



Incident Management & Response in der Cloud

Armin Schneider – CISSP, ISO 27001 LA

Specialist Solution Architect – Security & Compliance

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 – Accounts



Global infrastructure



AWS account



AWS Identity and Access Management (IAM)

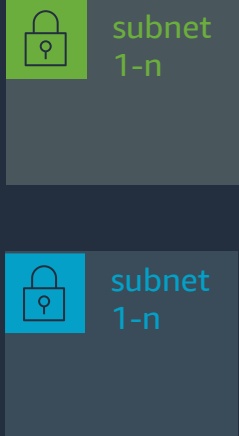


Region

Resources

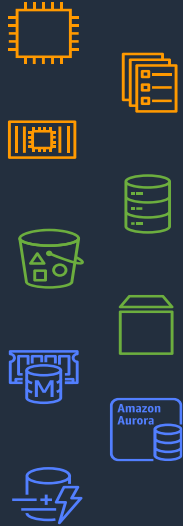


VPC 1-n

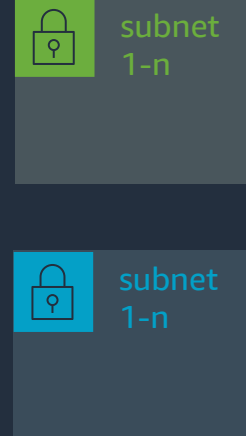


Region 1-n

Resources



VPC 1-n

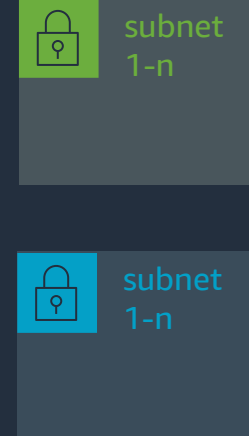


Region 1-n

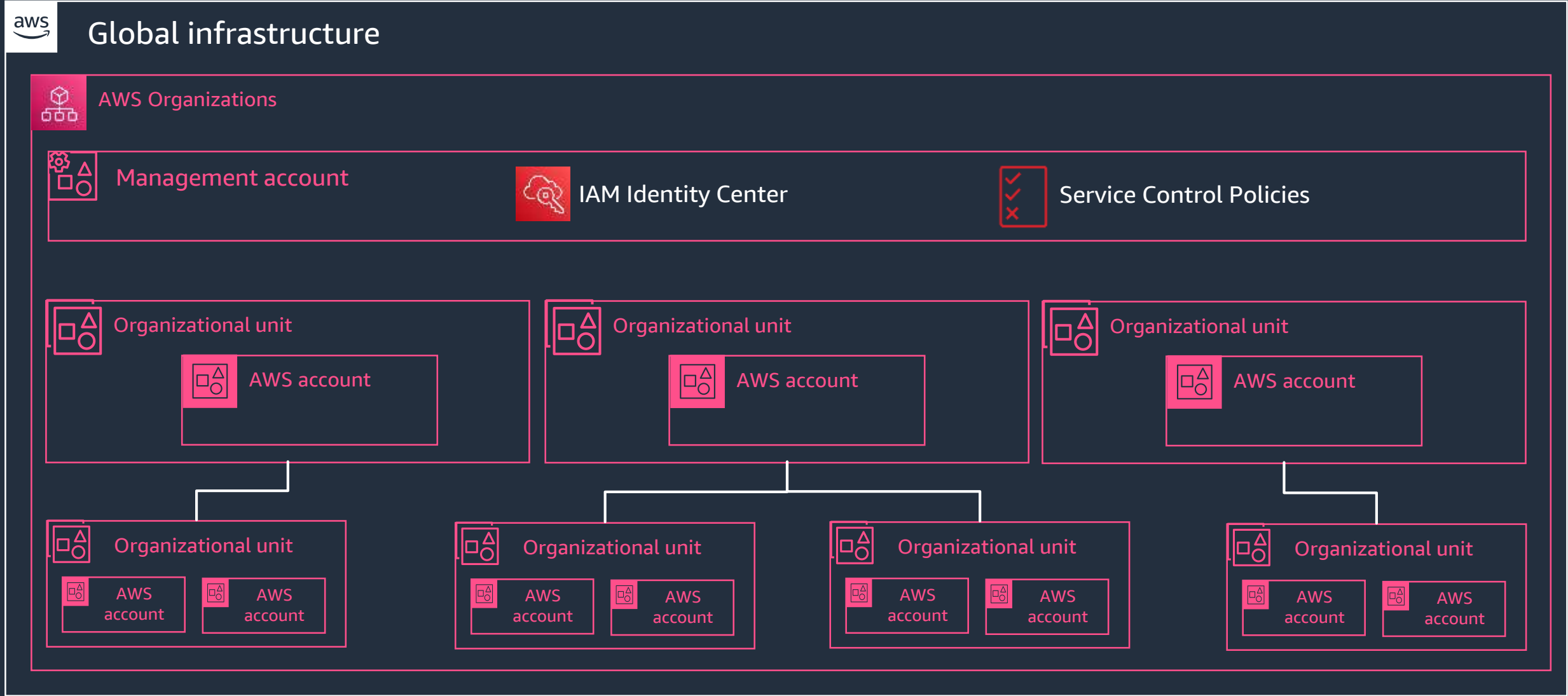
Resources



VPC 1-n



AWS Cloud – Multiple accounts & organizations

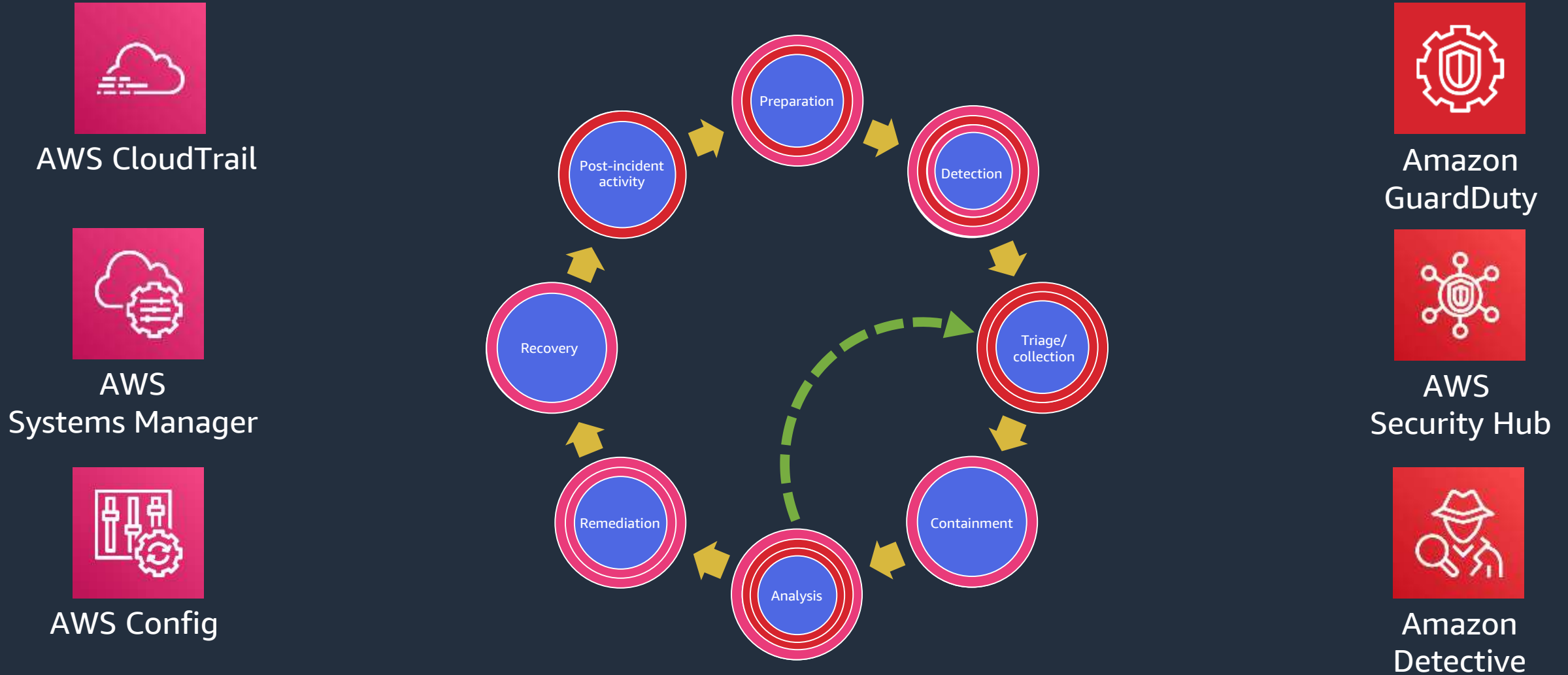


What remains the same

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



Detection



Detection using AWS services



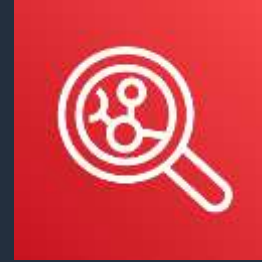
GuardDuty

**Analyze log data
for anomalies and
malicious behavior**



AWS
Config

**Check configuration
status and rule
compliance**

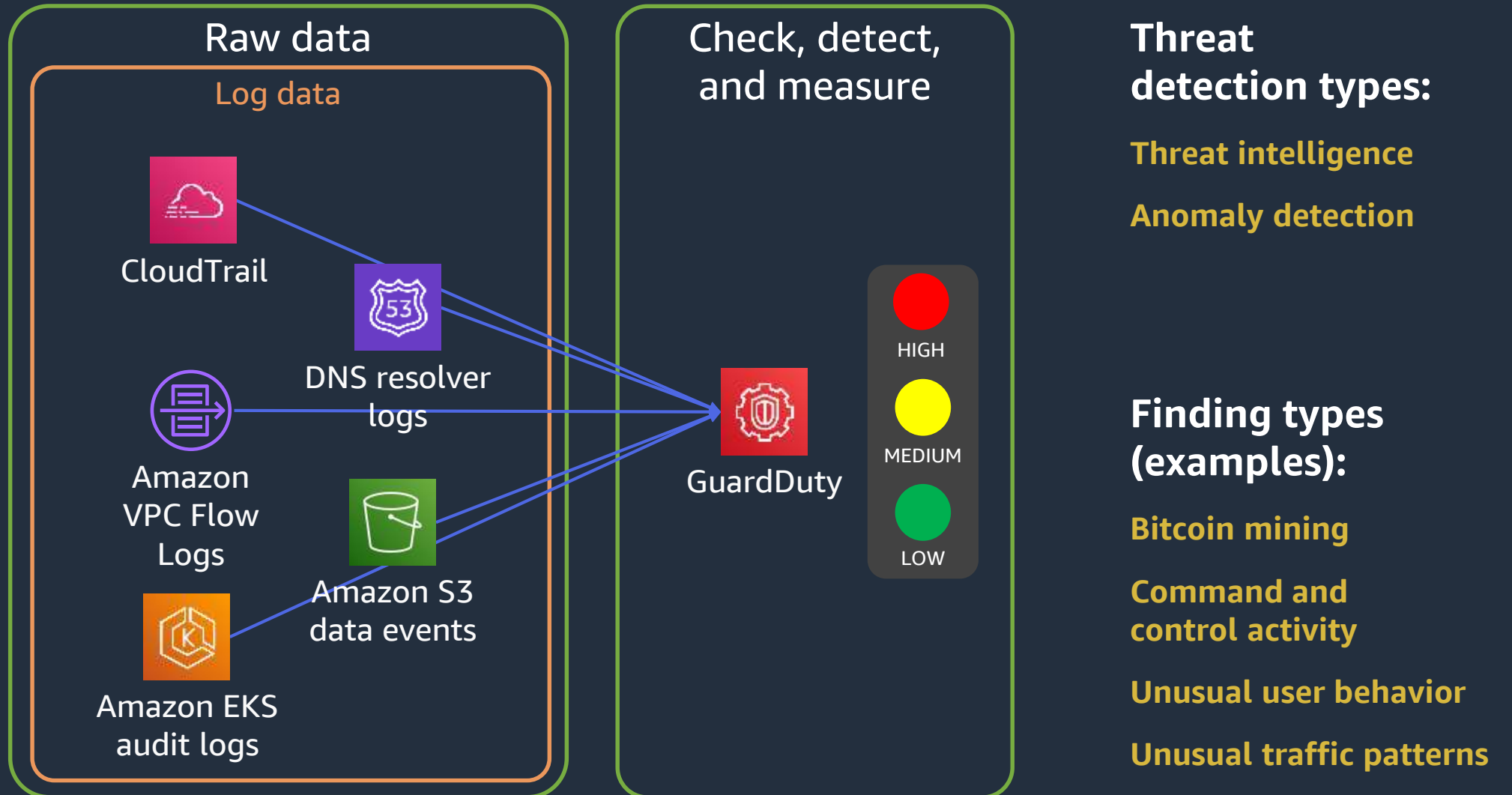


Amazon
Inspector

**Check for software
vulnerabilities**

How GuardDuty works

No configuration
needed for this
log source



GuardDuty finding

GuardDuty

Findings

Usage

Malware scans

Settings

Lists

S3 Protection

EKS Protection

Malware Protection

Accounts

What's New

Partners

GuardDuty > Findings

Showing 26 of 26

Findings Info



Suppress Findings Info


Current Add filter criteria


Saved rules Apply saved rules

	Finding type	Resource	Last seen	Account ID	Count
<input type="checkbox"/>	Recon:IAMUser/MaliciousIPCaller.Custom	SSM-SS-Role:	a month ago		5
<input type="checkbox"/>	Recon:IAMUser/MaliciousIPCaller.Custom	SSM-SS-Role:	a month ago		2
<input type="checkbox"/>	Recon:IAMUser/MaliciousIPCaller.Custom	AmazonSSMRoleForInstancesQuickSetup:	a month ago		10
<input type="checkbox"/>	Recon:IAMUser/MaliciousIPCaller.Custom	SSM-SS-Role:	a month ago		1
<input type="checkbox"/>	Recon:IAMUser/MaliciousIPCaller.Custom	AmazonSSMRoleForInstancesQuickSetup:	a month ago		4
<input type="checkbox"/>	Recon:IAMUser/MaliciousIPCaller.Custom	AmazonSSMRoleForInstancesQuickSetup:	a month ago		8
<input type="checkbox"/>	Recon:IAMUser/MaliciousIPCaller.Custom	AmazonSSMRoleForInstancesQuickSetup:	a month ago		5
<input type="checkbox"/>	Recon:IAMUser/MaliciousIPCaller.Custom	AmazonSSMRoleForInstancesQuickSetup:	a month ago		5
<input type="checkbox"/>	Recon:IAMUser/MaliciousIPCaller.Custom	AmazonSSMRoleForInstancesQuickSetup:	a month ago		6
<input type="checkbox"/>	Recon:IAMUser/MaliciousIPCaller.Custom	AmazonSSMRoleForInstancesQuickSetup:	a month ago		8
<input type="checkbox"/>	Policy:S3/AccountBlockPublicAccessDisabled	AWSReservedSSO_	a month ago		1
<input type="checkbox"/>	Recon:IAMUser/MaliciousIPCaller.Custom	AmazonSSMRoleForInstancesQuickSetup:	a month ago		2
<input type="checkbox"/>	Recon:IAMUser/MaliciousIPCaller.Custom	AmazonSSMRoleForInstancesQuickSetup:	a month ago		11
<input type="checkbox"/>	UnauthorizedAccess:EC2/MaliciousIPCaller.Custom	Instance: i-08d0c7a9c27319c16	a month ago		1
<input type="checkbox"/>	Execution:EC2/MaliciousFile	Instance: i-07a954a1	3 months ago		1
<input type="checkbox"/>	Backdoor:EC2/C&CActivity.B!DNS	Instance: i-0569ee2f	3 months ago		2
<input type="checkbox"/>	Backdoor:EC2/C&CActivity.B!DNS	Instance: i-07a954a1	3 months ago		4




GuardDuty findings details

Backdoor:EC2/C&CActivity.BIDNS 
Finding ID: 66c1226d25db6dc7a231a31e11136d5 


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

 Investigate with Detective



Overview

Severity	HIGH	
Region	eu-west-1	
Count	2	
Account ID	[REDACTED]	
Resource ID	i-0569[REDACTED] 	
Created at	07-28-2022 14:48:53 (3 months ago)	
Updated at	07-28-2022 15:10:20 (3 months ago)	



Malware scan

Scan ID	54515726fb2ee2fa21fe23117475c6c5 
Scan status	COMPLETED
Start time	07-28-2022 14:50:02
End time	07-28-2022 14:55:58
Security status	CLEAN

Resource affected



Resource role	TARGET 
Resource type	Instance 


Instance details


Instance ID	i-0569[REDACTED] 
Instance type	t2.large
Instance state	running
Availability zone	eu-west-1c
Image ID	ami-01efa4023f0f5a042 
Image description	Amazon Linux 2 Kernel 5.10 AMI Z.0.20211225.0 x86_64 HVM gp2
Launch time	07-28-2022 13:42:31

IAM instance profile





ARN	arn:aws:iam::[REDACTED]:instance-profile/EC2-PROWLER-WITH-SSM
-----	---

Execution:EC2/MaliciousFile 
Finding ID: 5ac1227e2cd55ae820270e2f4f886d7h 

High 2 security risk(s) detected including EICAR-Test-File (not a virus) on EC2 instance i-07a9[REDACTED] 




 Investigate with Detective

Overview




Severity	HIGH	
Region	eu-west-1	
Count	1	
Account ID	[REDACTED]	
Resource ID	i-07a[REDACTED] 	
Created at	07-28-2022 15:26:04 (3 months ago)	
Updated at	07-28-2022 15:26:04 (3 months ago)	
Scan ID	9453f5942e896cab64e9ef2646f95893 	

Threats detected (2)


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

Name	EICAR-Test-File (not a virus) 
Severity	HIGH 
Hash	275a021bbfb6489e54d471899f7db9d1663fc695[REDACTED] 
File path	/Users/Administrator/Downloads/eicar.com
File name	eicar.com
Volume ARN	arn:aws:ec2:eu-west-[REDACTED]:volume/vol-0ae2852772e47777b


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

Name	EICAR-Test-File (not a virus) 
Severity	HIGH 
Hash	275a021bbfb6489e54d471899f7db9d1663fc695ec2fe2a2c453[REDACTED] 
File path	/Users/Administrator/Downloads/eicar_com.zip=>eicar.com
File name	eicar_com.zip=>eicar.com
Volume ARN	arn:aws:ec2:eu-west-[REDACTED]:volume/vol-0ae285[REDACTED]

Resource affected

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

Instance details

Instance ID	i-07a[REDACTED] 
-------------	---

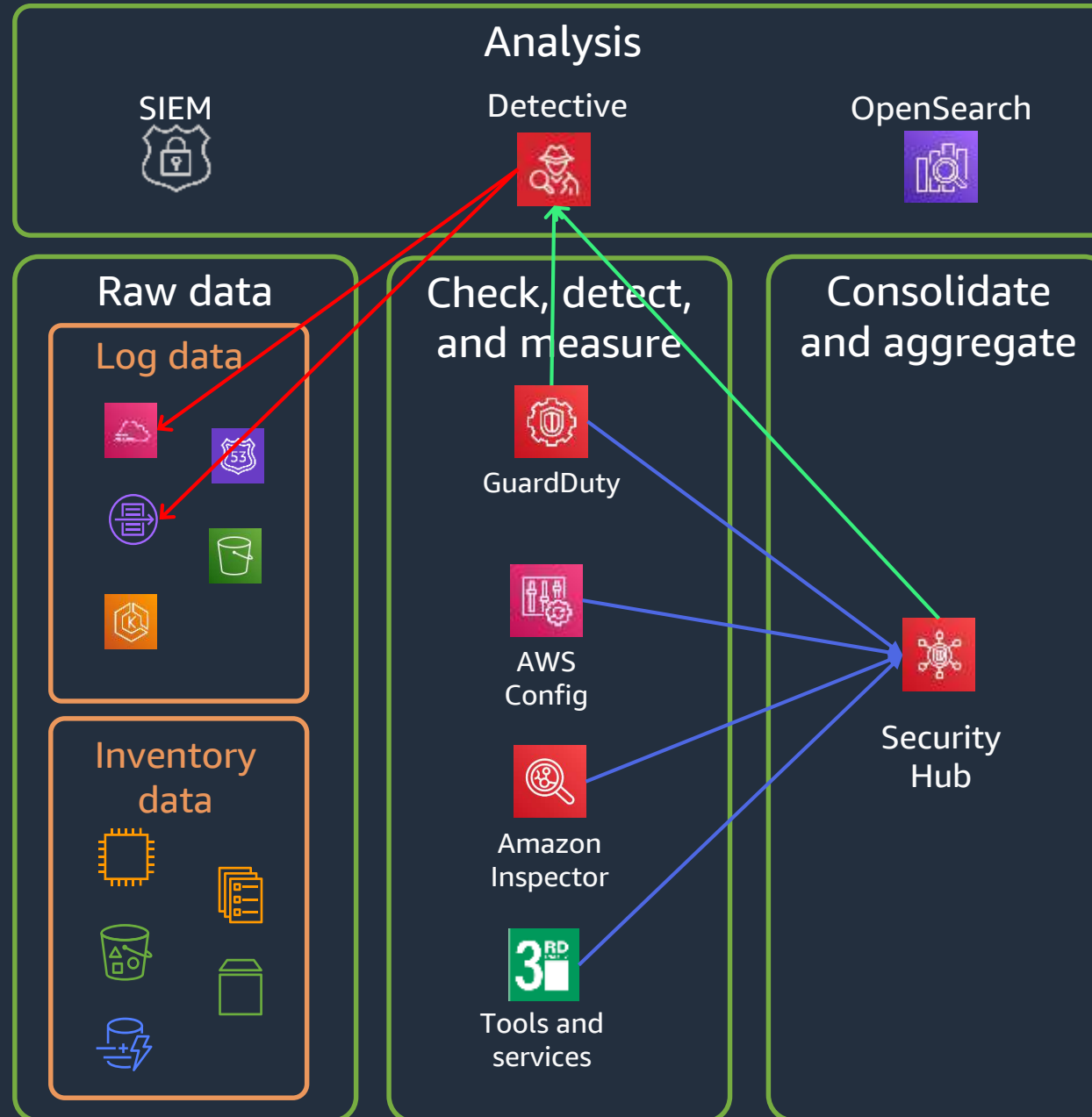


Analysis



If we need to do further Analysis

Do Context based
and targeted
analysis



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

Summary

Security standards

Insights

Findings

Integrations

Settings

What's new

Security Hub > Findings

Findings

A finding is a security issue or a failed security check.

Product name is GuardDuty

Workflow status is NEW

Workflow status is NOTIFIED

Record state is ACTIVE

Add filters

< 1 >

	Severity	Workflow status	Record State	Region	Account Id	Company	Product
<input type="checkbox"/>	LOW	NEW	ACTIVE	eu-west-1		Amazon	GuardDuty
<input type="checkbox"/>	LOW	NEW	ACTIVE	eu-west-1		Amazon	GuardDuty
<input type="checkbox"/>	LOW	NEW	ACTIVE	eu-west-1		Amazon	GuardDuty
<input type="checkbox"/>	HIGH	NEW	ACTIVE	eu-west-1		Amazon	GuardDuty
<input type="checkbox"/>	HIGH	NEW	ACTIVE	eu-west-1		Amazon	GuardDuty
<input type="checkbox"/>	LOW	NEW	ACTIVE	eu-west-1		Amazon	GuardDuty

Regions: All Linked Regions

Command and Control server domain name queried by EC2 instance i-08d0c7a9c27319c16.

Finding ID: arn:aws:guardduty:eu-west-1::detector/00fb24fd6522fd652/finding/3cc1aaad733323d7a2568b9713aab1f6

HIGH

EC2 instance i-08d0c7a9c27319c16 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

Account Name

Forensic Account

Severity (original)

8

Created at

2022-09-19T10:46:04.134Z

Updated at

2022-09-27T08:39:57.403Z

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&fid=

Types and Related Findings

Resources

Investigate in Amazon Detective

Investigate finding

Investigate using Detective

Detective

Summary

Finding groups New

Search

Settings

Account management

General

Preferences

Usage

What's new 23

Getting started

Video tutorials

Detective > Search > GuardDuty/3cc1aad733323d7a2569b9713aab1f6

Scope time Info

09/19/2022 09:00 UTC > 09/27/2022 08:00 UTC

Entities related to GuardDuty finding 3cc1aad733323d7a2569b9713aab1f6

Filter by type, name, or ID

54.59

IP address

See profile

First observed

Total times observed

Last observed

09/26/2022 05:43 UTC

Last observed location

Distinct AWS users and roles

Count of related user agents

54.3

IP address

See profile

First observed

Total times observed

Last observed

09/19/2022 10:03 UTC

Last observed location

Distinct AWS users and roles

Count of related user agents

AWS account

See profile

No attributes available for this entity

i-08d0

EC2 instance

See profile

EC2 instance

i-08d0

Node

ARN

arn:aws:ec2:eu-west-1::instance/i-08d0c7a9c27319c16

Associated VPC

vpc-01

EKS cluster

AWS account

Creation date

03/24/2022 09:00 UTC

Created by

AWSReservedSSO

Role

EC-SSM_53

Command and Control server domain name queried by EC2 instance i-08d0

Backdoor EC2/C&C/Activity/BIDS Info

Finding ID: 3cc1aad733323d7a2569b9713aab1f6

Archive finding

EC2 instance i-08d0 is querying a domain name associated with a known Command & Control server.

Overview

Severity

Count

Account ID

Resource ID

Created at

Updated at

High

5

i-08d0

09/19/2022 10:46 UTC

09/27/2022 08:39 UTC

Resource affected

Resource role

Resource type

Instance ID

Instance type

Instance state

Availability zone

Image ID

Image description

Launch time

TARGET

Instance

i-08d0

t2.medium

running

eu-west-1b

ami-0069d66985b09d219

Amazon Linux 2 Kernel 5.10 AMI 2.0.20220316.0 x86_64

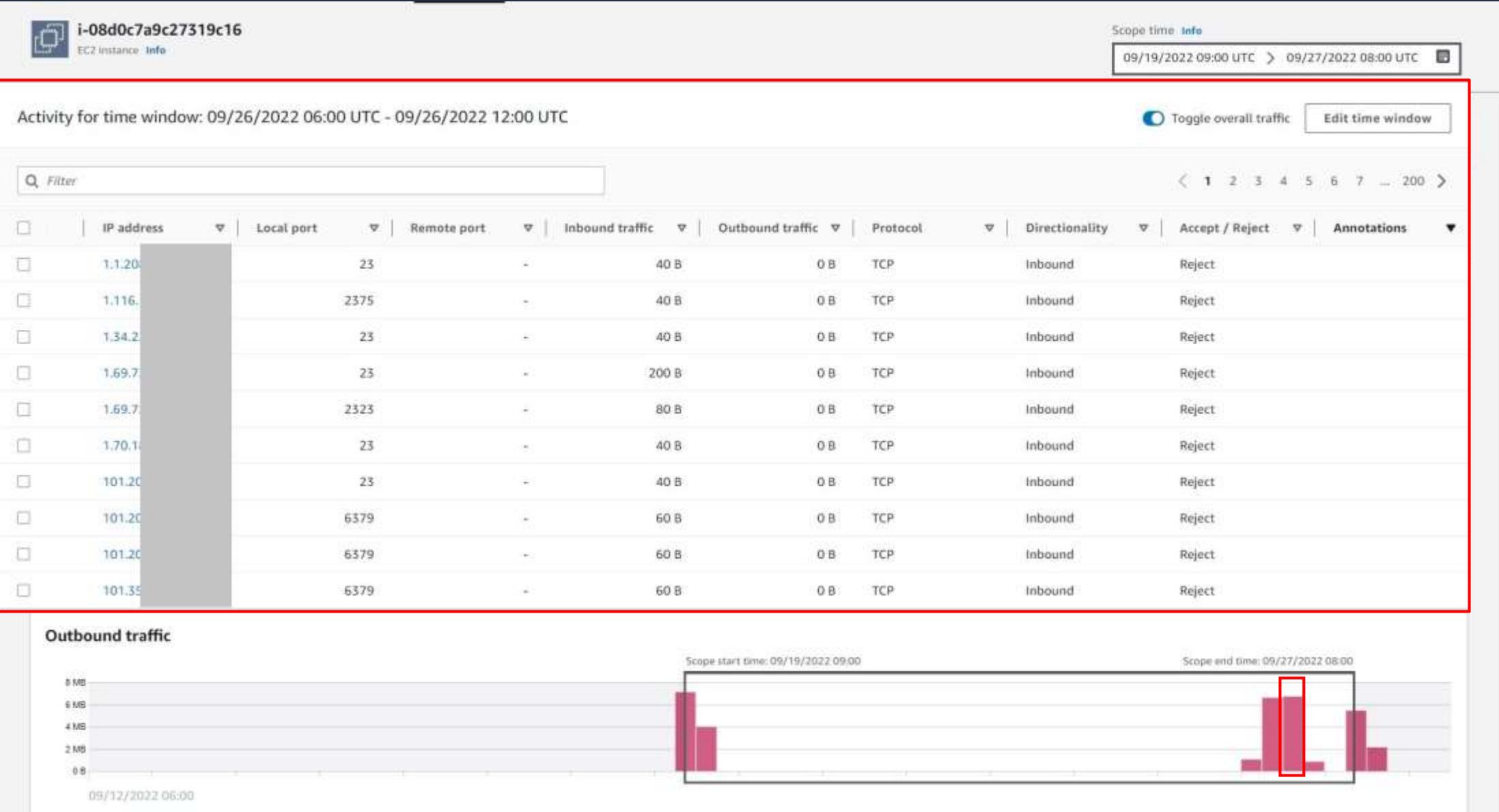
09/27/2022 07:15 UTC

Iam instance profile

ARN

arn:aws:iam:::instance-profile/EC-SS...

Investigate using Detective



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!

Armin Schneider – CISSP, ISO 27001 LA
Specialist Solution Architect – Security & Compliance

Halle 6 – Stand Nr. 6-202