
AWS
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

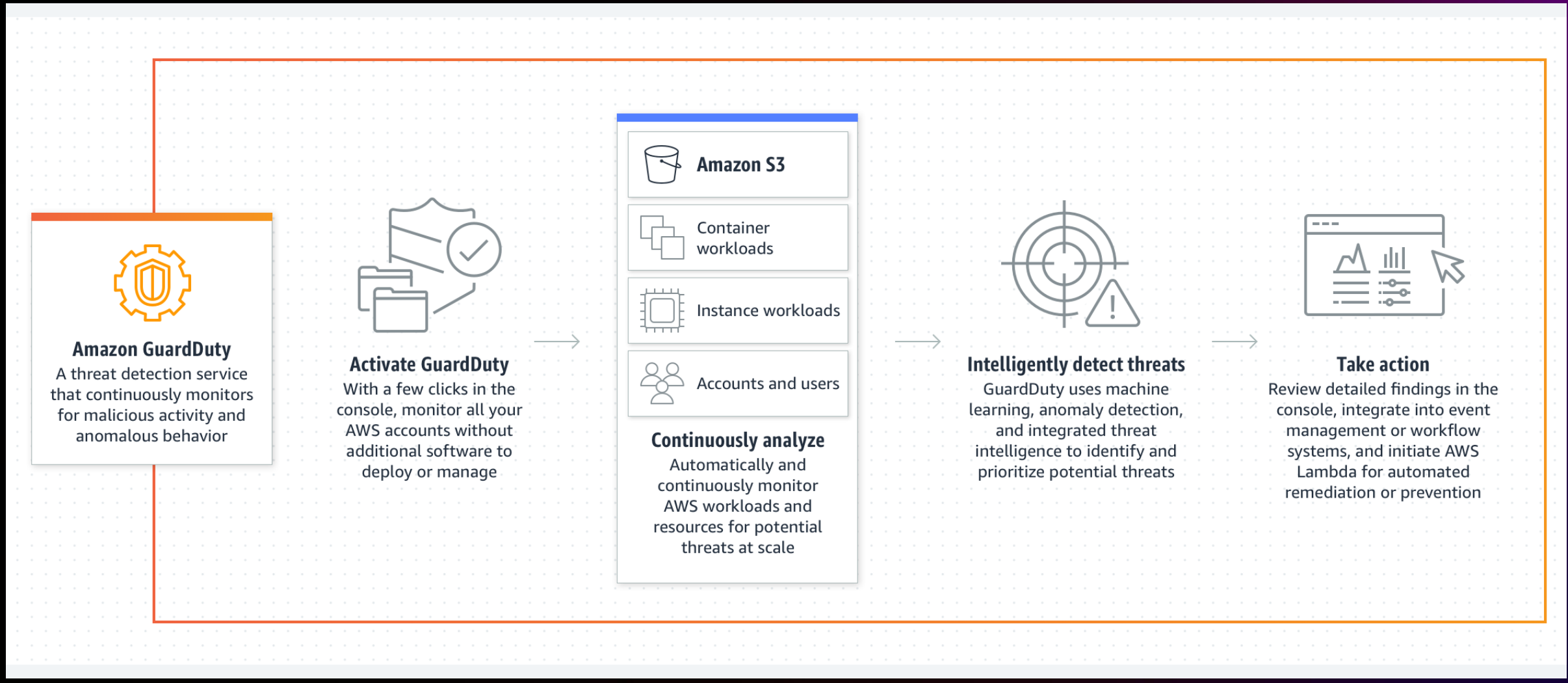
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

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

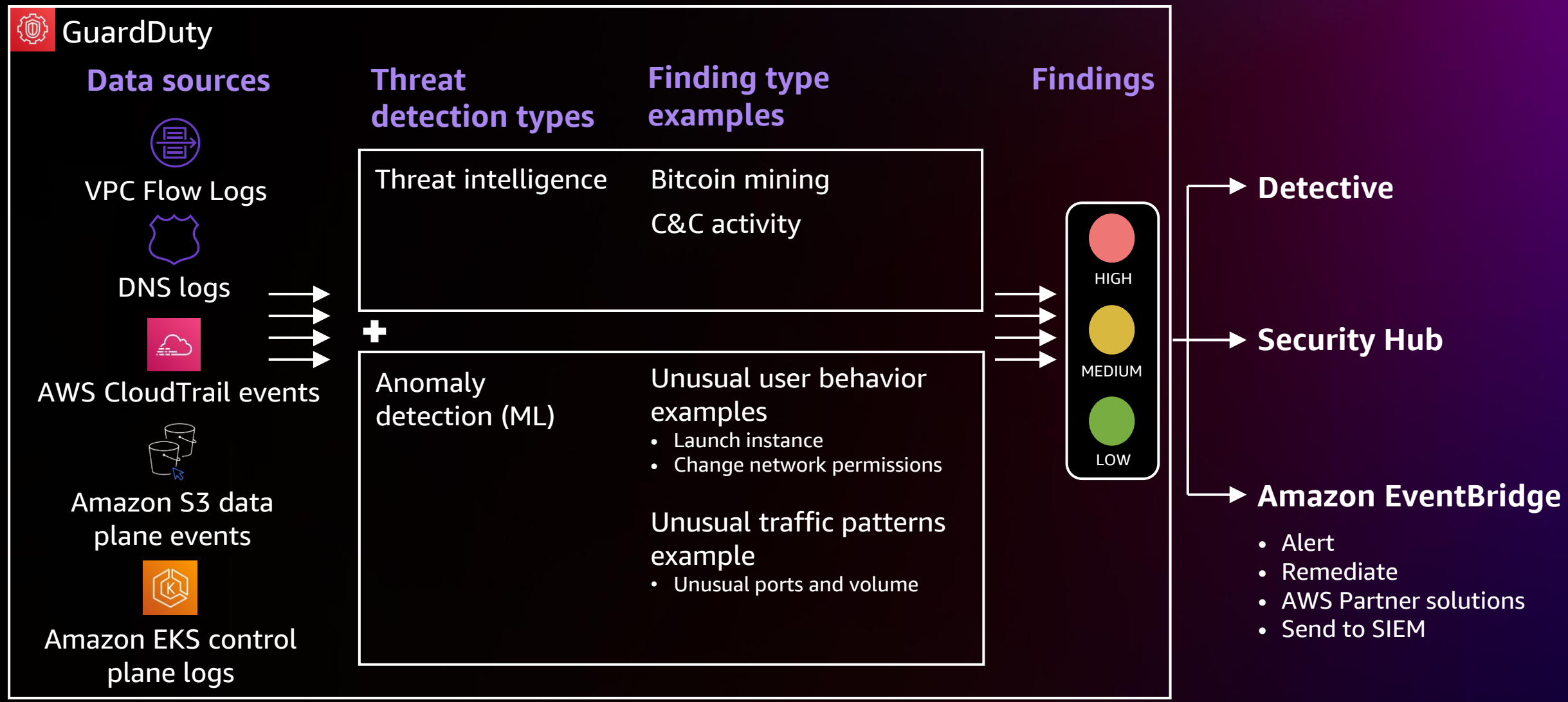
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Amazon GuardDuty: How it works



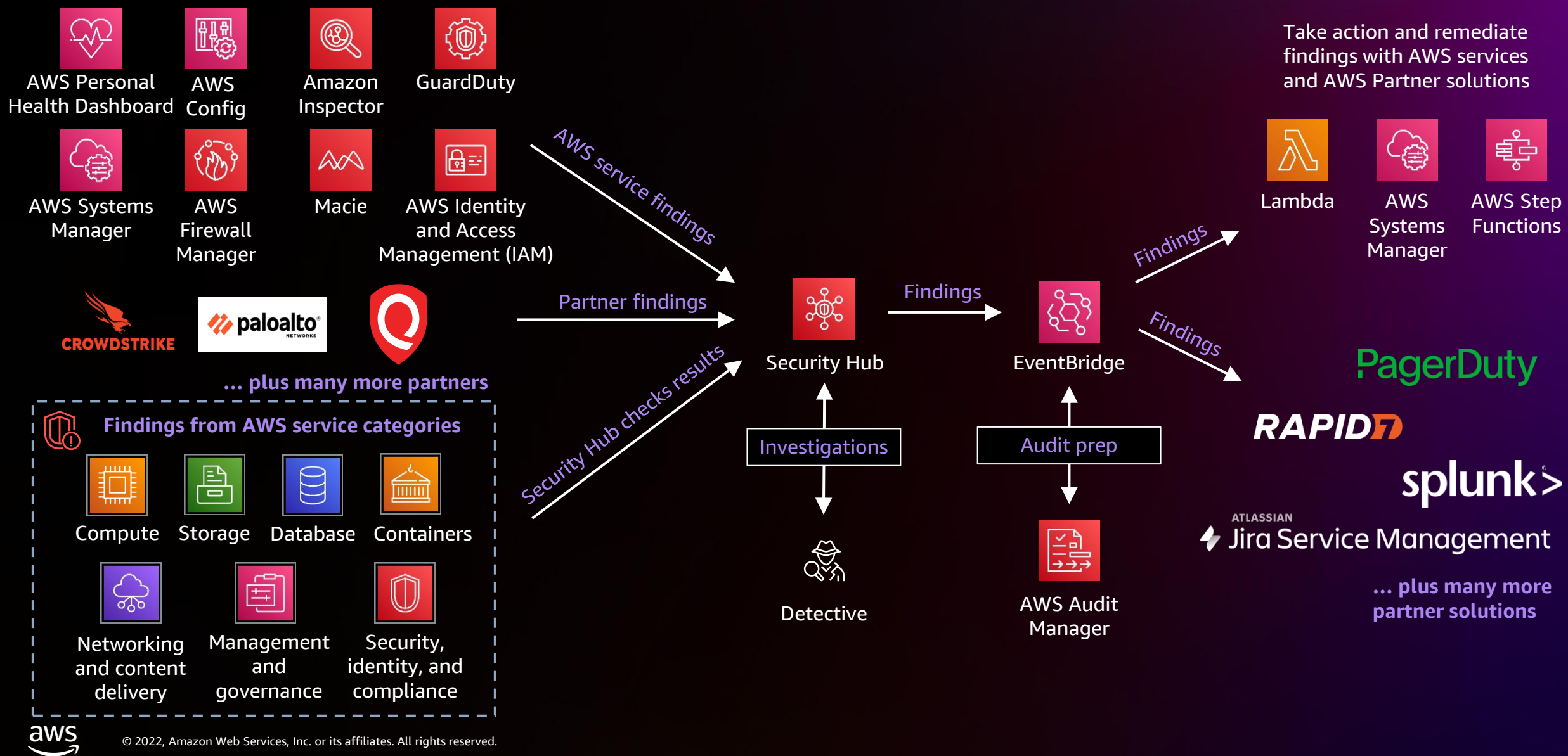
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

How GuardDuty works



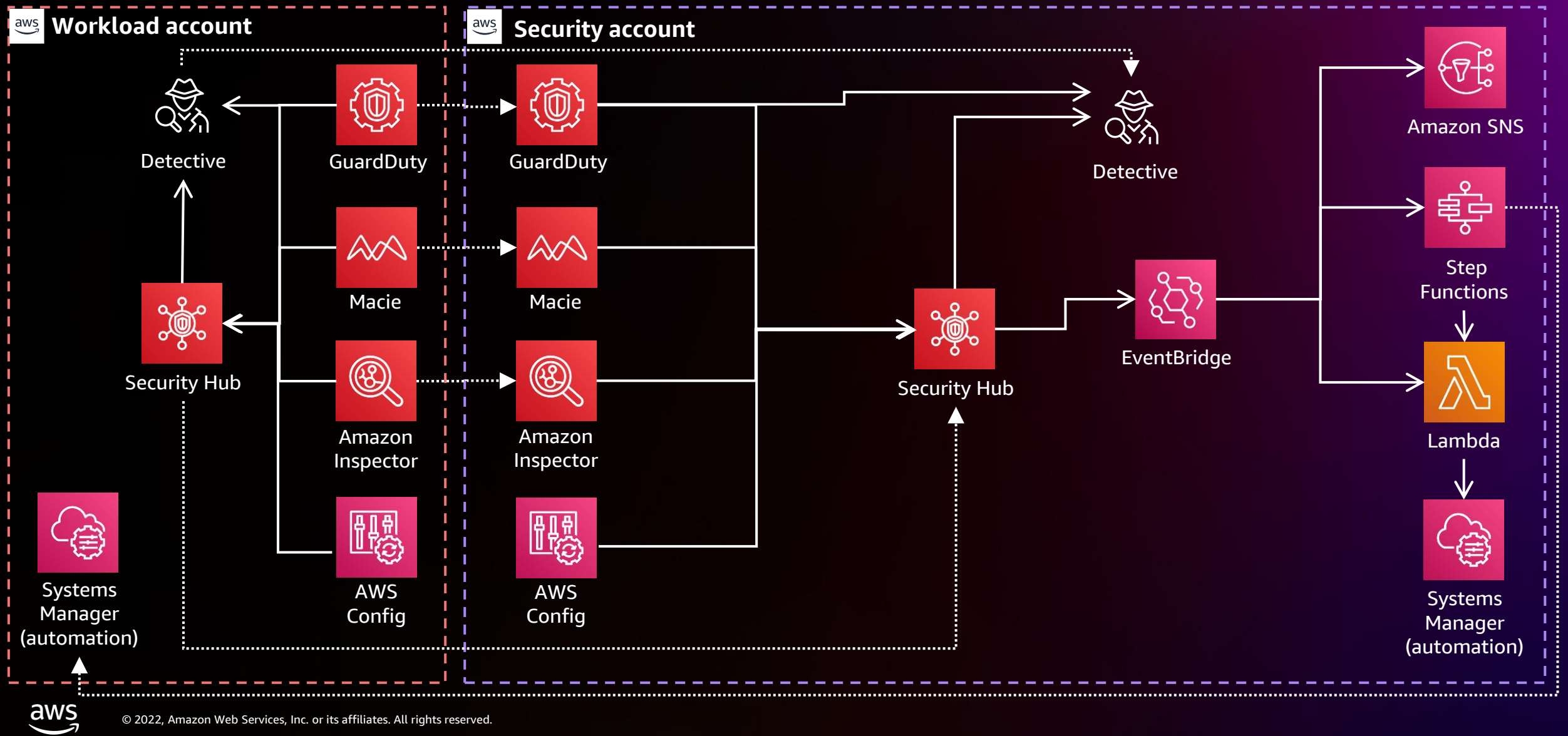
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Security finding flows



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Multi-account setup



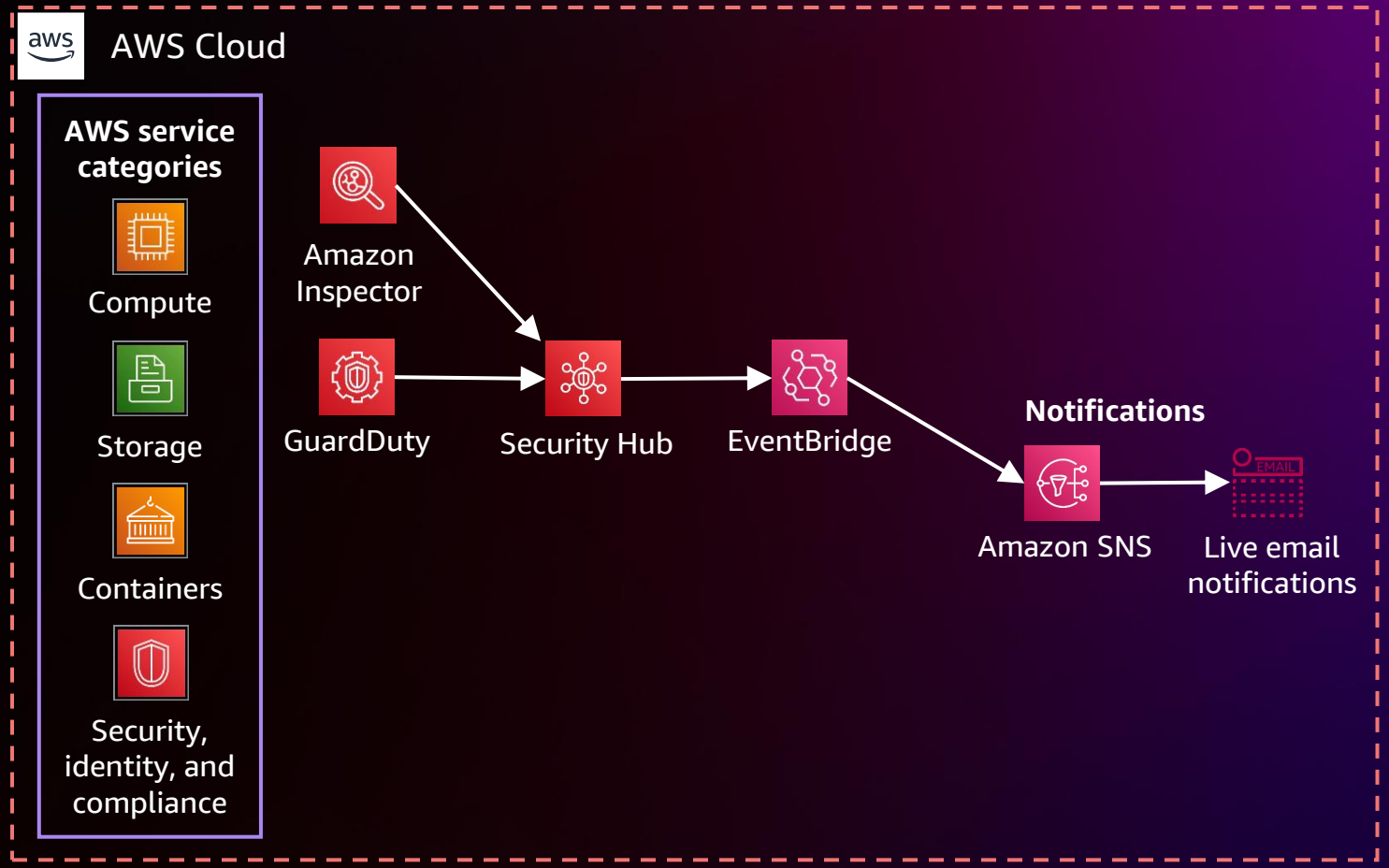
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Workshop details: 11 modules

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Workshop overview: Introduction to GuardDuty

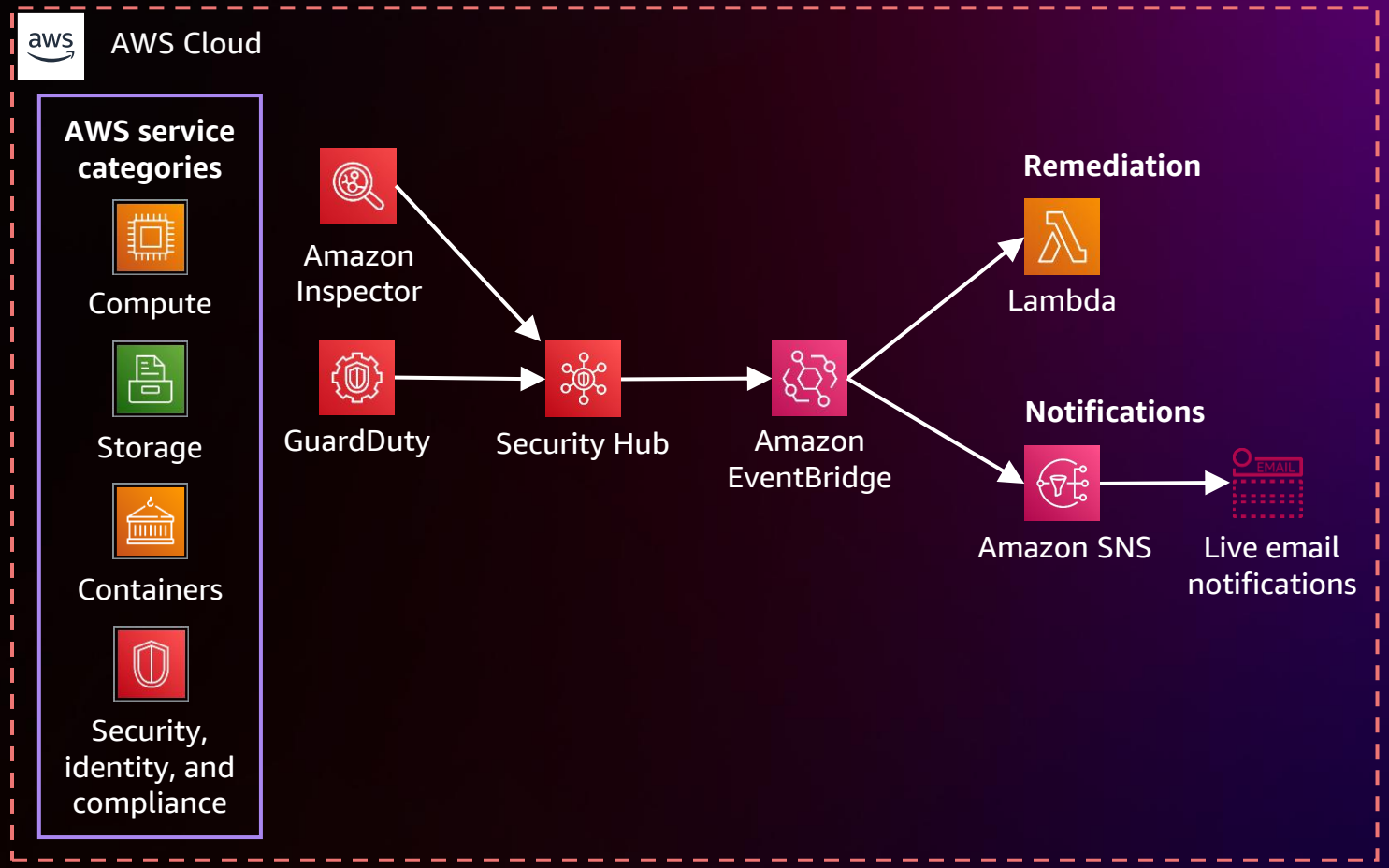
1. GuardDuty walkthrough
2. Understanding a GuardDuty finding
3. Suppressing findings
4. Building a threat list
5. Aggregating findings with Security Hub
6. Setting up GuardDuty notifications



aws
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

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



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Workshop logistics

Join the workshop:

https://catalog.workshops.aws/join

Event access code:

c65c-09c388-ba

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

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**

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.