AWS re:Invent

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

SEC202-R2

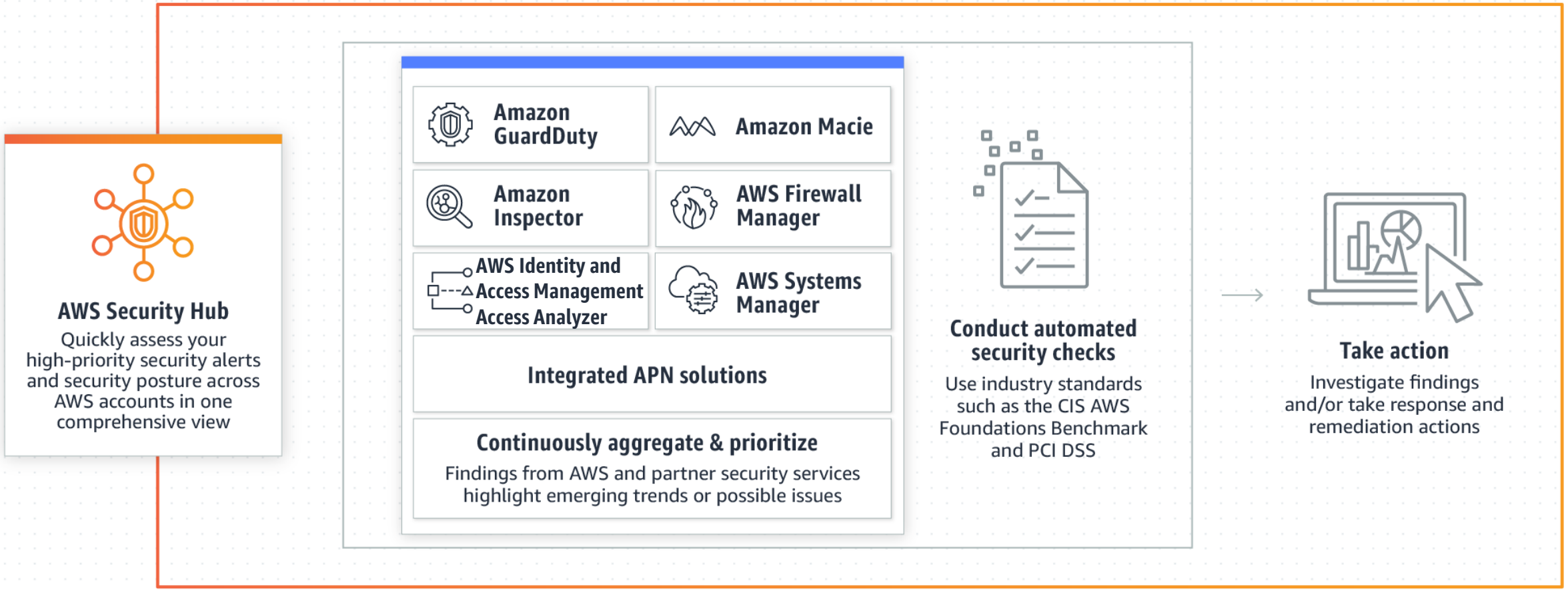
Integration, prioritization, and response with AWS Security Hub

Justin Criswell
Security Solutions Architect
AWS

Nicholas Jaeger
Solutions Architect
AWS

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

Security Hub overview



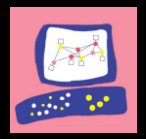
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

AWS Security Hub information flows



And more to come…

AWS service findings





Partner findings

Plus dozens of others…



Plus dozens of others…

Security checks results



AWS Security Hub

Investigations



Amazon Detective

Findings



Findings



Remediation actions

Audit prep



AWS Audit Manager

Findings

Taking action partners

ATLASSIAN

PagerDuty

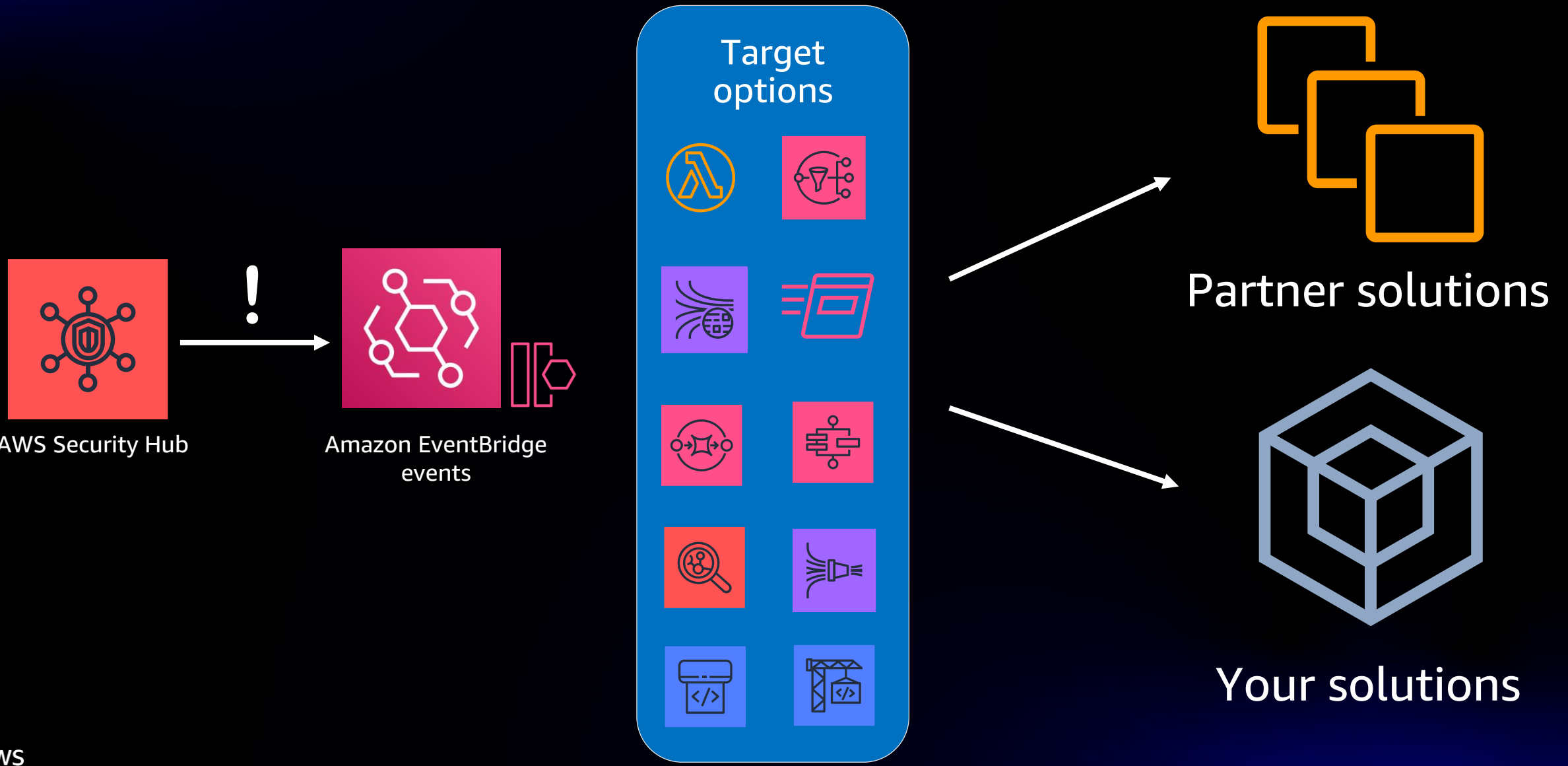
slack

Plus many others…

aws

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

Taking action with Security Hub



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

Workshop details

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

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 (Amazon EC2) instance
- Deploy remediation playbooks for CIS benchmarks

Module 4 - Implement finding enrichment and notification – 25 min

- Post Security Hub findings into Slack
- Use custom action to add Amazon EC2 tags to finding notes

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

Logistics for this workshop training

Tuesday
0b93-1c4f3d4074-10

Workshop guide:
- https://security-hub-workshop.awssecworkshops.com/

Workshop AWS account:
- https://dashboard.eventengine.run
- Enter Event Hash
- Click AWS Console
- Click Open

SSID: @reInventWorkshops
Password: Exper1ment21

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

Thank you!

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