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

SEC329-R

AWS security services for container threat detection

Scott Ward (he/him)

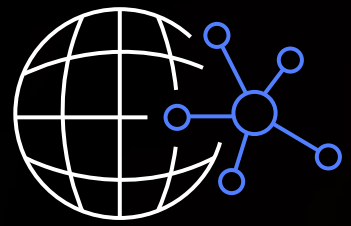
Principal Solutions Architect
Amazon Web Services

Mrunal Shah (he/him)

Head of Container Security
Warner Bros. Discovery - HBO Max

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

Container security challenges



Scale



Short-lived



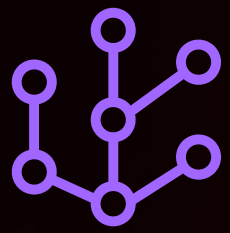
Different



Insecure sources



Lack of expertise



Network configuration



Lack of visibility

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

What are best practices for securing container workloads running on AWS?

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



Amazon GuardDuty EKS Protection

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

Amazon GuardDuty



Amazon GuardDuty

A threat detection service that continuously monitors for compromised accounts, anomalous behavior, and malware



Activate GuardDuty

With a few clicks in the console, monitor all your AWS accounts without additional software to deploy or manage



Amazon S3



Container workloads



Instance workloads



Accounts and users

Continuously analyze

Automatically and continuously monitor AWS workloads and resources for potential threats at scale



Intelligently detects threats

GuardDuty uses machine learning anomaly detection, malware scanning, and integrated threat intelligence to identify and prioritize potential threats



Take action

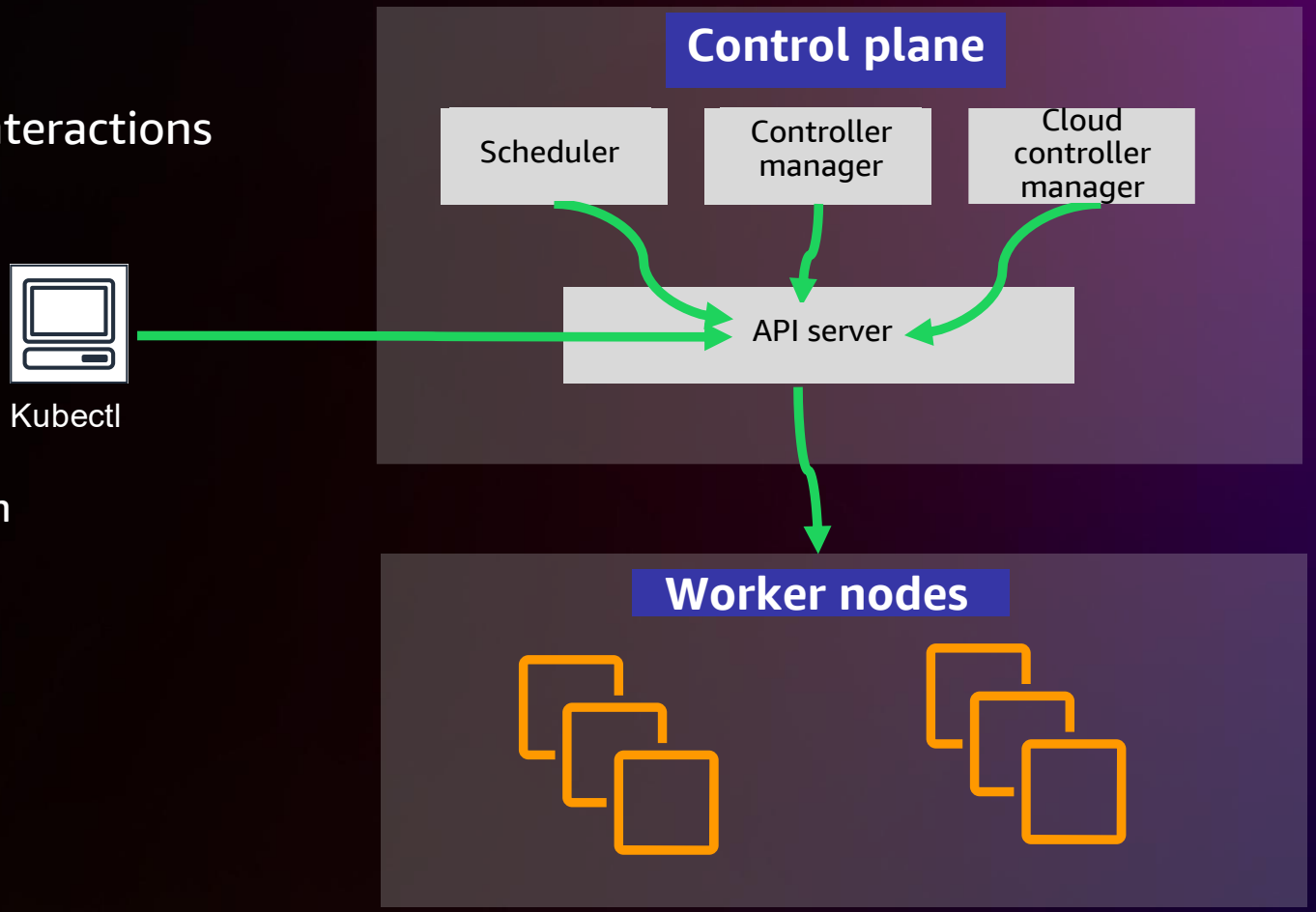
Review detailed findings in the console, integrate into event management or workflow systems, and initiate AWS Lambda for automated remediation or prevention

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

Kubernetes control plane API and audit logs

- Kubernetes control plane API – HTTP API to **query** and **manipulate** the state of API objects in Kubernetes
  - Pods, namespaces, ConfigMaps, events

- Audit logs provide information on API interactions
  - What happened?
  - When did it happen?
  - Who initiated it?
  - On what did it happen?
    - Endpoints, pods, ConfigMap, and so on
  - Where was it observed?
  - From where was it initiated?
  - To where was it going?



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

GuardDuty EKS Protection finding types

Policy

- Exposed dashboard
- Admin access to default service account
- Anonymous access granted

Malicious access

- Data discovery, exfiltration, or modification from:
  - Tor
  - Successful anonymous access
  - Malicious IPs

Suspicious behavior

- Execution in Kubernetes system pod
- Container with sensitive mount
- Privilege container

GuardDuty immediately begins to analyze Kubernetes data sources from your Amazon EKS clusters and monitors them for malicious and suspicious activity

GuardDuty aligns findings using the MITRE ATT&CK framework

Credential access Defense evasion Discovery Impact

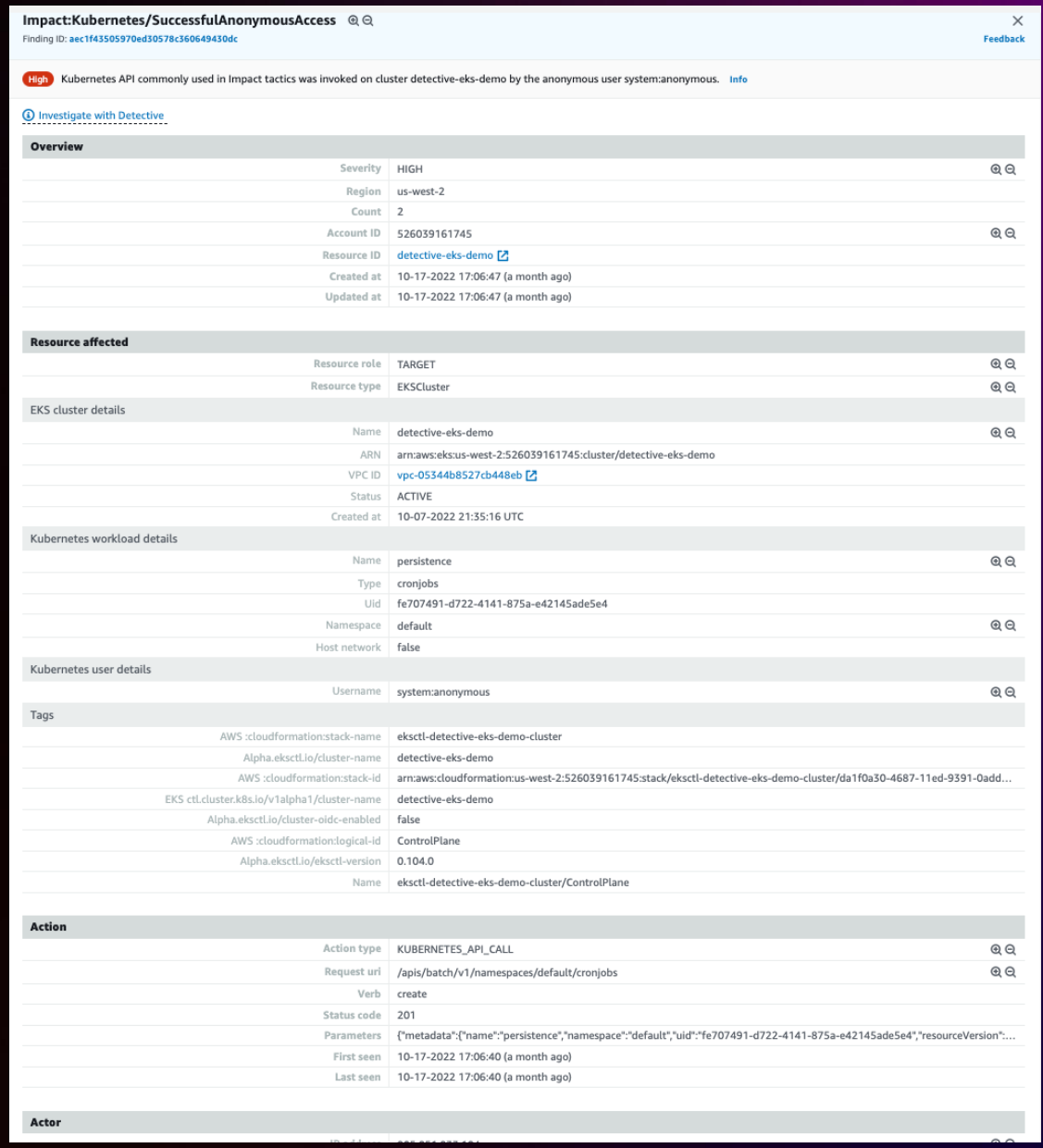
Privilege escalation Policy Execution Persistence

aws

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

GuardDuty EKS Finding details

- Finding description and remediation guidance
- Severity
- First and last observed
- Resources impacted
  - Cluster
  - Workload
  - User
- Action
  - Action type
  - Request URI
  - Verb
  - Status
  - Parameters



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

Remediation of GuardDuty Kubernetes findings

GuardDuty Kubernetes remediation guidance:
https://docs.aws.amazon.com/guardduty/latest/ug/guardduty-remediate-kubernetes.html

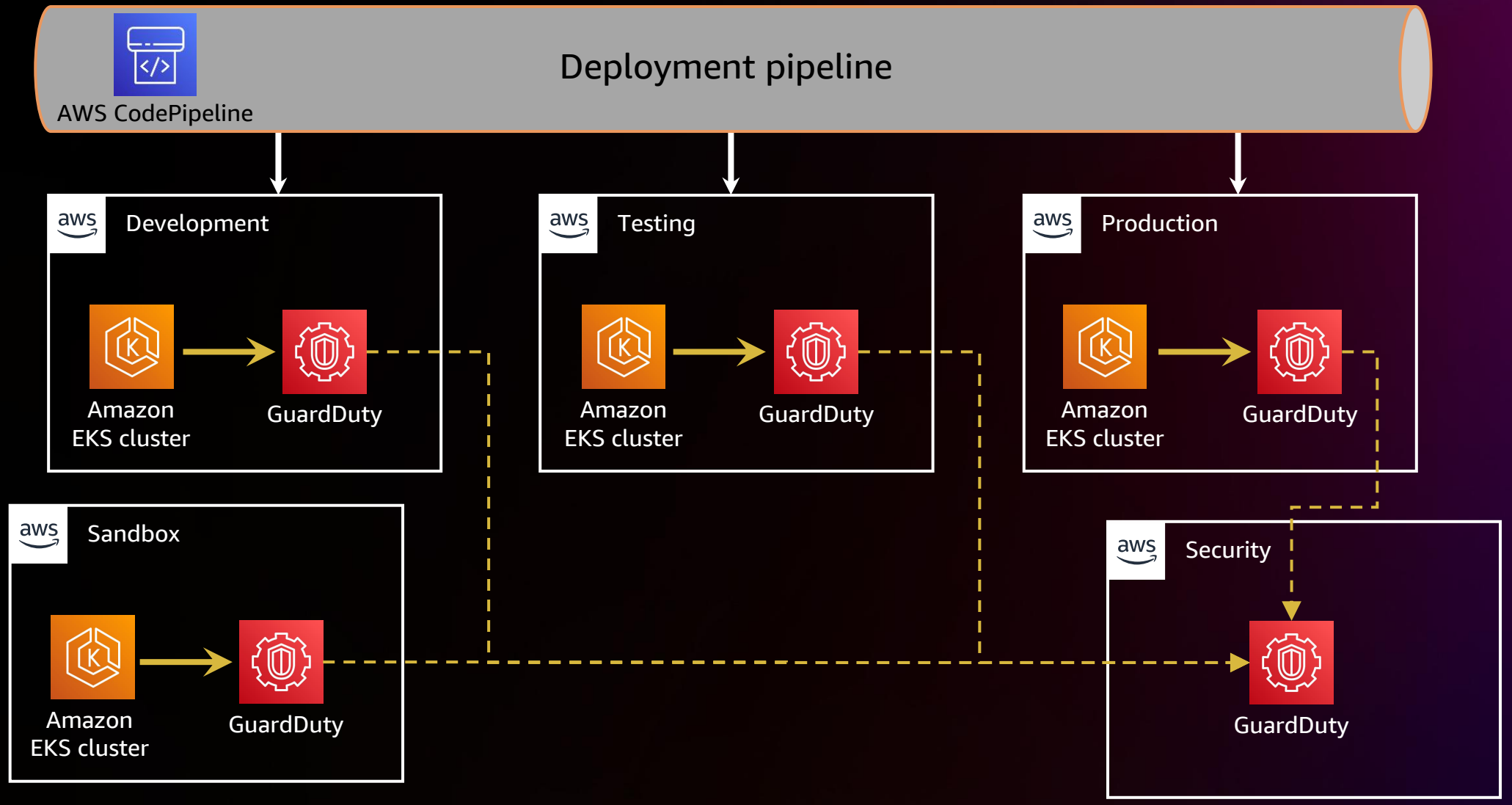
Amazon EKS security best practices:
https://aws.github.io/aws-eks-best-practices/security/docs/

- Make the cluster API endpoint private
  - If a public endpoint is a must, then safe list specific CIDR IP addresses
- Review and revoke unnecessary anomalous access
- Take reverse actions where appropriate
- Rotate credentials and secrets of impacted users
- Isolate pods, revoke pod credentials, and gather data for forensics
- Terminate pods or nodes
- Patch container image and re-deploy

Automate wherever you can

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

Where can you use GuardDuty EKS Protection?



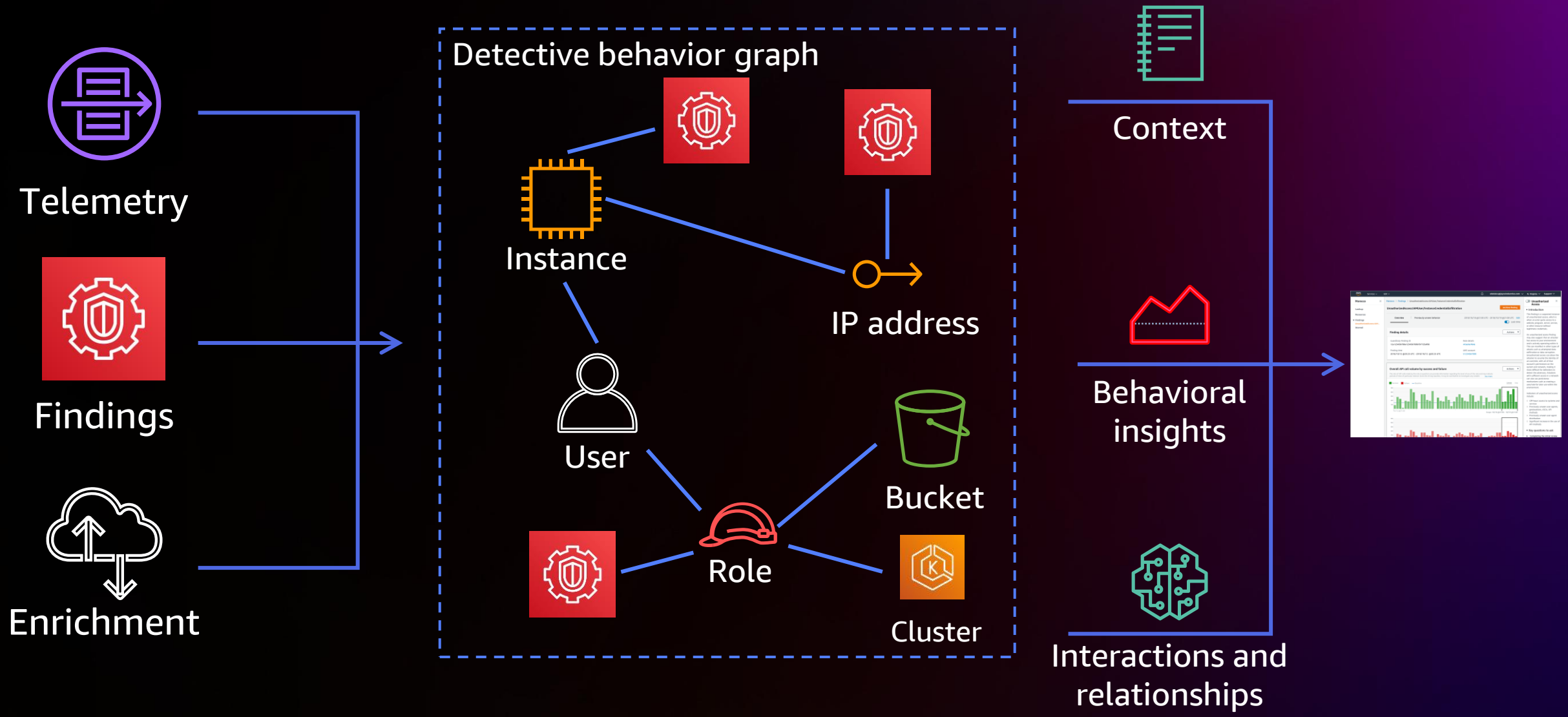
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.



Amazon Detective for Amazon EKS

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

Automated data collection, synthesis & analysis



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

Amazon Detective for Amazon EKS



- Based on Amazon EKS audit logs and other Detective sources
- Unified view of Amazon EKS clusters and interactions with the clusters over time
- Investigate from GuardDuty findings or your own search
- Review Amazon EKS specific activity
- New investigation tabs for Kubernetes activity and API calls

aws

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

Detective for Amazon EKS resource visibility

Detective resources

AWS account

IAM user

IAM role

Role session

Amazon EC2 instance

IP address

Amazon EKS cluster

Kubernetes pod

Container image

Kubernetes subject

New for Amazon EKS

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

Kubernetes with GuardDuty and Detective

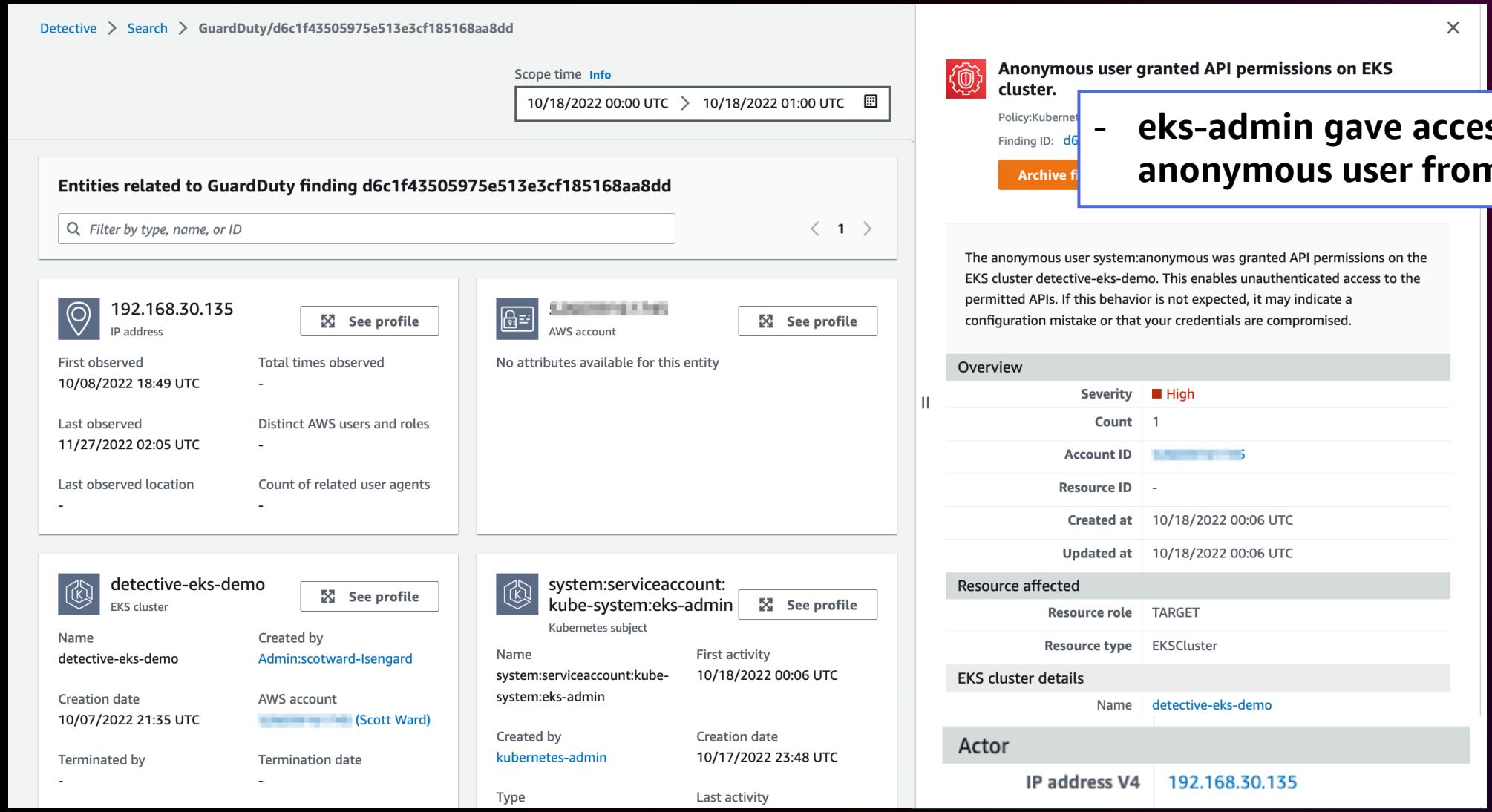
Amazon GuardDuty alerted you about an Amazon EKS finding:
“Anonymous user granted API permissions on EKS cluster”

Use Amazon Detective for Amazon EKS to

1. Identify the root cause
2. Identify how the scenario happened
3. Identify the impact

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

Starting point: A finding from Amazon GuardDuty

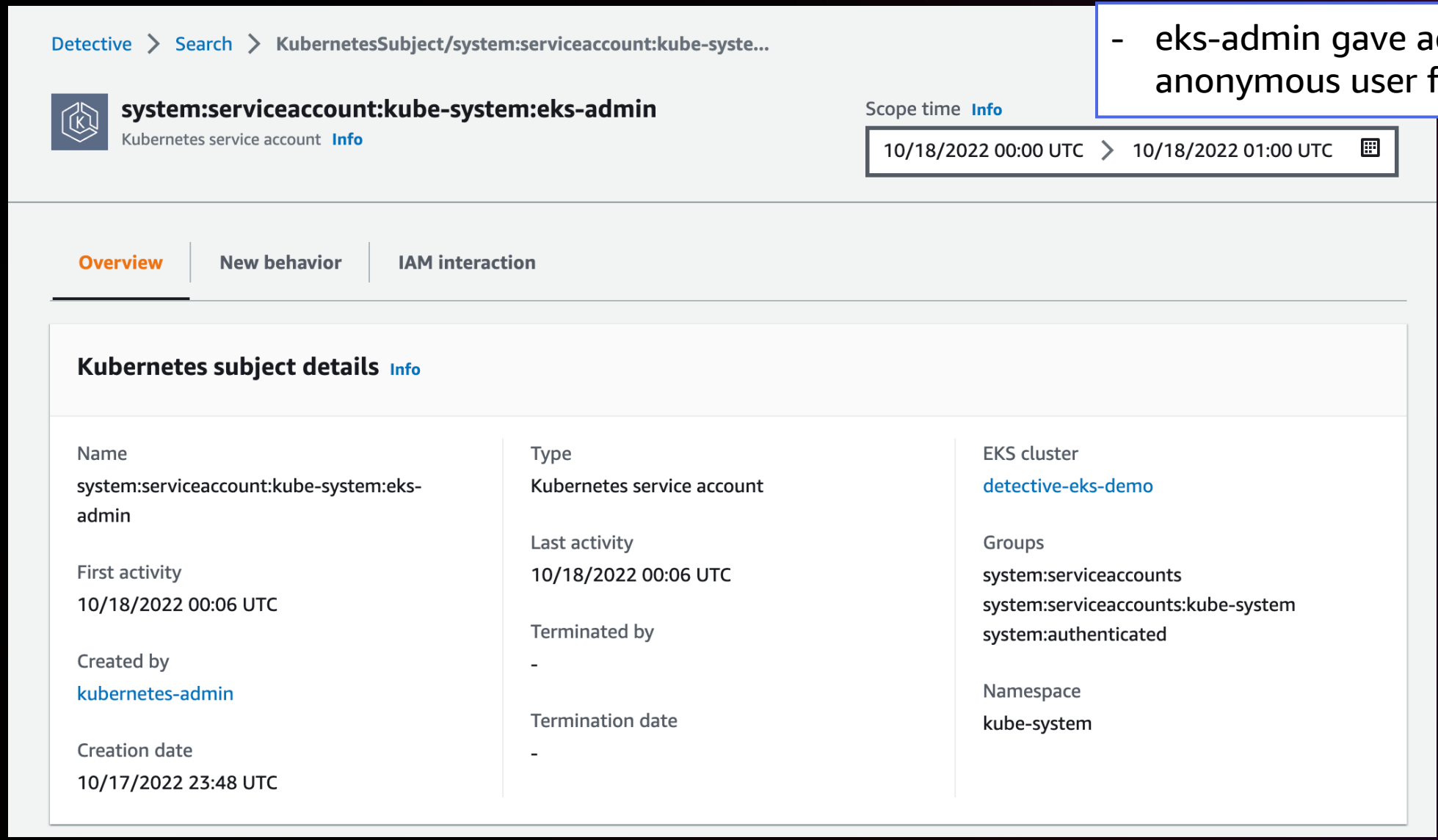


- **eks-admin gave access to the anonymous user from 192.168.30.135**

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

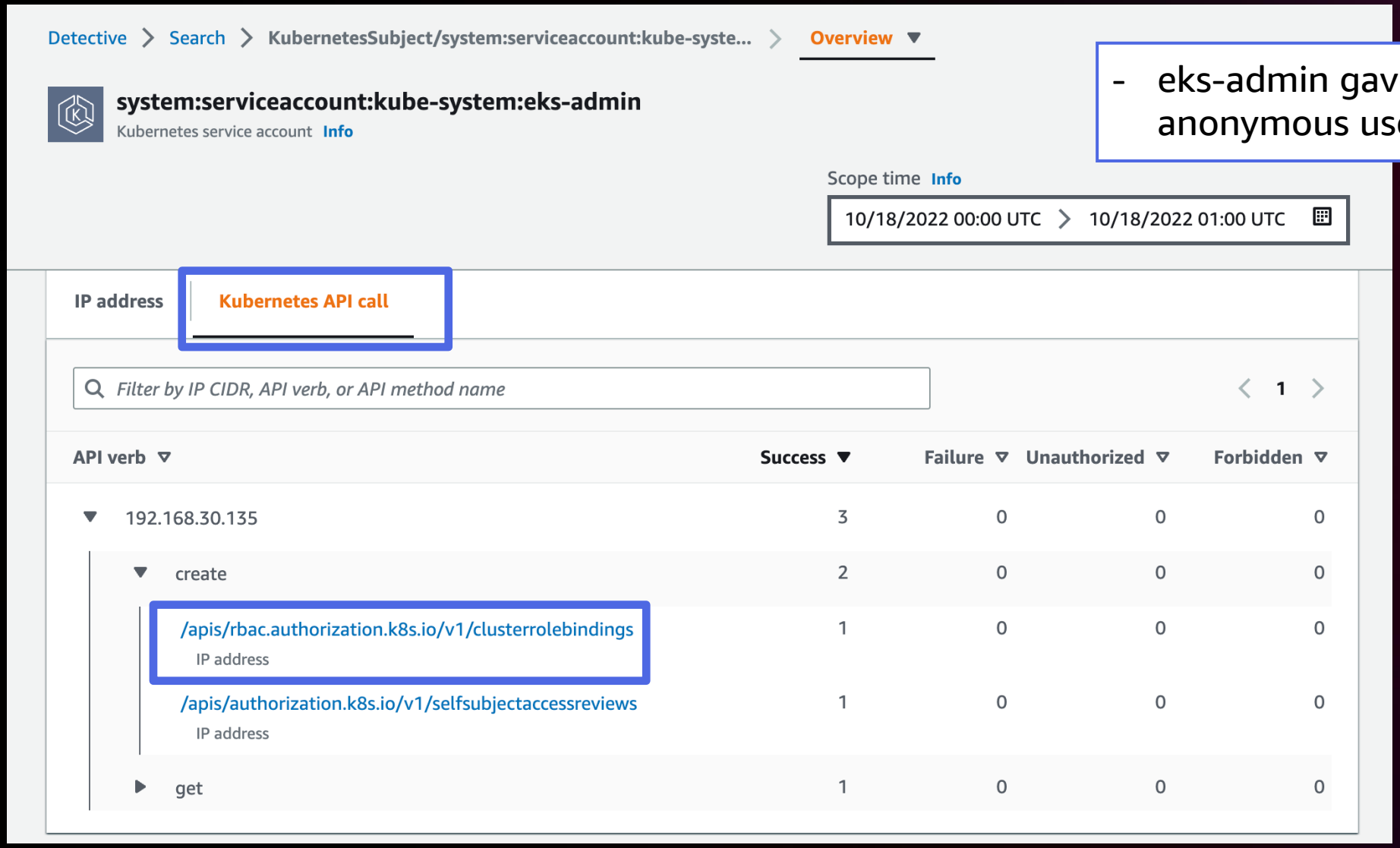
Finding the root cause – service account

- eks-admin gave access to the anonymous user from **192.168.30.135**



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

Finding the root cause – service account

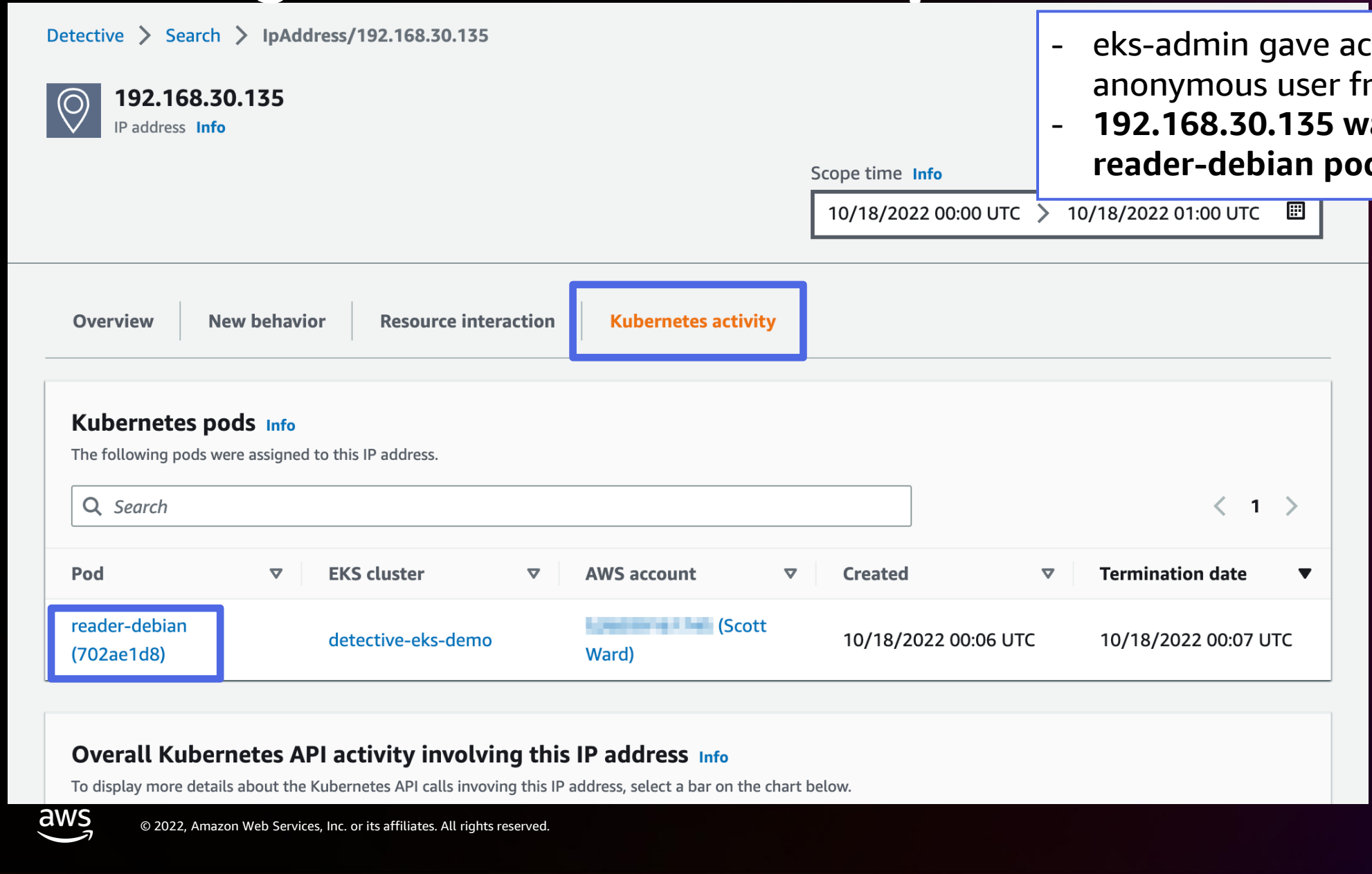


- eks-admin gave access to the anonymous user from **192.168.30.135**

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

Finding the root cause – ip address

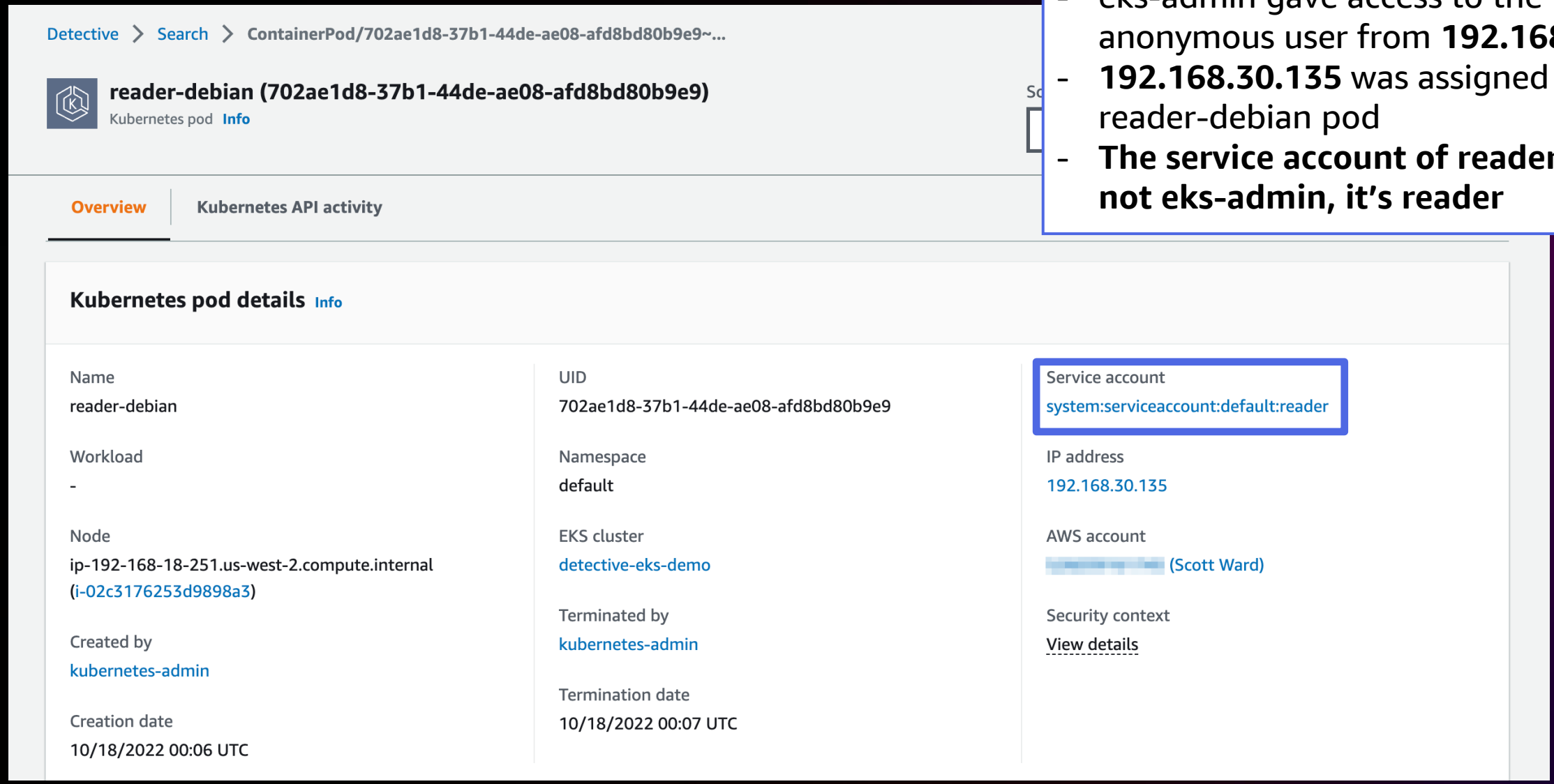
- eks-admin gave access to the anonymous user from **192.168.30.135**
- **192.168.30.135 was assigned to the reader-debian pod**



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

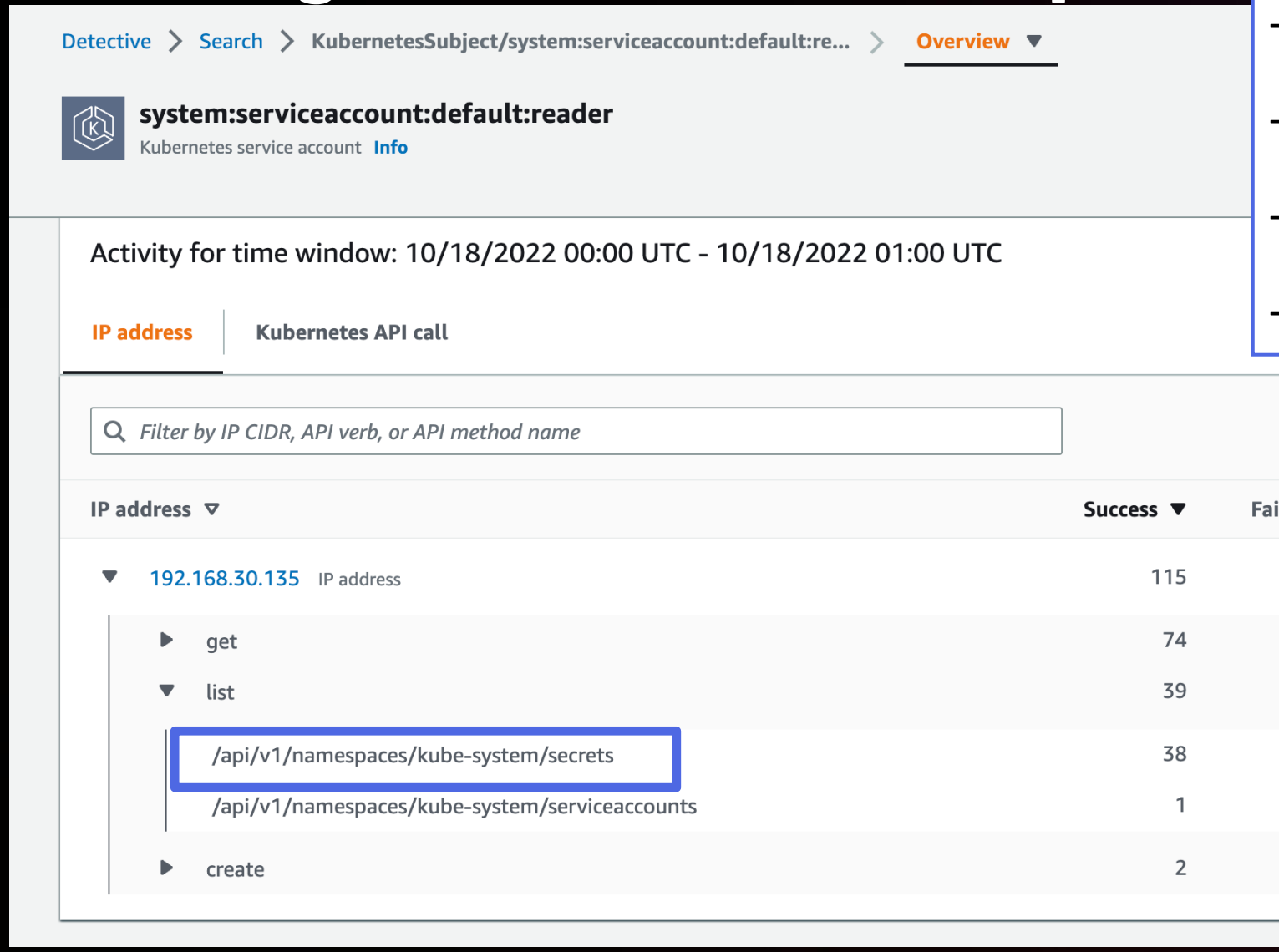
Finding the root cause - pod

- eks-admin gave access to the anonymous user from **192.168.30.135**
- **192.168.30.135** was assigned to the reader-debian pod
- **The service account of reader-debian is not eks-admin, it's reader**



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

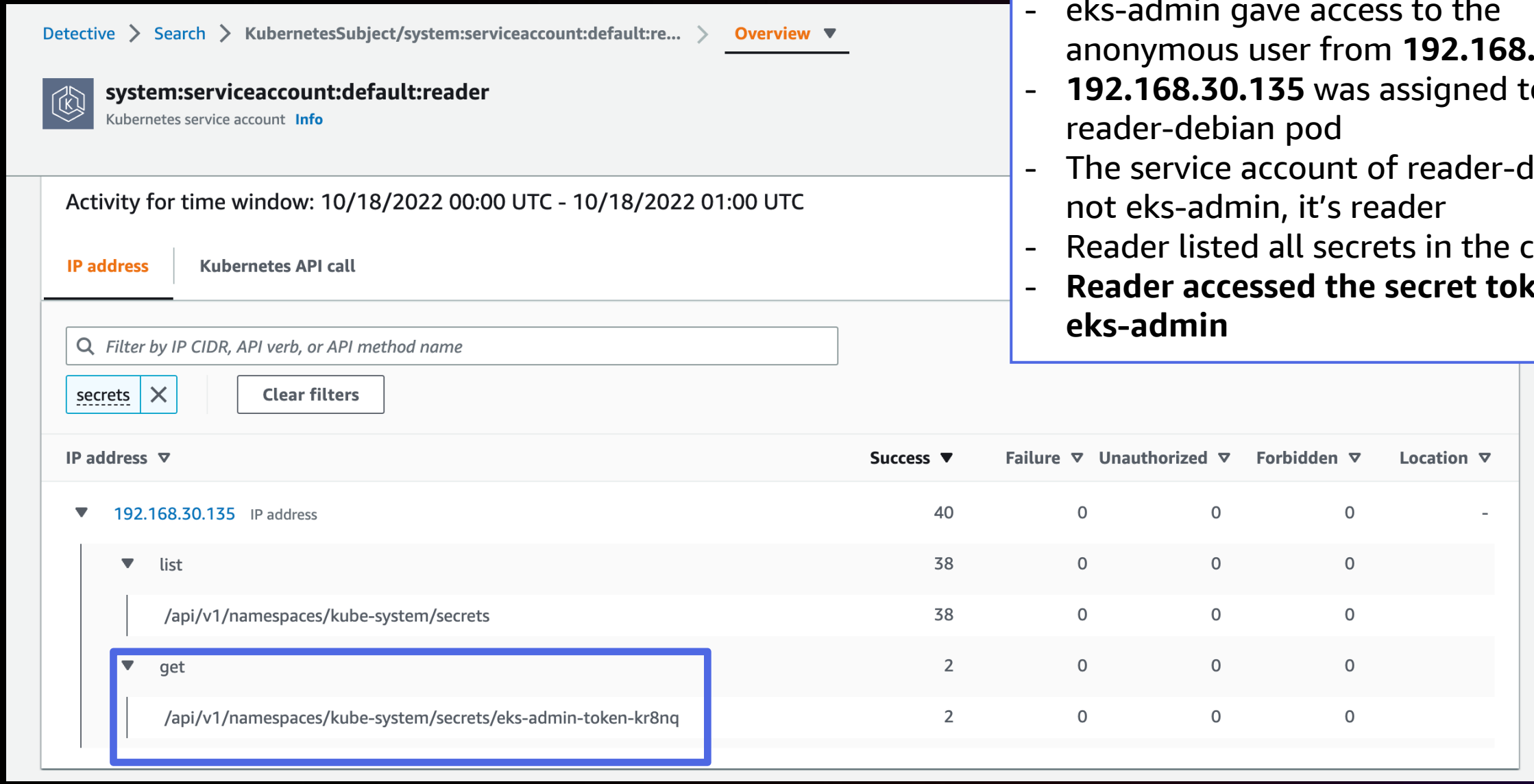
Finding the root cause - pod



- eks-admin gave access to the anonymous user from **192.168.30.135**
- **192.168.30.135** was assigned to the reader-debian pod
- The service account of reader-debian is not eks-admin, it's reader
- **Reader listed all secrets in the cluster**

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

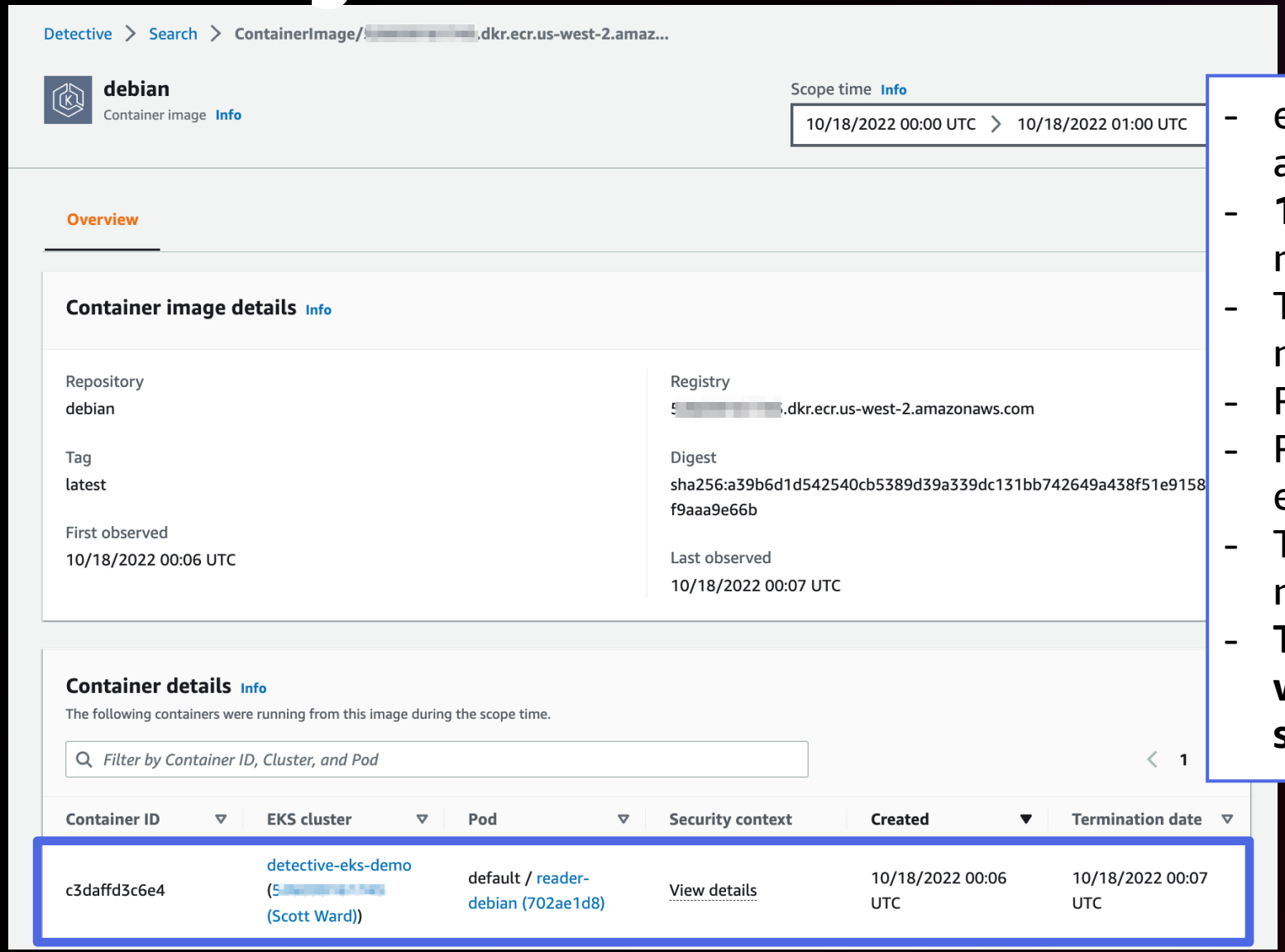
Finding the root cause – pod



- eks-admin gave access to the anonymous user from **192.168.30.135**
- **192.168.30.135** was assigned to the reader-debian pod
- The service account of reader-debian is not eks-admin, it's reader
- Reader listed all secrets in the cluster
- **Reader accessed the secret token for eks-admin**

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

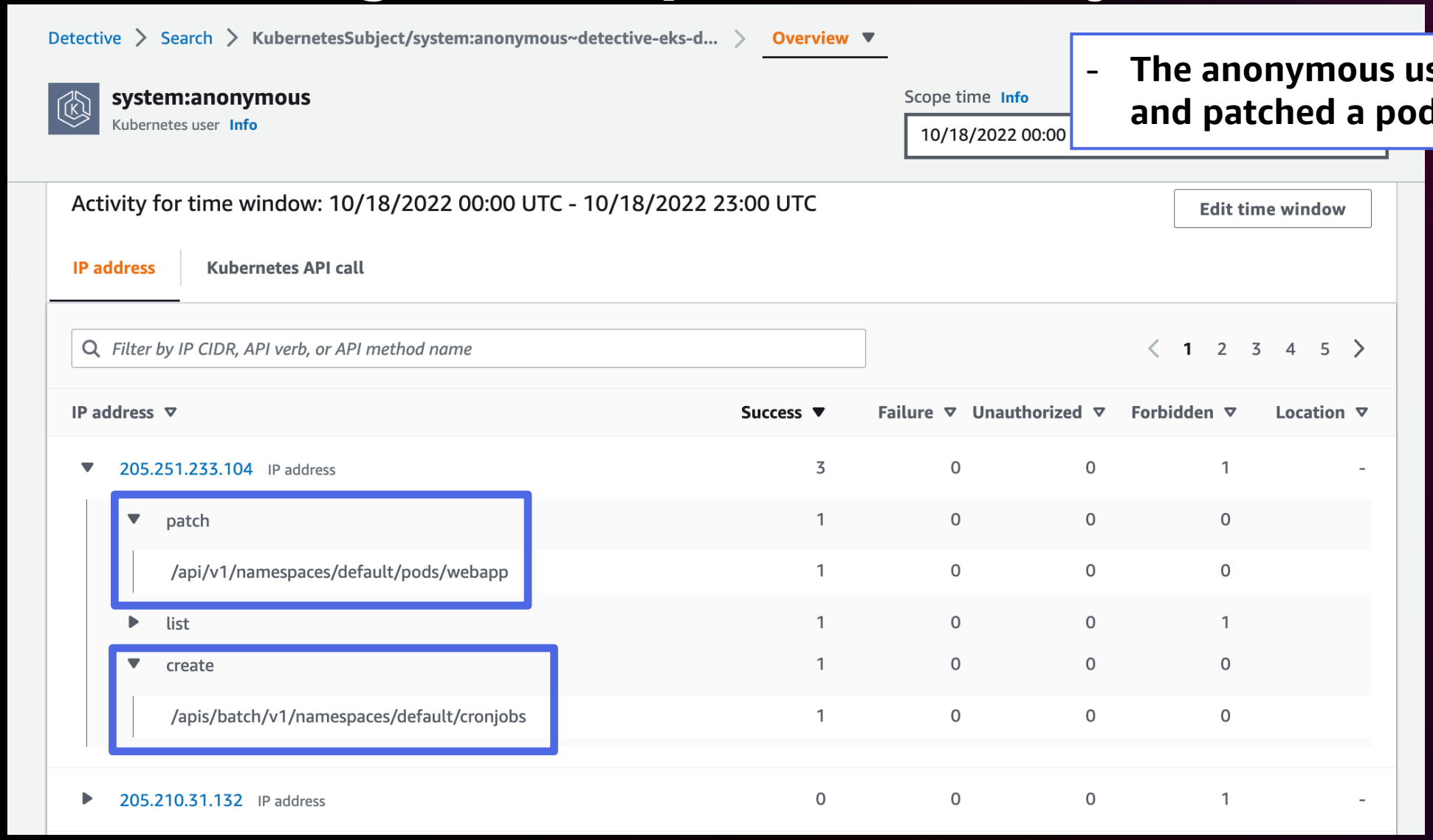
Finding the root cause - containers



- eks-admin gave access to the anonymous user from **192.168.30.135**
- **192.168.30.135** was assigned to the reader-debian pod
- The service account of reader-debian is not eks-admin, it's reader
- Reader listed all secrets in the cluster
- Reader accessed the secret token for eks-admin
- The reader-debian pod was not accessed remotely using "exec"
- **The specific debian container image with this hash only is deployed to the suspicious reader-debian pod**

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

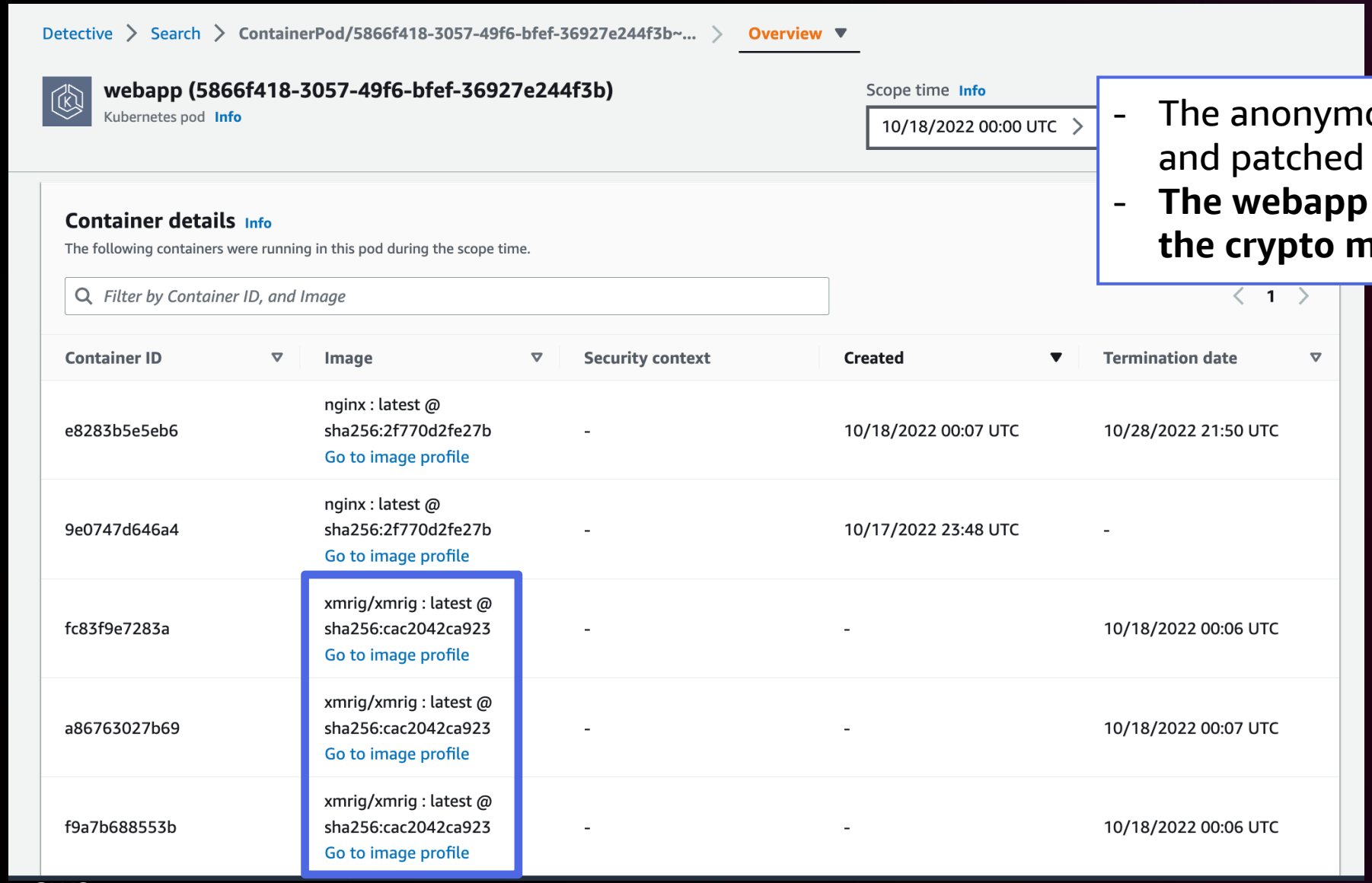
Reviewing the impact – anonymous user



- **The anonymous user created a CronJob and patched a pod named webapp**

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

Reviewing the impact – webapp pod



- The anonymous user created a CronJob and patched a pod named webapp
- **The webapp pod had containers from the crypto mining image xmrig**

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

Investigation summary

Root cause

A container from an unusual debian image

How the scenario happened

The container extracted the secret token for the eks-admin

Then, it granted access to the anonymous user

Impact

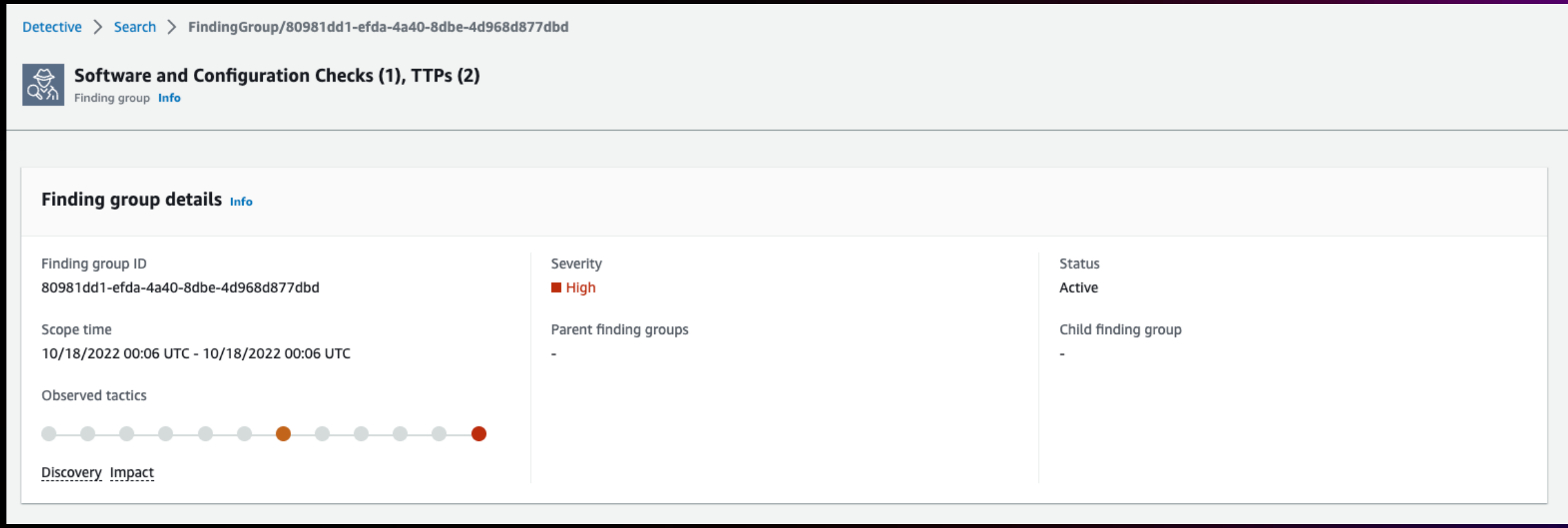
An anonymous user created a CronJob

It also modified the webapp pod with a crypto mining container image

aws

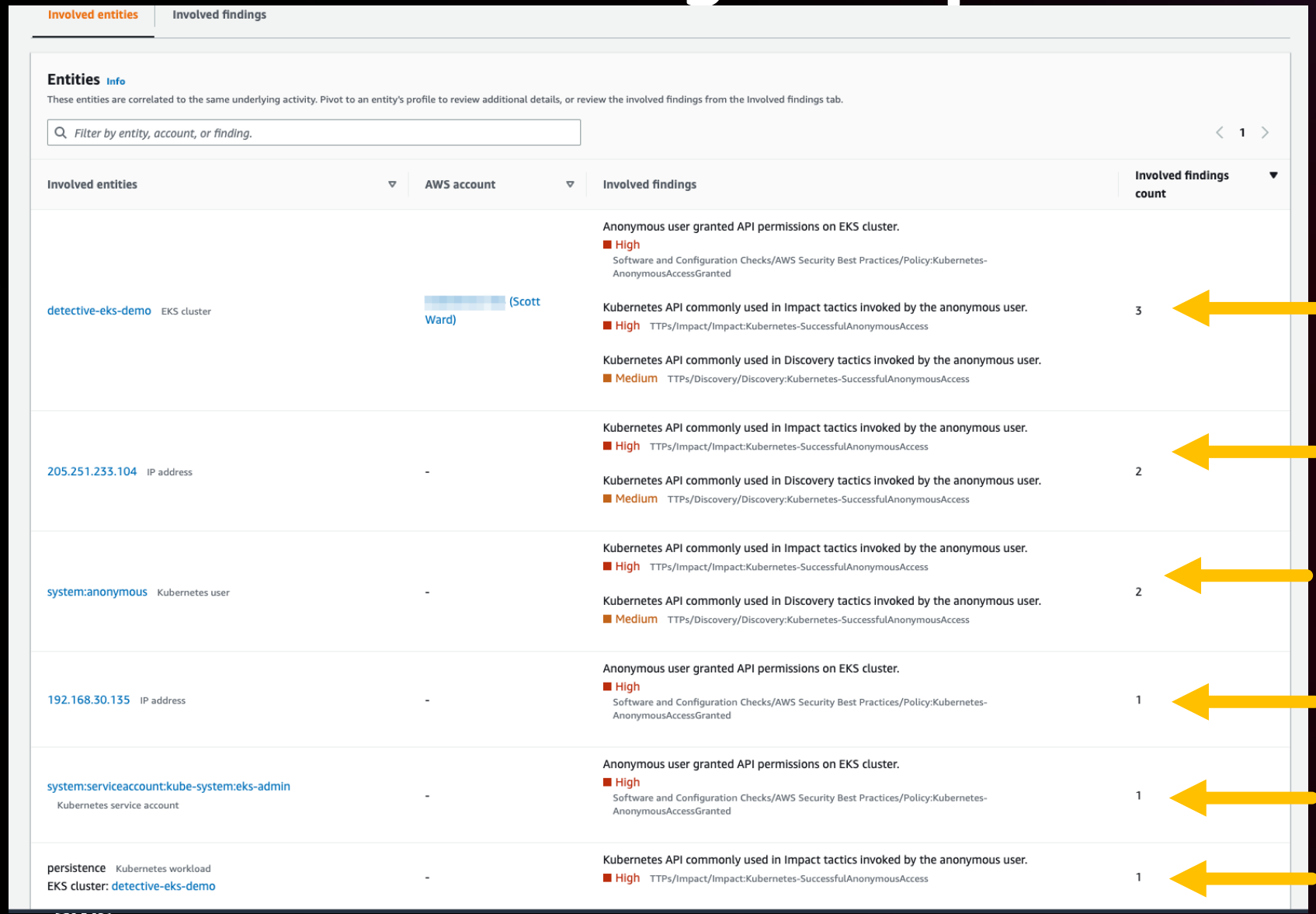
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Detective Finding Groups



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

Detective Finding Groups



GuardDuty Findings

IP address used in anonymous access

Anonymous user access

IP Address of Pod granting access

Eks-admin grants anonymous access

Persistence API calls in EKS cluster

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



Amazon GuardDuty Malware Protection

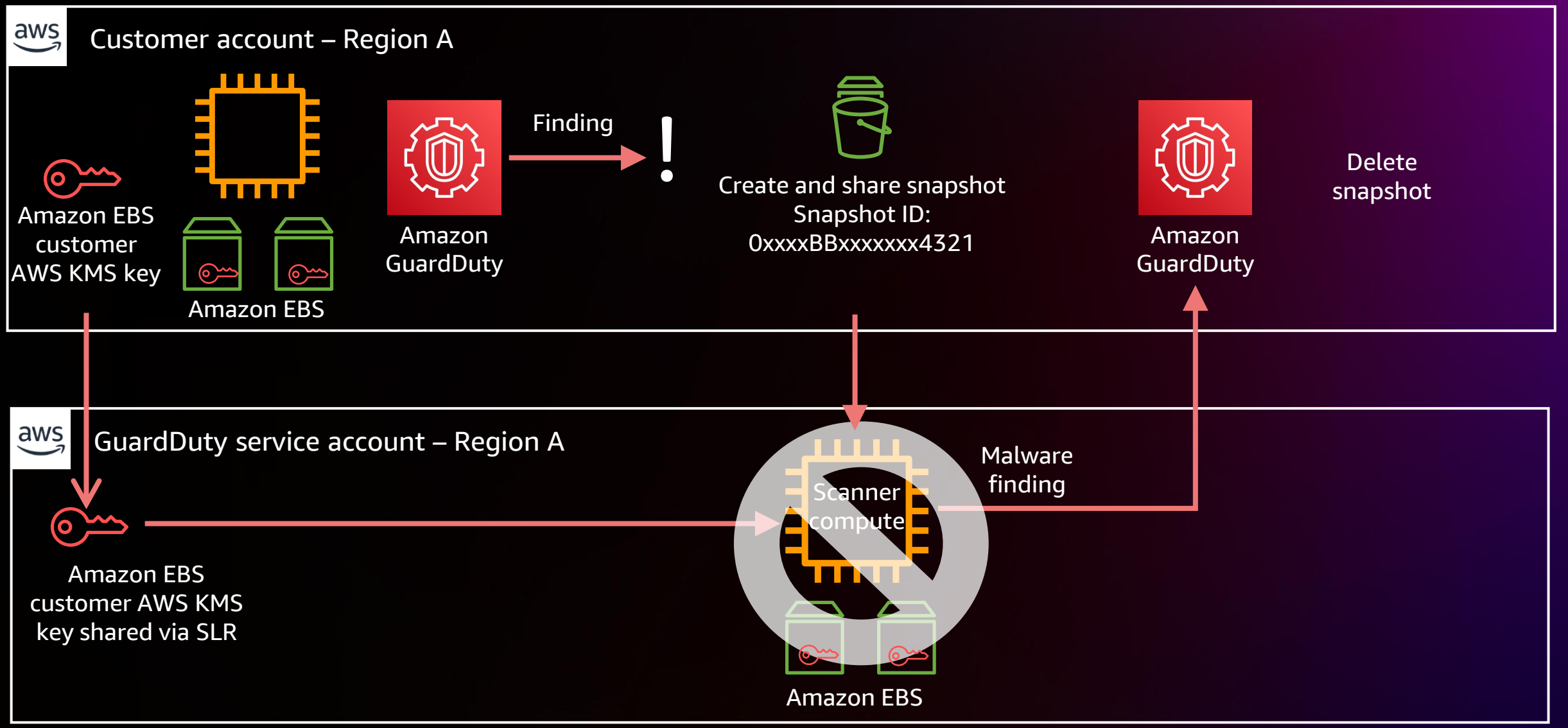
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

What is GuardDuty Malware Protection?

- Fully managed malware detection service
- Scans Amazon EC2 workloads based on certain GuardDuty findings
  - EC2, Amazon EKS on EC2, Amazon ECS on EC2, self-managed containers on EC2.
  - Detected malware creates new finding in GuardDuty
- Uses third-party engines, machine learning, and threat intelligence to identify potential malware
- Agentless: No security software required

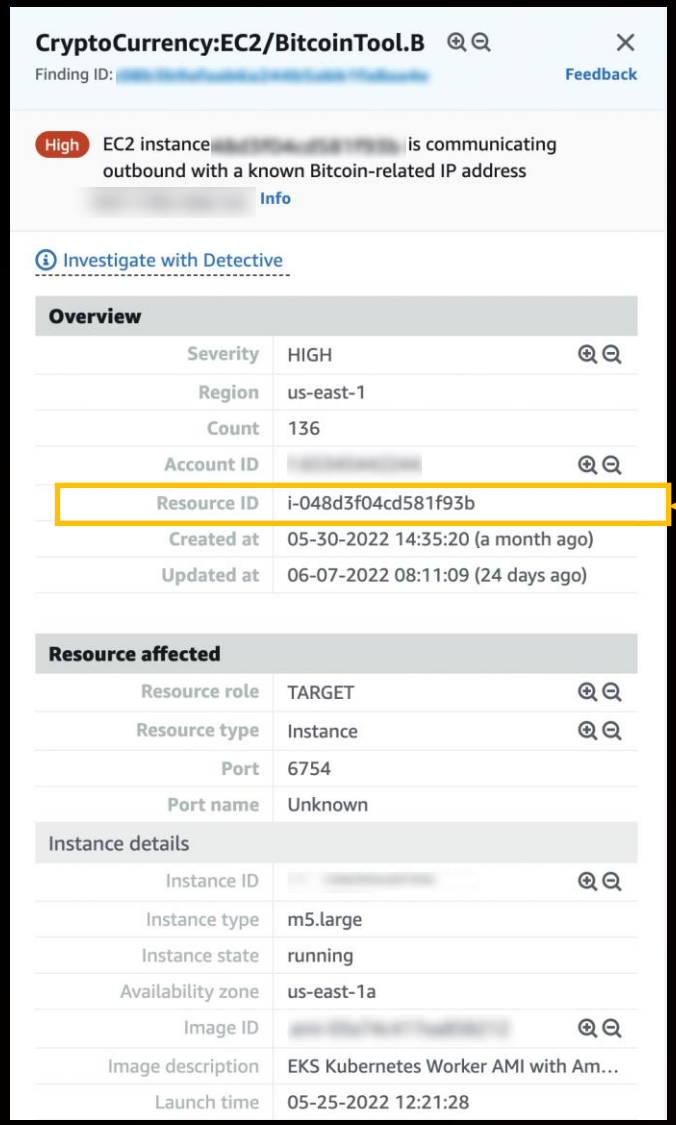
aws
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

How does it work?

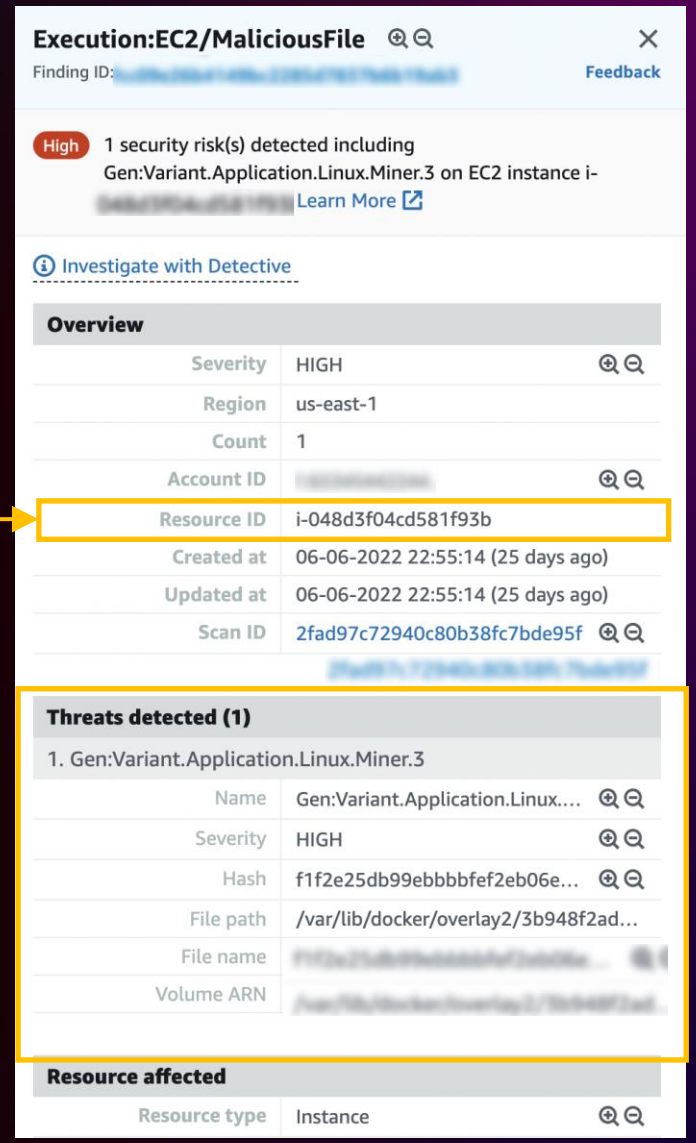


© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

GuardDuty Malware Protection findings

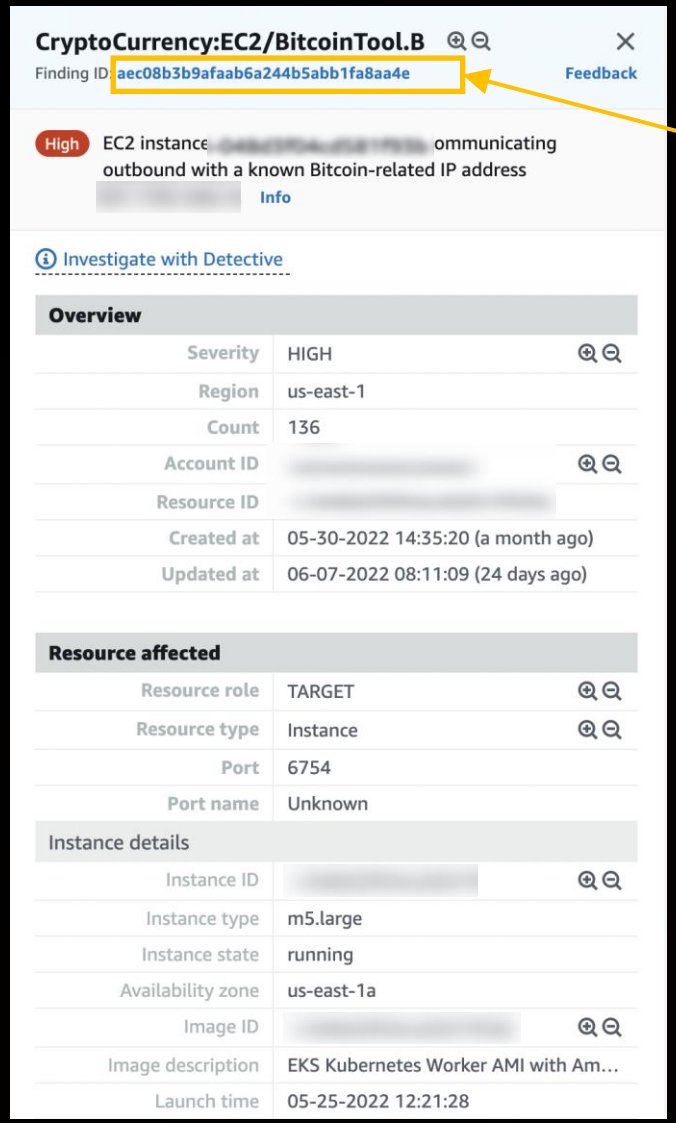


GuardDuty finding for Amazon EC2 instance communicating to bitcoin-related IP initiates a malware scan, detecting a Linux miner malware on the same instance



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

GuardDuty Malware Protection findings



CryptoCurrency:EC2/BitcoinTool.B

Finding ID: aec08b3b9afaab6a244b5abb1fa8aa4e Feedback

High EC2 instance [redacted] ommunicating outbound with a known Bitcoin-related IP address [redacted] Info

Investigate with Detective

Overview

Severity	HIGH
Region	us-east-1
Count	136
Account ID	[redacted]
Resource ID	[redacted]
Created at	05-30-2022 14:35:20 (a month ago)
Updated at	06-07-2022 08:11:09 (24 days ago)

Resource affected

Resource role	TARGET
Resource type	Instance
Port	6754
Port name	Unknown

Instance details

Instance ID	[redacted]
Instance type	m5.large
Instance state	running
Availability zone	us-east-1a
Image ID	[redacted]
Image description	EKS Kubernetes Worker AMI with Am…
Launch time	05-25-2022 12:21:28

Alert correlation between network-based and malware-related threats

Malware scan details

Scan ID	2fad97c72940c80b38fc7bde95f
Scan started at	06-06-2022 22:45:01 (25 days ago)
Scan completed at	06-06-2022 22:55:14 (24 days ago)
Files scanned	78407
Total gb scanned	4
Trigger finding ID	aec08b3b9afaab6a244b5abb…

Volume details

arn:aws:ec2:us-east-1[redacted]:volume/vol-04fb86f8c1fed5960

Volume ARN	arn:aws:ec2:us-east-[redacted]…
Snapshot ARN	arn:aws:ec2:us-east-[redacted]…
Status	Scanned
Encryption type	UNENCRYPTED
Device name	/dev/xvda

Threat intelligence details

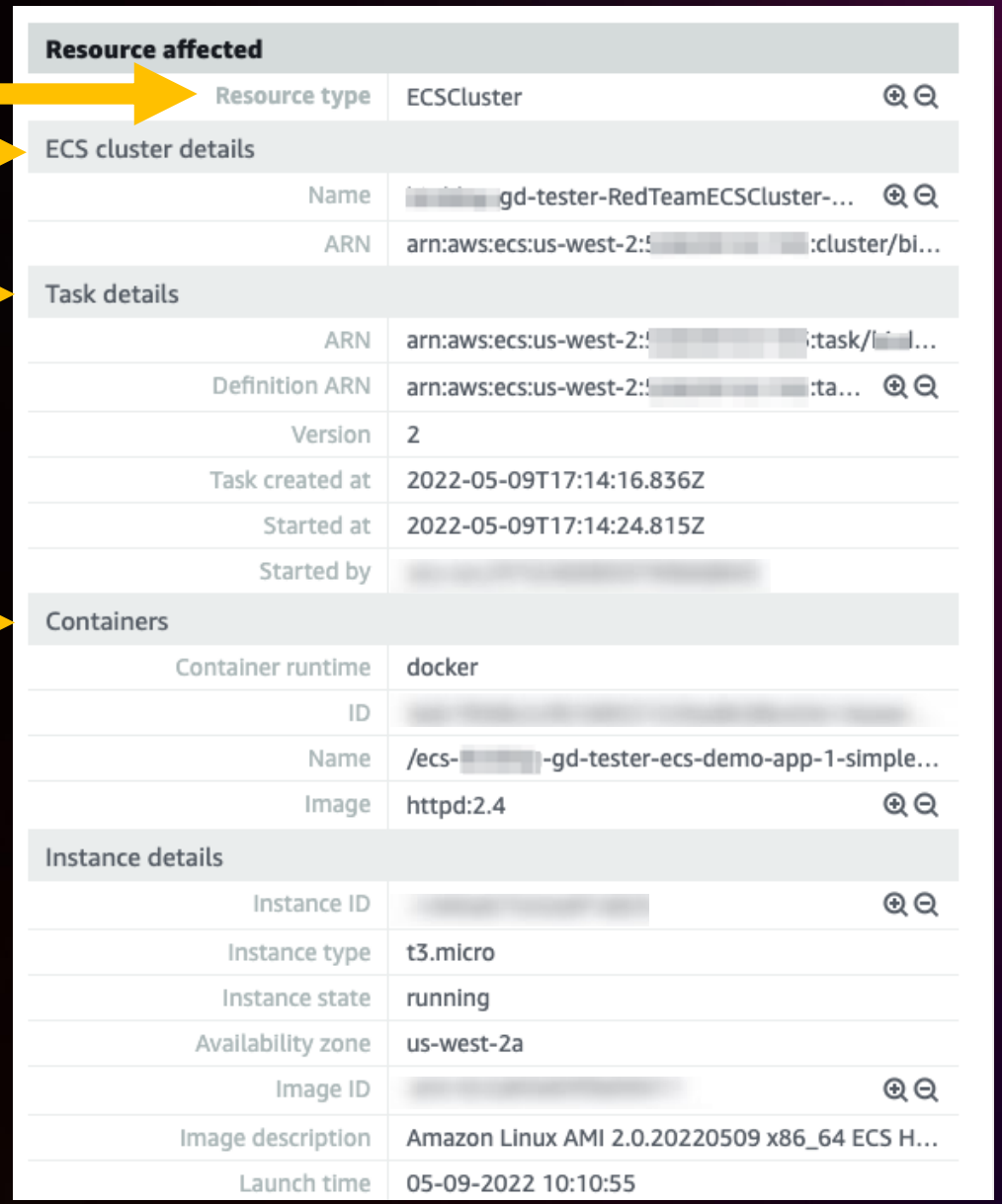
Sources	Bitdefender

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

GuardDuty Malware Protection findings – Containers

GuardDuty Malware Protection is container-aware, that is, it can detect malware files on Amazon ECS, Amazon EKS, and customer-managed Kubernetes running on Amazon EC2 instances

Allows customers to investigate the exact container that is compromised versus just the host



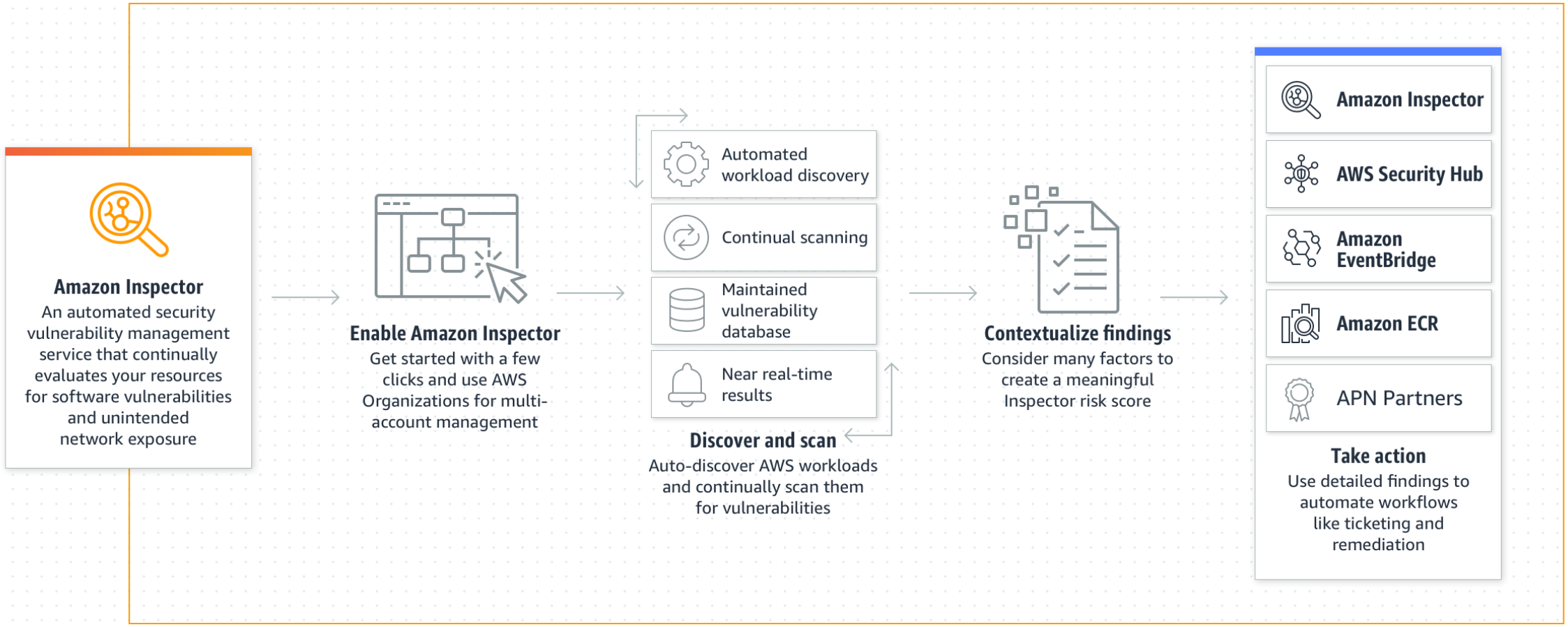
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.



Amazon Inspector

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

Amazon Inspector – How it works



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

How Amazon Inspector scans container images

Retrieve the image from Amazon ECR

Extract each layer of the image

Look at the OS and the installed packages

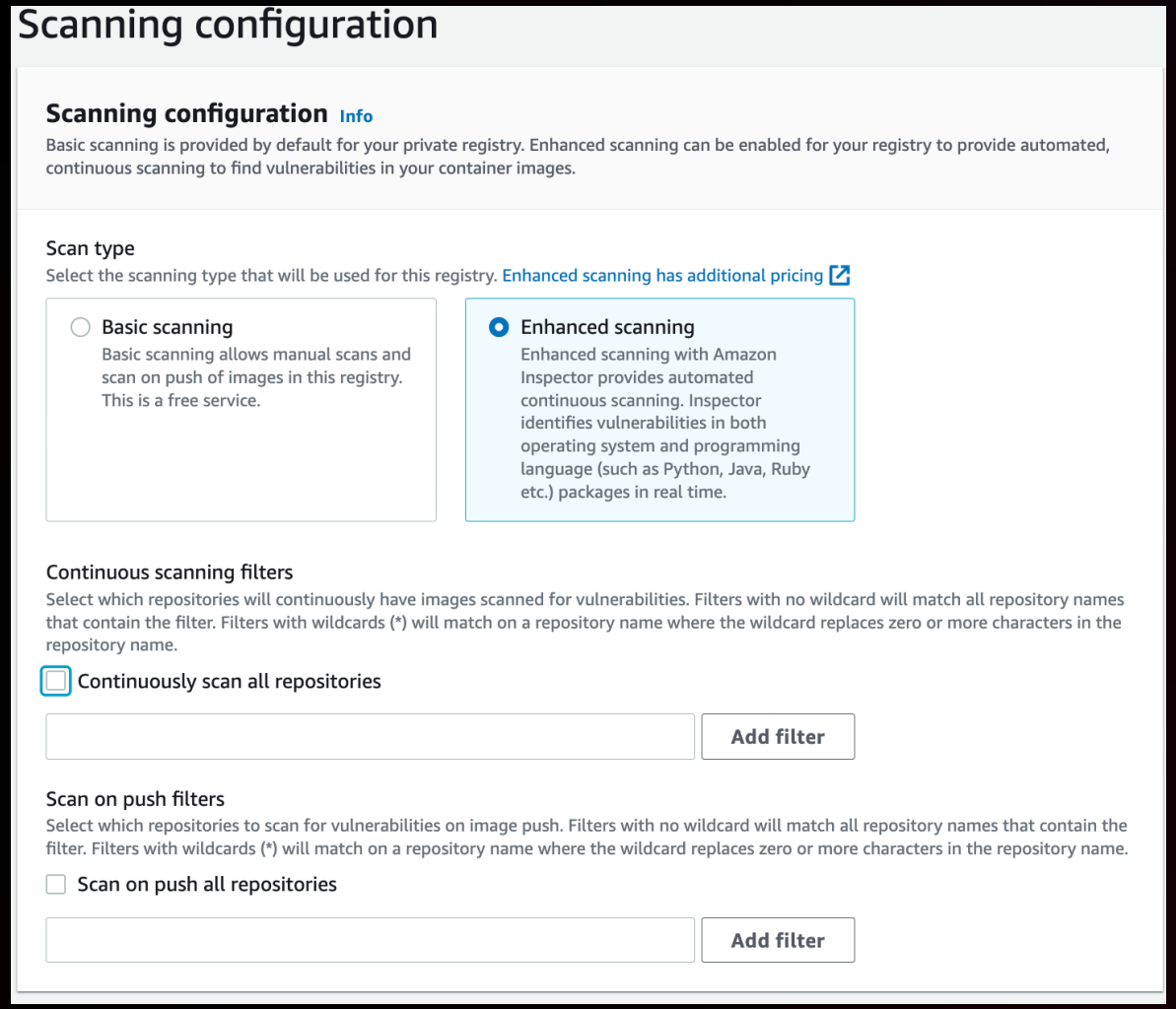
Look through the file system for other files

Compare against vulnerability database



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

Amazon Inspector configuration for container scanning



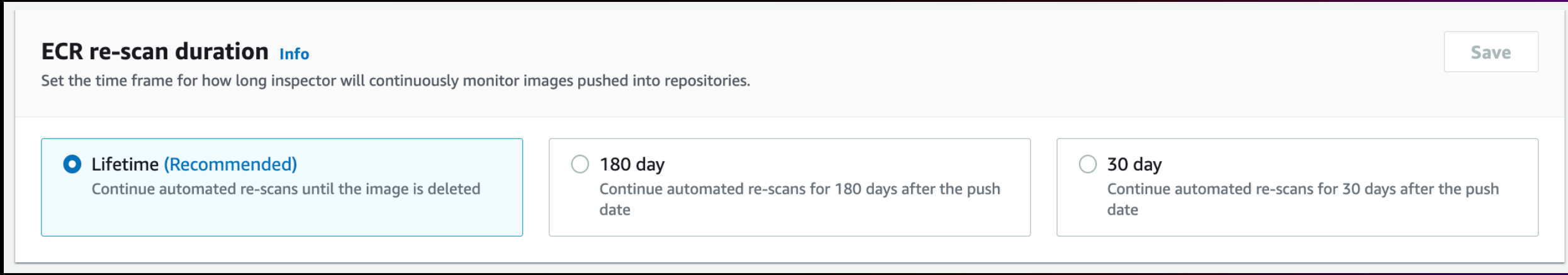
Configure repositories for continuous or on-push scanning

Configured in Amazon ECR private registry settings

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

Amazon Inspector configuration for container scanning

Configure re-scan configuration for continuous scanning

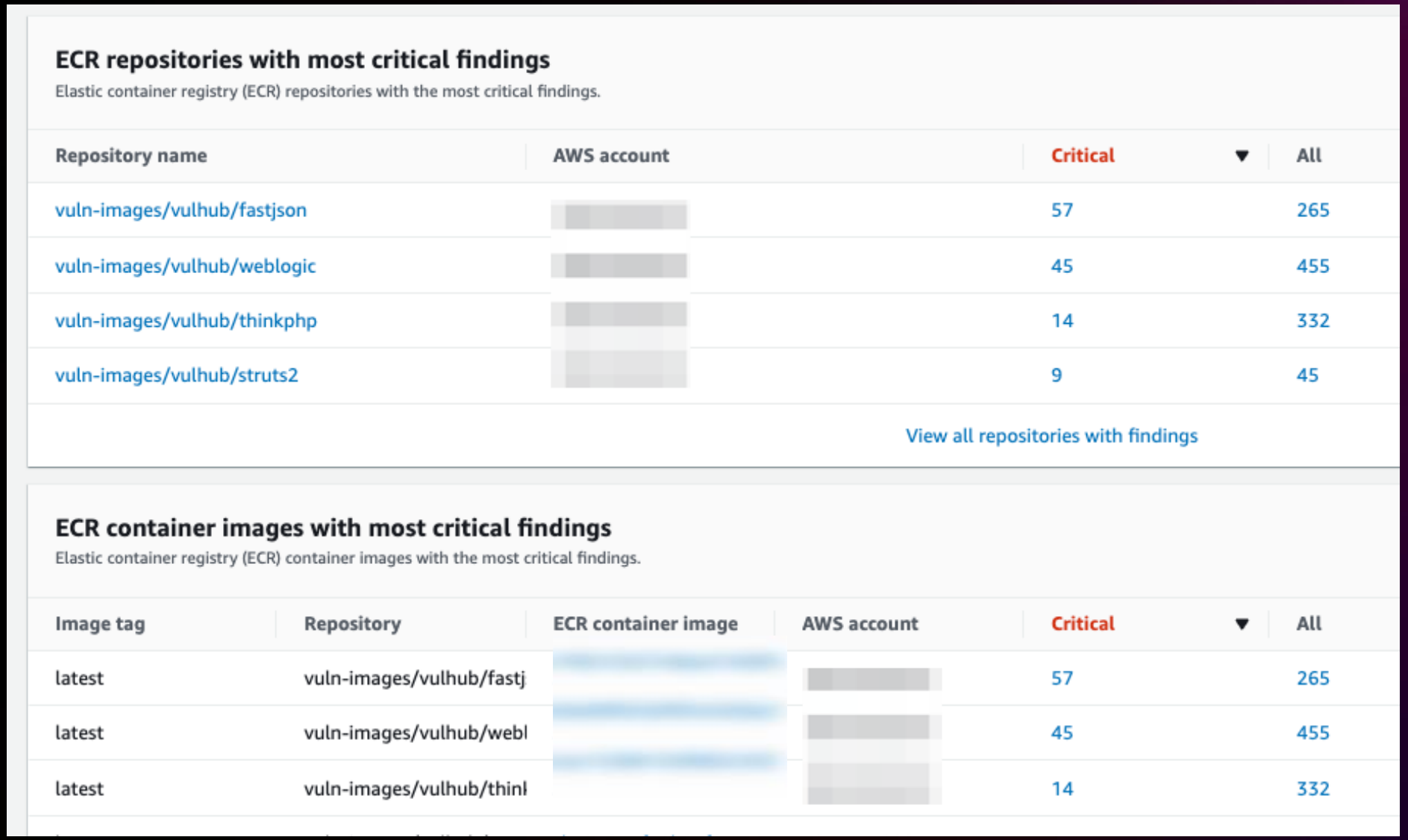


After re-scan duration is reached for an image:

- Image status changes to “inactive” with a reason code of “expired”
- Findings for the image are closed
- Closed findings are deleted after 30 days

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

Amazon Inspector container image summary info



ECR repositories with most critical findings

Elastic container registry (ECR) repositories with the most critical findings.

Repository name	AWS account	Critical ▼	All
vuln-images/vulhub/fastjson	[redacted]	57	265
vuln-images/vulhub/weblogic	[redacted]	45	455
vuln-images/vulhub/thinkphp	[redacted]	14	332
vuln-images/vulhub/struts2	[redacted]	9	45

View all repositories with findings

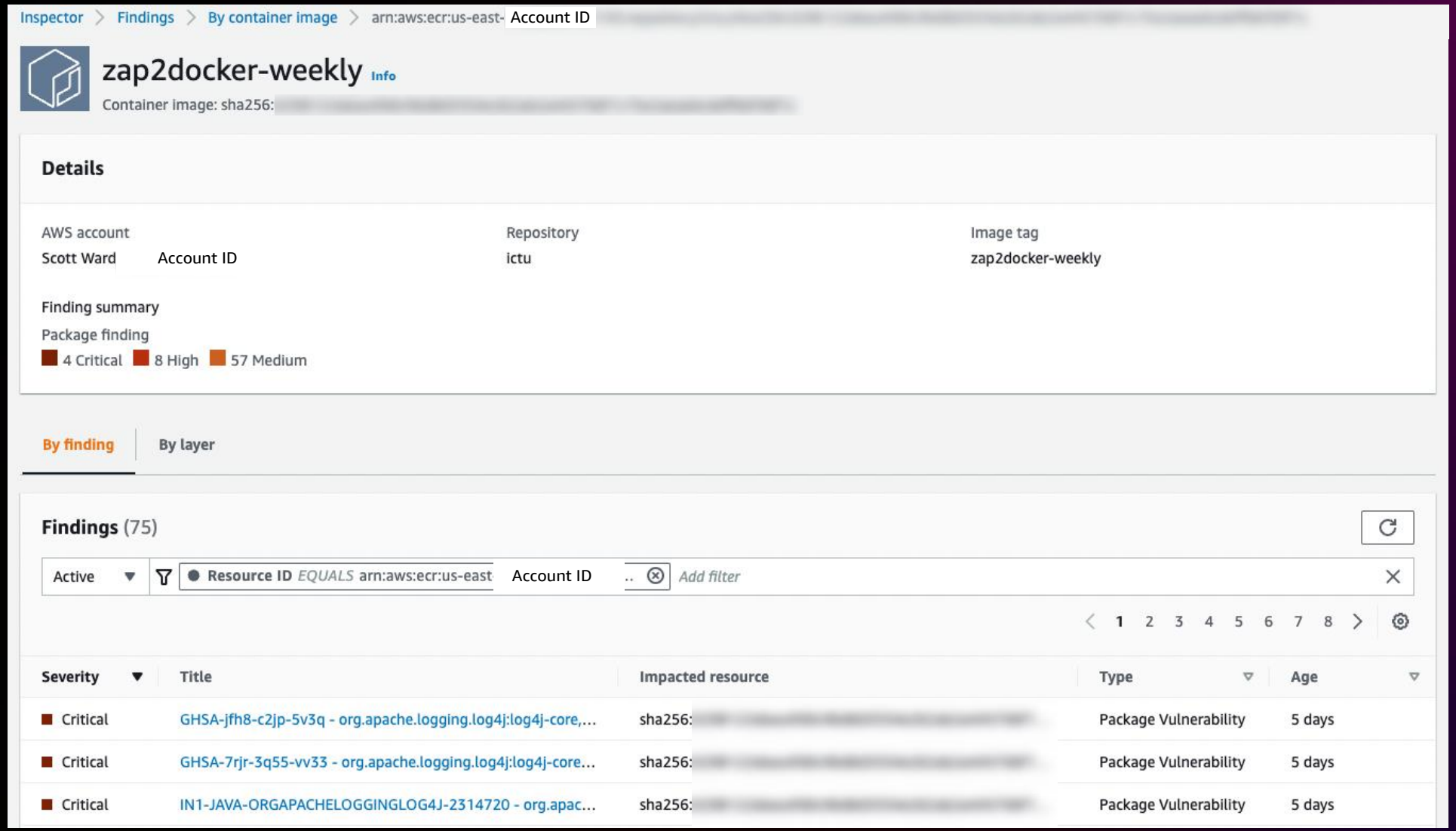
ECR container images with most critical findings

Elastic container registry (ECR) container images with the most critical findings.

Image tag	Repository	ECR container image	AWS account	Critical ▼	All
latest	vuln-images/vulhub/fastj	[redacted]	[redacted]	57	265
latest	vuln-images/vulhub/webl	[redacted]	[redacted]	45	455
latest	vuln-images/vulhub/thinl	[redacted]	[redacted]	14	332

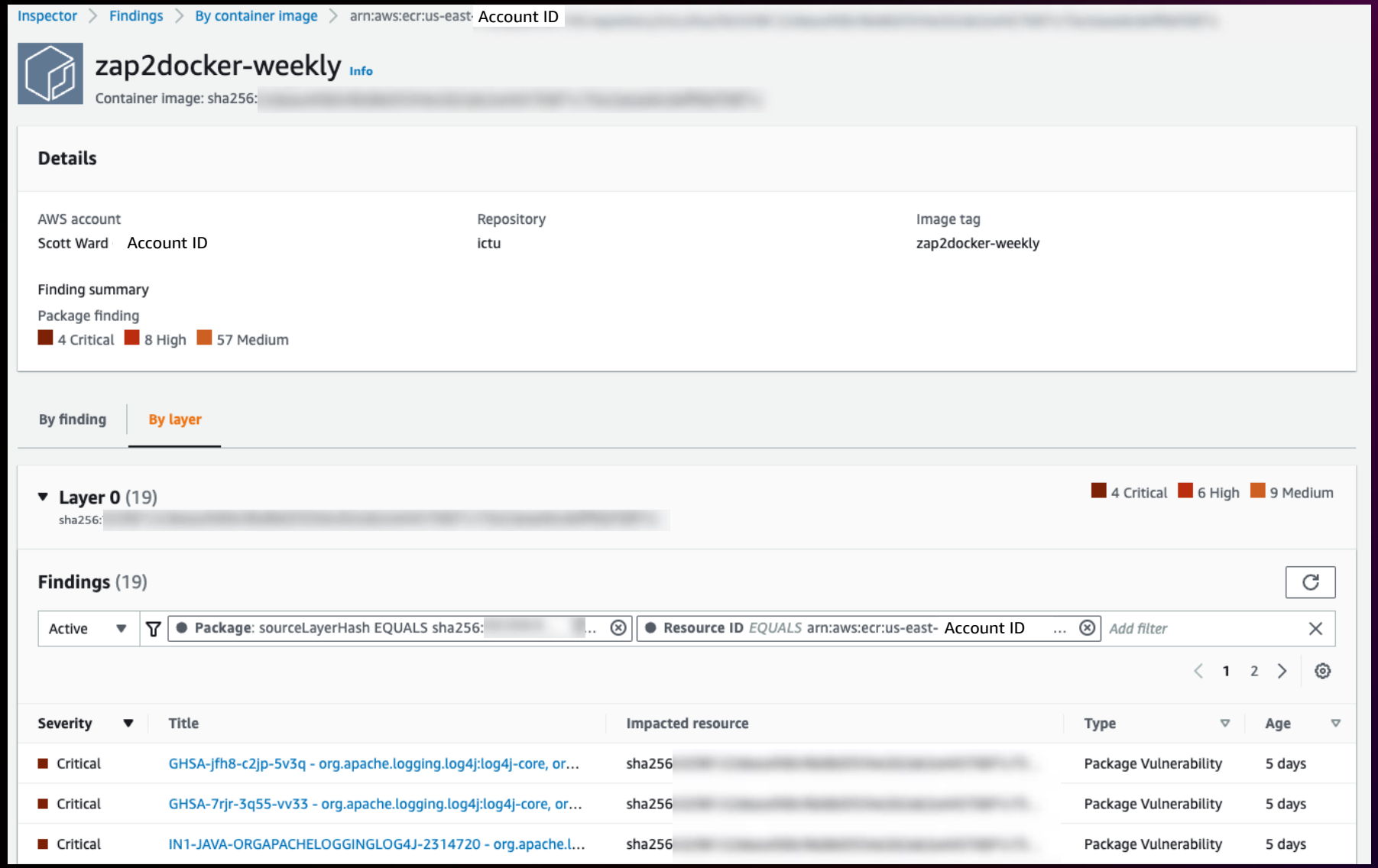
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Amazon Inspector container image findings



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

Amazon Inspector image layer findings

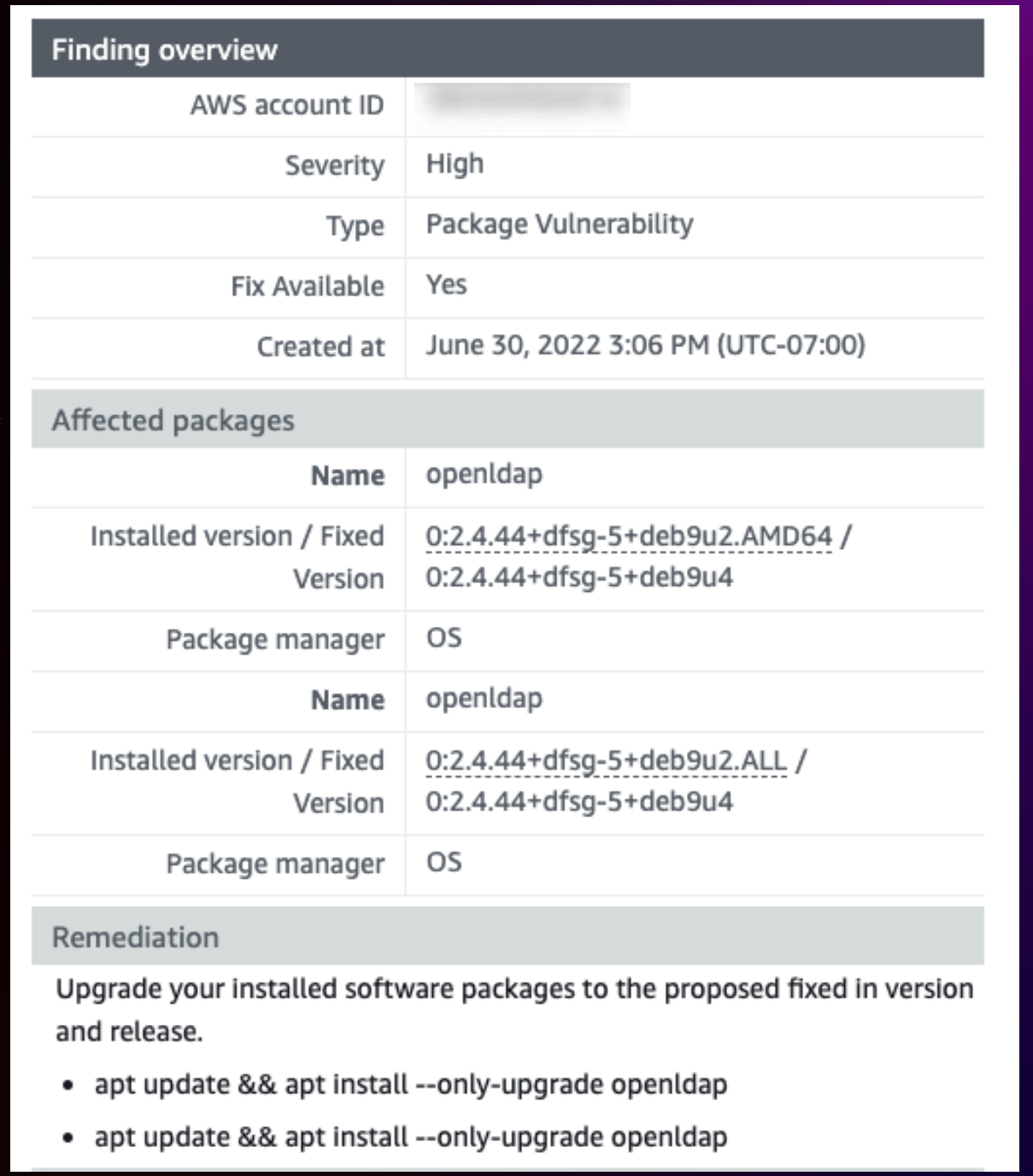


© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Remediation guidance

Fixed version for affected packages

Remediation to upgrade software packages



Finding overview

AWS account ID	[redacted]
Severity	High
Type	Package Vulnerability
Fix Available	Yes
Created at	June 30, 2022 3:06 PM (UTC-07:00)

Affected packages

Name	openldap
Installed version / Fixed Version	0:2.4.44+dfsg-5+deb9u2.AMD64 / 0:2.4.44+dfsg-5+deb9u4
Package manager	OS
Name	openldap
Installed version / Fixed Version	0:2.4.44+dfsg-5+deb9u2.ALL / 0:2.4.44+dfsg-5+deb9u4
Package manager	OS

Remediation

Upgrade your installed software packages to the proposed fixed in version and release.

- apt update && apt install --only-upgrade openldap
- apt update && apt install --only-upgrade openldap

aws

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

Consumption of Amazon Inspector findings



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

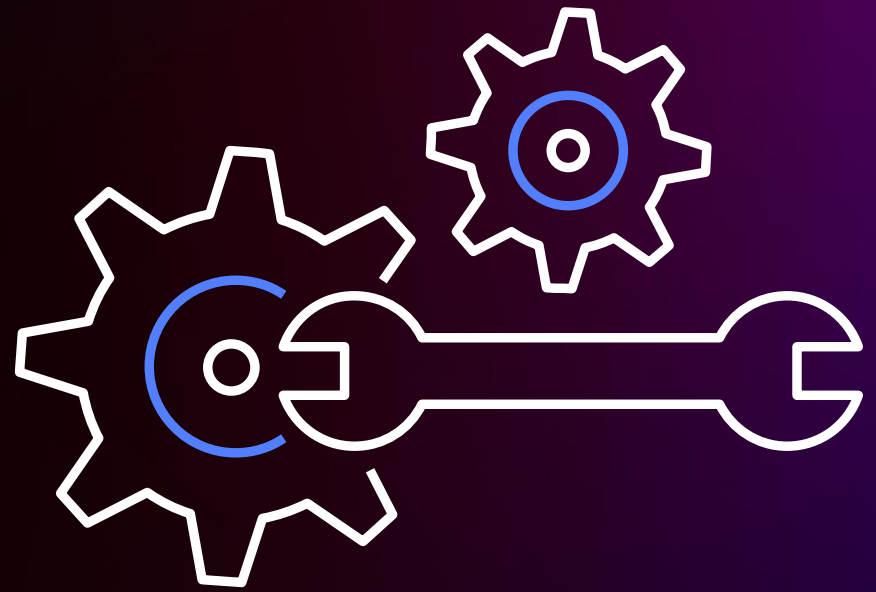
Remediating Amazon Inspector container findings

Delete the image in the Amazon ECR repository

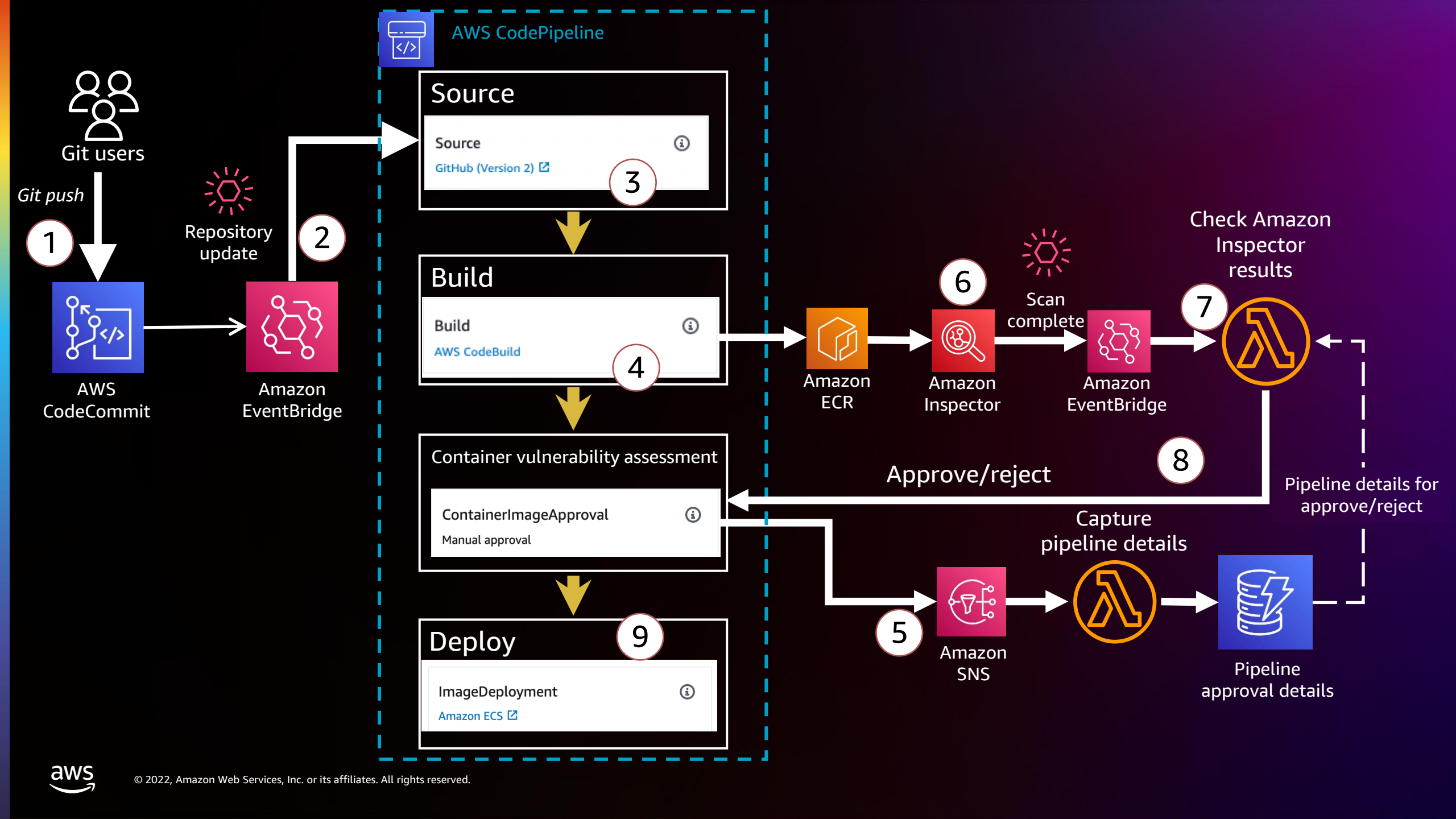
- Closes associated findings

Publish an updated image

- Updates scan results



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



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

Using inspector in build and deploy pipelines

AWS Security Blog

Use Amazon Inspector to manage your build and deploy pipelines for containerized applications

by Scott Ward | on 03 NOV 2022 | in Amazon Elastic Container Registry, Amazon Inspector, Intermediate (200), Security, Identity, & Compliance, Technical How-To | Permalink | Comments | Share



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

HBO Max

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



One-of-a-kind streaming service, delivering unique stories, complex characters, immersive new worlds

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



HBO Max – Infrastructure scale

- Mix of K8S and EKS self-managed nodes
- Tens of thousands of containers during prime time
- Billions of API requests/day
- Hundreds of clusters
- Hundreds of microservices
- Petabytes of logs/year

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

Container risks and threats

- Vulnerable application code
- Poorly configured containers and pods
- Insecure networking
- Vulnerable hosts

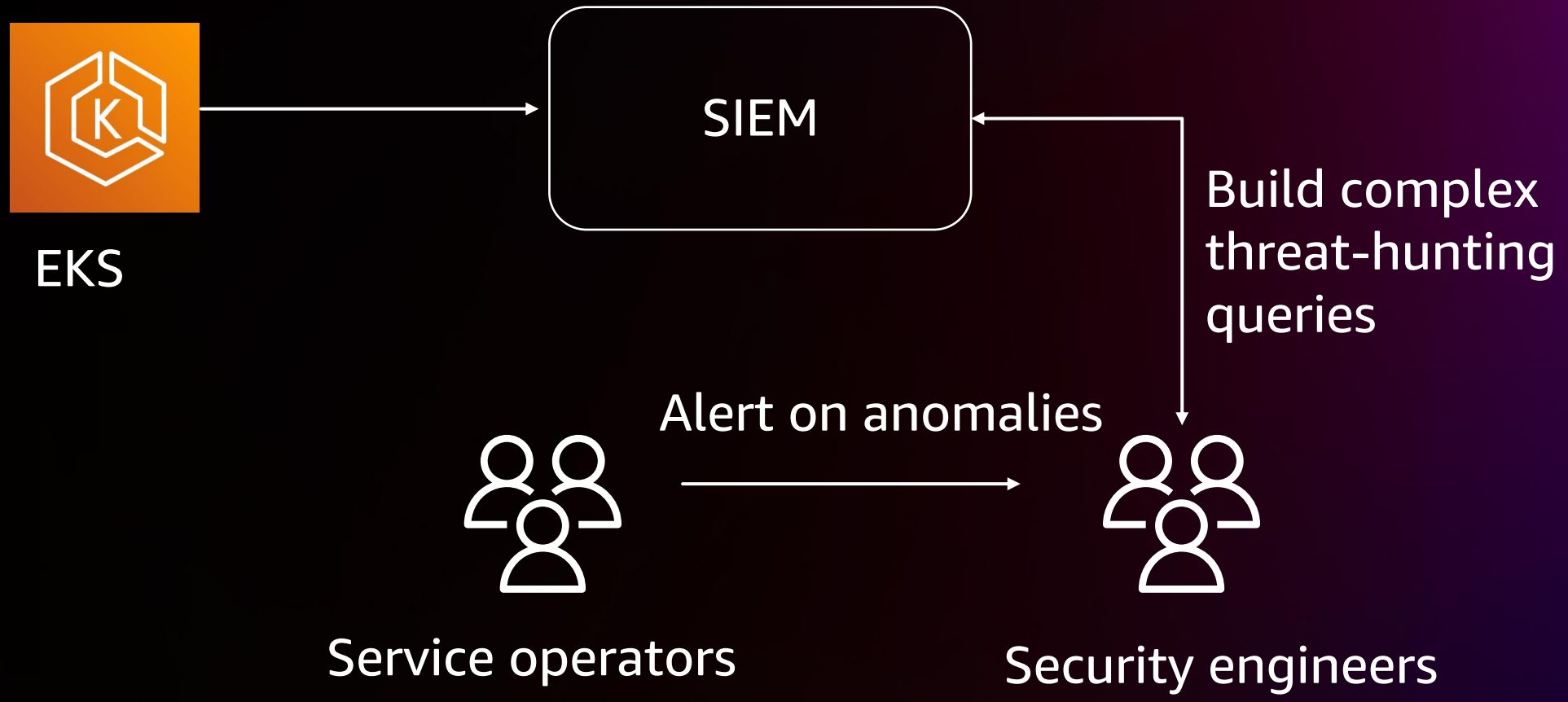
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Container risks and threats

- Overprivileged services and users on the cluster
- Secrets exposure

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

Traditional threat detection



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

Challenges with traditional threat detection

01 Difficult to detect malicious patterns

02 Complex queries for disjointed datasets

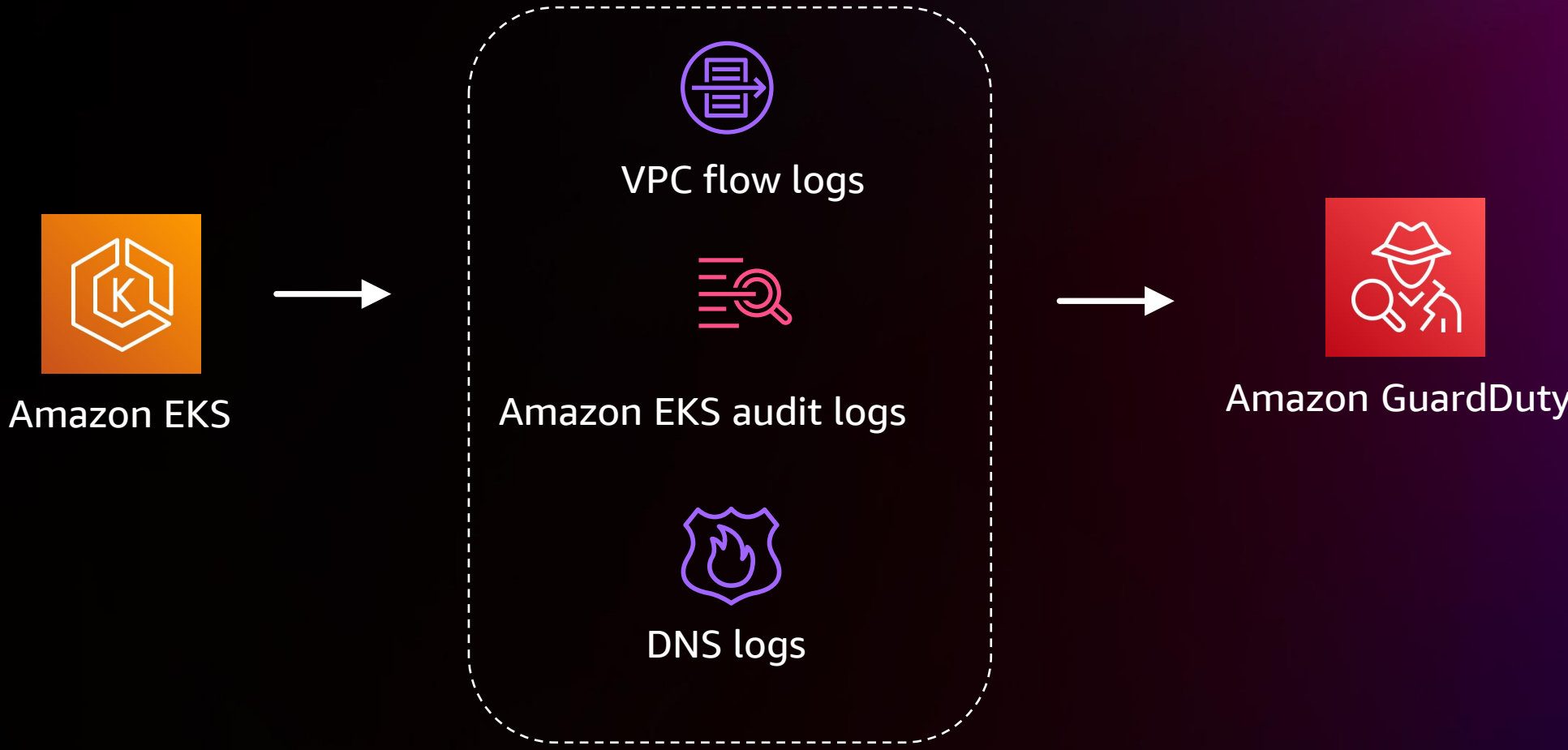
03 Complex infrastructure setup required

04 Real-time alerts not always achievable

aws

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

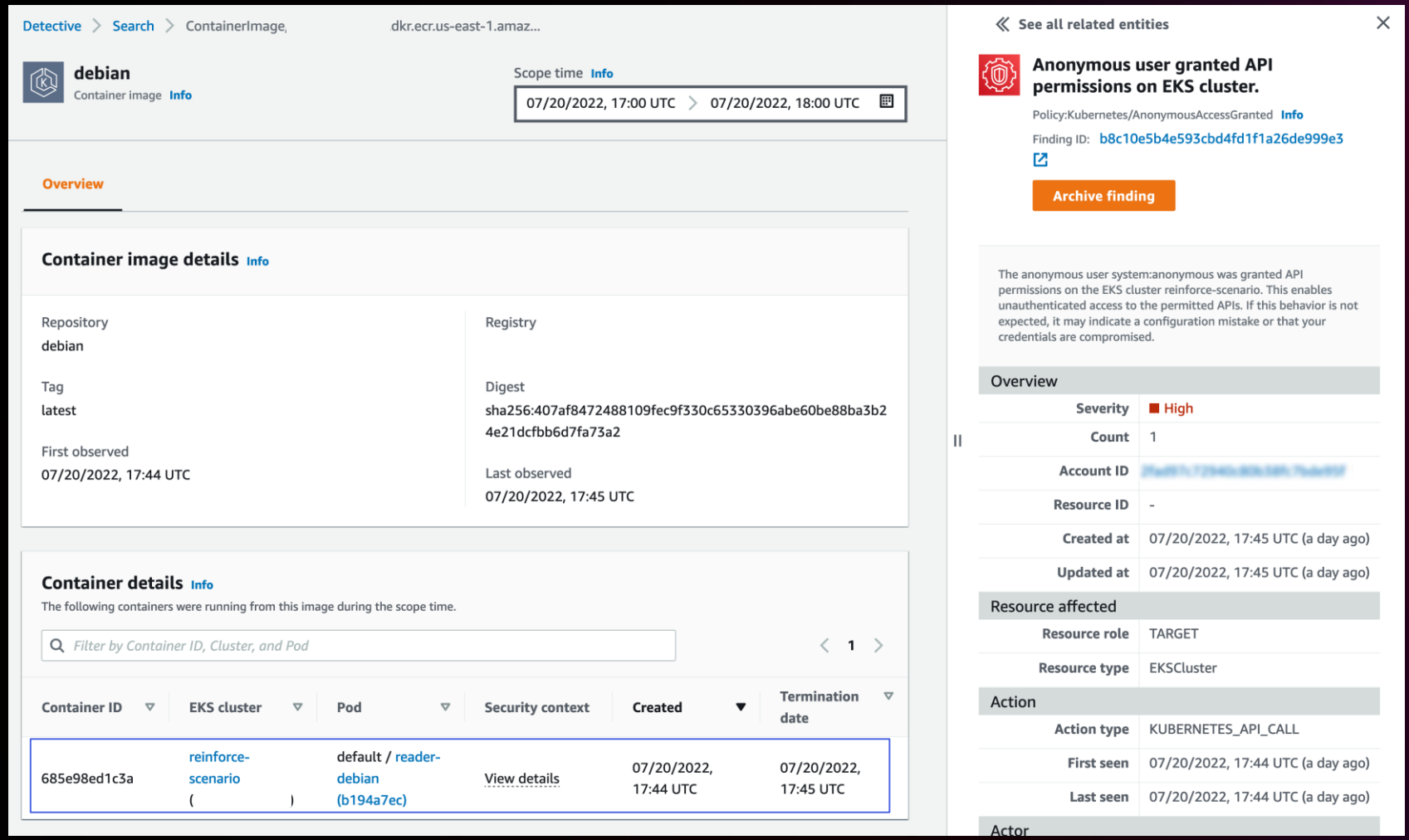
GuardDuty to the rescue



Automated cluster threat monitoring

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

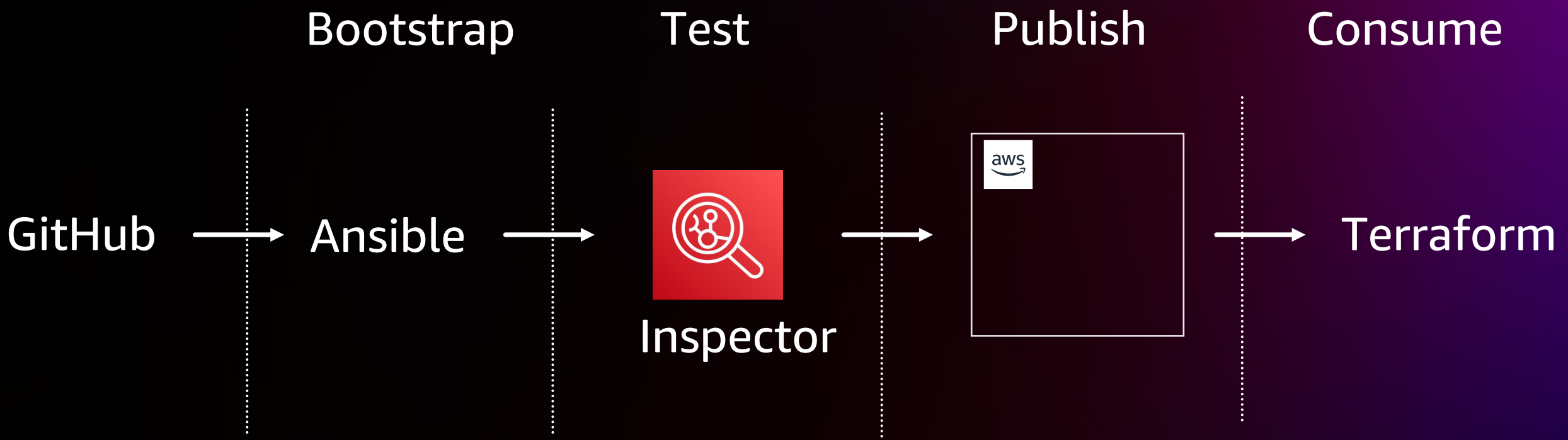
Investigate with Detective



Amazon Detective is integrated with Amazon GuardDuty and provides a set of linked data to conduct faster and more efficient investigations

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

Inspector – Gold AMI build process



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

How does Inspector help with fixing image issues?

Detect → Remediate → Verify

- Detect Vulnerable Image
- Identify Layers introducing Vulnerabilities

- Swap to a more secure base image
- Upgrade Packages
- Remove Packages

- Verify security
- Enforce continuous compliance

aws

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

Multi-stage docker builds

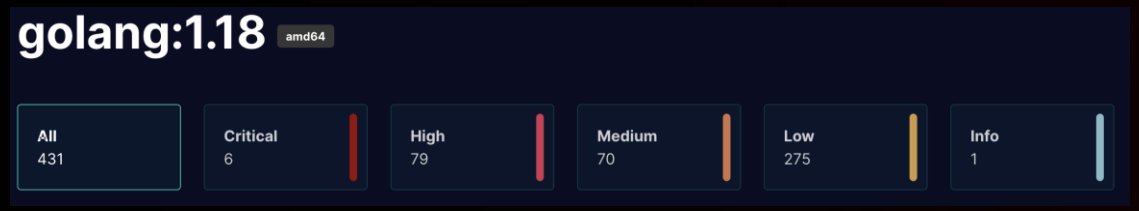
```
FROM golang:1.18
WORKDIR /go/src/app
COPY . .

RUN go mod download
RUN CGO_ENABLED=0 go build -o /go/bin/app
CMD ["/app"]
```



```
# Use build image to build the binary.
FROM golang:1.18 as build
WORKDIR /go/src/app
COPY . .
RUN go mod download
RUN CGO_ENABLED=0 go build -o /go/bin/app

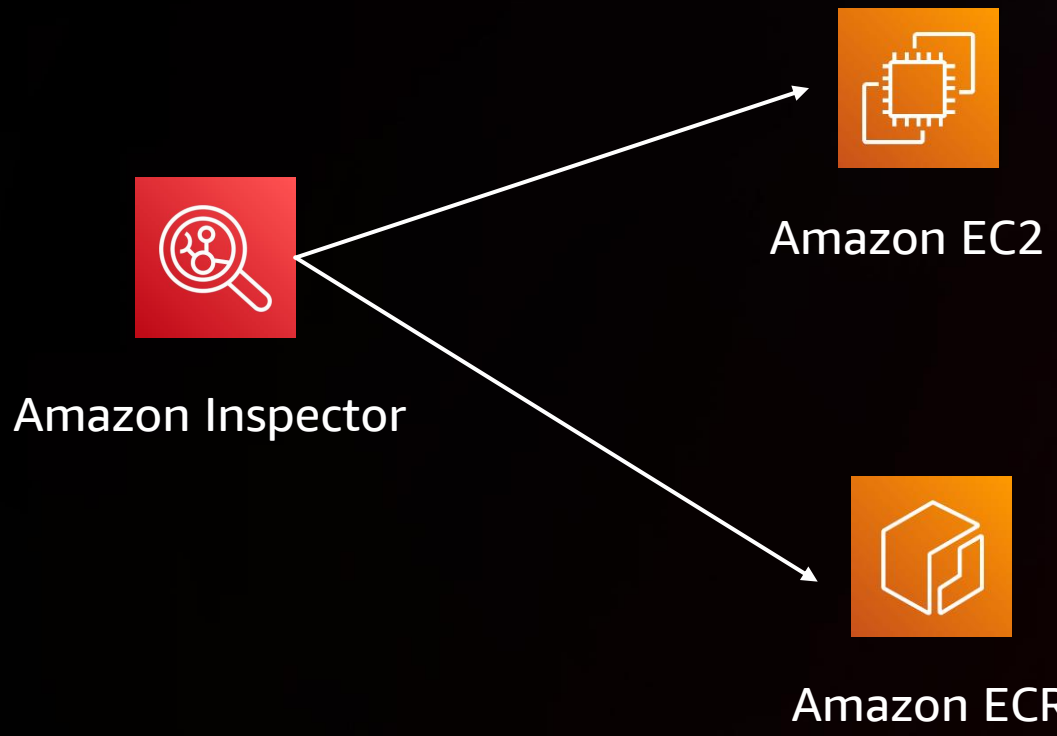
# Copy only build artifact to a new secure image.
FROM gcr.io/distroless/static-debian11
COPY --from=build /go/bin/app /
CMD ["/app"]
```





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

Inspector - Container registry and host scanning

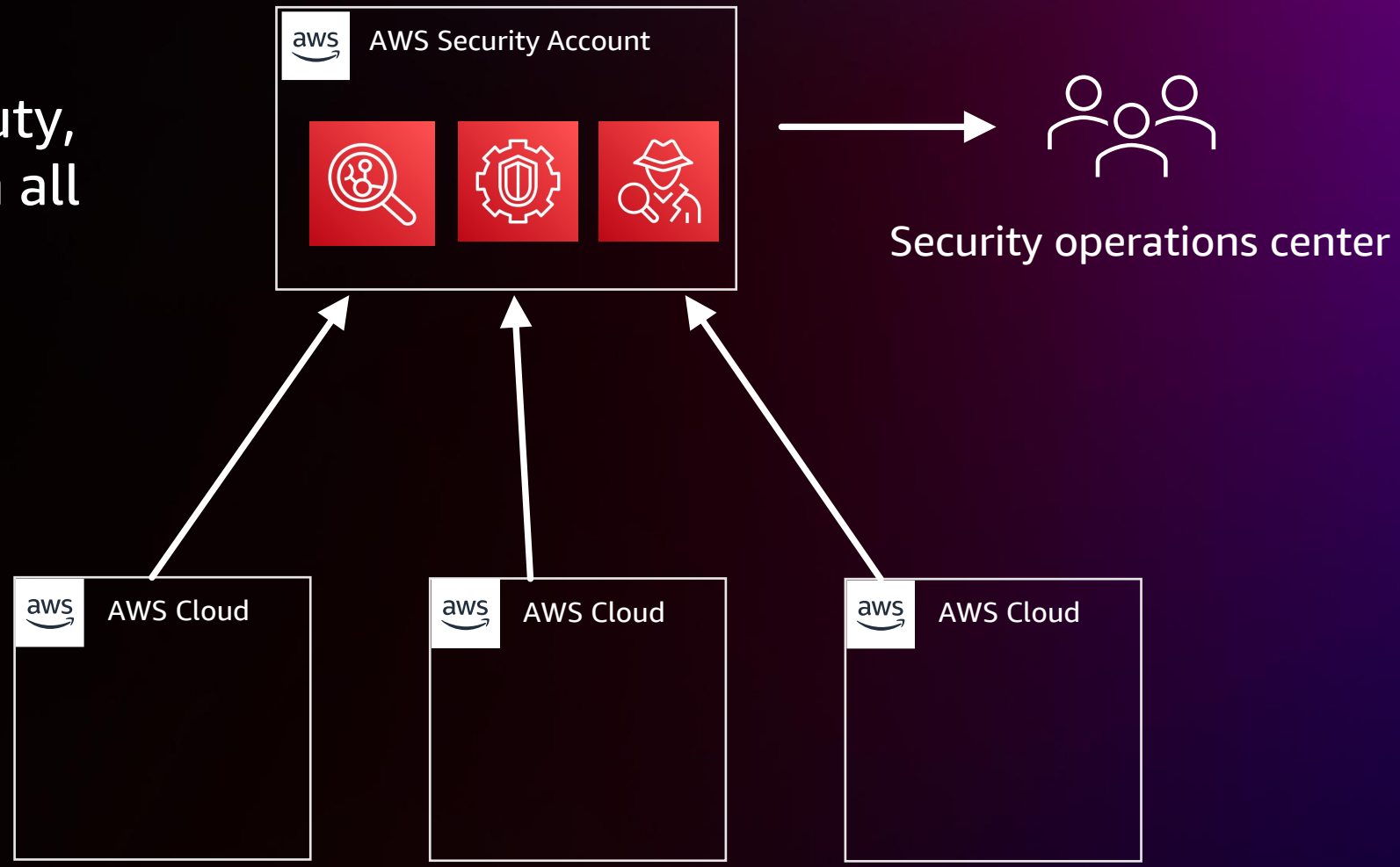


Inspector provides automated vulnerability management for both hosts and containers

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

Logging and monitoring – Organization

Consolidate Amazon GuardDuty, Inspector, and Detective from all accounts into one



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