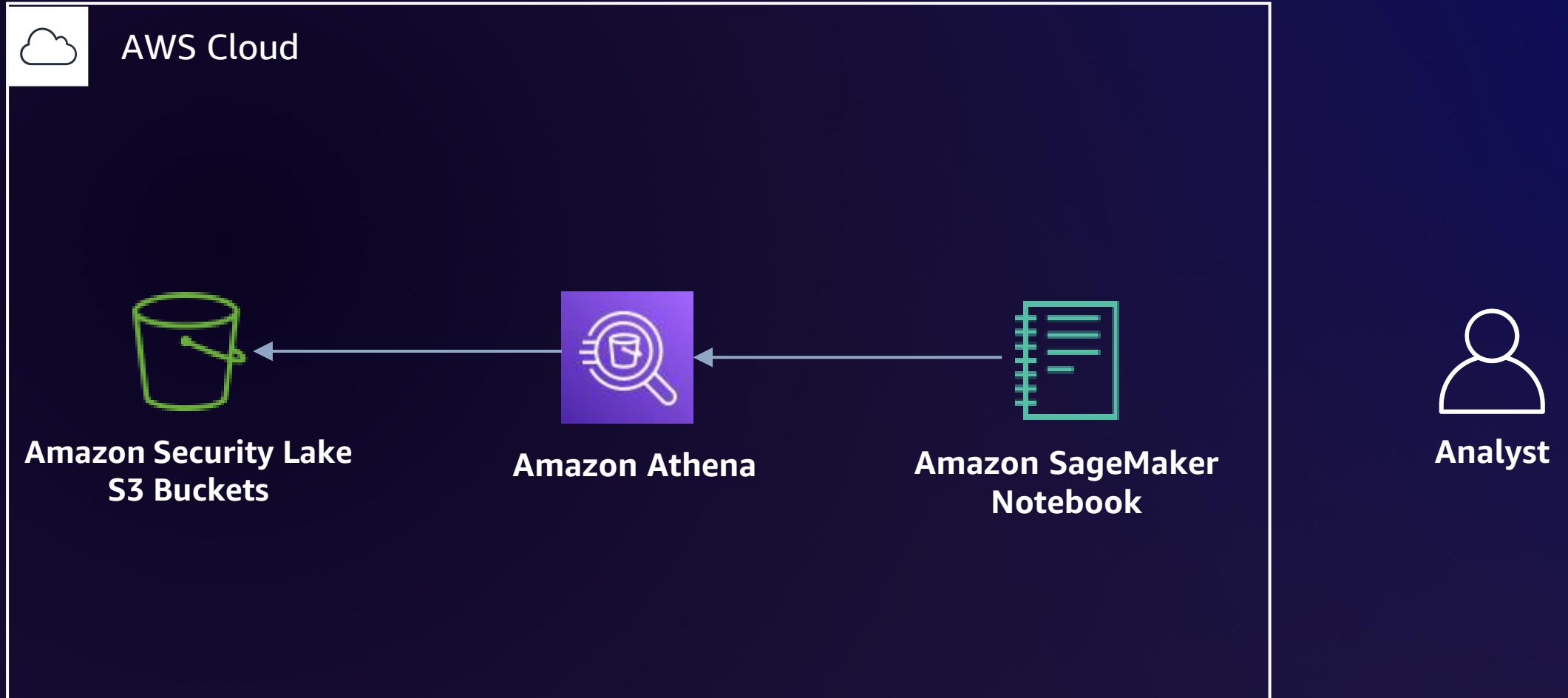


Enhanced incident response lifecycle



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!

Anna McAbee

annaaws@amazon.com

 @amcabee13

 [linkedin.com/in/anna-mcabee](https://www.linkedin.com/in/anna-mcabee)

Shannon Brazil

awslady@amazon.com

 @4n6lady

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



Please complete
the session survey
in the mobile app