

# AWS re:Invent

NOV. 28 – DEC. 2, 2022 | LAS VEGAS, NV

# 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

# Agenda

## The incident response lifecycle

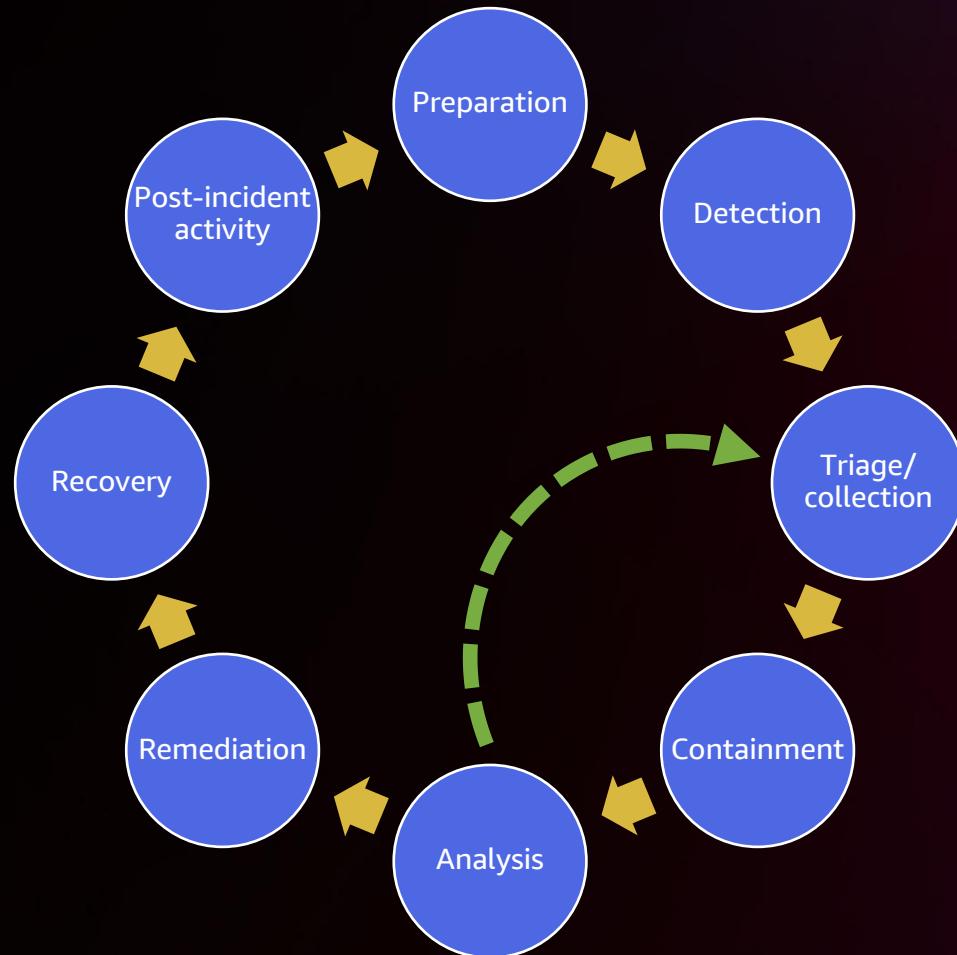
- What's different in the cloud
- What remains the same
- How cloud-native services are related to the cycle

## Let's look into the phases

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

## Summary and conclusion

# Incident response lifecycle



Based on NIST 800-61 incident response lifecycle

# 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 Cloud – Global infrastructure



## Global infrastructure

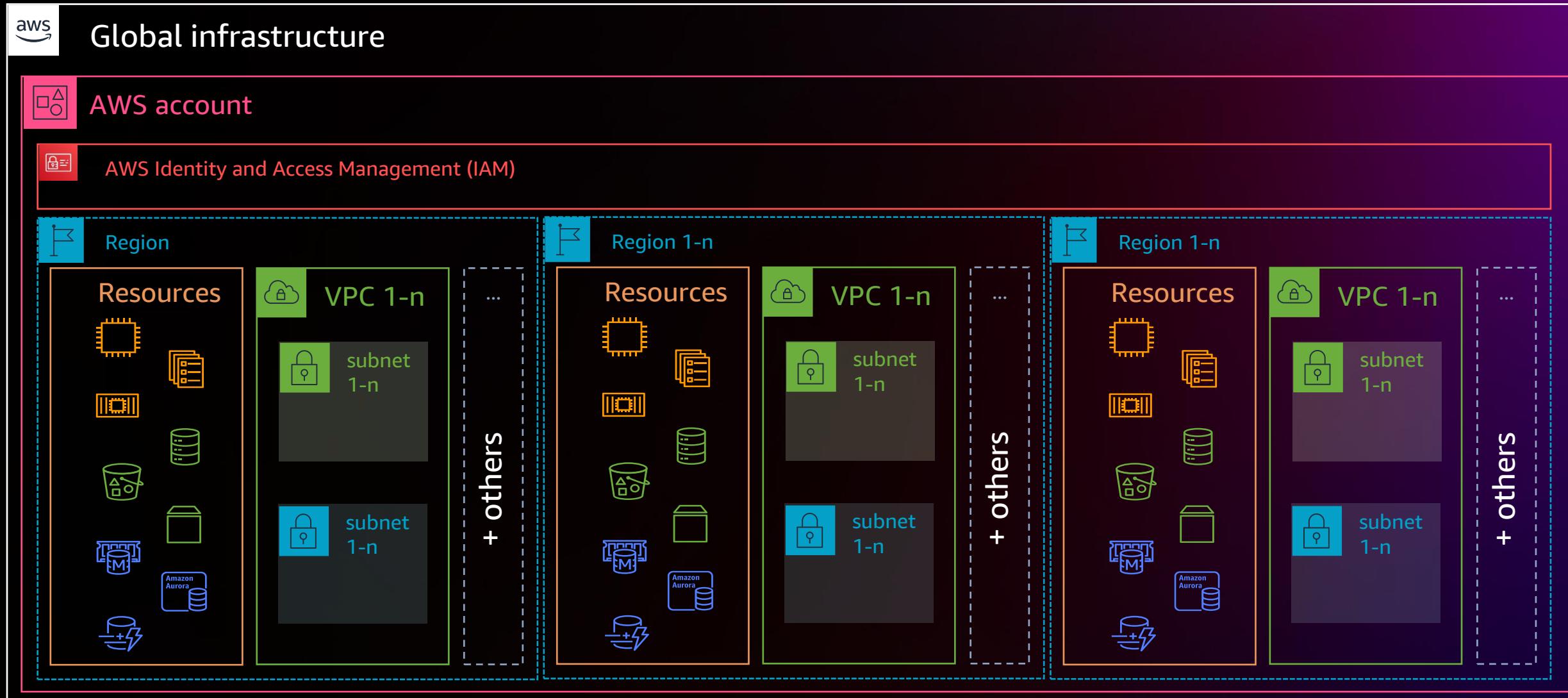


[aws.amazon.com/about-aws/global-infrastructure](https://aws.amazon.com/about-aws/global-infrastructure)



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

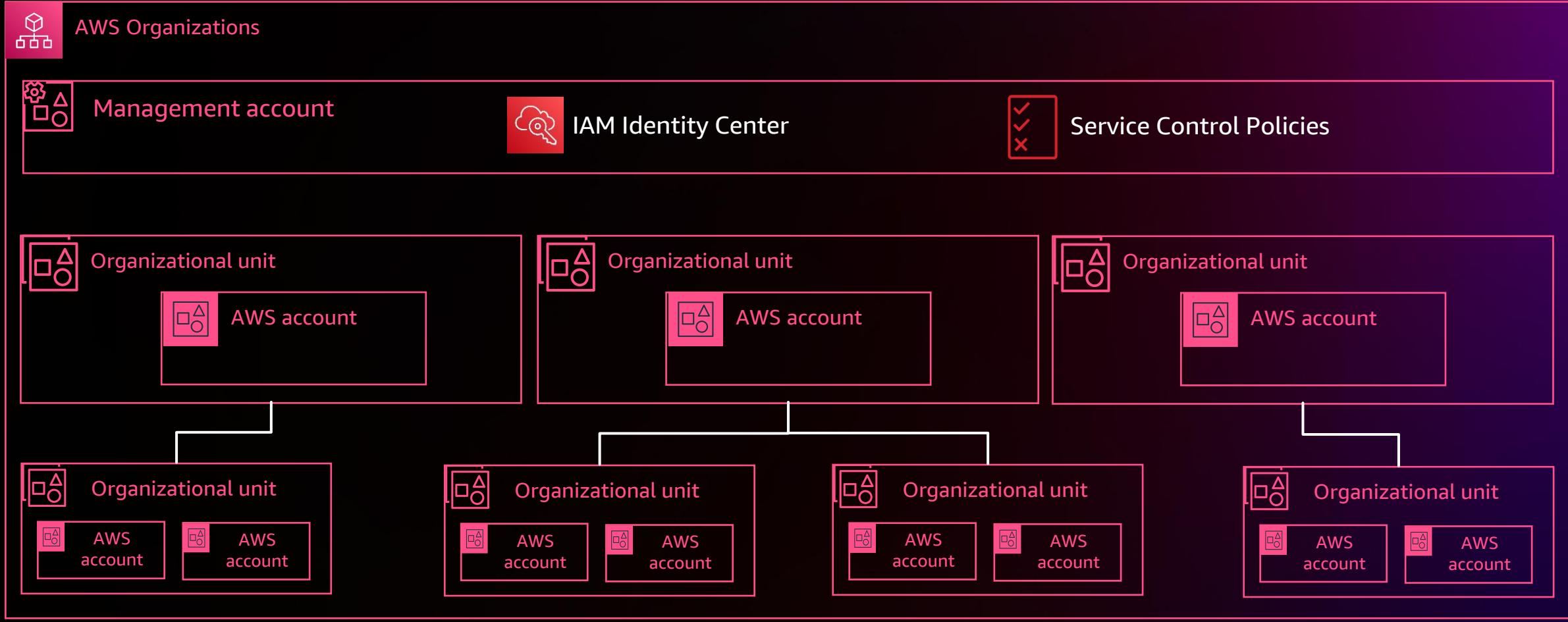
# AWS Cloud - Accounts



# AWS Cloud – Multiple accounts & organizations



Global infrastructure



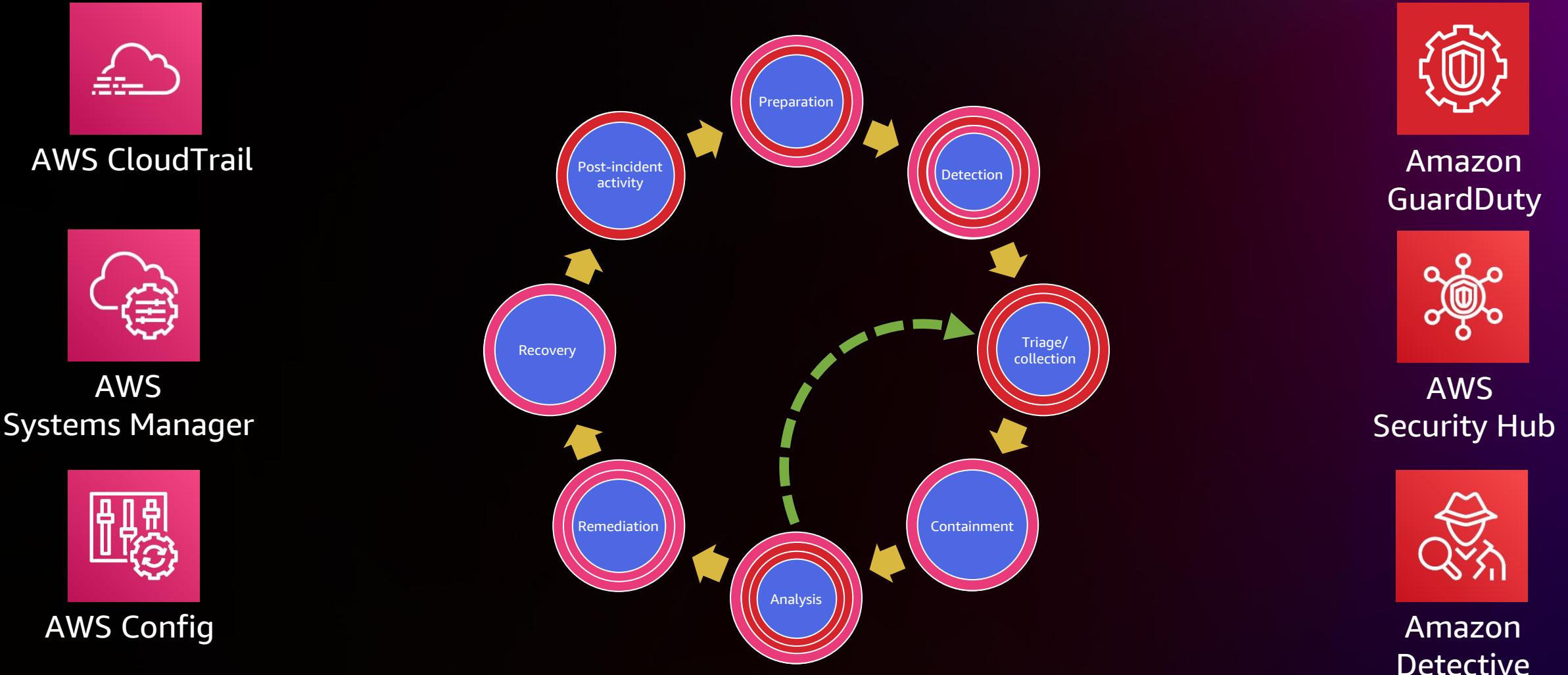
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# What remains the same

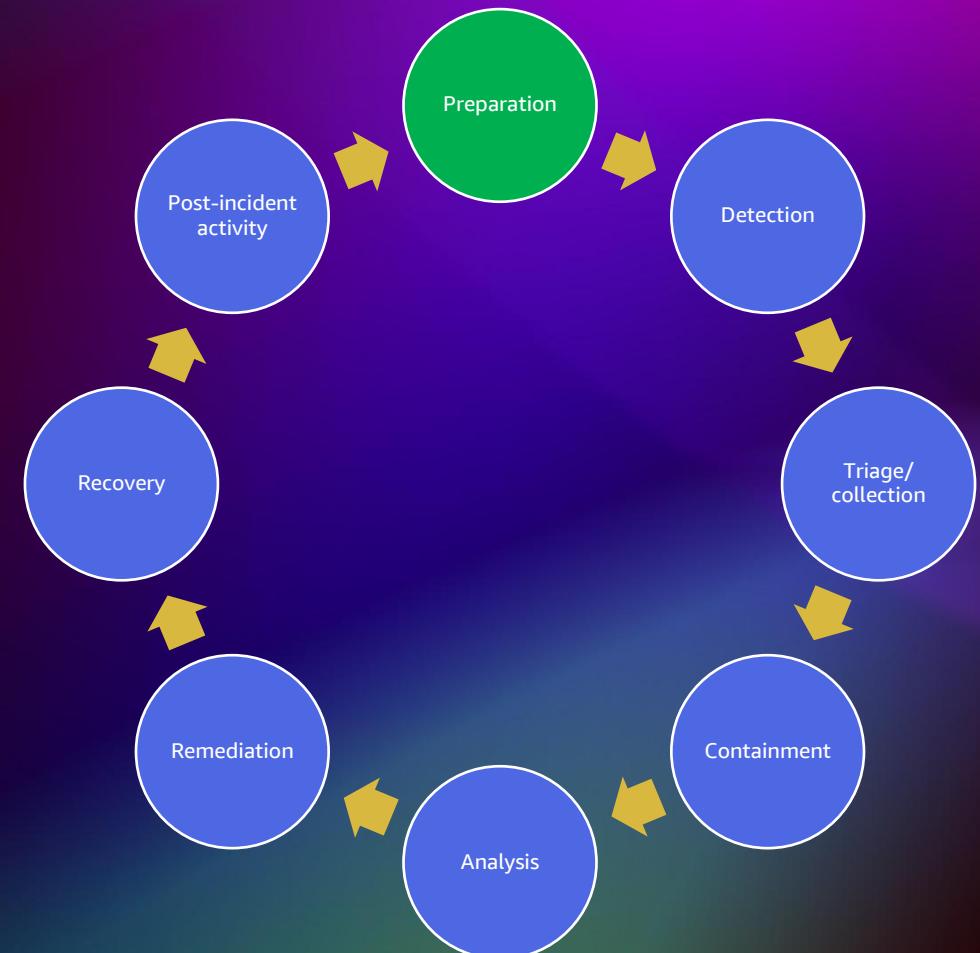
That said, many other incident response tasks remain the same

- 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

# How cloud-native services are related to the cycle



# Preparation



# Configure core services in AWS

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

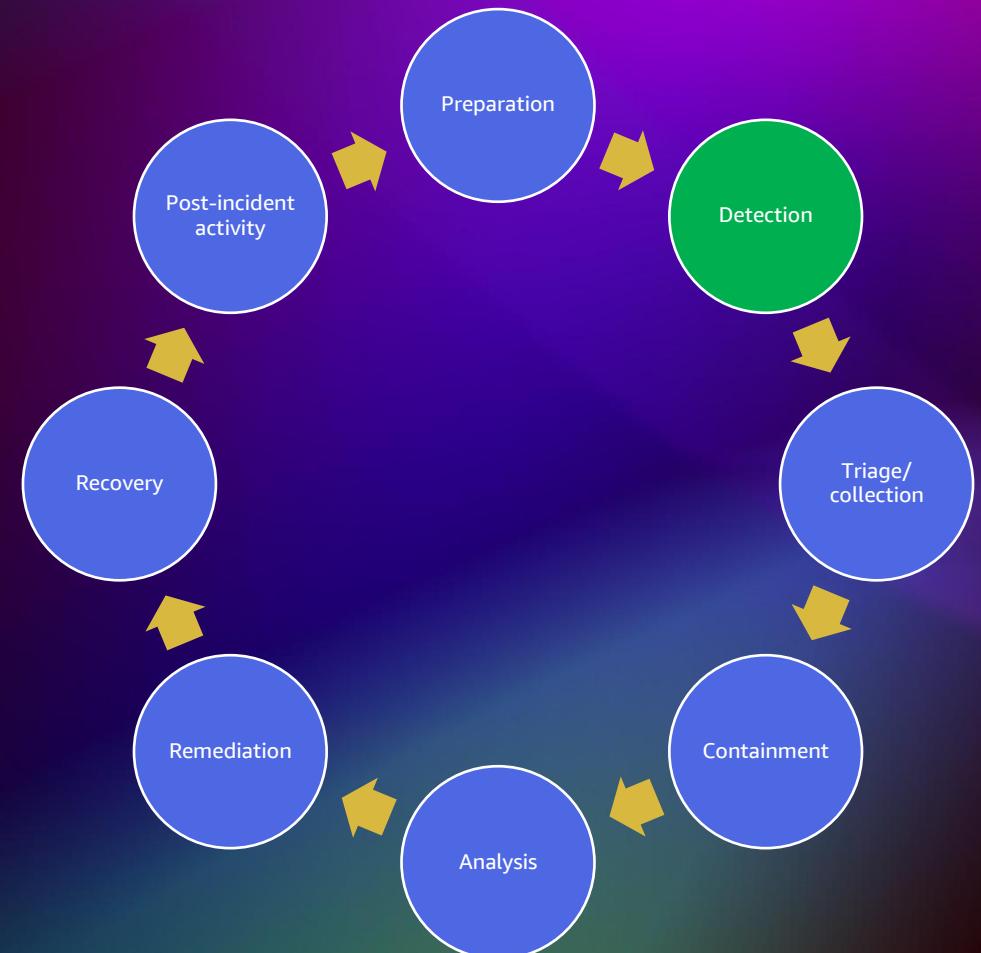
# Configure core logs in AWS

- ✓ 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
- ✓ ...

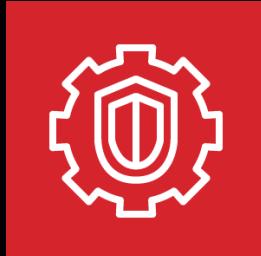
# Prepare your forensic environment in AWS

- ✓ 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
- ✓ . . .

# Detection

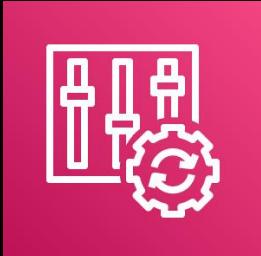


# Detection using AWS services



GuardDuty

Analyze log data  
for anomalies and  
malicious behavior



AWS  
Config

Check configuration  
status and rule  
compliance

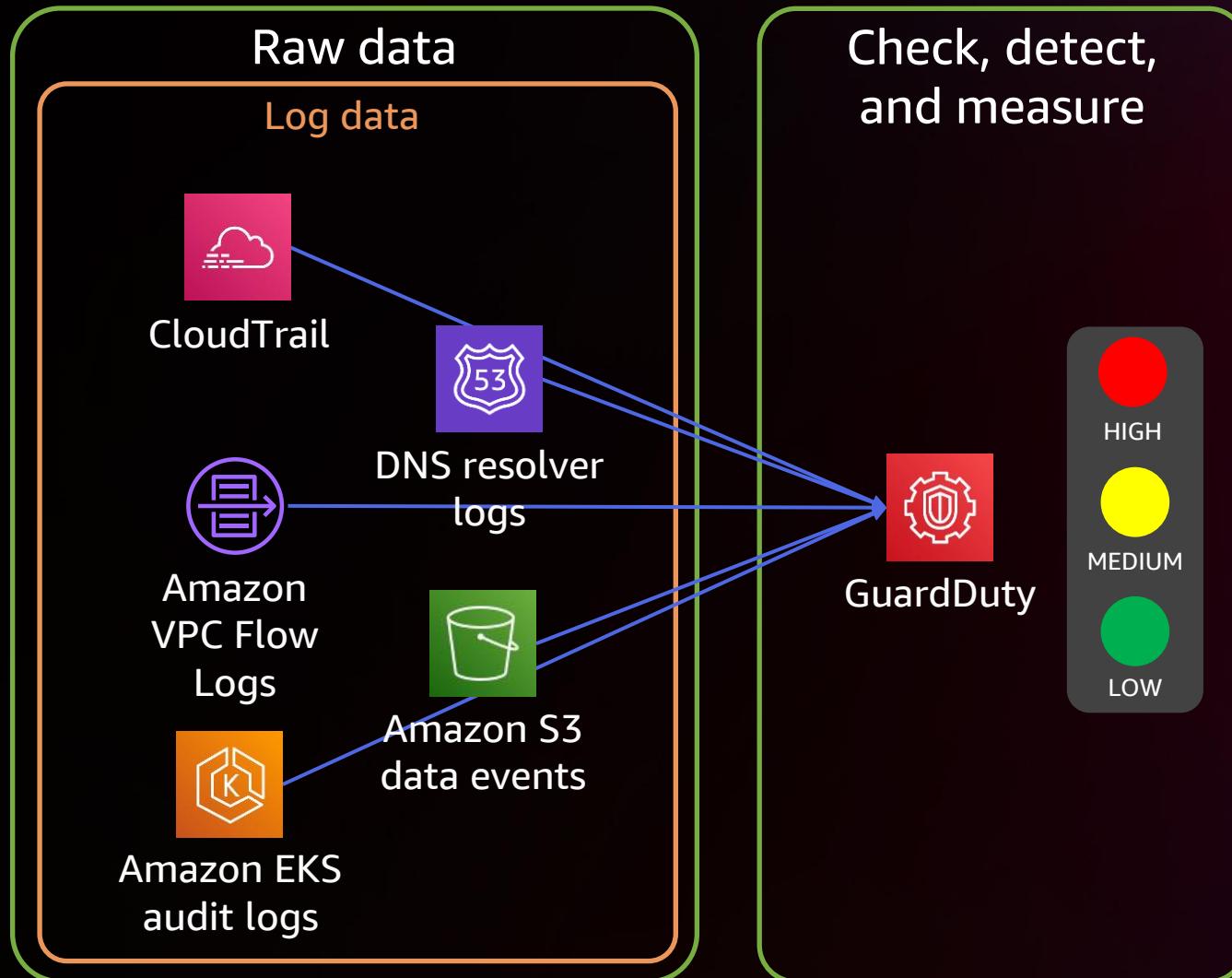


Amazon  
Inspector

Check for software  
vulnerabilities

# 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

# GuardDuty findings

Findings [Info](#)

[Suppress Findings](#) [Info](#)

[Current](#) [Add filter criteria](#)

Saved rules [Apply saved rules](#)

[Actions](#)

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



# GuardDuty findings details

⚠️ Backdoor:EC2/C&CActivity.B!DNS      Instance: [i-07a954a1fbc76df2e](#)

**Backdoor:EC2/C&CActivity.B!DNS** ⚡ Feedback

Finding ID: [9ec1226c76c28c10b70cb0d4626d560](#)

**High** EC2 instance i-07a954a1fbc76df2e is querying a domain name associated with a known Command & Control server. [Info](#)

ⓘ Investigate with Detective

**Overview**

Severity	HIGH
Region	eu-west-1
Count	4
Account ID	[REDACTED]
Resource ID	<a href="#">i-07a954a1fbc76df2e</a>
Created at	07-28-2022 14:47:23 (2 months ago)
Updated at	07-28-2022 15:09:04 (2 months ago)

**Malware scan**

Scan ID	9453f5942e896cab64e9ef2646f95893
Scan status	COMPLETED
Start time	07-28-2022 14:50:01
End time	07-28-2022 15:26:04
Security status	INFECTED

**Resource affected**

Resource role	TARGET
Resource type	Instance

**Instance details**

Instance ID	i-07a954a1fbc76df2e
Instance type	t2.xlarge
Instance state	running
Availability zone	eu-west-1c
Image ID	ami-08b3f7210f8afa7e3
Launch time	07-28-2022 12:23:35

**IAM instance profile**

ARN	arn:aws:iam::1:instance-profile/EC2-PROWLER-WITH-SSM
-----	--

⚠️ Execution:EC2/MaliciousFile      Instance: [i-07a954a1fbc76df2e](#)

**Execution:EC2/MaliciousFile** ⚡ Feedback

Finding ID: [3ac1227e2cd55ae820270e2f4fb86d7b](#)

**High** 2 security risk(s) detected including EICAR-Test-File (not a virus) on EC2 instance i-07a954a1fbc76df2e. [Info](#)

ⓘ Investigate with Detective

**Overview**

Severity	HIGH
Region	eu-west-1
Count	1
Account ID	[REDACTED]
Resource ID	<a href="#">i-07a954a1fbc76df2e</a>
Created at	07-28-2022 15:26:04 (2 months ago)
Updated at	07-28-2022 15:26:04 (2 months ago)
Scan ID	<a href="#">9453f5942e896cab64e9ef2646f95893</a>

**Threats detected (2)**

1. EICAR-Test-File (not a virus)

Name	EICAR-Test-File (not a virus)
Severity	HIGH
Hash	275a021bbfb6489e54d471899f7db9d1663fc695ec2fe2a2c45...
File path	/Users/Administrator/Downloads/eicar.com
File name	eicar.com
Volume ARN	arn:aws:ec2:eu-west-

2. EICAR-Test-File (not a virus)

Name	EICAR-Test-File (not a virus)
Severity	HIGH
Hash	275a021bbfb6489e54d471899f7db9d1663fc695ec2fe2a2c45...
File path	/Users/Administrator/Downloads/eicar_com.zip=>eicar.com
File name	eicar_com.zip=>eicar.com
Volume ARN	arn:aws:ec2:eu-west-

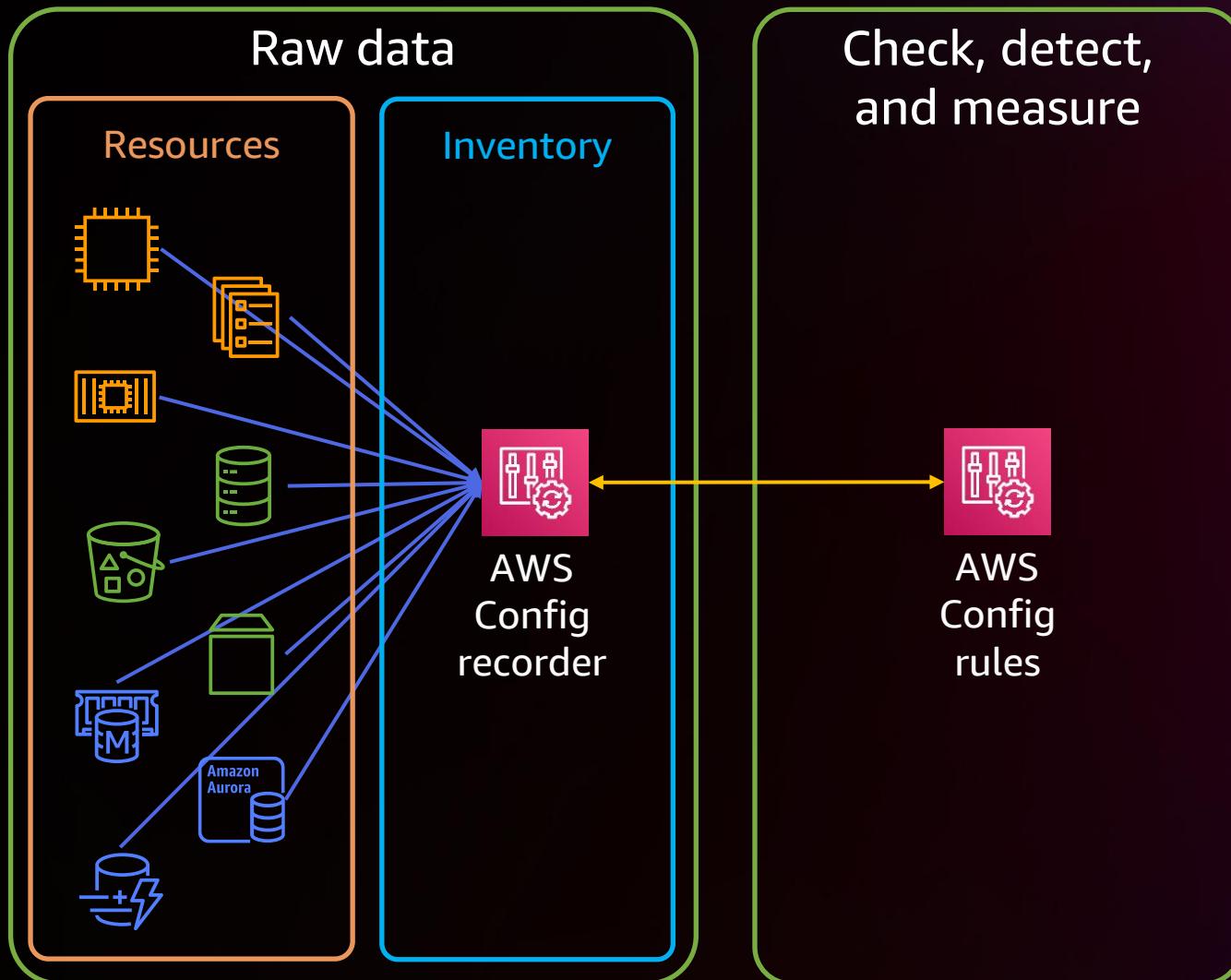
**Resource affected**

Resource type	Instance
---------------	----------



# 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

# AWS Config resources

## Resource Inventory

Search existing or deleted resources recorded by AWS Config. For a specific resource, view the resource details, configuration timeline, or compliance timeline. The resource configuration timeline allows you to view all the configuration items captured over time for a specific resource. The resource compliance timeline allows you to view compliance status changes. To query your resource configurations, use the [advanced SQL query editor](#).

**Resources**

Resource category: AWS resources | Resource type: Multiple Selected | Compliance: Any compliance status

**Resource identifier - optional**

Include deleted resources

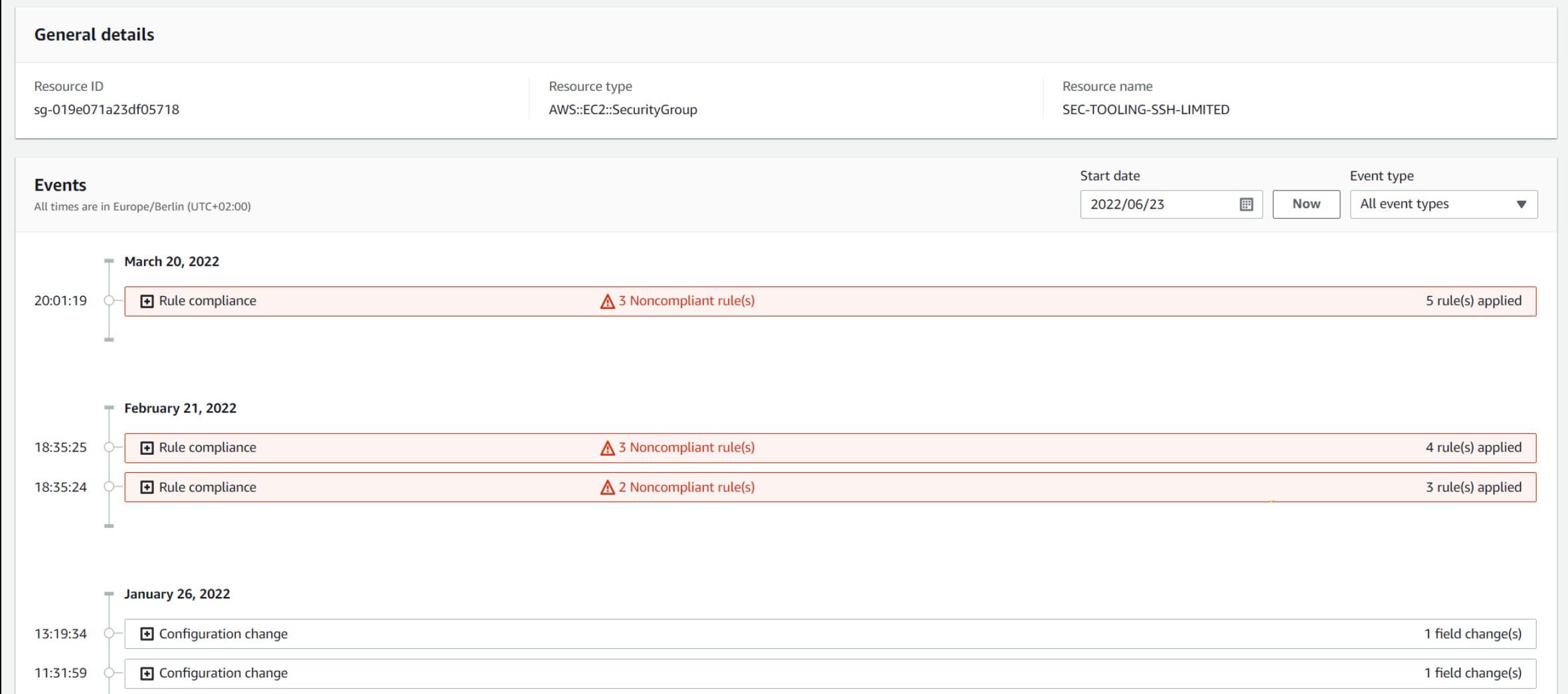
1 / 1

Resource identifier	Type	Compliance
sg-019e071a23df05718	EC2 SecurityGroup	⚠ Noncompliant
sg-04113ea6e68c26d4b	EC2 SecurityGroup	⚠ Noncompliant
sg-048d5ac026fe26139	EC2 SecurityGroup	✓ Compliant
sg-0cd88dd079707cd4b	EC2 SecurityGroup	⚠ Noncompliant
sg-addaf3f3	EC2 SecurityGroup	⚠ Noncompliant



# AWS Config resources timeline

## Timeline



# 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					
		<a href="#">View details</a>	<a href="#">Edit rule</a>	<a href="#">Actions ▾</a>	<a href="#">Add rule</a>
Name		Remediation action	Type	Compliance	
<a href="#">EmrMasterNoPublicIp-conformance-pack-uqghya0wp</a>		Not set	AWS managed	-	
<a href="#">EfsEncryptedCheck-conformance-pack-uqghya0wp</a>		Not set	AWS managed	-	
<a href="#">CloudTrailLogFileValidationEnabled-conformance-pack-vieezssqt</a>		Not set	AWS managed	Compliant	
<a href="#">CMKBackingKeyRotationEnabled-conformance-pack-vieezssqt</a>		Not set	AWS managed	4 Noncompliant resource(s)	
<a href="#">Ec2SecurityGroupAttachedToEni-conformance-pack-uqghya0wp</a>		Not set	AWS managed	11 Noncompliant resource(s)	
<a href="#">CloudwatchLogGroupEncrypted-conformance-pack-uqghya0wp</a>		Not set	AWS managed	24 Noncompliant resource(s)	
<a href="#">Ec2ManagedinstanceAssociationCompliance-conformance-pack-uqghya0wp</a>		Not set	AWS managed	Compliant	
<a href="#">AcmCertificateExpirationCheck-conformance-pack-uqghya0wp</a>		Not set	AWS managed	2 Noncompliant resource(s)	
<a href="#">IamPasswordPolicyCheck-conformance-pack-vieezssqt</a>		Not set	AWS managed	1 Noncompliant resource(s)	
<a href="#">CloudTrailCloudWatchLogsEnabled-conformance-pack-vieezssqt</a>		Not set	AWS managed	1 Noncompliant resource(s)	



# AWS Config rules details

CMKBackingKeyRotationEnabled-conformance-pack-vieezssqt

Actions ▾

▼ Rule details

Description

Checks that key rotation is enabled for each key and matches to the key ID of the customer created customer master key (CMK). The rule is compliant, if the key rotation is enabled for specific key object.

Config rule ARN

arn:aws:config:eu-west-1: [REDACTED] config-rule/aws-service-rule/config-conforms.amazonaws.com/config-rule-siz3qq

Trigger type

Periodic: 12 hours

Scope of changes

-

Last successful evaluation

⌚ September 19, 2022 6:12 AM

Edit

▼ Resources in scope

View details Remediate C

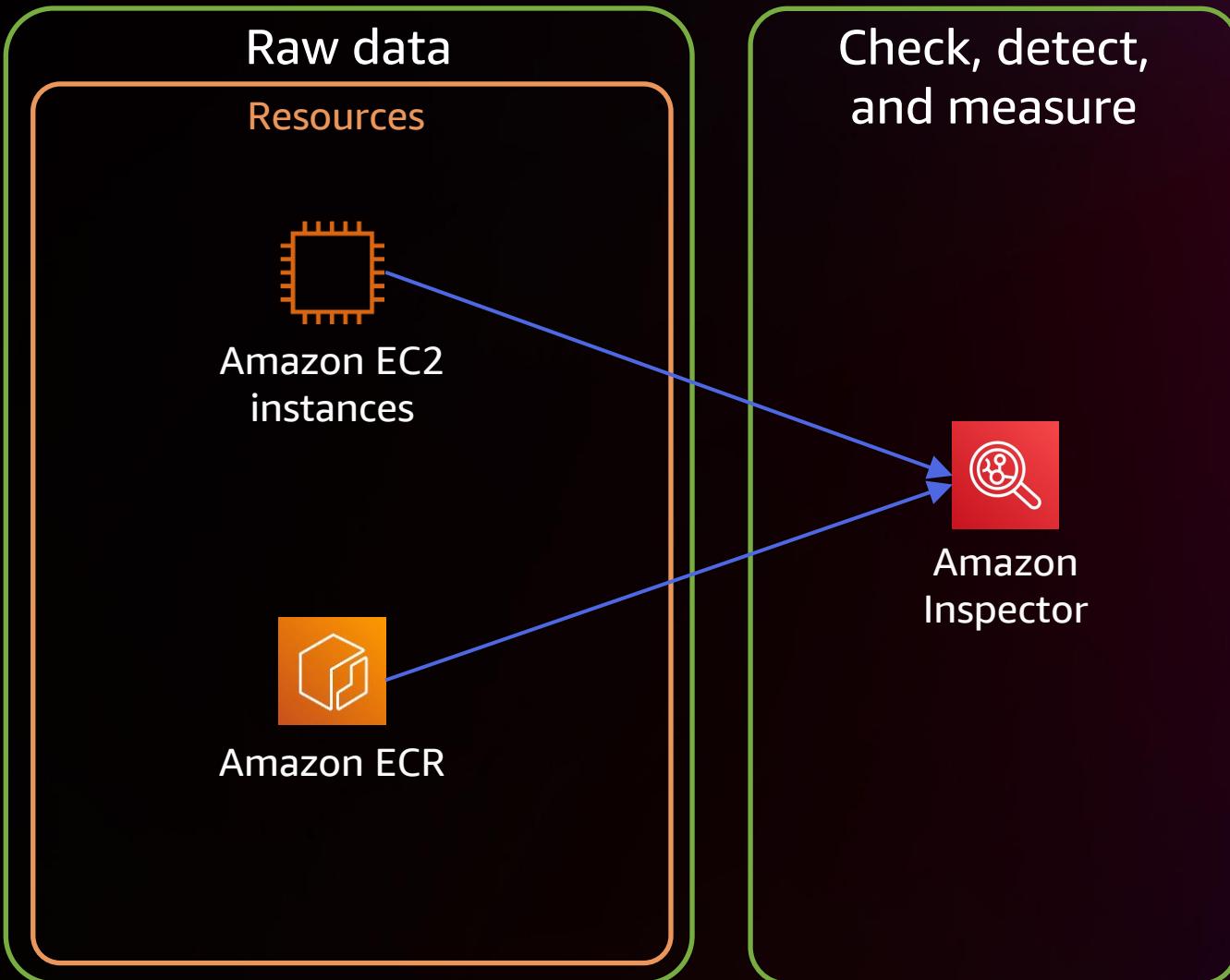
Noncompliant ▾

< 1 > ⏪ ⏩ ⏴

ID	Type	Status	Annotation	Compliance
b9e77947-1283-4406-ba37-c0199928f998	KMS Key	-	-	⚠️ Noncompliant
bc7ee0d3-72ae-4e90-be7a-46f4f01f1d5b	KMS Key	-	-	⚠️ Noncompliant
cb9d2583-ba15-4bee-9be3-48d65f45708a	KMS Key	-	-	⚠️ Noncompliant
d128e4a1-9864-43c0-b2d1-468c50183f48	KMS Key	-	-	⚠️ Noncompliant

# 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**

# Amazon Inspector summary

Summary Info

Viewing data from all accounts

**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 0 total findings	21 Critical 700 total findings	0 Critical 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



# Amazon Inspector findings

CVE-2022-34903 - gnupg2  
Finding ID: arn:aws:inspector:eu-west-1:finding/6346c87d9e9889d1f351d820eb563324

A vulnerability was found in GnuPG. This issue occurs due to an escape detection loop at the write\_status\_text\_and\_buffer() function in g10/cpr.c. This flaw allows a malicious actor to bypass access control.

Finding details   Inspector Score

Finding overview

AWS account ID	[REDACTED]
Severity	Medium
Type	Package Vulnerability
Fix Available	Yes
Created at	September 11, 2022 2:17 PM (UTC+02:00)

Affected packages

Name	gnupg2
Installed version / Fixed Version	0:2.0.22-5.amzn2.0.4.X86_64 / 0:2.0.22-5.amzn2.0.5
Package manager	OS

Remediation

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

- yum update gnupg2

Vulnerability details

Vulnerability ID	CVE-2022-34903
Vulnerability source	REDHAT_CVE
Inspector Score	5.1
Inspector Scoring vector	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N
CVSS 3.1	6.5 (Source: NVD)
Scoring vector	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:L/A:N
CVSS 3.1	5.9 (Source: REDHAT_CVE)
Scoring vector	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N
CVSS 2.0	5.8 (Source: NVD)
Scoring vector	AV:N/AC:M/Au:N/C:P/I:P/A:N

Related vulnerabilities

No related vulnerabilities.

Resource affected

Resource ID	i-09b01a0dd43b58600
Type	AWS EC2 Instance
EC2 instance type	t3.medium
Platform	AMAZON_LINUX_2
VPC ID	vpc-029f8d652099f281f
Subnet ID	subnet-0f9b358412b471a6c
AMI	ami-089950bc622d39ed8
Launched at	September 11, 2022 2:09 PM (UTC+02:00)

CVE-2022-34903 - gnupg2  
Finding ID: arn:aws:inspector:eu-west-1:finding/6346c87d9e9889d1f351d820eb563324

A vulnerability was found in GnuPG. This issue occurs due to an escape detection loop at the write\_status\_text\_and\_buffer() function in g10/cpr.c. This flaw allows a malicious actor to bypass access control.

Finding details   Inspector Score

CVSS v3 (REDHAT\_CVE)   Inspector

5.9   5.1

The Inspector score is lower. Changed metrics: Attack Vector

CVSS score metrics

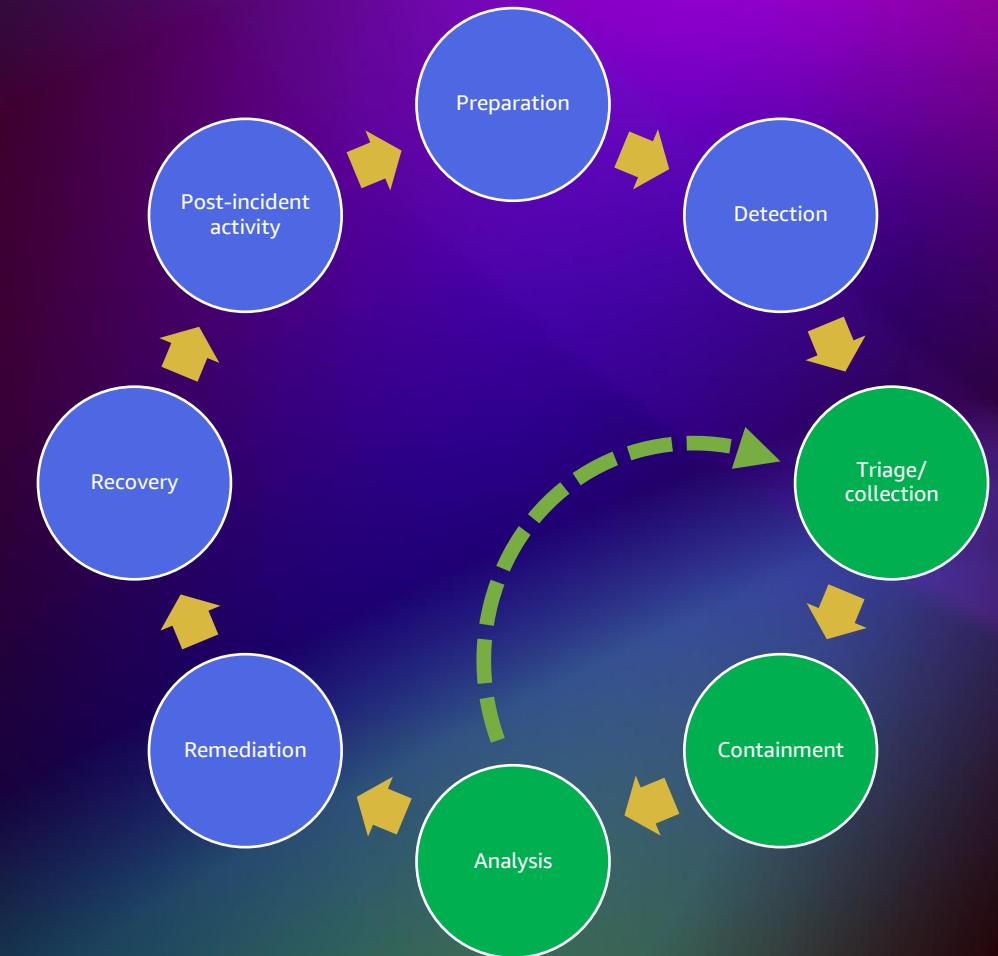
Metric	CVSS	Inspector
Attack Vector	Network	Network
Attack Complexity	High	High
Privileges Required	None	None
User Interaction	None	None
Scope	Unchanged	Unchanged
Confidentiality	None	None
Integrity	High	High
Availability	None	None

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

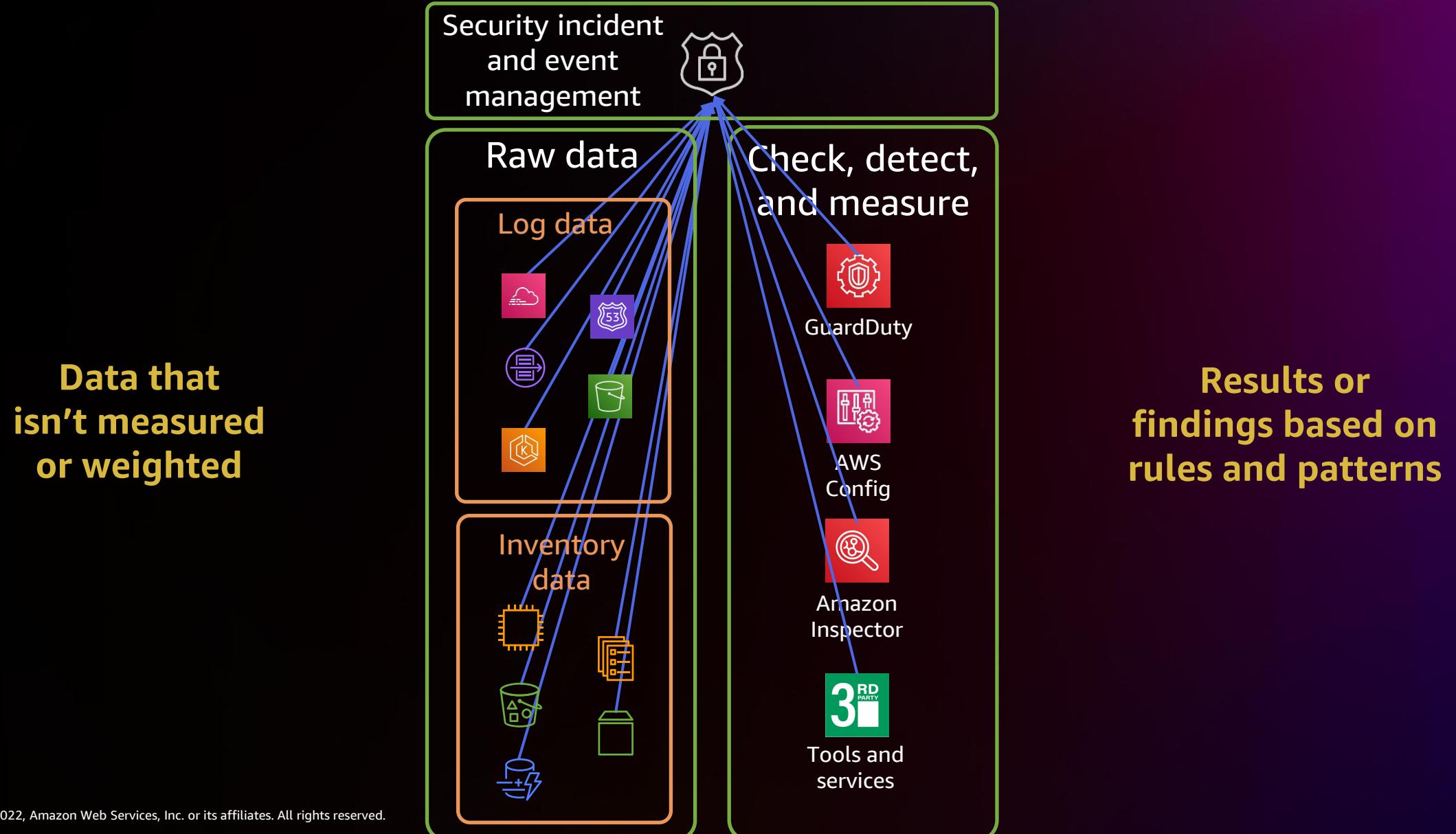
**Changes are based on the network reachability analysis**



# Collection Containment Analysis

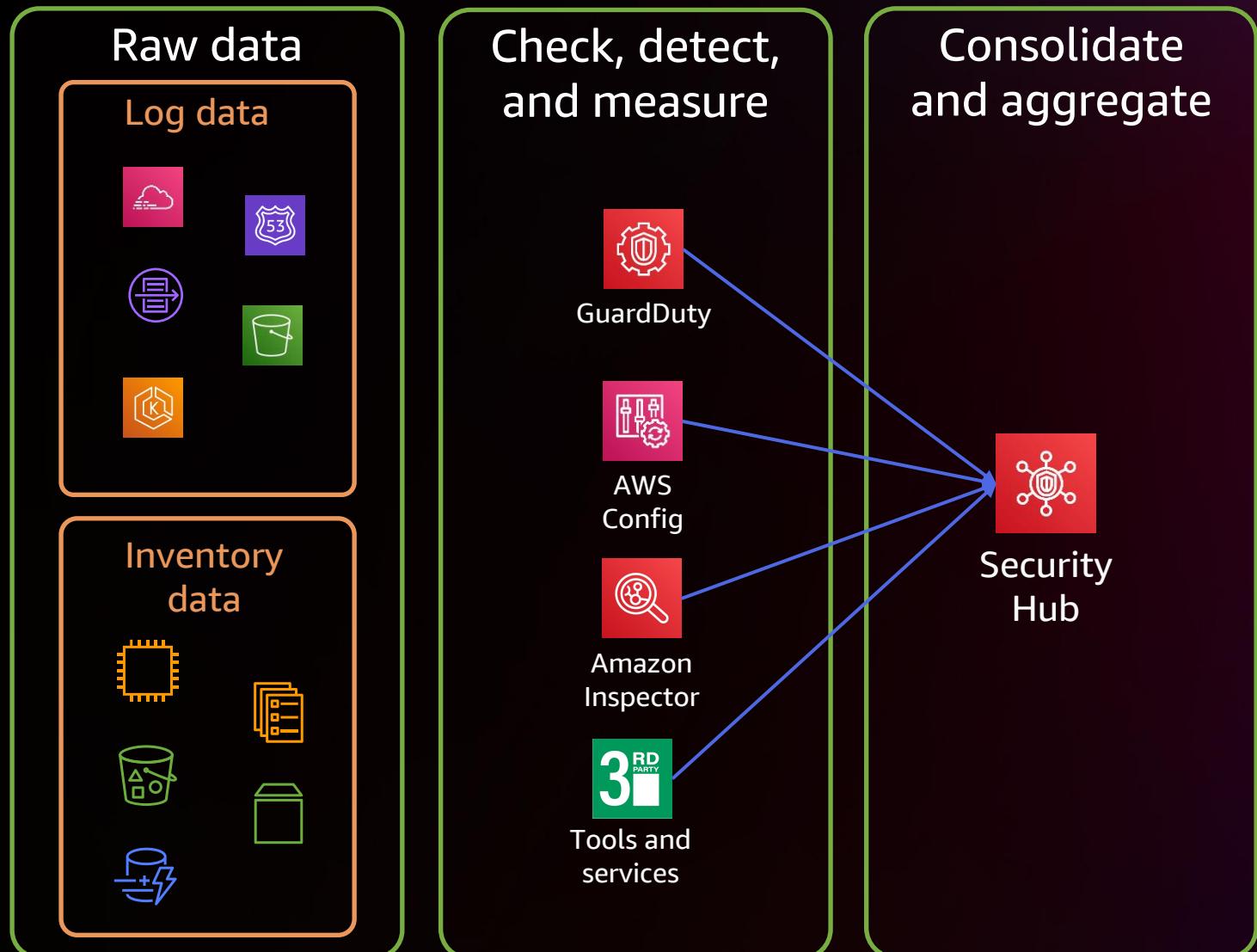


# Triage and collection – What do we have so far?



# 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

# Security Hub summary

Security Hub X Security standards

Summary Security standards Insights Findings Integrations Settings What's new

Resources with the most failed security checks

	Failed checks
arn:aws:s3::: [REDACTED]	12
arn:aws:s3::: [REDACTED]	12
arn:aws:es:eu-west-1:[REDACTED]:domain/[REDACTED]	11
arn:aws:s3:::secure-cabbage-[REDACTED]	11
arn:aws:s3:::athena-[REDACTED]	10

Standard Passed Failed Score ▲

Standard	Passed	Failed	Score
CIS AWS Foundations Benchmark v1.2.0	5	23	18%
CIS AWS Foundations Benchmark v1.4.0	8	19	30%
PCI DSS v3.2.1	24	20	55%
AWS Foundational Security Best Practices v1.0.0	104	71	59%

[View all standards](#)

**Findings by Region**

Findings from all linked Regions are visible from the aggregation Region.

Region	Critical	High	Medium	Low
Europe (Ireland) [Current Region]	125	1141	2588	598
Europe (Frankfurt)	7	9	69	24
US East (N. Virginia)	2	1	11	7

All linked Regions (6) Linked Regions with findings (3)

# Security Hub findings

Security Hub X

Summary  
Security standards  
**Insights**  
**Findings** Product name is GuardDuty X Workflow status is NEW X Workflow status is NOTIFIED X Record state is ACTIVE X Add filters

Settings  
What's new 4

<input type="checkbox"/>	Severity	Workflow status	Record State	Region	Account Id	Company	Product	Title	Resource
<input type="checkbox"/>	MEDIUM	NEW	ACTIVE	eu-west-1		Amazon	GuardDuty	Reconnaissance API ListInstanceAssociations was invoked from an IP address on a custom threat list.	EC2 Instance <a href="#">i-098f302ff7851db51</a>
<input type="checkbox"/>	MEDIUM	NEW	ACTIVE	eu-west-1		Amazon	GuardDuty	Reconnaissance API ListInstanceAssociations was invoked from an IP address on a custom threat list.	EC2 Instance <a href="#">i-098f302ff7851db51</a>
<input type="checkbox"/>	MEDIUM	NEW	ACTIVE	eu-west-1		Amazon	GuardDuty	Reconnaissance API ListInstanceAssociations was invoked from an IP address on a custom threat list.	EC2 Instance <a href="#">i-098f302ff7851db51</a>
<input type="checkbox"/>	MEDIUM	NEW	ACTIVE	eu-west-1		Amazon	GuardDuty	Reconnaissance API ListInstanceAssociations was invoked from an IP address on a custom threat list.	EC2 Instance <a href="#">i-098f302ff7851db51</a>
<input type="checkbox"/>	MEDIUM	NEW	ACTIVE	eu-west-1		Amazon	GuardDuty	Reconnaissance API ListInstanceAssociations was invoked from an IP address on a custom threat list.	EC2 Instance <a href="#">i-098f302ff7851db51</a>
<input type="checkbox"/>	HIGH	NEW	ACTIVE	eu-west-1		Amazon	GuardDuty	Data exfiltration through DNS queries from EC2 instance i-08d0c7a9c27319c16.	EC2 Instance <a href="#">i-08d0c7a9c27319c16</a>
<input type="checkbox"/>	MEDIUM	NEW	ACTIVE	eu-west-1		Amazon	GuardDuty	Reconnaissance API ListInstanceAssociations was invoked from an IP address on a custom threat list.	EC2 Instance <a href="#">i-098f302ff7851db51</a>
<input type="checkbox"/>	HIGH	NEW	ACTIVE	eu-west-1		Amazon	GuardDuty	Command and Control server domain name queried by EC2 instance i-08d0c7a9c27319c16.	EC2 Instance <a href="#">i-08d0c7a9c27319c16</a>
<input type="checkbox"/>	LOW	NEW	ACTIVE	eu-west-1		Amazon	GuardDuty	Amazon S3 Block Public Access was disabled for account.	IAM Access Key <a href="#">ASIAZ5I6V5OV2R7GLXI</a>
<input type="checkbox"/>	MEDIUM	NEW	ACTIVE	eu-west-1		Amazon	GuardDuty	Reconnaissance API ListInstanceAssociations was invoked from an IP address on a custom threat list.	EC2 Instance <a href="#">i-098f302ff7851db51</a>
<input type="checkbox"/>	MEDIUM	NEW	ACTIVE	eu-west-1		Amazon	GuardDuty	Reconnaissance API ListInstanceAssociations was invoked from an IP address on a custom threat list.	EC2 Instance <a href="#">i-098f302ff7851db51</a>
<input type="checkbox"/>	MEDIUM	NEW	ACTIVE	eu-west-1		Amazon	GuardDuty	EC2 instance i-08d0c7a9c27319c16 communicating with disallowed IP address.	EC2 Instance <a href="#">i-08d0c7a9c27319c16</a>
<input type="checkbox"/>	HIGH	NEW	ACTIVE	eu-west-1		Amazon	GuardDuty	2 security risk(s) detected including EICAR-Test-File (not a virus) on EC2 instance i-07a954a1fbcb76df2e.	EC2 Instance <a href="#">i-07a954a1fbcb76df2e</a>
<input type="checkbox"/>	HIGH	NEW	ACTIVE	eu-west-1		Amazon	GuardDuty	Command and Control server domain name queried by EC2 instance i-0569ee2fd39c70828.	EC2 Instance <a href="#">i-0569ee2fd39c70828</a>



# Security Hub finding details

Command and Control server domain name queried by EC2 instance i-0569ee2fd39c70828. X

Finding ID: arn:aws:guardduty:eu-west-1:detector/c2bc8ca87a1c16a25de44cd8a700d912/finding/66c1226d26db6adc7a231a31e11136d5

**HIGH**  
EC2 instance i-0569ee2fd39c70828 is querying a domain name associated with a known Command & Control server.

Workflow status	RECORD STATE
New	ACTIVE Set by the finding provider
AWS account ID	Severity (original)
	8 ⓘ
Created at	Updated at
2022-07-28T12:48:53.686Z ⓘ	2022-07-28T13:10:20.259Z ⓘ
Product name	Severity label
GuardDuty ⓘ	■ HIGH ⓘ
Company name	Source URL
Amazon ⓘ	<a href="https://eu-west-1.console.aws.amazon.com/guardduty/home?region=eu-west-1#/findings?macros=current&amp;fld=66c1226d26db6adc7a231a31e11136d5">https://eu-west-1.console.aws.amazon.com/guardduty/home?region=eu-west-1#/findings?macros=current&amp;fld=66c1226d26db6adc7a231a31e11136d5</a> ⓘ

► Types and Related Findings  
► Resources  
► Investigate in Amazon Detective  
► Finding Provider Fields

▼ Types and Related Findings

Types

TTPs/Command and Control/Backdoor:EC2-C&CActivity.B!DNS

▼ Resources

Resources detail

arn:aws:ec2:eu-west-1:instance/i-0569ee2fd39c70828

Resource type	Resource region
AwsEc2Instance ⓘ	eu-west-1 ⓘ
Resource ID	EC2 instance type
arn:aws:ec2:eu-west-1:instance/i-0569ee2fd39c70828 ⓘ	t2.large ⓘ
EC2 instance image ID	EC2 instance subnet ID
ami-01efa4023f0f3a042 ⓘ	subnet-07007d1b8f78af20 ⓘ
EC2 instance launched at	
2022-07-28T11:42:31.000Z ⓘ	

► Investigate in Amazon Detective

▼ Finding Provider Fields

Finding Provider Fields detail

Finding Provider Field

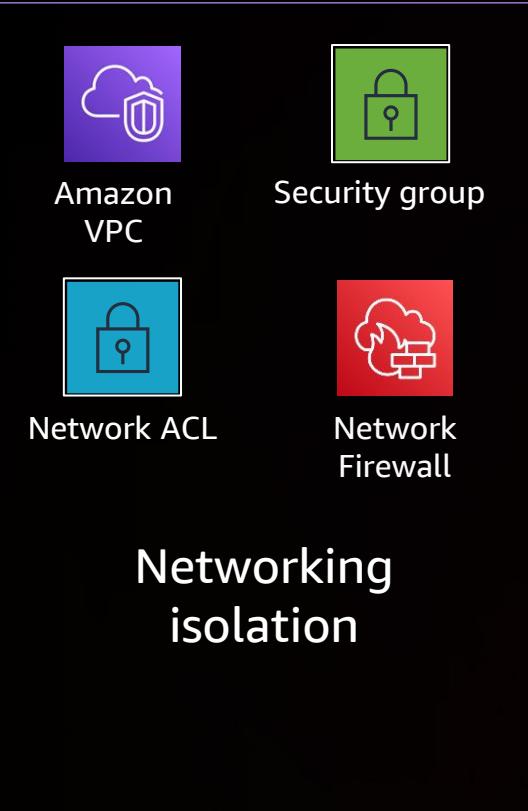
Provider severity label

■ HIGH ⓘ

Types

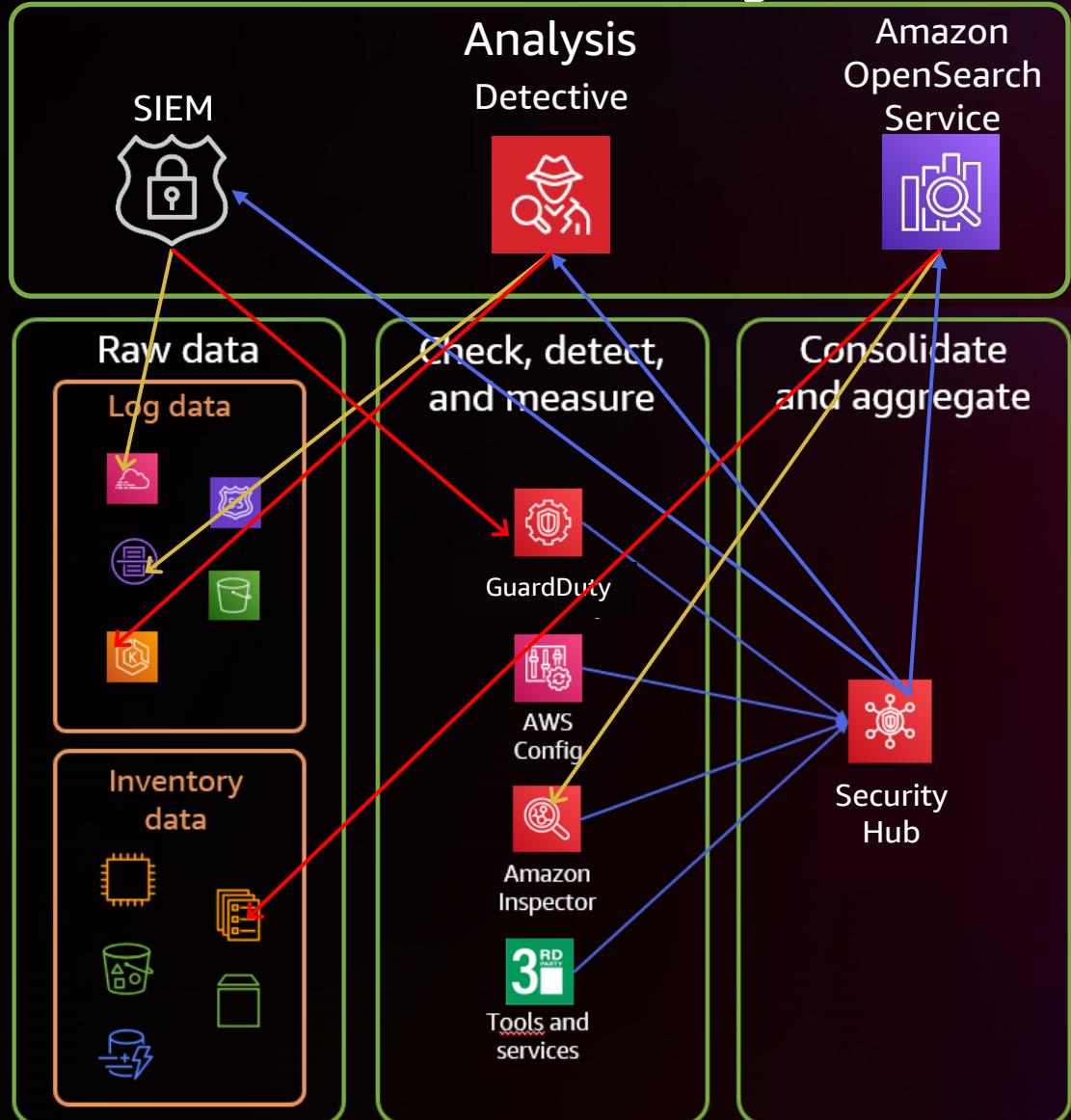
TTPs/Command and Control/Backdoor:EC2-C&CActivity.B!DNS

# Continuous containment in the cloud



# 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

# Investigate using Detective

**Security Hub** X

Summary  
Security standards

Insights  
**Findings**

Integrations

Settings

What's new 4

Severity	Status	Type	Last Seen	Region	Provider	Service	Description
MEDIUM	NEW	ACTIVE	eu-west-1	Amazon	GuardDuty	ListInstanceAssociations was invoked from an IP address on a custom threat list.	
MEDIUM	NEW	ACTIVE	eu-west-1	Amazon	GuardDuty	Reconnaissance API ListInstanceAssociations was invoked from an IP address on a custom threat list.	
MEDIUM	NEW	ACTIVE	eu-west-1	Amazon	GuardDuty	Reconnaissance API ListInstanceAssociations was invoked from an IP address on a custom threat list.	
MEDIUM	NEW	ACTIVE	eu-west-1	Amazon	GuardDuty	Reconnaissance API ListInstanceAssociations was invoked from an IP address on a custom threat list.	
HIGH	NEW	ACTIVE	eu-west-1	Amazon	GuardDuty	Data exfiltration through DNS queries from EC2 instance i-08d0c7a9c27319c16.	
MEDIUM	NEW	ACTIVE	eu-west-1	Amazon	GuardDuty	Reconnaissance API ListInstanceAssociations was invoked from an IP address on a custom threat list.	
HIGH	NEW	ACTIVE	eu-west-1	Amazon	GuardDuty	Command and Control server domain name queried by EC2 instance i-08d0c7a9c27319c16.	
LOW	NEW	ACTIVE	eu-west-1	Amazon	GuardDuty	Amazon S3 Block Public Access was disabled for account.	
MEDIUM	NEW	ACTIVE	eu-west-1	Amazon	GuardDuty	Reconnaissance API ListInstanceAssociations was invoked from an IP address on a custom threat list.	
MEDIUM	NEW	ACTIVE	eu-west-1	Amazon	GuardDuty	Reconnaissance API ListInstanceAssociations was invoked from an IP address on a custom threat list.	

**Command and Control server domain name queried by EC2 instance i-0569ee2fd39c70828.** X

Finding ID: arn:aws:guardduty:eu-west-1: :detector/c2bc8ca87a1c16a25de44cd8a700d912 /finding/66c1226d26db6adc7a231a31e11136d5

**HIGH**  
EC2 instance i-0569ee2fd39c70828 is querying a domain name associated with a known Command & Control server.

Workflow status: New RECORD STATE: ACTIVE Set by the finding provider

AWS account ID: [REDACTED] Severity (original): 8

Created at: 2022-07-28T12:48:53.686Z Updated at: 2022-07-28T13:10:20.259Z

Product name: GuardDuty Severity label: HIGH

Company name: Amazon Source URL: https://eu-west-1.console.aws.amazon.com/guardduty/home?region=eu-west-1#/findings?macros=current&31e11136d5

► Types and Related Findings  
► Resources  
▼ Investigate in Amazon Detective  
Investigate finding  
► Finding Provider Fields



# Investigate using Detective

Detective X

Summary  
Search

Settings

Account management  
General  
Preferences  
Usage

What's new 19

Getting started  
Video tutorials

Detective > Search > GuardDuty/66c1226d26db6adc7a231a31e11136d5

Scope time Info  
07/28/2022, 11:00 UTC > 07/28/2022, 12:00 UTC Edit

**Entities related to GuardDuty finding 66c1226d26db6adc7a231a31e11136d5**

Filter by type, name, or ID

<p><span style="color: #0070C0;">📍</span> 10.200.0.119 IP address</p> <p>First observed: 01/26/2022, 09:13 UTC Last observed: 09/02/2022, 14:05 UTC Last observed location: -</p> <p>Total times observed: - Distinct AWS users and roles: - Count of related user agents: -</p> <p><span style="border: 1px solid #ccc; padding: 2px;">See profile</span></p>	<p><span style="color: #0070C0;">🔒</span> AWS account</p> <p>No attributes available for this entity</p> <p><span style="border: 1px solid #ccc; padding: 2px;">See profile</span></p>
<p><span style="color: #0070C0;">📍</span> 63.32.149.69 IP address</p> <p>First observed: 01/26/2022, 09:48 UTC Last observed: 09/02/2022, 14:02 UTC Last observed location: -</p> <p>Total times observed: 4,890 Distinct AWS users and roles: 1 Count of related user agents: 200</p> <p><span style="border: 1px solid #ccc; padding: 2px;">See profile</span></p>	<p><span style="color: #0070C0;">chip</span> i-0569ee2fd39c70828 EC2 instance</p> <p>EC2 instance: i-0569ee2fd39c70828 <span style="border: 1px solid #ccc; padding: 2px;">Edit</span></p> <p>AWS account: <span style="background-color: #f0f0f0; border: 1px solid #ccc; padding: 2px;">[REDACTED]</span></p> <p>Node: - ARN: arn:aws:ec2:eu-west-1:<span style="background-color: #f0f0f0; border: 1px solid #ccc; padding: 2px;">[REDACTED]</span>:instance/i-0569ee2fd39c70828 Associated VPC: vpc-00c903a9c05c00692 EKS cluster: -</p> <p>Creation date: 01/26/2022, 09:13 UTC Created by: AWSReservedSSO_Administrator Role: EC2-PROWLER-WITH-SSM</p> <p><span style="border: 1px solid #ccc; padding: 2px;">See profile</span></p>

⚙️ Command and Control server domain name queried by EC2 instance i-0569ee2fd39c70828.

Backdoor:EC2/C&CActivity.B!DNS Info

Finding ID: 66c1226d26db6adc7a231a31e11136d5 Edit

Archive finding

EC2 instance i-0569ee2fd39c70828 is querying a domain name associated with a known Command & Control server.

**Overview**

Severity	High
Count	2
Account ID	<span style="background-color: #f0f0f0; border: 1px solid #ccc; padding: 2px;">[REDACTED]</span>
Resource ID	i-0569ee2fd39c70828
Created at	07/28/2022, 12:48 UTC (2 months ago)
Updated at	07/28/2022, 13:10 UTC (2 months ago)

**Resource affected**

Resource role	TARGET
Resource type	Instance
Instance ID	i-0569ee2fd39c70828
Instance type	t2.large
Instance state	running
Availability zone	eu-west-1c
Image ID	ami-01efa4023f0f3a042
Image description	Amazon Linux 2 Kernel 5.10 AMI 2.0.20211223.0 x...
Launch time	07/28/2022, 11:42 UTC

**Iam instance profile**

ARN	arn:aws:iam: <span style="background-color: #f0f0f0; border: 1px solid #ccc; padding: 2px;">[REDACTED]</span> :instance-profile/EC2-...
ID	AIPATRKNUAWV4XISVEGFA

**Tags**

Name	PROWLER-SEC-TOOLING
------	---------------------



# Investigate using Detective

i-0569ee2fd39c70828  
EC2 instance [Info](#)

Scope time [Info](#)  
07/28/2022, 11:00 UTC > 07/28/2022, 12:00 UTC [Edit](#)

Title	AWS account	Finding type	First observed	Last observed	Finding severity
Command and Control server domain name queried by EC2 instance i-0569ee2fd39c70828.	[REDACTED]	Backdoor:EC2/C&CActivity.B!DNS	07/28/2022, 11:51 UTC	07/28/2022, 11:51 UTC	High

Activity for time window: 07/28/2022, 11:00 UTC - 07/28/2022, 12:00 UTC

[Toggle overall traffic](#) [Edit time window](#)

IP address	Local port	Remote port	Inbound traffic	Outbound traffic	Protocol	Directionality	Accept / Reject	Annotations
106.12.222.241	6379	-	60 B	0 B	TCP	Inbound	Reject	
106.52.164.90	6379	-	60 B	0 B	TCP	Inbound	Reject	
113.254.103.178	5555	-	40 B	0 B	TCP	Inbound	Reject	
116.73.119.250	23	-	40 B	0 B	TCP	Inbound	Reject	
121.234.179.11	23	-	40 B	0 B	TCP	Inbound	Reject	
122.11.139.65	23	-	40 B	0 B	TCP	Inbound	Reject	
123.160.221.4	8829	-	52 B	0 B	TCP	Inbound	Reject	
123.160.221.6	8187	-	52 B	0 B	TCP	Inbound	Reject	
137.184.222.195	44140	-	40 B	0 B	TCP	Inbound	Reject	
138.199.32.102	139	-	40 B	0 B	TCP	Inbound	Reject	

[Linear](#) [Log](#)

07/28/2022, 11:00 - 07/28/2022, 12:00

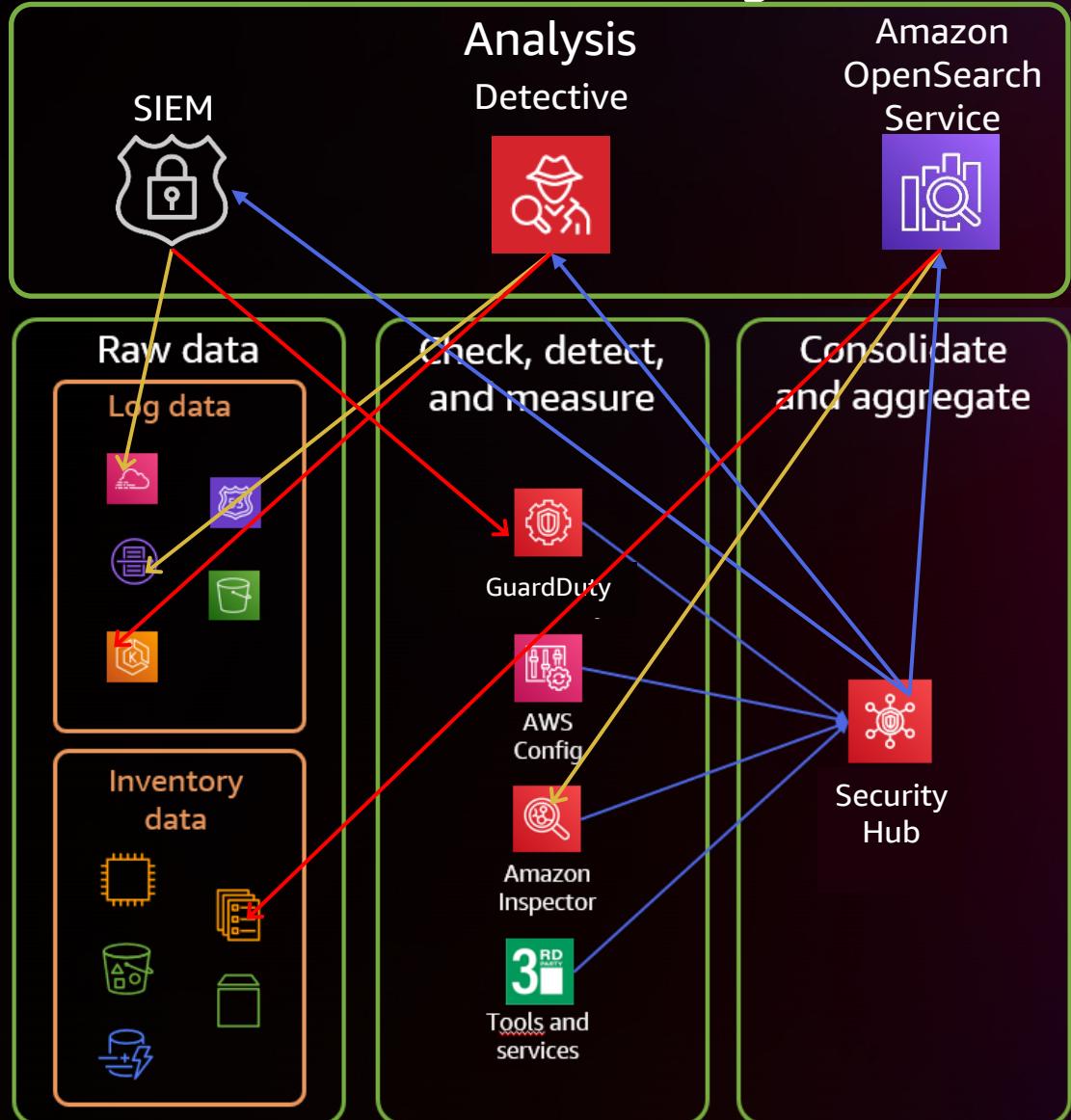
07/28/2022, 11:00 - 07/28/2022, 12:00

07/28/2022, 11:00 - 07/28/2022, 12:00



# If we need to do further analysis

In both cases this analysis is typically targeted to specific sources



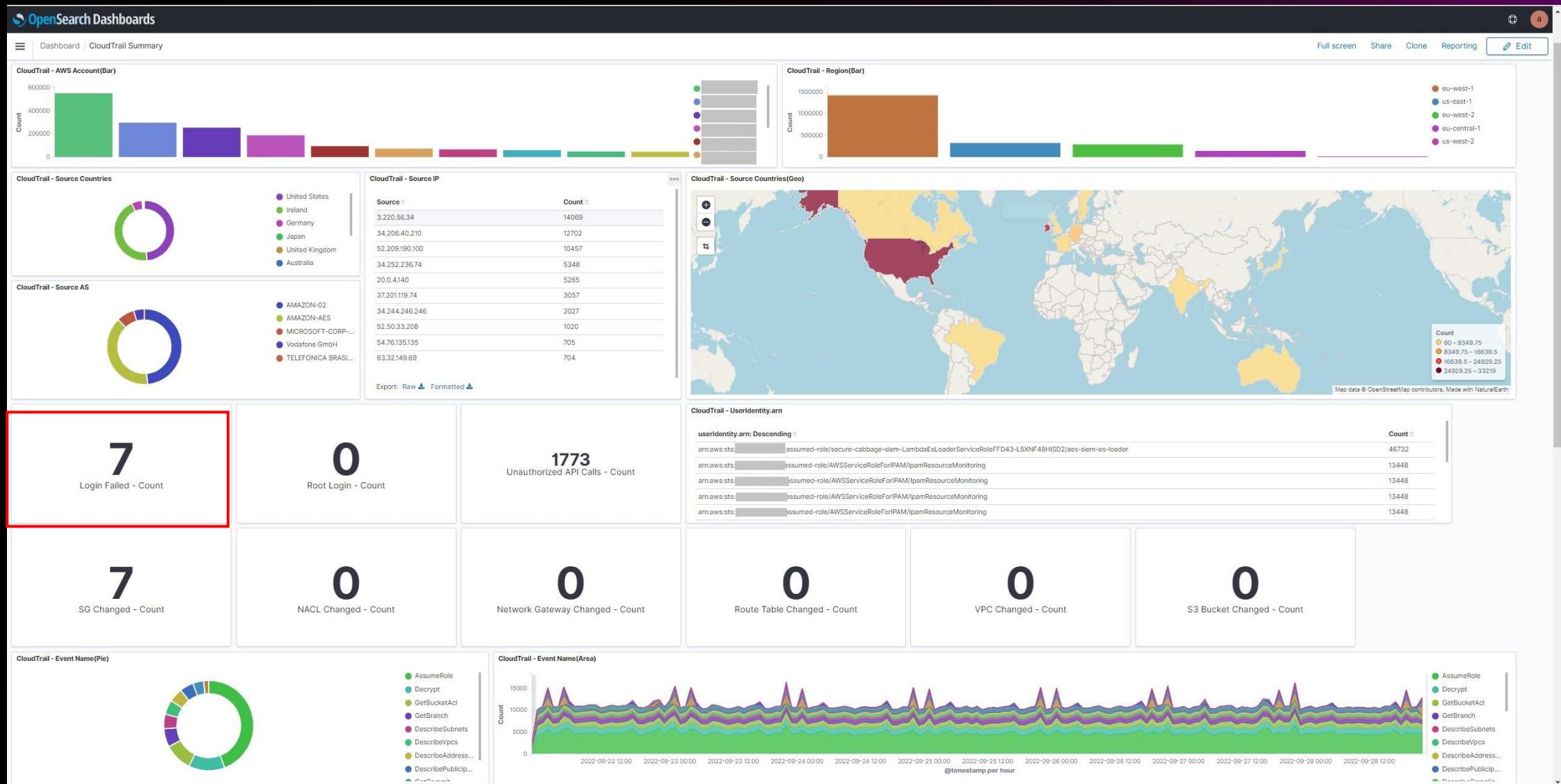
**From an existing finding:**

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

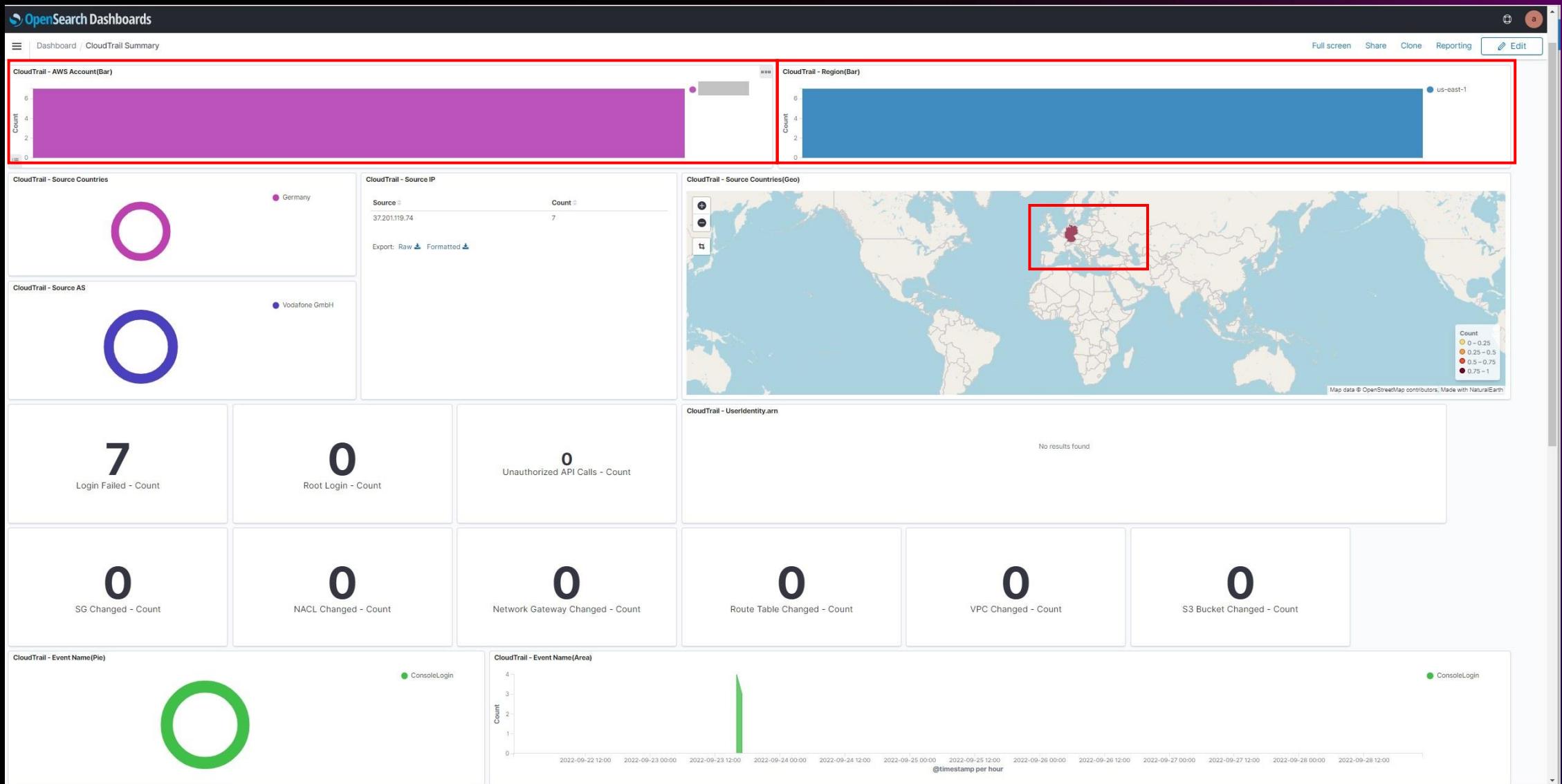
**Without an existing finding:**

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

# Investigate using OpenSearch Service



# Investigate using OpenSearch Service



# Investigate using OpenSearch Service

Time	cloud.account.id	cloud.region	eventName	user.name	eventSource
> 09/23 17:10:53	[REDACTED]	us-east-1	ConsoleLogin	DemoAdmin	signin.amazonaws.com
> 09/23 17:10:49	[REDACTED]	us-east-1	ConsoleLogin	DemoAdmin	signin.amazonaws.com
search - CloudTrail					
<pre># _id          06c3c6ce-82ac-45ee-b8b7-072c21e36718 # _index       log-aws-cloudtrail-2022-09 # _score        - # _type         _doc # additionalEventData.LoginTo https://us-east-1.console.aws.amazon.com/console/home?hashArgs=%23&amp;isAuthCode=true&amp;nc2=h_ct&amp;region=us-east-1&amp;skipRegion=true&amp;src=header-signin&amp;state=hashArgsFromTB_us-east-1_805c6fb04047a99f # additionalEventData.MFAUsed No # additionalEventData.MobileVersion No # awsRegion    us-east-1 # cloud.account.id [REDACTED] # cloud.provider aws # cloud.region   us-east-1 # ecs.version   1.10.0 # error.message Failed authentication # errorMessage  Failed authentication # event.action   ConsoleLogin # event.category iam # event.ingested 09/23 17:15:04 # event.kind     event # event.module   signin.amazonaws.com # event.outcome  failure # eventCategory Management # eventID        06c3c6ce-82ac-45ee-b8b7-072c21e36718 # eventName      ConsoleLogin # eventSource    signin.amazonaws.com # eventTime      09/23 17:10:49 # eventType      AwsConsoleSignIn # eventVersion   1.08 # managementEvent true # readOnly       false # recipientAccountId [REDACTED] # related.ip    37.201.119.74</pre>					



# Remediation

# Recovery

# Post-incident activity





# Challenges



Auditors and  
regulators

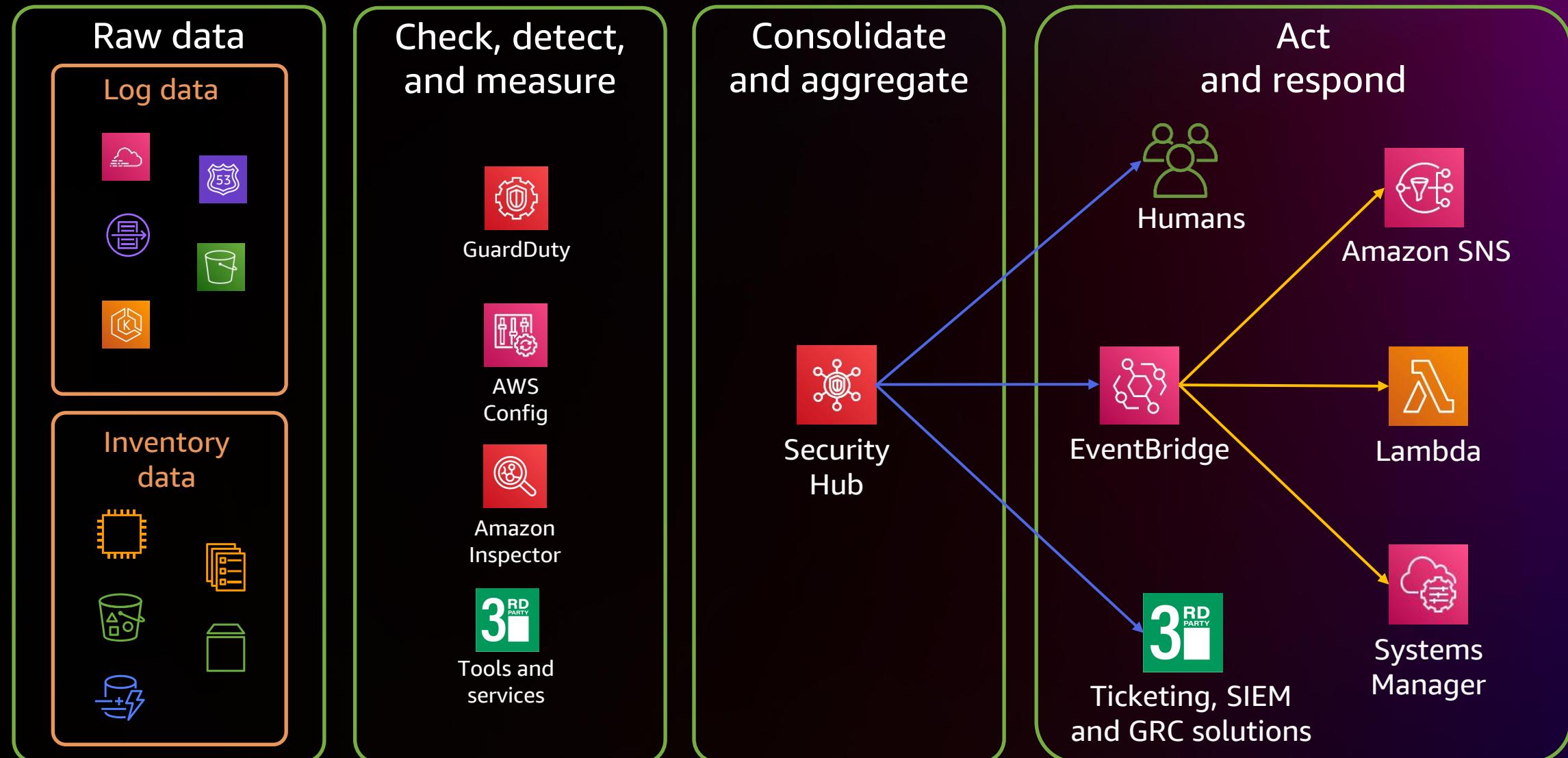


Customers



“What happened?  
At what time?”

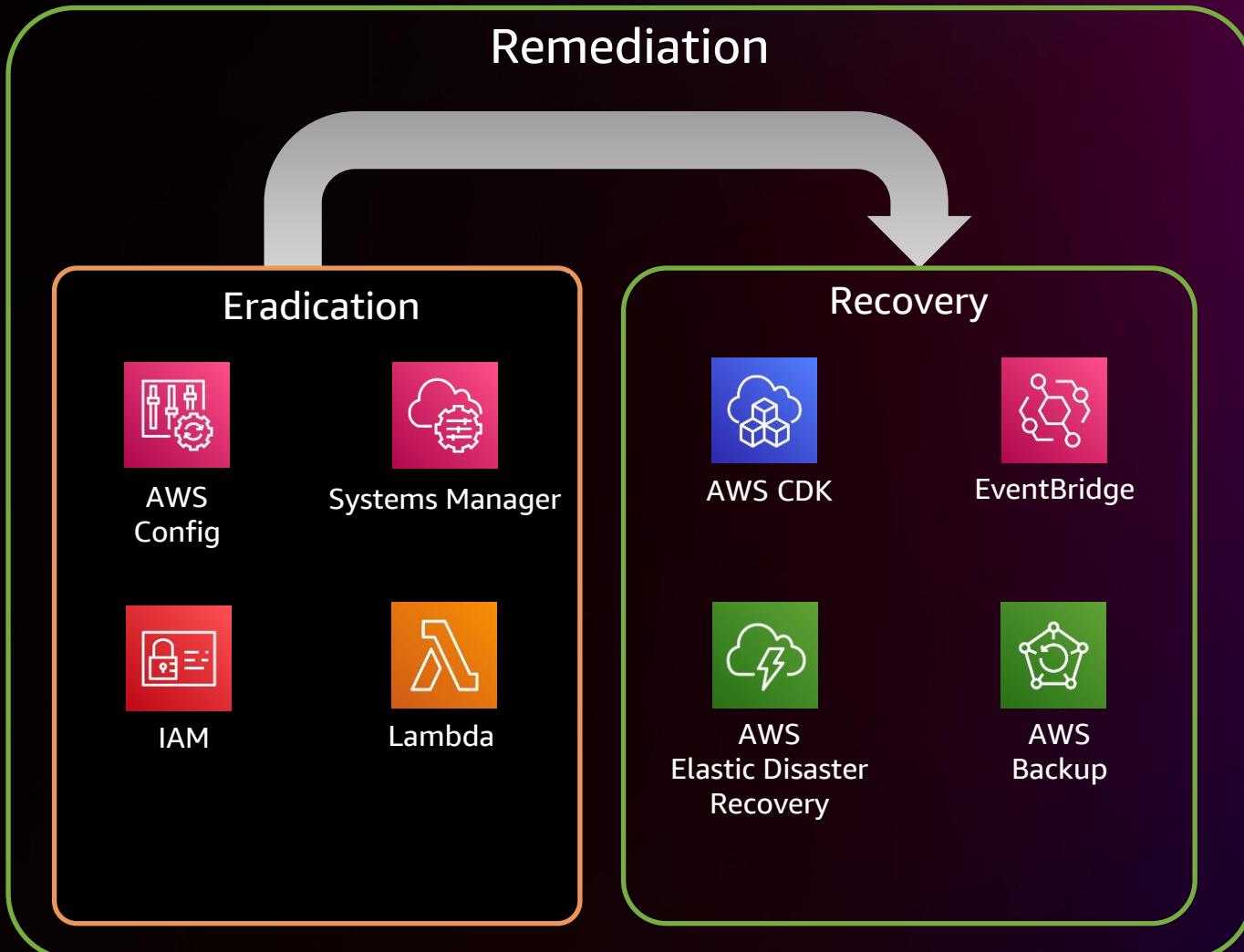
# How AWS Security Hub can trigger actions



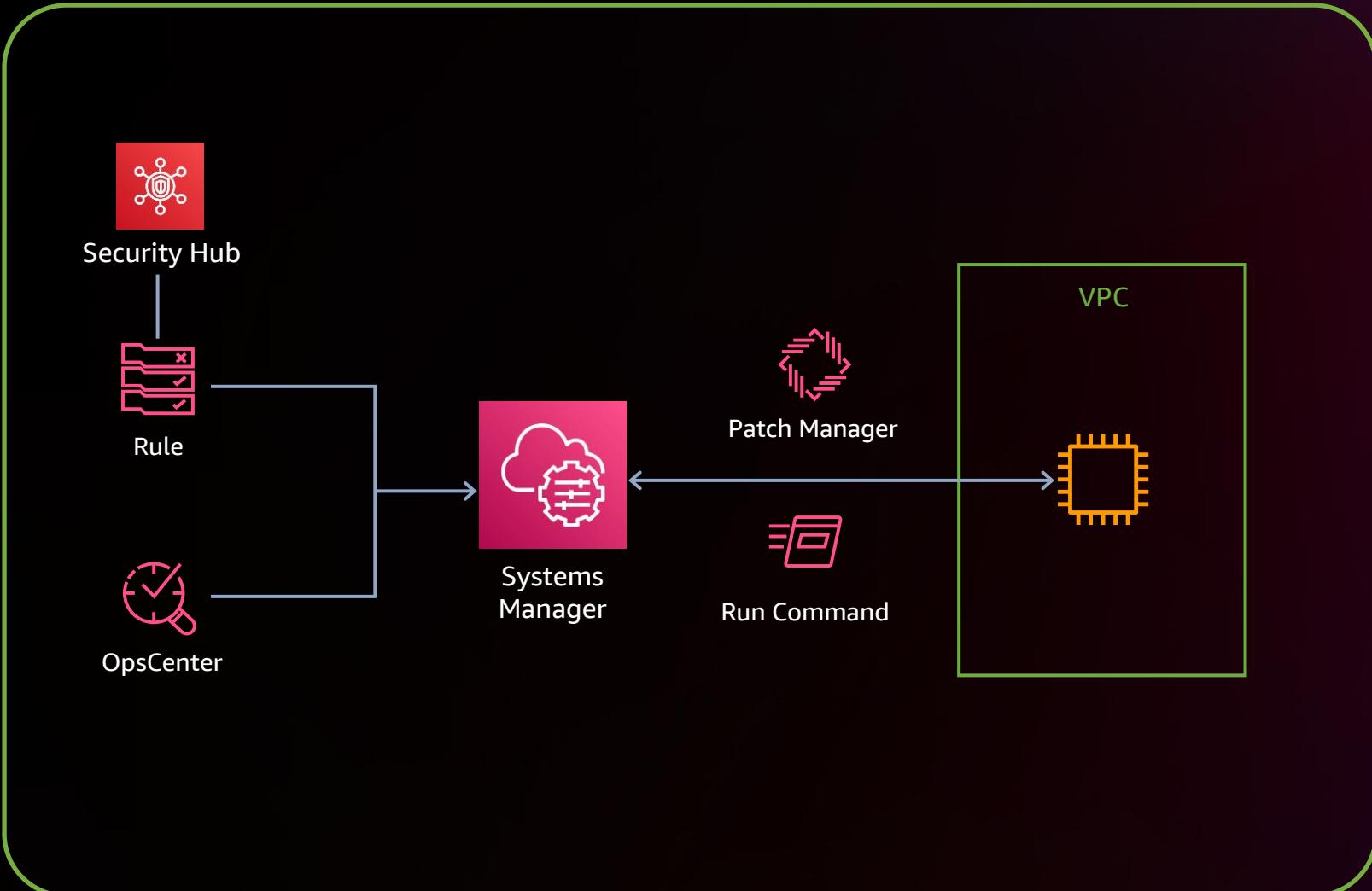
# Remediation and Recovery

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

NIST 800-61



# 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**

# Systems Manager

AWS Systems Manager X

Quick Setup

Operations Management

- Explorer (selected)
- OpsCenter
- CloudWatch Dashboard
- Incident Manager

Application Management

- Application Manager
- AppConfig
- Parameter Store

Change Management

- Change Manager
- Automation
- Change Calendar
- Maintenance Windows

Node Management

- Fleet Manager
- Compliance
- Inventory
- Hybrid Activations
- Session Manager
- Run Command
- State Manager
- Patch Manager
- Distributor

## Explorer

OpsData Filter

Select a resource data sync ▾ Region ▾

Filter by OpsItem source, tag keys, or tag values

Search:

OpsItem by status

Actions ▾
277 Unresolved
277 Open

Non-compliant instances for patching

Under 15 days: Total non-compliant resources: 4 Critical non-compliant resources: 0

15-90 days: Total non-compliant resources: 0 Critical non-compliant resources: 0

Over 90 days: Total non-compliant resources: 0 Critical non-compliant resources: 0

Desired state compliance status

Compliance status of Quick Setup associations.

Association name	Total compliant resources	Total non-compliant resources	Compliance percentage
AWS-QuickSetup-SSMHostMgmt-ScanForPatches-tzrpw	1	5	⚠️ 17%
AWS-QuickSetup-SSMHostMgmt-CollectInventory-tzrpw	6	0	✅ 100%
AWS-QuickSetup-SSMHostMgmt-UpdateSSMAgent-tzrpw	6	0	✅ 100%
AWS-PatchNowAssociation	5	0	✅ 100%

OpsItem by severity

Critical	High	Medium
18	259	0
Low	Unspecified	0



# Patch Manager

AWS Systems Manager X

AWS Systems Manager > Patch Manager

## Patch Manager

Dashboard | Compliance reporting | Patch baselines | Patches | Patch groups | Settings

**Configure patching** **Patch now**

**Amazon EC2 instance management**  
Snapshot of EC2 instances in your AWS account that are and are not managed by Systems Manager.

**Reporting not enabled**  
To view the EC2 instance snapshot, enable the Amazon EC2 OpsData source in Explorer and set up recording in AWS Config. [Learn more](#)

[Enable Explorer](#)

**Compliance summary**  
Summary of compliance status for managed nodes that have previously reported patch data.



Compliant: 1 | Critical noncompliant: 0  
High noncompliant: 0 | Other noncompliant: 4

**Noncompliance counts**  
The number of noncompliant nodes for each of the most common reasons for being out of compliance.

Nodes with missing patches	4
Nodes with failed patches	0
Nodes pending reboot	0

**Compliance reports**  
Count of instances based on the age of their most recent patching compliance reports.



Compliance reported within the past 7 days: 4  
Compliance not reported within the past 7 days: 0  
Compliance never reported: 0

**Patch operations history (4)**  
This summary of recent patching operations indicates whether an operation was started manually, or started by a maintenance window or State Manager association. Choose an operation link to view the command output.

Patch operation	Started by	Document name	End time	Status	Targets
Scan	Association	AWS-RunPatchBaseline	September 22, 2022 at 5:07 PM GMT+2	Success	Instanceids: *
Scan	Association	AWS-RunPatchBaselineAssociation	September 22, 2022 at 5:04 PM GMT+2	Success	Instanceids: 4
Scan	Association	AWS-RunPatchBaselineAssociation	September 19, 2022 at 3:47 PM GMT+2	Success	Instanceids: i-08d0c7a9c27319c16
Scan	Association	AWS-RunPatchBaselineAssociation	September 19, 2022 at 9:41 AM GMT+2	Success	Instanceids: i-08d0c7a9c27319c16

**Recurring patching tasks (2)**  
The following is a list of State Manager associations and maintenance windows that run any patching-related task. Choose a task name to view its details.



# Patch Manager

AWS Systems Manager   X

AWS Systems Manager > Patch Manager > Patch now

**New Features**  
We listened to your concerns and now we provide a way to orchestrate complex patch operations in a way that does not compromise your fleet's availability. The Patch Lifecycle Hooks feature is available under advanced options below.

**Patch instances now** Info

**Basic configuration**  
Scan for missing patches or install patches, with or without rebooting. For more patching options, use the [Configure patching](#) page.

**Patching operation**

Scan  
 Scan and install

**Reboot option**  
Specify whether Patch Manager should reboot your instances, or reboot on a schedule

Reboot if needed  
 Do not reboot my instances  
 Schedule a reboot time New

**Instances to patch**  
Choose whether to patch all instances or only the instances you specify

Patch all instances  
 Patch only the target instances I specify

**Target selection**  
Choose a method for selecting targets.

Specify instance tags  
Specify one or more tag key-value pairs to select instances that share those tags.

Choose instances manually  
Manually select the instances you want to register as targets.

Choose a resource group  
Choose a resource group that includes the resources you want to target.

**Specify instance tags**  
Specify one or more instance tag key-value pairs to identify the instances where the tasks will run.

Task  Incident Remediation

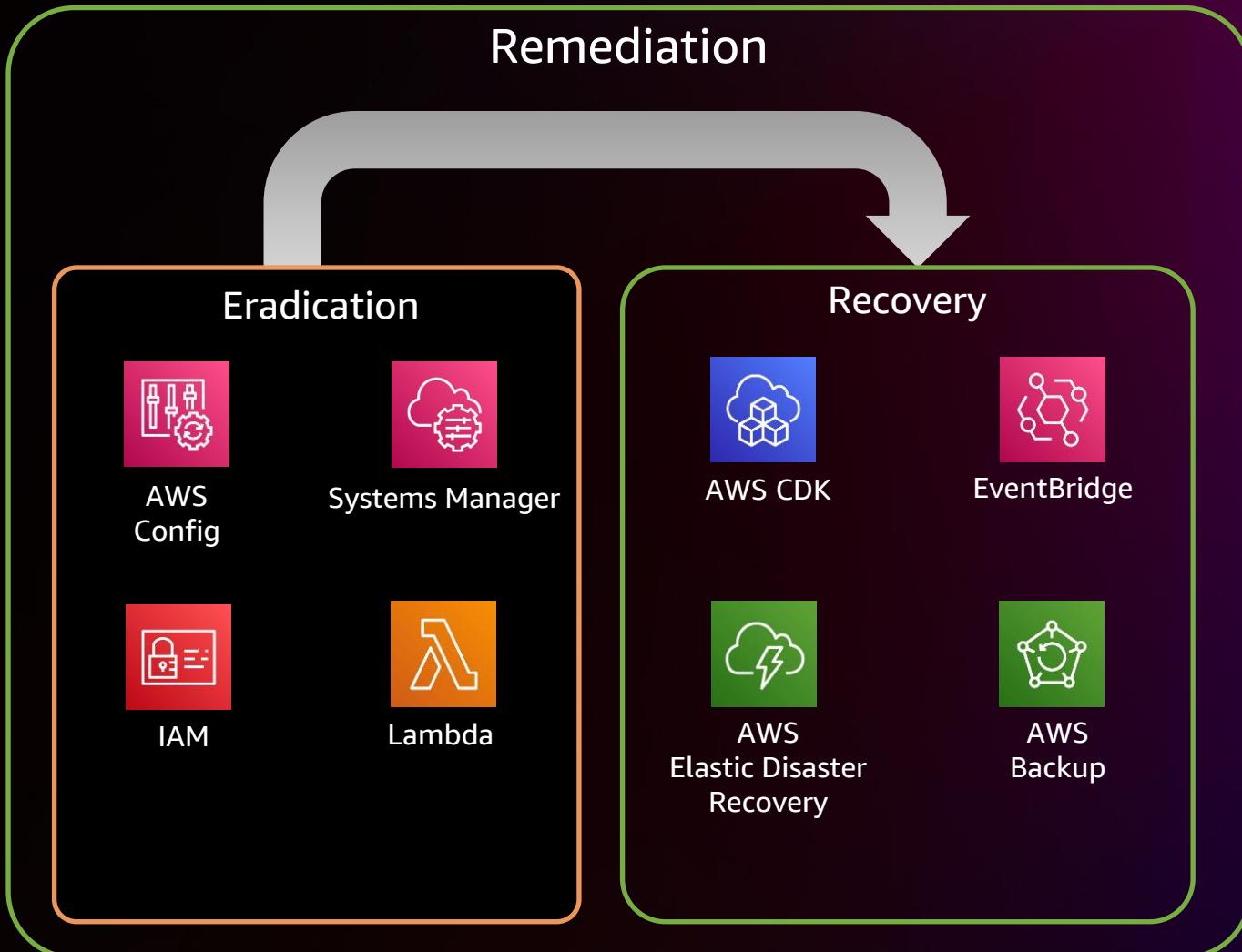
**Patching log storage** New  
Select or create an S3 bucket for storing patching operation logs. Select **Do not store logs** if you don't require log information.



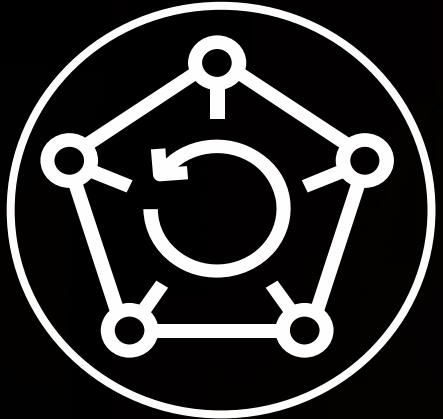
# Remediation and Recovery

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

NIST 800-61



# AWS Backup

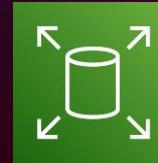


AWS Backup

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



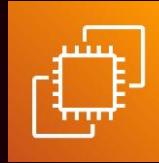
Amazon RDS



Amazon EBS



Amazon EFS



Amazon EC2



AWS Storage  
Gateway



Amazon DynamoDB



Amazon FSx  
for Lustre

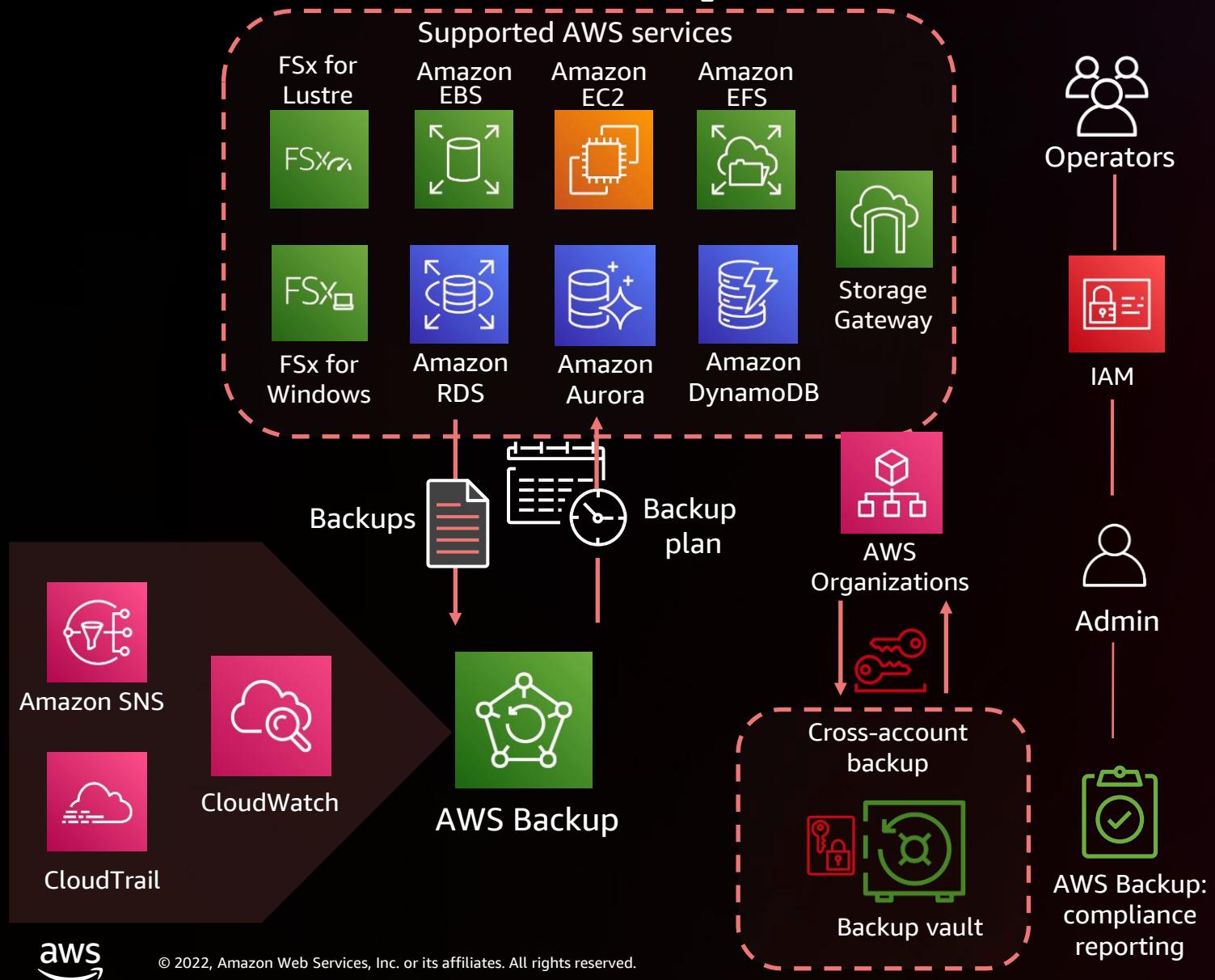


Amazon FSx for  
Windows File Server



Amazon Aurora

# How AWS Backup works



## Automate the restore processes

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

- AWS CDK
- AWS CloudFormation

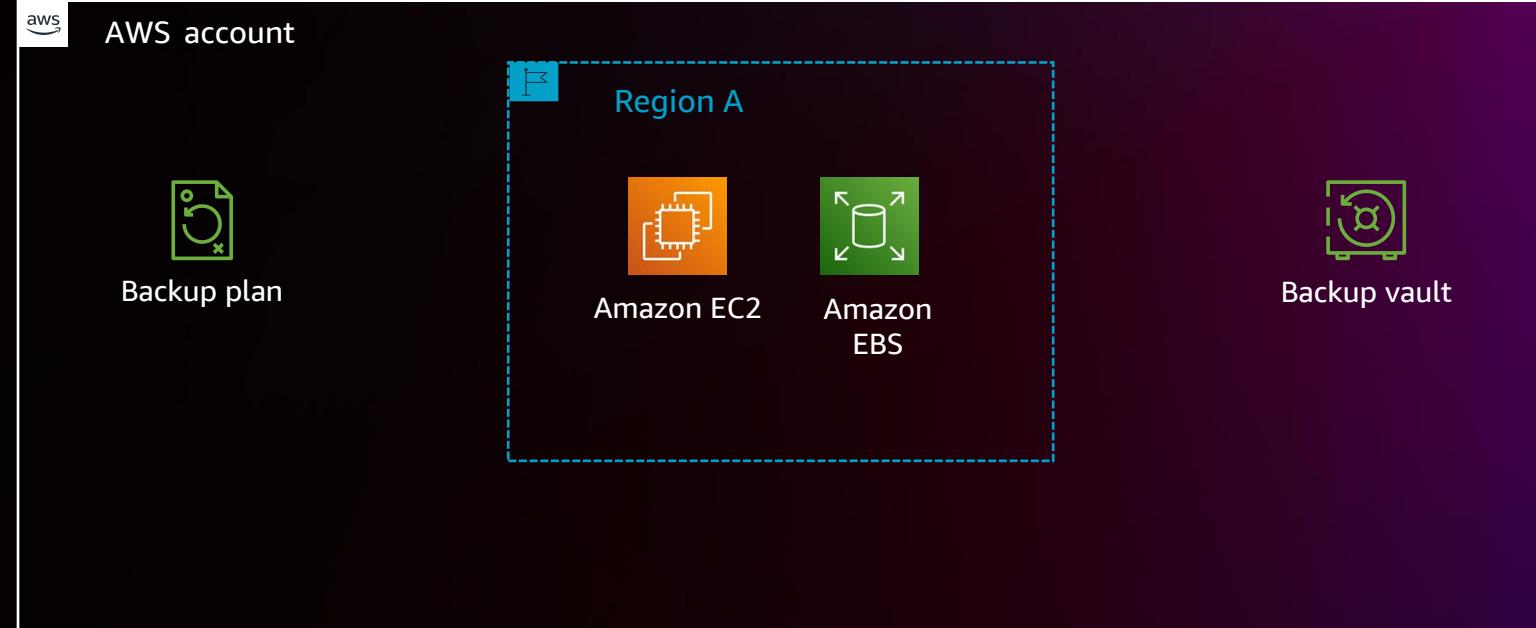
Or third-party services like Terraform

## Scale through AWS Organizations

Automate backups across accounts and organizational units

Restrict access to backup plans

# AWS Backup – Cross-account and cross-Region



**Protecting prepared environments against account compromise**



# AWS Backup

AWS Backup < X AWS Backup > Backup vaults > bronze ⓘ

bronze

Manage vault lock Delete vault Edit access policy

Summary

Backup vault name: bronze Creation date: October 18, 2022, 17:11:35 (UTC+02:00) KMS encryption key ID: c727821f-6677- [copy]

Backup vault ARN: arn:aws:backup:eu-central-1: [copy]

Vault lock: -

Recovery points (1140)

Filter by resource type, recovery point ID, status, resource ID or source account ID

Recovery point ID	Status	Resource ID	Resource type	Backup type	Creation time	Source account ID
image/ami-022e095607279c61e	Completed	instance/i-060	EC2	Image	November 15, 2022, 08:00:00 (UTC+01:00)	005
snapshot/snap-083e1b6615c988e12	Completed	volume/vol-0f	EBS	Snapshot	November 15, 2022, 08:00:00 (UTC+01:00)	005
image/ami-0fea7dfca34518d14	Completed	instance/i-012	EC2	Image	November 15, 2022, 08:00:00 (UTC+01:00)	005
image/ami-0dd360df9e3130782	Completed	instance/i-0fce	EC2	Image	November 15, 2022, 08:00:00 (UTC+01:00)	005
snapshot/snap-0629fe0e94d1b15dc	Completed	volume/vol-04	EBS	Snapshot	November 15, 2022, 08:00:00 (UTC+01:00)	005
snapshot/snap-0f3e621fbb4fd650b	Completed	volume/vol-0b	EBS	Snapshot	November 15, 2022, 08:00:00 (UTC+01:00)	005
image/ami-0093815ffb1e3078	Completed	instance/i-012	EC2	Image	November 15, 2022, 07:00:00 (UTC+01:00)	005
image/ami-08cf492fc2359a31e	Completed	instance/i-0fce	EC2	Image	November 15, 2022, 07:00:00 (UTC+01:00)	005

# AWS Backup – Backup plan

AWS Backup X AWS Backup > Backup plans > bronze-plan

## bronze-plan

**Global backup plan**  
Backup plans created from AWS Organizations policies are not allowed to be deleted or edited.

### Summary

Backup plan name	Version ID	Last modified	Last runtime
bronze-plan	YTk4Y2ZjY2ltZjNmMC00MzIzLWE3NjEtZWVhODNkMjk1NDFk	November 6, 2022, 16:32:12 (UTC+01:00)	November 15, 2022, 09:01:01 (UTC+01:00)

### Backup rules (1)

Backup rules specify the backup schedule, backup window, and lifecycle rules.

**Allow Backup vault access**  
The Backup rule "bronze-rule" contains a copy rule to another account. You can allow access to your vault when editing the rule.

Name	Backup vault	Destination Backup vault
bronze-rule	bronze	bronze

### Resource assignments (1)

Resource assignments specify which resources will be backed up by this Backup plan.

Name	IAM role ARN	Creation time
bronze-resource-assignment	arn:aws:iam:::role/backup-role	November 6, 2022, 16:32:12 (UTC+01:00)



# AWS Backup – Protected resources

The screenshot shows the AWS Backup console interface. On the left, a navigation sidebar lists various sections: My account, External resources, My organization, and Backup Audit Manager. The 'Protected resources' link under 'My account' is highlighted with a red box. The main content area displays a table titled 'Protected resources (7)'. The table has columns for Resource ID, Resource type, and Last backup. A search bar and filter button are at the top of the table. An orange 'Create on-demand backup' button is located in the top right corner. The table data is as follows:

Resource ID	Resource type	Last backup
volume/vol-0b9	EBS	November 15, 2022, 09:00:00 (UTC+01:00)
volume/vol-048	EBS	November 15, 2022, 09:00:00 (UTC+01:00)
volume/vol-0f4	EBS	November 15, 2022, 08:00:00 (UTC+01:00)
instance/i-0fcefa	EC2	November 15, 2022, 08:00:00 (UTC+01:00)
instance/i-0609	EC2	November 15, 2022, 08:00:00 (UTC+01:00)
instance/i-01afc	EC2	November 15, 2022, 08:00:00 (UTC+01:00)
instance/i-0128	EC2	November 15, 2022, 08:00:00 (UTC+01:00)

# AWS Backup – Backup policy

The screenshot shows the AWS Organizations console with the 'Policies' section selected. The 'Backup policies' page is displayed, showing two customer-managed backup policies:

Name	Kind	Description
bronze-backup-policy	Customer managed policy	policy for reinvent demo 1hr frequency, 5 day retention in local
Daily-Backup-Policy	Customer managed policy	Daily-Backup-Policy

The 'bronze-backup-policy' row is highlighted with a red box. To the right, a large red box highlights the JSON content of the selected policy:

```
{  
  "plans": {  
    "bronze-plan": {  
      "regions": {  
        "@@assign": [  
          "eu-west-1"  
        ]  
      },  
      "rules": {  
        "bronze-rule": {  
          "schedule_expression": {  
            "@@assign": "cron(0 5/1 ? * * *)"  
          },  
          "start_backup_window_minutes": {  
            "@@assign": "60"  
          },  
          "complete_backup_window_minutes": {  
            "@@assign": "120"  
          },  
          "lifecycle": {  
            "delete_after_days": {  
              "@@assign": "5"  
            }  
          },  
          "target_backup_vault_name": {  
            "@@assign": "bronze"  
          },  
          "copy_actions": {  
            "arn:aws:backup:eu-central-1:  
            :backup-vault:bronze": {  
              "target_backup_vault_arn": {  
                "@@assign": "arn:aws:backup:eu-central-1:  
                :backup-vault:bronze"  
              },  
              "lifecycle": {  
                "delete_after_days": {  
                  "@@assign": "10"  
                }  
              }  
            }  
          }  
        }  
      }  
    }  
  }  
}
```

# AWS Backup – Restore

AWS Backup X ?

AWS Backup > Protected resources > instance/i-0fce7f1633abaa48

**Resource details** Info **Create on-demand backup**

**Summary**

Resource ID	instance/i-0fce7f1633abaa48	Resource type	EC2
		Last backup	November 15, 2022, 08:00:00 (UTC+01:00)

**Recovery points (163)** C **Restore**

Filter by recovery point ID 1 2 3 4 5 6 7 ... 17 > ⚙️

Recovery point ID	Status	Backup type	Creation time
image/ami-0d...	Completed	Image	November 15, 2022, 08:00:00 (UTC+01:00)
image/ami-08...	Completed	Image	November 15, 2022, 07:00:00 (UTC+01:00)
image/ami-0d...	Completed	Image	November 15, 2022, 06:00:00 (UTC+01:00)
image/ami-06...	Completed	Image	November 15, 2022, 00:00:00 (UTC+01:00)
image/ami-09...	Completed	Image	November 14, 2022, 23:00:00 (UTC+01:00)
image/ami-08...	Completed	Image	November 14, 2022, 22:00:00 (UTC+01:00)
image/ami-01...	Completed	Image	November 14, 2022, 21:00:00 (UTC+01:00)
image/ami-07...	Completed	Image	November 14, 2022, 20:00:00 (UTC+01:00)
image/ami-0f...	Completed	Image	November 14, 2022, 19:00:00 (UTC+01:00)
image/ami-01...	Completed	Image	November 14, 2022, 18:00:00 (UTC+01:00)



# AWS Backup – Restore

AWS Backup < X AWS Backup > Protected resources > instance/i-0fce7f1633abaa48 > Restore backup ⓘ

## Restore backup

Restore EC2 instances so they can centrally manage backups with other resources while being able to use the key features like scheduled backups, lifecycle management, and quick restores. To access full instance restore capabilities go to [Instance Launch Wizard](#) ⓘ

**Network settings**

Instance type [Info](#)  
Define the compute and memory capacity of the instance.  
t2.large - 2 vCPU, 8 GiB RAM

Virtual Private Cloud (VPC)  
Select the VPC to define the virtual networking environment.  
Default VPC ( ) ▾ C

Subnet [Info](#)  
Specify a range of IP addresses in your VPC that can be used to isolate different EC2 resources from each other or from the internet. Each subnet resides in one Availability Zone.  
No preference (default subnet in any Availability Zone) ▾ C

Security groups [Info](#)  
Specify security groups to determine a set of firewall rules that control the traffic for your instance.  
Add a security group ▾ C  
default X

Instance IAM role [Info](#)  
Specify the IAM role that will automatically deploy AWS credentials to the EC2 instance.  
Restore with original IAM role ▾



# Post-incident activity

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



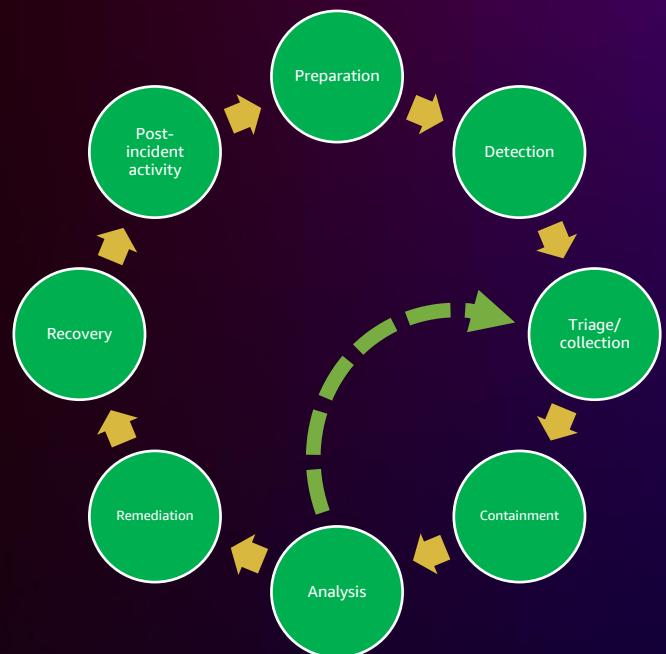
[nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf](https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf)



© 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



# Thank you!



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