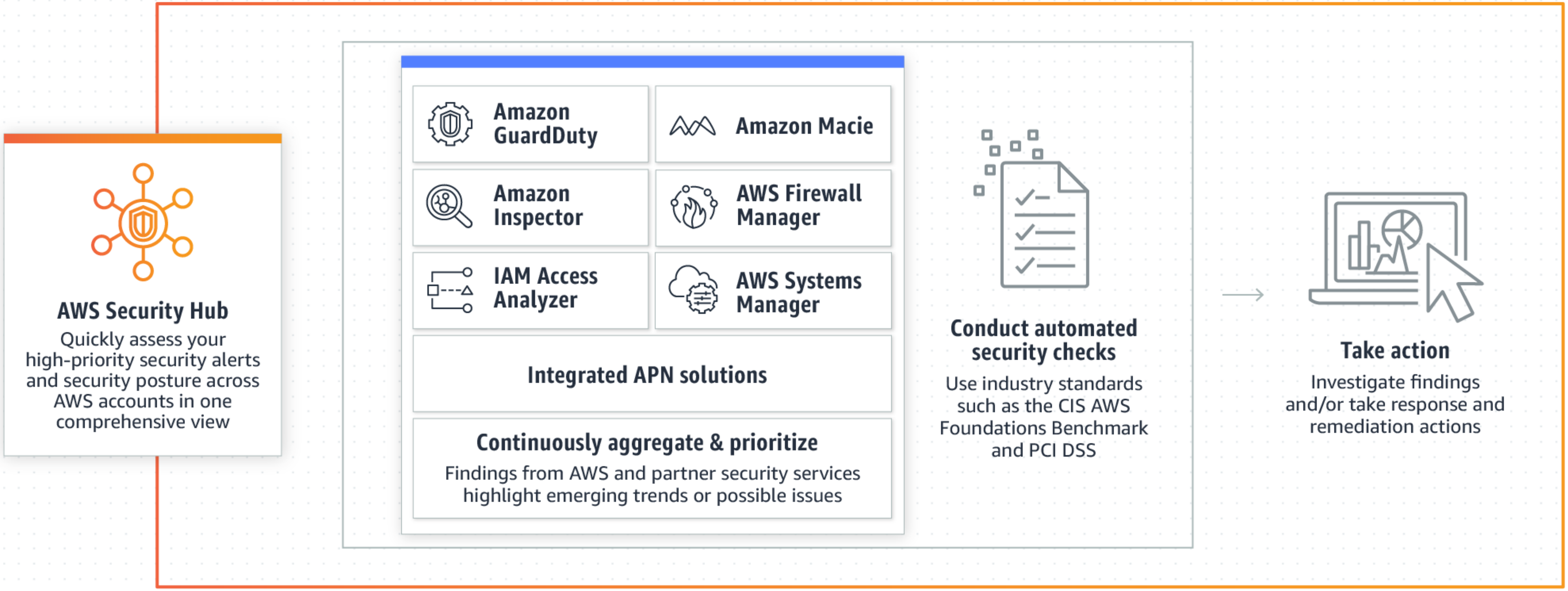
Integration, prioritization, and response with AWS Security Hub

Marshall Jones

Security Specialist Solutions Architect
Amazon Web Services

Security Hub overview



AWS Security Hub

Quickly assess your high-priority security alerts and security posture across AWS accounts in one comprehensive view

Amazon GuardDuty

Amazon Macie

Amazon Inspector

AWS Firewall Manager

IAM Access Analyzer

AWS Systems Manager

Integrated APN solutions

Continuously aggregate & prioritize

Findings from AWS and partner security services highlight emerging trends or possible issues

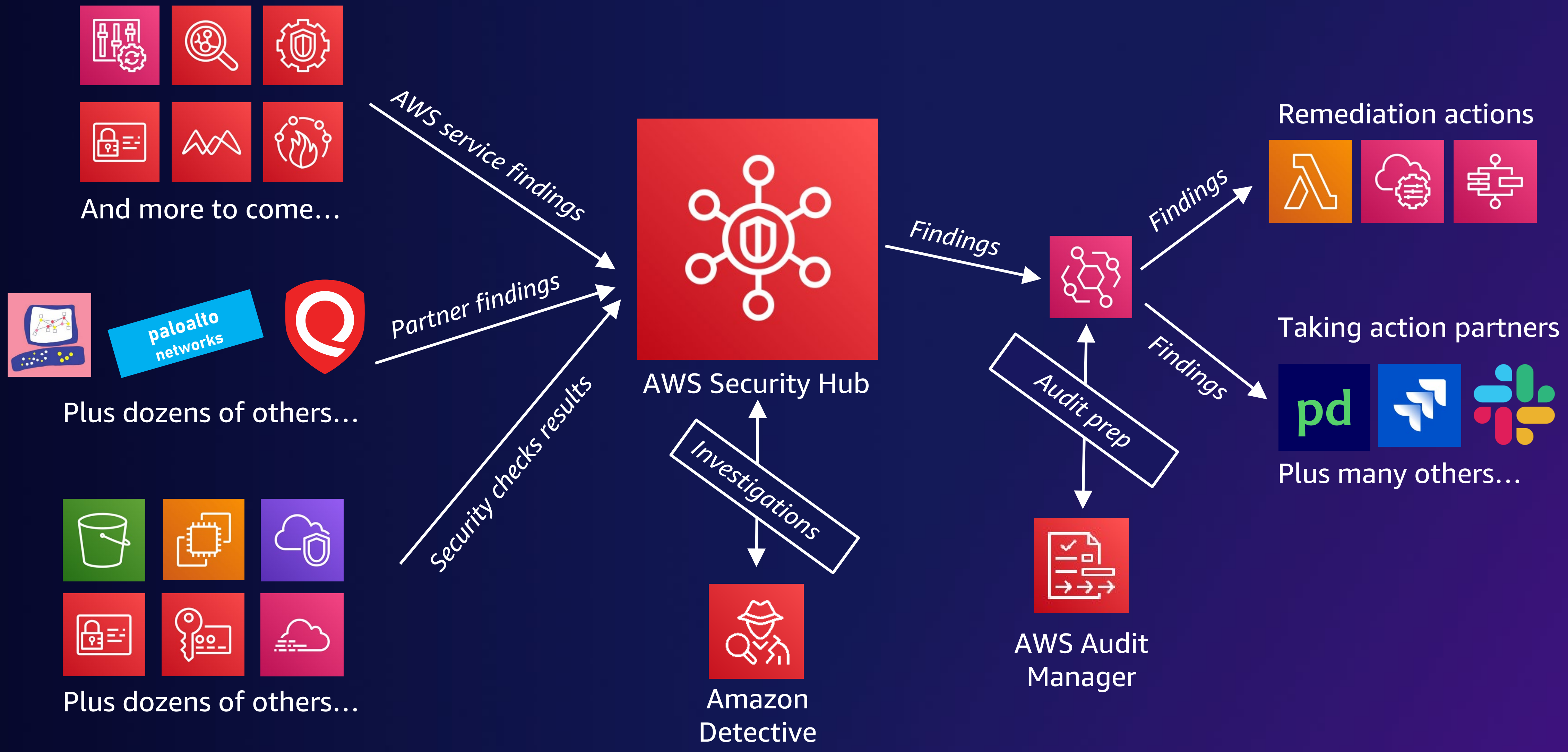
Conduct automated security checks

Use industry standards such as the CIS AWS Foundations Benchmark and PCI DSS

Take action

Investigate findings and/or take response and remediation actions

AWS Security Hub information flows



And more to come…

AWS service findings

Plus dozens of others…

Partner findings

Plus dozens of others…

Security checks results

AWS Security Hub

Investigations

Amazon Detective

Findings

Audit prep

AWS Audit Manager

Findings

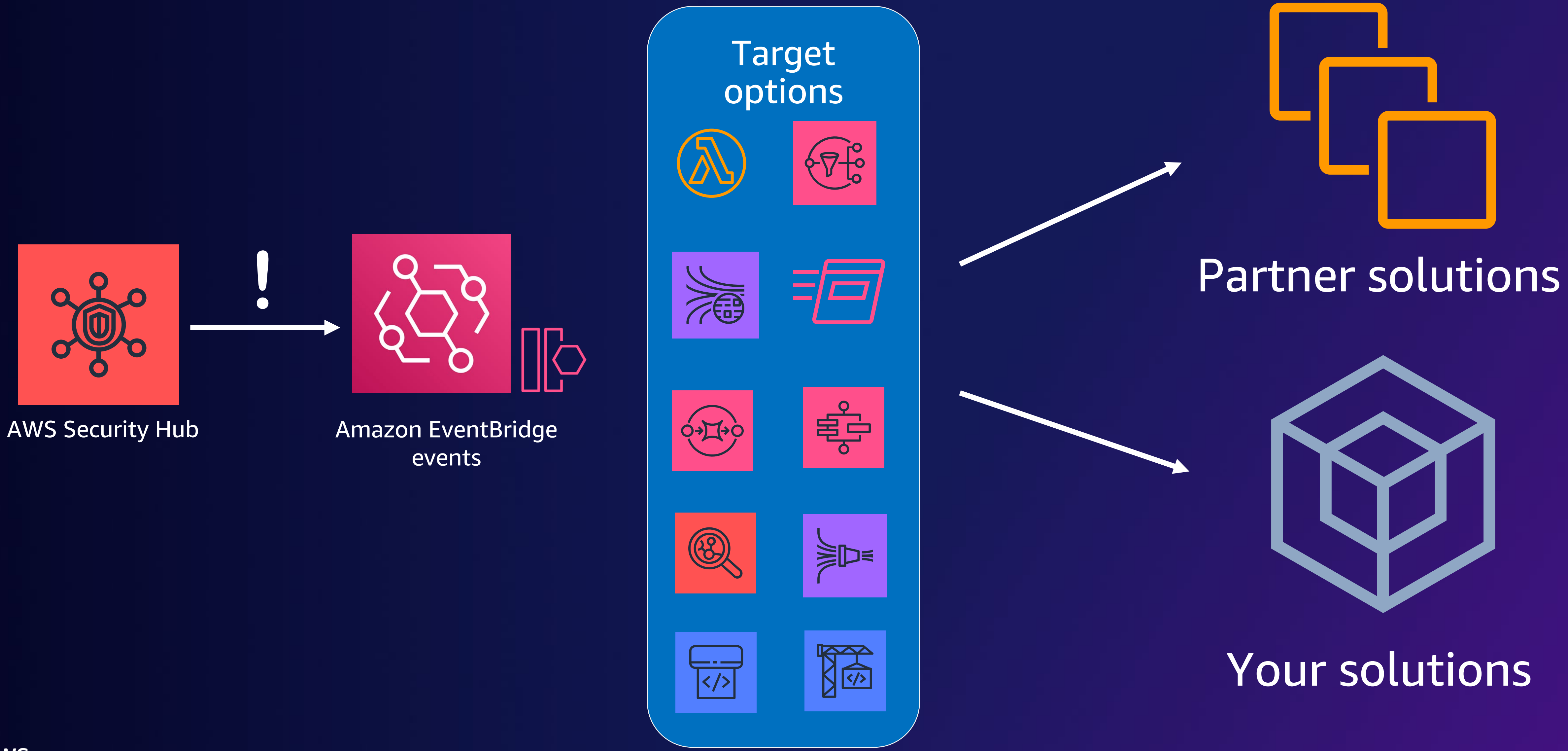
Remediation actions

Findings

Taking action partners

Plus many others…

Taking action with Security Hub



AWS Security Hub

!

Amazon EventBridge events

Target options

Partner solutions

Your solutions

Workshop details

High-level view of the workshop

Module 1 - Tour of Security Hub – 15 min

Module 2 - Create custom insights and custom findings – 25 min

Identify non-compliant instances by using AWS Config rules

Create and visualize findings in Security Hub

Module 3 - Implement custom actions and remediation – 25 min

Use custom AWS Lambda function to isolate an Amazon Elastic Compute Cloud (EC2) instance

Deploy remediation playbooks for CIS benchmarks

Module 4 - Implement finding enrichment and notification – 25 min

Use custom action to add Amazon EC2 tags to finding notes

Post Security Hub findings into Slack

Logistics for this workshop training

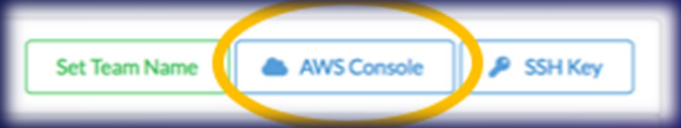
Workshop guide:

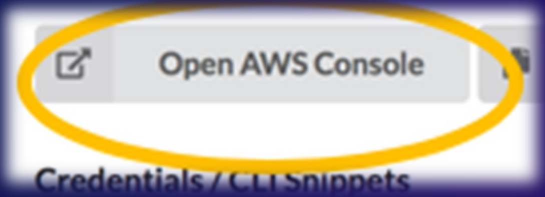
https://catalog.workshops.aws/security-hub

Workshop AWS account:

Event Engine Hash

1. Go to https://dashboard.eventengine.run
2. Enter Event Hash
3. Click AWS Console
4. Click Open AWS Console





Thank you!

Nicholas Jaeger

https://www.linkedin.com/in/nickjaeger/

Please complete the session survey