Security Checks for PCI DSS

With AWS Security Hub

Rima Tanash, Security Engineer - AWS Security Hub
Michael Guzman, Consultant - AWS Security Assurance Services
Logan Culotta, Consultant - AWS Security Assurance Services

aws

Agenda

1. AWS Security Hub Overview
2. PCI DSS in Security Hub Deep-Dive
3. Demo
4. Using CLI to Enable and Describe Security Standards and Controls
5. Wrap-Up

aws

AWS Security Hub Overview

Problem statements

Backlog of compliance requirements

1. Many compliance requirements, and not enough time to build the checks

Too many security alert formats

2. Dozens of security tools with different data formats

Too many security alerts

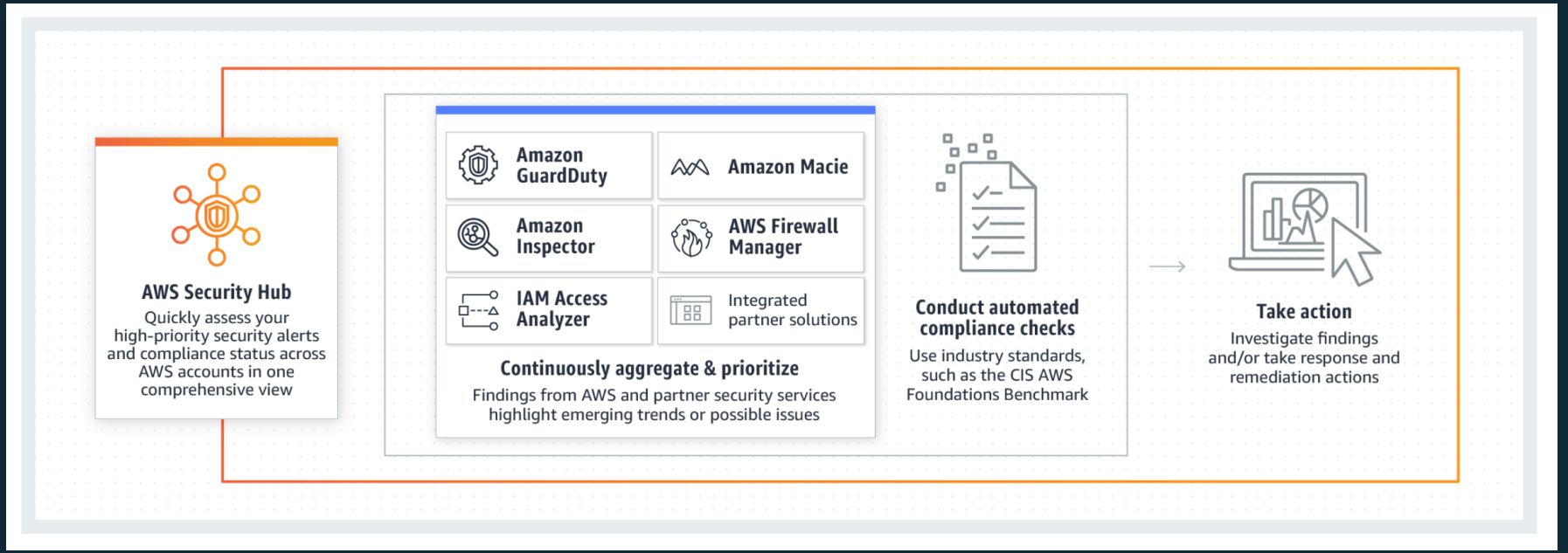
3. Large volume of alerts, and the need to prioritize and take action

Lack of an integrated view

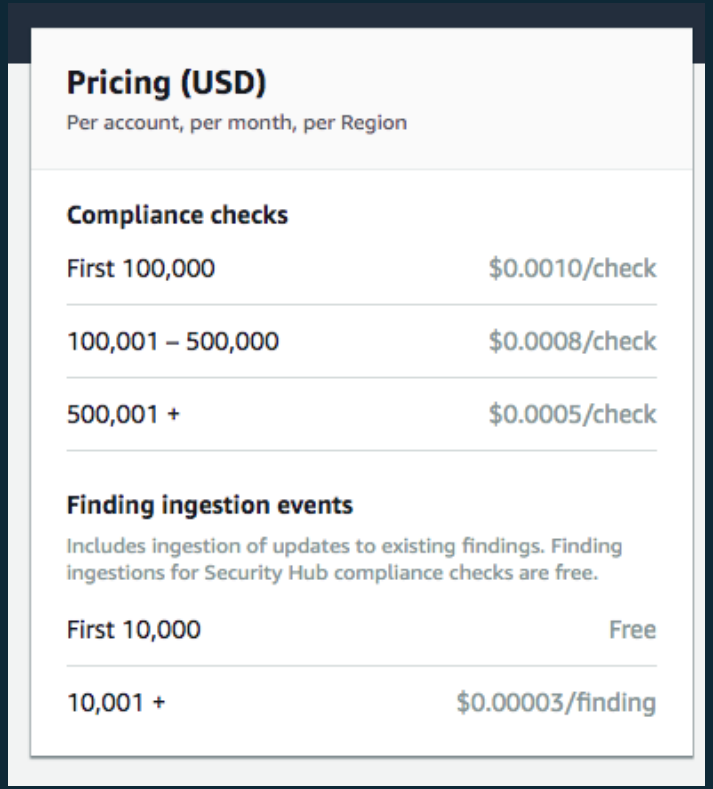
4. Lack of an integrated view of security and compliance across accounts

aws

AWS Security Hub overview



Rollout plans and pricing



Pricing (USD)

Per account, per month, per Region

Compliance checks

First 100,000	$0.0010/check
100,001 – 500,000	$0.0008/check
500,001 +	$0.0005/check

Finding ingestion events

Includes ingestion of updates to existing findings. Finding ingestions for Security Hub compliance checks are free.

First 10,000	Free
10,001 +	$0.00003/finding

30-day free trial

Supported Regions (18)

- Asia Pacific (Hong Kong)
- Asia Pacific (Mumbai)
- Asia Pacific (Seoul)
- Asia Pacific (Singapore)
- Asia Pacific (Sydney)
- Asia Pacific (Tokyo)
- Canada (Central)
- EU (Frankfurt
- EU (Ireland)
- EU (London)
- EU (Paris)
- EU (Stockholm)
- Middle East (Bahrain)
- South America (Sao Paulo)
- US East (N. Virginia)
- US East (Ohio)
- US West (N. California)
- US West (Oregon)

aws

Partner integrations (41 total external partners)

Forwarding findings into AWS Security Hub

Firewalls

SOPHOS Security made simple. · f5 · paloalto NETWORKS · Barracuda · imperva · Check Point SOFTWARE TECHNOLOGIES LTD.

Vulnerability

tenable · Qualys. Continuous Security · RAPID7 insightVM

Endpoint

CROWDSTRIKE · Symantec. · aqua · Twistlock

Compliance

turbot · paloalto NETWORKS · McAfee Together is power. · Check Point SOFTWARE TECHNOLOGIES LTD. · Cloud Custodian

MSSP

ARMOR CLOUD SECURITY. UNCOMPROMISED.™ · ALERT LOGIC

Other

CYBERARK

AWS Security Hub

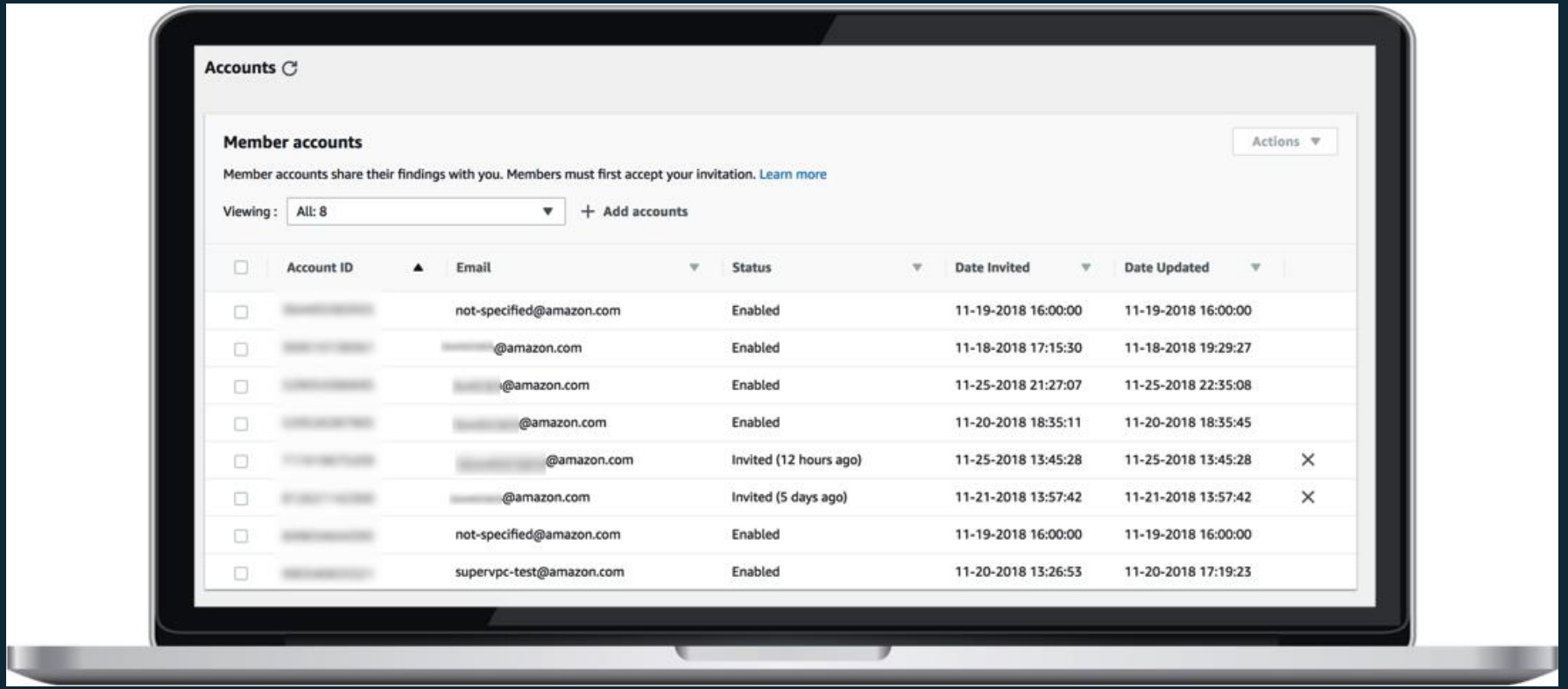
Amazon CloudWatch Events

Event (event-based)

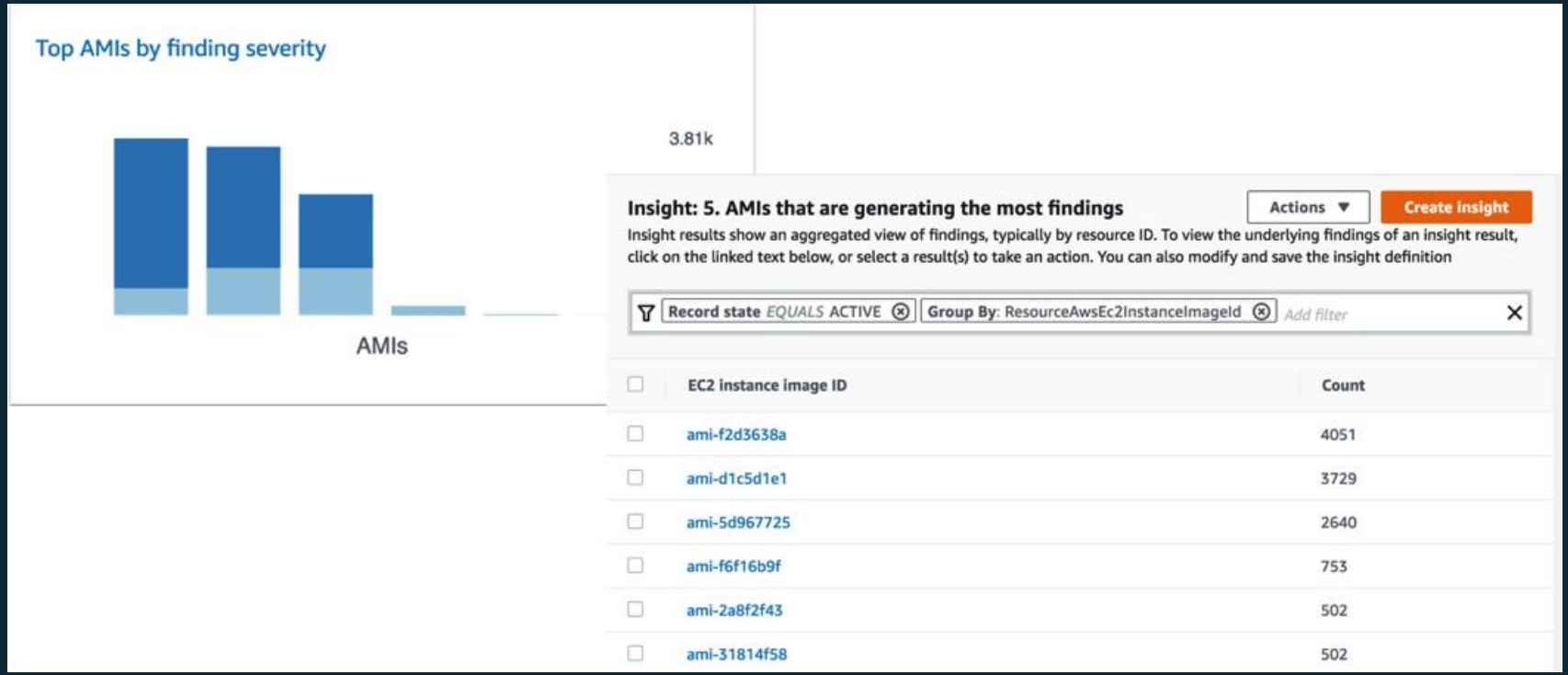
"Taking Action"

servicenow · DEMISTO A PALO ALTO NETWORKS COMPANY · ATLASSIAN · RAPID7 insightConnect · pagerduty · splunk> phantom · IBM Security · splunk> · sumologic · slack · Cloud Custodian

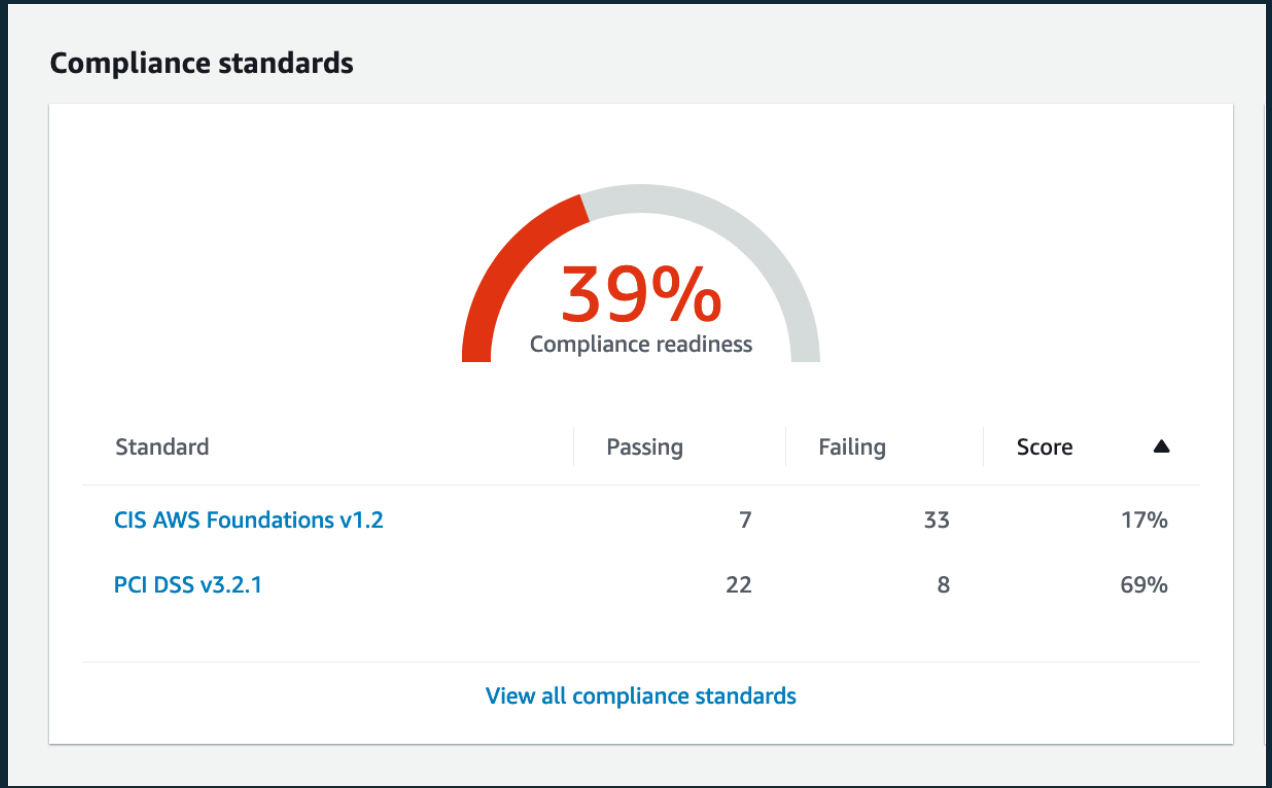
Setup and multi-account



Insights



Standards



PCI DSS 3.2.1 History

PCI Data Security Standard – High Level Overview

Build and Maintain a Secure Network and Systems	1. Install and maintain a firewall configuration to protect cardholder data 2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	3. Protect stored cardholder data 4. Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	5. Protect all systems against malware and regularly update anti-virus software or programs 6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures	7. Restrict access to cardholder data by business need to know 8. Identify and authenticate access to system components 9. Restrict physical access to cardholder data
Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data 11. Regularly test security systems and processes
Maintain an Information Security Policy	12. Maintain a policy that addresses information security for all personnel

aws

AWS SAS ProServe Team

AWS Security Assurance Services, LLC

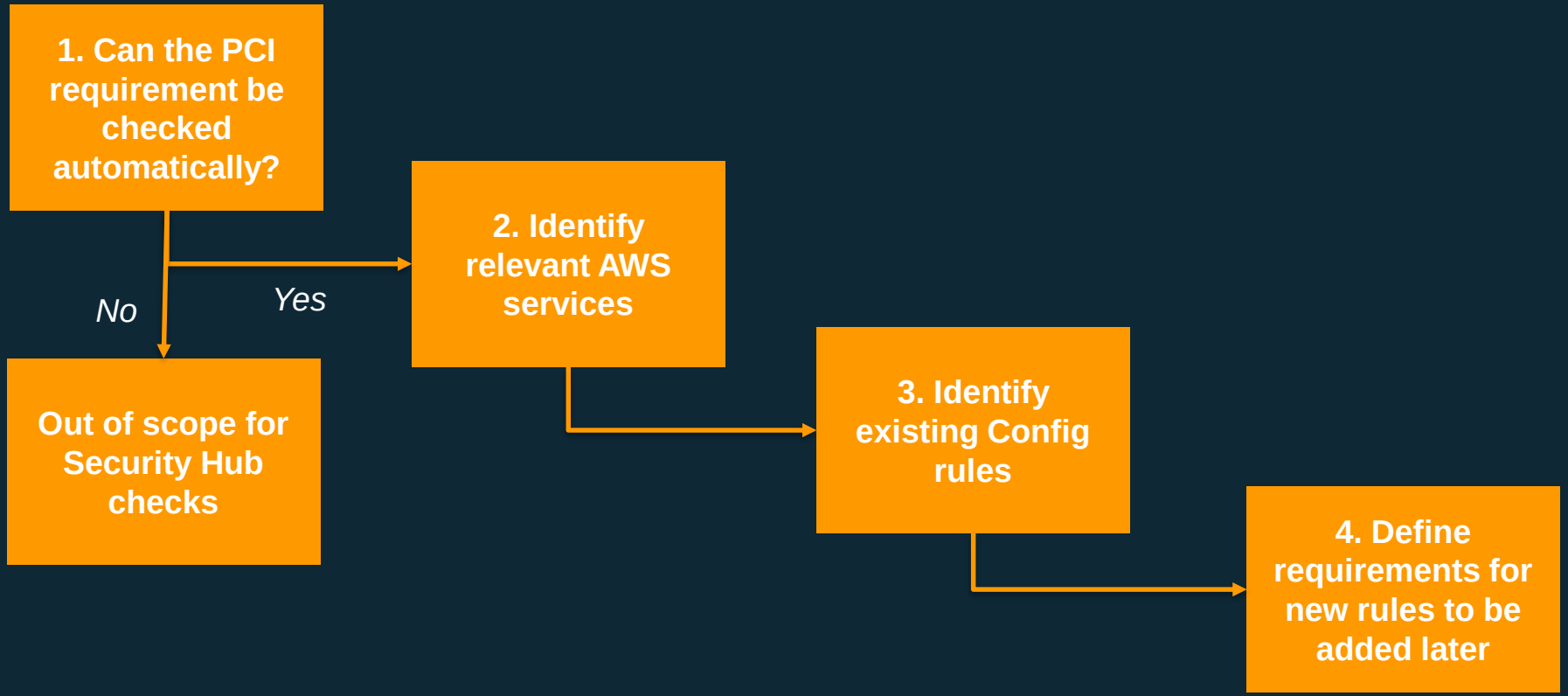
✓ Who we are:

- A PCI DSS Qualified Security Assessor Company (QSAC)
- A wholly owned subsidiary of AWS, positioned as a GSP in the Security & Infrastructure (SRC) group.
- PCI Qualified Security Assessors (QSA's) certified by the PCI SSC
- Launched in July 2018, QSAC in October 2018
- 12 experienced PCI QSA's across the US

https://w.amazon.com/bin/view/AWS/Teams/Proserve/SRC/SAS/

aws

QSA Validation and Input Processes



AWS Security Hub PCI DSS User Guide structure

[PCI.S3.2] S3 buckets should prohibit public read access

Severity: Critical

Resource: S3 bucket

AWS Config rule: `s3-bucket-public-read-prohibited`

This AWS control checks whether your S3 buckets allow public read access by evaluating the Block Public Access settings, the bucket policy, and the bucket access control list (ACL).

Unless you explicitly require everyone on the internet to be able to write to your S3 bucket, you should ensure that your S3 bucket is not publicly writable.

It does not check for read access to the bucket by internal principals, such as IAM roles. You should ensure that access to the bucket is restricted to authorized principals only.

Remediation

To remove public access for an S3 bucket

1. Open the Amazon S3 console at https://console.aws.amazon.com/s3/.
2. Choose the name of the bucket identified in the finding.
3. Choose **Permissions** and then choose **Public access settings**.
4. Choose **Edit**, select all four options, and then choose **Save**.
5. If prompted, enter `confirm` and then choose **Confirm**.

Related PCI DSS Requirements

This AWS control is related to the following PCI DSS requirements:

PCI DSS 1.2.1: Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment, and specifically deny all other traffic.

If you use an S3 bucket to store cardholder data, the bucket should prohibit public read access. Public read access might violate the requirement to allow only necessary traffic to and from the CDE.

PCI DSS 1.3.1: Implement a DMZ to limit inbound traffic to only system components that provide authorized publicly accessible services, protocols, and ports.

If you use an S3 bucket to store cardholder data, the bucket should prohibit public read access. Public read access might violate the requirement to limit inbound traffic to only system components that provide authorized publicly accessible services, protocols, and ports.

PCI DSS 1.3.2: Limit inbound Internet traffic to IP addresses within the DMZ.

If you use an S3 bucket to store cardholder data, the bucket should prohibit public read access. Public read access might violate the requirement to limit inbound Internet traffic to IP addresses within the DMZ.

PCI DSS 1.3.6: Place system components that store cardholder data (such as a database) in an internal network zone, segregated from the DMZ and other untrusted networks.

If you use an S3 bucket to store cardholder data, the bucket should prohibit public read access. Public read access might violate the requirement to place system components that store cardholder data in an internal network zone, segregated from the DMZ and other untrusted networks.

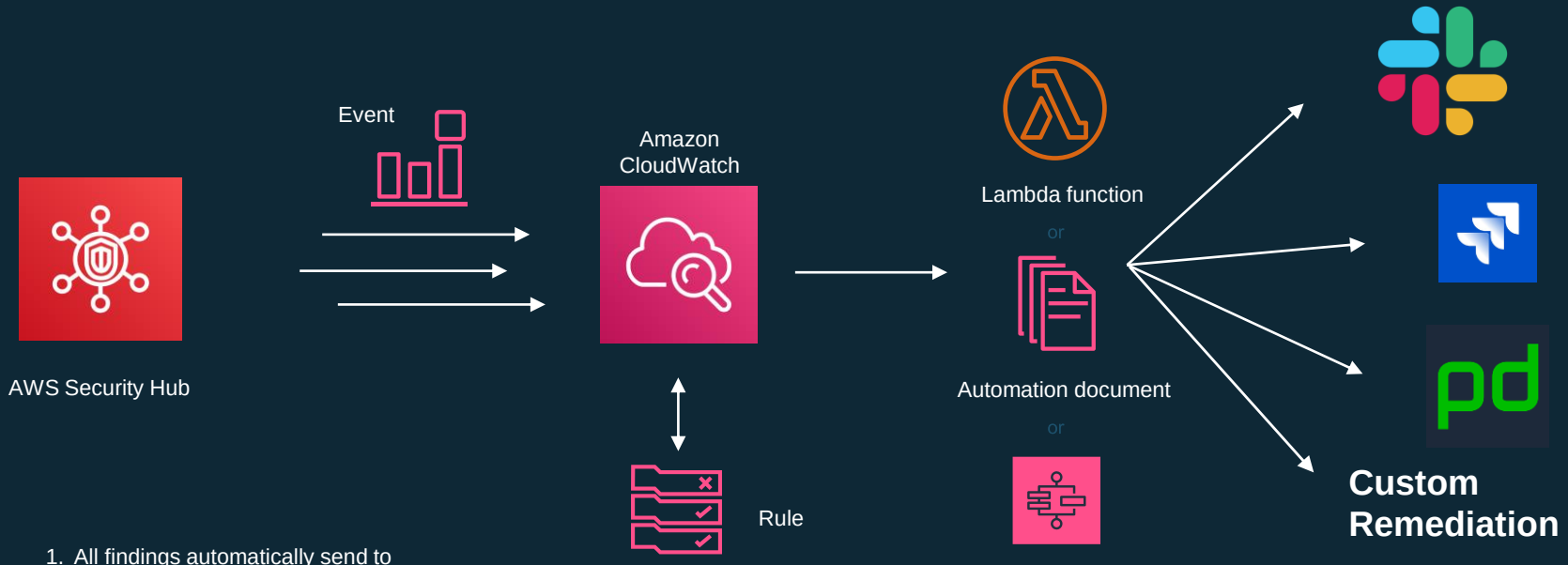
PCI DSS 7.2.1: Establish an access control system(s) for systems components that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed. This access control system(s) must include the following: Coverage of all system components.

If you use an S3 bucket to store cardholder data, the bucket should prohibit public read access. Public read access might violate the requirement to ensure access to systems components is restricted to least privilege necessary, or a user's need to know.

aws

Demo

Customizable response and remediation actions



1. All findings automatically send to CloudWatch events, **and**
2. Security Hub user can select findings in the console and take a custom action on them. These findings are sent to CloudWatch decorated with a custom action ID

3. User creates Amazon CloudWatch Events rules to look for certain findings associated with a custom action ID or findings with specific characteristics.

4. The rule defines a target, typically a Lambda function, Step Function, or Automation document

5. The target could be things like a chat, ticketing, on-call management, SOAR platform, or custom remediation playbook

Additional Resources for Remediation

Webinars and videos:

- Taking Action on Security Hub findings (with customer use cases presented by Northwestern Mutual and HERE)
- Security Hub best practices
- Remediating GuardDuty and Security Hub findings

Blog posts:

- Automated response and remediation with Security Hub
- Getting started with security response automation

aws

Demo - CLI

Wrap-Up