aws SUMMIT

LONDON | APRIL 27, 2022

SE-05

Threat detection & remediation in the Cloud

Rodrigo Ferroni

STAM - Security Specialist

AWS

Agenda

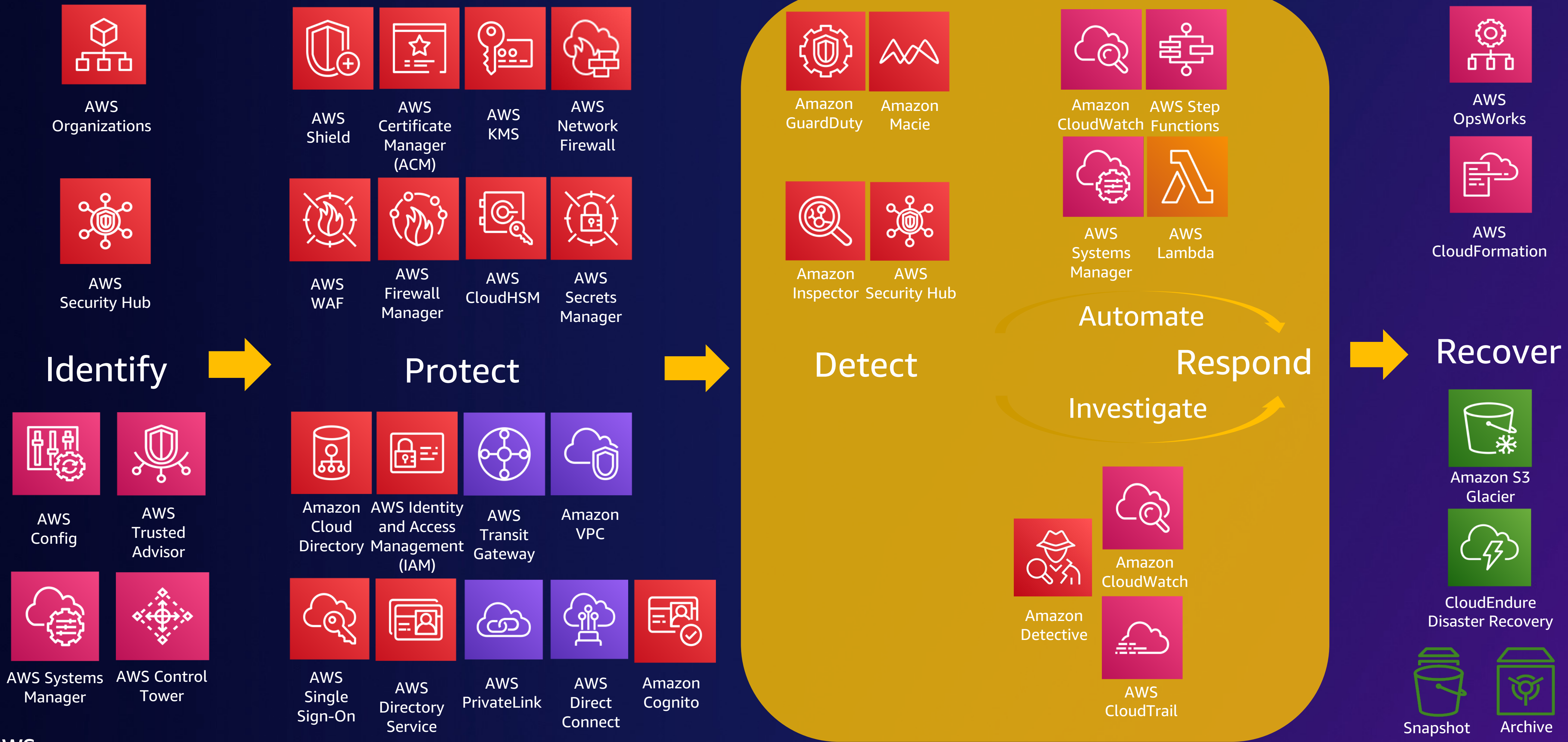
AWS layered security services portfolio

Security across multiple accounts and regions

Threat detection and remediation using native AWS security services – What's New

Demo

AWS foundational and layered security services



Identify

AWS Organizations

AWS Security Hub

AWS Config

AWS Trusted Advisor

AWS Systems Manager

AWS Control Tower

Protect

AWS Shield

AWS Certificate Manager (ACM)

AWS KMS

AWS Network Firewall

AWS WAF

AWS Firewall Manager

AWS CloudHSM

AWS Secrets Manager

Amazon Cloud Directory

AWS Identity and Access Management (IAM)

AWS Transit Gateway

Amazon VPC

AWS Single Sign-On

AWS Directory Service

AWS PrivateLink

AWS Direct Connect

Amazon Cognito

Detect

Amazon GuardDuty

Amazon Macie

Amazon Inspector

AWS Security Hub

Respond

Automate

Investigate

Amazon CloudWatch

AWS Step Functions

AWS Systems Manager

AWS Lambda

Amazon Detective

Amazon CloudWatch

AWS CloudTrail

Recover

AWS OpsWorks

AWS CloudFormation

Amazon S3 Glacier

CloudEndure Disaster Recovery

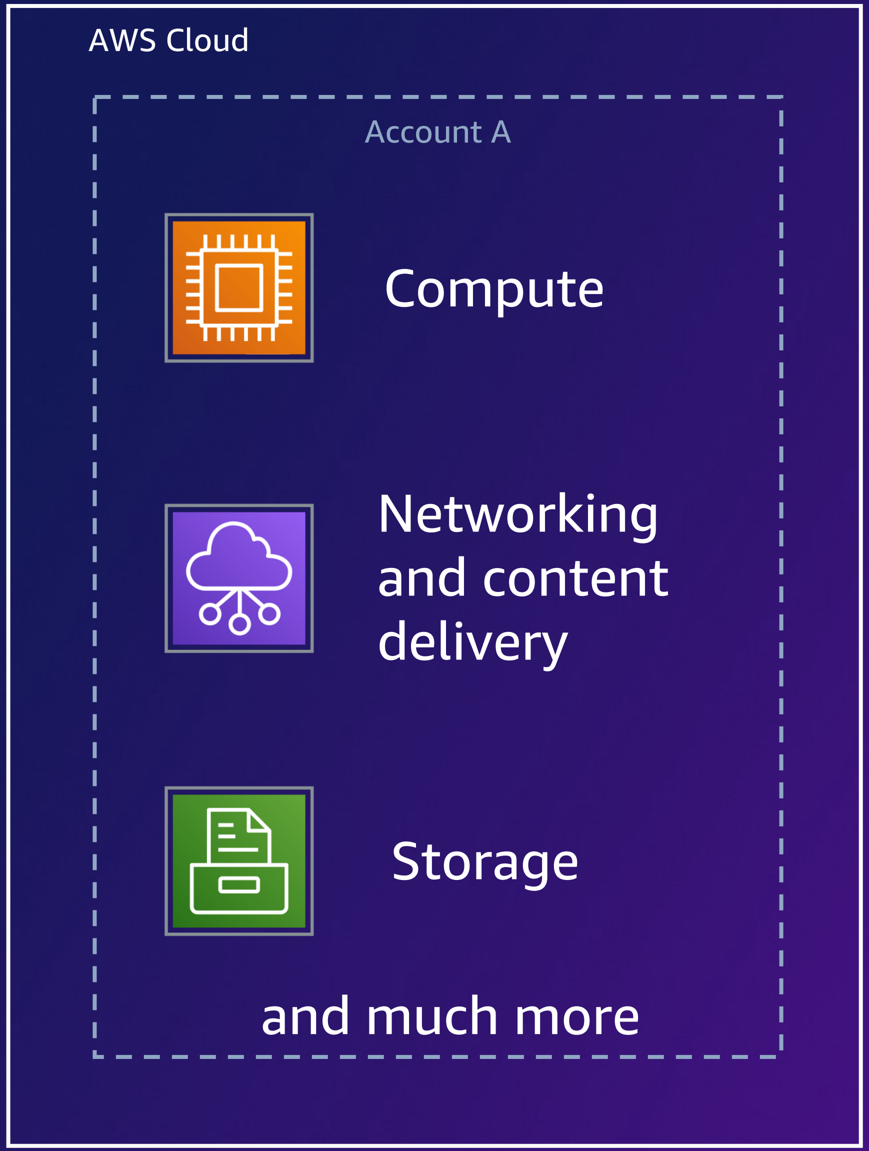
Snapshot

Archive

Understanding an AWS account

- Each AWS account
  - Is a resource container for AWS cloud services
  - Is an explicit security boundary

- Over time, customers will add more accounts to support more applications and services



AWS Cloud

Account A

Compute

Networking and content delivery

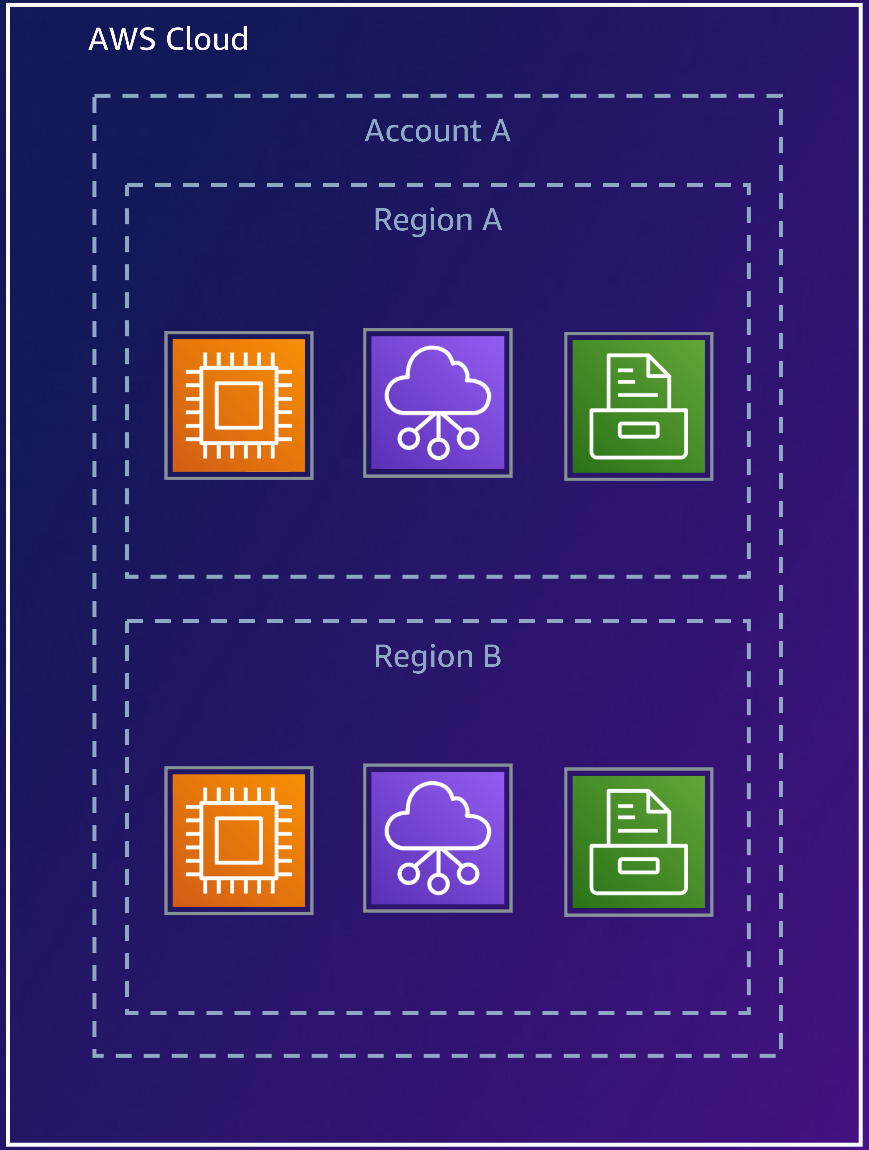
Storage

and much more

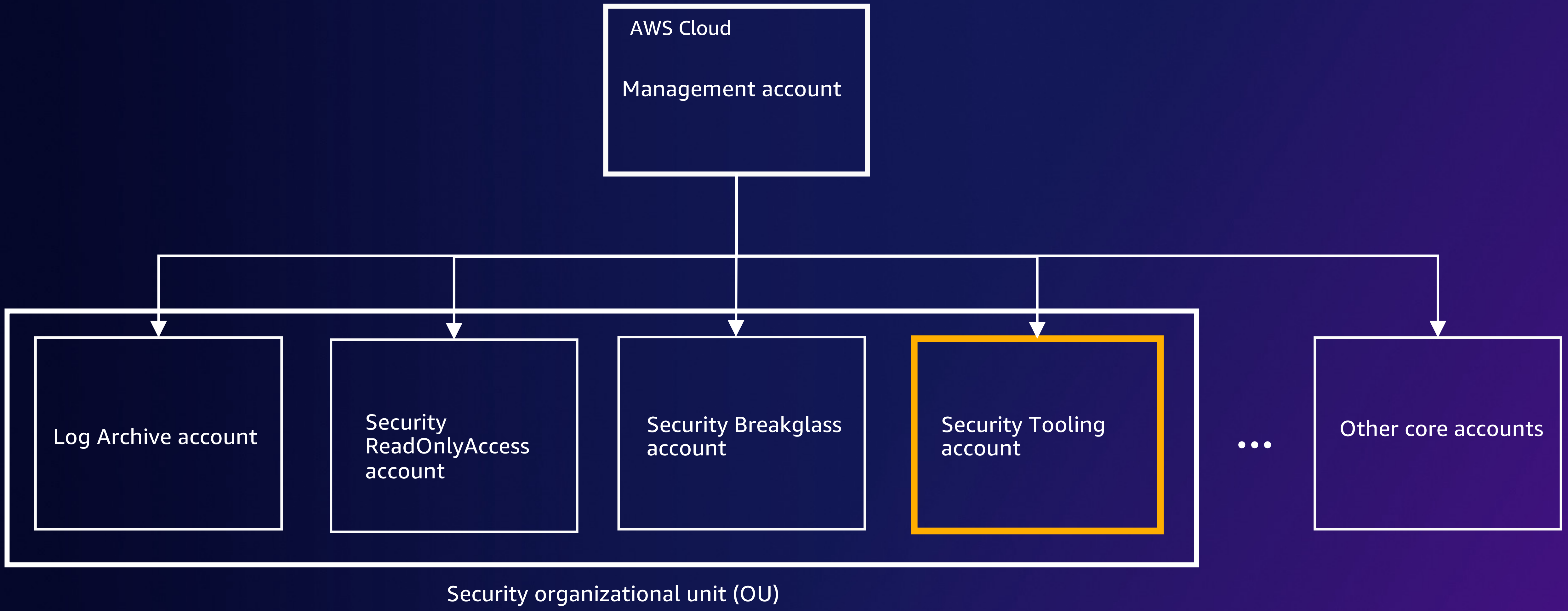
Understanding an AWS region

- Each AWS region
  - Is a resource container for AWS cloud services
  - Is an explicit security boundary

- Over time, customers can opt to split workloads across multiple AWS regions



Security organizational unit: Multi-account strategy



Threat detection and remediation using native AWS security services

Amazon **GuardDuty**

Amazon **Detective**

Amazon **Macie**

Amazon **Inspector**

AWS **Security Hub**

What’s New - Scalable and centralized management

Administrator/member setup

Designate a centralized delegated administrator

Add all member accounts

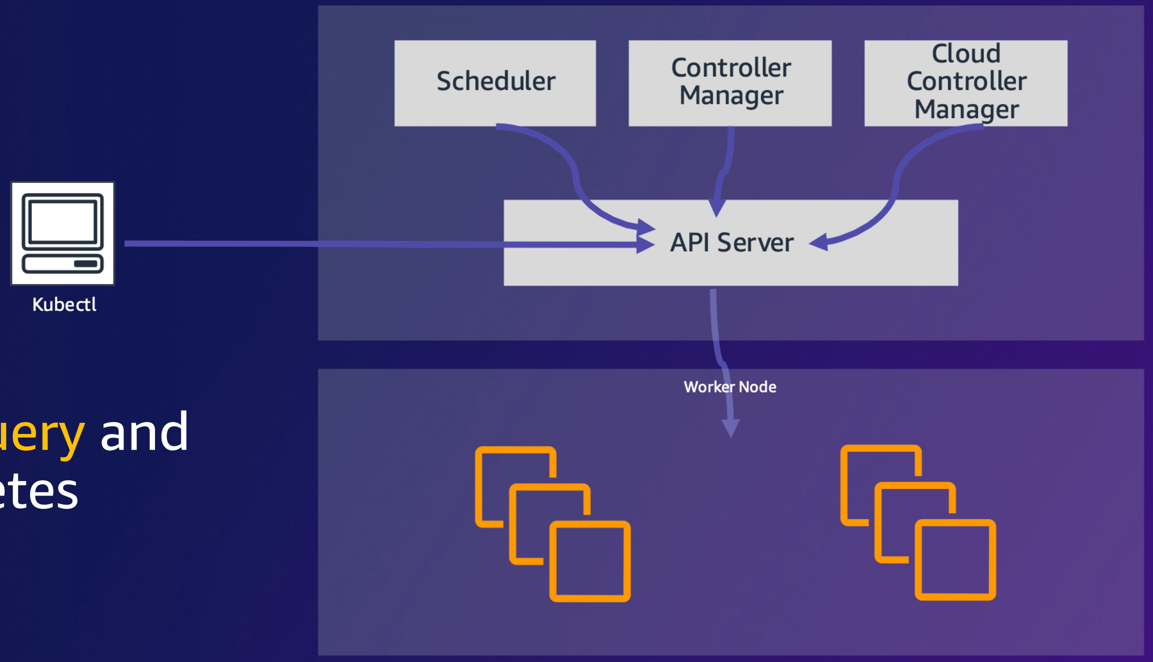
Auto-enable services and features on all member accounts and enable view findings across multiple regions.

Amazon **GuardDuty**

Protect your AWS accounts with intelligent threat detection

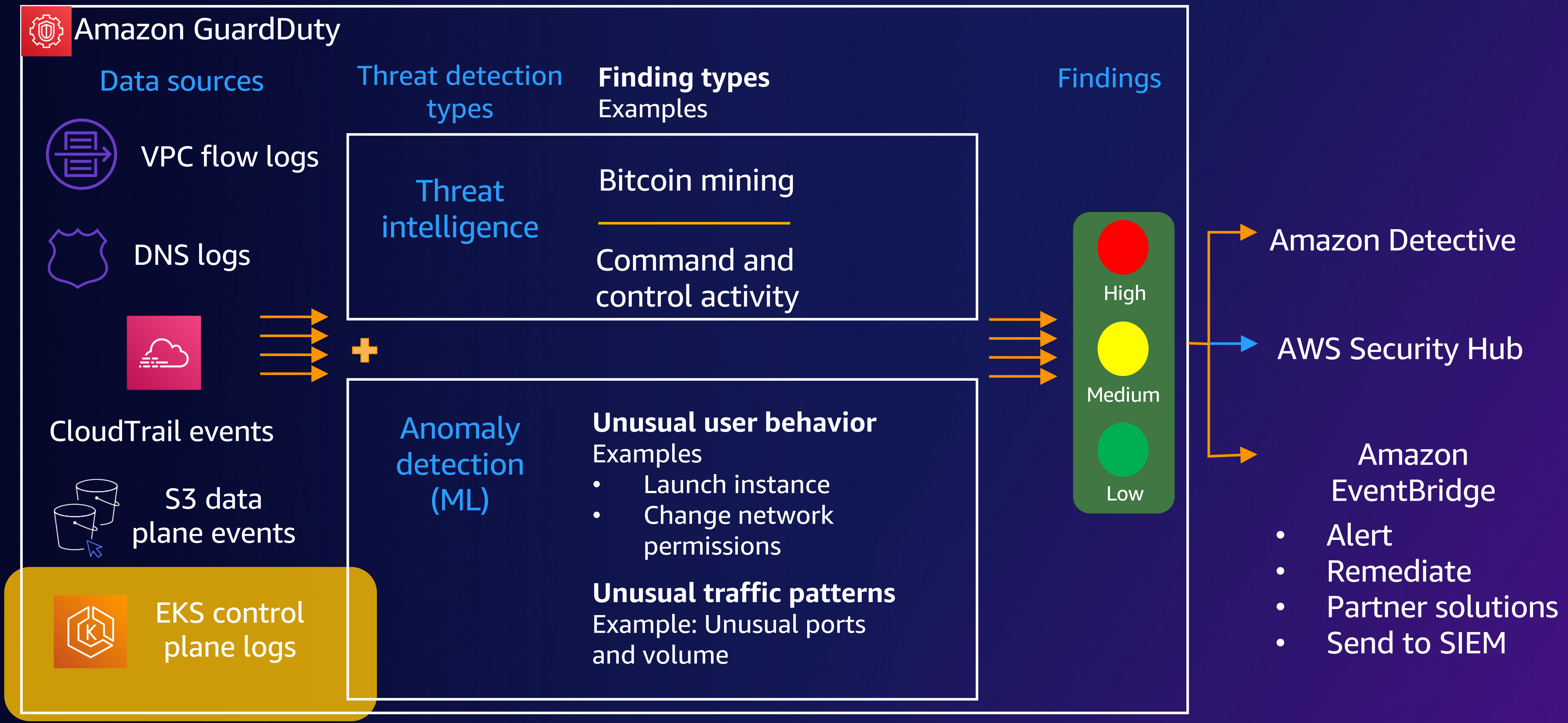
What's New - Amazon EKS control plane API and audit logs

GuardDuty can now generate findings for your Amazon EKS resources through the monitoring of Kubernetes audit logs



Kubernetes control plane API – HTTP API to query and manipulate the state of API objects in Kubernetes

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

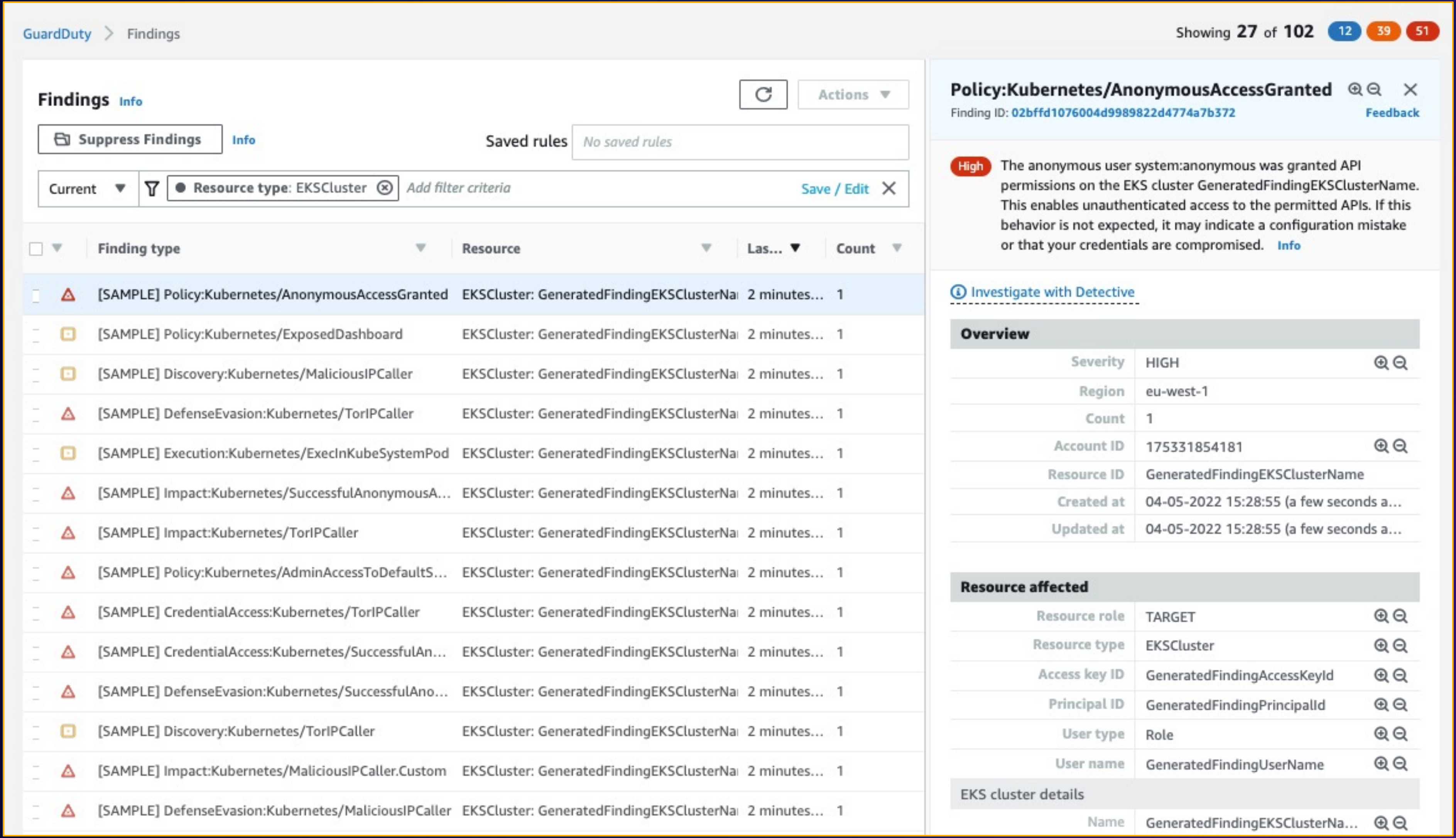
- High
- Medium
- Low

Amazon Detective

AWS Security Hub

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

Generating sample findings GuardDuty - EKS



Showing 27 of 102 12 39 51

Findings Info

Saved rules: No saved rules

Current ▼ | Resource type: EKSCluster | Add filter criteria | Save / Edit

□		Finding type	Resource	Las...	Count
□	△	[SAMPLE] Policy:Kubernetes/AnonymousAccessGranted	EKSCluster: GeneratedFindingEKSClusterNa	2 minutes...	1
□	□	[SAMPLE] Policy:Kubernetes/ExposedDashboard	EKSCluster: GeneratedFindingEKSClusterNa	2 minutes...	1
□	□	[SAMPLE] Discovery:Kubernetes/MaliciousIPCaller	EKSCluster: GeneratedFindingEKSClusterNa	2 minutes...	1
□	△	[SAMPLE] DefenseEvasion:Kubernetes/TorIPCaller	EKSCluster: GeneratedFindingEKSClusterNa	2 minutes...	1
□	□	[SAMPLE] Execution:Kubernetes/ExecInKubeSystemPod	EKSCluster: GeneratedFindingEKSClusterNa	2 minutes...	1
□	△	[SAMPLE] Impact:Kubernetes/SuccessfulAnonymousA...	EKSCluster: GeneratedFindingEKSClusterNa	2 minutes...	1
□	△	[SAMPLE] Impact:Kubernetes/TorIPCaller	EKSCluster: GeneratedFindingEKSClusterNa	2 minutes...	1
□	△	[SAMPLE] Policy:Kubernetes/AdminAccessToDefaultS...	EKSCluster: GeneratedFindingEKSClusterNa	2 minutes...	1
□	△	[SAMPLE] CredentialAccess:Kubernetes/TorIPCaller	EKSCluster: GeneratedFindingEKSClusterNa	2 minutes...	1
□	△	[SAMPLE] CredentialAccess:Kubernetes/SuccessfulAn...	EKSCluster: GeneratedFindingEKSClusterNa	2 minutes...	1
□	△	[SAMPLE] DefenseEvasion:Kubernetes/SuccessfulAno...	EKSCluster: GeneratedFindingEKSClusterNa	2 minutes...	1
□	□	[SAMPLE] Discovery:Kubernetes/TorIPCaller	EKSCluster: GeneratedFindingEKSClusterNa	2 minutes...	1
□	△	[SAMPLE] Impact:Kubernetes/MaliciousIPCaller.Custom	EKSCluster: GeneratedFindingEKSClusterNa	2 minutes...	1
□	△	[SAMPLE] DefenseEvasion:Kubernetes/MaliciousIPCaller	EKSCluster: GeneratedFindingEKSClusterNa	2 minutes...	1

Policy:Kubernetes/AnonymousAccessGranted

Finding ID: 02bffd1076004d9989822d4774a7b372

High The anonymous user system:anonymous was granted API permissions on the EKS cluster GeneratedFindingEKSClusterName. This enables unauthenticated access to the permitted APIs. If this behavior is not expected, it may indicate a configuration mistake or that your credentials are compromised. Info

Overview

Severity	HIGH
Region	eu-west-1
Count	1
Account ID	175331854181
Resource ID	GeneratedFindingEKSClusterName
Created at	04-05-2022 15:28:55 (a few seconds a...
Updated at	04-05-2022 15:28:55 (a few seconds a...

Resource affected

Resource role	TARGET
Resource type	EKSCluster
Access key ID	GeneratedFindingAccessKeyId
Principal ID	GeneratedFindingPrincipalId
User type	Role
User name	GeneratedFindingUserName

EKS cluster details

Name	GeneratedFindingEKSClusterNa...

What’s New - Amazon GuardDuty Enhances Detection of EC2 Instance Credential Exfiltration

GuardDuty adds the ability to detect when your Amazon Elastic Compute Cloud (Amazon EC2) instance credentials are being used from another AWS Account.

- This finding informs you when your instance credentials are accessed by an AWS account outside your AWS environment.
  UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.InsideAWS

- This improved version of the finding learns the typical locations your credentials are used from to reduce findings from traffic routed through on premise networks.
  UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS

Amazon **Detective**

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

Amazon Detective – How it works

INVESTIGATIVE LAYER

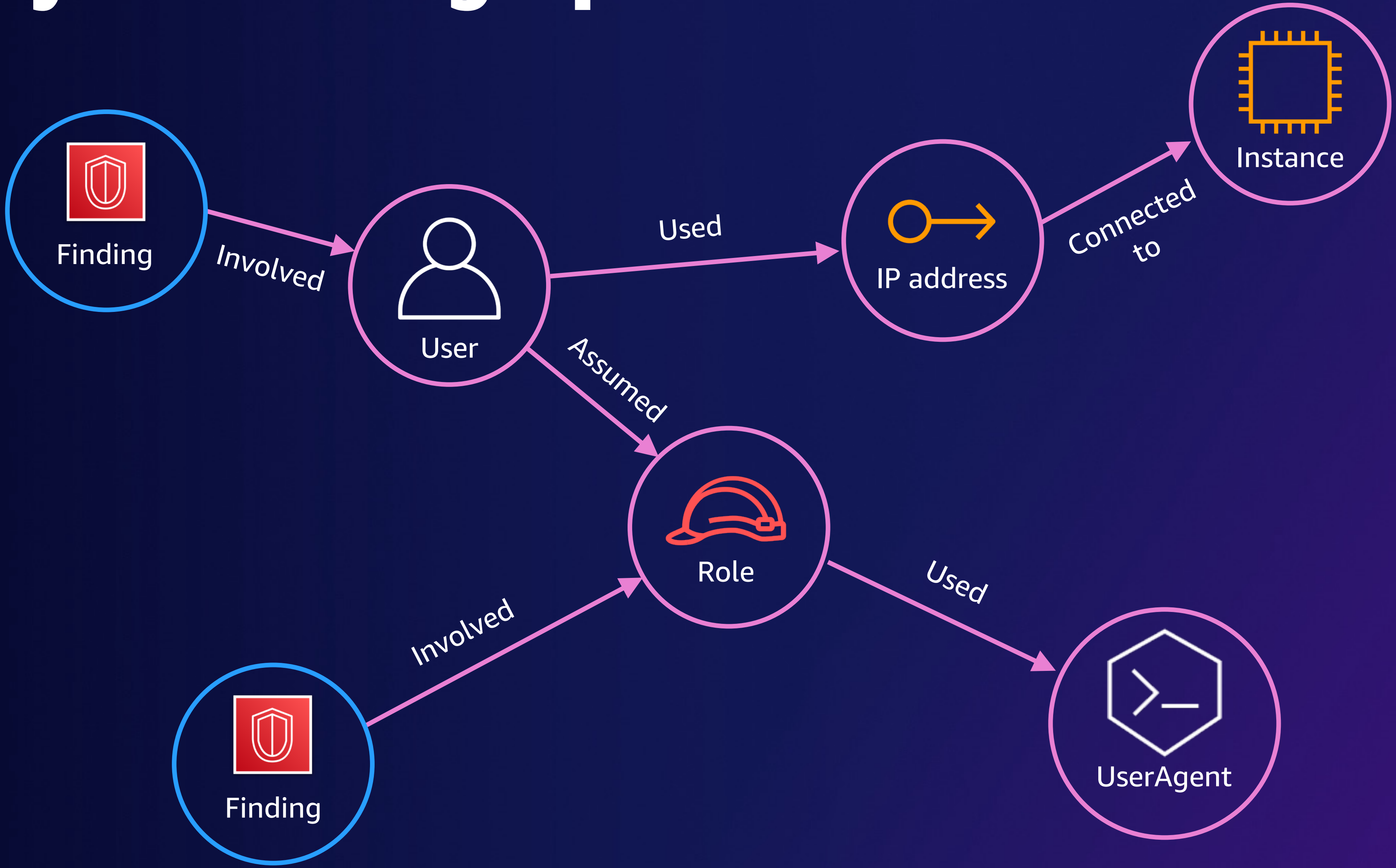
Quickly analyze, investigate, and identify the root cause of security issues

Built-in data collection

Automated analysis

Visual insights

Security behavior graph



What's New - 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 at scale

Amazon Macie - How it works

Gain visibility and evaluate

- Bucket inventory
- Bucket policies

Discover sensitive data

- Inspection jobs
- Flexible scope

Centrally manage at scale

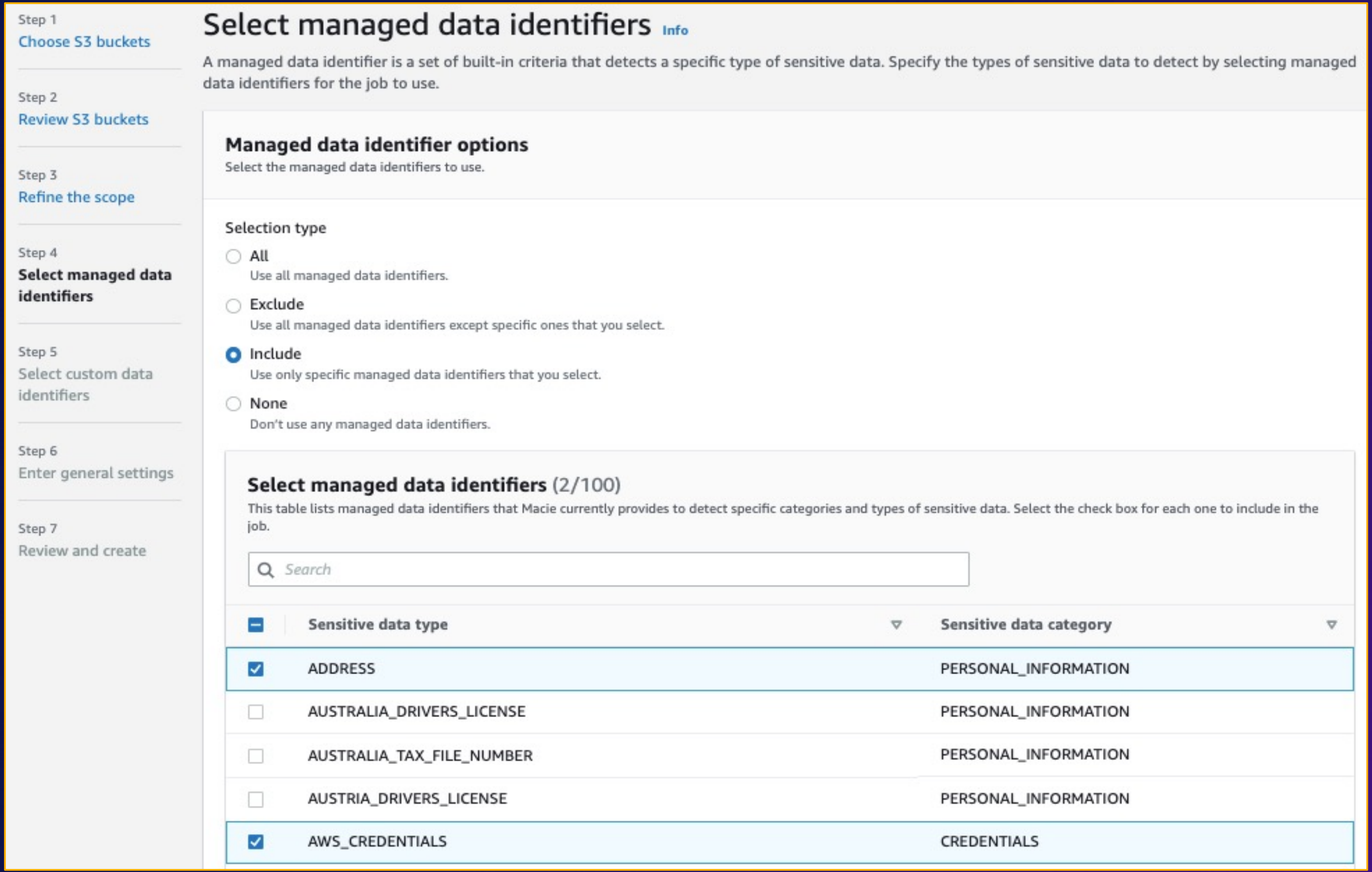
- AWS Organizations
- Managed & custom data detections

Automate and take actions

- Detailed findings
- Management APIs

What's New – 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.

Search

⊟	Sensitive data type	Sensitive data category
☑	ADDRESS	PERSONAL_INFORMATION
☐	AUSTRALIA_DRIVERS_LICENSE	PERSONAL_INFORMATION
☐	AUSTRALIA_TAX_FILE_NUMBER	PERSONAL_INFORMATION
☐	AUSTRIA_DRIVERS_LICENSE	PERSONAL_INFORMATION
☑	AWS_CREDENTIALS	CREDENTIALS

What's New – Amazon Macie enhances machine learning models 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 at scale

Amazon Inspector

Automated and continuous vulnerability management at scale

Scale with simplified management

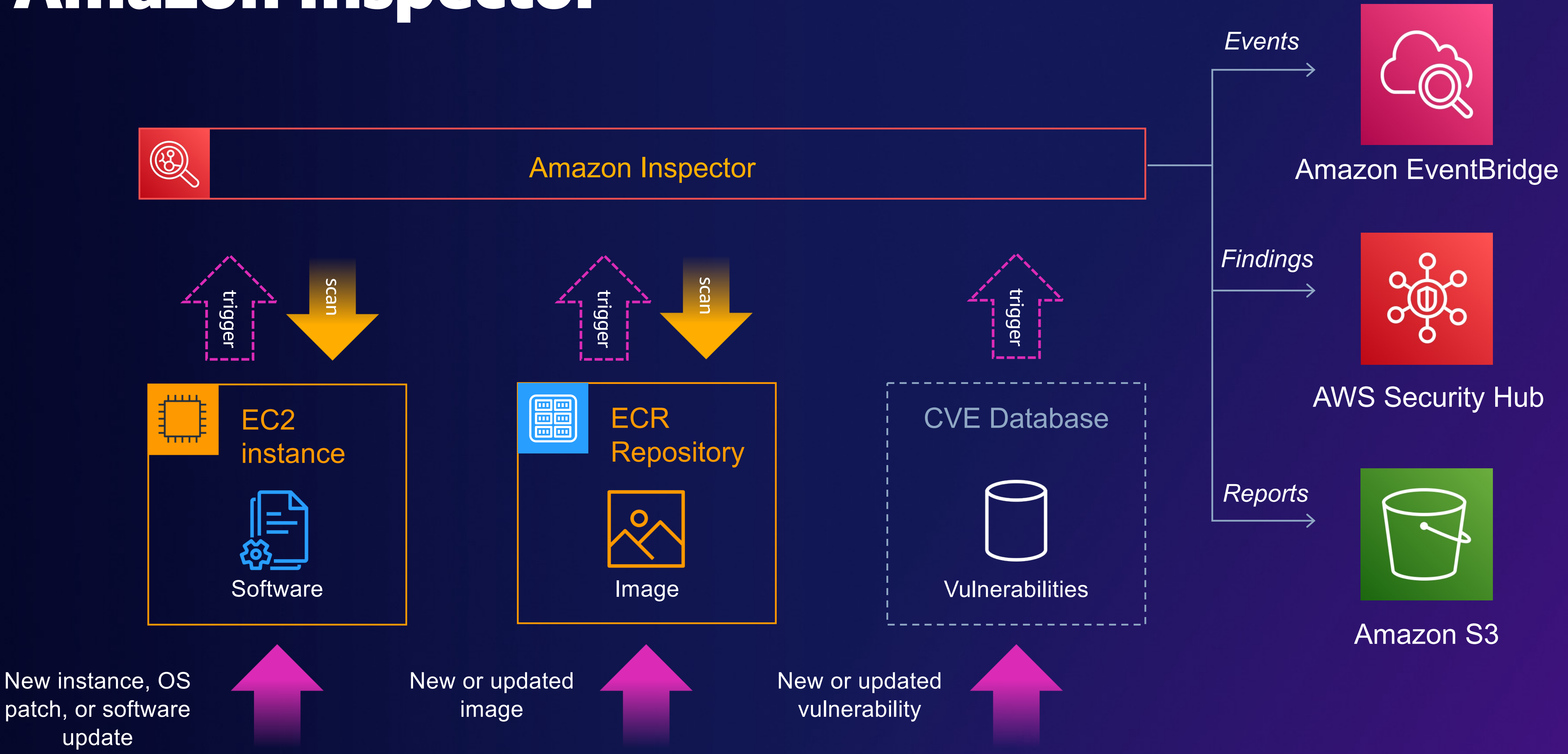
Gain centralized visibility

Automated discovery and continual scanning

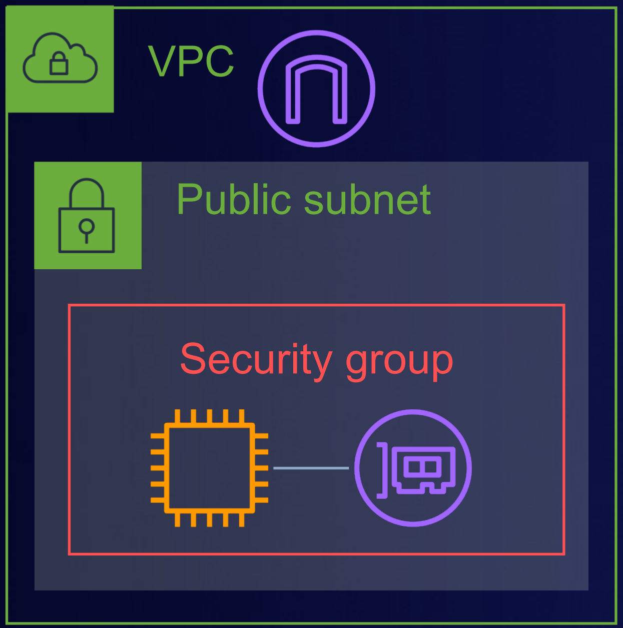
Prioritize with contextualized scoring

Automate workflows and take actions

Amazon Inspector



EC2 Scanning - Network Reachability

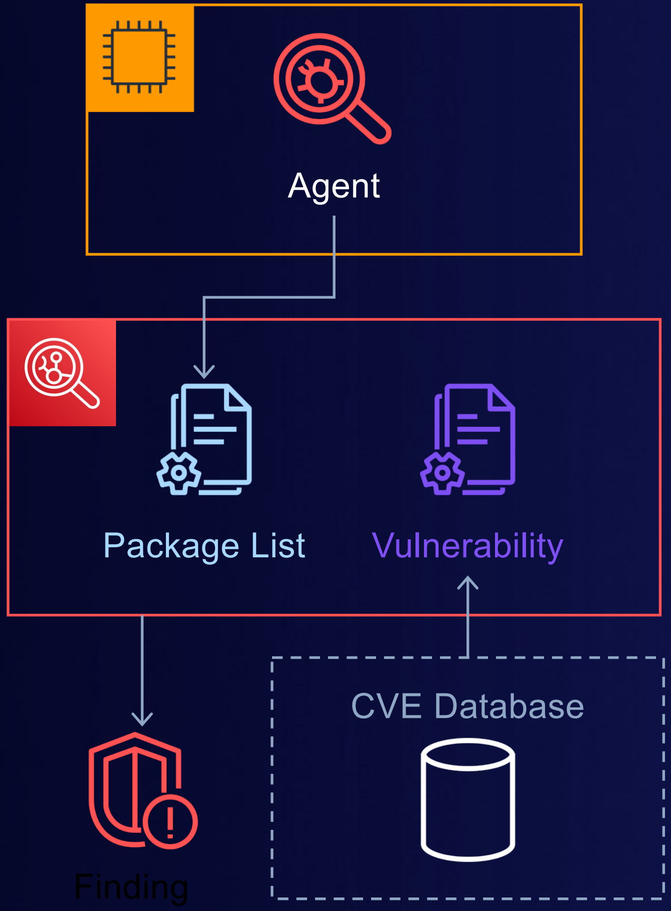


- Inspector runs reachability analysis on all EC2 instances once every 24 hours

- Inspector uses advanced heuristics to determine network reachability on each EC2 instance instead of port scanning

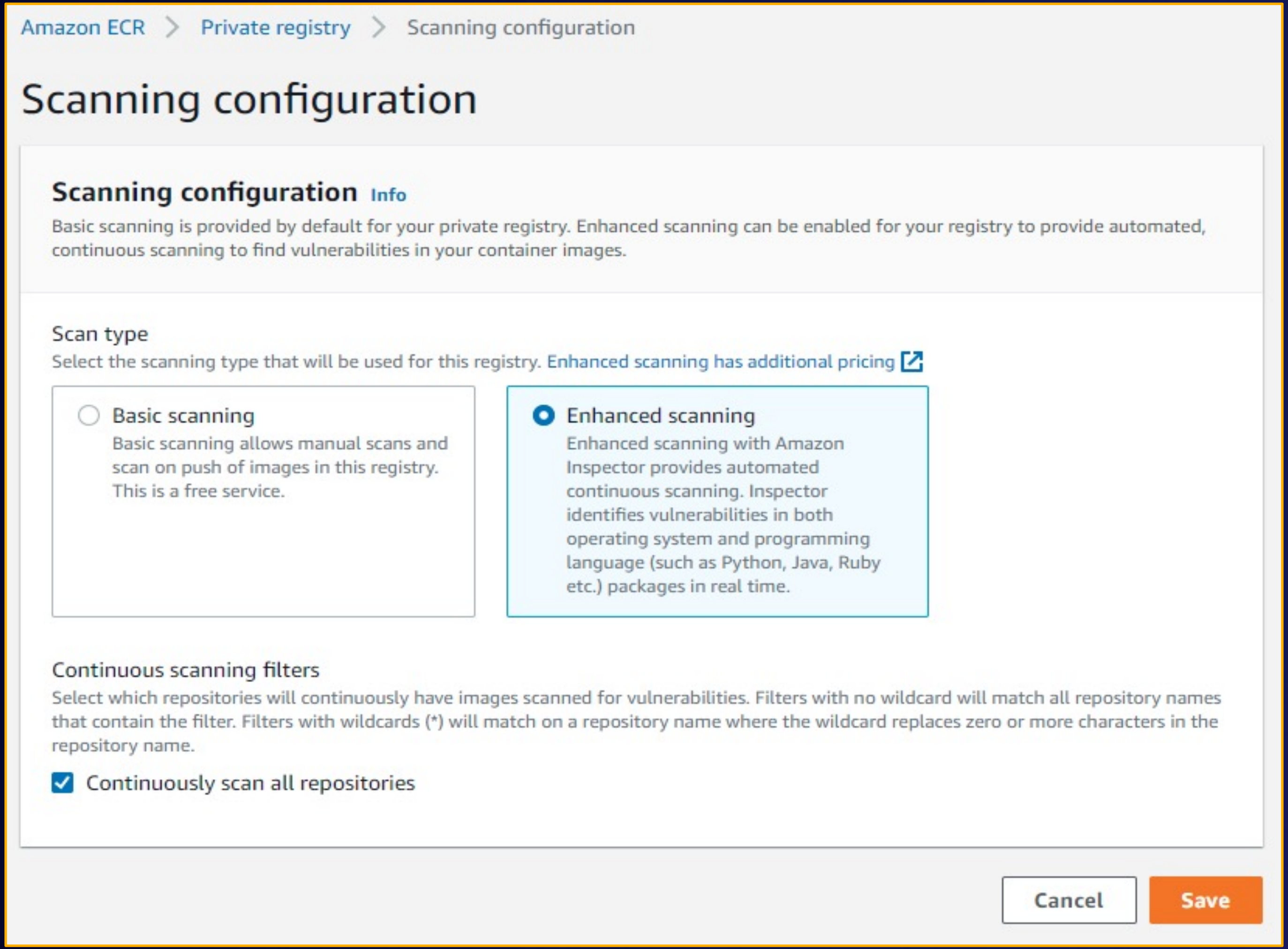
- Like all Inspector findings, network reachability findings can be suppressed for instances that should be publicly exposed, i.e. web servers.

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



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

Once Inspector is enabled, Enhanced Scanning becomes the default scan type for all ECR registries

ECR Scanning - Enhanced Scanning

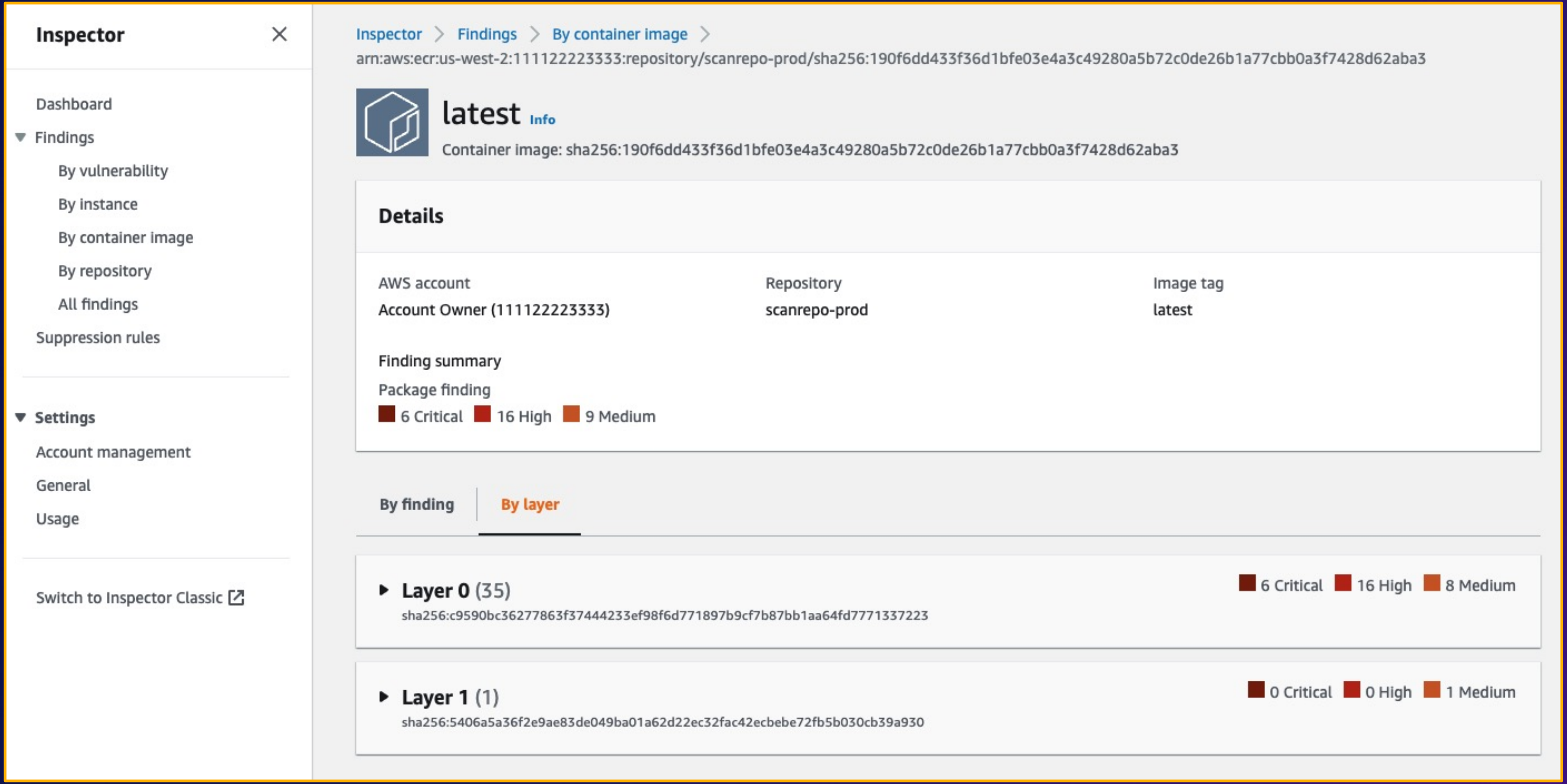
When using Enhanced Scanning on a registry, each repository can be configured to use Continuous Scanning or Scan-on-Push

- 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



arn:aws:ecr:us-west-2:111122223333:repository/scanrepo-prod/sha256:190f6dd433f36d1bfe03e4a3c49280a5b72c0de26b1a77cbb0a3f7428d62aba3

latest

Container image: sha256:190f6dd433f36d1bfe03e4a3c49280a5b72c0de26b1a77cbb0a3f7428d62aba3

Details

AWS account	Repository	Image tag
Account Owner (111122223333)	scanrepo-prod	latest

Finding summary

Package finding

🟥 6 Critical 🟥 16 High 🟧 9 Medium

Layer 0 (35) — 🟥 6 Critical 🟥 16 High 🟧 8 Medium

sha256:c9590bc36277863f37444233ef98f6d771897b9cf7b87bb1aa64fd7771337223

Layer 1 (1) — 🟥 0 Critical 🟥 0 High 🟧 1 Medium

sha256:5406a5a36f2e9ae83de049ba01a62d22ec32fac42ecbebe72fb5b030cb39a930

AWS **Security Hub**

Automate AWS security checks and centralize security alerts

AWS Security Hub

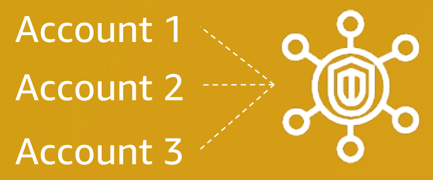
Centrally view and manage security alerts and automate security checks

Save time with aggregated findings

Improve security posture with automated checks

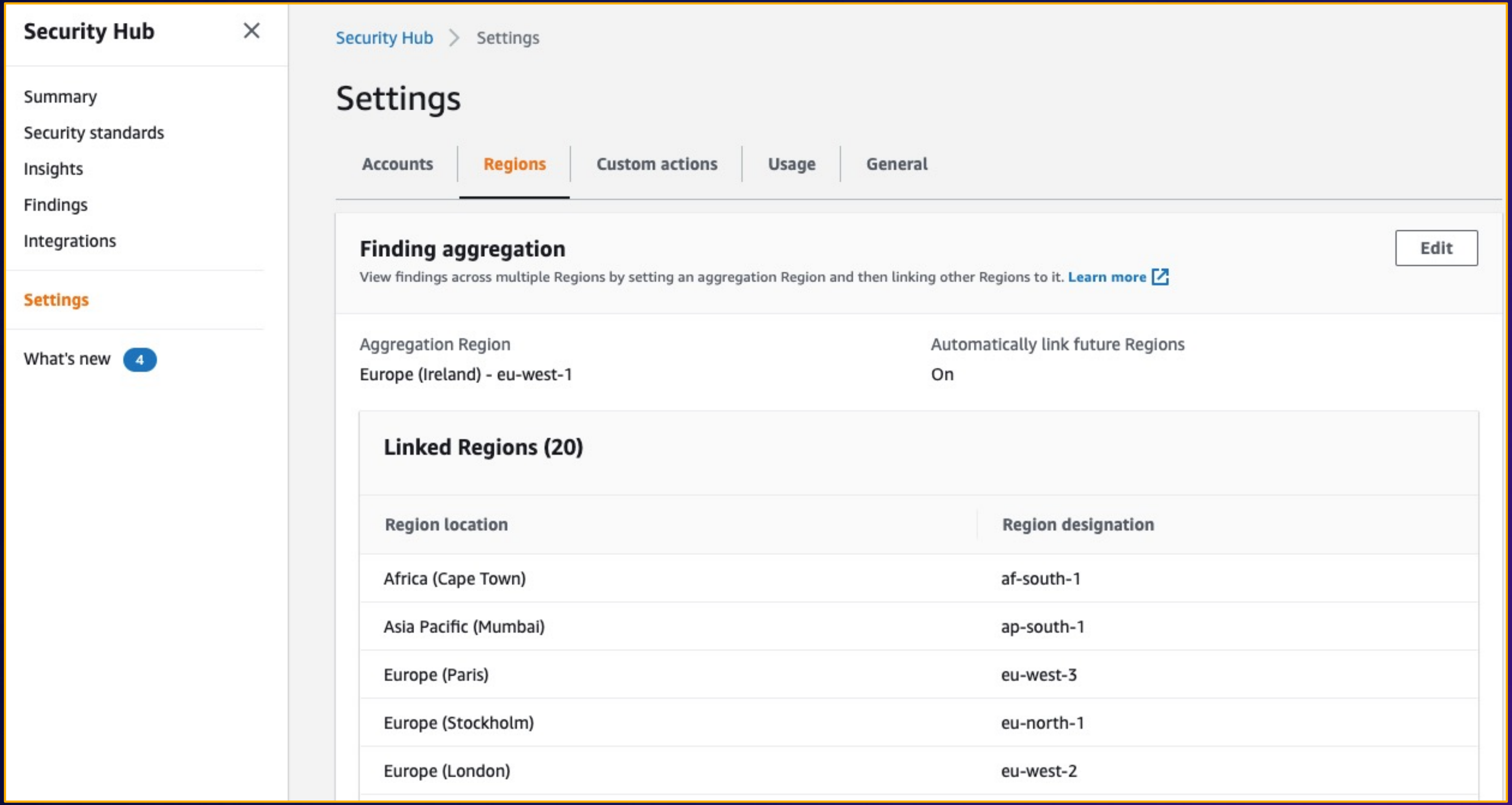
Curated security best practices

Seamless integration with standardized findings format



Multi-account Multi-region support

What's New – now support cross-Region aggregation of security scores and compliance statuses



Settings

Finding aggregation

View findings across multiple Regions by setting an aggregation Region and then linking other Regions to it. Learn more

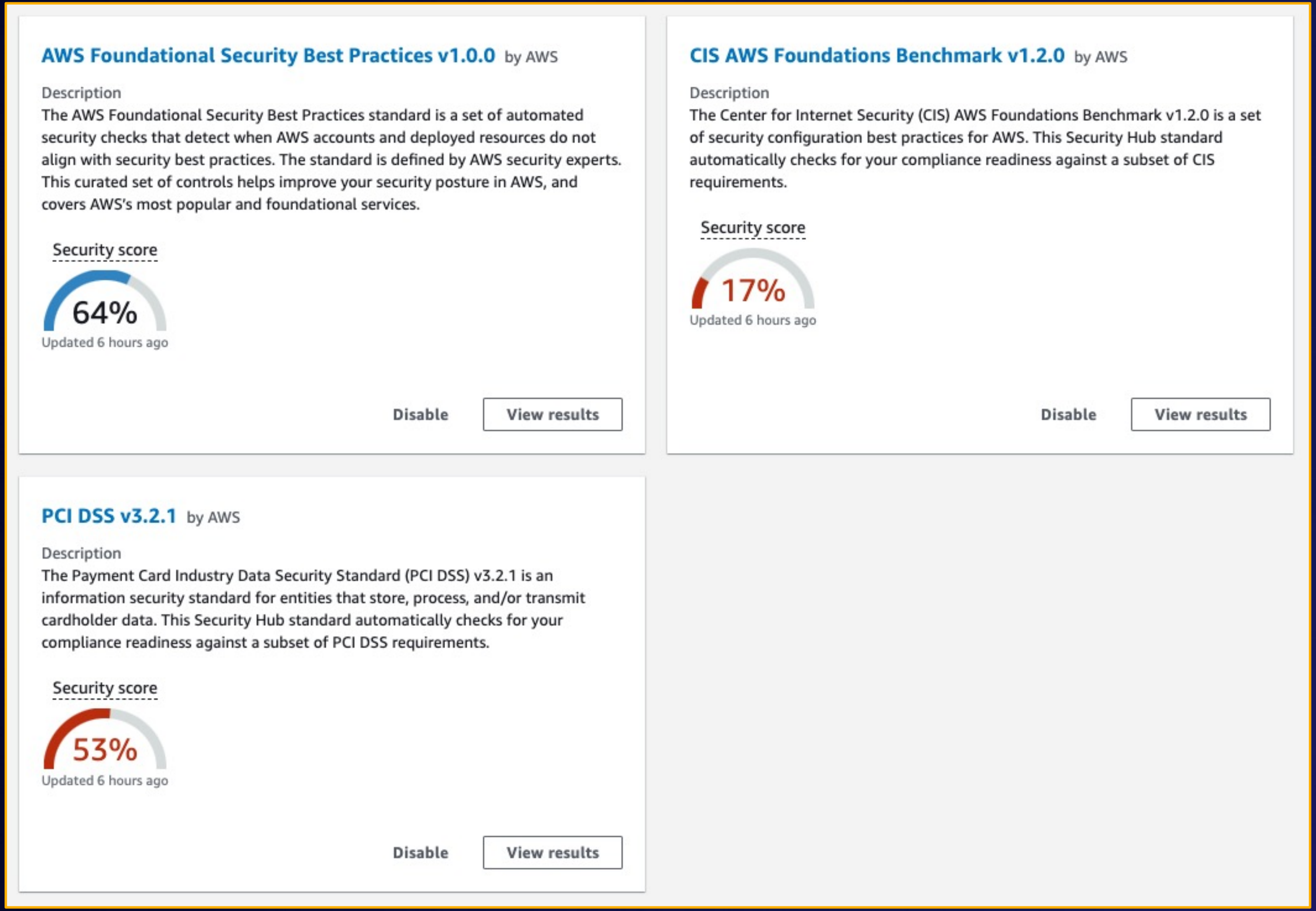
Aggregation Region: Europe (Ireland) - eu-west-1

Automatically link future Regions: On

Linked Regions (20)

Region location	Region designation
Africa (Cape Town)	af-south-1
Asia Pacific (Mumbai)	ap-south-1
Europe (Paris)	eu-west-3
Europe (Stockholm)	eu-north-1
Europe (London)	eu-west-2

What's New – Added new controls 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

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

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

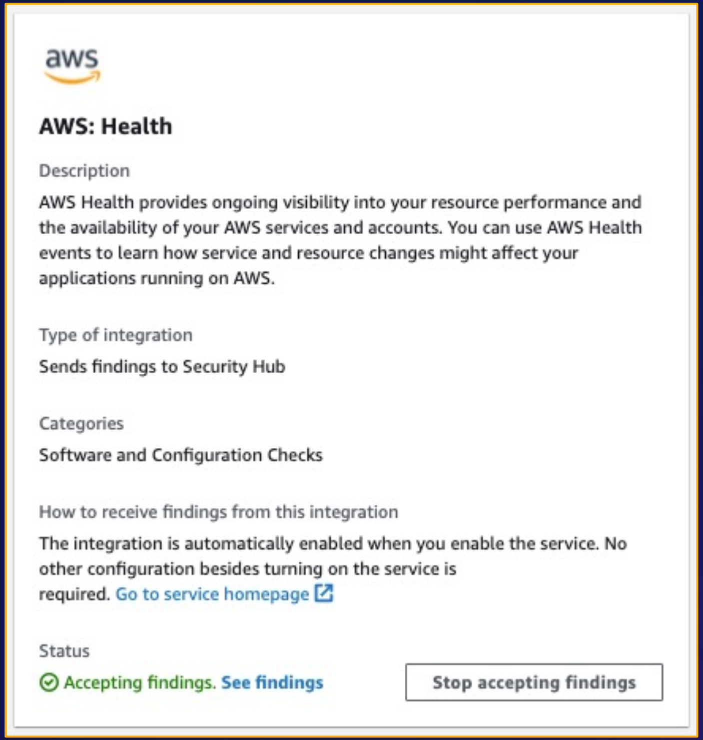
53%

Updated 6 hours ago

- 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

What's New – 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

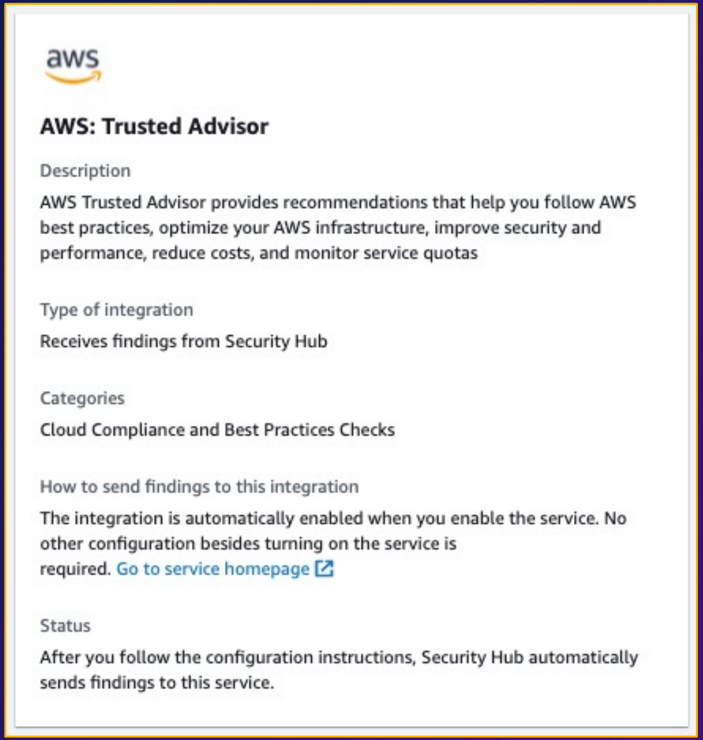
Software and Configuration Checks

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



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

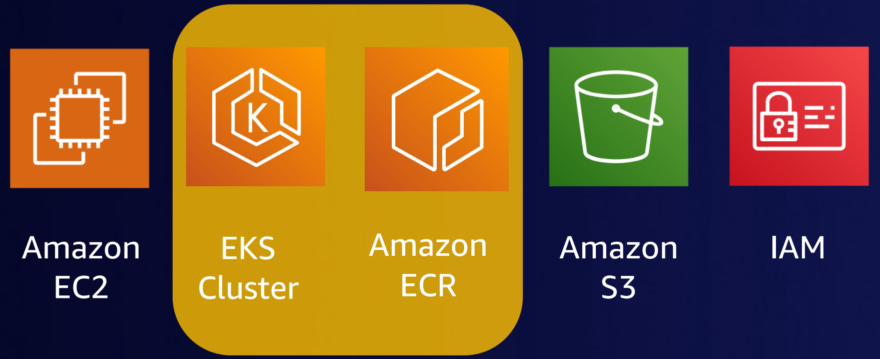
Status

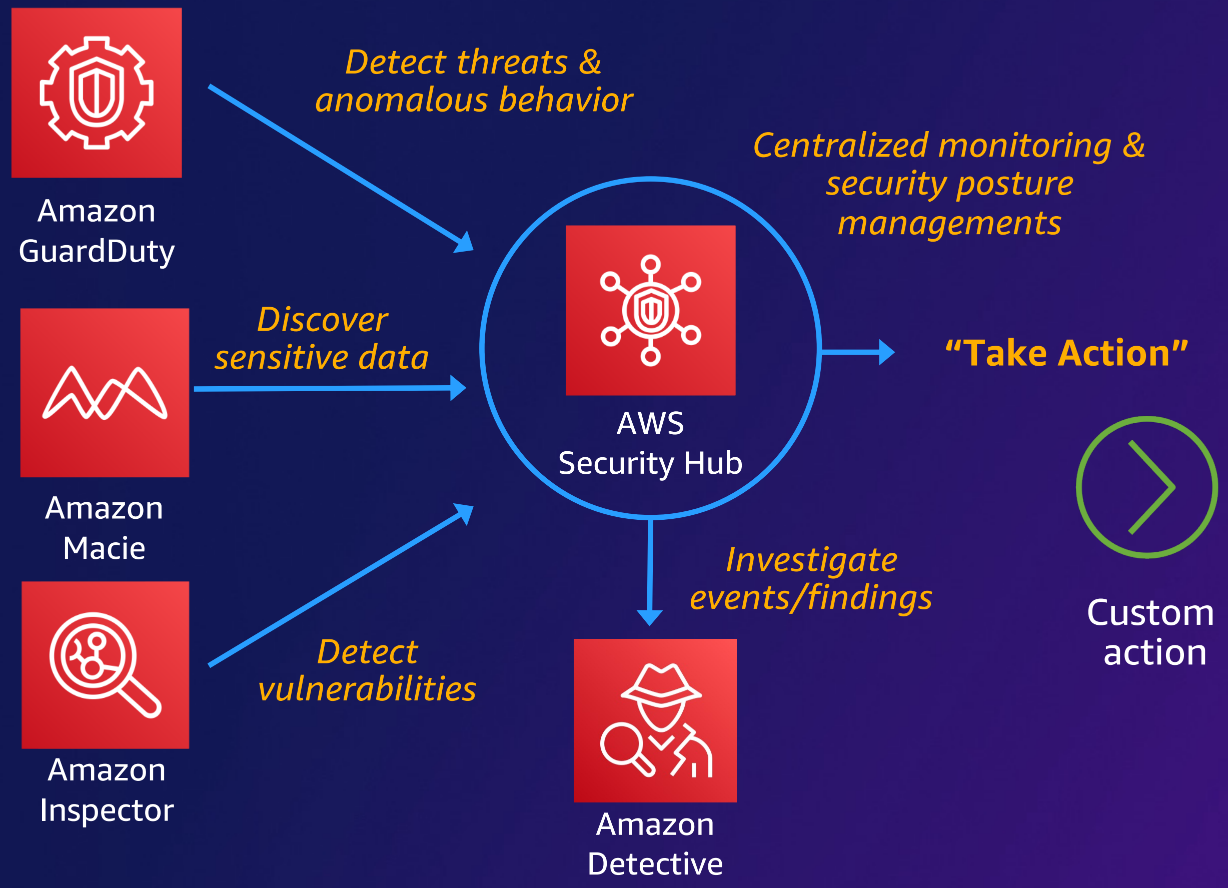
After you follow the configuration instructions, Security Hub automatically sends findings to this service.

How do I perform response and remediation?

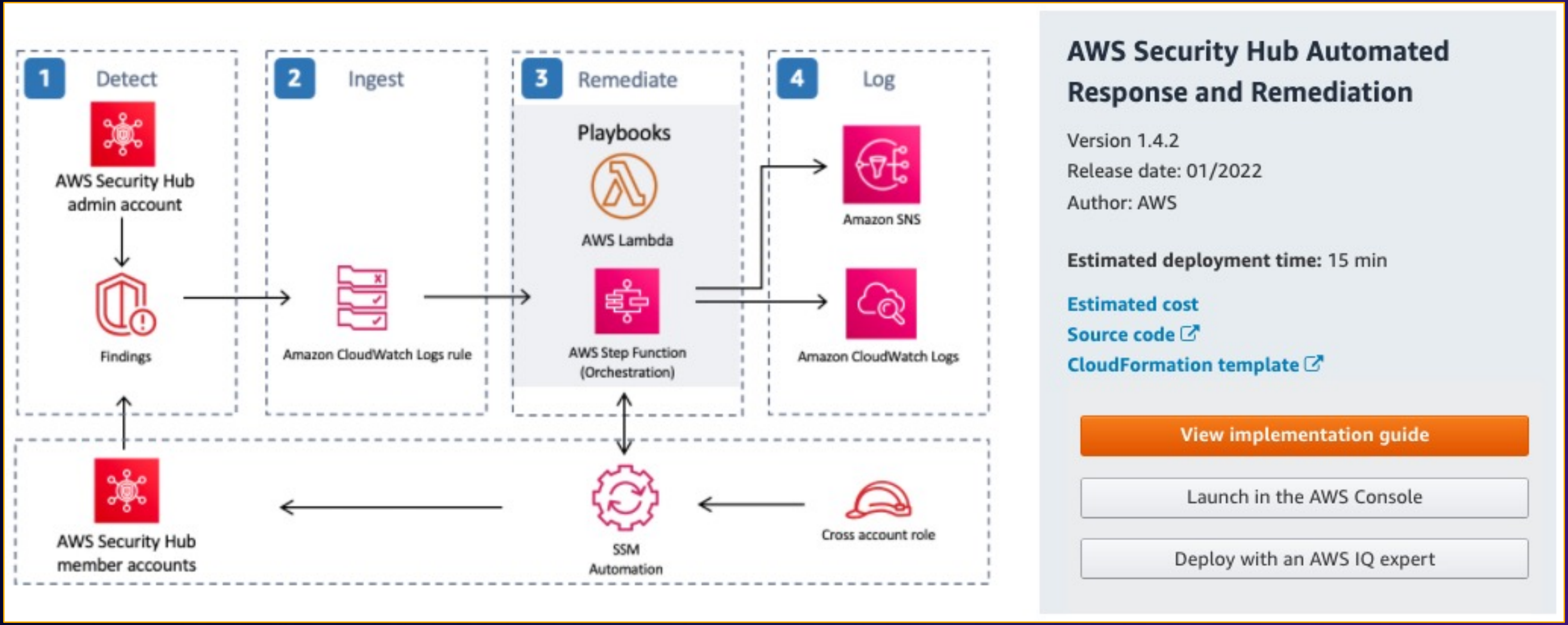
Remediation using native AWS security services

Security Monitoring and Threat Detection





AWS Security Hub Automated Response and Remediation solution architecture


1 Detect
AWS Security Hub admin account
Findings
2 Ingest
Amazon CloudWatch Logs rule
3 Remediate
Playbooks
AWS Lambda
AWS Step Function (Orchestration)
4 Log
Amazon SNS
Amazon CloudWatch Logs
AWS Security Hub member accounts
SSM Automation
Cross account role

AWS Security Hub Automated Response and Remediation

Version 1.4.2

Release date: 01/2022

Author: AWS

Estimated deployment time: 15 min

Estimated cost

Source code

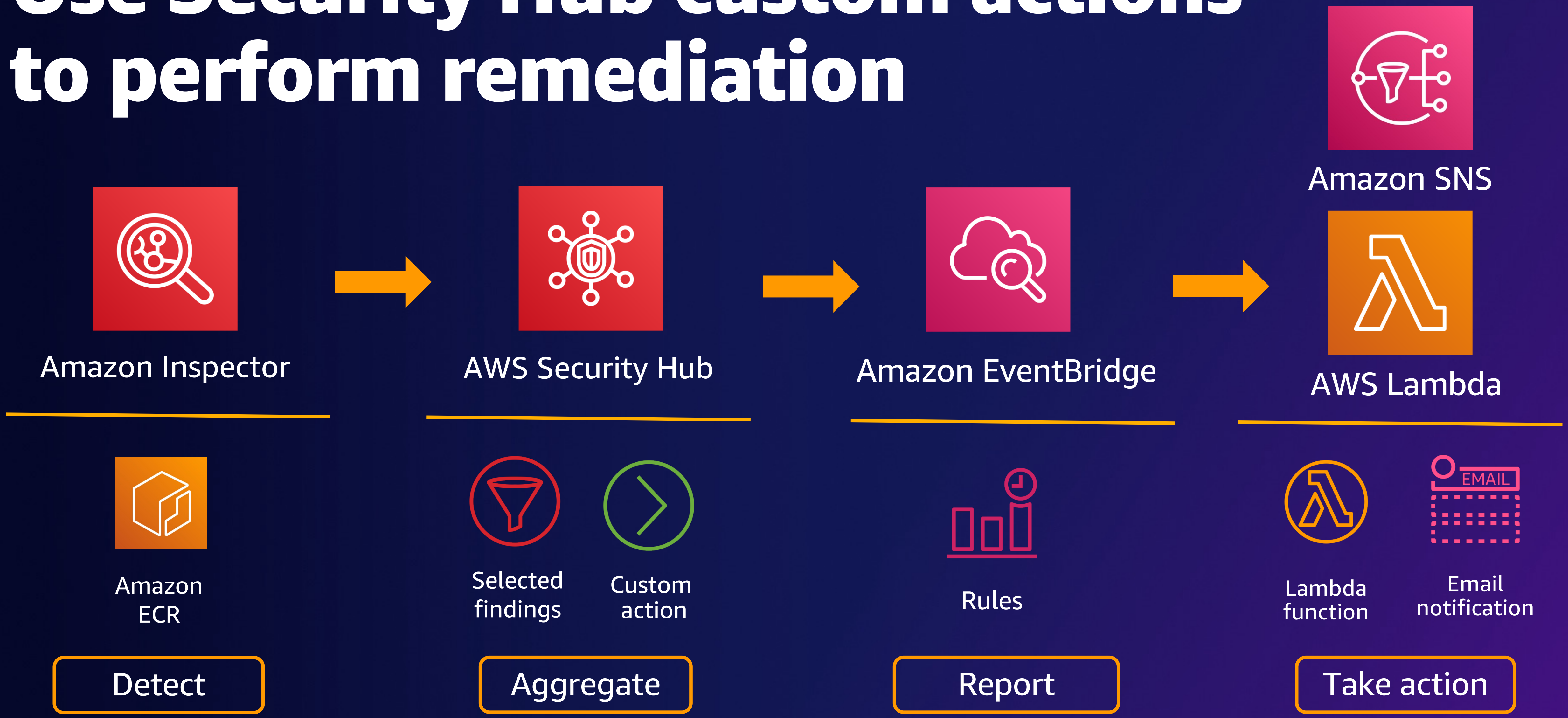
CloudFormation template

View implementation guide
Launch in the AWS Console
Deploy with an AWS IQ expert

https://aws.amazon.com/solutions/implementations/aws-security-hub-automated-response-and-remediation/

Demo

Use Security Hub custom actions to perform remediation



Amazon Inspector

Amazon ECR

Detect

AWS Security Hub

Selected findings

Custom action

Aggregate

Amazon EventBridge

Rules

Report

Amazon SNS

AWS Lambda

Lambda function

EMAIL

Email notification

Take action

Thank you!

Rodrigo Ferroni

https://linkedin.com/in/rferroni/

Learn in-demand AWS Cloud skills

AWS Skill Builder

Access **500+ free** digital courses and Learning Plans

Explore resources with a variety of skill levels and **16+** languages to meet your learning needs

Deepen your skills with digital learning on demand

Train now

AWS Certifications

Earn an industry-recognized credential

Receive Foundational, Associate, Professional, and Specialty certifications

Join the **AWS Certified community** and get exclusive benefits

Access **new** exam guides

Please complete the session survey