AWS Threat Detection & Incident Response Workshop

Nicholas Jaeger
Enterprise Solutions Architect
Security Technical Field Community
jaegernj@amazon.com

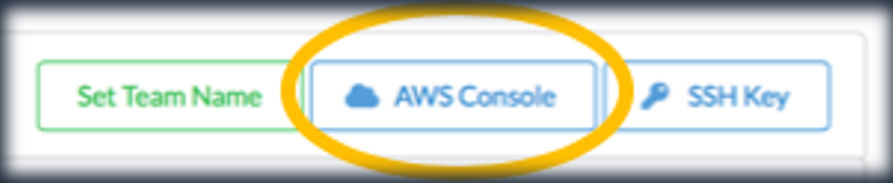
Agenda

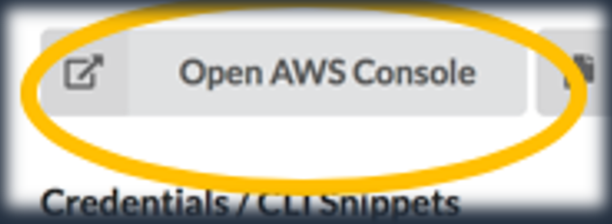
1. Lab Environment Access
2. AWS Security Services
3. Workshop Architecture
4. Scenarios
5. Q&A

Workshop Setup - Account Access

**Use US West
(Oregon)
us-west-2**

- **https://dashboard.eventengine.run**
- Enter HASH ID (see Chime chat)
- Click AWS Console
- Click Open AWS Console





+1

Use US West (Oregon)
us-west-2

Run the CloudFormation Template

Modules/Scenarios

1. Explore AWS Security Hub
2. Creating an Integration for Security Alerts (EventBridge & Lambda)
3. Investigating Misconfigured Resources (Config)
4. Identifying Public Resources (IAM Access Analyzer)
5. Automating Remediation (Security Hub, EventBridge & Lambda)
6. Investigating a Threat (GuardDuty & Detective)

AWS security, identity, and compliance solutions

Identity and access management

- **AWS Identity and Access Management (IAM)**
- AWS Single Sign-On
- AWS Organizations
- AWS Directory Service
- Amazon Cognito
- AWS Resource Access Manager

Detective controls

- **AWS Security Hub**
- **Amazon GuardDuty**
- Amazon Inspector
- **Amazon CloudWatch**
- **AWS Config**
- AWS CloudTrail
- VPC Flow Logs
- AWS IoT Device Defender

Infrastructure protection

- AWS Firewall Manager
- AWS Network Firewall
- AWS Shield
- AWS WAF – Web application firewall
- Amazon Virtual Private Cloud
- AWS PrivateLink
- AWS Systems Manager

Data protection

- Amazon Macie
- AWS Key Management Service (KMS)
- AWS CloudHSM
- AWS Certificate Manager
- AWS Secrets Manager
- AWS VPN
- Server-Side Encryption

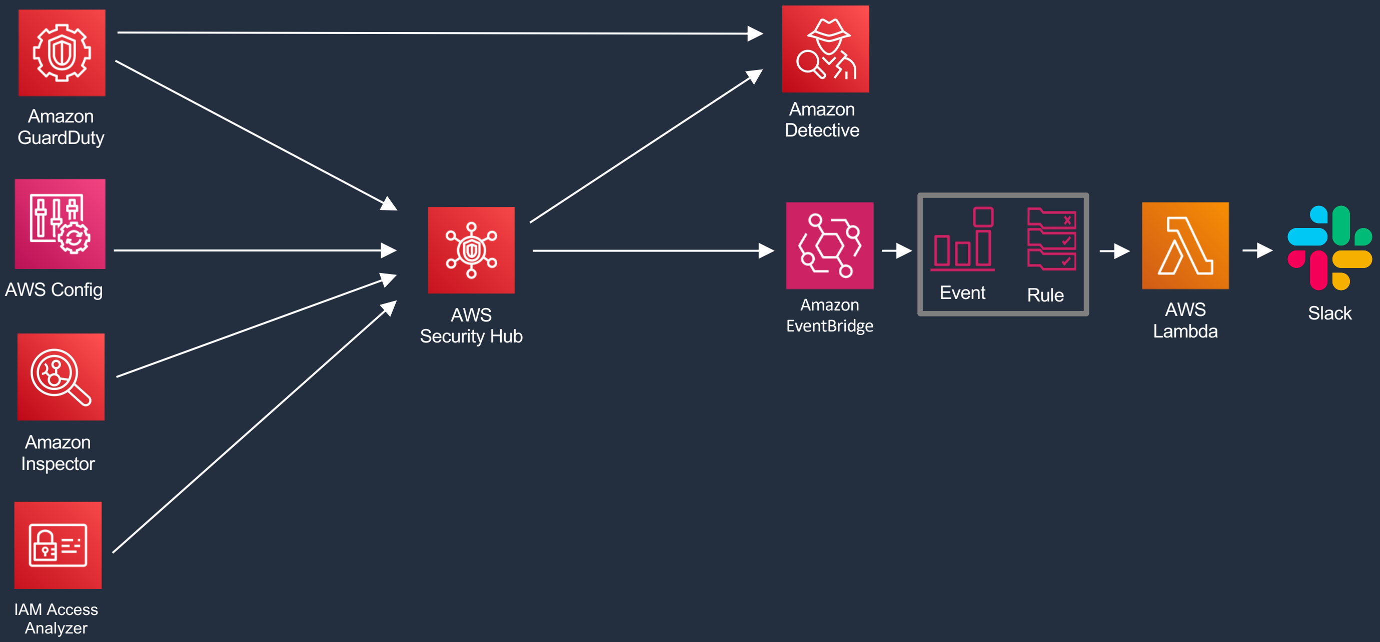
Incident response

- **Amazon Detective**
- CloudEndure DR
- **AWS Config Rules**
- **AWS Lambda**

Compliance

- AWS Artifact
- AWS Audit Manager

Workshop Architecture



Questions?