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

SEC309

Threat detection and incident response using cloud-native services

Margo Cronin

Specialist Solutions Architect,
Security & Compliance
AWS

Armin Schneider

Specialist Solutions Architect,
Security & Compliance
AWS

aws

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

Agenda

The incident response lifecycle

- What's different in the cloud
- What remains the same
- How cloud-native services are related to the cycle

Let's look into the phases

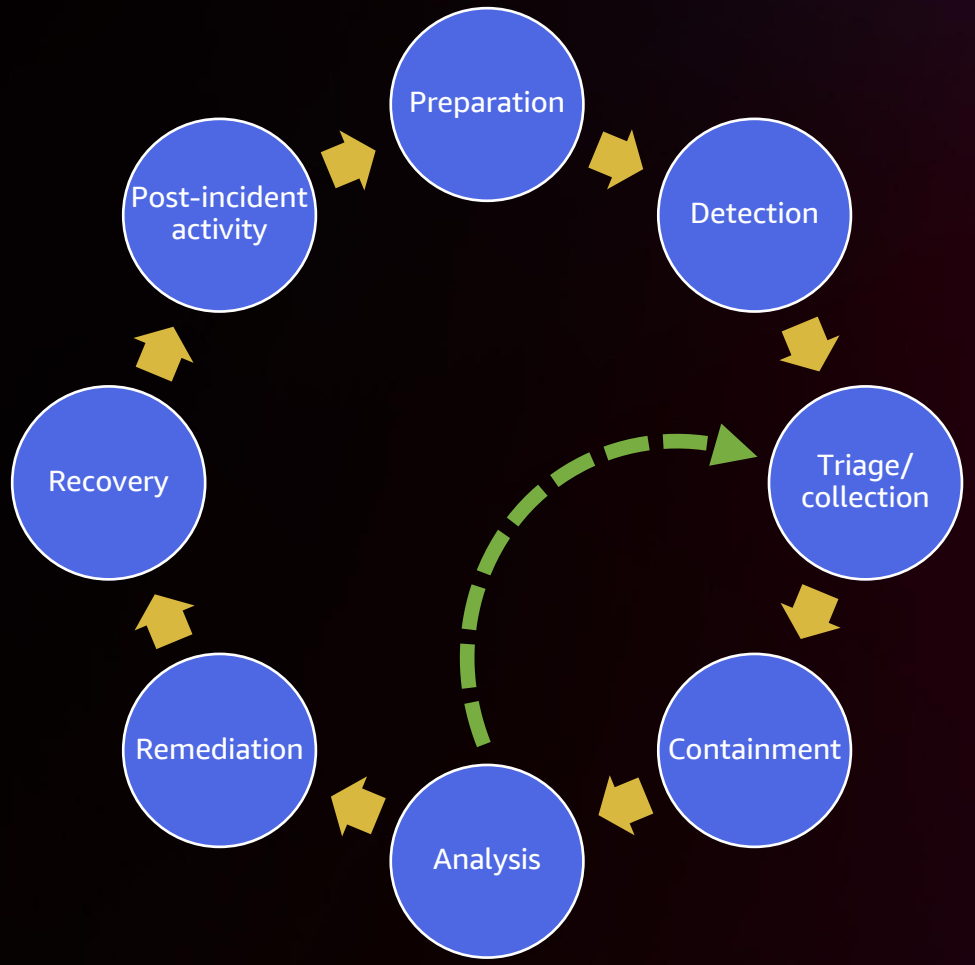
- Preparation
- Detection
- Triage – Collection, containment, and analysis
- Remediation, recovery, and post-incident activity

Summary and conclusion

aws

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

Incident response lifecycle



Based on NIST 800-61 incident response lifecycle

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

What’s different in the cloud

The cloud does add an additional layer, **the control plane**

- Offers a paradigm shift in how environments exist/operate
- Contains additional logs and artifacts to understand and analyze
- Offers much more scalable methods for response
- Continuous iteration between lifecycle phases

aws

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

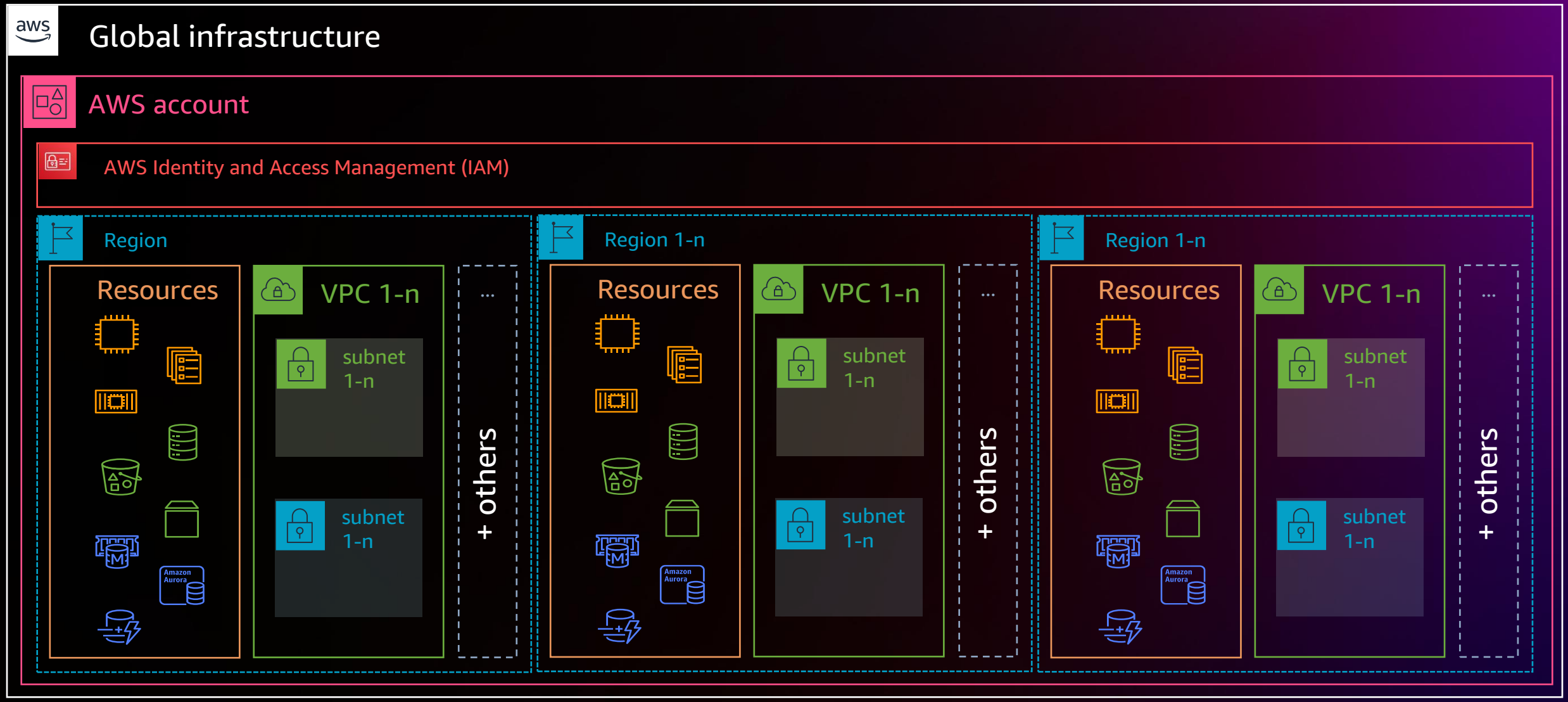
AWS Cloud – Global infrastructure



aws.amazon.com/about-aws/global-infrastructure

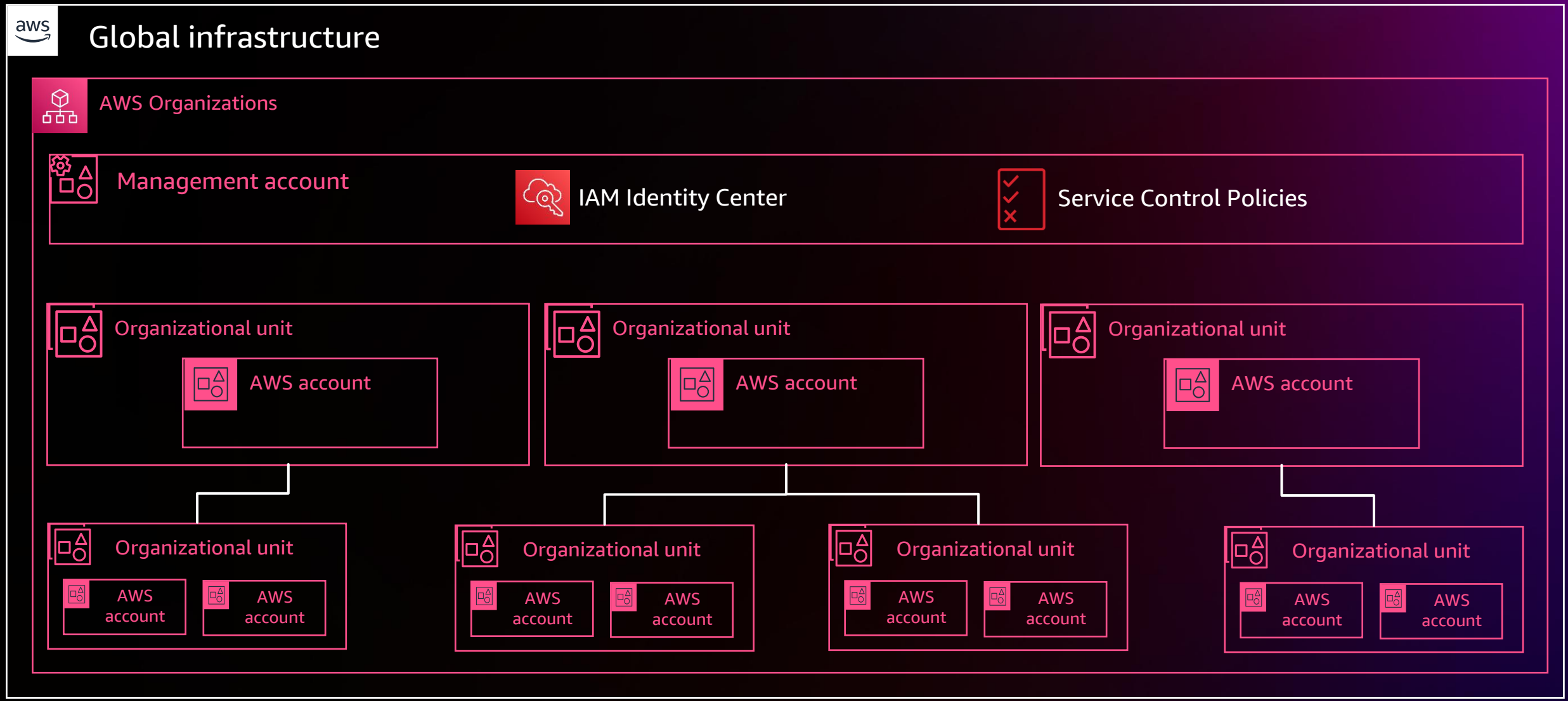
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

AWS Cloud – Accounts



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

AWS Cloud – Multiple accounts & organizations



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

What remains the same

That said, many other incident response tasks remain the same

- The general process for performing incident response
- Subject-matter expertise is still critical for being effective
- Native (OS) logs still need to be monitored, acquired, and analyzed
- Endpoints still need to be acquired and analyzed

aws

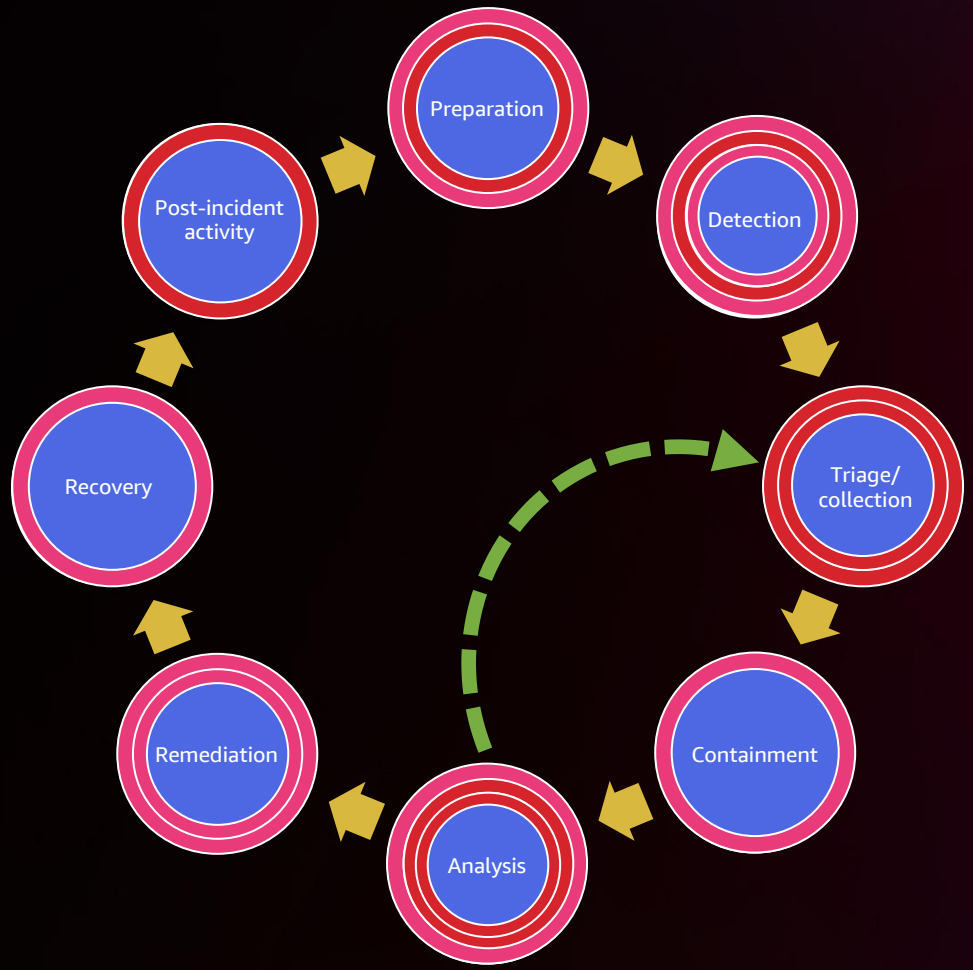
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

How cloud-native services are related to the cycle

AWS CloudTrail

AWS Systems Manager

AWS Config



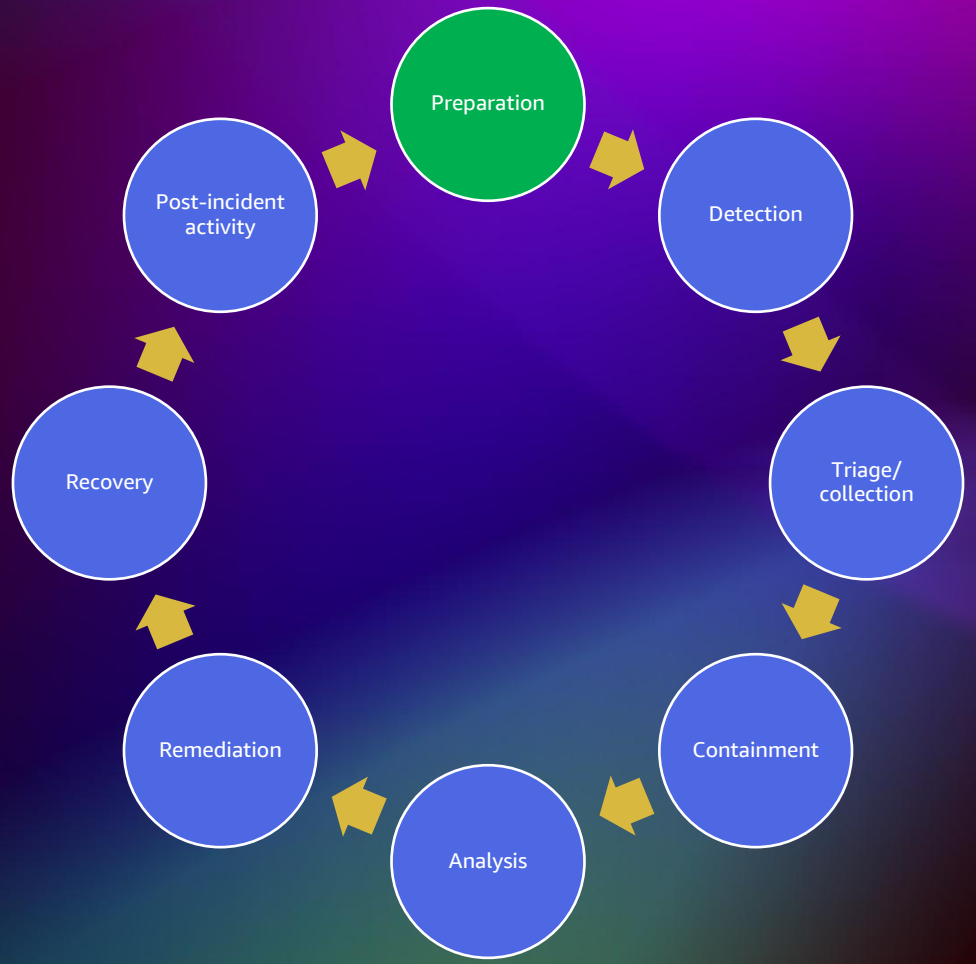
Amazon GuardDuty

AWS Security Hub

Amazon Detective

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

Preparation



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

Configure core services in AWS

- ✓ AWS Config
- ✓ Amazon GuardDuty
- ✓ AWS Systems Manager
- ✓ AWS Firewall Manager
- ✓ AWS Security Hub
- ✓ AWS WAF
- ✓ Amazon Detective
- ✓ . . .

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

Configure core logs in AWS

- ✓ AWS CloudTrail
- ✓ Amazon CloudWatch
- ✓ Load balancers: Application Load Balancer, Elastic Load Balancing (ELB), Network Load Balancer
- ✓ Amazon CloudFront
- ✓ AWS Network Firewall
- ✓ Amazon Route 53
- ✓ Amazon S3 Access Logs
- ✓ Amazon VPC Flow Logs
- ✓ AWS WAF Logs
- ✓ . . .

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

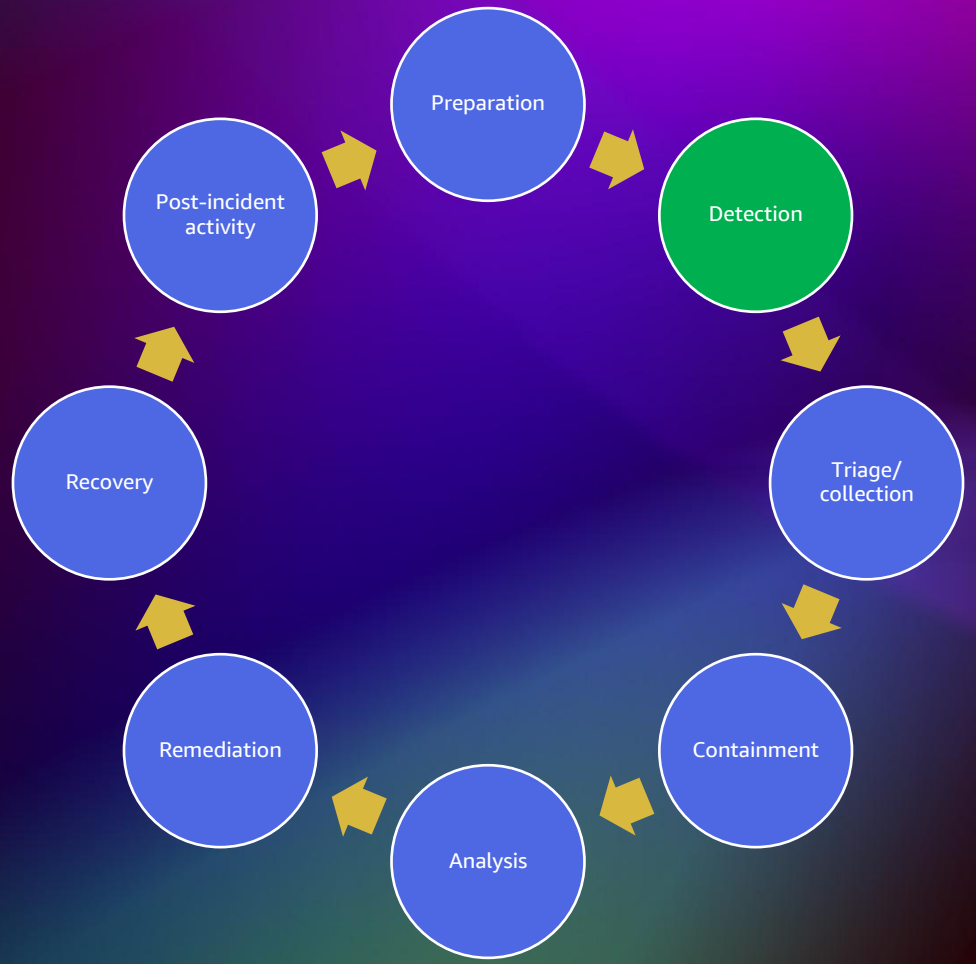
Prepare your forensic environment in AWS

- ✓ Create forensic organizational unit/accounts
- ✓ Configure service control policies
- ✓ Prepare containment mechanisms
  - ✓ Host firewall, security groups, NACLs, . . .
  - ✓ Amazon VPC Traffic Mirroring
- ✓ Prepare forensic tools
- ✓ Have your log analysis ready
- ✓ . . .

aws

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

Detection



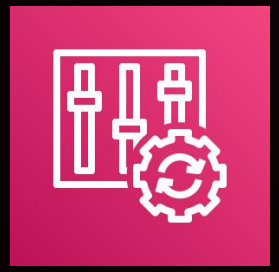
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Detection using AWS services



GuardDuty

Analyze log data for anomalies and malicious behavior



AWS Config

Check configuration status and rule compliance



Amazon Inspector

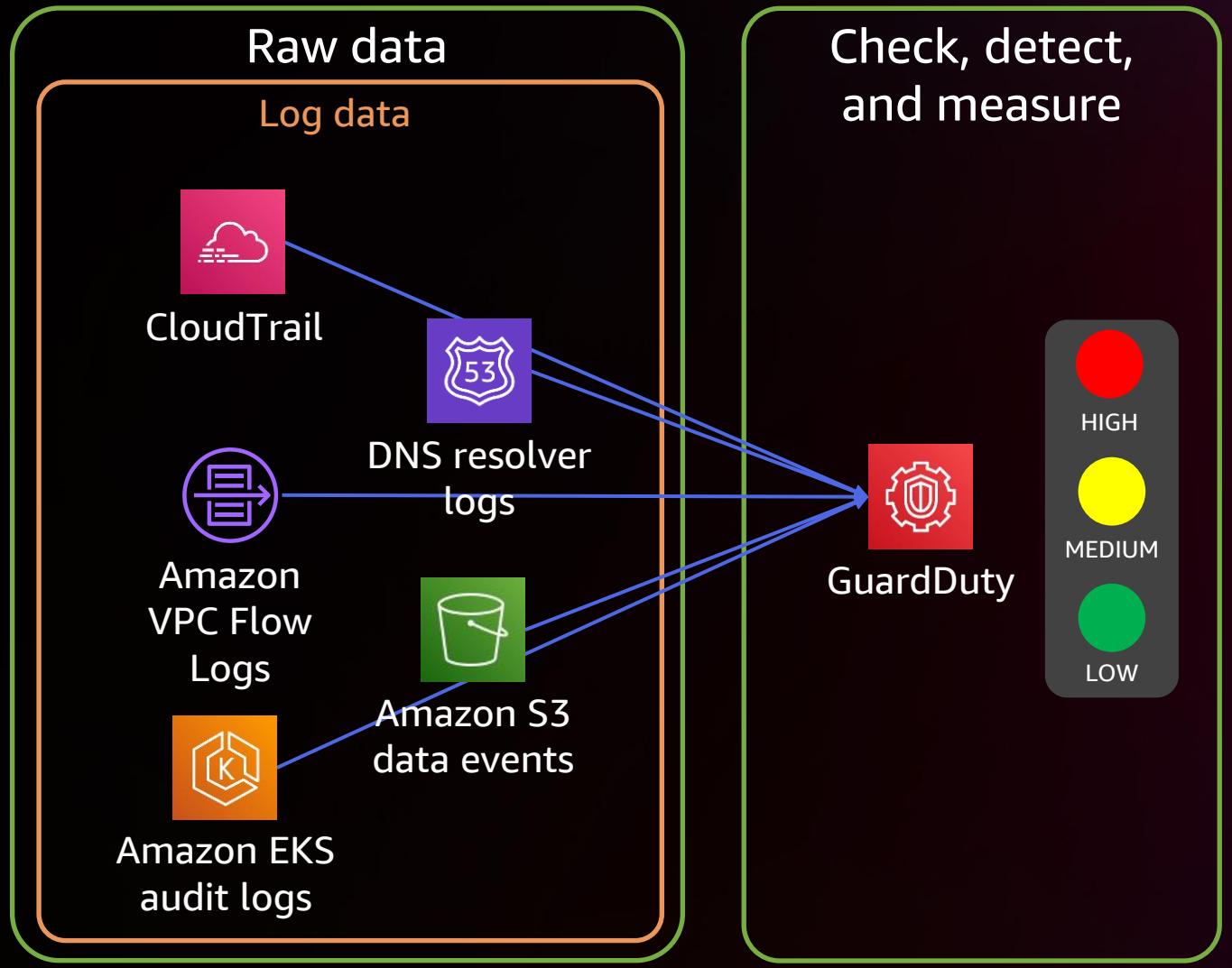
Check for software vulnerabilities

aws

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

How GuardDuty works

No configuration needed for this log source



Threat detection types:

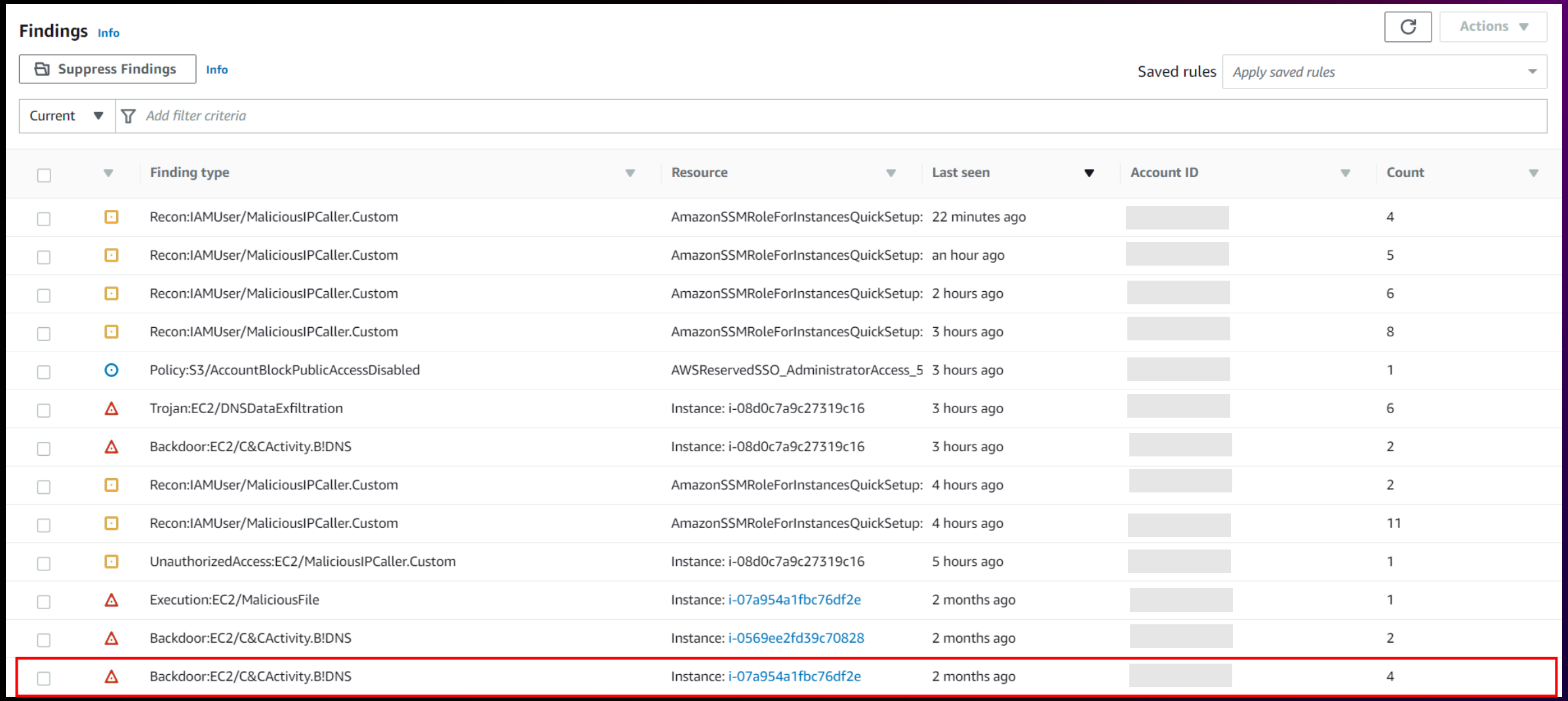
- Threat intelligence
- Anomaly detection

Finding types (examples):

- Bitcoin mining
- Command and control activity
- Unusual user behavior
- Unusual traffic patterns

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

GuardDuty findings



Findings Info

Actions

Suppress Findings Info

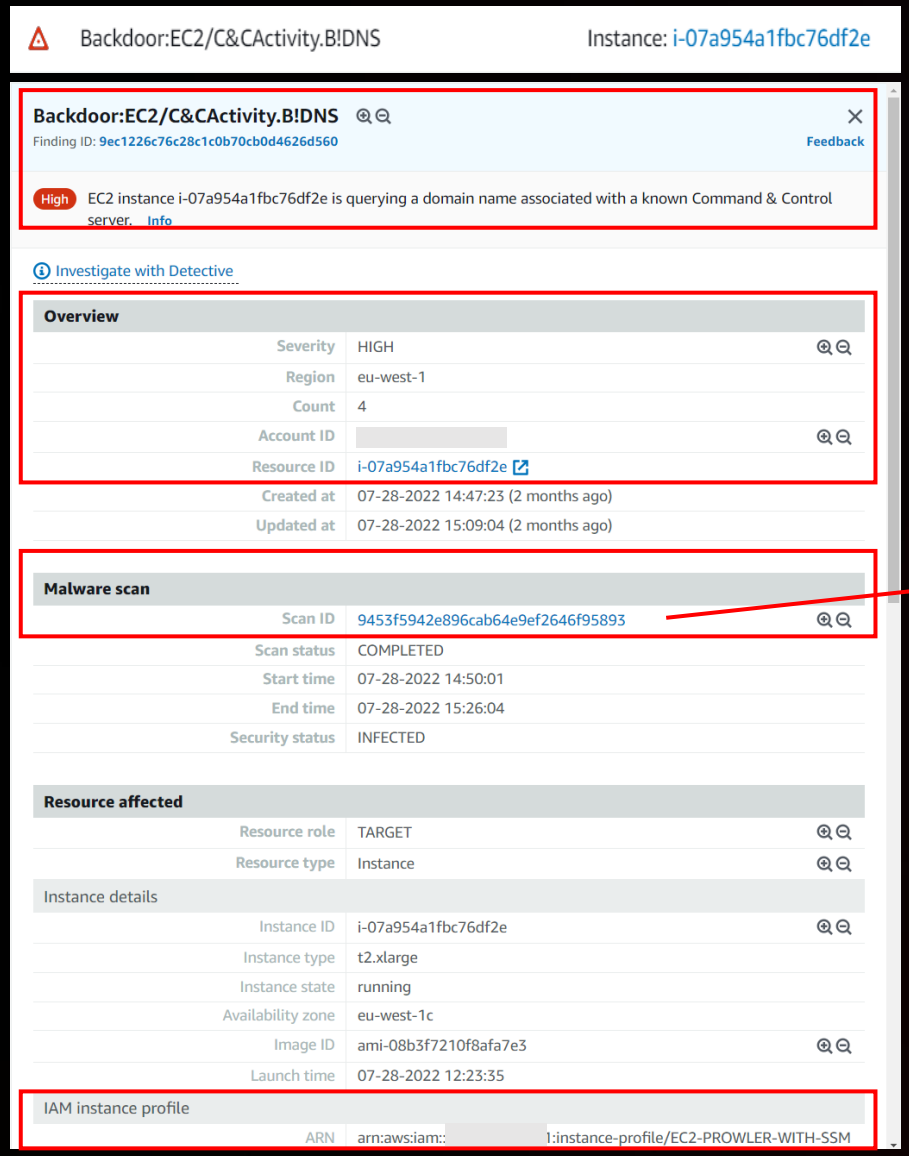
Saved rules: Apply saved rules

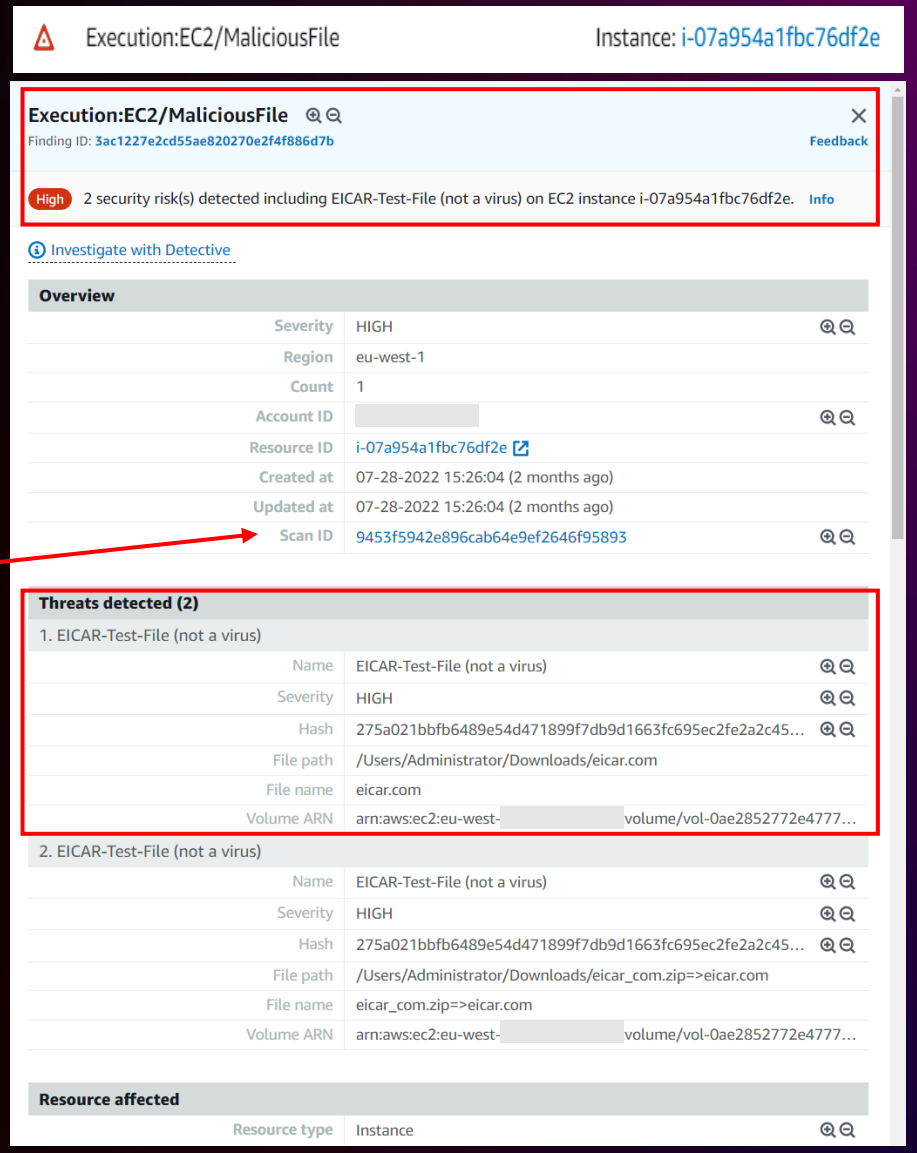
Current | Add filter criteria

Finding type	Resource	Last seen	Account ID	Count
Recon:IAMUser/MaliciousIPCaller.Custom	AmazonSSMRoleForInstancesQuickSetup:	22 minutes ago		4
Recon:IAMUser/MaliciousIPCaller.Custom	AmazonSSMRoleForInstancesQuickSetup:	an hour ago		5
Recon:IAMUser/MaliciousIPCaller.Custom	AmazonSSMRoleForInstancesQuickSetup:	2 hours ago		6
Recon:IAMUser/MaliciousIPCaller.Custom	AmazonSSMRoleForInstancesQuickSetup:	3 hours ago		8
Policy:S3/AccountBlockPublicAccessDisabled	AWSReservedSSO_AdministratorAccess_5	3 hours ago		1
Trojan:EC2/DNSDataExfiltration	Instance: i-08d0c7a9c27319c16	3 hours ago		6
Backdoor:EC2/C&CActivity.B!DNS	Instance: i-08d0c7a9c27319c16	3 hours ago		2
Recon:IAMUser/MaliciousIPCaller.Custom	AmazonSSMRoleForInstancesQuickSetup:	4 hours ago		2
Recon:IAMUser/MaliciousIPCaller.Custom	AmazonSSMRoleForInstancesQuickSetup:	4 hours ago		11
UnauthorizedAccess:EC2/MaliciousIPCaller.Custom	Instance: i-08d0c7a9c27319c16	5 hours ago		1
Execution:EC2/MaliciousFile	Instance: i-07a954a1fbc76df2e	2 months ago		1
Backdoor:EC2/C&CActivity.B!DNS	Instance: i-0569ee2fd39c70828	2 months ago		2
Backdoor:EC2/C&CActivity.B!DNS	Instance: i-07a954a1fbc76df2e	2 months ago		4

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

GuardDuty findings details

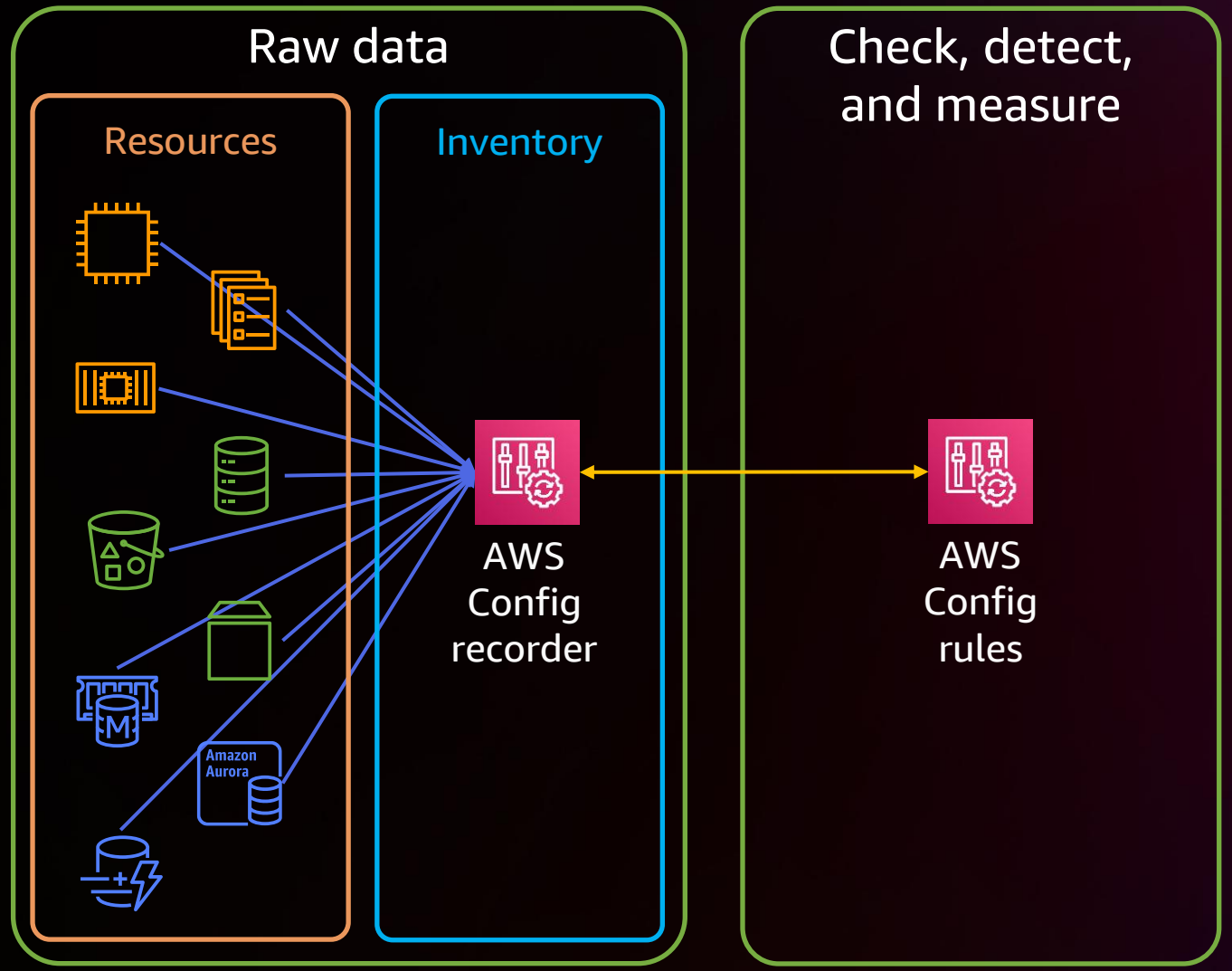




© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

How AWS Config works

Rules are mostly triggered based on changes



Config rules:

Managed rules to show if resources comply with common best practices

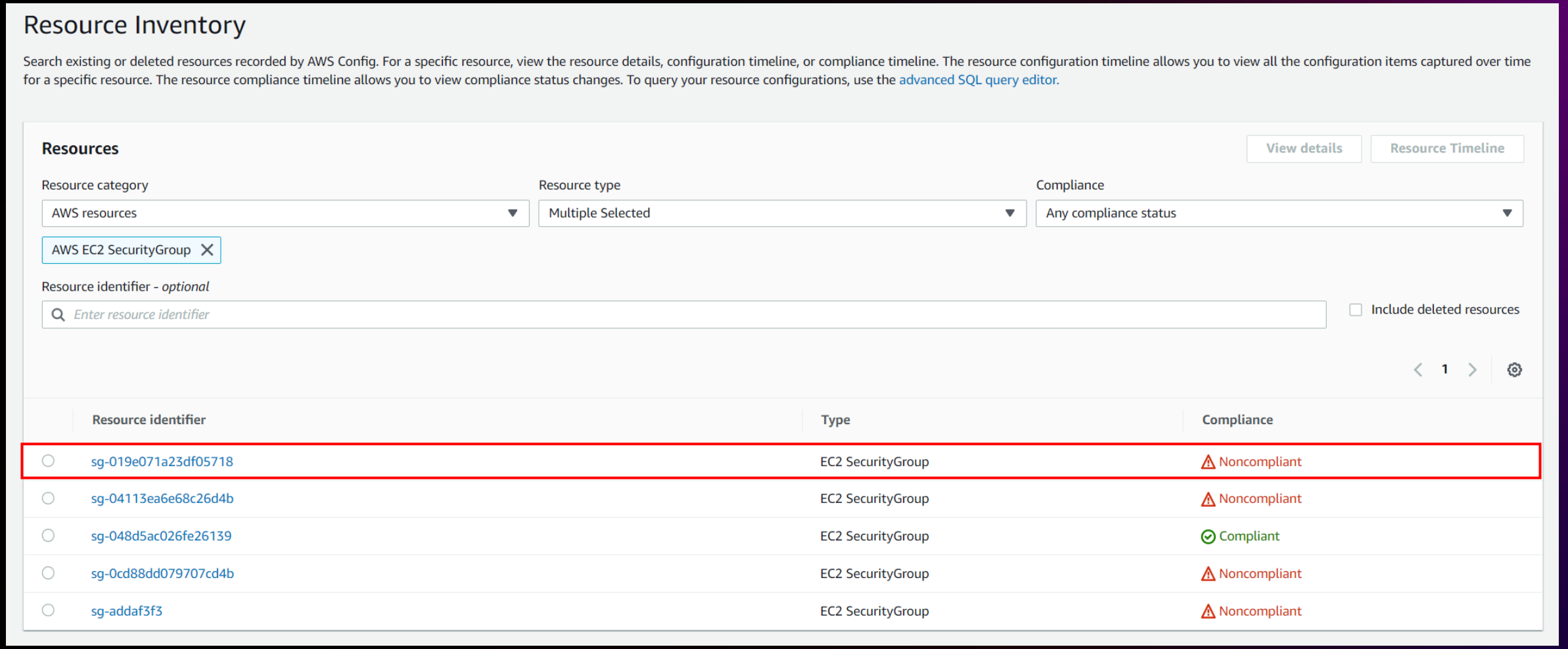
Build custom rules while using guard custom policy or AWS Lambda functions

Conformance packs (CP):

Sample CPs, based on industry recommendations, or custom CPs can be used to group rules into a general-purpose compliance framework

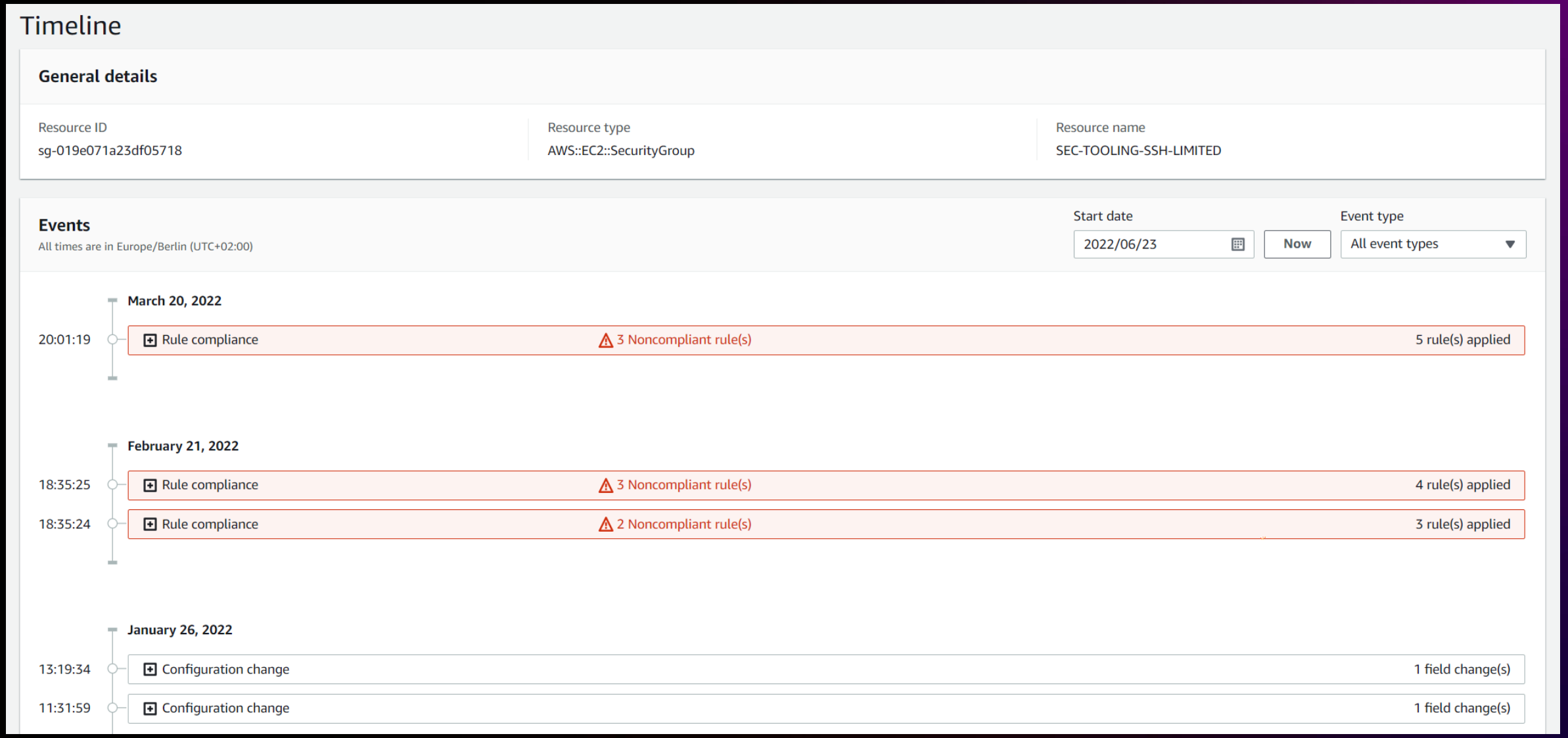
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

AWS Config resources



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

AWS Config resources timeline



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

AWS Config rules

Rules

Rules represent your desired configuration settings. AWS Config evaluates whether your resource configurations comply with relevant rules and summarizes the compliance results.

Rules

View details | Edit rule | Actions | Add rule

Any status

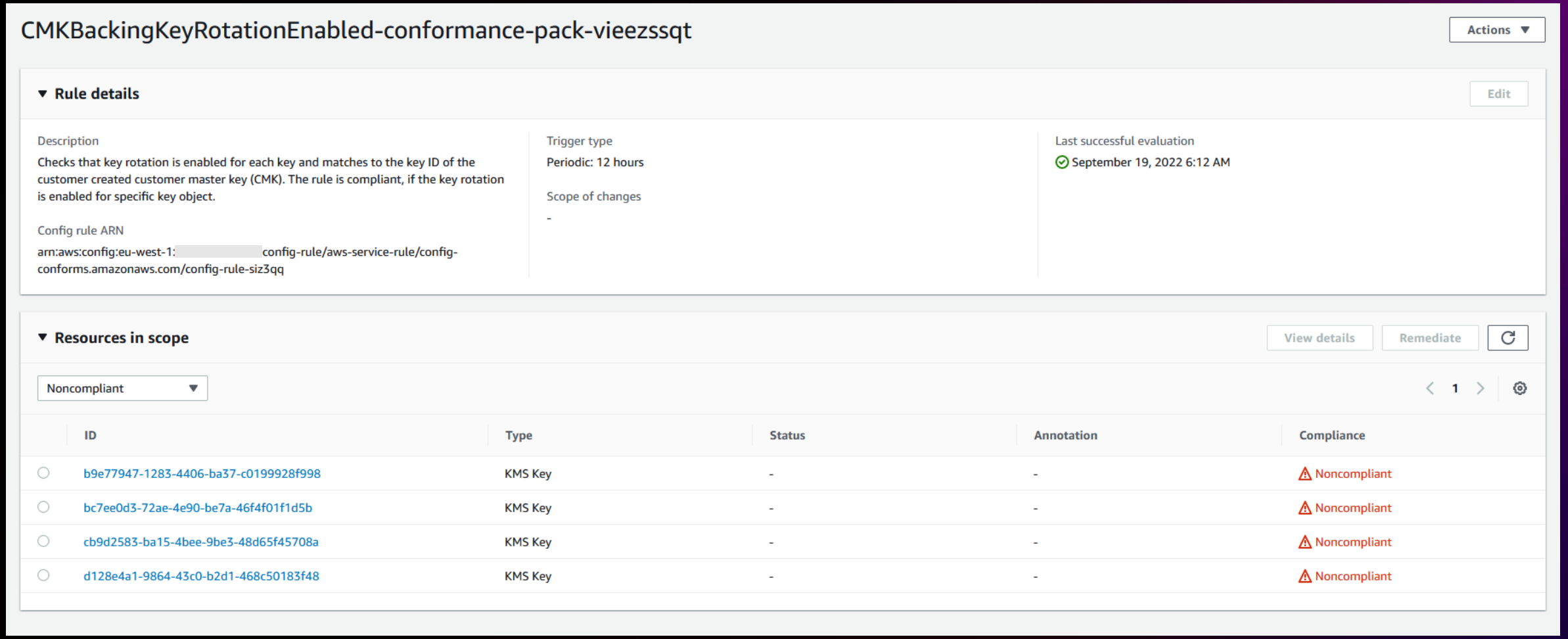
1 2 3 ...

Name	Remediation action	Type	Compliance
EmrMasterNoPublicIp-conformance-pack-uqghya0wp	Not set	AWS managed	-
EfsEncryptedCheck-conformance-pack-uqghya0wp	Not set	AWS managed	-
CloudTrailLogFileValidationEnabled-conformance-pack-vieezssqt	Not set	AWS managed	Compliant
CMKBackingKeyRotationEnabled-conformance-pack-vieezssqt	Not set	AWS managed	4 Noncompliant resource(s)
Ec2SecurityGroupAttachedToEni-conformance-pack-uqghya0wp	Not set	AWS managed	11 Noncompliant resource(s)
CloudwatchLogGroupEncrypted-conformance-pack-uqghya0wp	Not set	AWS managed	24 Noncompliant resource(s)
Ec2ManagedinstanceAssociationComplian-conformance-pack-uqghya0wp	Not set	AWS managed	Compliant
AcmCertificateExpirationCheck-conformance-pack-uqghya0wp	Not set	AWS managed	2 Noncompliant resource(s)
IAMPasswordPolicyCheck-conformance-pack-vieezssqt	Not set	AWS managed	1 Noncompliant resource(s)
CloudTrailCloudWatchLogsEnabled-conformance-pack-vieezssqt	Not set	AWS managed	1 Noncompliant resource(s)

aws

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

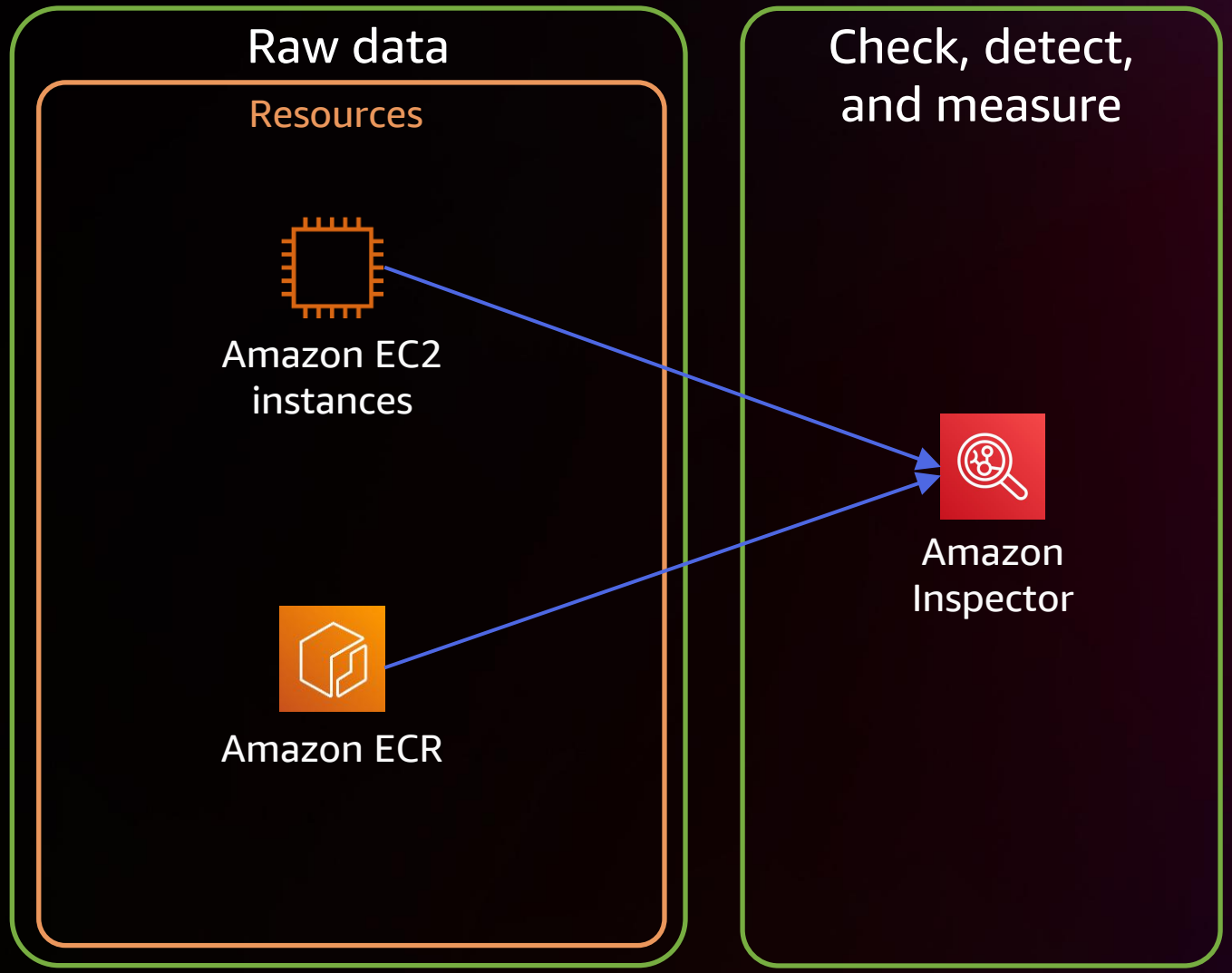
AWS Config rules details



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

How Amazon Inspector works

Continuous scans based on software changes and new or updated vulnerability intelligence



Vulnerability assessment:

Automatically discover vulnerabilities in near real time

Identify zero-day vulnerabilities quickly by using more than 50 intelligence sources

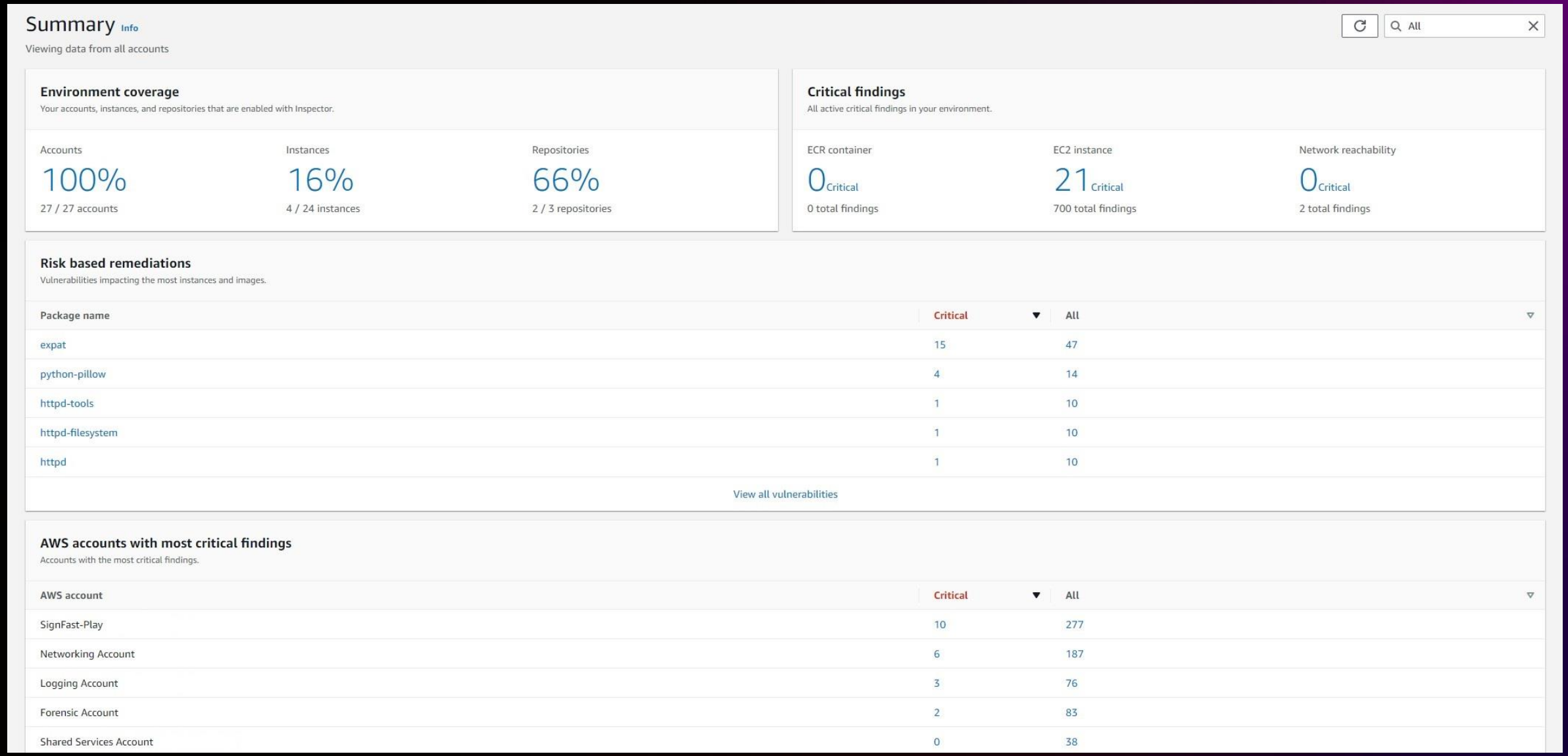
Network accessibility analysis:

Prioritize findings using context-based risk scores

aws

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

Amazon Inspector summary



Summary Info

Viewing data from all accounts

All

Environment coverage

Your accounts, instances, and repositories that are enabled with Inspector.

Accounts	Instances	Repositories
100%	16%	66%
27 / 27 accounts	4 / 24 instances	2 / 3 repositories

Critical findings

All active critical findings in your environment.

ECR container	EC2 instance	Network reachability
0 Critical	21 Critical	0 Critical
0 total findings	700 total findings	2 total findings

Risk based remediations

Vulnerabilities impacting the most instances and images.

Package name	Critical	All
expat	15	47
python-pillow	4	14
httpd-tools	1	10
httpd-filesystem	1	10
httpd	1	10

View all vulnerabilities

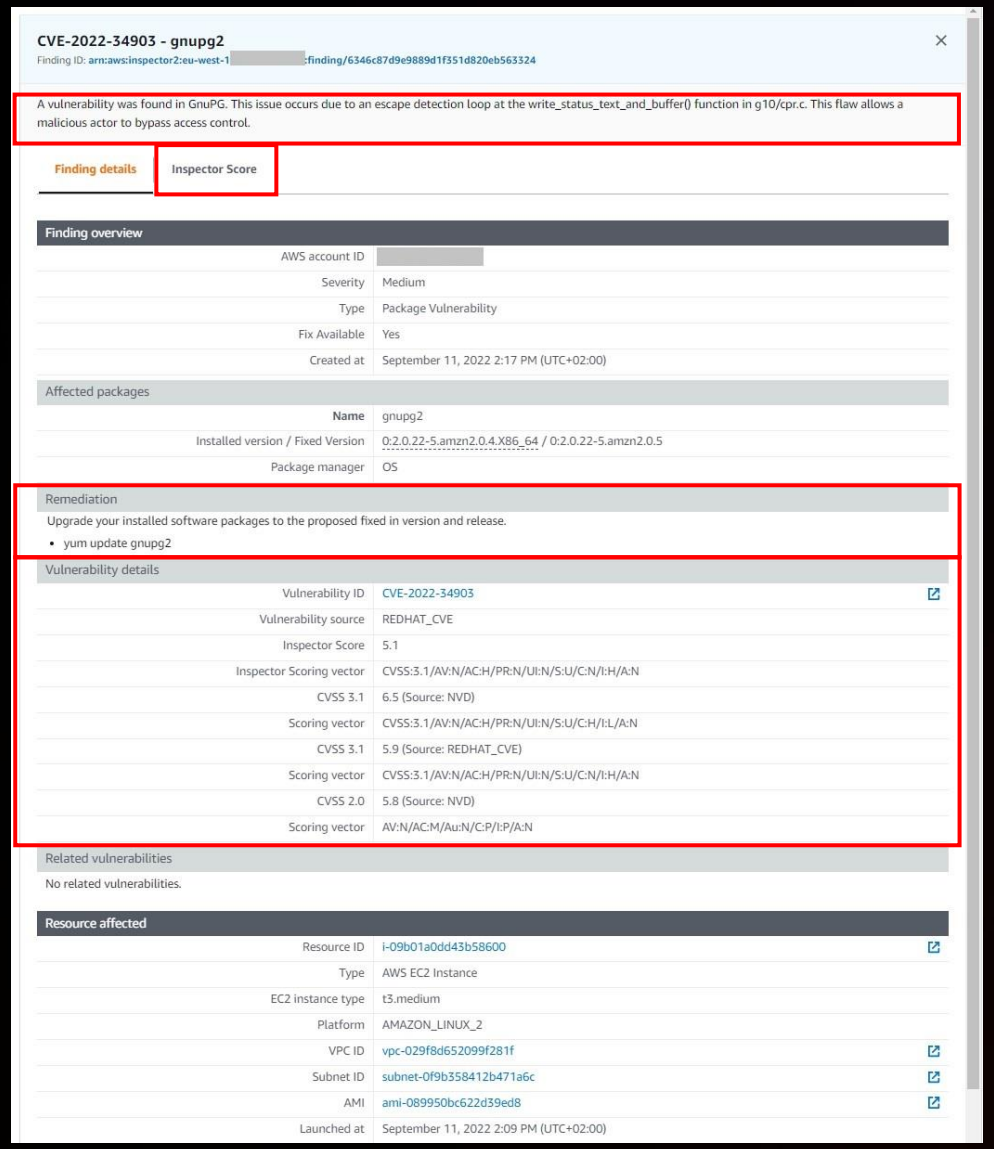
AWS accounts with most critical findings

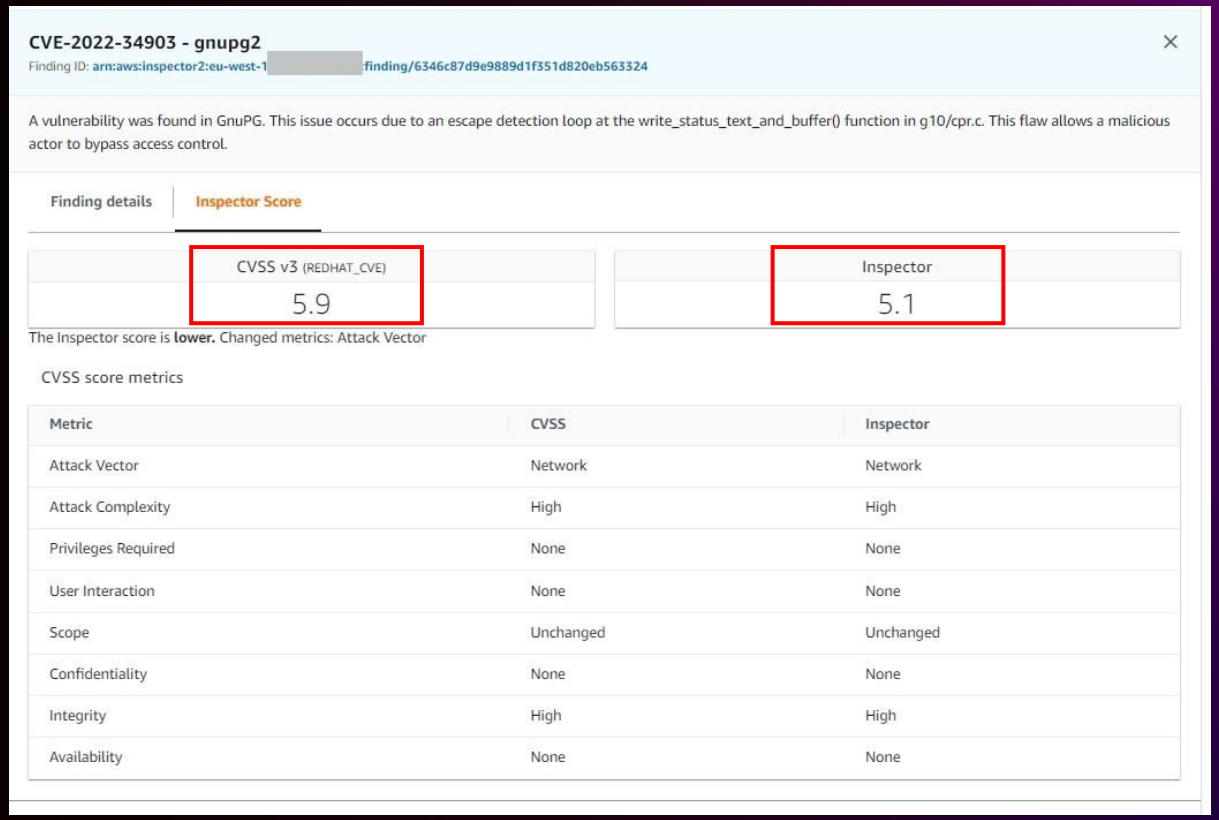
Accounts with the most critical findings.

AWS account	Critical	All
SignFast-Play	10	277
Networking Account	6	187
Logging Account	3	76
Forensic Account	2	83
Shared Services Account	0	38

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

Amazon Inspector findings



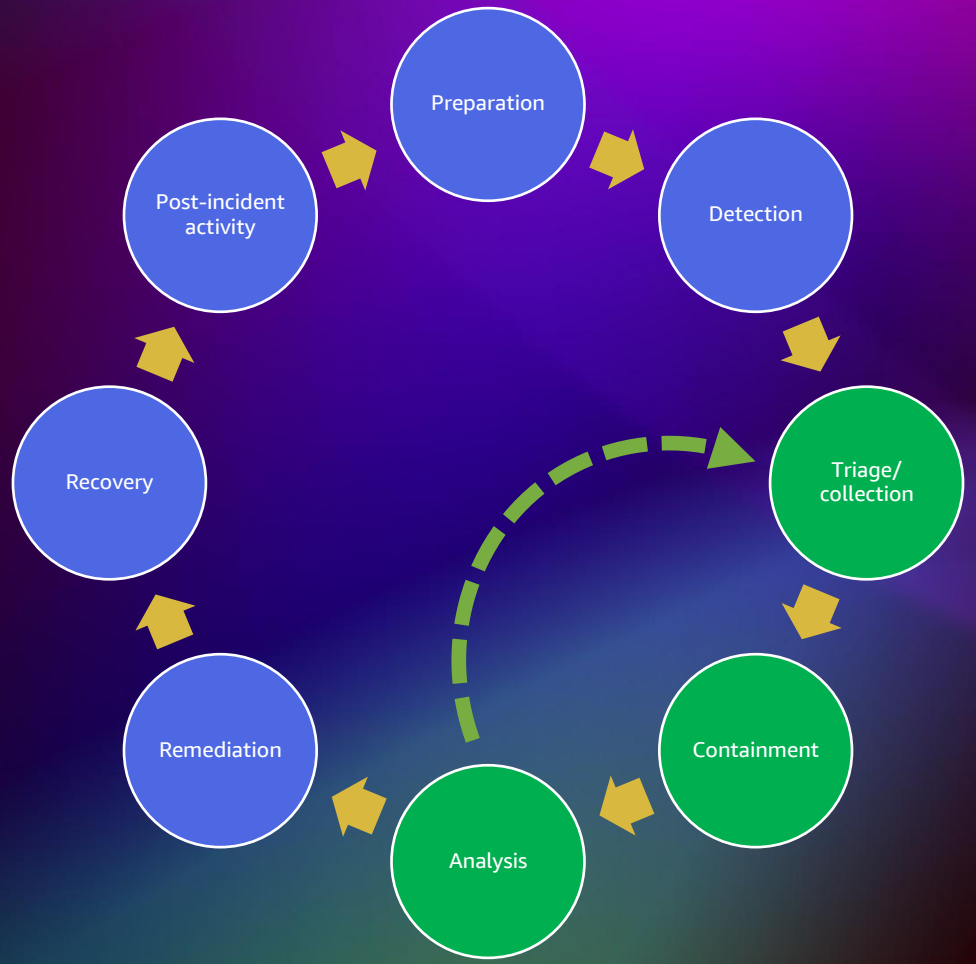


The Amazon Inspector score is lower because of a changed attack vector

Changes are based on the network reachability analysis

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

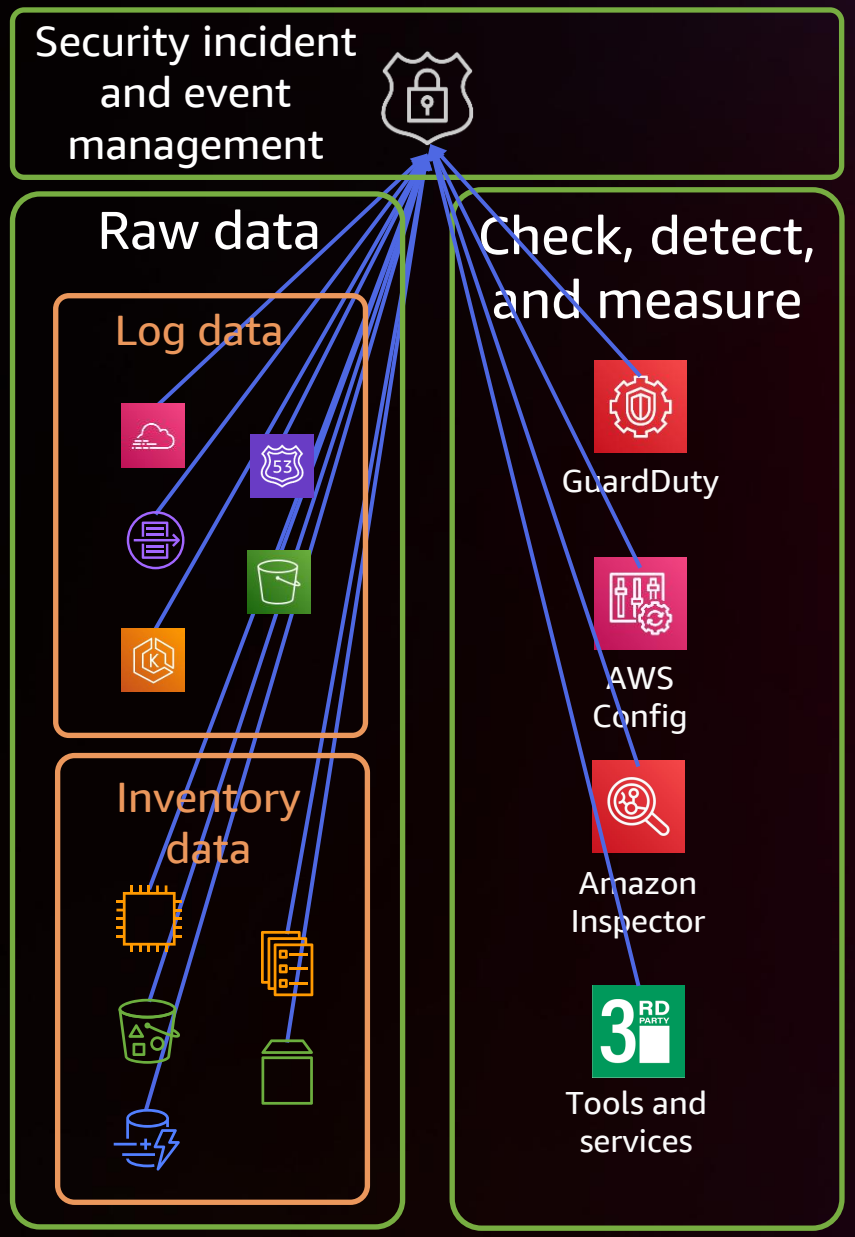
Collection
Containment
Analysis



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

Triage and collection – What do we have so far?

Data that isn't measured or weighted

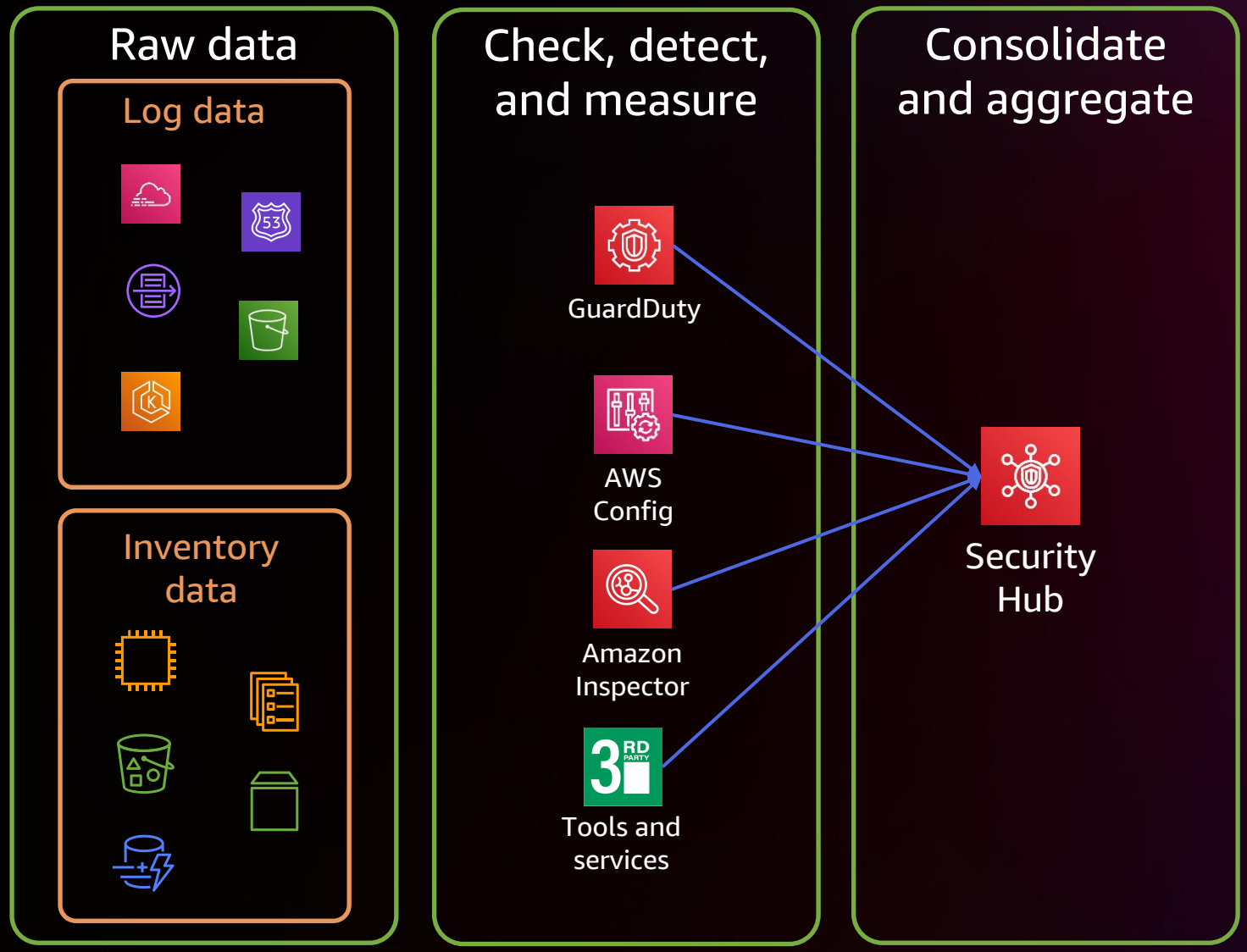


Results or findings based on rules and patterns

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

How Security Hub works

A single, standardized data format for all of your findings



Cloud security posture management:

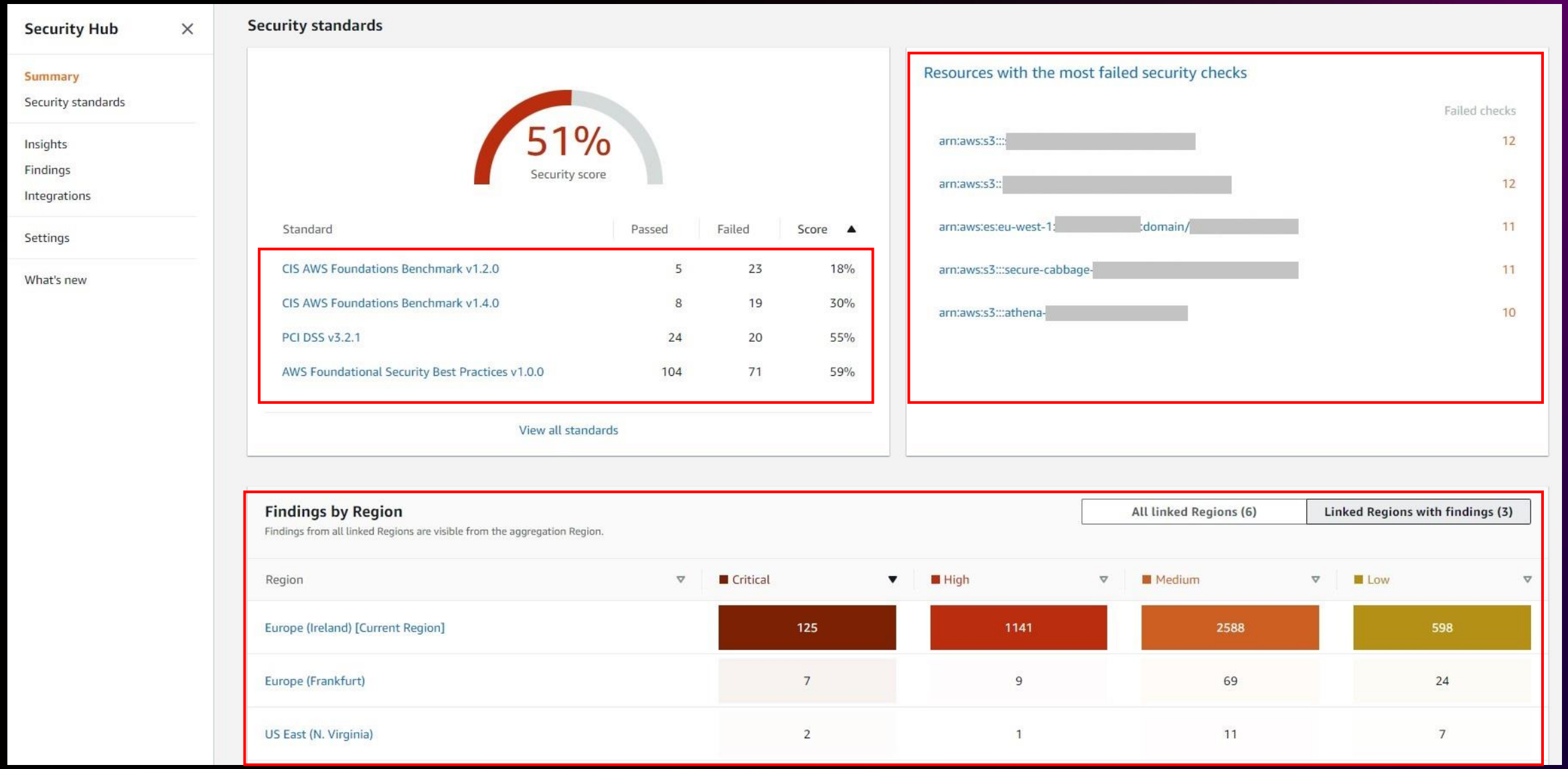
Automated, continuous security checks based on industry and vendor best practices

Consolidated findings:

Aggregates security findings generated by AWS security services and partners across accounts and Regions

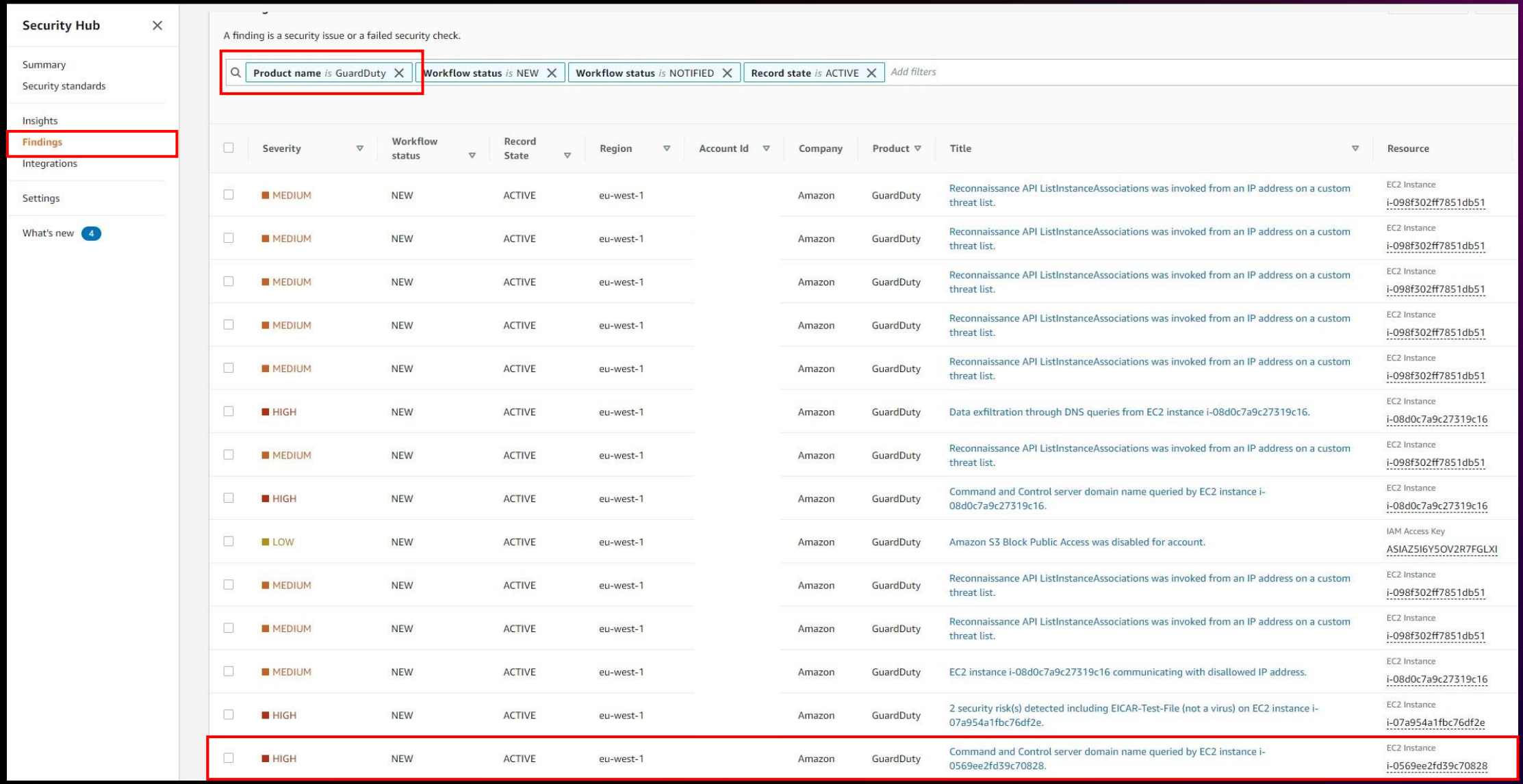
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Security Hub summary



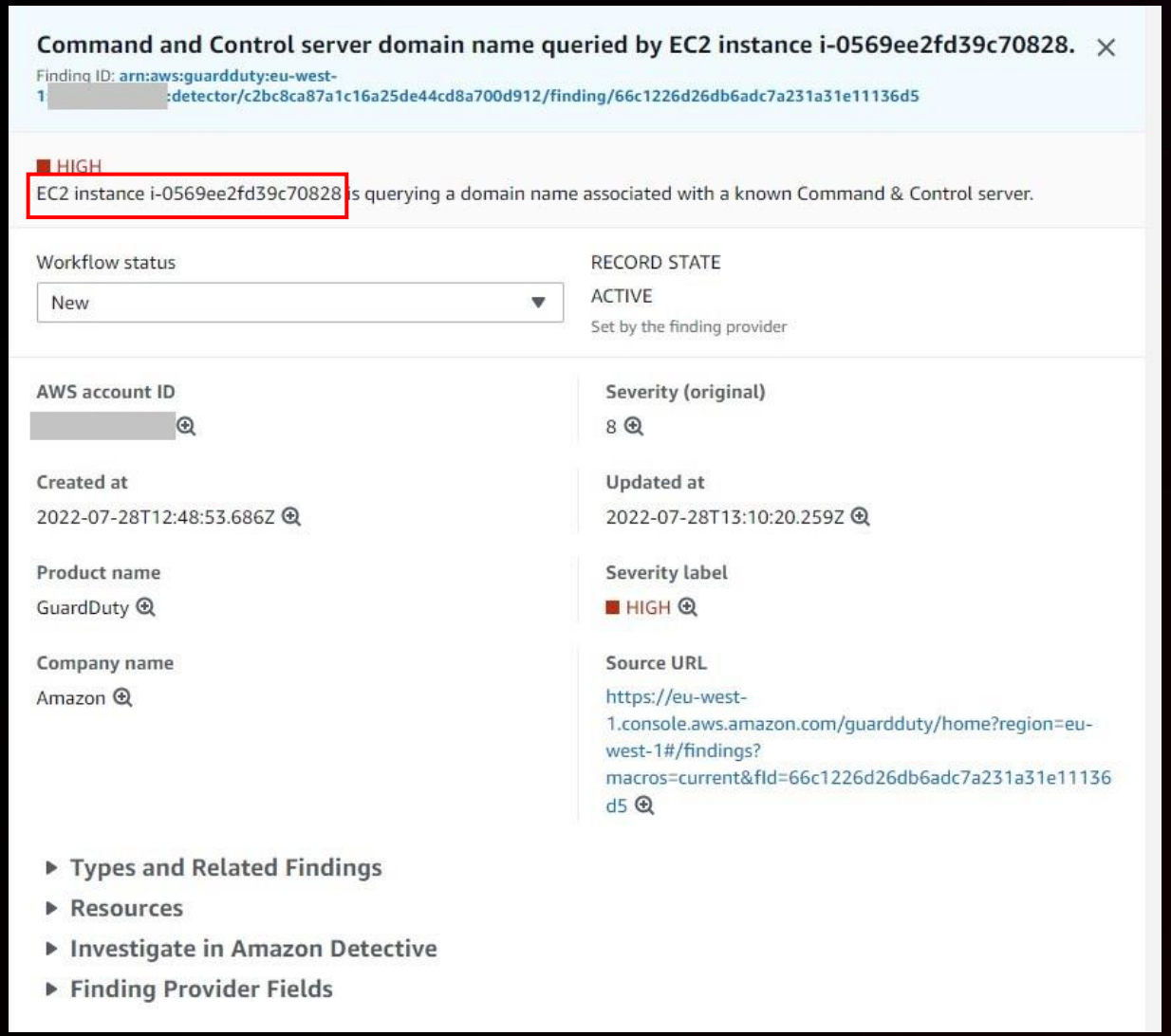
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

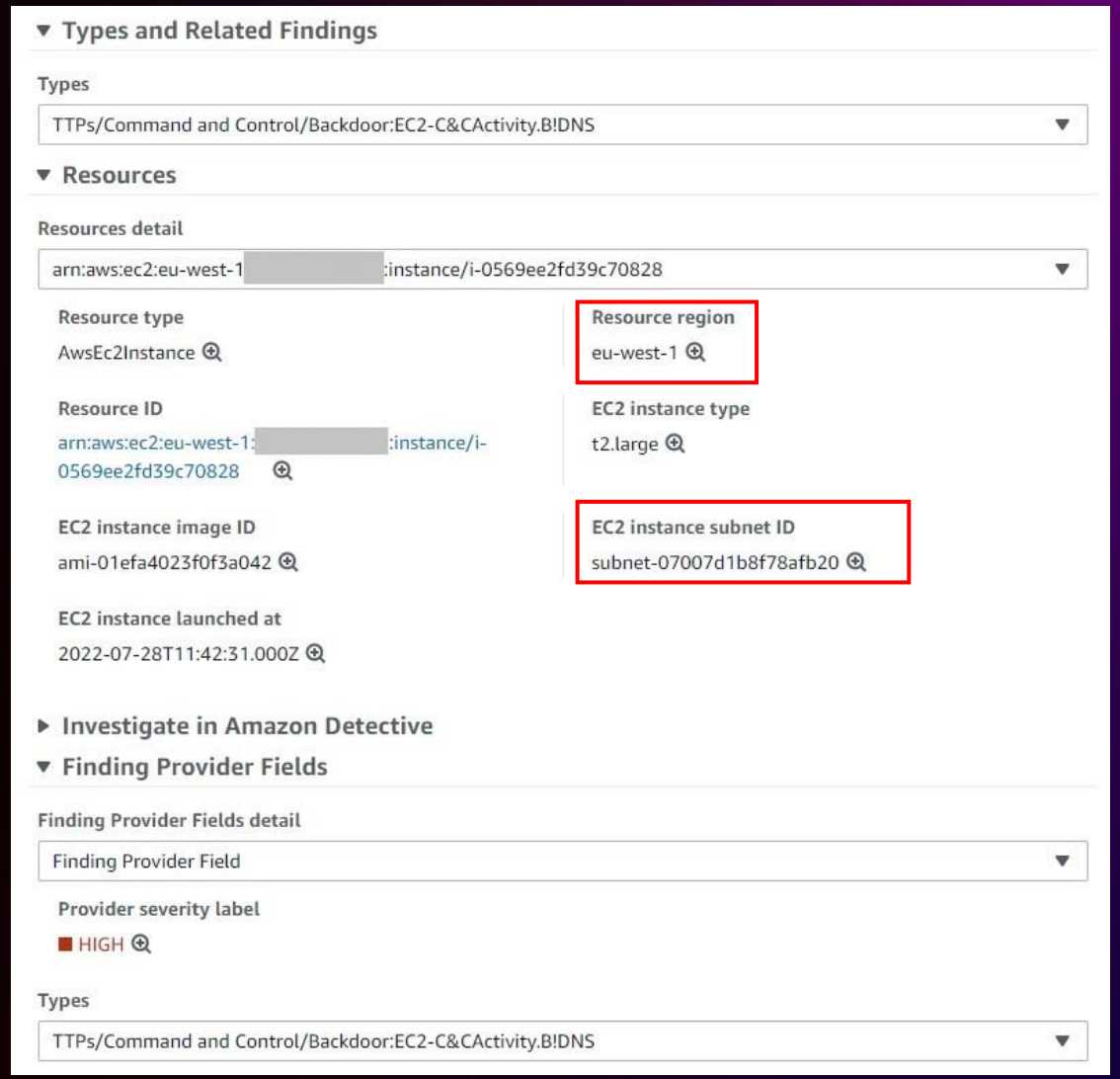
Security Hub findings



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

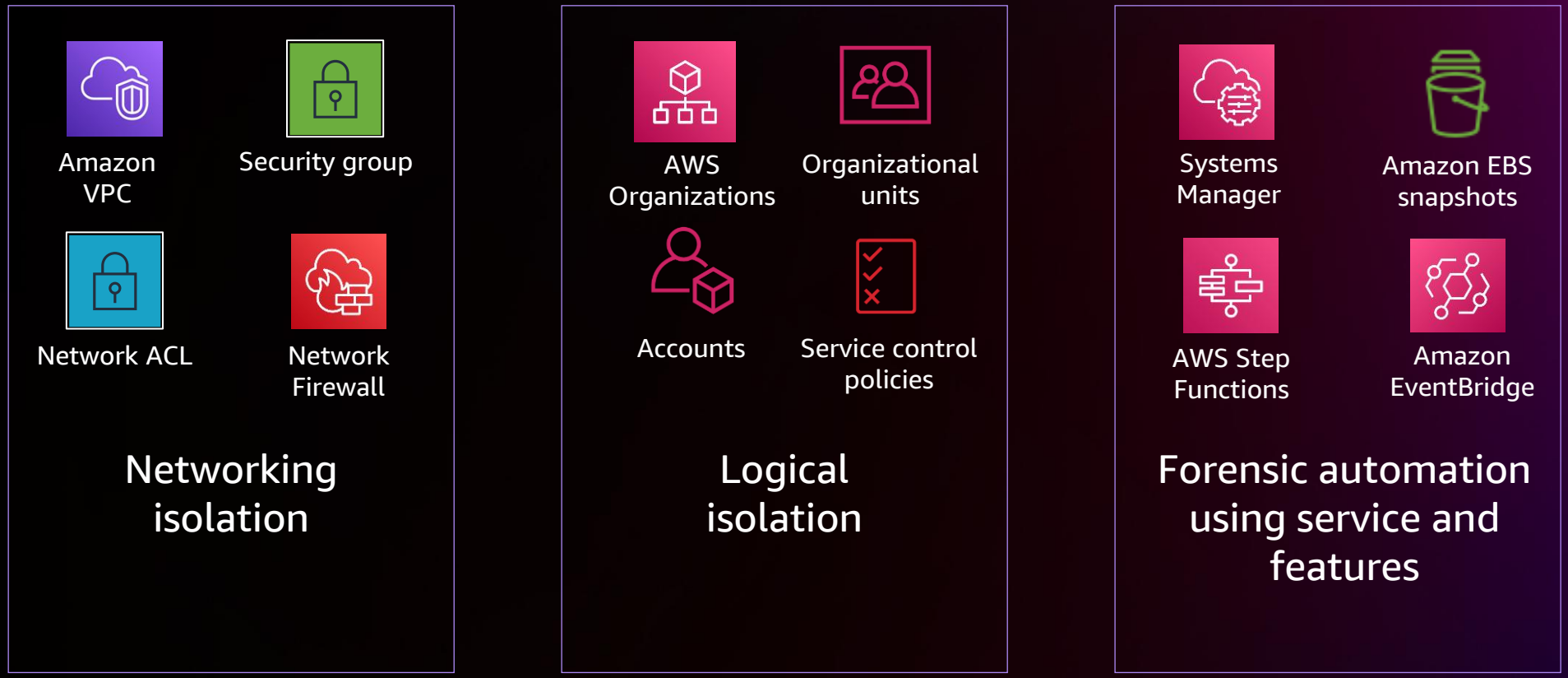
Security Hub finding details





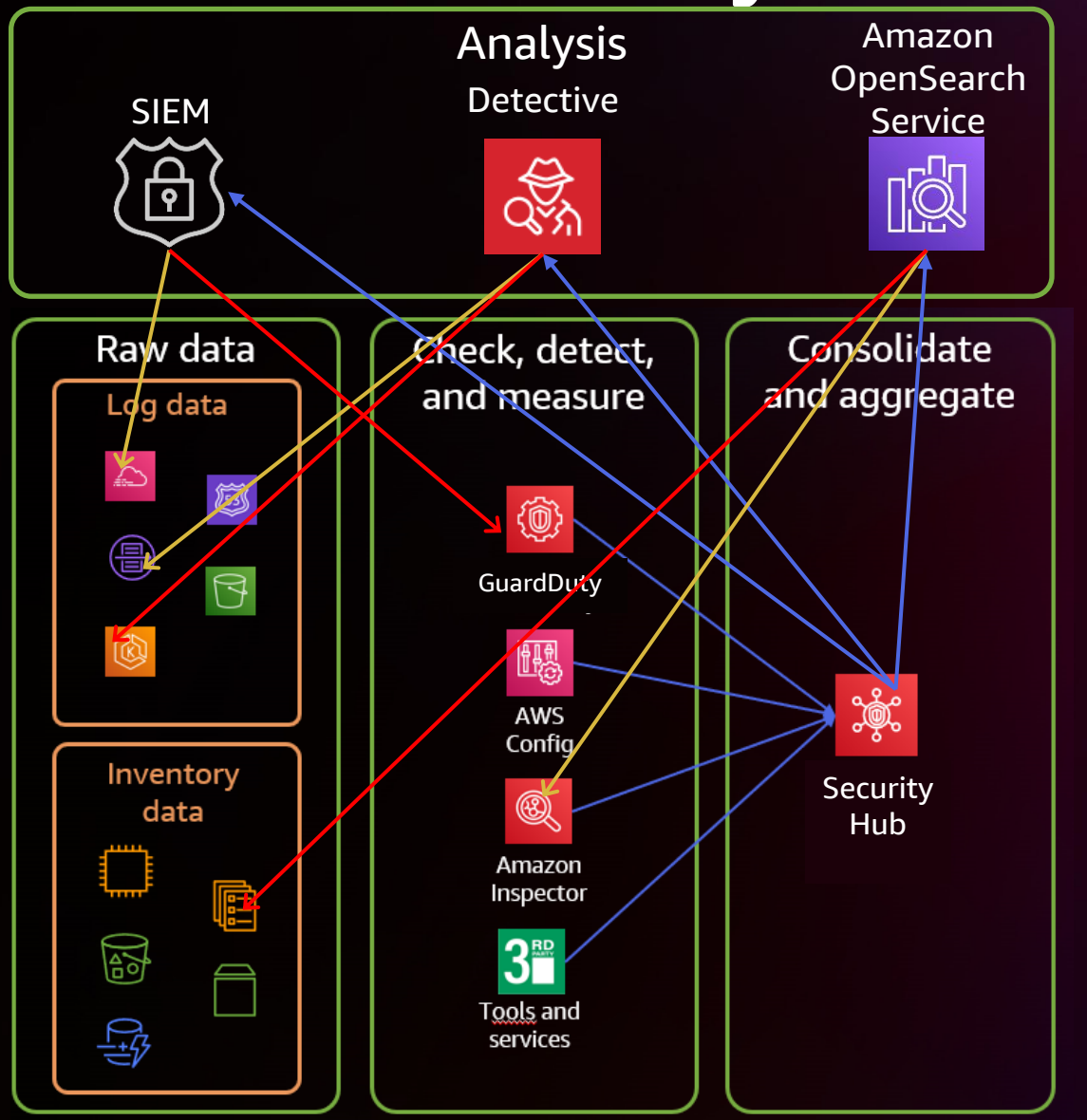
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Continuous containment in the cloud



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

If we need to do further analysis



In both cases this analysis is typically targeted to specific sources

From an existing finding:

Analyze and search through related raw and result data (findings)

Without an existing finding:

Analyze and search through all raw and result data based on your own path

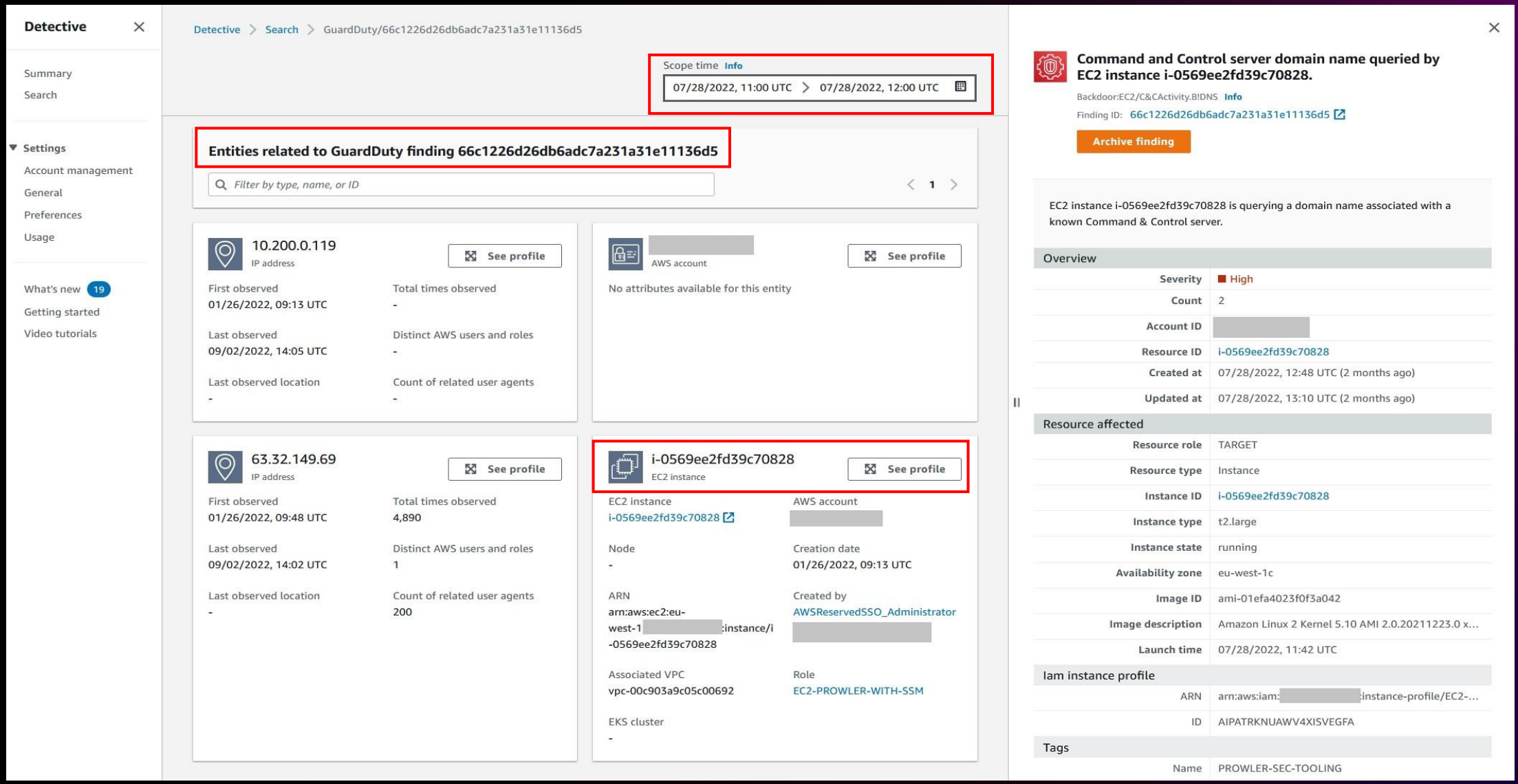
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Investigate using Detective



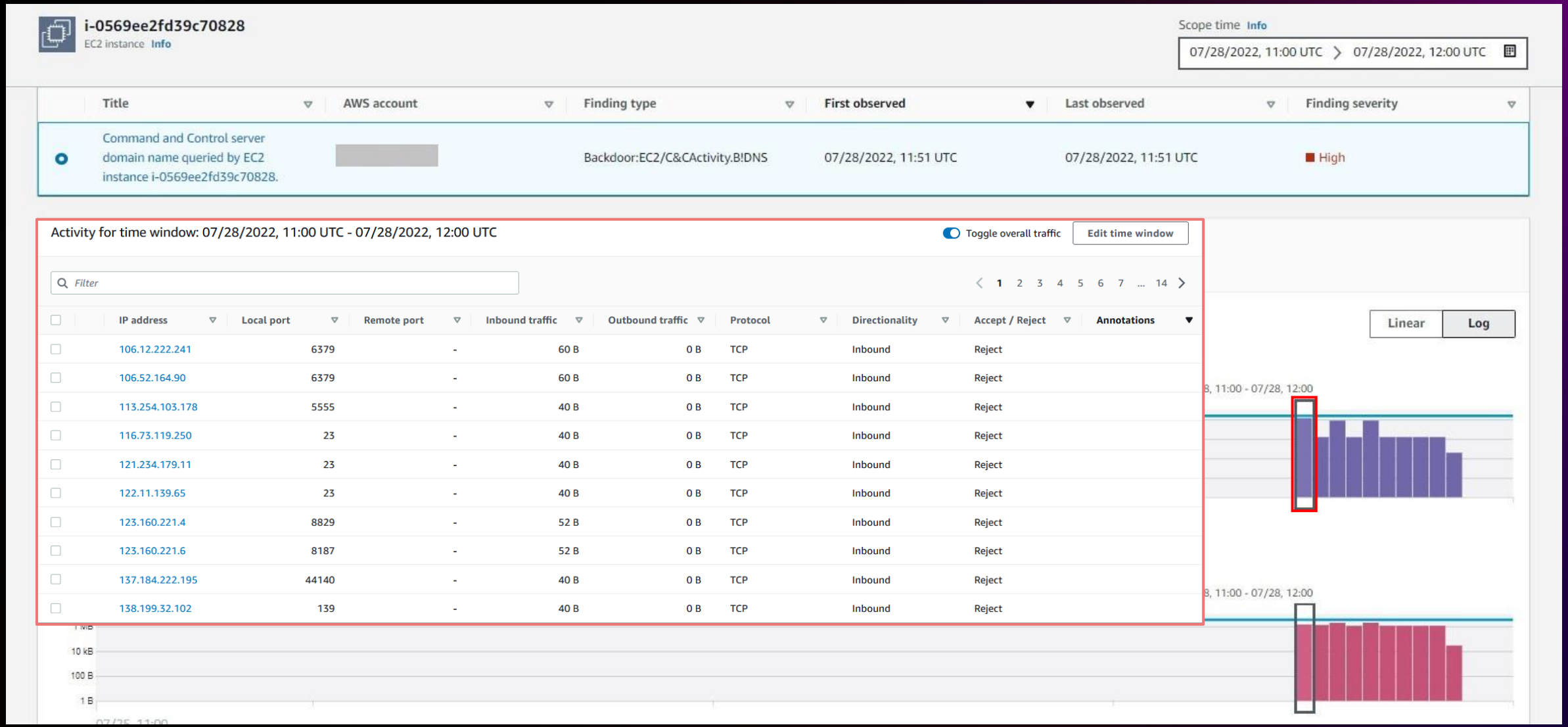
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Investigate using Detective



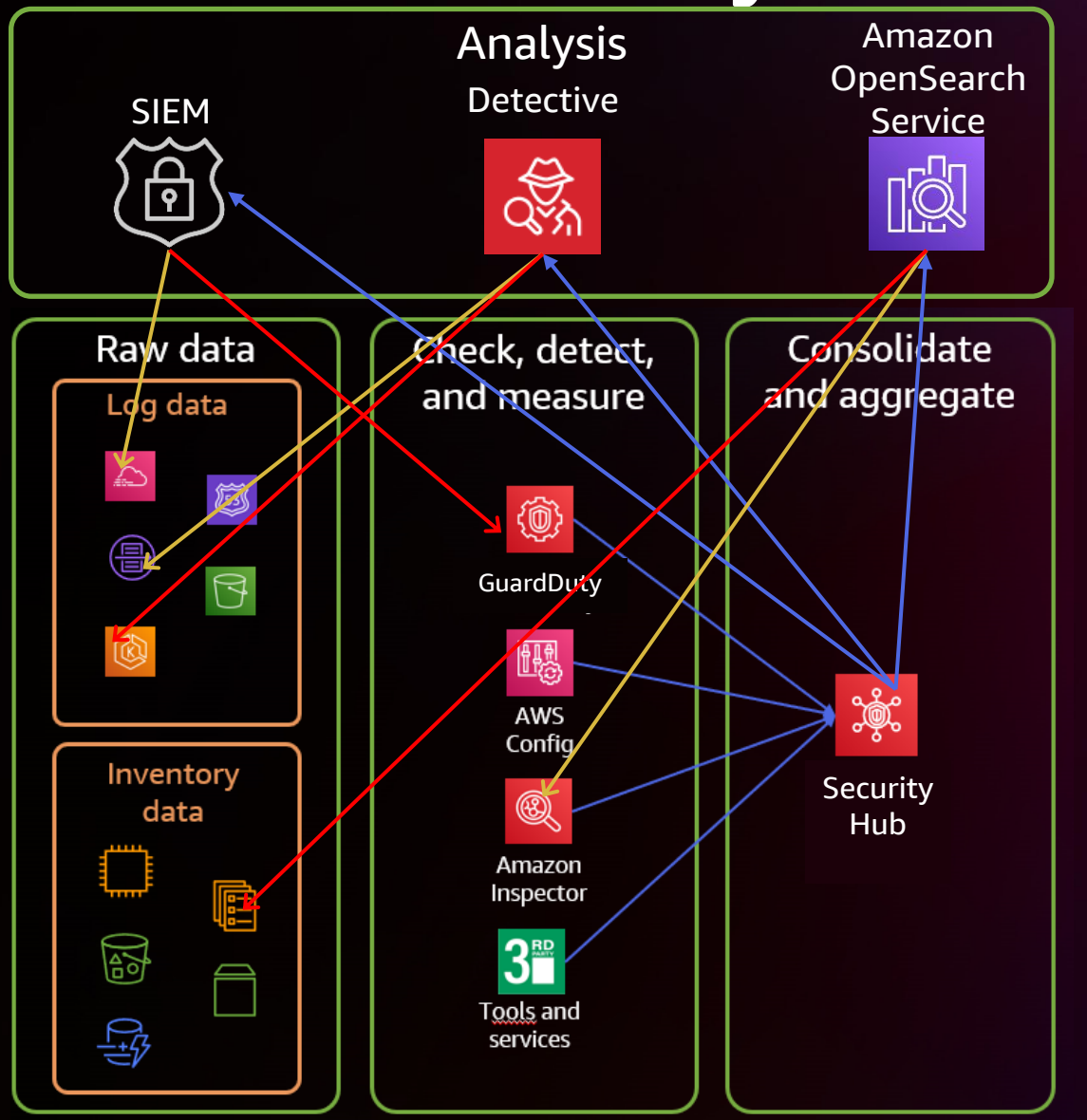
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Investigate using Detective



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

If we need to do further analysis



In both cases this analysis is typically targeted to specific sources

From an existing finding:

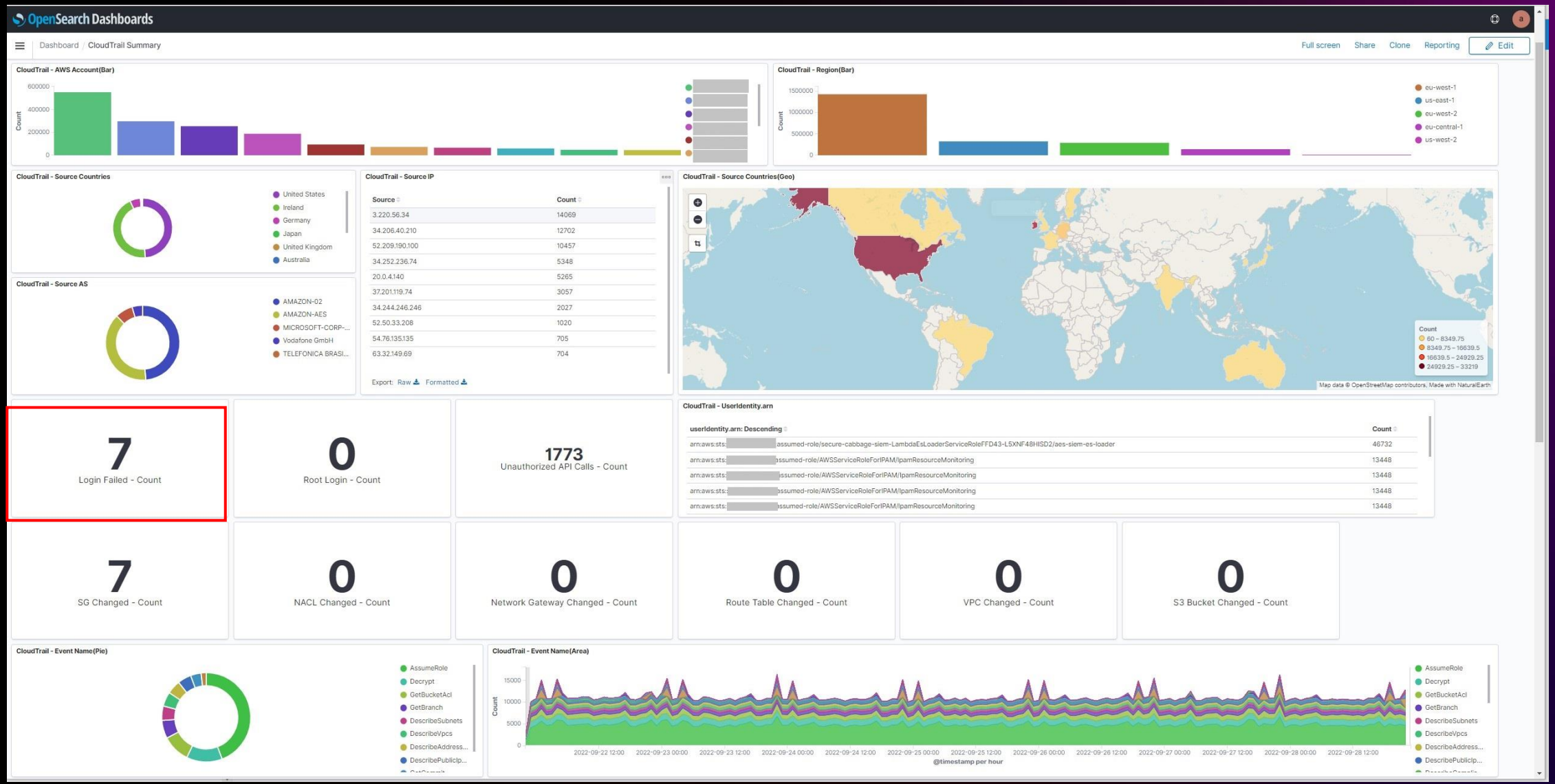
Analyze and search through related raw and result data (findings)

Without an existing finding:

Analyze and search through all raw and result data based on your own path

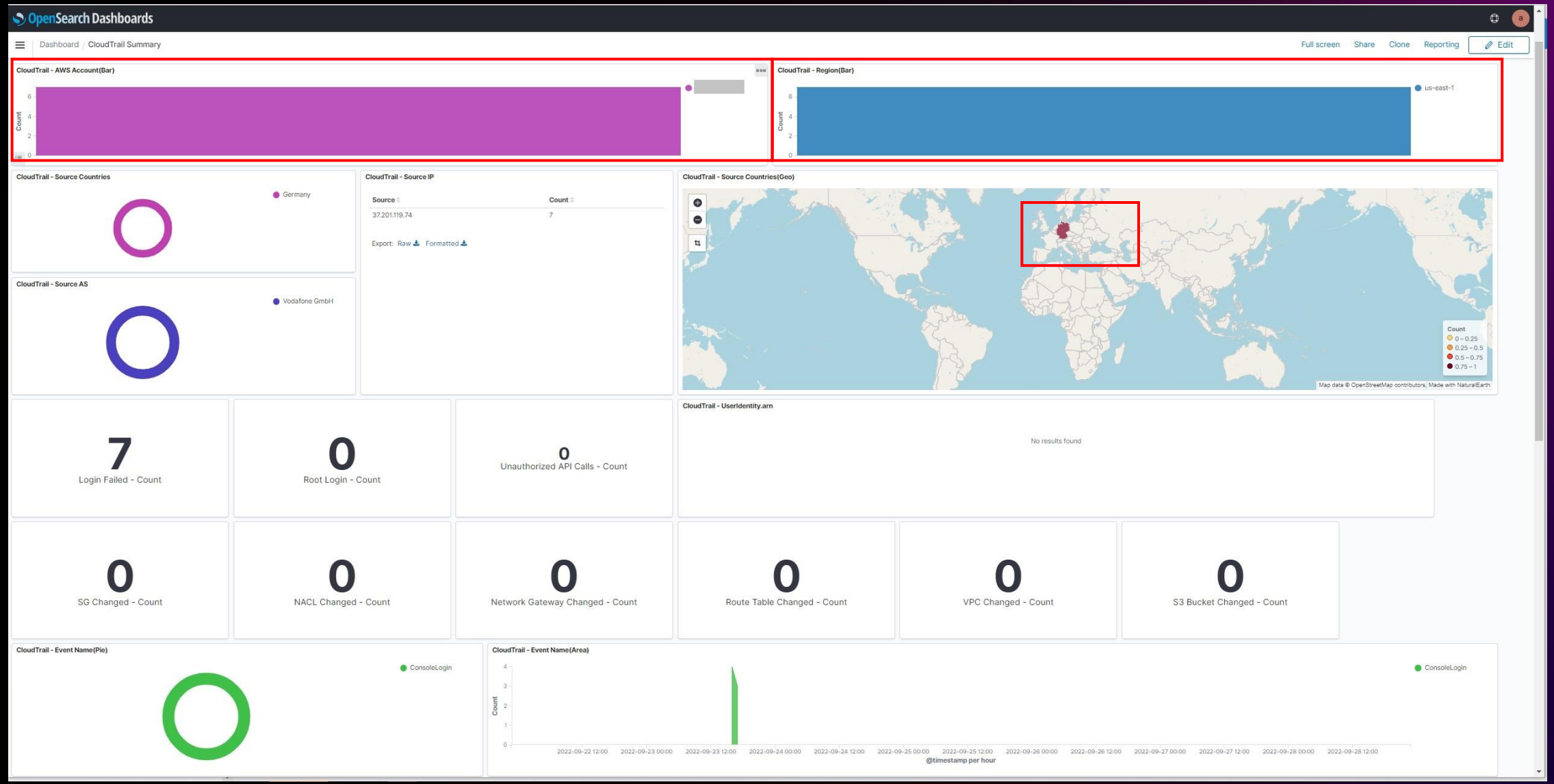
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Investigate using OpenSearch Service



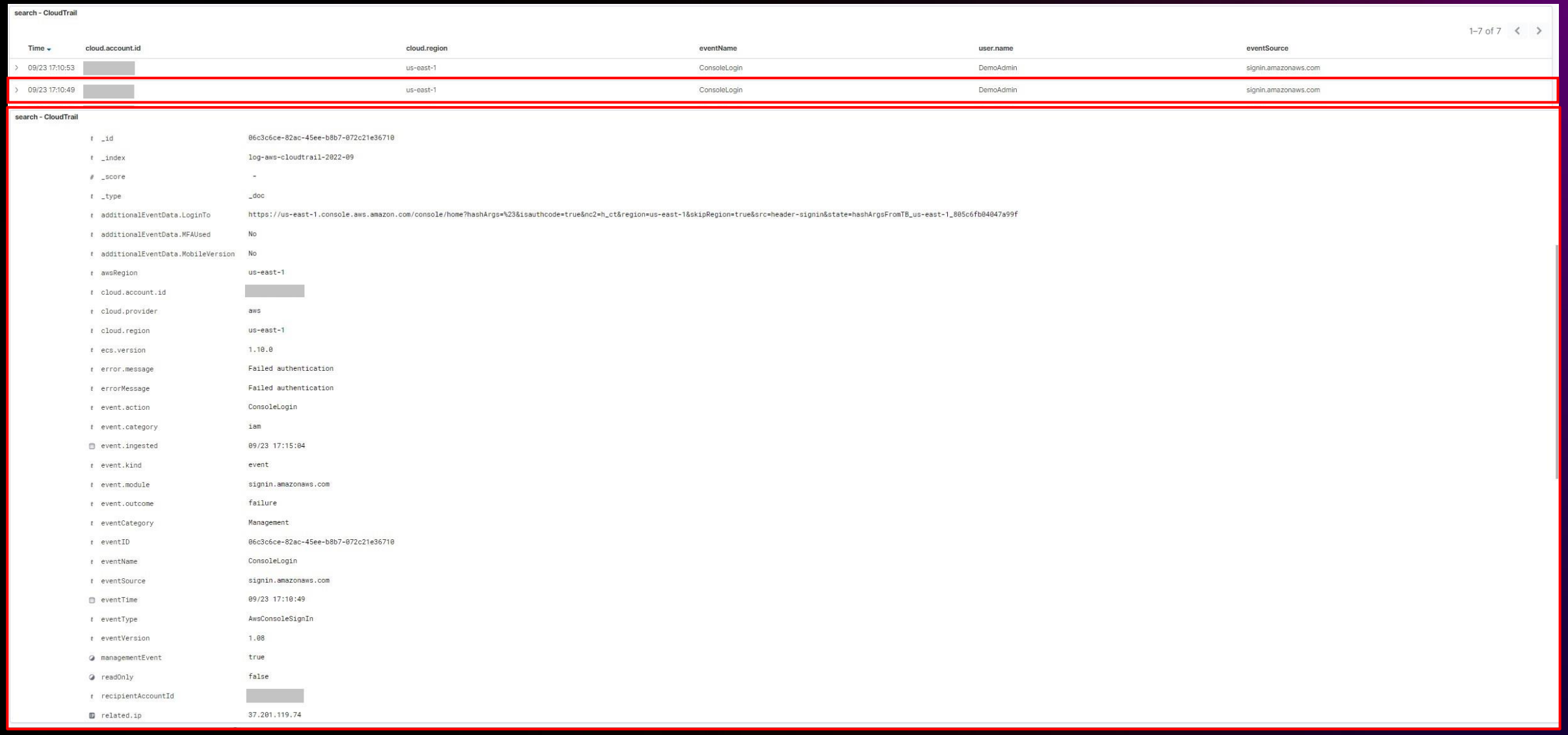
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Investigate using OpenSearch Service



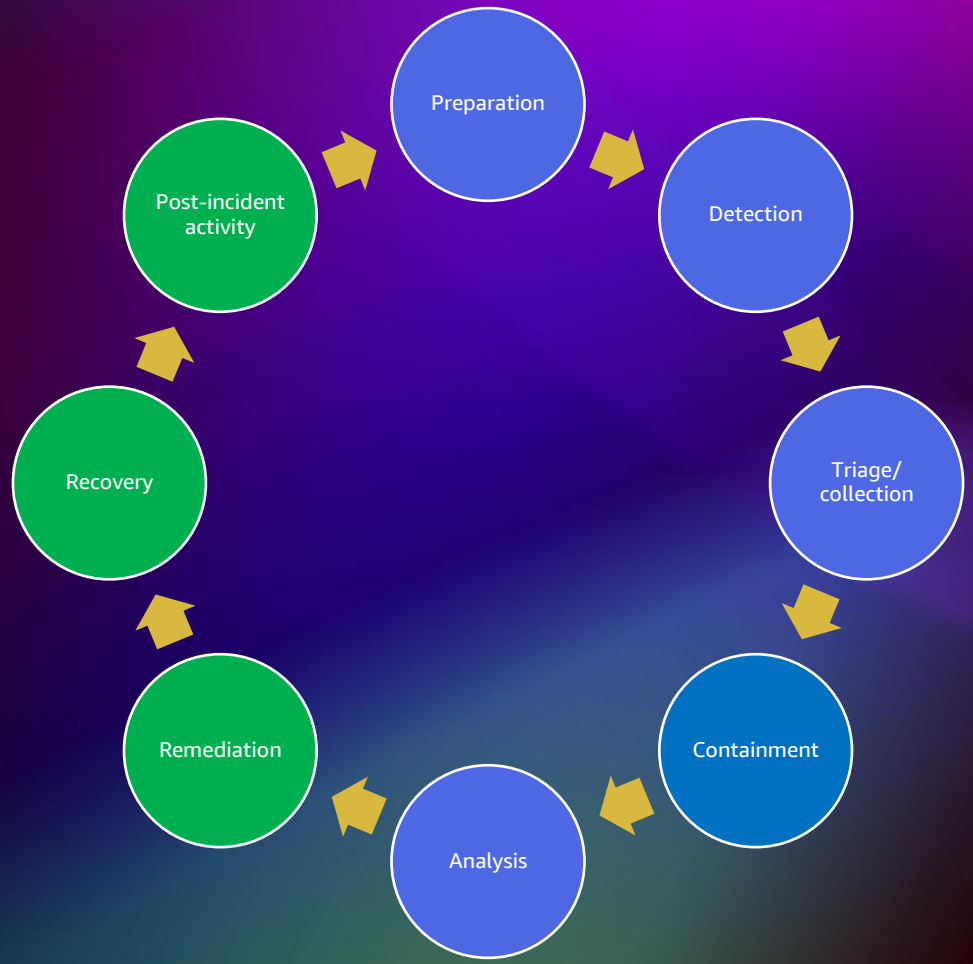
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Investigate using OpenSearch Service



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

Remediation
Recovery
Post-incident activity



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



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

Challenges



Auditors and regulators



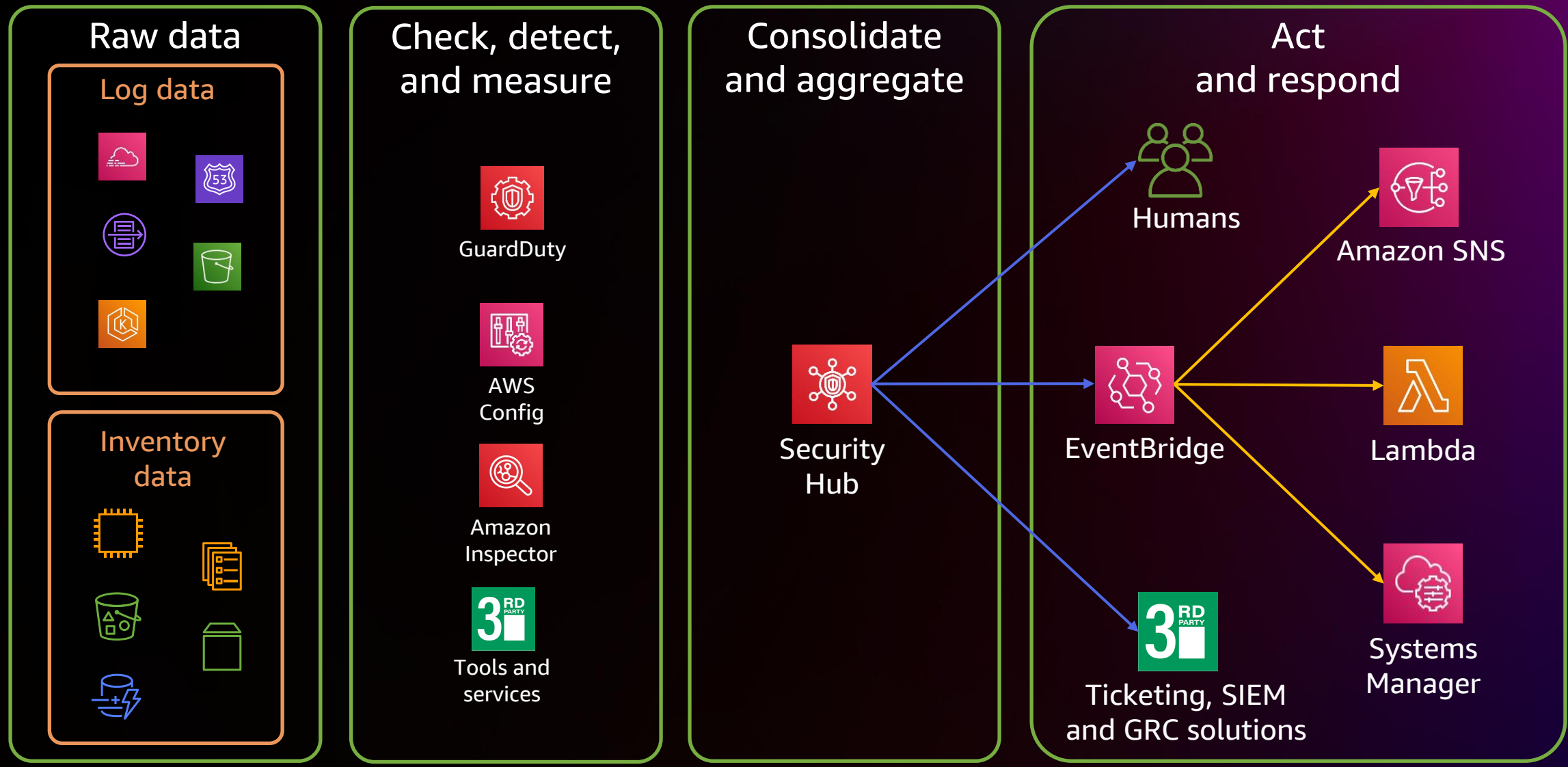
Customers



“What happened? At what time?”

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

How AWS Security Hub can trigger actions

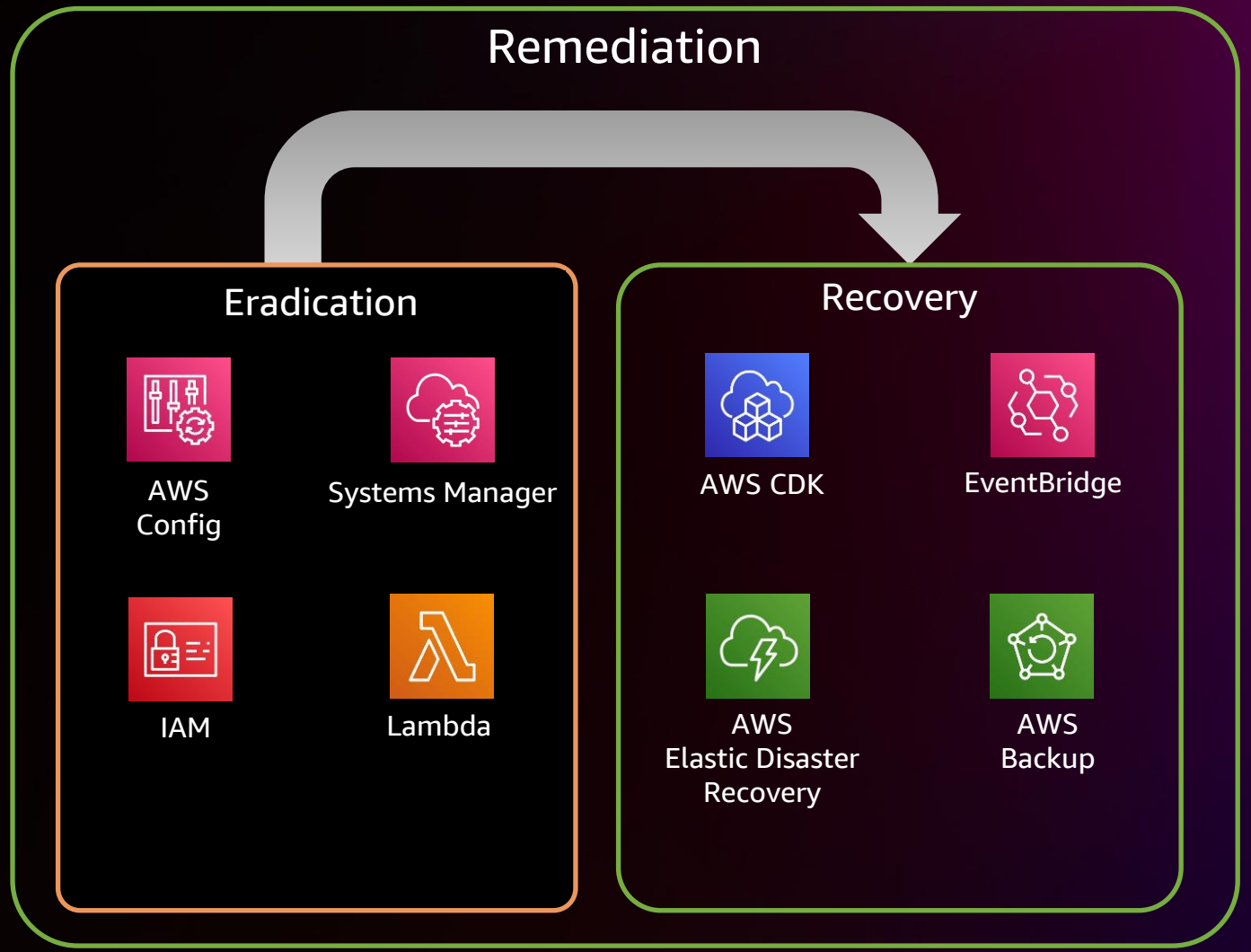


© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Remediation and Recovery

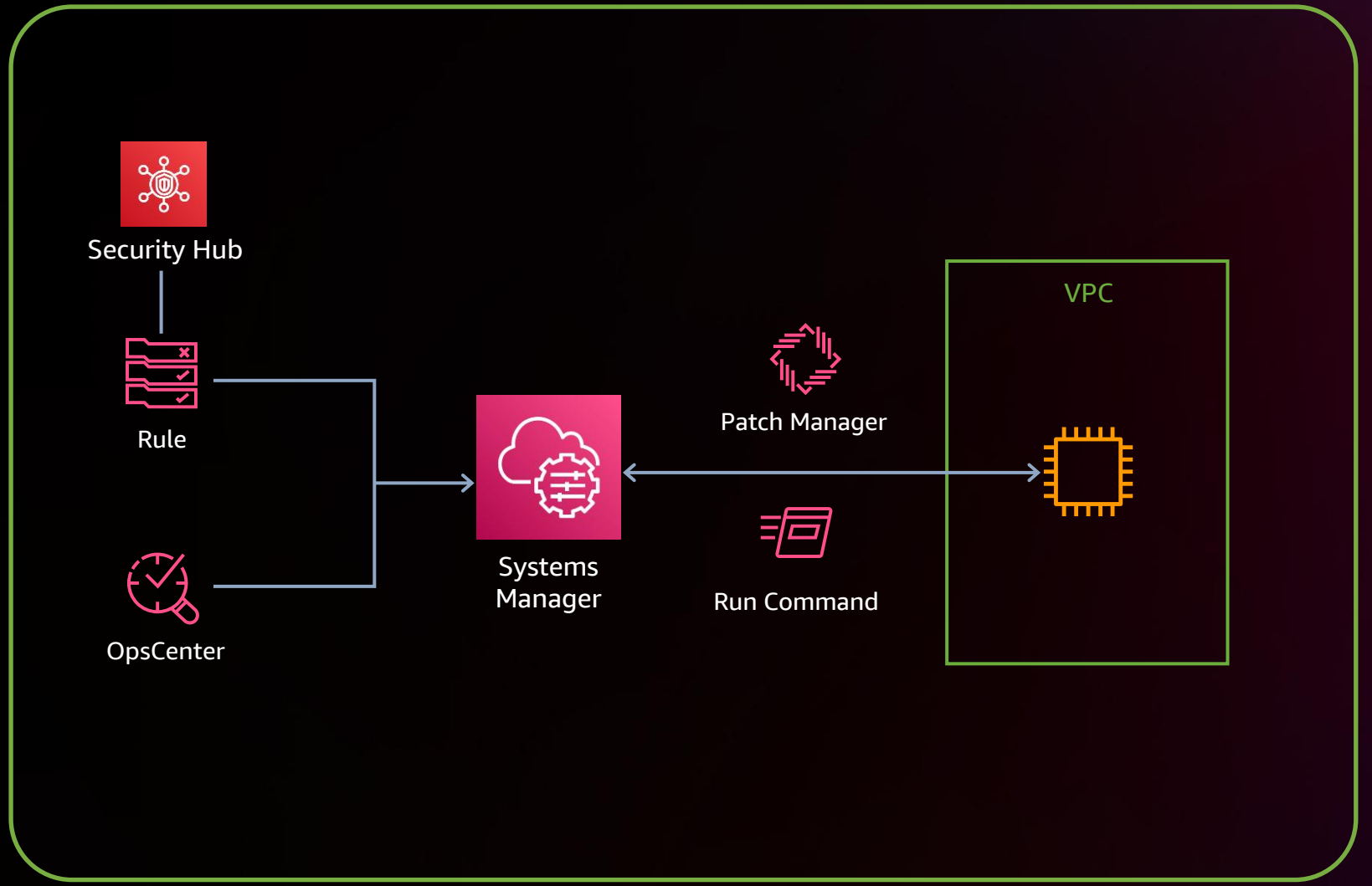
“Eradication and recovery should be done in a phased approach so that remediation steps are prioritized.”

NIST 800-61



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

Systems Manager



Patch Manager, a capability of Systems Manager:

Maintain instance compliance against your patch, configuration, and custom policies

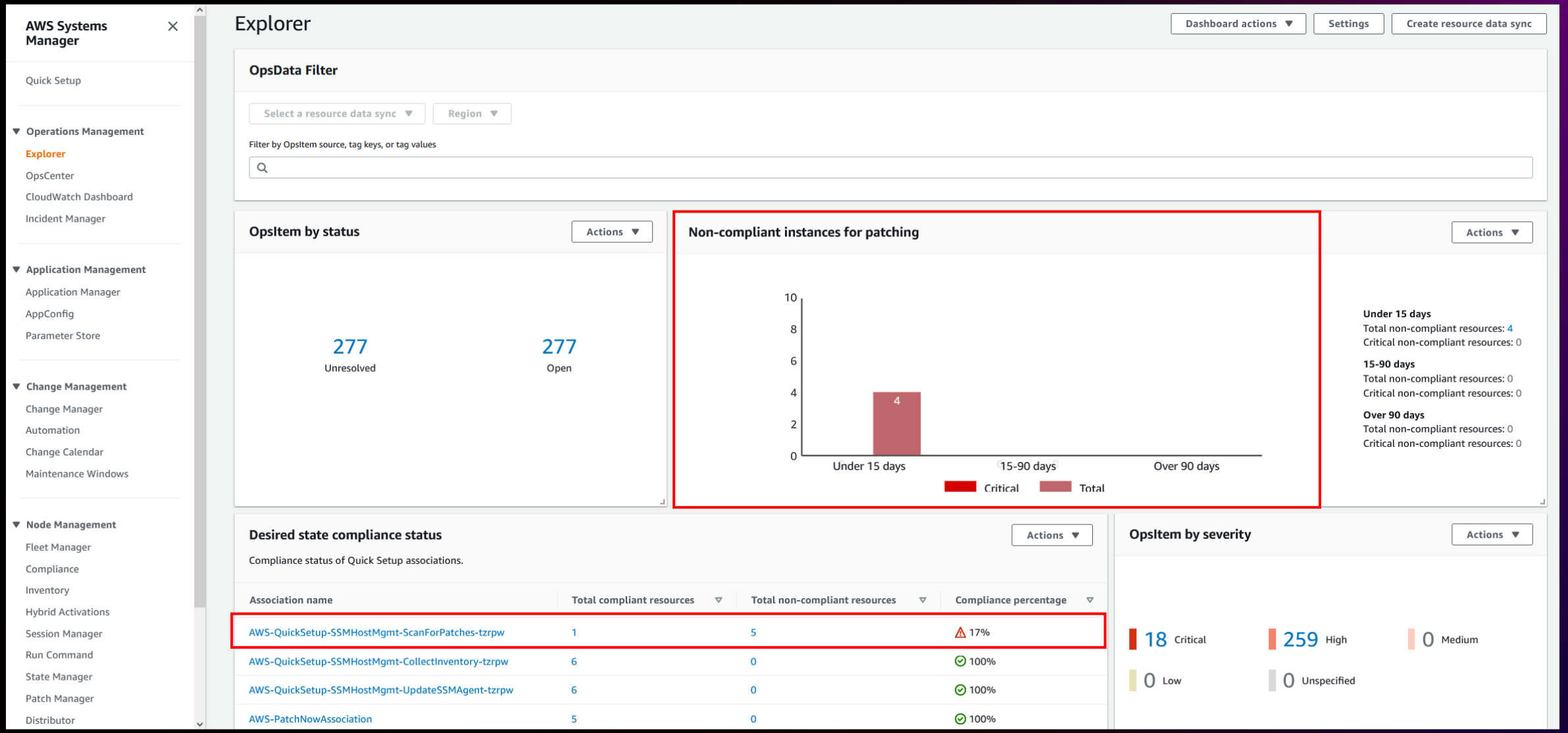
OpsCenter, a capability of Systems Manager:

Central location to view, investigate, and resolve operational items

aws

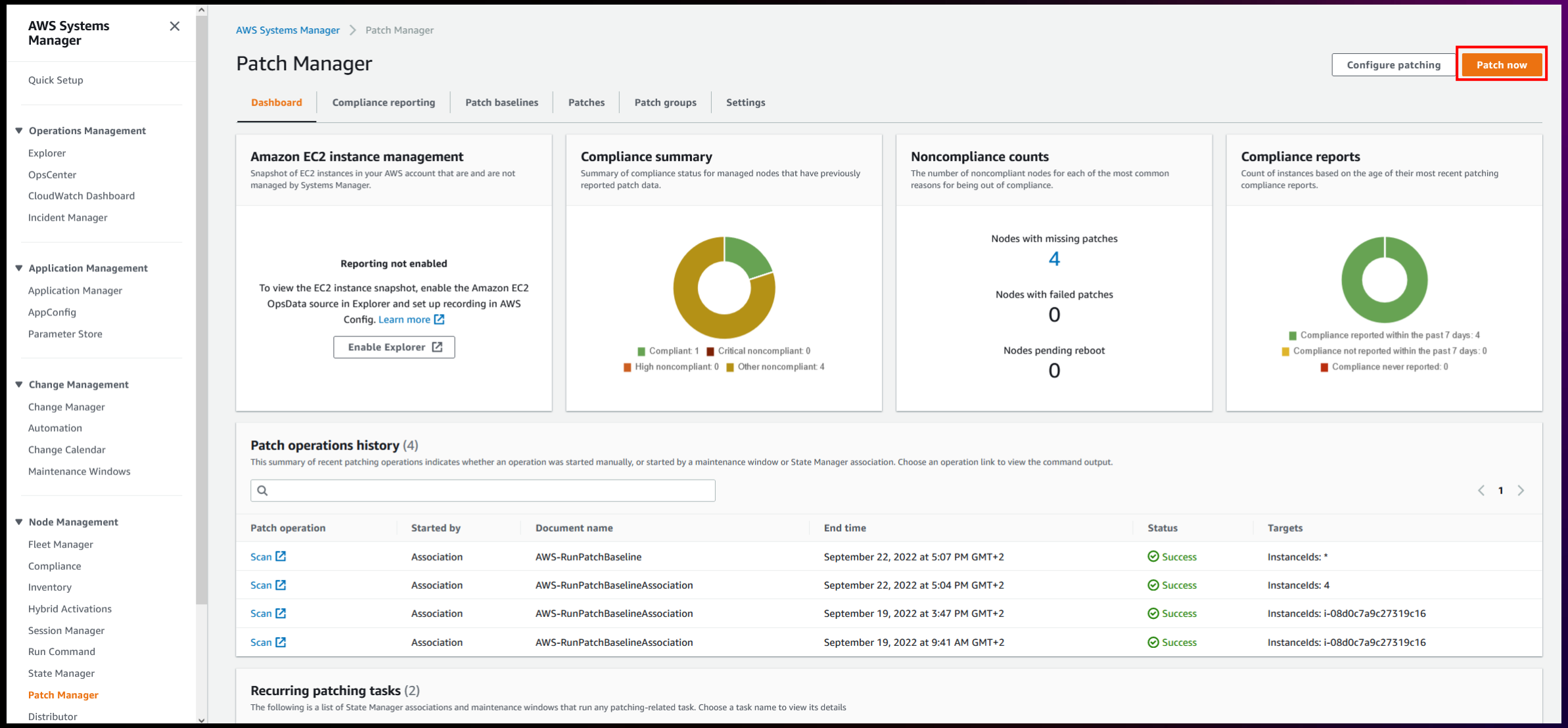
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Systems Manager



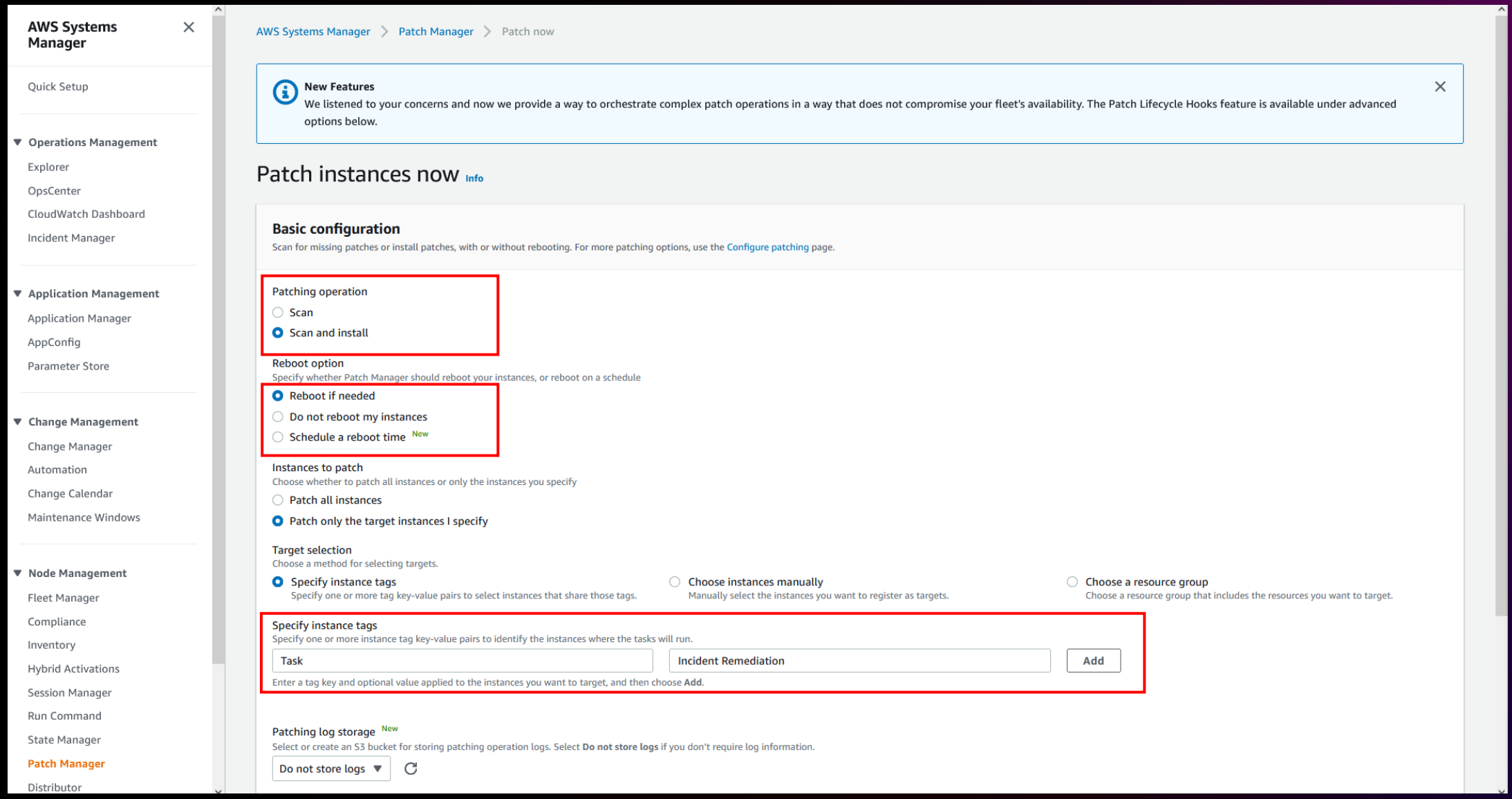
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Patch Manager



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

Patch Manager

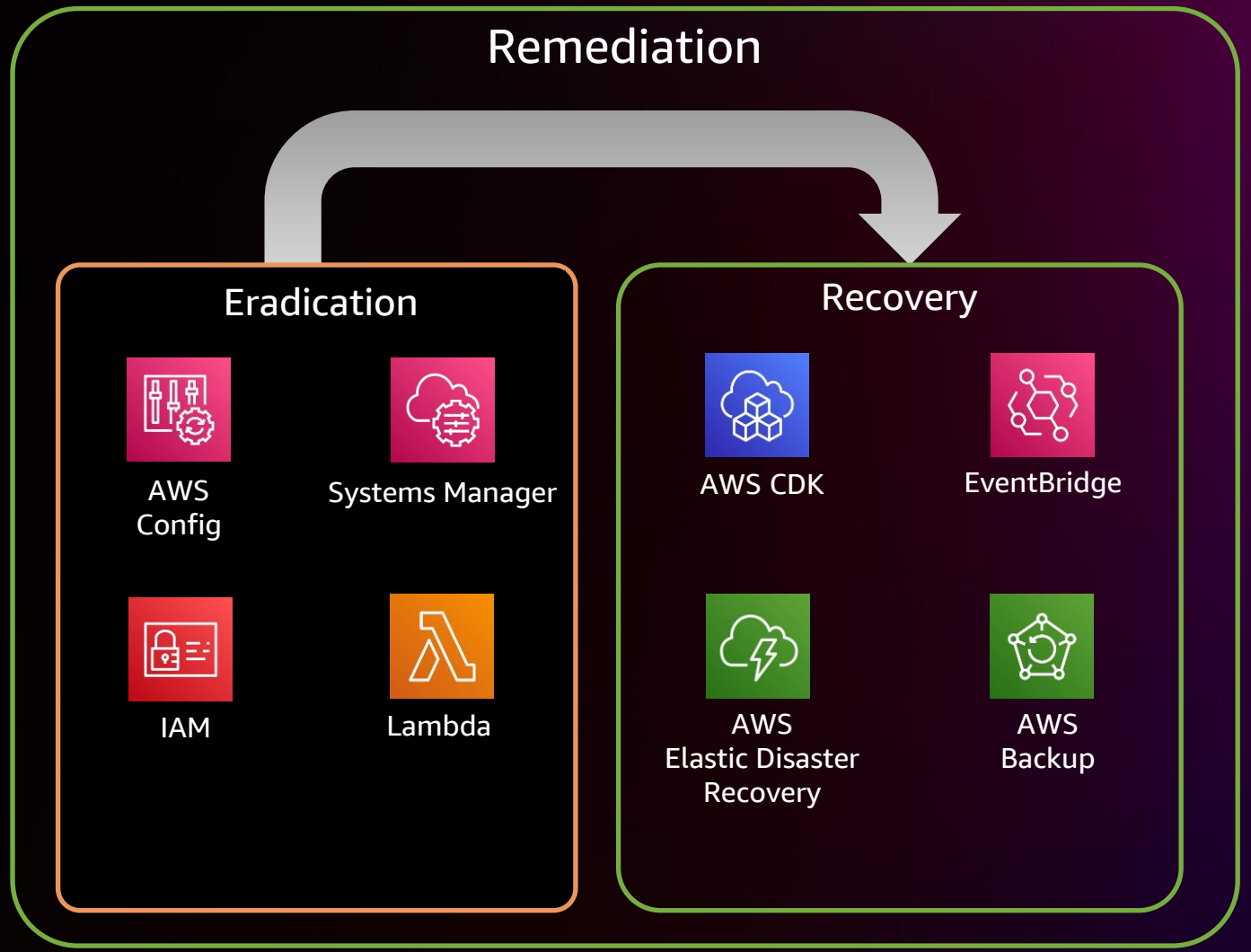


© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Remediation and Recovery

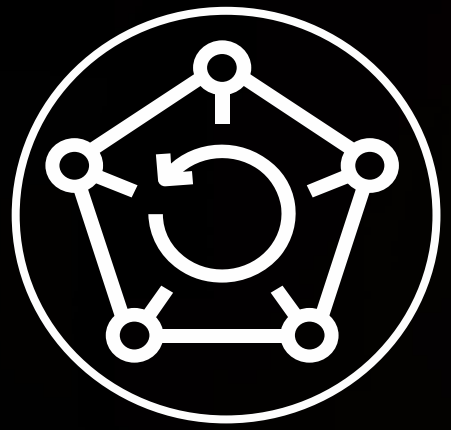
“Eradication and recovery should be done in a phased approach so that remediation steps are prioritized.”

NIST 800-61



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

AWS Backup



AWS Backup

A fully managed, policy-based backup service that makes it easy to centrally manage and automate the backup of data across AWS services



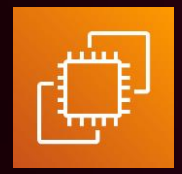
Amazon RDS



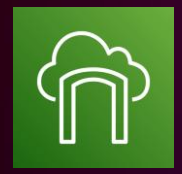
Amazon EBS



Amazon EFS



Amazon EC2



AWS Storage Gateway



Amazon DynamoDB



Amazon FSx for Lustre



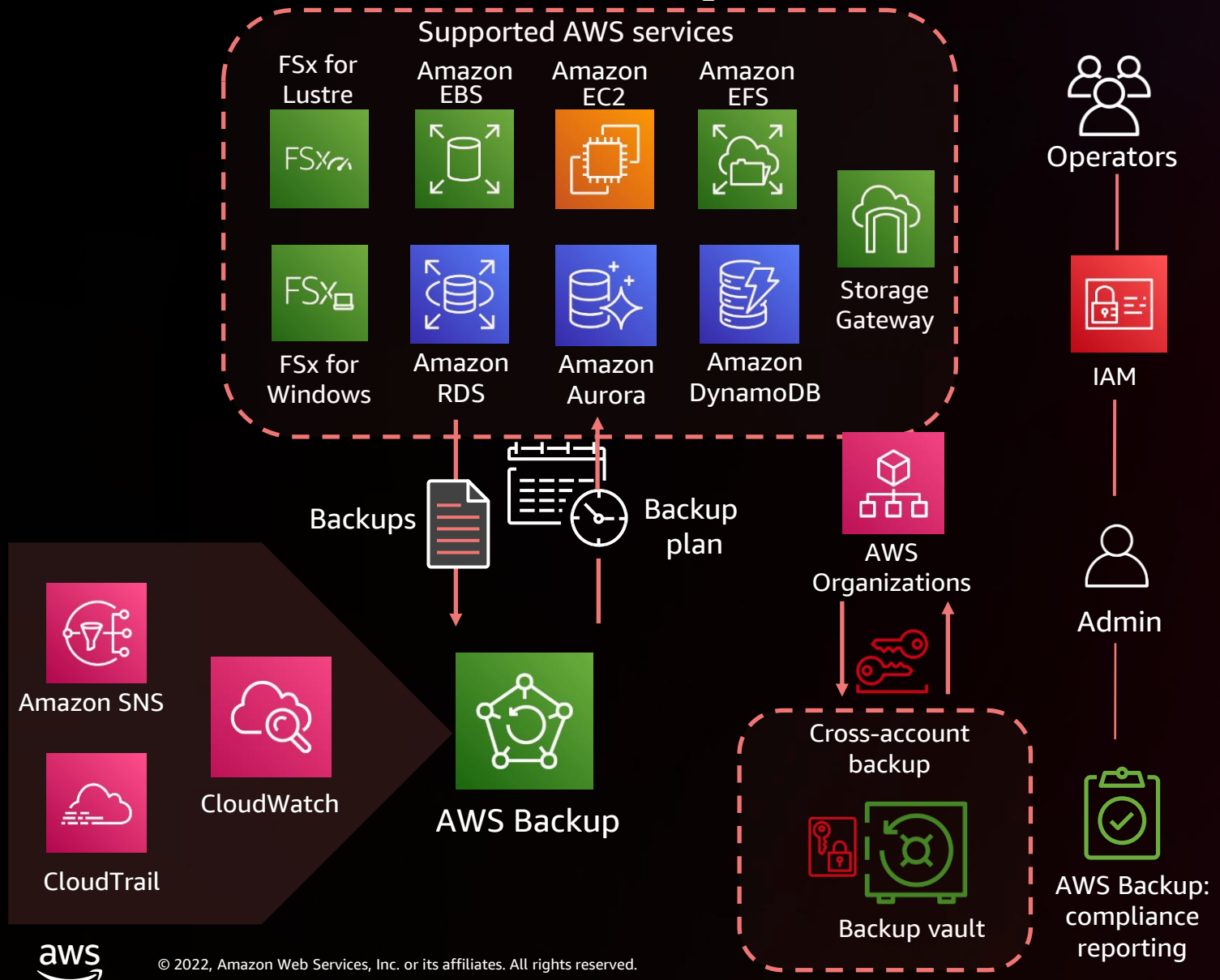
Amazon FSx for Windows File Server



Amazon Aurora

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

How AWS Backup works



Automate the restore processes

Restore using AWS cloud-native services or third-party services such as

- **AWS CDK**
- **AWS CloudFormation**

Or third-party services like Terraform

Scale through AWS Organizations

Automate backups across accounts and organizational units

Restrict access to backup plans

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

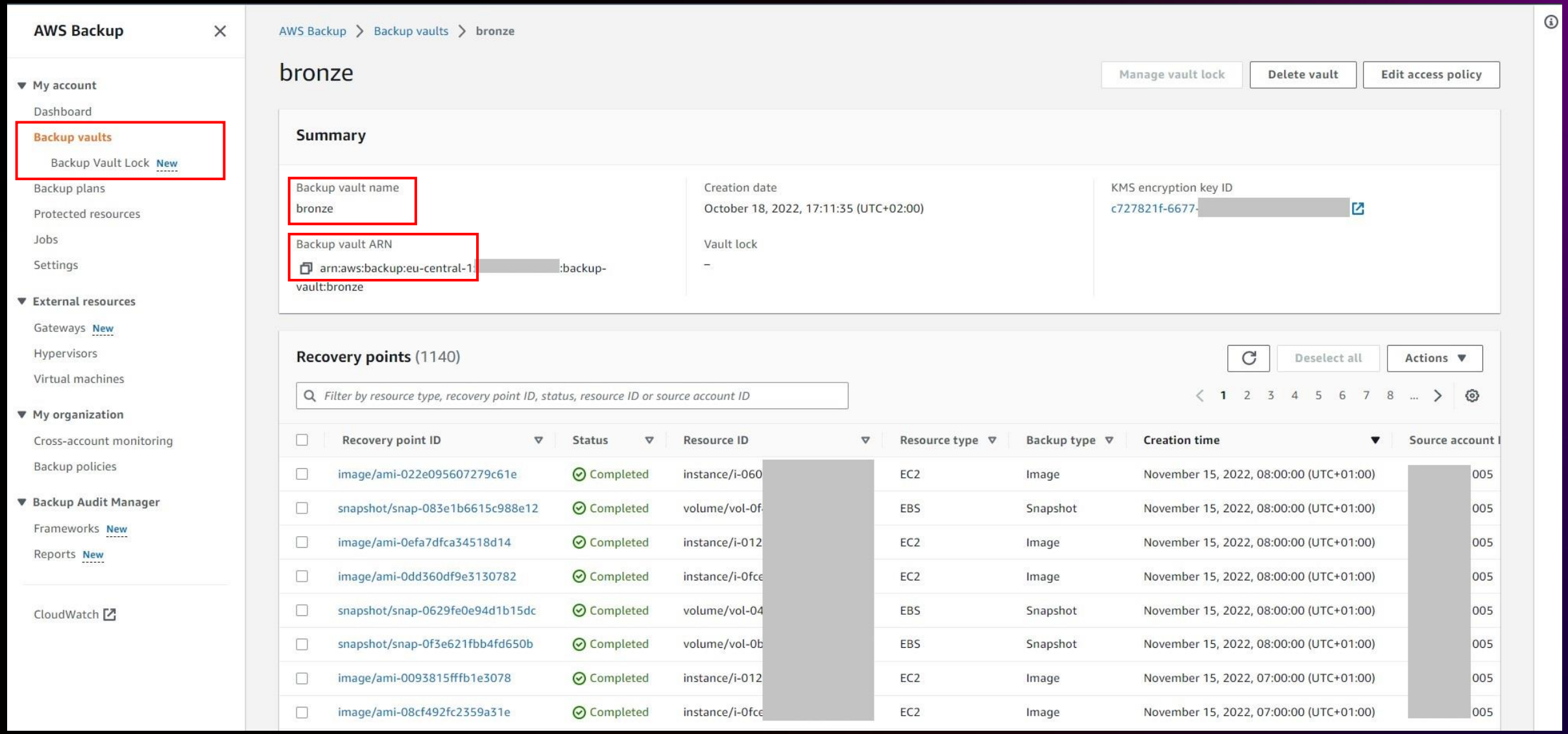
AWS Backup – Cross-account and cross-Region



Protecting prepared environments against account compromise

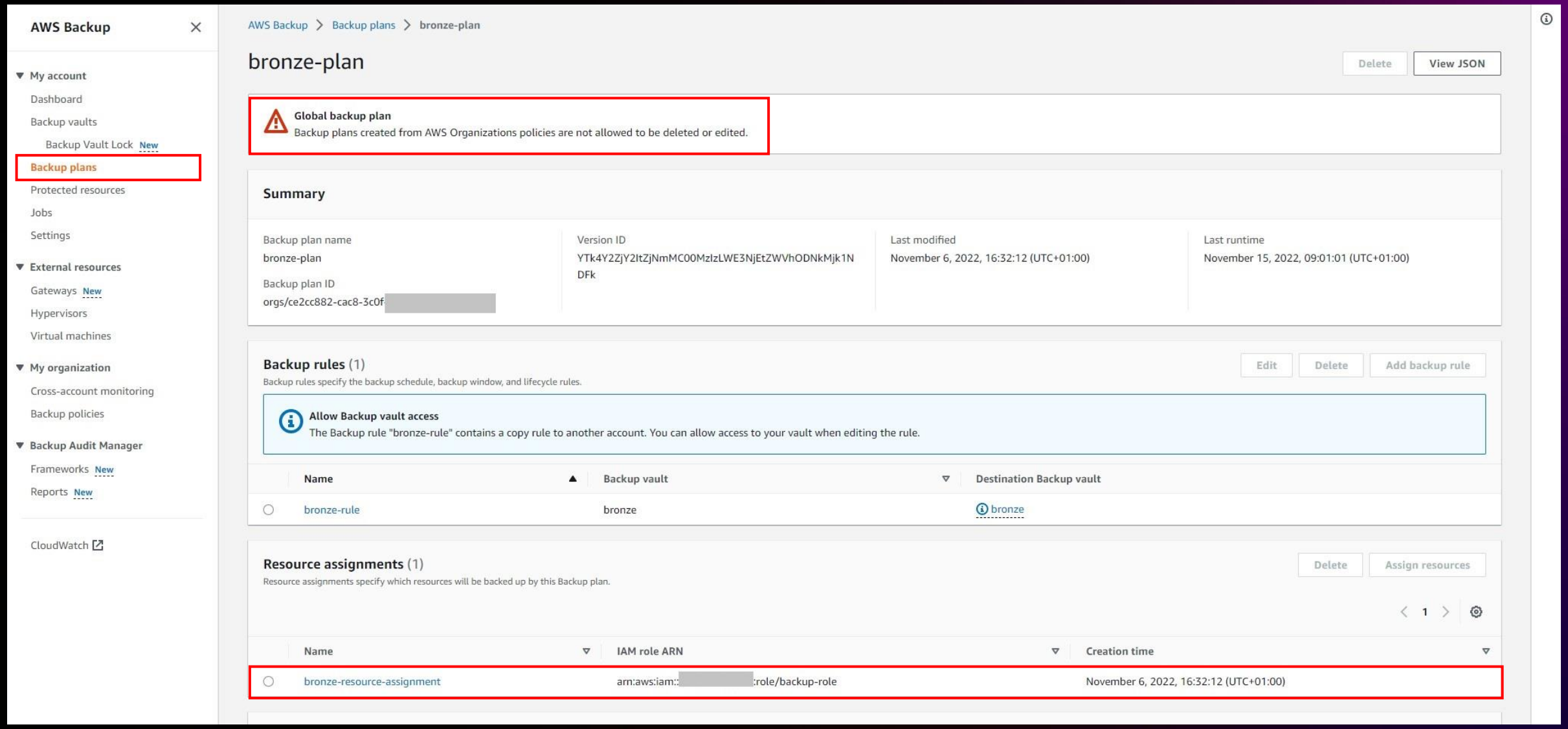
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

AWS Backup



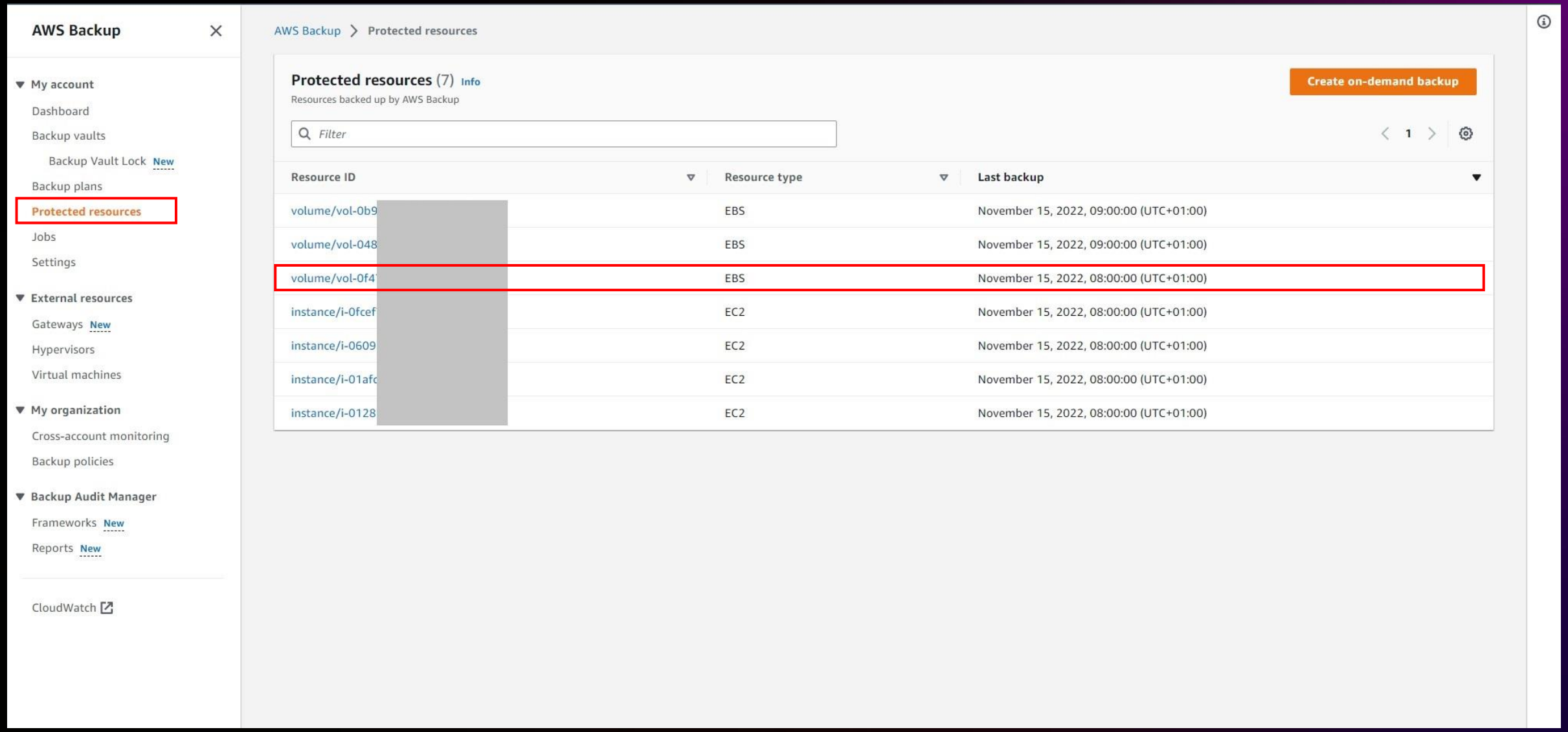
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

AWS Backup – Backup plan



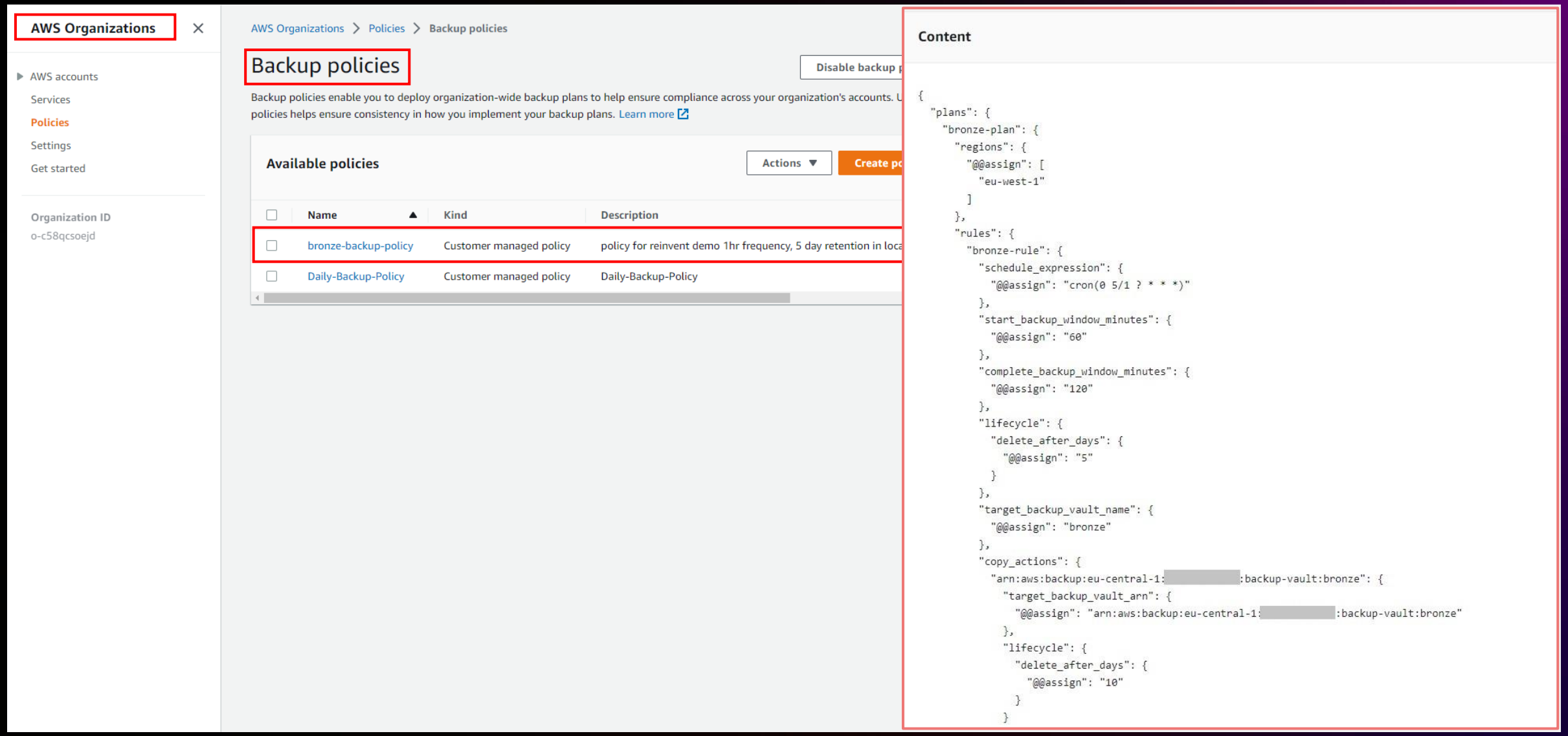
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

AWS Backup – Protected resources



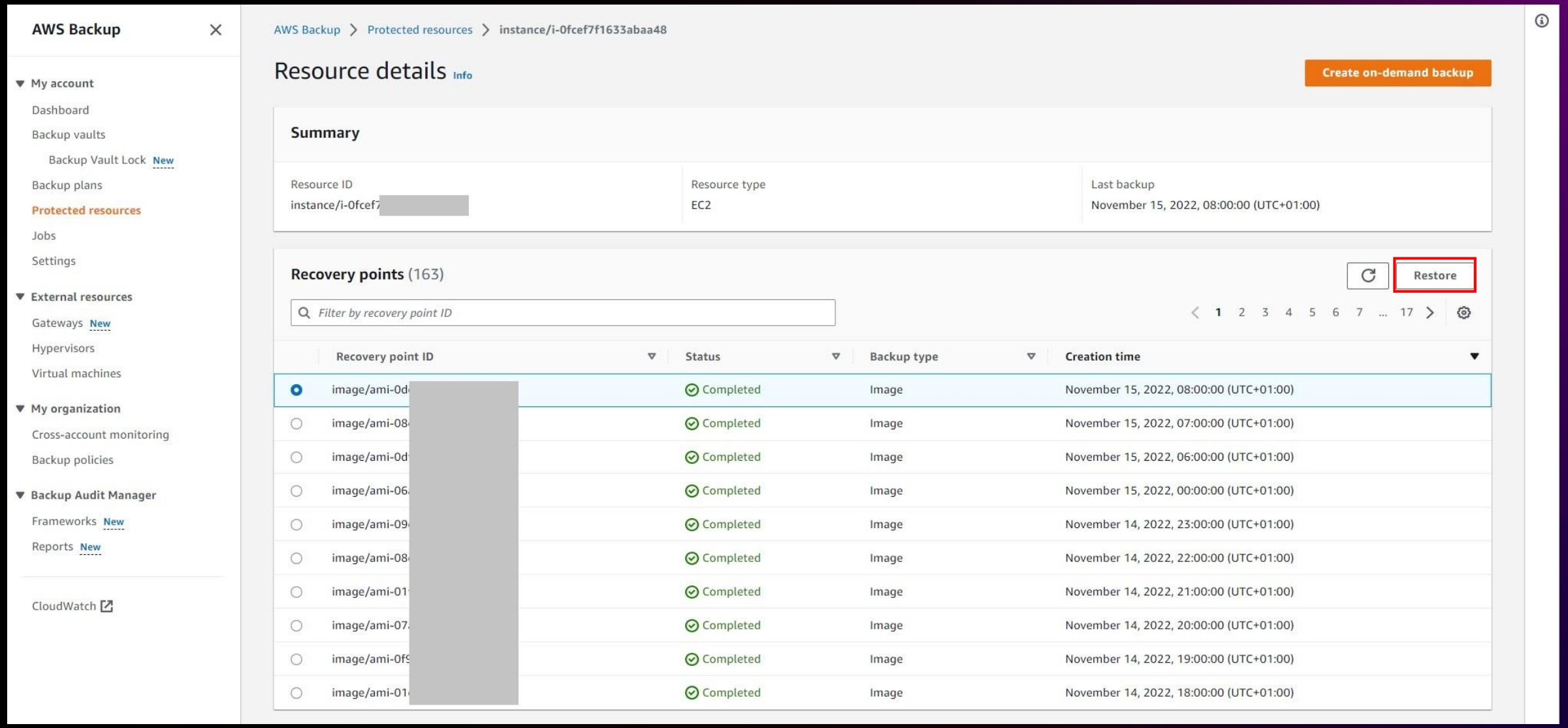
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

AWS Backup – Backup policy



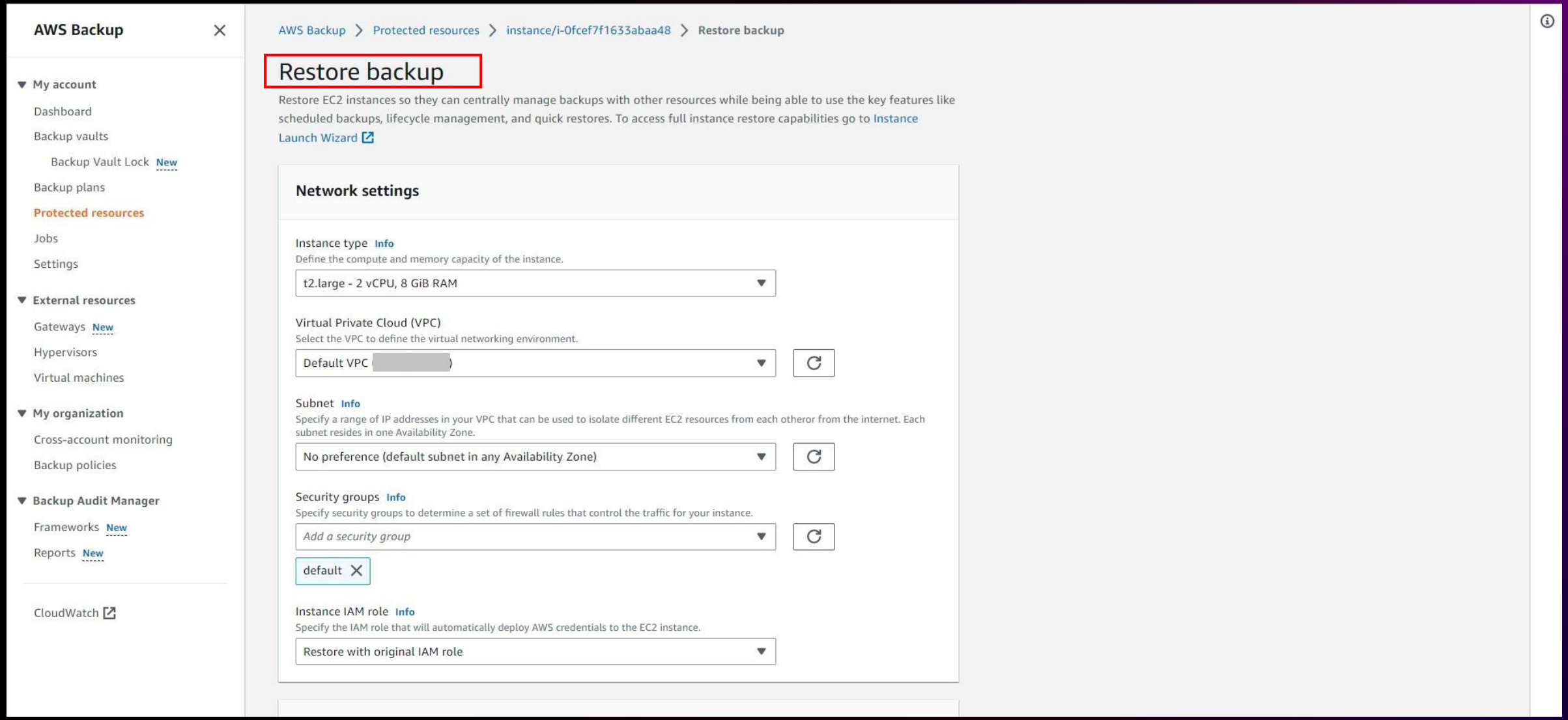
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

AWS Backup – Restore



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

AWS Backup – Restore



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

Post-incident activity

"One of the most important parts of incident response is also the most often omitted: learning and improving."

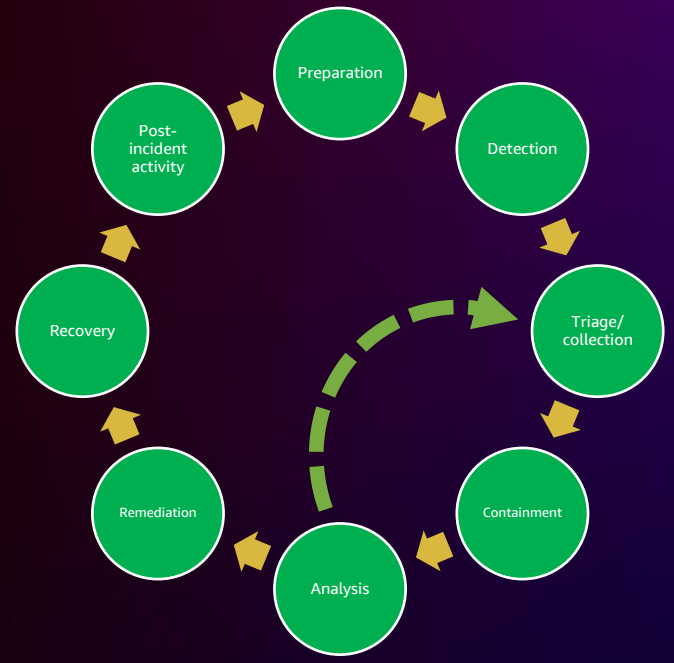


nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

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

Summary and conclusion

- ✓ Cloud-native services enable continuous and iterative progress through the threat detection and incident response lifecycle
- ✓ The entire enterprise landscape can be monitored, (logs) acquired, and analyzed
- ✓ Recovery and remediation is automated
- ✓ Cloud-native services supporting analysis and SIEM
- ✓ Quick feedback into the preparation phase



aws
© 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.