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

PRT328

SPONSORED BY CROWDSTRIKE

3 steps to help mitigate cloud risks with CrowdStrike and AWS

Justin Harris

Solutions Architect
CrowdStrike

Sameer Vasanthapuram

Principal Product Manager
CrowdStrike

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

Agenda

Challenges for security teams

Cloud-native applications

Shifting security left

Securing clouds and runtimes

APIs and orchestration

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

The asks of security teams



Speed



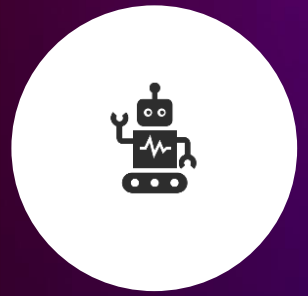
Visibility



Security posture



Runtime protection



Automation

Collaborative security

Cloud-native applications

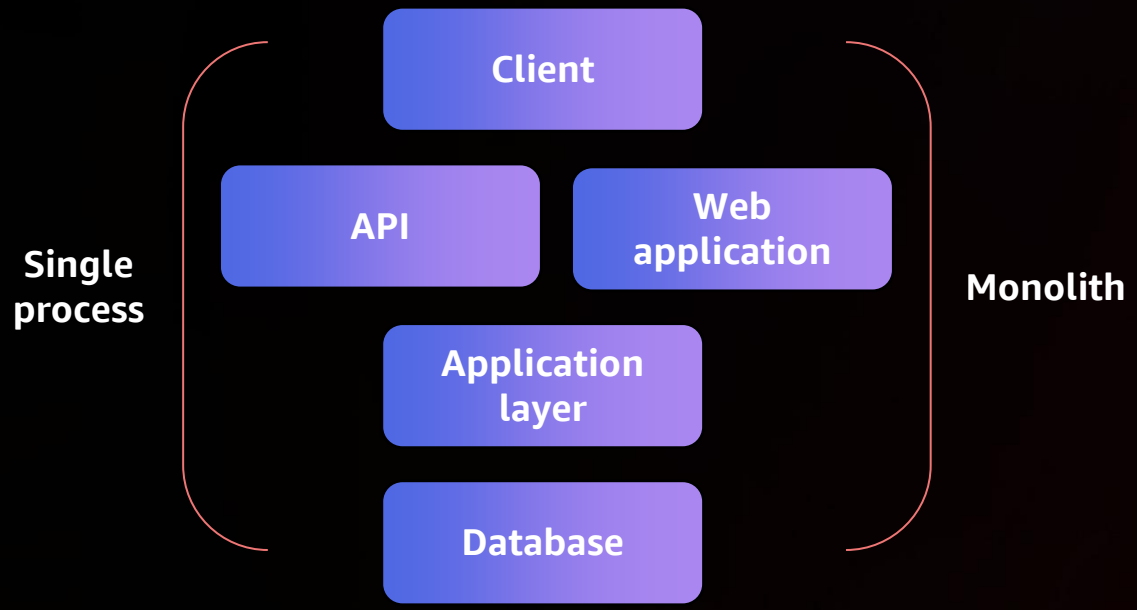
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Cloud-native applications

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

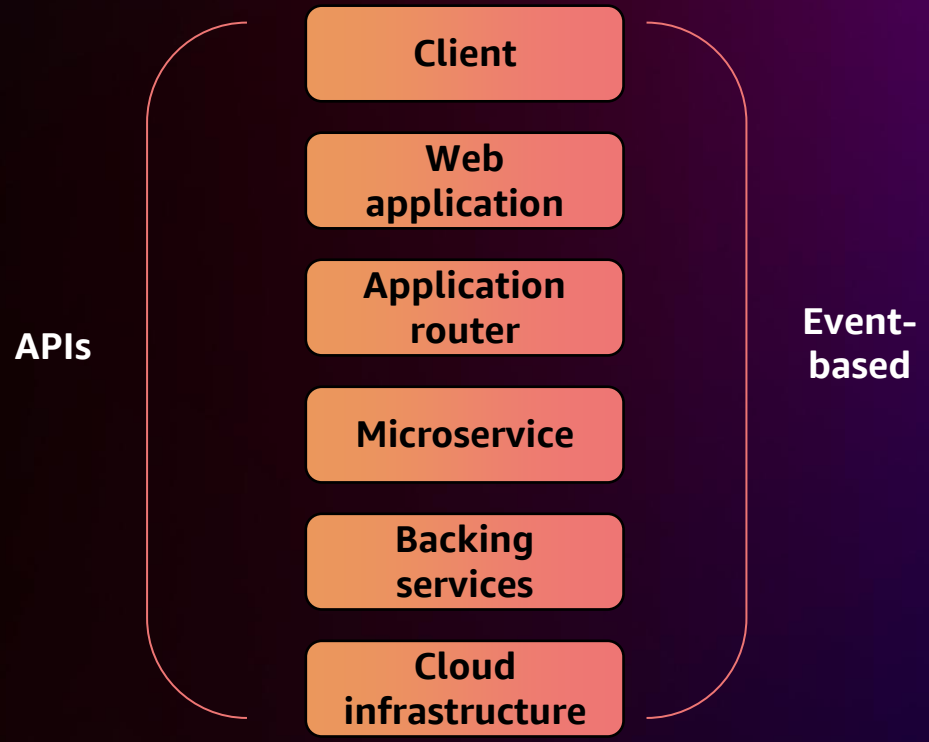
Cloud-native applications

Three-tier web app



Single large team

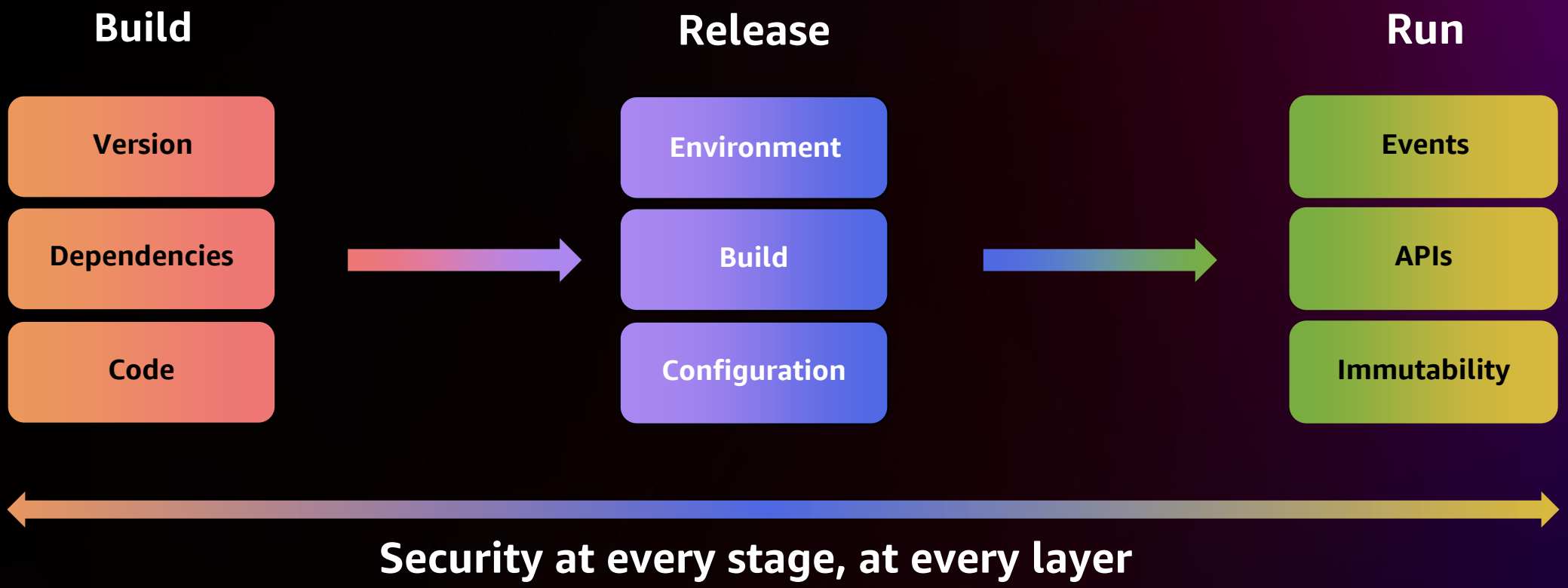
Cloud-native applications



Multiple two-pizza teams

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

Cloud-native applications: Lifecycle

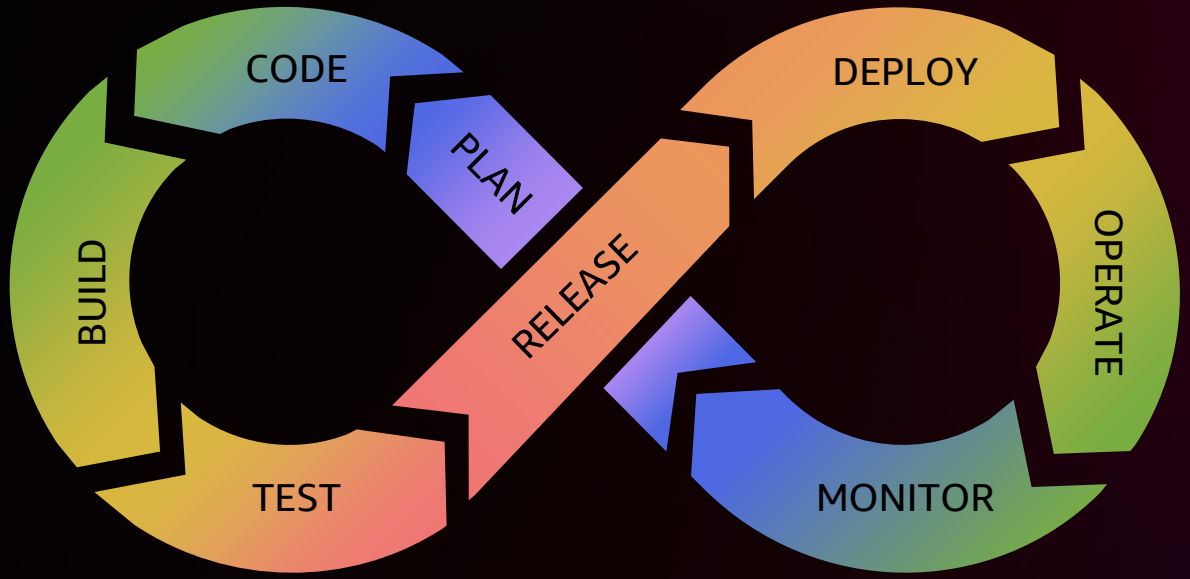


aws
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Securing cloud-native applications at scale

Codebase per application, built to be continuously delivered

Hundreds of deploys across applications, every day



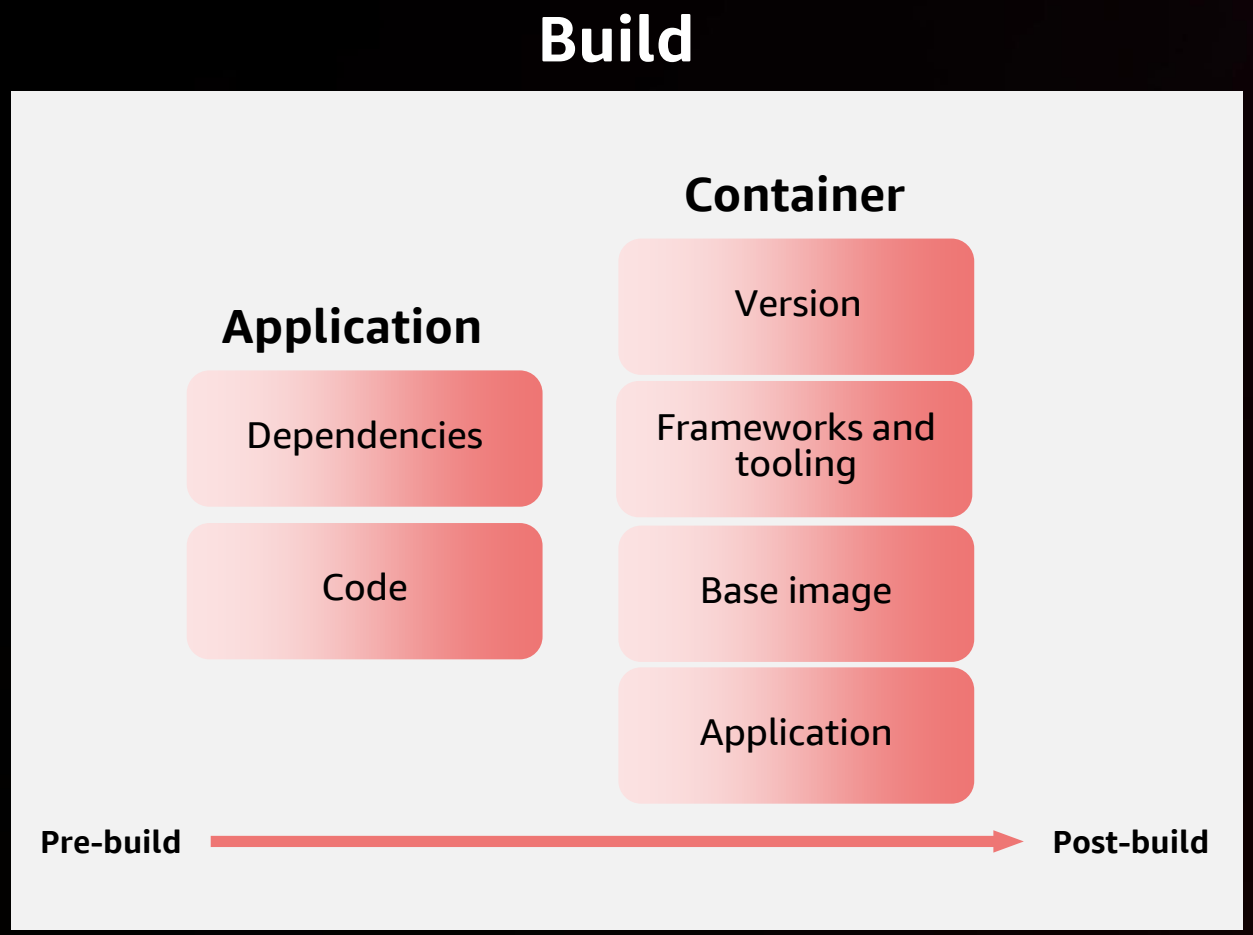
Running on cloud with thousands of containers

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

Security best practices: Build to run

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

Security in the build room



Security shifts left

Layer security controls

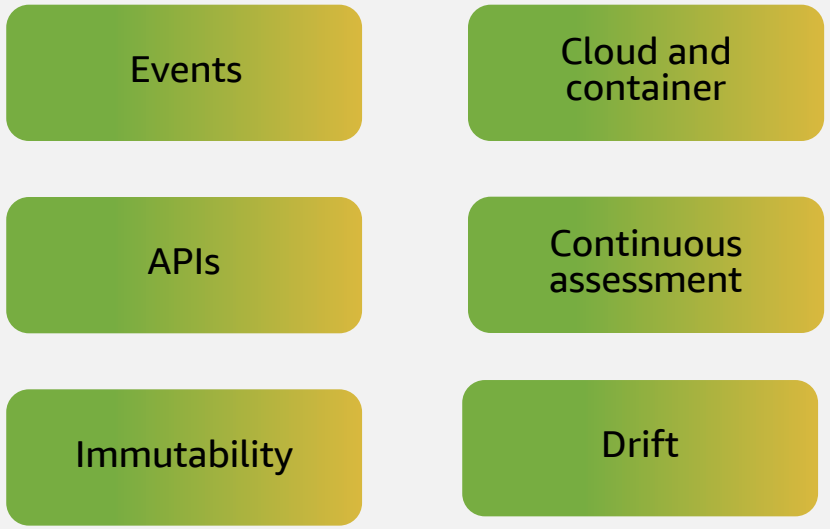
- Identify all repositories, code bases
- Software packages and dependencies
- Scan for risks, exposure, and vulnerabilities

Empower developers to build securely

- Framework for pre-build to post-build security
- Tooling to help developers
- Scan and audit across deployments to promote

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

Runtime security at the speed of the cloud



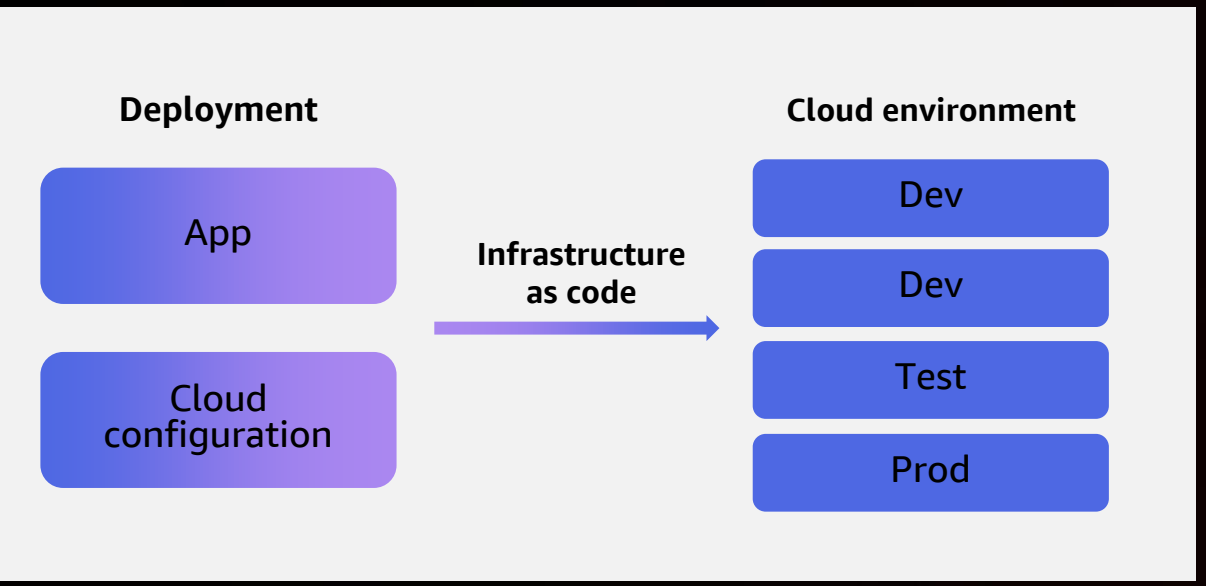
Securing container runtimes

- Short-lived, elastic environments
- Scale and volume of events
- Variance in infrastructure and orchestrators
- Immutable infrastructure and builds
- Tooling to monitoring container runtimes

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

Securing the cloud in cloud-native applications





Empower cloud teams to move quickly

- Shared responsibility models
- Visibility into cloud services
- Governance and compliance regulations
- User and identity management

Empower security teams to scale

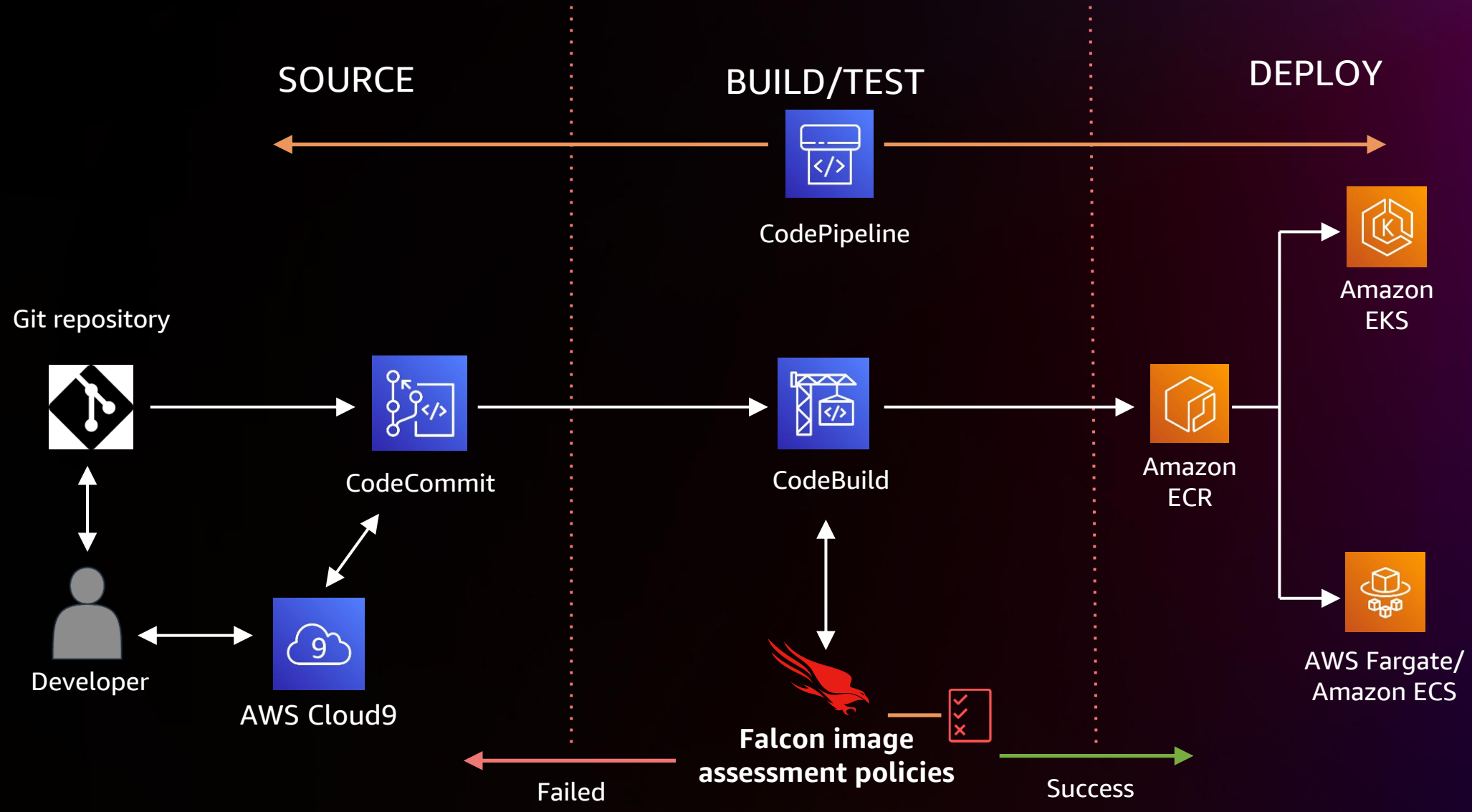
- Build threat models for cloud services
- Standardize risk scores and assessments
- Layer preventive and detective controls
- Policy as code for continuous assessments
- Automation for SOC/IR teams

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

Shifting security left

© 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.

Falcon CWP and Amazon ECR

2. Connect all your Amazon ECR registries to Falcon CWP

Amazon ECR

Container image

Container image

Container image

Falcon CWP (image assessment)

1. Define image policies

Amazon ECR

Container image

Container image

Container image



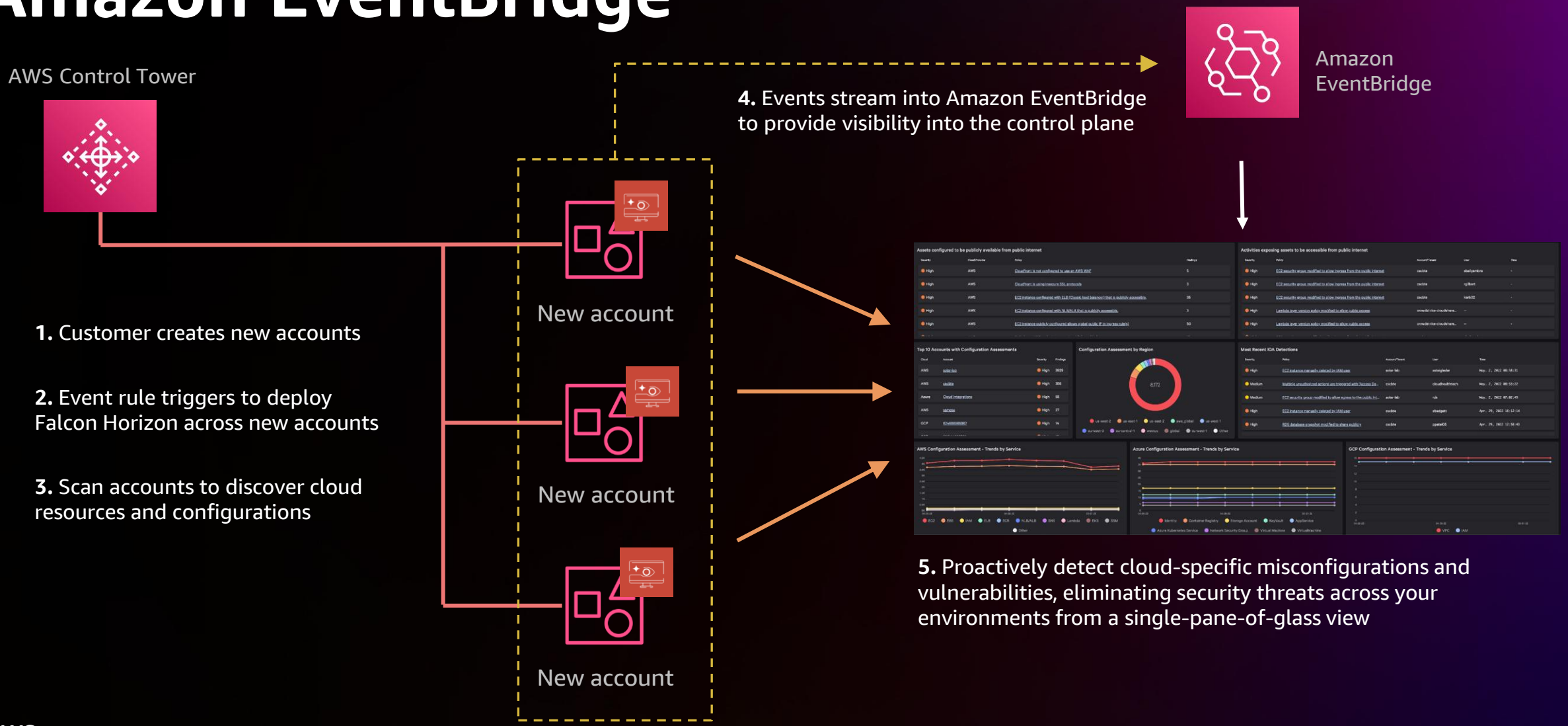
3. Analyze and respond to hidden malware and vulnerabilities from outdated libraries and identify misconfigurations, all from a single dashboard across all your environments

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

Securing AWS accounts

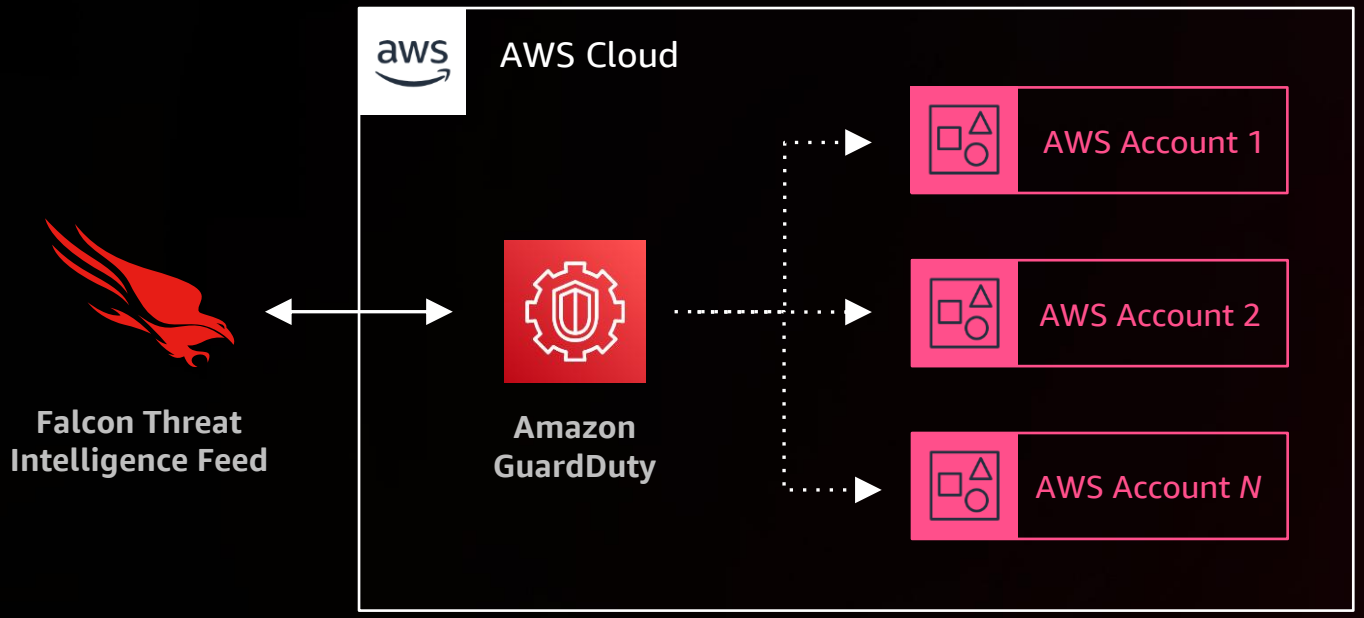
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Falcon Horizon, AWS Control Tower, and Amazon EventBridge



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

Falcon Intelligence and Amazon GuardDuty



Premier threat feed

CrowdStrike provides the intelligence feed that powers the threat detection services for customers of Amazon GuardDuty

Crowdsourced telemetry

Trillions of raw telemetry events are processed per day through CrowdStrike's Threat Graph to identify new threats in real time

Indicators of compromise

Amazon GuardDuty relies on the feed of IOCs provided by CrowdStrike that includes malicious domains, IP addresses, and hashes

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

Securing cloud environments

Cloud Infrastructure Entitlement Management (CIEM)



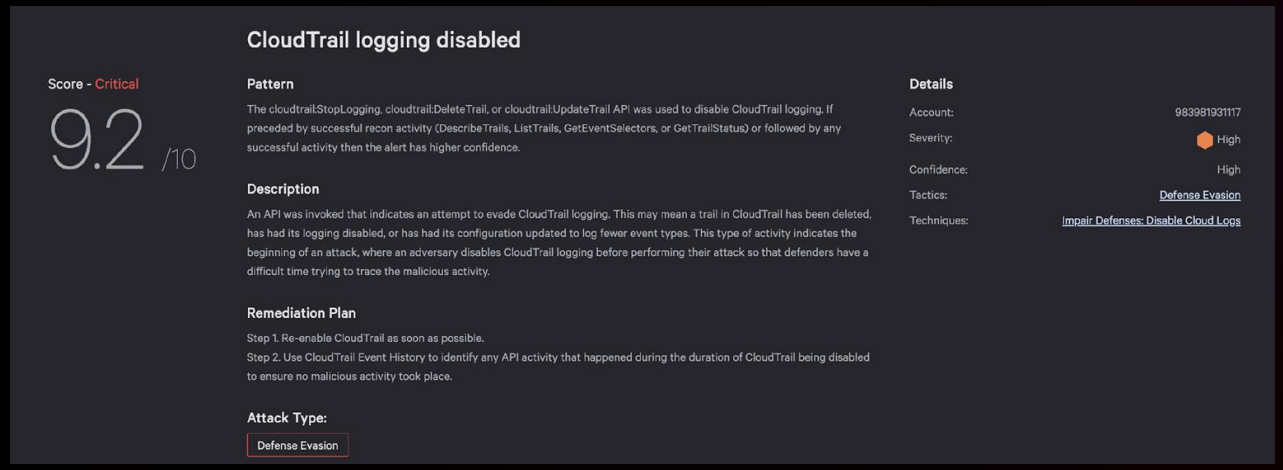
Analyzing identities

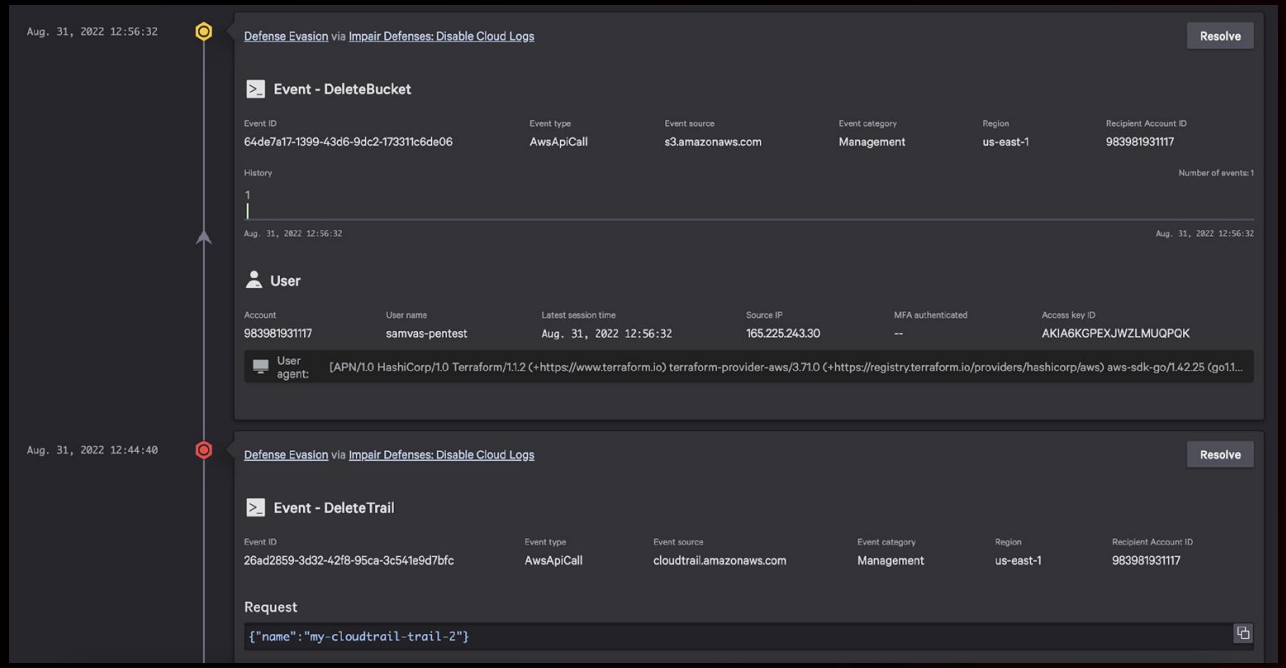
Least privilege management

- Users, roles, and their permissions
- Identity hygiene – activity and policy
- Overly permissive policies
- Behavioral detections for identities
- Dashboards

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

Indicators of Attack (IOA) for cloud





Securing cloud environments

Indicators of Attack (IOA)

Detect anomalous behavior in cloud

- Identify risks with just API activity
- 60+ IOAs for cloud environments
- Identify reconnaissance and post-exploit activity
- Severity scores to improve confidence of alerts
- Mapped to MITRE ATT&CK TTPs

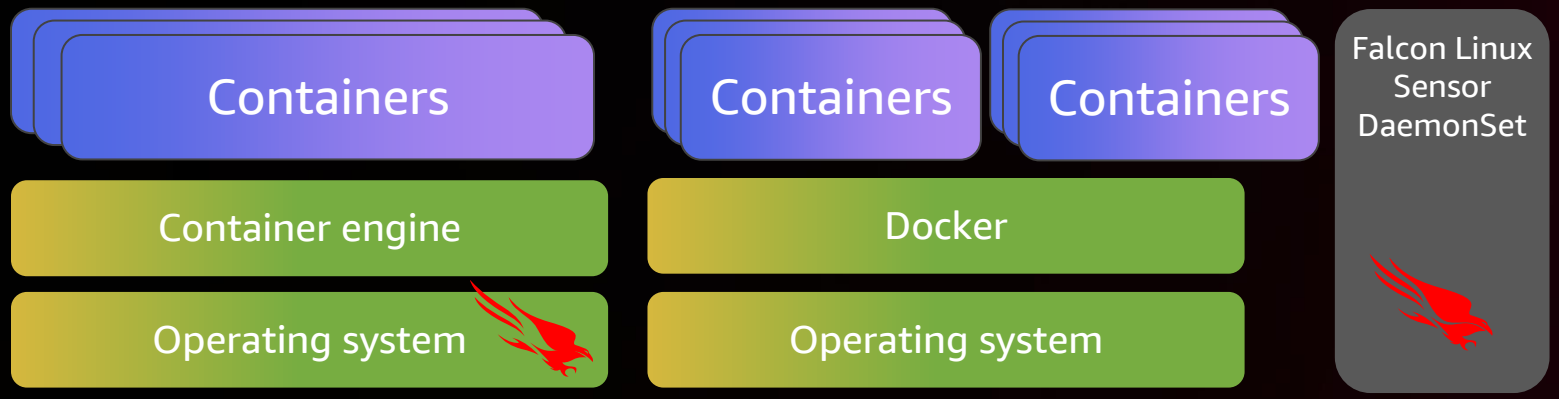
aws
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Securing runtimes on AWS compute

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

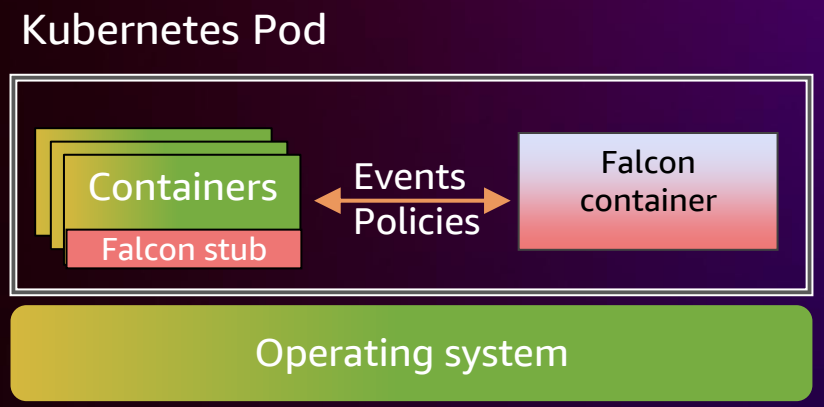
Securing runtimes

Linux sensor



Secures both worker nodes and containers

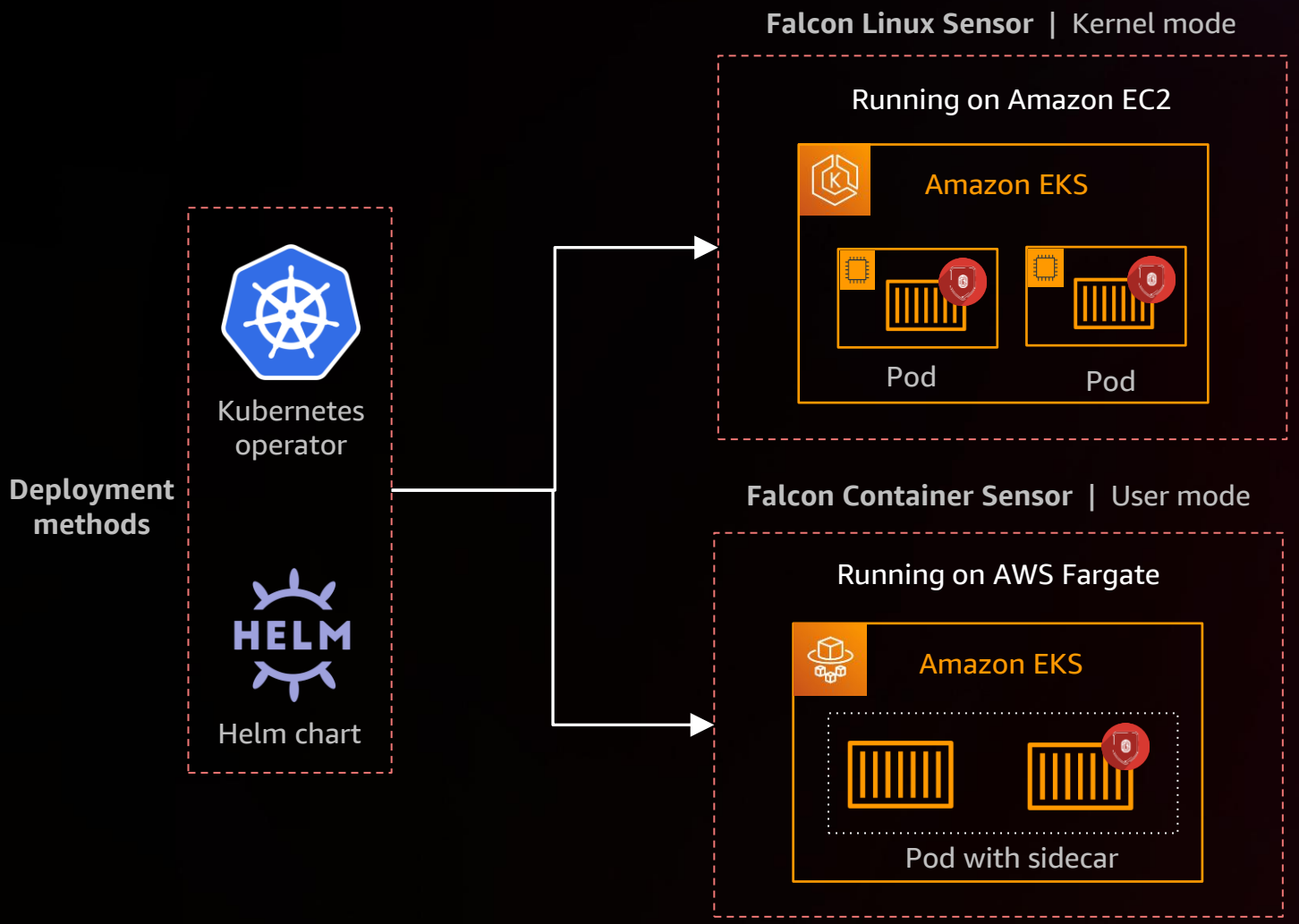
Falcon container



Serverless containers

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

Falcon CWP, Amazon EKS, AWS Fargate



Native tooling

Using native tooling, such as Kubernetes operators and Helm charts to secure your applications easily at scale

Runtime protection

Defends containers and Kubernetes applications against active events using AI/ML and IOAs to protect against known and unknown, zero-day events

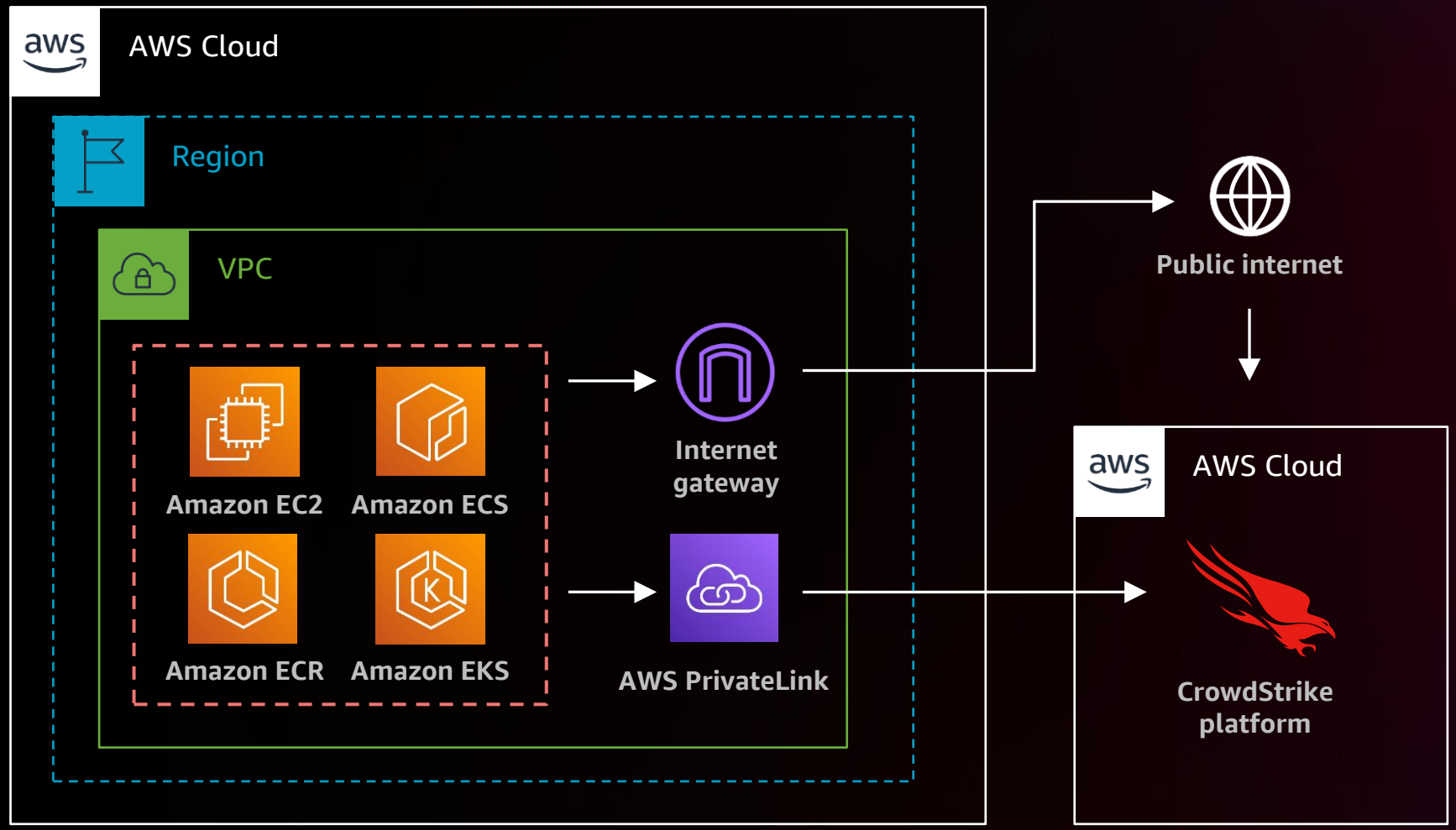
Container drift prevention

Enforces container immutability by detecting new binaries created and executed inside containers

aws

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

Falcon CWP and AWS PrivateLink



Secure connectivity

All communications to the CrowdStrike platform traverse through the AWS backbone instead of public internet to reduce exposure to external threats

Maintain compliance

Customers operating in financial, government, and healthcare sectors have strict governance around sensitive data

AWS PrivateLink helps ensure data stays on the Amazon network where the necessary controls are already in place

Simplify networking

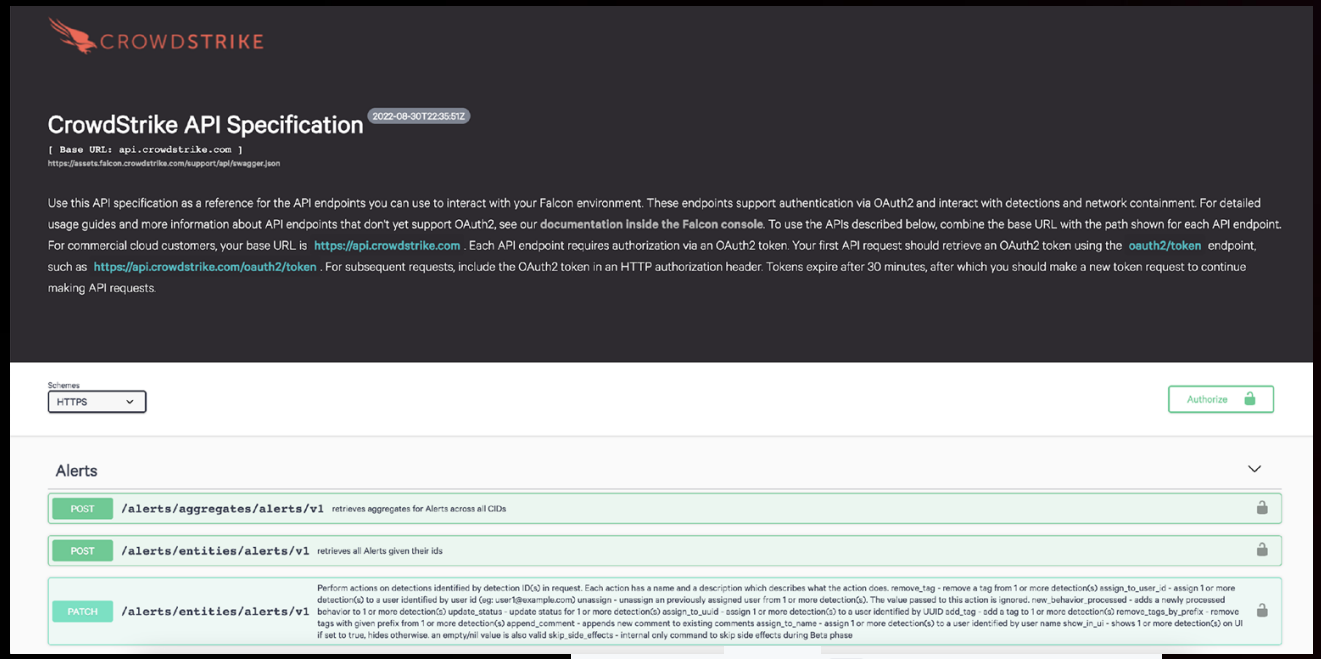
Remove the need for firewall rules, specific route table entries, and expensive internet gateways to simplify your network architecture

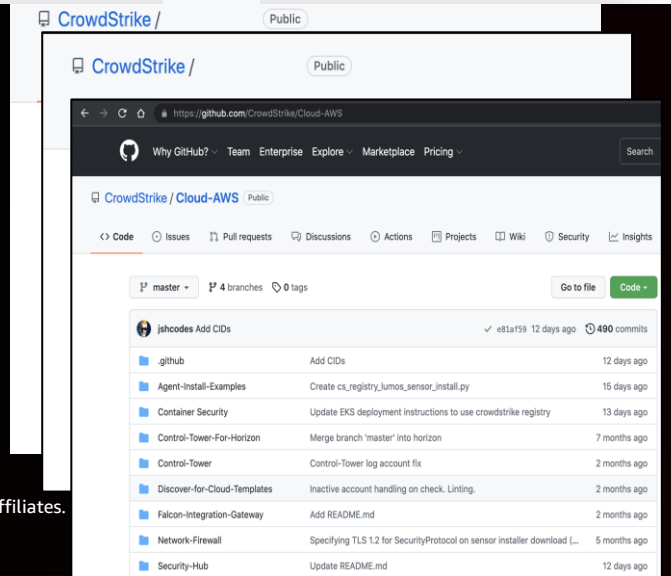
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Automation and orchestration

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

Automation



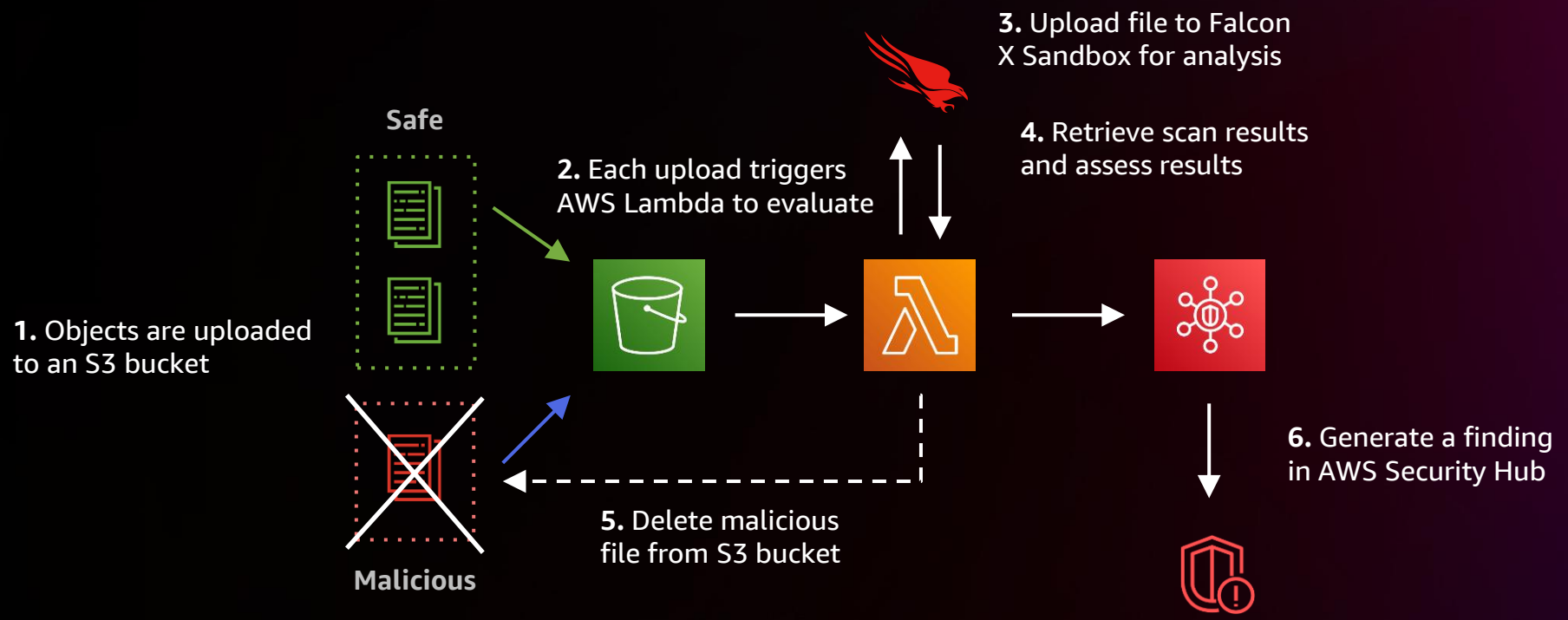


APIs and orchestration integrations

- API first, built on a cloud-native platform
- OAuth2-authenticated API endpoints
- Access swagger files and API docs
- Integrations with cloud provider services
- Extend via workflows and webhooks
- FalconPy: Python SDK for Falcon

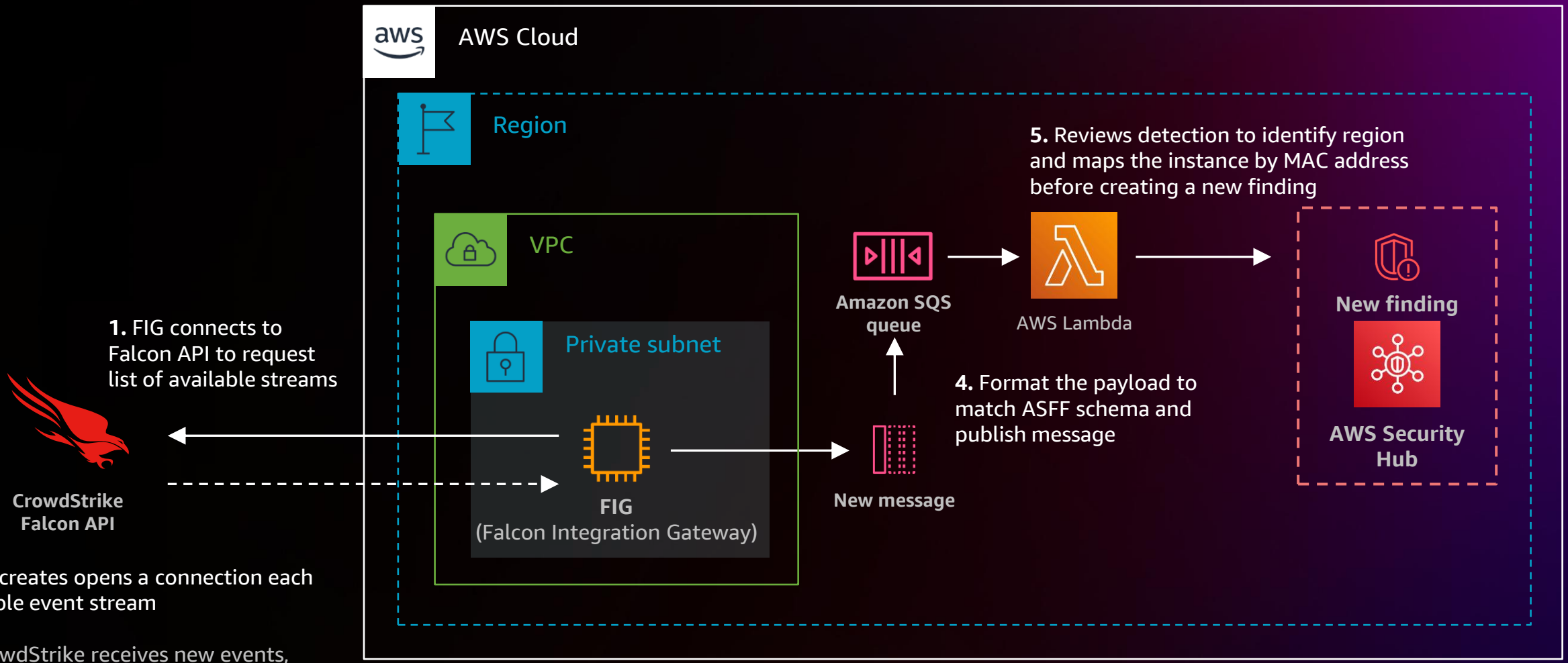
aws
© 2022, Amazon Web Services, Inc. or its affiliates.

Falcon Intelligence and Amazon S3



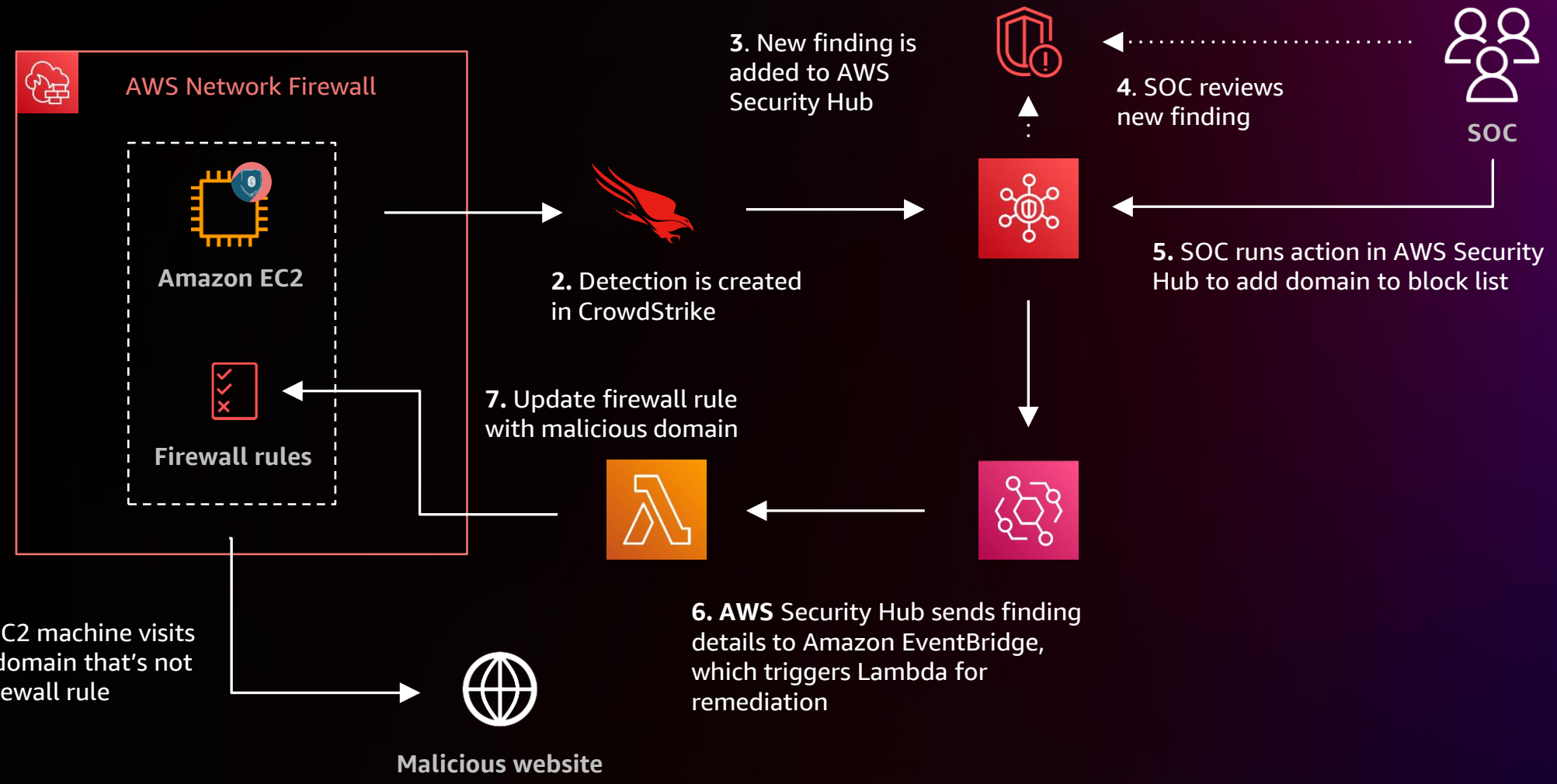
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Falcon and AWS Security Hub



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

Falcon X and AWS Network Firewall



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

Summary

Cloud-native apps

Challenge traditional security tools

Shifting left

Collaboration and tooling to work with dev teams

Layered security

Security needs to be built in from build to run

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

Thank you!

Sameer Vasanthapuram
sameer.vasanthapuram@crowdstrike.com

Justin Harris
Justin.harris@crowdstrike.com



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

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