AWS re:Invent

NOV. 29 – DEC. 3, 2021 | LAS VEGAS, NV

SEC401

Building incident response playbooks for AWS

Bohan Li
Security Transformation Consultant
AWS Professional Services

Freddy Kasprzykowski
Security Transformation Consultant
AWS Professional Services

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Expectations

The focus is to learn the simulation-based playbook development framework.

You might not be able to finish crafting the playbook today; that's fine!

Some actions will take more time than expected to complete, such as assuming IAM roles, running simulation scripts, and crafting Athena queries.

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

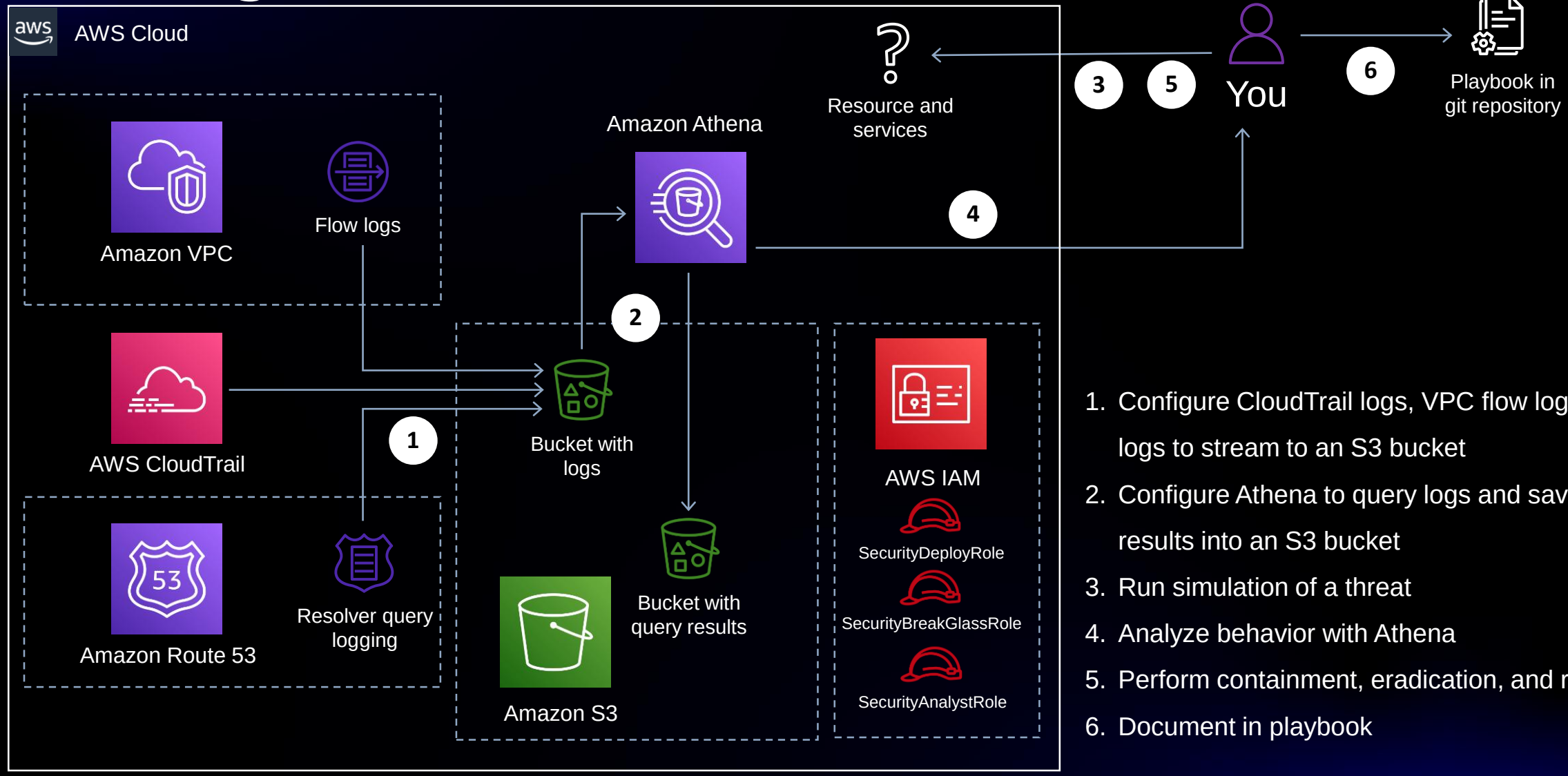
“Everyone has a plan until they’ve been hit.”

Joe Louis

Boxing heavyweight champion from 1937 to 1949

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Building backwards: Simulation driven



1. Configure CloudTrail logs, VPC flow logs, DNS logs to stream to an S3 bucket
2. Configure Athena to query logs and save results into an S3 bucket
3. Run simulation of a threat
4. Analyze behavior with Athena
5. Perform containment, eradication, and recovery
6. Document in playbook

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Resources

Main workshop page

https://aws-incident-response-playbooks.workshop.aws/

AWS account access – Use your Team Hash

https://dashboard.eventengine.run/

Playbook samples, simulation scripts, and CFT

https://github.com/awslabs/aws-incident-response-playbooks-workshop

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Ask us anything!

AWS incident response experts are available throughout the session to assist you.

We’re happy to answer any questions you might have. Don’t be shy!



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

“I did the best I could with what I had.”

Joe Louis

Boxing heavyweight champion from 1937 to 1949

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Thank you!

Bohan Li
bohanli@amazon.com

Freddy Kasprzykowski
freski@amazon.com

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.