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

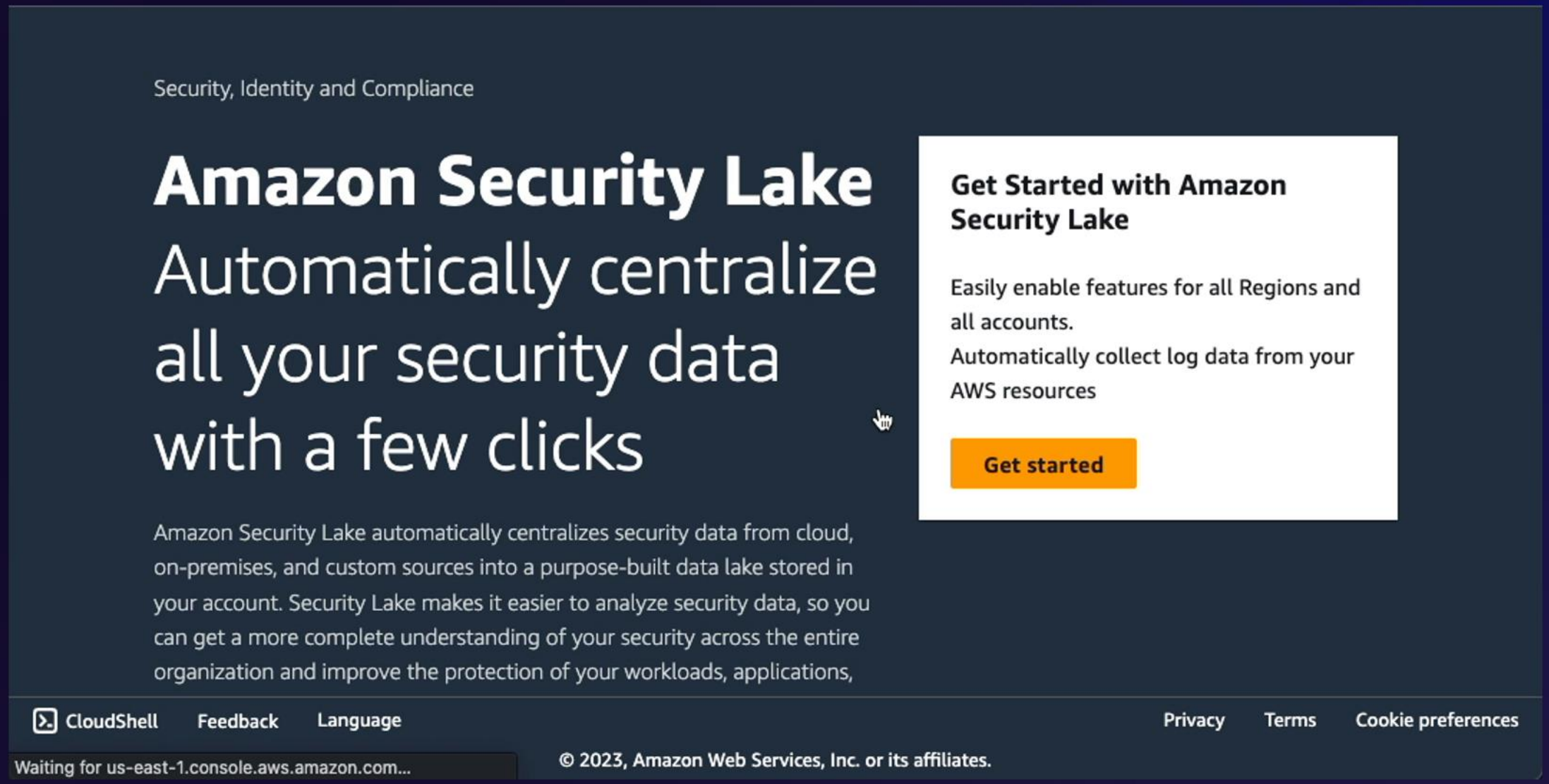
- Incident response tools
- Live incident response
- Summary and Q&A

Architecture and incident response tools

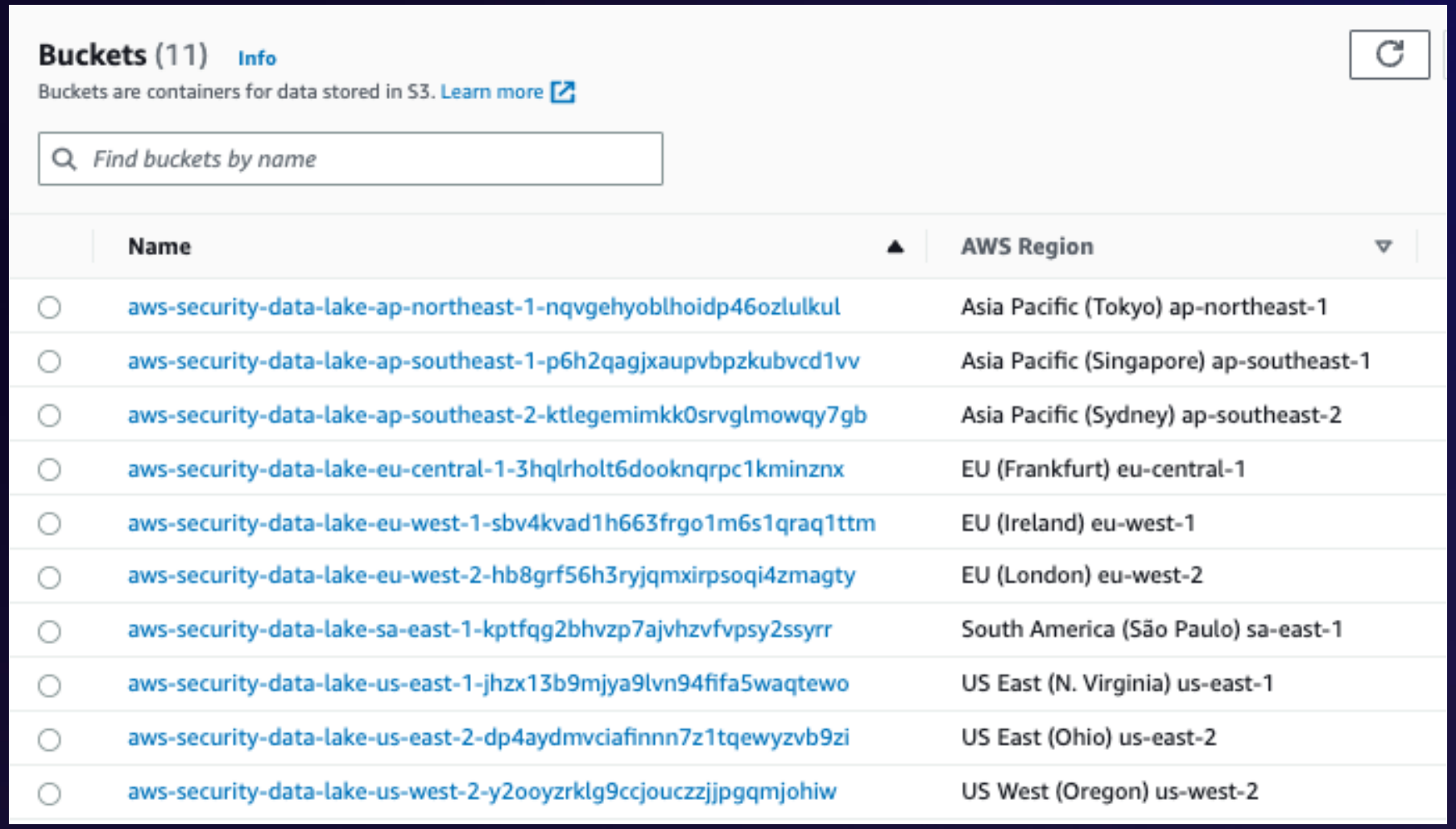
Analysis architecture

Amazon Security Lake basics

Amazon Security Lake setup



Amazon Security Lake: Provisioned Amazon S3 buckets



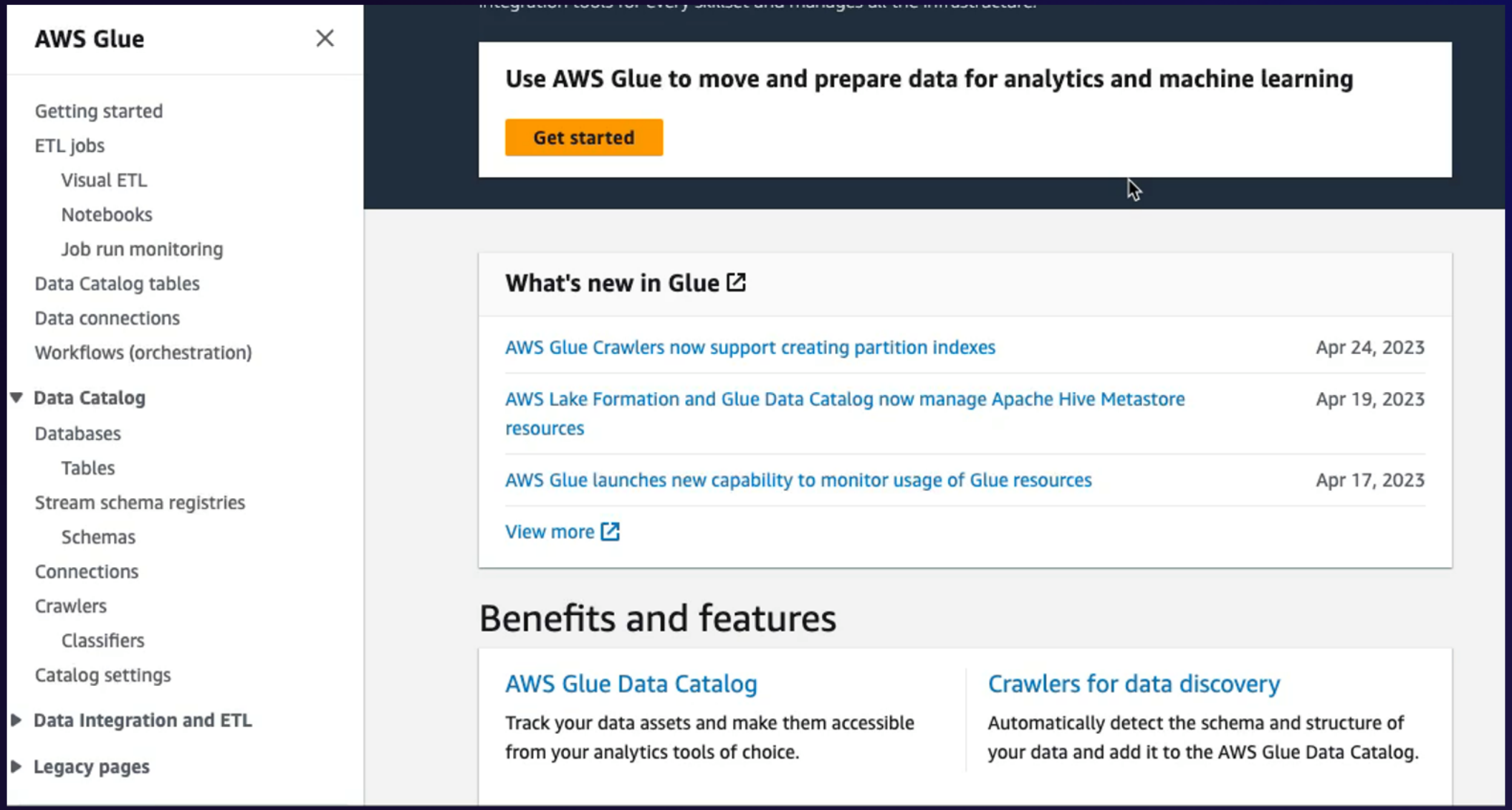
Buckets (11) Info

Buckets are containers for data stored in S3. Learn more

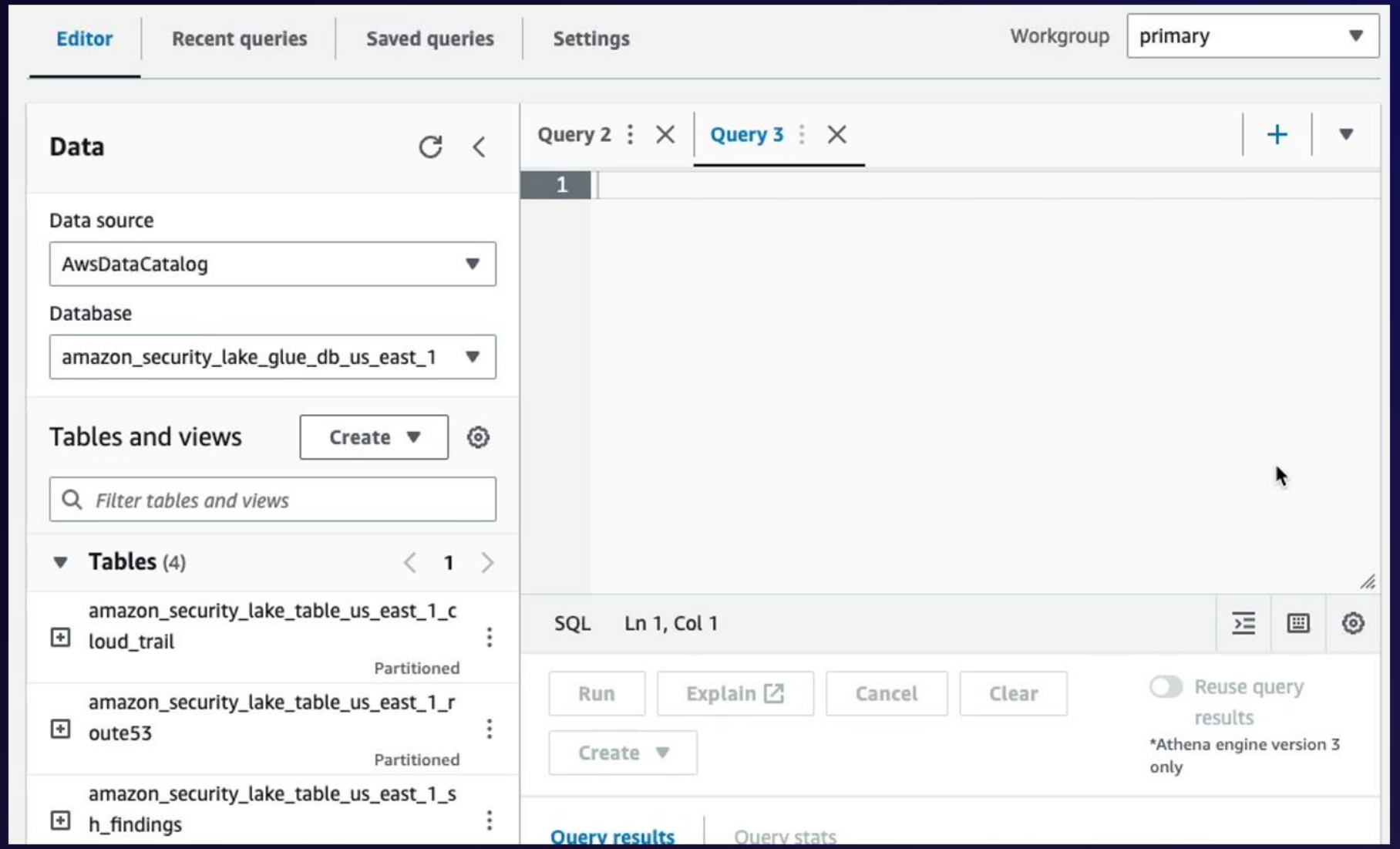
Find buckets by name

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-1-3hqlrholt6dooknqrpc1kminznx	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-kptfqg2bhvzp7ajvhzvfvpsy2ssyrr	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-y2ooyzrklg9ccjouczzjjpgqmjohiw	US West (Oregon) us-west-2

Amazon Security Lake: AWS Glue tables



Amazon Security Lake: Amazon Athena queries

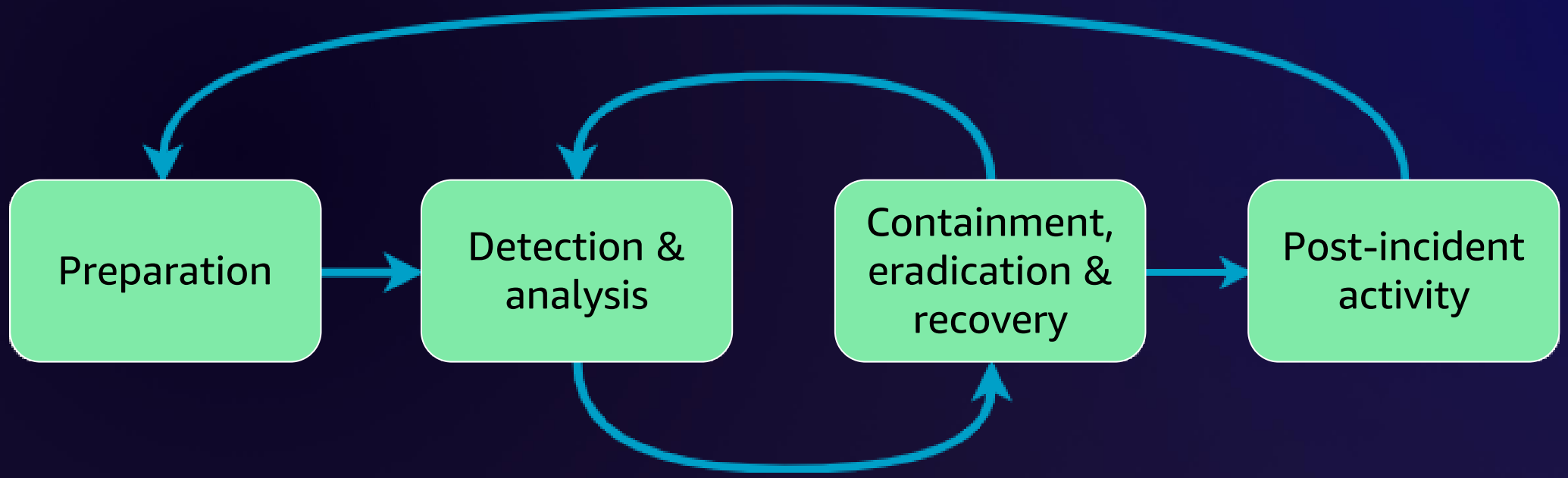


Jupyter Notebooks

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**

Incident response lifecycle

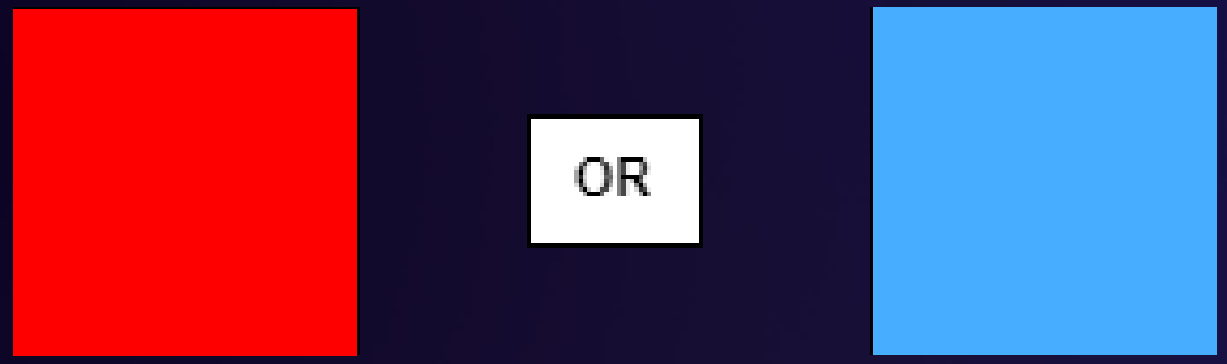


Source: NIST 800-61 Incident Response Lifecycle

Live incident response

Session details

Incident response requires **teamwork!**

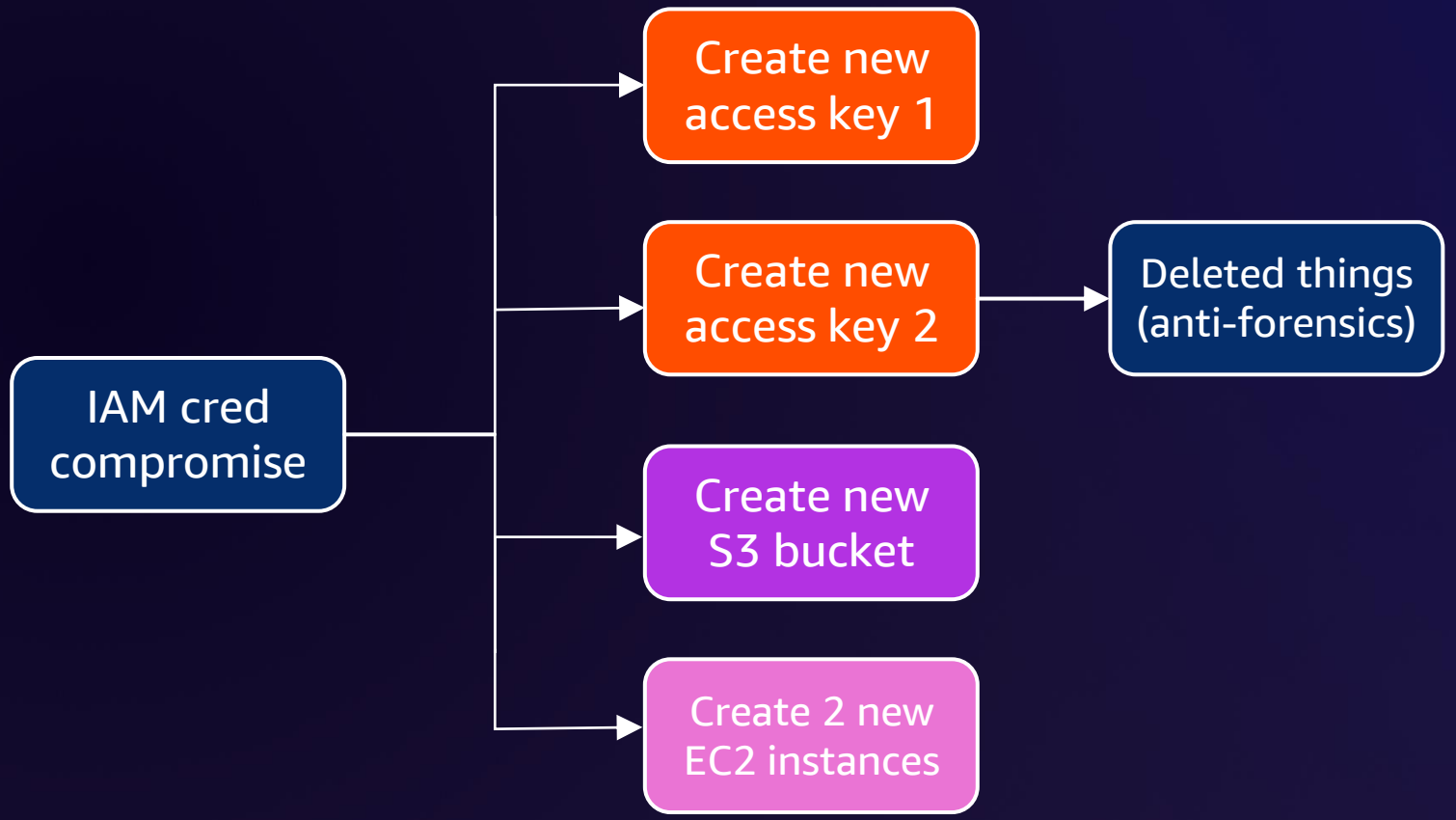


The **most popular** vote will be chosen as the action.

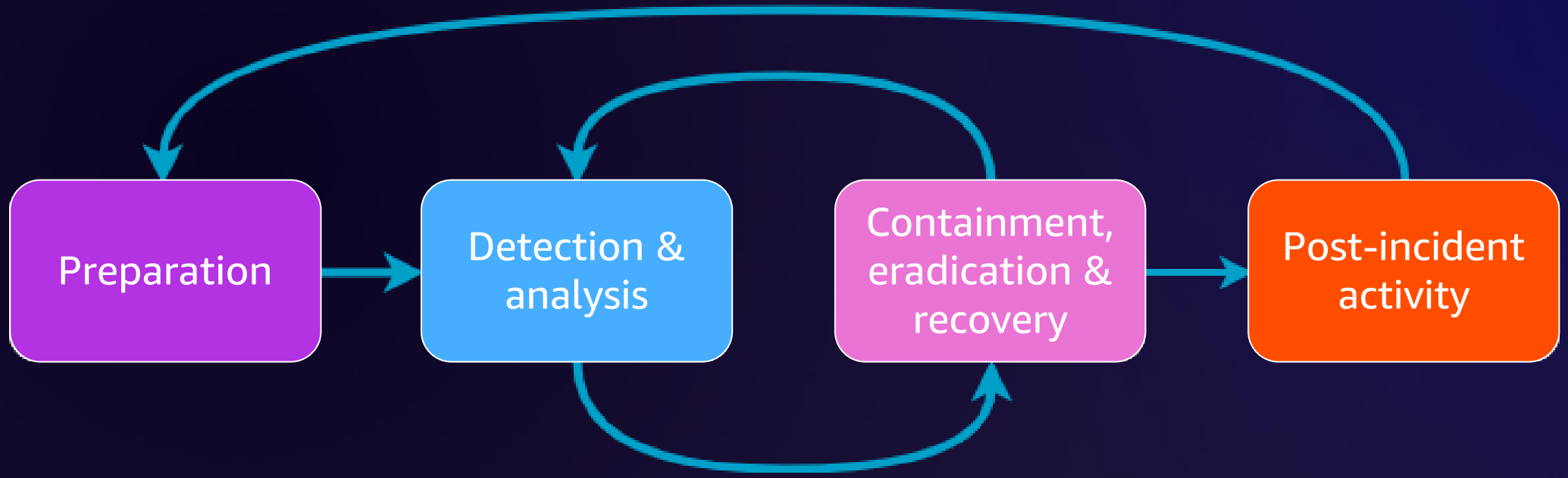
Game time

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!

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