## re:Invent

NOV. 28 - DEC. 2, 2022 | LAS VEGAS, NV

**SEC301-R** 

# Threat detection and response workshop

Nicholas Jaeger (he/him)

Sr. Security Specialist SA, AWS WWSO Amazon Web Services

Ajit Puthiyavettle (he/him)

Sr. Solutions Architect, AWS WWCS
Amazon Web Services



## Use AWS services to secure your cloud environment and achieve operational excellence



Centralize threat detection and monitoring

Improve security posture assessment

Optimize vulnerability management

Streamline root cause analysis

Improve sensitive data discovery

Initiate and route workflows to existing systems

Prioritize critical findings

Automate remediation

Scale deployments

### **Amazon GuardDuty: How it works**



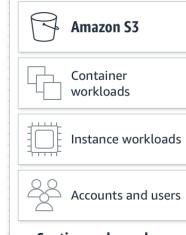
#### **Amazon GuardDuty**

A threat detection service that continuously monitors for malicious activity and anomalous behavior



#### **Activate GuardDuty**

With a few clicks in the console, monitor all your AWS accounts without additional software to deploy or manage



#### Continuously analyze

Automatically and continuously monitor AWS workloads and resources for potential threats at scale



#### Intelligently detect threats

GuardDuty uses machine learning, anomaly detection, and integrated threat intelligence to identify and prioritize potential threats

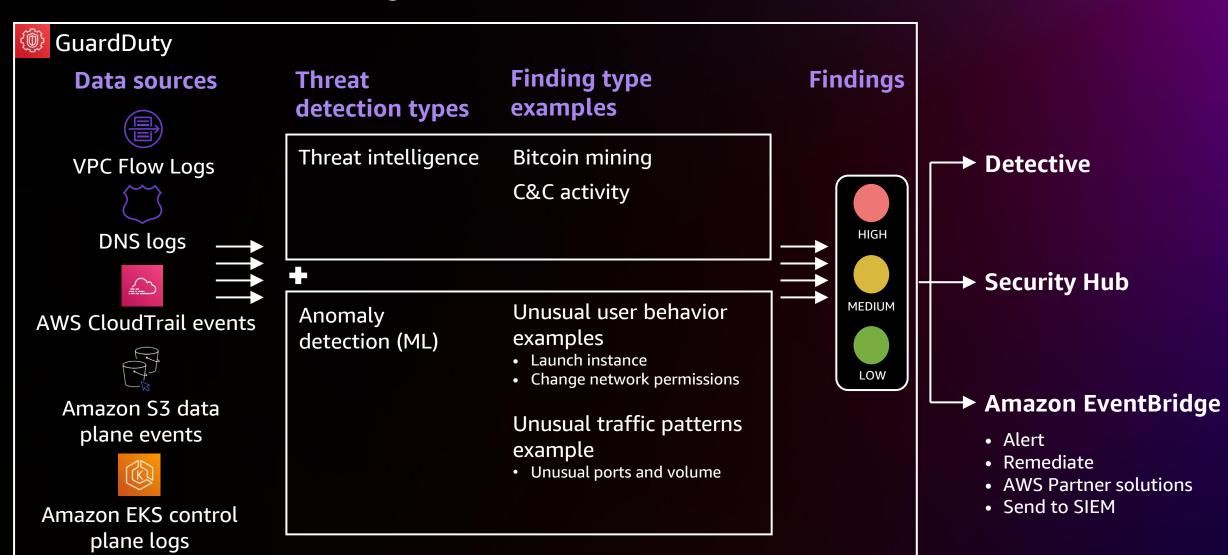


#### Take action

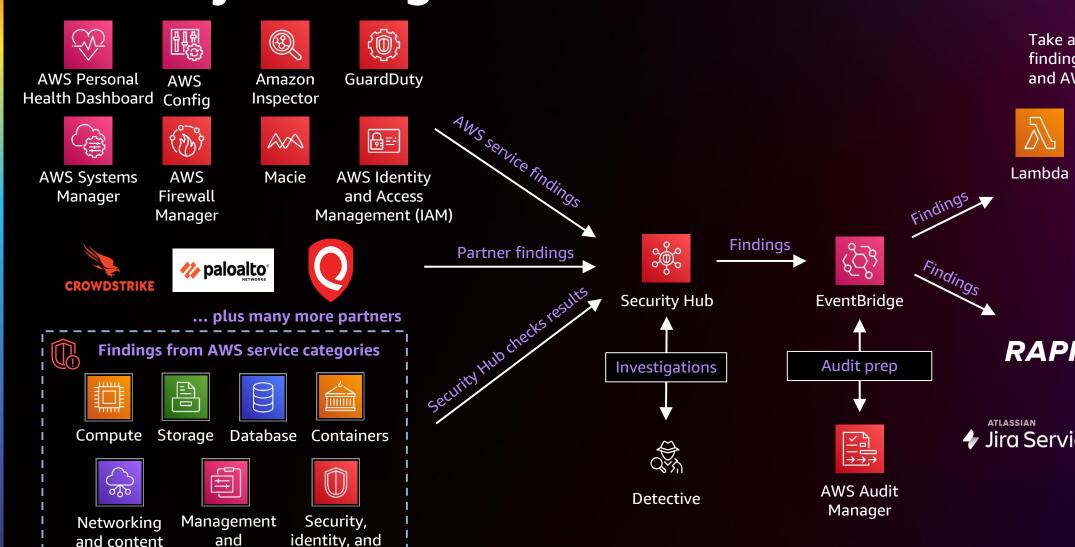
Review detailed findings in the console, integrate into event management or workflow systems, and initiate AWS Lambda for automated remediation or prevention



#### **How GuardDuty works**



#### **Security finding flows**



Take action and remediate findings with AWS services and AWS Partner solutions





**AWS Systems** Manager

**AWS Step Functions** 

**PagerDuty** 





Jira Service Management

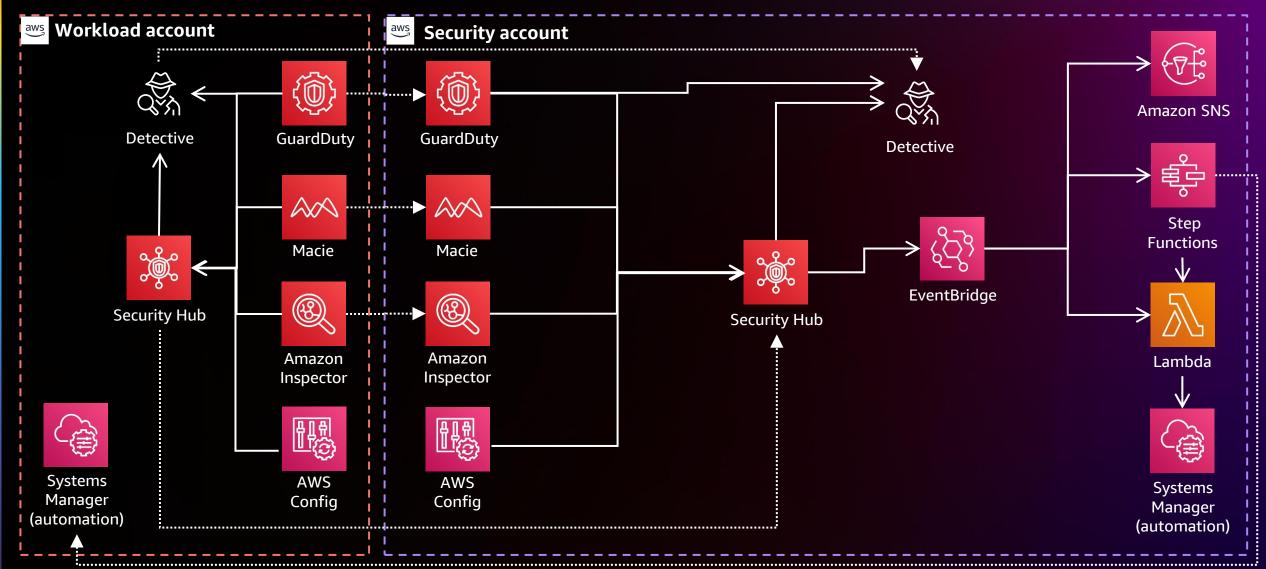
... plus many more partner solutions

delivery

governance

compliance

### Multi-account setup

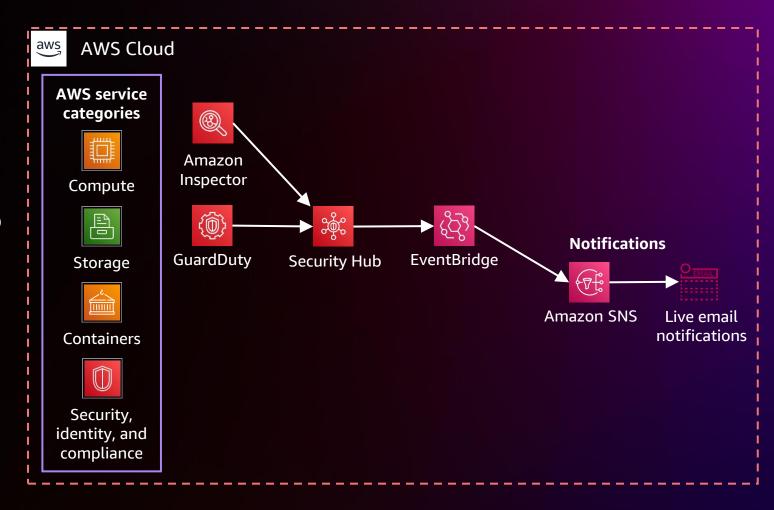


## Workshop details: 11 modules



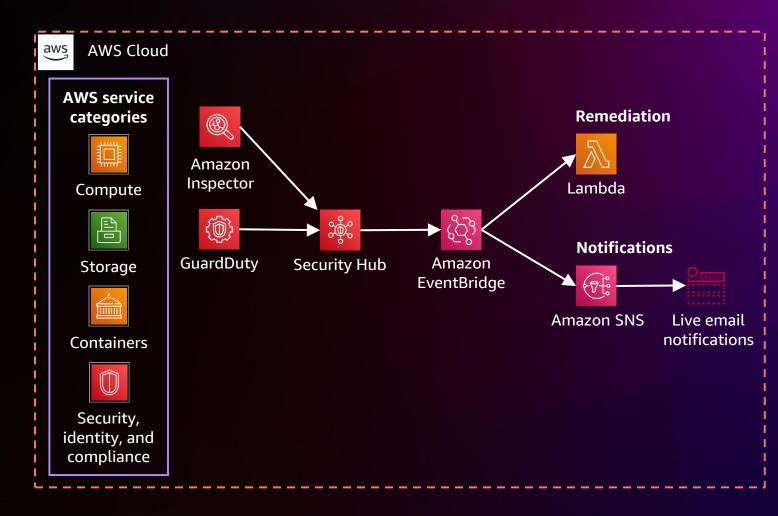
### Workshop overview: Introduction to GuardDuty

- 1. GuardDuty walkthrough
- 2. Understanding a GuardDuty finding
- 3. Suppressing findings
- 4. Building a threat list
- 5. Aggregating findings with Security Hub
- 6. Setting up GuardDuty notifications



## Workshop overview: Threat detection and incident response (TDIR)

- 7. TDIR scenario compromised IAM credentials
- 8. TDIR scenario compromised Amazon EC2 instance
- 9. TDIR scenario compromised Amazon S3 bucket
- 10. TDIR scenario IAM role credential exfiltration
- 11. TDIR scenario Amazon EKS GuardDuty findings remediation



## Workshop logistics

Join the workshop:

https://catalog.workshops.aws/join

Event access code:

c65c-09c388-ba



# Thank you!

Nicholas Jaeger (he/him)
jaegernj@amazon.com
https://www.linkedin.com/in/nickjaeger/

Ajit Puthiyavettle (he/him)
aputhiy@amazon.com
https://www.linkedin.com/in/ajit-puthiyavettle/



Please complete the session survey in the **mobile app** 

