



THREAT DETECTION

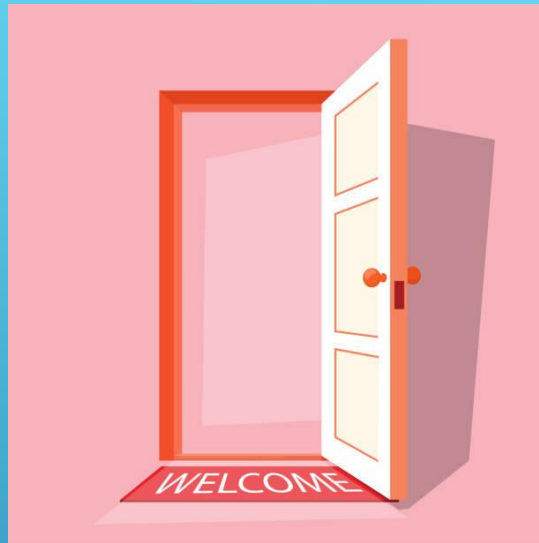
Using AWS Security Tools

DETECTION RELATED TERMS

- ▶ A **vulnerability** is a weakness in the system
- ▶ A **threat** is a possibility for an event or act to exploit a vulnerability
- ▶ A **risk** is the potential for loss, damage, or destruction of resources due to a threat.



Open Door



Thief



Burglary/Theft



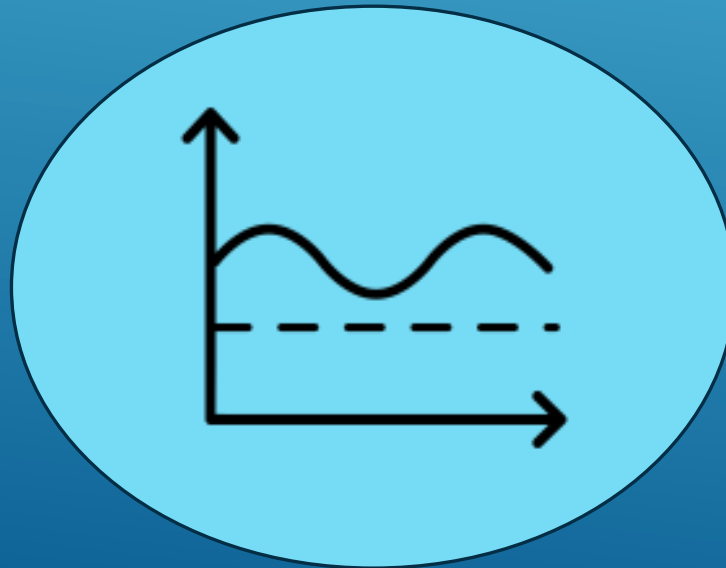
EXAMPLE OF THREATS

- ▶ Denial-of-service attacks
- ▶ Malware infections
- ▶ Unauthorized access or insider threats
- ▶ Misconfigurations and poor change control
- ▶ Mismatched port-application traffic
- ▶ Unusual Domain Name System (DNS) requests
- ▶ Unusual outbound network traffic
- ▶ Anomalies in privileged user account activity
- ▶ Geographical irregularities (source of traffic)
- ▶ Unusually high traffic at irregular hours
- ▶ Multiple, repeated, or irregular login attempts



WHAT IS A BASELINE?

- ▶ A baseline is a set of metrics used to define the **normal working conditions** of your workload
- ▶ **Current state**, configuration, and use of resources
- ▶ Peak network times and port and protocol used
- ▶ Identities, access, and authorizations based on requirements



DEEP SET OF SECURITY TOOLS & SERVICES



Identity

AWS Identity and Access Management (IAM)
AWS Single Sign-On
AWS Directory Service
Amazon Cognito
AWS Organizations
AWS Secrets Manager
AWS Resource Access Manager (AWS RAM)



Detect

AWS Security Hub
Amazon GuardDuty
Amazon Detective
AWS CloudTrail
Amazon CloudWatch
Amazon VPC flow logs
AWS Config
Amazon Inspector



Infrastructure protection

AWS Systems Manager
AWS Shield
AWS WAF
(web application firewall)
AWS Firewall Manager
Amazon Inspector
Amazon VPC



Data protection

AWS Key Management Service (AWS KMS)
AWS CloudHSM
AWS Certificate Manager (ACM)
Amazon Macie
Server-side encryption



Respond

AWS Config rules
AWS Lambda
Systems Manager

SECURITY BEST PRACTICES



Logging network traffic
Logging user and API traffic
Visibility and pattern analysis

Enhancing Monitoring
Anomaly Detection
Automated threat detection
Managing alerts and findings
Root Cause Analysis

Assess and audit resource configurations
Scanning for vulnerability and network reachability

AWS CLOUDTRAIL FUNCTIONS

- ▶ Simplify compliance audits by automatically recording and storing activity logs for an AWS account.
- ▶ Increase visibility into user and resource activity.
- ▶ Discover and troubleshoot security
- ▶ capturing a comprehensive history of changes

AWS CloudTrail tracks the **who, what, where, and when of any API calls** that occurs in your AWS environment.

INTEGRATE WITH CLOUDWATCH LOGS

- ▶ Monitor and alert on specific events.
- ▶ Simple searching is provided.
- ▶ Use AWS Config to ensure CloudTrail is sending events to CloudWatch Logs.
- ▶ Create Metric Filters
- ▶ Create Metric based Alarm



INDICATORS OF COMPROMISE

- ▶ Abnormal CPU utilization
- ▶ Significant or sudden increases in database reads
- ▶ Mismatched port-application traffic
- ▶ Unusual DNS requests
- ▶ Unusual outbound network traffic
- ▶ Anomalies in privileged user account activity
- ▶ Geographical irregularities (source of traffic)
- ▶ Unusually high traffic at irregular hours
- ▶ Multiple, repeated, or irregular login attempts

CLOUDWATCH ALARMS BEST PRACTICES

Example of areas that should be monitored with CloudWatch Alarms:

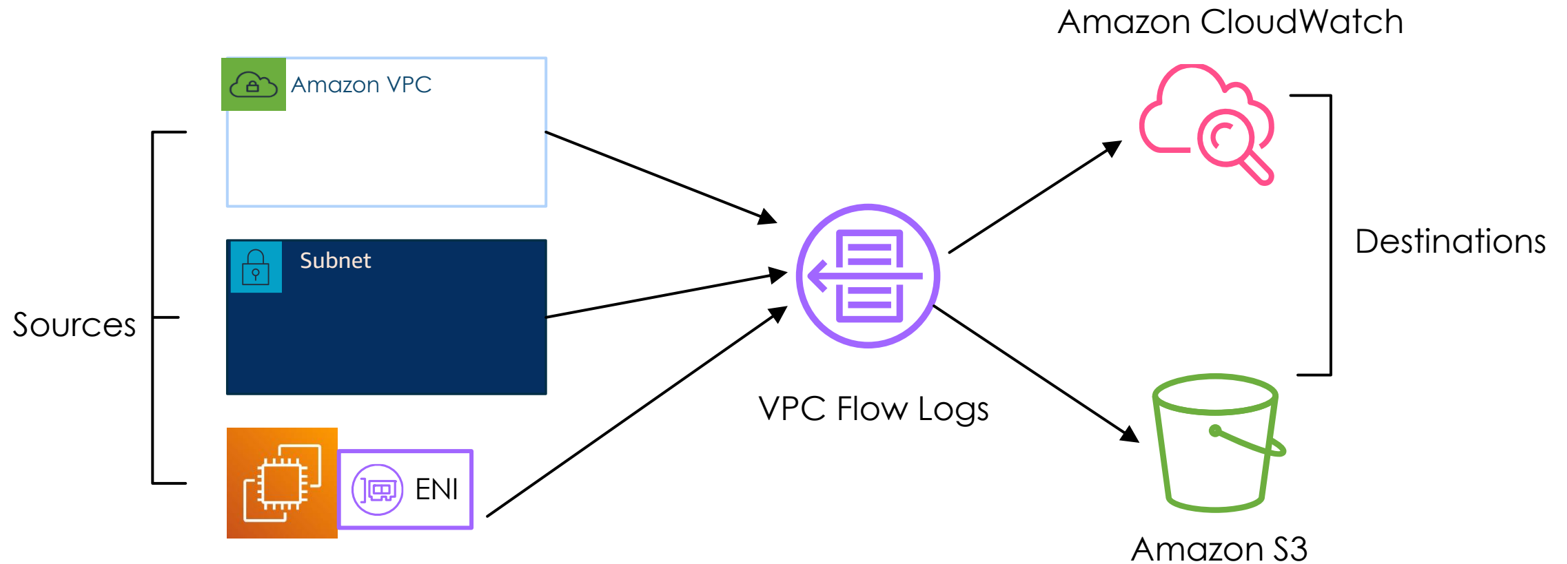
- ▶ AWS Console sign-In requests without MFA
- ▶ IAM policy configuration changes
- ▶ Root account usage
- ▶ Authorization failures; unauthorized API calls made within your AWS account
- ▶ AWS KMS key configuration changes
- ▶ AWS CloudTrail configuration changes
- ▶ AWS EC2 instance and S3 changes
- ▶ AWS VPC, Route table, Internet Gateway, ACLs or security group configuration changes

VPC FLOWLOGS

- Captures information about the **IP traffic going to and from** network interfaces
- VPC Flow Logs can be turned on per **elastic network interface**, per **subnet**, or per **Virtual Private Network**



FLOW LOG SOURCES-DESTINATIONS



FLOW LOG RECORD FORMAT

Version	2
Account ID	123456789010
Interface ID	eni-02b10a1942934552f
Source address	172.16.1.3
Destination address	172.16.32.46
Source port	36490
Destination port	443
Protocol	6
Packets	78
Bytes	5040
Start	1960245064
End	1960245070
Action	ACCEPT
Log status	OK

AWS THREAT DETECTION SECURITY SERVICES



Amazon
Macie



Amazon
Inspector



Amazon
GuardDuty



Amazon
Detective



AWS
Security Hub



Amazon GuardDuty

Protect your AWS accounts with intelligent threat detection

WHAT IS GUARDDUTY?

GuardDuty is a threat detection service that uses machine learning, anomaly detection, and integrated threat intelligence to identify and prioritize potential threats

- ➡ Identify malicious and highly suspicious activity
- ➡ Continuous security monitoring for AWS accounts, workloads, and data stored in Amazon S3

EXAMPLE GUARDDUTY FINDING

GuardDuty

Findings

Usage

Malware scans

Settings

Lists

S3 Protection

EKS Protection

Malware Protection

RDS Protection [Preview](#)

Accounts

What's New

Partners

GuardDuty > Findings

Showing 52 of 52

Findings

Suppress Findings

Info

Saved rules

Apply saved rules

Current

Add filter criteria

<input type="checkbox"/>	Finding type	Resource	L	Accou...	C...
<input type="checkbox"/>	Execution:ECS/MaliciousFile	ECSCluster: gd-tester-RedT	20 d...	5091524309...	1
<input type="checkbox"/>	Execution:EC2/MaliciousFile	Instance: i-009612f3d2232	20 d...	5091524309...	1
<input checked="" type="checkbox"/>	UnauthorizedAccess:EC2/SSHBr...	Instance: i-009612f3d2232	20 d...	5091524309...	1
<input type="checkbox"/>	Trojan:EC2/DNSDataExfiltration	Instance: i-009612f3d2232	20 d...	5091524309...	9
<input type="checkbox"/>	UnauthorizedAccess:EC2/SSHBr...	Instance: i-0e405385a63c0	20 d...	5091524309...	1
<input type="checkbox"/>	Backdoor:EC2/C&CActivity.B!DNS	Instance: i-009612f3d2232	20 d...	5091524309...	1
<input type="checkbox"/>	CryptoCurrency:EC2/BitcoinTool...	Instance: i-009612f3d2232	20 d...	5091524309...	4
<input type="checkbox"/>	Recon:EC2/Portscan	Instance: i-009612f3d2232	20 d...	5091524309...	1

UnauthorizedAccess:EC2/SSHBrut...

Finding ID: 40c28929c4e7213f6bea2e159cf7061f

Feedback

High

i-009612f3d2232c84b is performing SSH brute force attacks against 172.16.0.26. Brute force attacks are used to gain unauthorized access to your instance by guessing the SSH password.

Info

Investigate with Detective

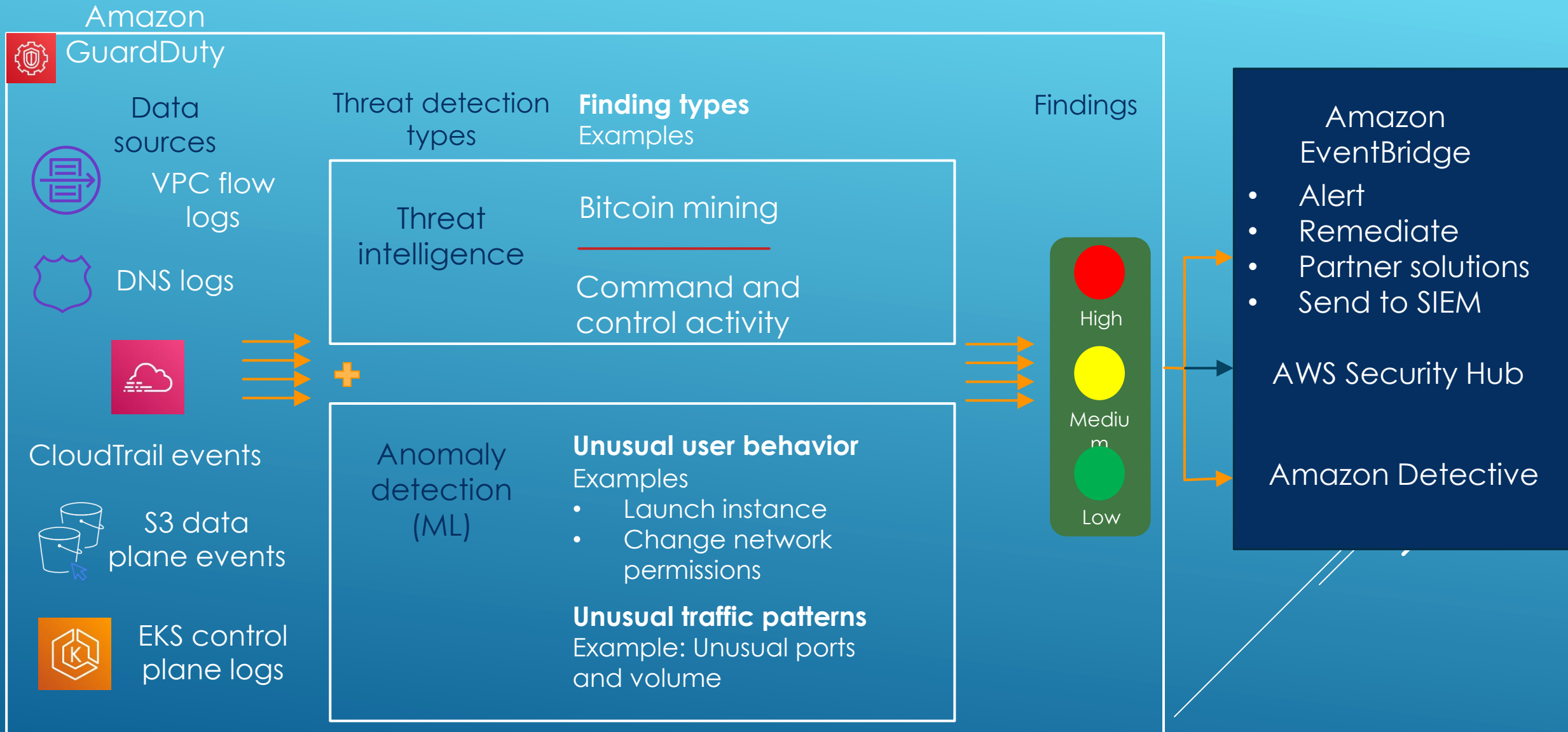
Overview

Severity	HIGH
Region	us-east-1
Count	1
Account ID	509152430977
Resource ID	i-009612f3d2232c84b
Created at	12-14-2022 15:29:02 (20 days ...)
Updated at	12-14-2022 15:29:02 (20 days ...)

Malware scan

Scan ID 341b0e365818f70999b...

AMAZON GUARDDUTY - HOW IT WORKS





Amazon Detective

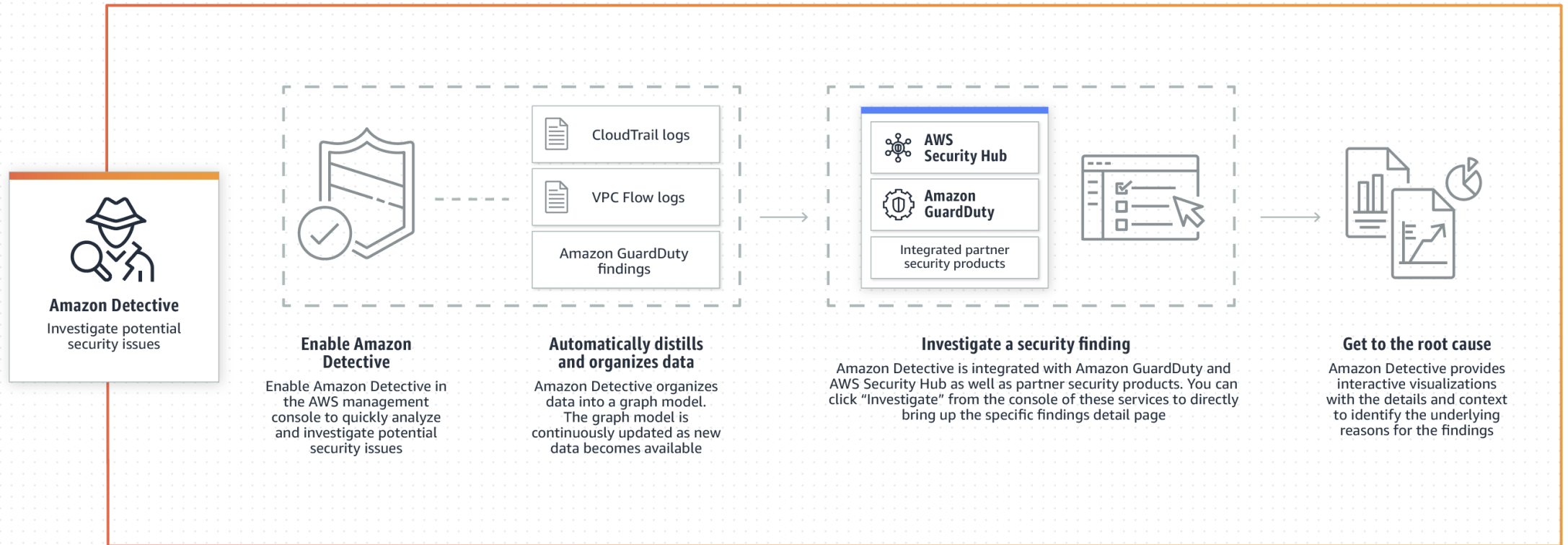
Analyze and visualize security data to rapidly get to the root cause of potential security issues



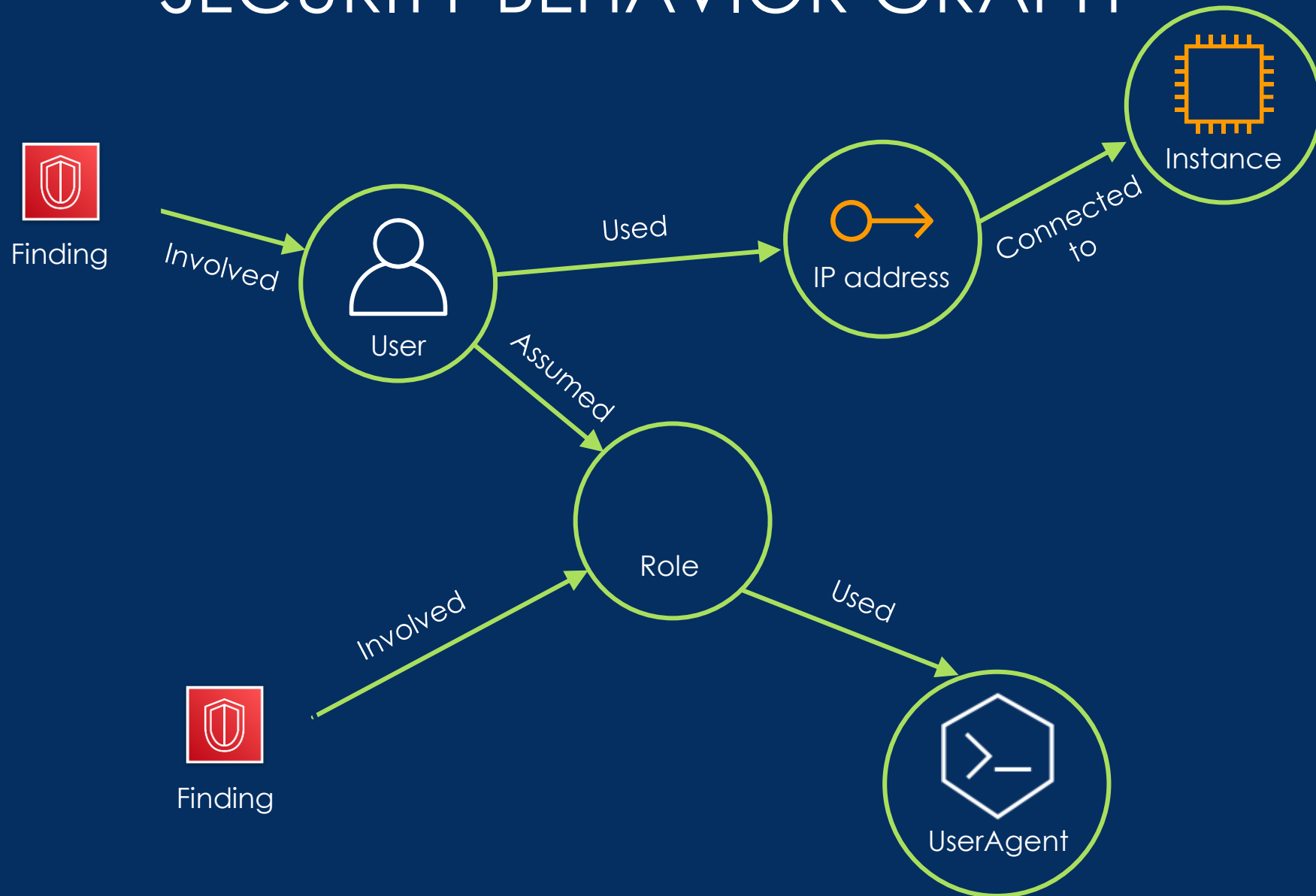
Who done it???



AMAZON DETECTIVE - HOW IT WORKS



SECURITY BEHAVIOR GRAPH



EXTRAS - AMAZON DETECTIVE NOW SUPPORTS GUARDDUTY FINDINGS RELATED TO S3 AND DNS

Amazon Detective expands security investigation support for Amazon Simple Storage Service (S3) that helps to answer questions like:

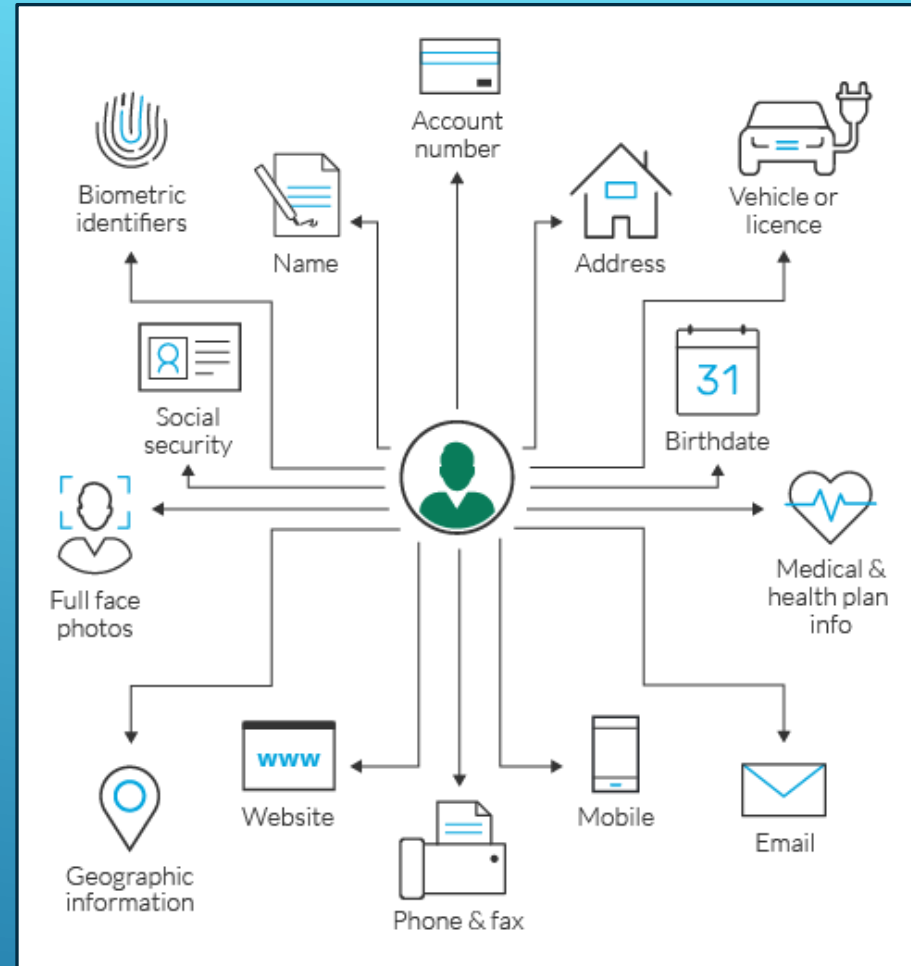
- Who created the S3 bucket?
- When was the S3 bucket created?
- Who made the S3 bucket public?
- Did the user execute sensitive APIs such as disable logging on other S3 buckets?

Also for those DNS-related findings you can deep dive on those related to low-reputation domain names (such as those associated with cryptocurrency-related activities) and algorithmically-generated domains.

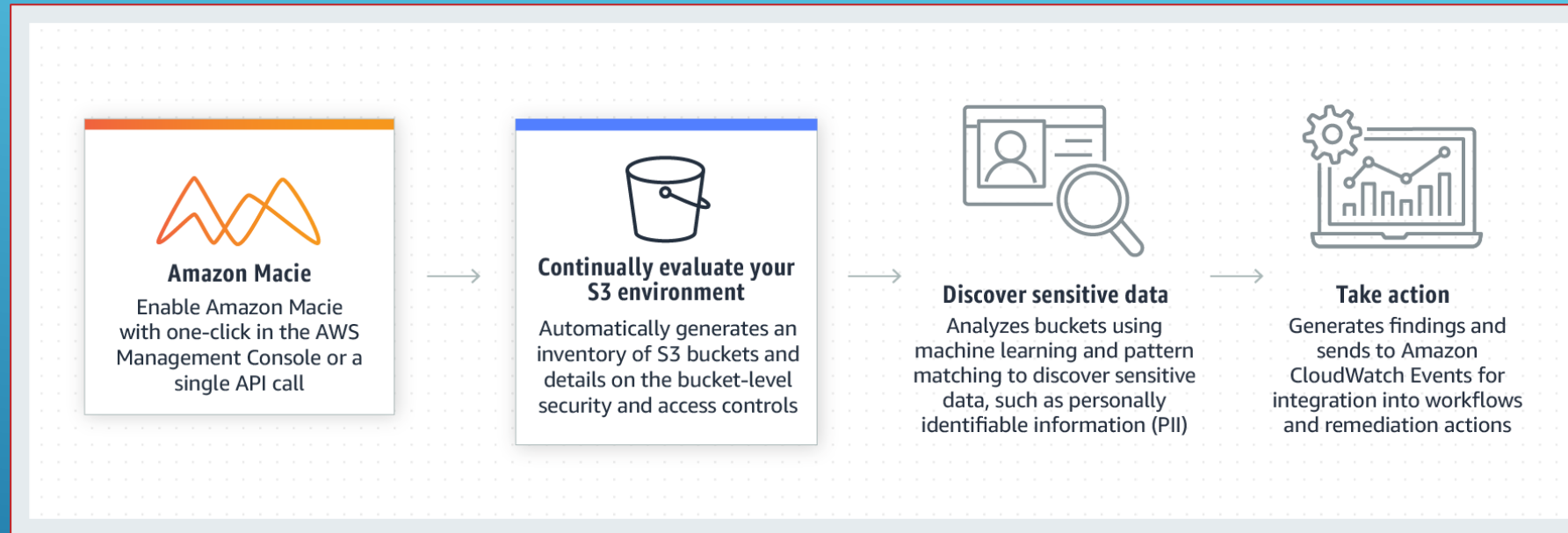


Amazon Macie

Discover and protect your sensitive data



AMAZON MACIE - HOW IT WORKS



Discover
sensitive data

EXTRA – AMAZON MACIE ADD SUPPORT FOR SELECTING MANAGED DATA IDENTIFIER FOR JOBS

When you create a sensitive data discovery job, you can now specify which **managed data identifiers** you want the job to use.

Step 1
Choose S3 buckets

Step 2
Review S3 buckets

Step 3
Refine the scope

Step 4
Select managed data identifiers

Step 5
Select custom data identifiers

Step 6
Enter general settings

Step 7
Review and create

Select managed data identifiers [Info](#)

A managed data identifier is a set of built-in criteria that detects a specific type of sensitive data. Specify the types of sensitive data to detect by selecting managed data identifiers for the job to use.

Managed data identifier options

Select the managed data identifiers to use.

Selection type

☐ All
Use all managed data identifiers.

☐ Exclude
Use all managed data identifiers except specific ones that you select.

☒ Include
Use only specific managed data identifiers that you select.

☐ None
Don't use any managed data identifiers.

Select managed data identifiers (2/100)

This table lists managed data identifiers that Macie currently provides to detect specific categories and types of sensitive data. Select the check box for each one to include in the job.

<input type="checkbox"/>	Sensitive data type	Sensitive data category
<input checked="" type="checkbox"/>	ADDRESS	PERSONAL_INFORMATION
<input type="checkbox"/>	AUSTRALIA_DRIVERS_LICENSE	PERSONAL_INFORMATION
<input type="checkbox"/>	AUSTRALIA_TAX_FILE_NUMBER	PERSONAL_INFORMATION
<input type="checkbox"/>	AUSTRIA_DRIVERS_LICENSE	PERSONAL_INFORMATION
<input checked="" type="checkbox"/>	AWS_CREDENTIALS	CREDENTIALS

AMAZON MACIE EXTRAS - MACHINE LEARNING MODELS ENHANCED TO IMPROVE DISCOVERY FOR

Full names

The updated model extracts additional context from file headers and attributes to better inform detection and reporting of full names.

Passport numbers

We enhanced our keyword support and pattern identification system to detect a more diverse array of occurrences of passport numbers in S3 objects.

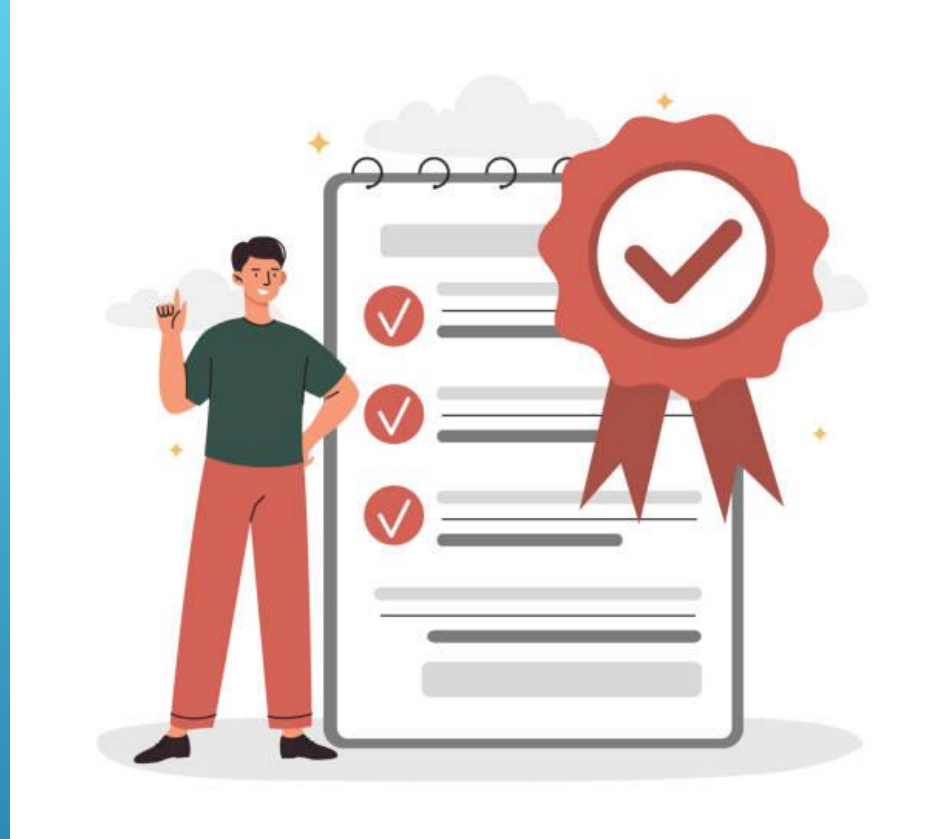
Mailing addresses

The updated model uses additional checks to validate city names, ZIP codes, and Postal Codes to produce more actionable results.

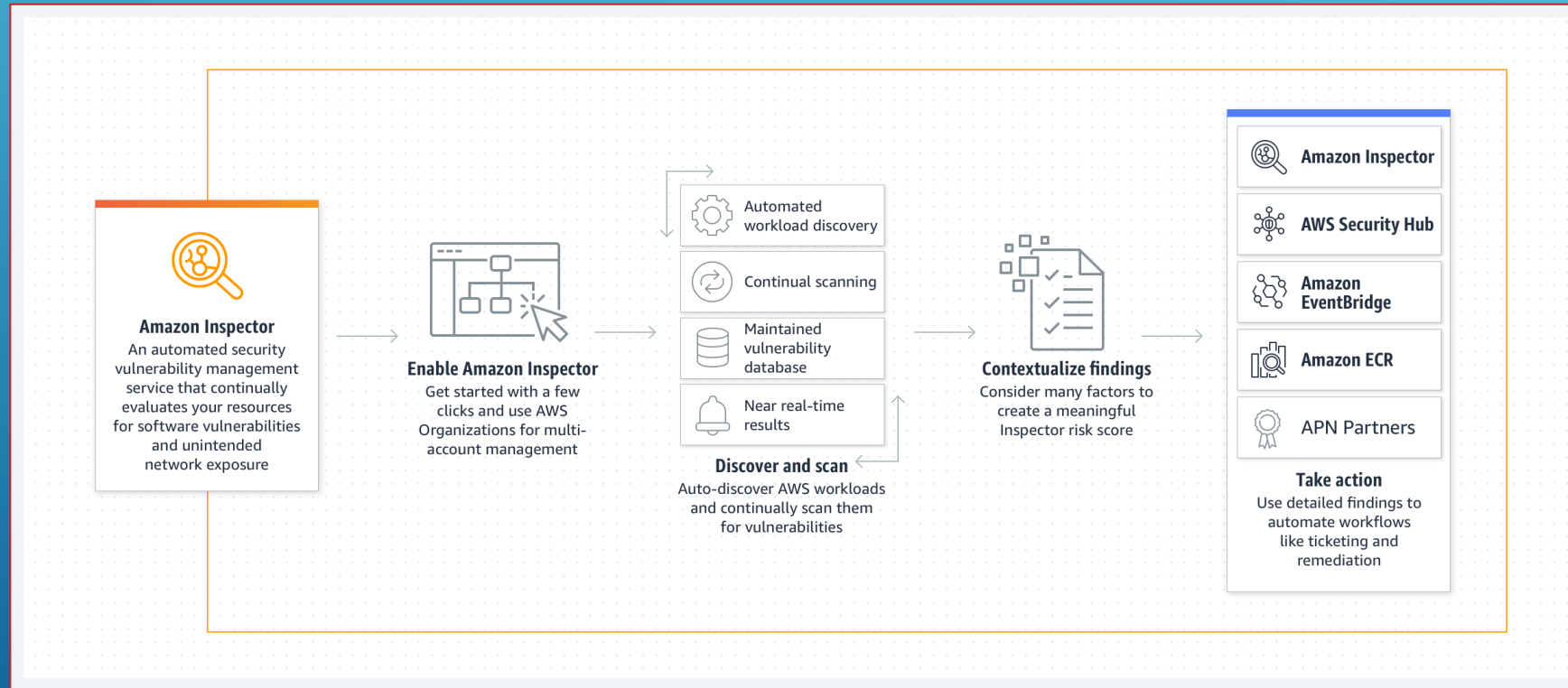


Amazon Inspector

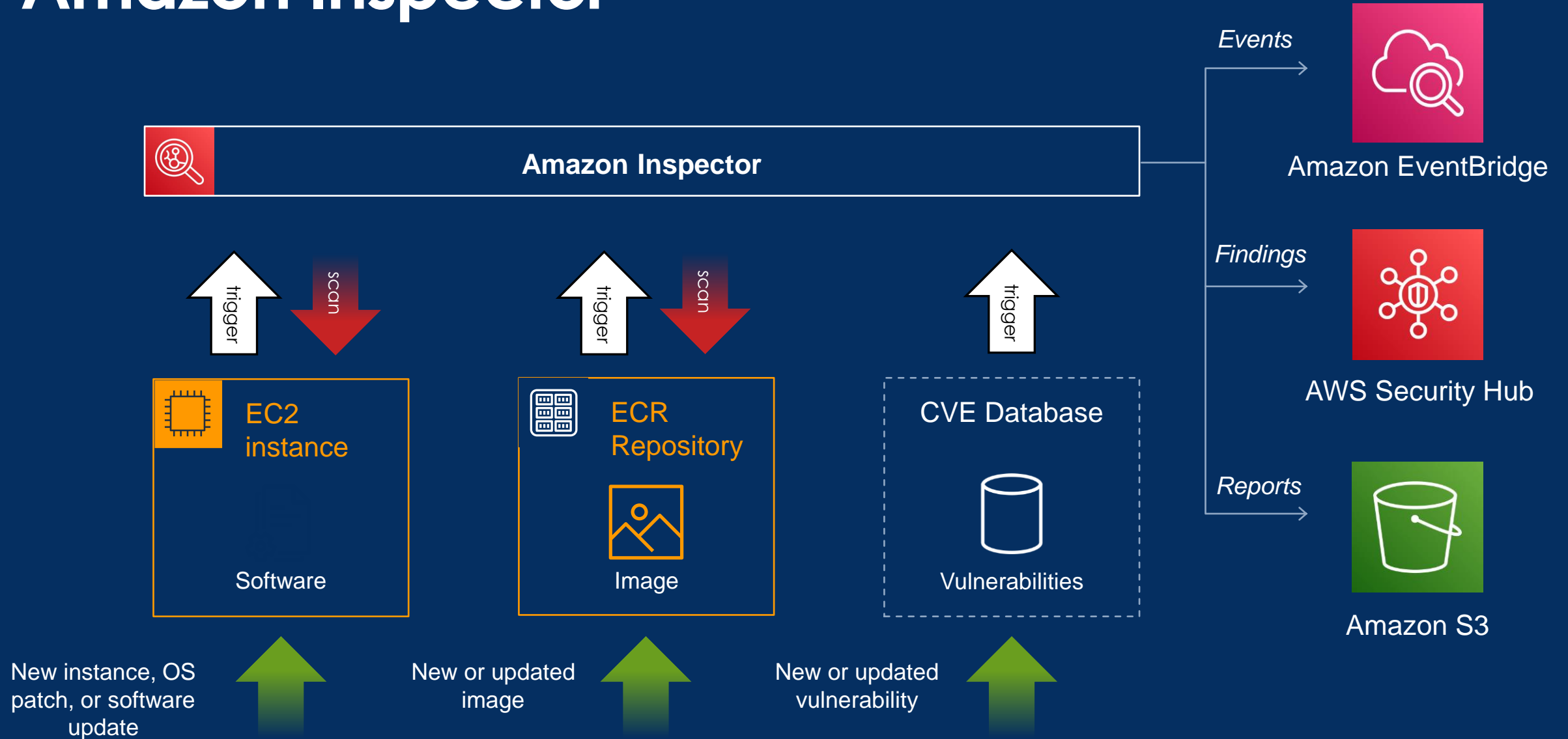
Automated and continual vulnerability management



AMAZON INSPECTOR - HOW IT WORKS



Amazon Inspector



EC2 scanning

Inspector scans EC2 instances for **network reachability** and **package vulnerabilities**



► Network reachability scanning

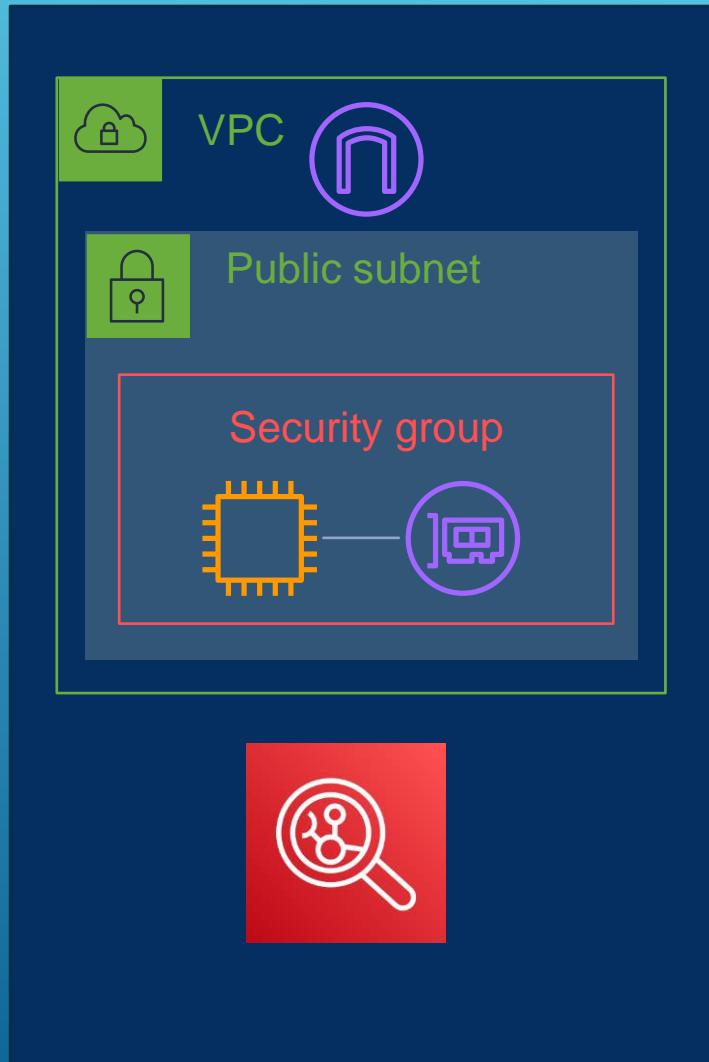
Does not require any agent to be installed



► Package vulnerability scanning

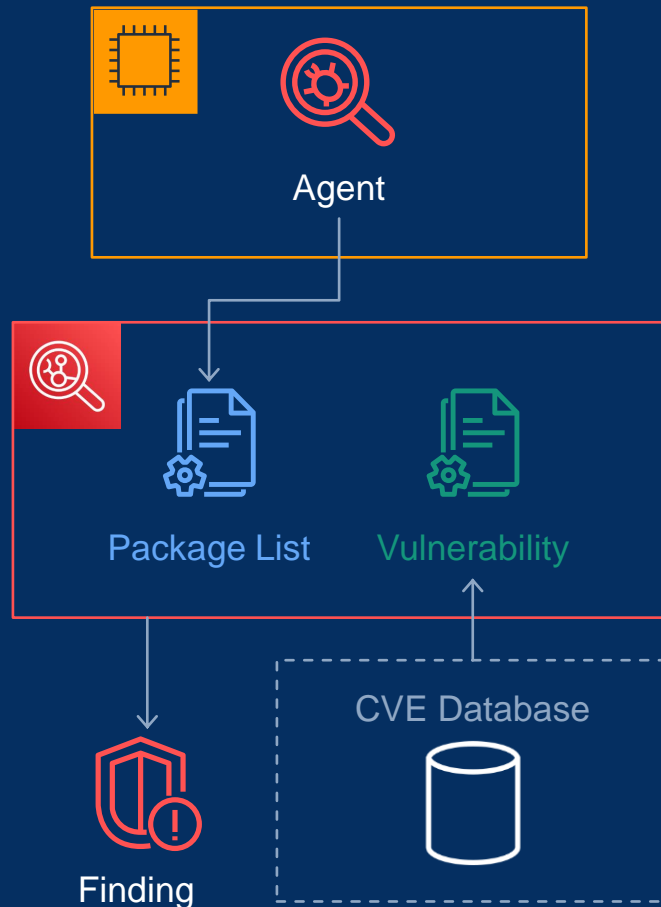
Requires the SSM agent installed on the instance

EC2 SCANNING - NETWORK REACHABILITY



- ▶ Inspector runs reachability analysis on all EC2 instances once every 24 hours
- ▶ Inspector uses advanced heuristics to determine network reachability on each EC2 instance instead of port scanning
- ▶ Like all Inspector findings, network reachability findings can be suppressed for instances that should be publicly exposed, i.e. web servers.

EC2 SCANNING - PACKAGE VULNERABILITY



- ▶ Inspector uses inventory data gathered from Systems Manager to determine what is and isn't installed on an instance
- ▶ Inspector correlates individual packages and their versions to known associated CVE's to report a finding
- ▶ When packages are installed or updated on an instance, a new review of the packages is triggered.

ECR SCANNING – ENHANCED SCANNING

When Inspector is enabled, Enhanced Scanning becomes the default scan type for all ECR registries, but can be changed back to Basic Scanning afterwards.

Amazon ECR > Private registry > Scanning configuration

Scanning configuration

Scanning configuration [Info](#)

Basic scanning is provided by default for your private registry. Enhanced scanning can be enabled for your registry to provide automated, continuous scanning to find vulnerabilities in your container images.

Scan type
Select the scanning type that will be used for this registry. [Enhanced scanning has additional pricing](#) [?](#)

☐ **Basic scanning**
Basic scanning allows manual scans and scan on push of images in this registry. This is a free service.

☒ **Enhanced scanning**
Enhanced scanning with Amazon Inspector provides automated continuous scanning. Inspector identifies vulnerabilities in both operating system and programming language (such as Python, Java, Ruby etc.) packages in real time.

Continuous scanning filters
Select which repositories will continuously have images scanned for vulnerabilities. Filters with no wildcard will match all repository names that contain the filter. Filters with wildcards (*) will match on a repository name where the wildcard replaces zero or more characters in the repository name.

☒ Continuously scan all repositories

[Cancel](#) [Save](#)

ECR SCANNING - ENHANCED SCANNING

When using Enhanced Scanning on a registry, each repository can be configured to use Continuous Scanning or Scan-on-Push



- ▶ Continuous Scanning monitors any change to either ECR images (on-push) or CVEs
- ▶ Images are scanned for up to 30 days after they are pushed.



- ▶ Scan-on-Push scans an image only when it is pushed to the repository, using the most up-to-date CVE data it has at the moment.

ECR SCANNING – ENHANCED SCANNING

The screenshot displays the AWS Inspector console interface. On the left is a navigation sidebar with sections for 'Findings' (including filters by vulnerability, instance, container image, repository, all findings, and suppression rules) and 'Settings' (including account management, general, and usage). A 'Switch to Inspector Classic' link is at the bottom of the sidebar.

The main content area shows the path 'Inspector > Findings > By container image' and the ARN of the scanned image. The image is identified as 'latest' with a container image SHA. Below this, a 'Details' section provides metadata: AWS account (111122223333), repository (scanrepo-prod), and image tag (latest). A 'Finding summary' indicates 6 Critical, 16 High, and 9 Medium findings.

The findings are categorized by layer. Under the 'By layer' tab, two layers are listed:

- Layer 0 (35)**: Contains 6 Critical, 16 High, and 8 Medium findings. The layer SHA is sha256:c9590bc36277863f3744423ef98f6d771897b9cf7b87bb1aa64fd7771337223.
- Layer 1 (1)**: Contains 0 Critical, 0 High, and 1 Medium finding. The layer SHA is sha256:5406a5a36f2e9ae83de049ba01a62d22ec32fac42ecbebe72fb5b030cb39a930.

Package Vulnerability findings for ECR Images include details regarding which image layer contains the vulnerability

- Dashboard
- Findings
 - By vulnerability
 - By account
 - By instance
 - By container image
 - By repository
 - All findings
- Suppression rules

- Settings
 - Account management
 - General
 - Usage

Switch to Inspector Classic

Account management

Manage your accounts, and review the coverage of your instances and repositories.

- Accounts
- Instances
- Repositories

Auto-enable scanning for new member accounts

☒ Automatically enable Inspector for all new member accounts

☒ EC2 scanning
Scan all EC2 instances for vulnerabilities

☒ ECR container scanning
Scan container images for vulnerabilities

Cancel

Save

My Organization (3)

Info

Refresh

Actions

Enable

Find accounts

<input type="checkbox"/>	Account number	Account name	Status	EC2 scanning	ECR container scanning
<input type="checkbox"/>			Enabled	Enabled	Enabled
<input type="checkbox"/>			Enabled	Enabled	Enabled
<input type="checkbox"/>			Enabled	Enabled	Enabled

Inspector

Dashboard

Findings

- By vulnerability
- By account
- By instance
- By container image
- By repository
- All findings
- Suppression rules

Settings

- Account management
- General
- Usage

Switch to Inspector Classic

Inspector > Dashboard

Summary

Viewing data from all accounts

Environment coverage

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

Accounts

100%

3 / 3 accounts

Instances

83%

5 / 6 instances

Repositories

100%

1 / 1 repository

Critical findings

All active critical findings in your environment.

ECR container

134

Critical

1277 total findings

EC2 Instance

2

Critical

1233 total findings

Network reachability

0

Critical

1 total finding

Risk based remediations

Vulnerabilities impacting the most instances and images.

Package name	Critical	All
openssl	16	93
libgd2	15	38
imagemagick	13	212
graphite2	12	51
curl	12	129

View all vulnerabilities

AWS accounts with most critical findings

Accounts with the most critical findings.

AWS account	Critical	All
	136	2511

Inspector

×

Dashboard

▼ Findings

By vulnerability

By account

By instance

By container image

By repository

All findings

Suppression rules

▼ Settings

Account management

General

Usage

Switch to Inspector Classic

Inspector > Settings > Account management > Instances

Account management

Manage your accounts, and review the coverage of your instances and repositories.

AccountsInstancesRepositories

All6

Scanning5

Not scanning1

Instances (6)

Info

🔄

🔍 ● Resource type EQUALS AWS EC2 Instance ⓘ Add filter

✕

< 1 >

EC2 instance	EC2 instance name	Account	AMI	Operating system	Status
I-0086541e745403d9c	--		ami-0e3533e9bd7f7b07a	LINUX	Scanning
I-074e6c5c955492e8b	--		ami-01cc5a4cf8a0ec059	UNKNOWN	Unmanaged Ec2 instance
I-0919a7def9924002c	--		ami-00d5e377dd7fad751	LINUX	Scanning
I-0b62b3416adb4ac14	--		ami-02ea8f348fa28c108	LINUX	Scanning
I-0ead3fdc1f11f53aa	--		ami-02ea8f348fa28c108	LINUX	Scanning
I-0ff9d19c794004b89	--		ami-02ea8f348fa28c108	LINUX	Scanning

Inspector

Dashboard

Findings

By vulnerability

By account

By instance

By container image

By repository

All findings

Suppression rules

Settings

Account management

General

Usage

Switch to Inspector Classic

Inspector > Findings

Findings: All findings

All findings ranked by severity.

By vulnerabilityBy accountBy instanceBy container imageBy repositoryAll findings

Findings (100+)

Choose a row to see the finding details.

ActiveResource ID EQUALS I-0ead3fdc1f11f53aaAdd filter

12345678...>

Severity	Title	Impacted resource
High	CVE-2020-12351 - kernel	I-0ead3fdc1f11f53aa
High	CVE-2020-28374 - kernel	I-0ead3fdc1f11f53aa
High	CVE-2019-18218 - file-libs, file	I-0ead3fdc1f11f53aa
High	CVE-2020-29661 - kernel	I-0ead3fdc1f11f53aa
High	CVE-2019-8912 - kernel	I-0ead3fdc1f11f53aa
High	CVE-2020-27815 - kernel	I-0ead3fdc1f11f53aa
High	CVE-2021-3653 - kernel	I-0ead3fdc1f11f53aa
High	CVE-2021-29154 - kernel	I-0ead3fdc1f11f53aa
High	CVE-2021-3347 - kernel	I-0ead3fdc1f11f53aa
High	CVE-2019-10142 - kernel	I-0ead3fdc1f11f53aa

CVE-2019-18218 - file-libs, file

cdf_read_property_info in cdf.c in file through 5.37 does not restrict the number of CDF_VECTOR elements, which allows a heap-based buffer overflow (4-byte out-of-bounds write).

Finding detailsInspector Score

CVSS v3 (REDHAT_CVE)

9.8

Inspector

8.4

The Inspector score is lower. Changed metrics: Attack Vector

CVSS score metrics

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



AWS Security Hub

Automate AWS security checks and centralize security alerts

HOW IT WORKS? – SECURITY POSTURE ASSESSMENT



AWS Security Hub

Quickly assess your high-priority security alerts and security posture across AWS accounts in one comprehensive view



Amazon GuardDuty



Amazon Macie



Amazon Inspector



AWS Firewall Manager



IAM Access Analyzer



AWS Systems Manager

Integrated APN solutions

Continuously aggregate & prioritize

Findings from AWS and partner security services highlight emerging trends or possible issues



Conduct automated security checks

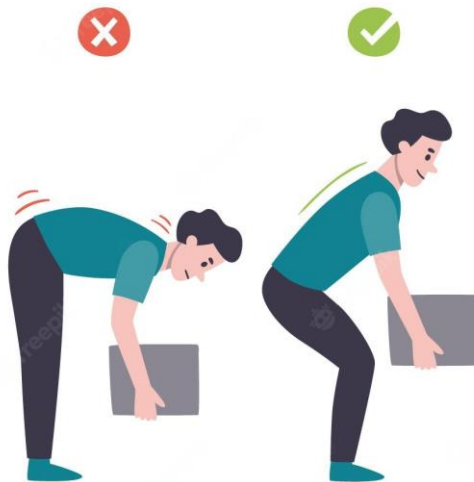
Use industry standards such as the CIS AWS Foundations Benchmark and PCI DSS



Take action

Investigate findings and/or take response and remediation actions

BAD POSTURE VS GOOD POSTURE



AUTOMATED SECURITY AND COMPLIANCE CHECKS

AWS Foundational Security Best Practices v1.0.0 by AWS

Description

The AWS Foundational Security Best Practices standard is a set of automated security checks that detect when AWS accounts and deployed resources do not align with security best practices. The standard is defined by AWS security experts. This curated set of controls helps improve your security posture in AWS, and covers AWS's most popular and foundational services.

Security score



Disable

View results

CIS AWS Foundations Benchmark v1.2.0 by AWS

Description

The Center for Internet Security (CIS) AWS Foundations Benchmark v1.2.0 is a set of security configuration best practices for AWS. This Security Hub standard automatically checks for your compliance readiness against a subset of CIS requirements.

Security score



Disable

View results

PCI DSS v3.2.1 by AWS

Description

The Payment Card Industry Data Security Standard (PCI DSS) v3.2.1 is an information security standard for entities that store, process, and/or transmit cardholder data. This Security Hub standard automatically checks for your compliance readiness against a subset of PCI DSS requirements.

Security score



Disable

View results

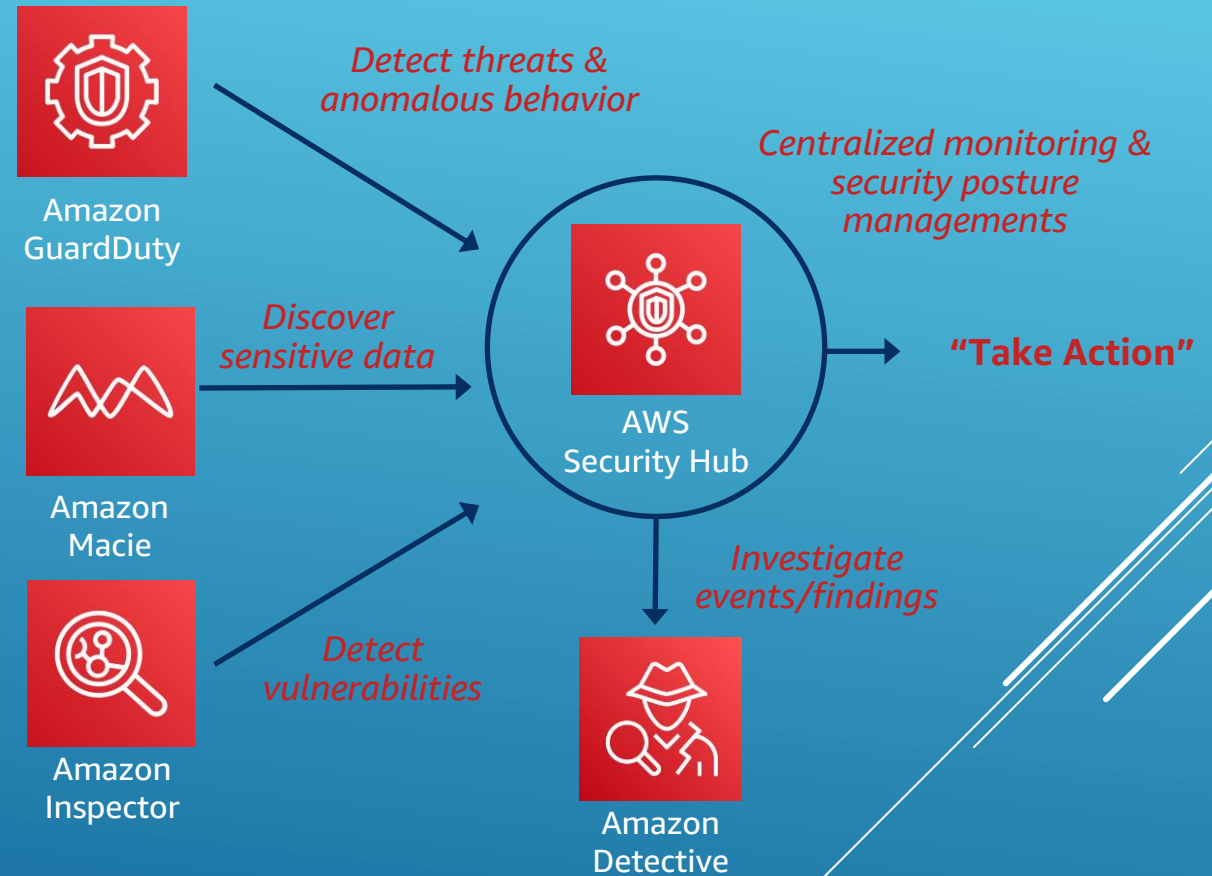


- ▶ 200+ fully automated, nearly continuous checks evaluated against preconfigured rules
- ▶ Findings are displayed on main dashboard for quick access
- ▶ Best practices information is provided to help mitigate gaps and be in compliance

SECURITY FINDING FLOWS



Security Hub checks results



SECURITY HUB INSIGHTS

1. AWS resources with the most findings

Security Hub managed insight



2. S3 buckets with public write or read permissions

Security Hub managed insight



3. AMIs that are generating the most findings

Security Hub managed insight



4. EC2 instances involved in known Tactics, Techniques, and Procedures (TTPs)

Security Hub managed insight



5. AWS principals with suspicious access key activity

Security Hub managed insight




6. AWS resources instances that don't meet security standards / best practices

Security Hub managed insight



EXTRAS – ADDED INTEGRATION WITH AWS HEALTH AND AWS TRUSTED ADVISOR

- AWS Health uses service-to-service event messaging to send findings to Security Hub.
- Trusted Advisor sends the results of its checks to Security Hub as Security Hub findings. Security Hub sends the results of its AWS Foundational Security Best Practices checks to Trusted Advisor.



AWS: Health

Description
AWS Health provides ongoing visibility into your resource performance and the availability of your AWS services and accounts. You can use AWS Health events to learn how service and resource changes might affect your applications running on AWS.


Type of integration
Sends findings to Security Hub

Categories
Software and Configuration Checks

How to receive findings from this integration
The integration is automatically enabled when you enable the service. No other configuration besides turning on the service is required. [Go to service homepage](#)

Status
✔ Accepting findings. [See findings](#)

[Stop accepting findings](#)



AWS: Trusted Advisor

Description
AWS Trusted Advisor provides recommendations that help you follow AWS best practices, optimize your AWS infrastructure, improve security and performance, reduce costs, and monitor service quotas

Type of integration
Receives findings from Security Hub

Categories
Cloud Compliance and Best Practices Checks

How to send findings to this integration
The integration is automatically enabled when you enable the service. No other configuration besides turning on the service is required. [Go to service homepage](#)

Status
After you follow the configuration instructions, Security Hub automatically sends findings to this service.



DEMO