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

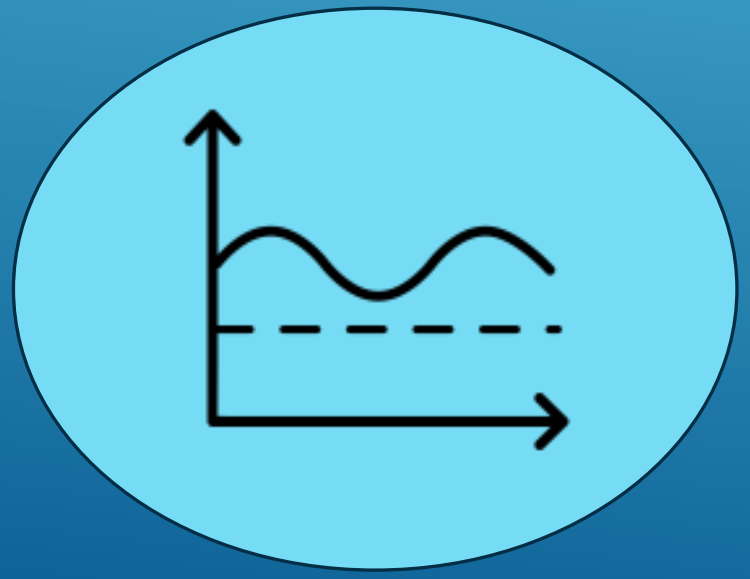
Burglary/Theft

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	Detect	Infrastructure protection	Data protection	Respond
AWS Identity and Access Management (IAM)	AWS Security Hub	AWS Systems Manager	AWS Key Management Service (AWS KMS)	AWS Config rules
AWS Single Sign-On	Amazon GuardDuty	AWS Shield	AWS CloudHSM	AWS Lambda
AWS Directory Service	Amazon Detective	AWS WAF (web application firewall)	AWS Certificate Manager (ACM)	Systems Manager
Amazon Cognito	AWS CloudTrail	AWS Firewall Manager	Amazon Macie	
AWS Organizations	Amazon CloudWatch	Amazon Inspector	Server-side encryption	
AWS Secrets Manager	Amazon VPC flow logs	Amazon VPC		
AWS Resource Access Manager (AWS RAM)	AWS Config			
	Amazon Inspector			

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:

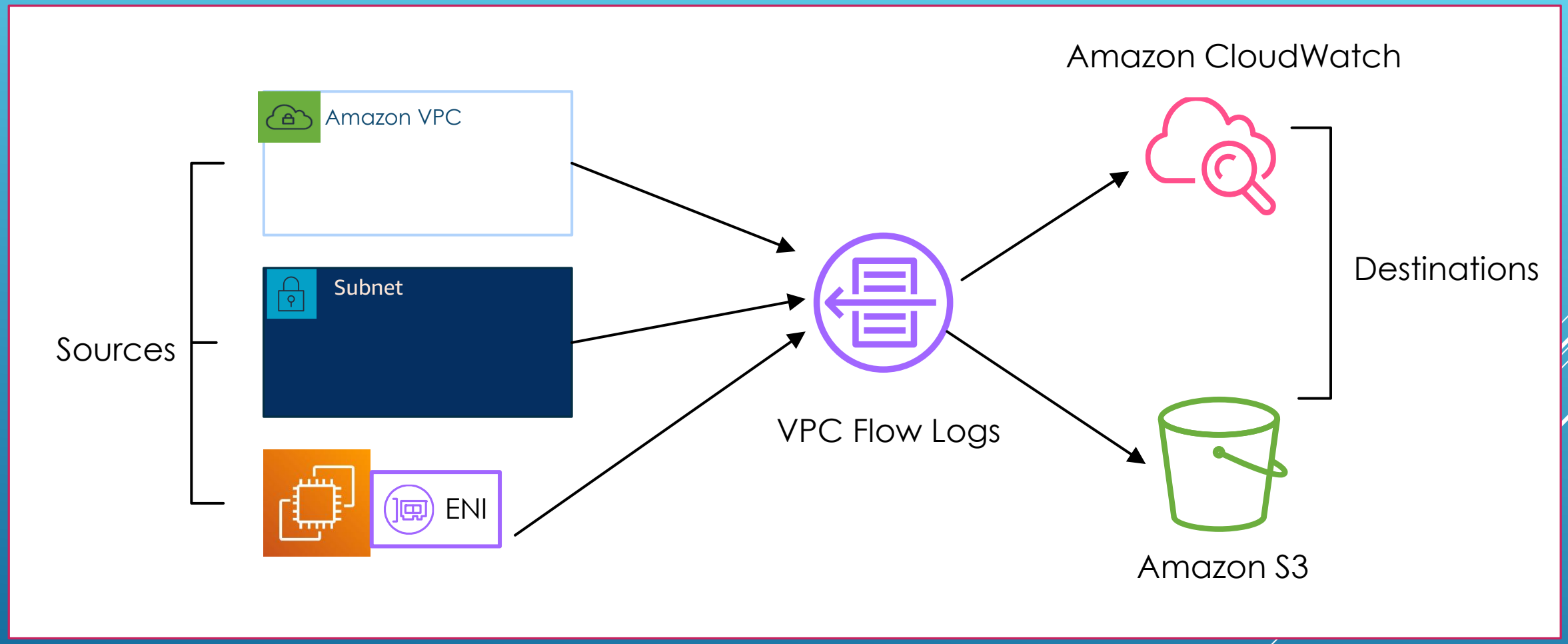
- AWS Console sign-In requests without MFA
- IAM policy configuration changes
- Root account usage
- Authorization failures; unauthorized API calls made within your AWS account
- AWS KMS key configuration changes
- AWS CloudTrail configuration changes
- AWS EC2 instance and S3 changes
- AWS VPC, Route 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 13 24 15

Findings Info

Actions

Suppress Findings Info

Saved rules Apply saved rules

Current Add filter criteria

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

Data sources

VPC flow logs

DNS logs

CloudTrail events

S3 data plane events

EKS control plane logs

Threat detection types

Finding types
Examples

Threat intelligence

Bitcoin mining

Command and control activity

Anomaly detection (ML)

Unusual user behavior
Examples
- Launch instance
- Change network permissions

Unusual traffic patterns
Example: Unusual ports and volume

Findings

High

Medium

Low

Amazon EventBridge
- Alert
- Remediate
- Partner solutions
- Send to SIEM

AWS Security Hub

Amazon Detective

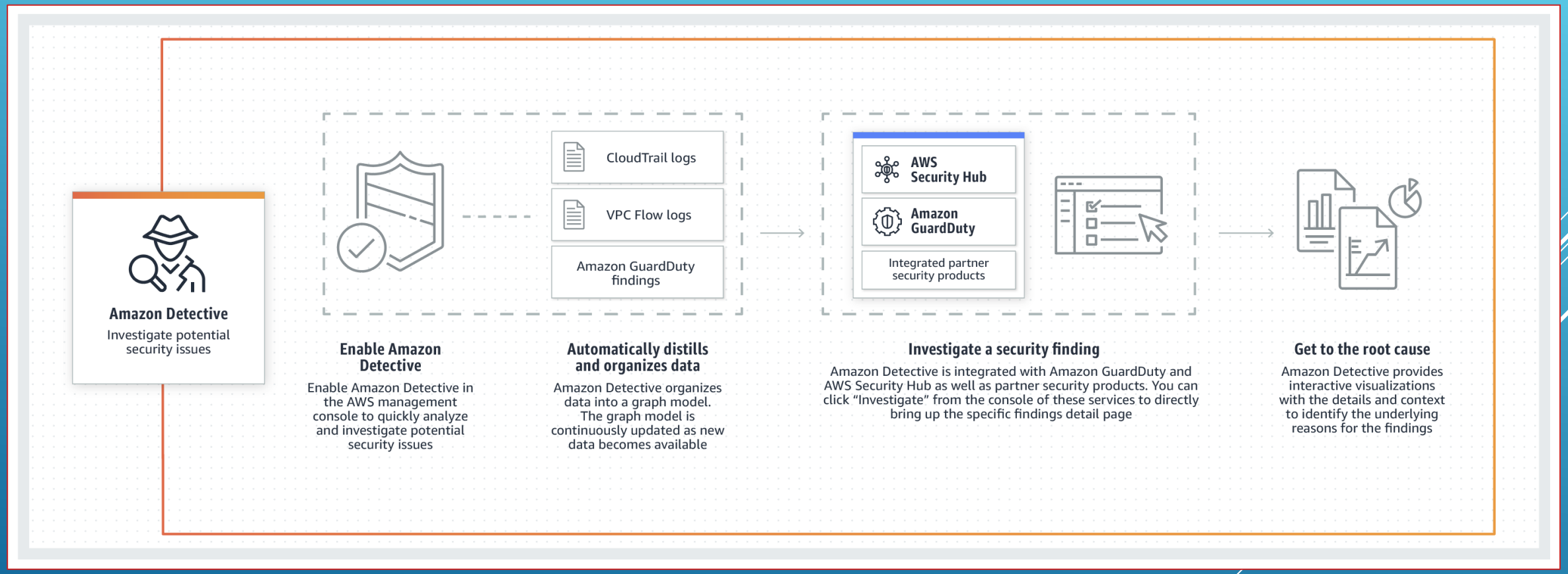
Amazon Detective

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

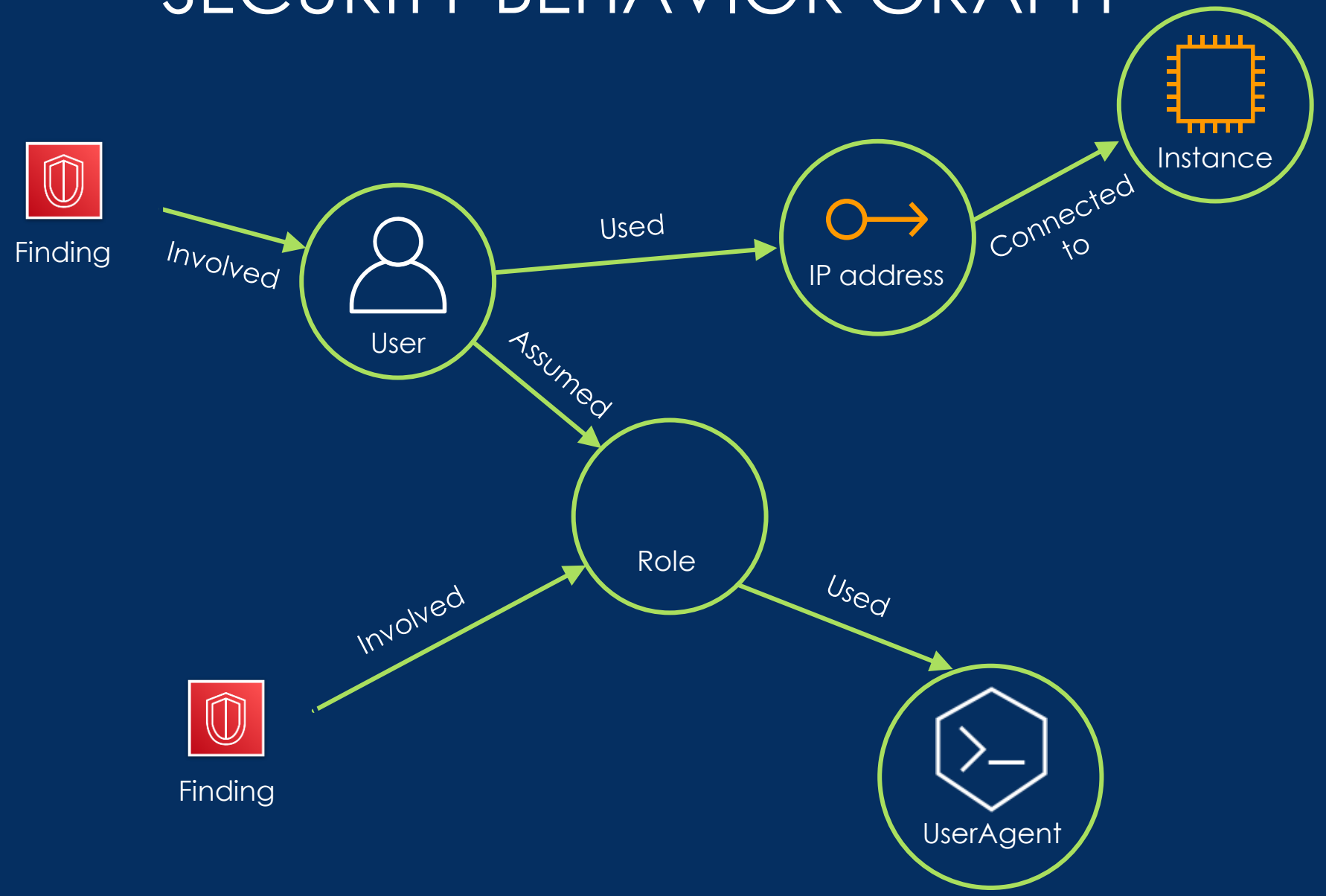

House robbery
Victim N2
blood on the floor
What was in bag
WHO IS HE!?
1 case
Was There
Buy coffee!
NEW VICTIM
No clue
NAME
OH
HI
MARK
CRIME
HOMICIDE
LOCATION
LONDON

Who done it???

AMAZON DETECTIVE - HOW IT WORKS



SECURITY BEHAVIOR GRAPH

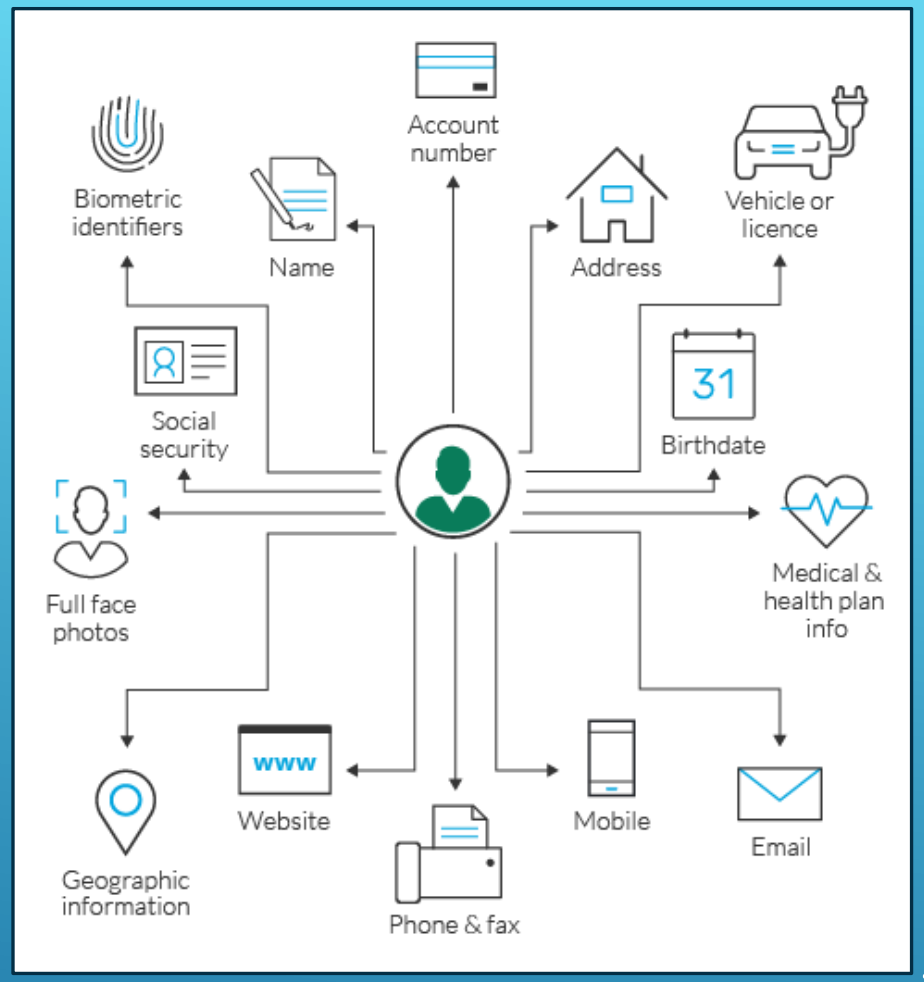


EXTRAS - **AMAZON DETECTIVE NOW SUPPORTS GUARDDUTY FINDINGS RELATED TO S3 AND DNS**

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?

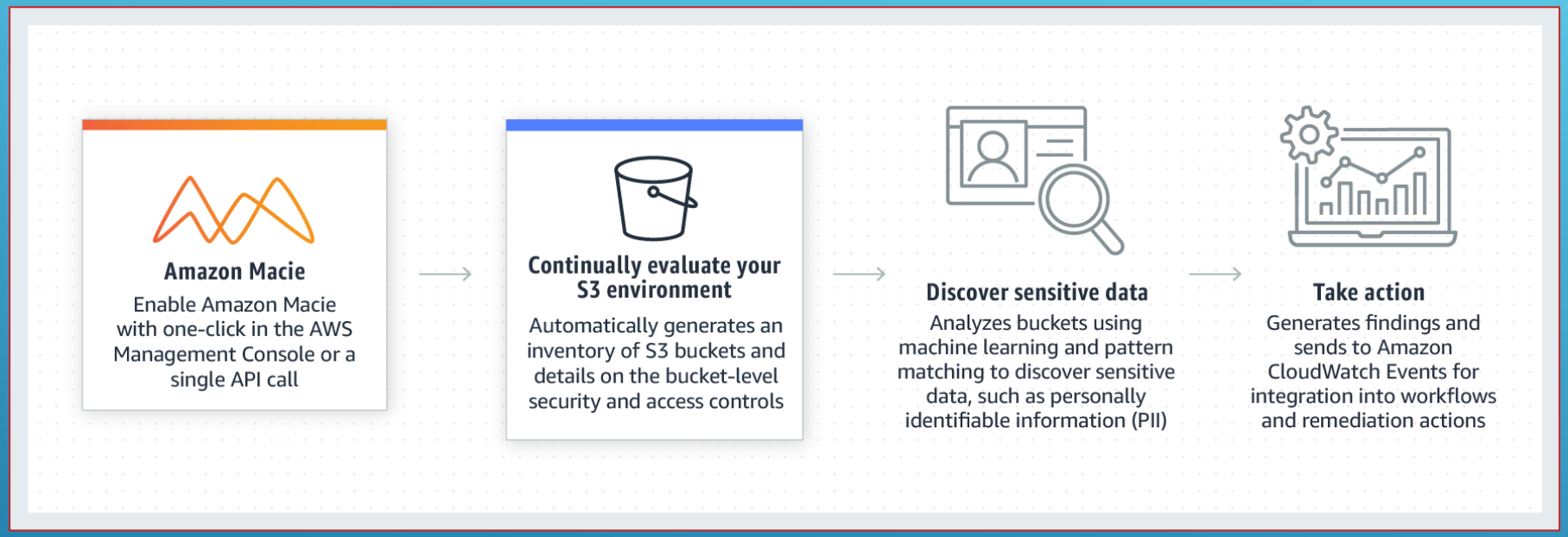
Also for those DNS-related findings you can deep dive on those related to low-reputation domain names (such as those associated with cryptocurrency-related activities) and algorithmically-generated domains.



Amazon Macie

Discover and protect your sensitive data

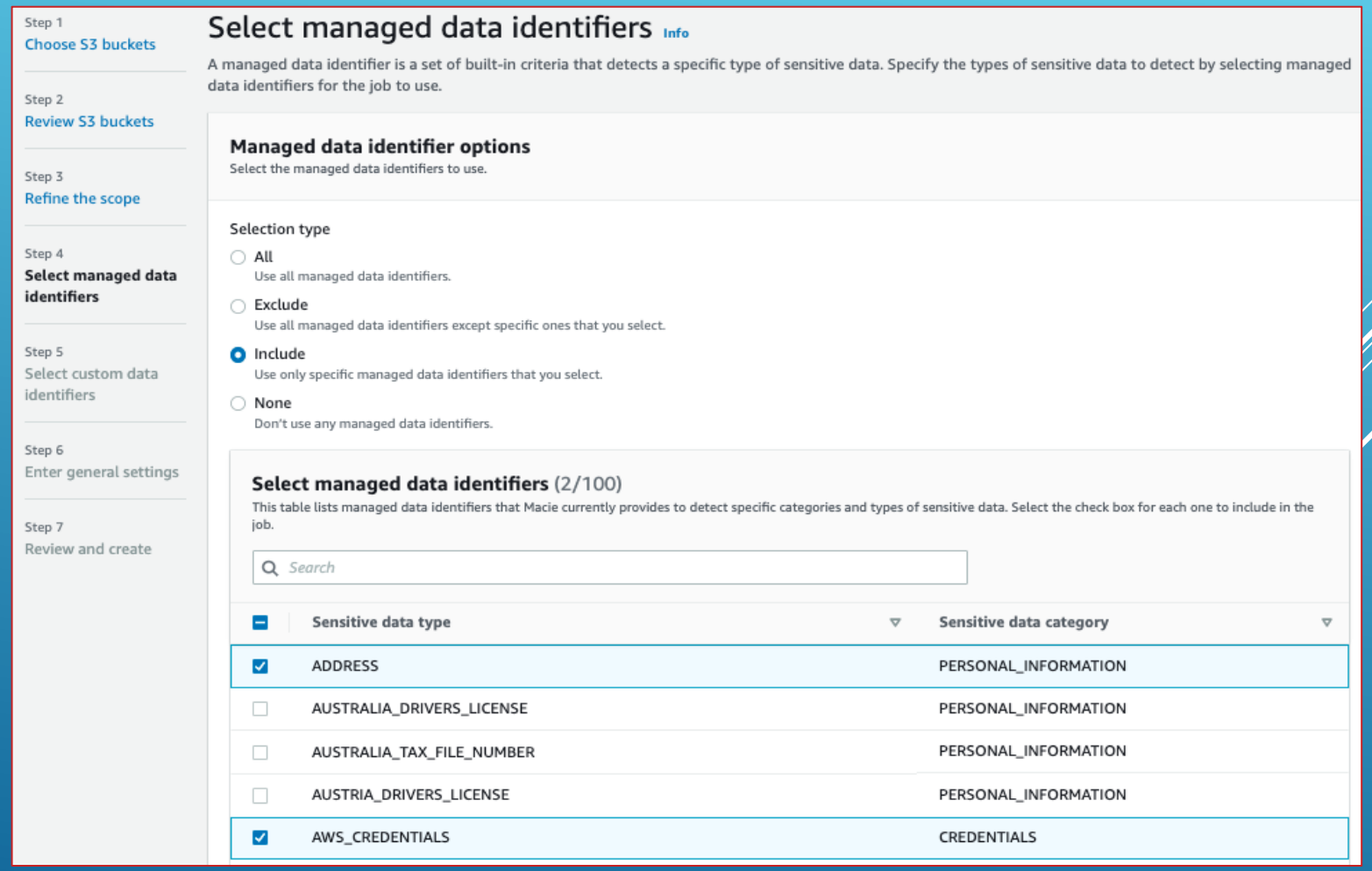
AMAZON MACIE - HOW IT WORKS



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.



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

Full names

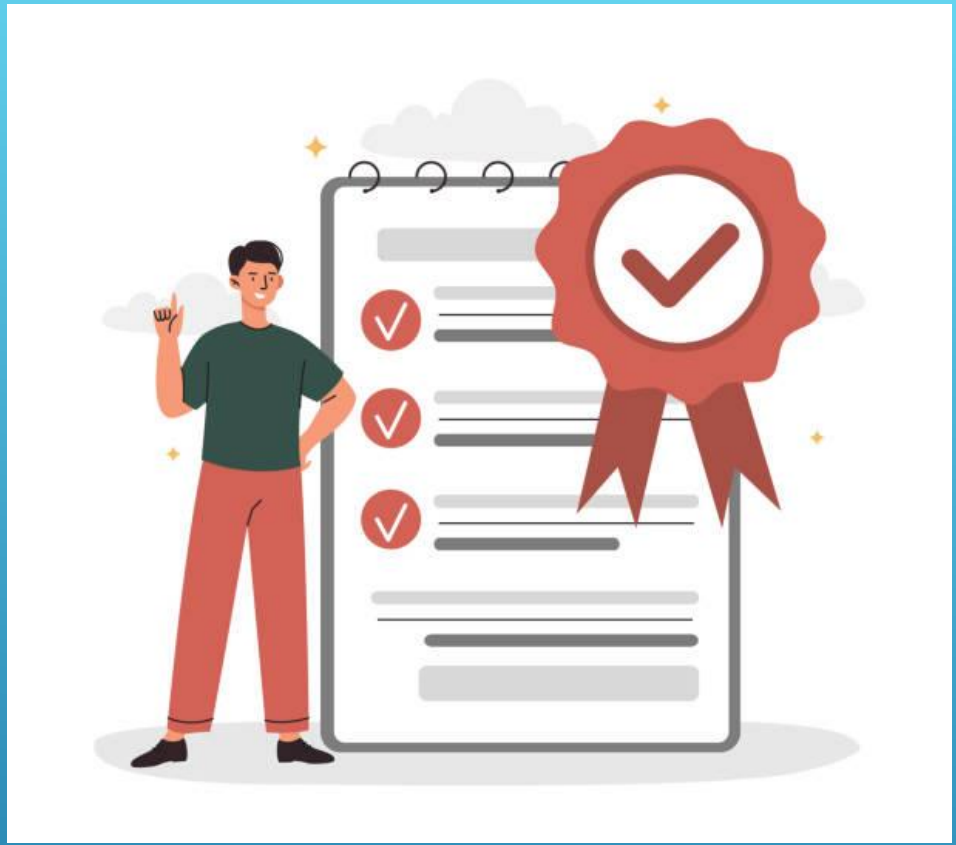
The updated model extracts additional context from file headers and attributes to better inform detection and reporting of full names.

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

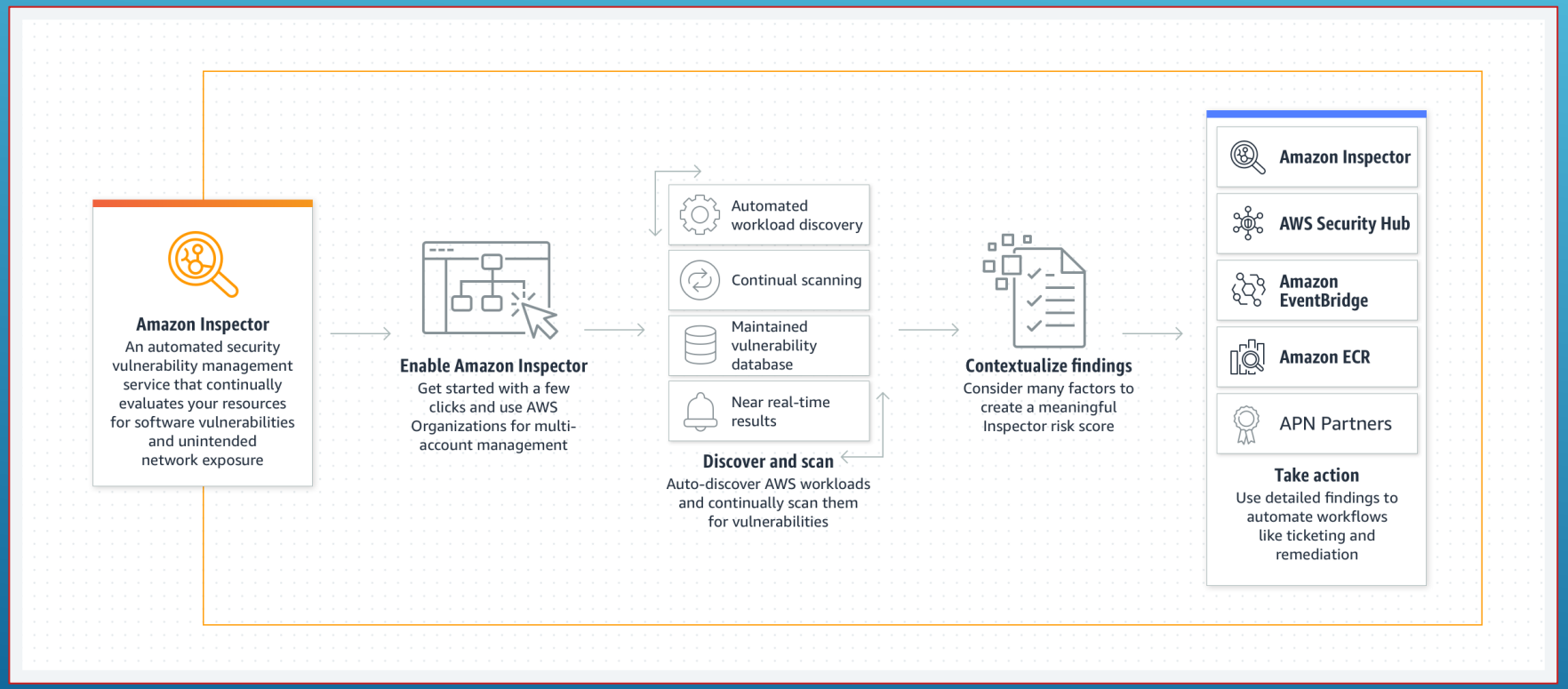
The updated model uses additional checks to validate city names, ZIP codes, and Postal Codes to produce more actionable results.



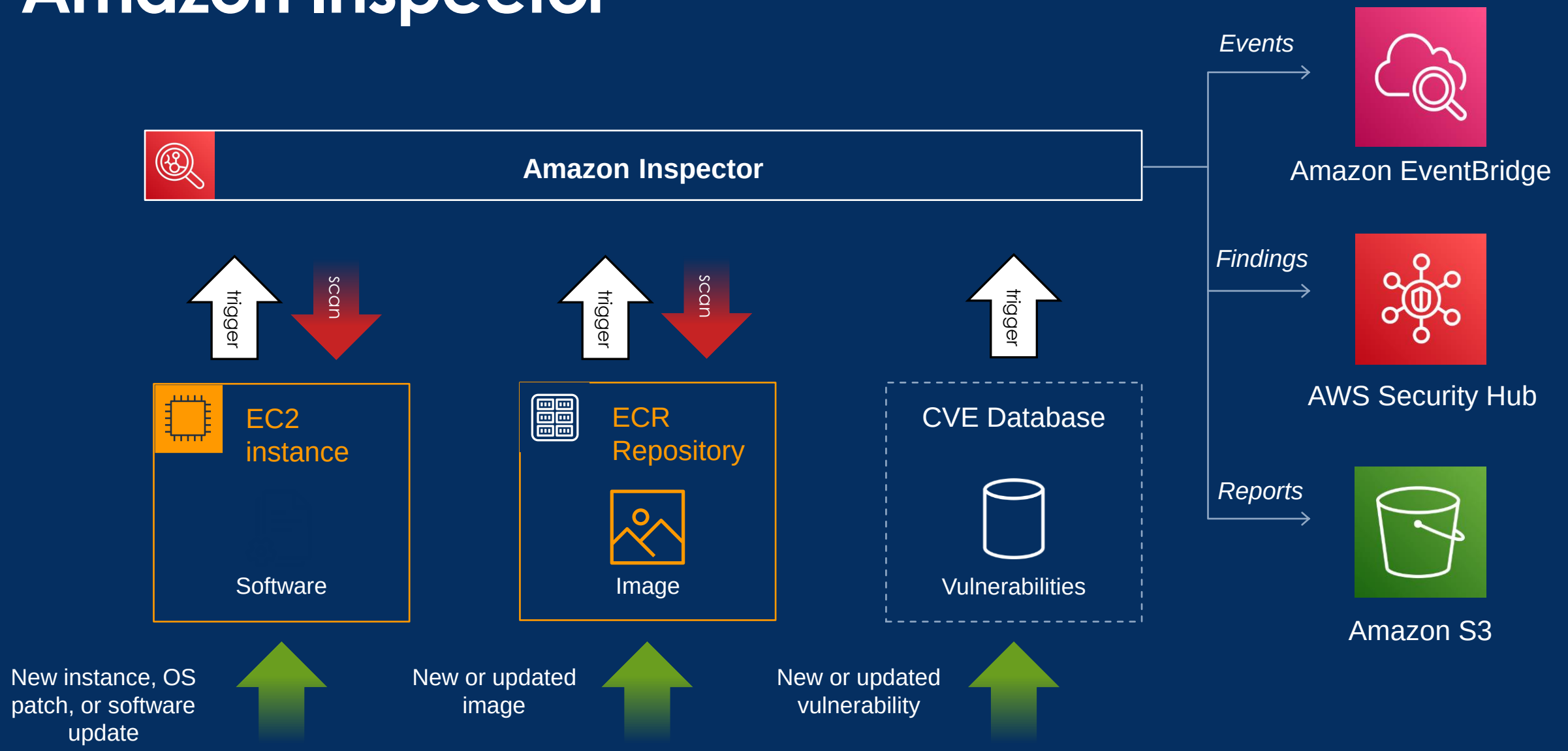
Amazon Inspector

Automated and continual vulnerability management

AMAZON INSPECTOR - HOW IT WORKS



Amazon Inspector



EC2 scanning

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

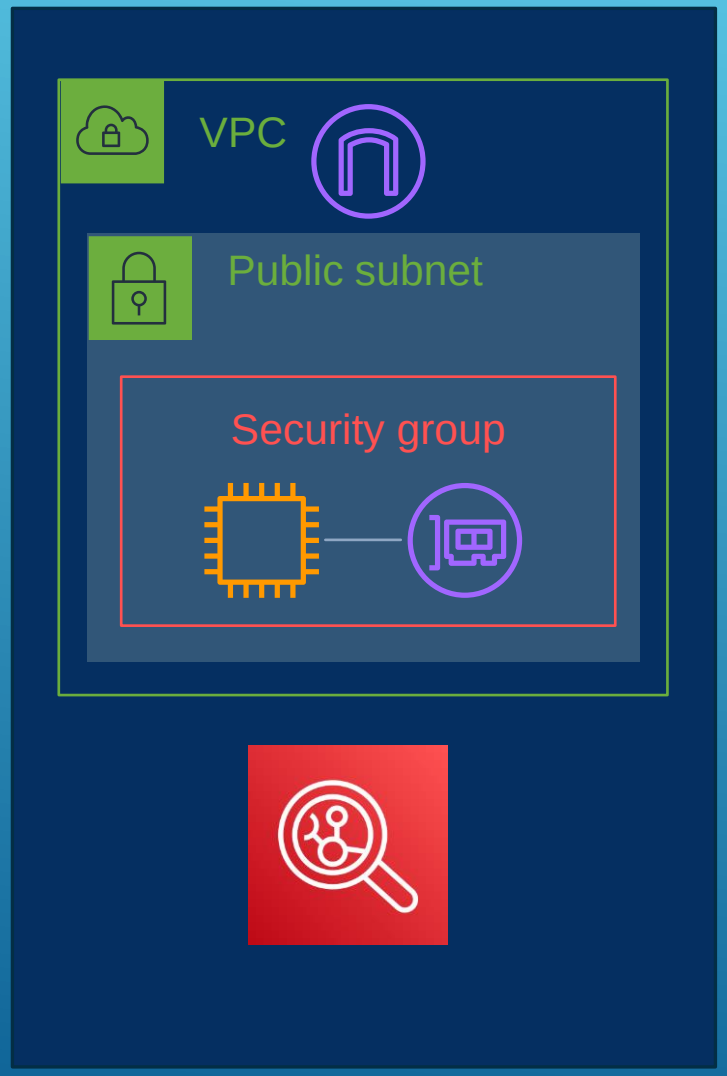
- **Network reachability scanning**

Does not require any agent to be installed

- **Package vulnerability scanning**

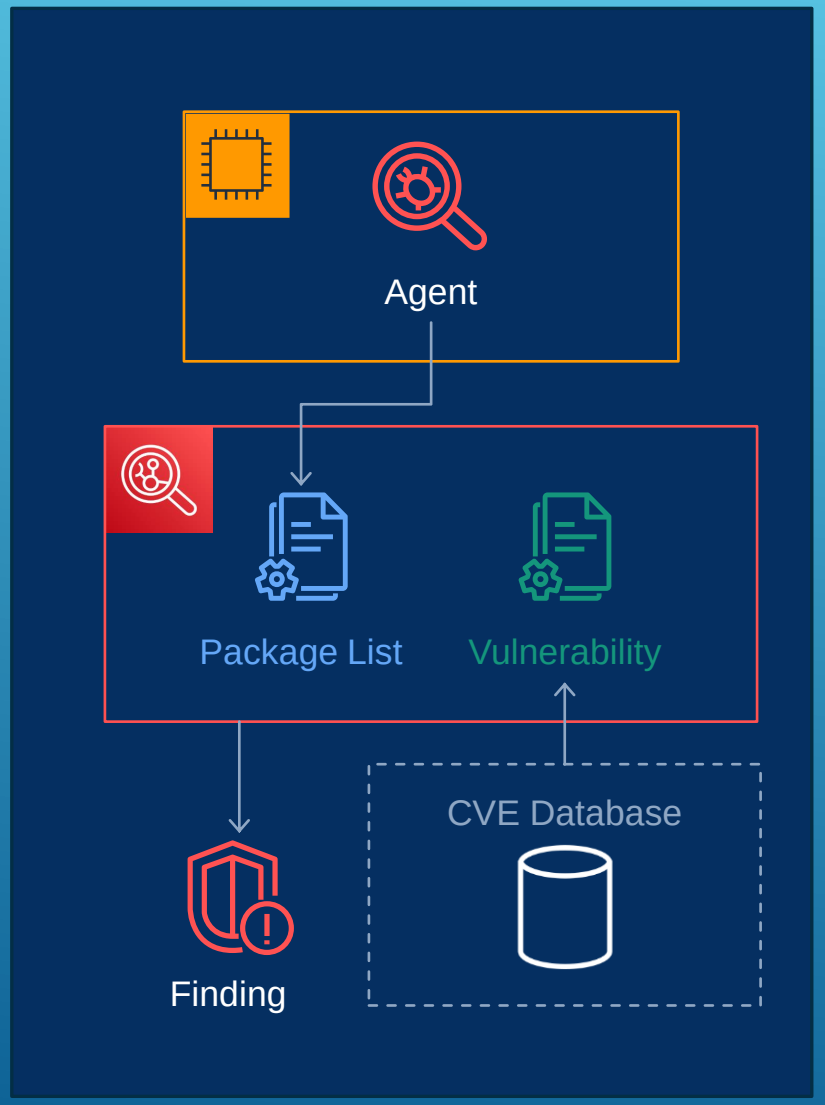
Requires the SSM agent installed on the instance

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.

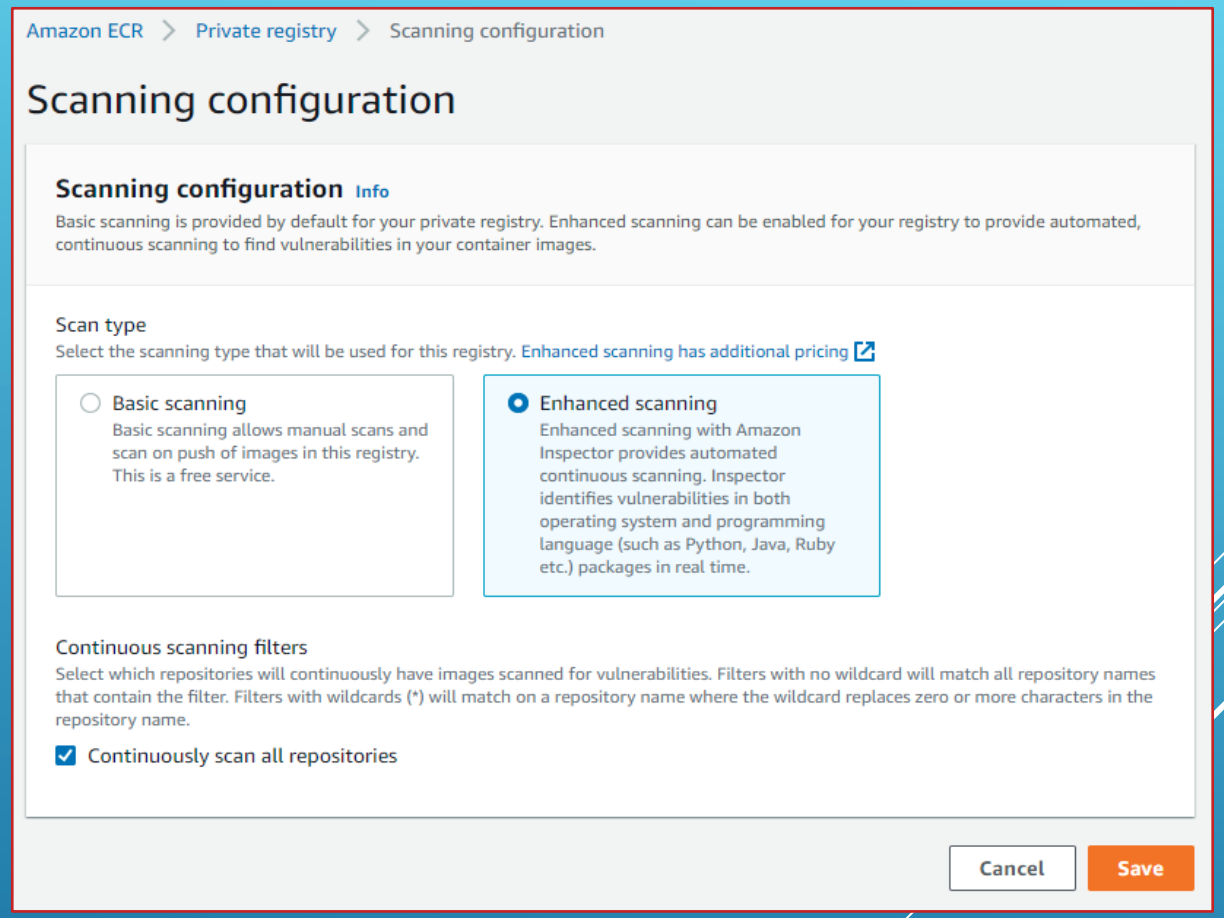
EC2 SCANNING - PACKAGE VULNERABILITY



- 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

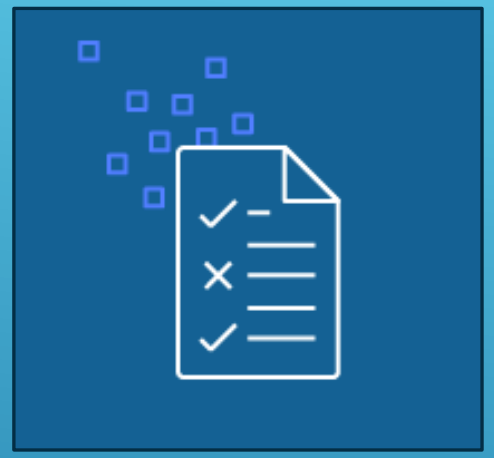
When Inspector is enabled, Enhanced Scanning becomes the default scan type for all ECR registries, but can be changed back to Basic Scanning afterwards.



ECR SCANNING - ENHANCED SCANNING

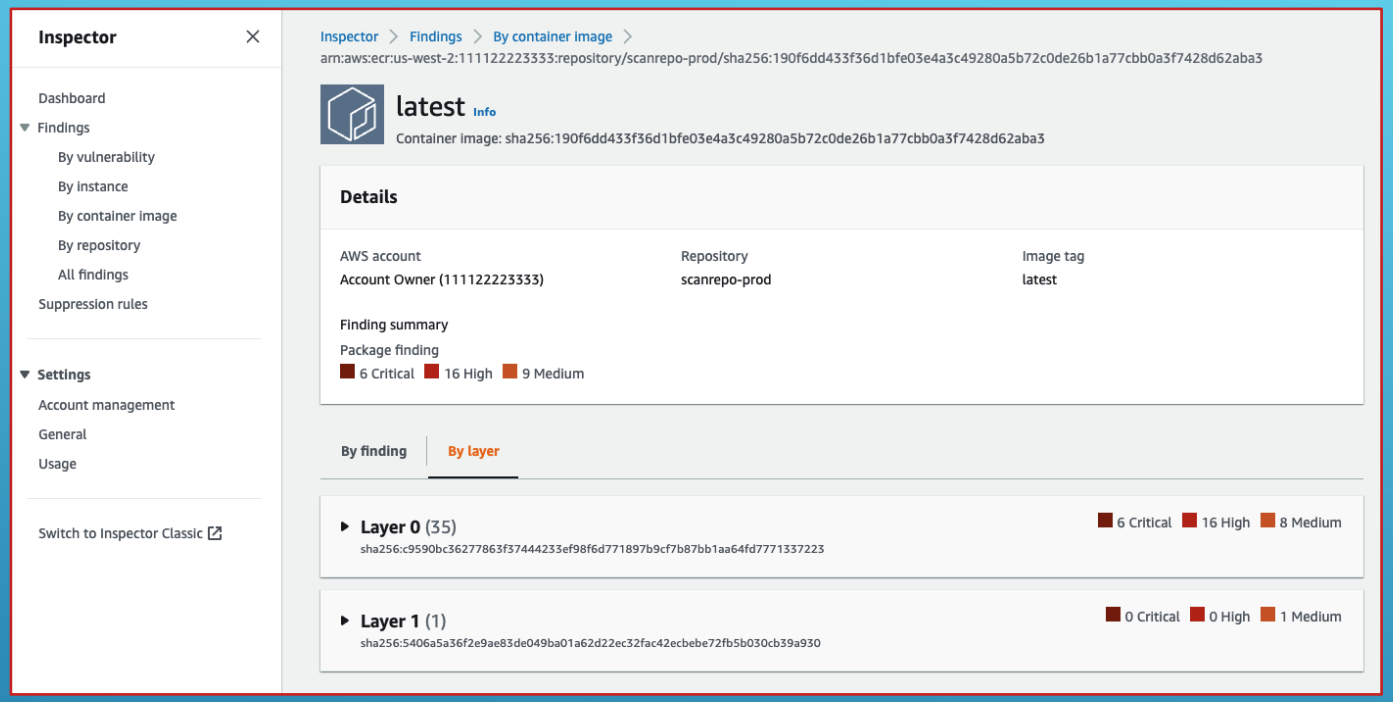
When using Enhanced Scanning on a registry, each repository can be configured to use Continuous Scanning or Scan-on-Push

- 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



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

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

Account management Info

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

- [x] EC2 scanning
  Scan all EC2 instances for vulnerabilities
- [x] ECR container scanning
  Scan container images for vulnerabilities

Cancel | Save

My Organization (3) Info

Actions | Enable

Find accounts

1

Account number	Account name	Status	EC2 scanning	ECR container scanning
[illegible]	[illegible]	Enabled	Enabled	Enabled
[illegible]	[illegible]	Enabled	Enabled	Enabled
[illegible]	[illegible]	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 Info

Viewing data from all accounts

All

Environment coverage

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

Accounts	Instances	Repositories
100%	83%	100%
3 / 3 accounts	5 / 6 instances	1 / 1 repository

Critical findings

All active critical findings in your environment.

ECR container	EC2 instance	Network reachability
134 Critical	2 Critical	0 Critical
1277 total findings	1233 total findings	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
[illegible]	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 Info

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

Accounts | Instances | Repositories

All	Scanning	Not scanning
6	5	1

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 Info

All findings ranked by severity.

By vulnerability | By account | By instance | By container image | By repository | All findings

Findings (100+)

Choose a row to see the finding details.

Export findings | Create suppression rule

Active | Resource ID EQUALS i-0ead3fdc1f11f53aa | Add filter

1 2 3 4 5 6 7 8 ...

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 details | Inspector Score

CVSS v3 (REDHAT_CVE)	Inspector
9.8	8.4

The Inspector score is **lower.** Changed metrics: Attack Vector

CVSS score metrics

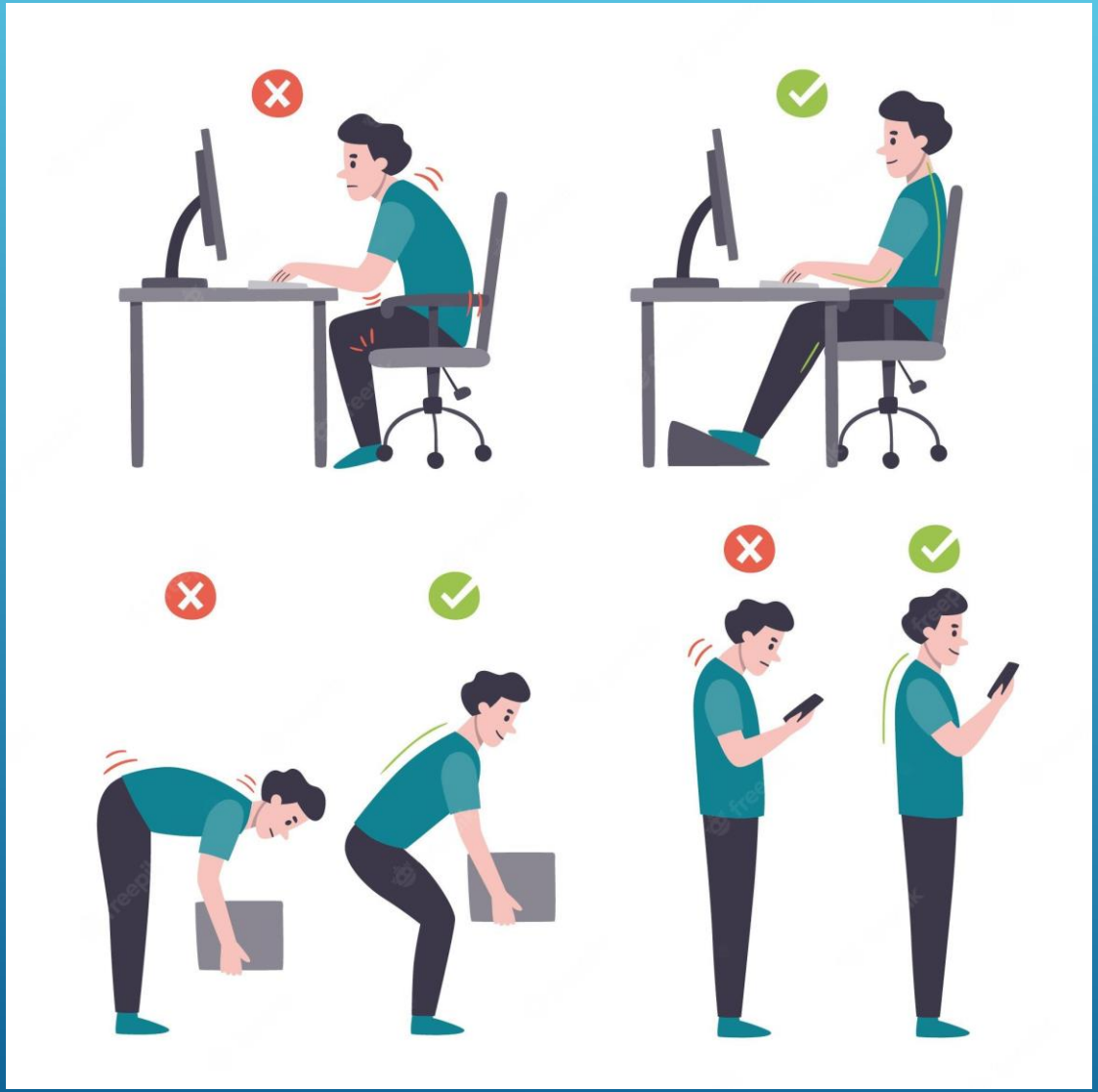
Metric	CVSS	Inspector
Attack Vector	Network	Local
Attack Complexity	Low	Low
Privileges Required	None	None
User Interaction	None	None
Scope	Unchanged	Unchanged
Confidentiality	High	High
Integrity	High	High
Availability	High	High

AWS Security Hub

Automate AWS security checks and centralize security alerts

HOW IT WORKS? – SECURITY POSTURE ASSESSMENT

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
64%
Updated 6 hours ago

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
17%
Updated 6 hours ago

Disable | View results

PCI DSS v3.2.1 by AWS

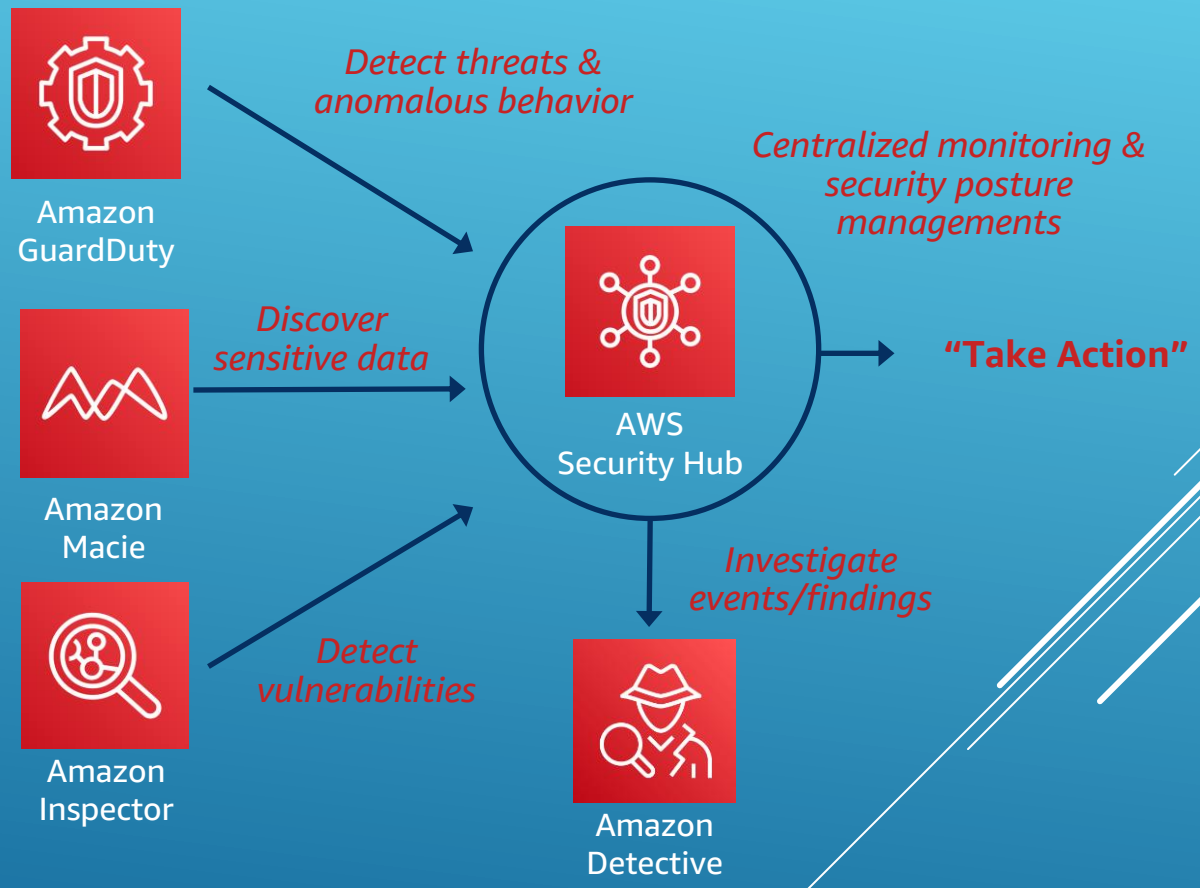
Description
The Payment Card Industry Data Security Standard (PCI DSS) v3.2.1 is an information security standard for entities that store, process, and/or transmit cardholder data. This Security Hub standard automatically checks for your compliance readiness against a subset of PCI DSS requirements.

Security score
53%
Updated 6 hours ago

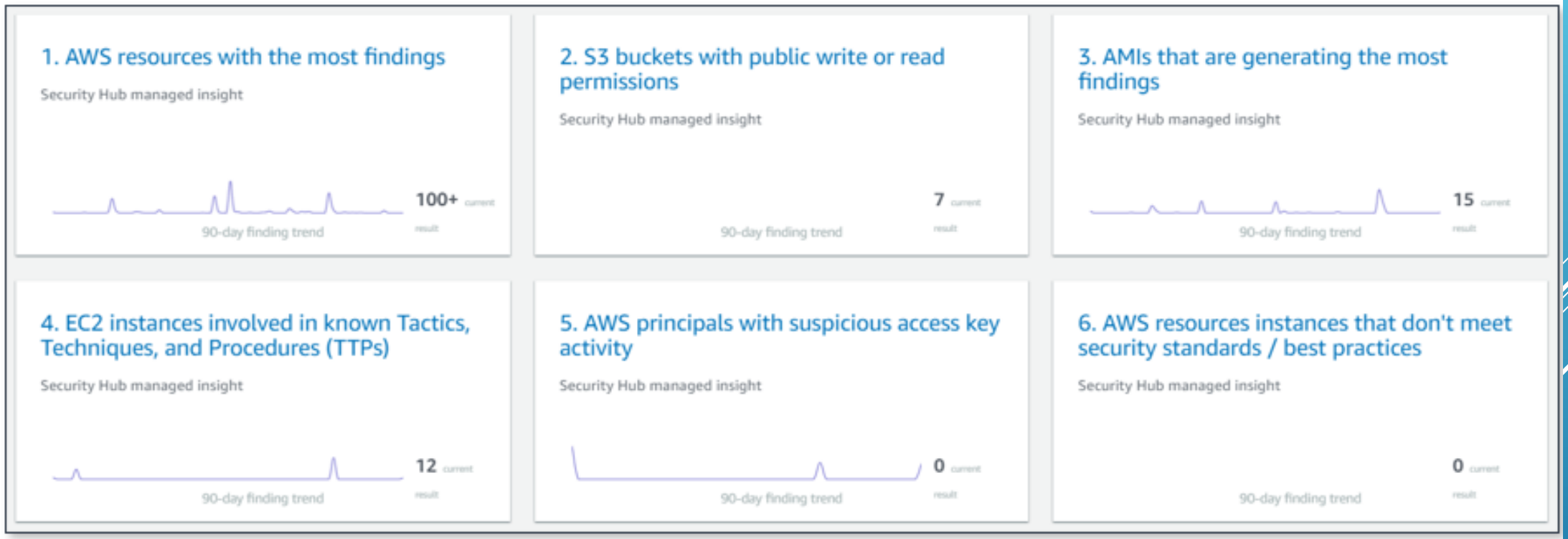
Disable | View results

- 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

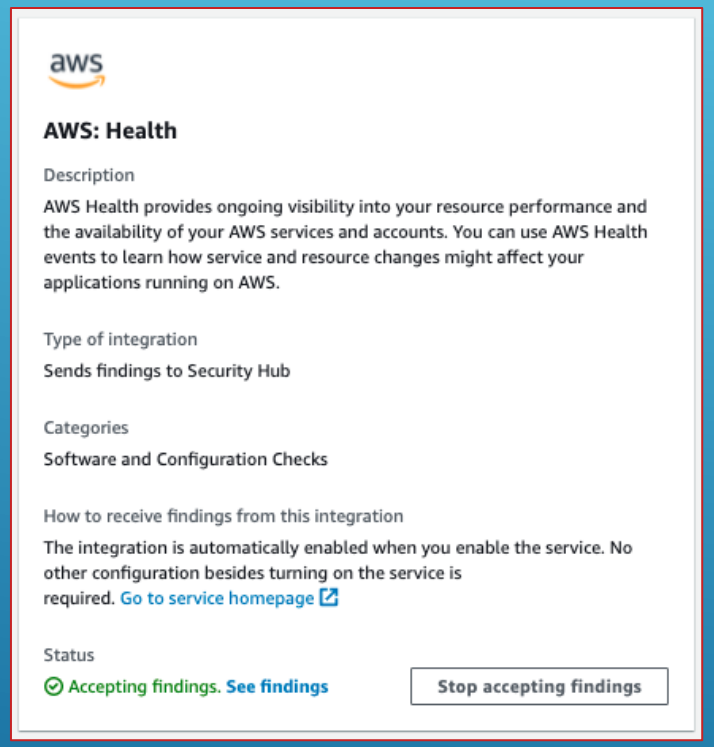


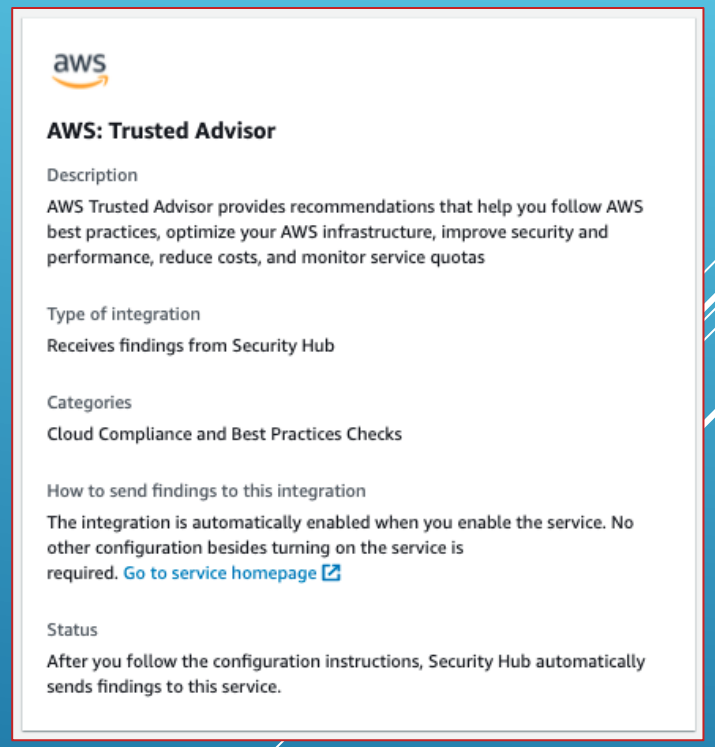
SECURITY HUB INSIGHTS



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.





DEMO