Layering AWS security services

Jason Rylands
Sr.Security Specialist
AWS Europe Central

Agenda

- Intro to AWS layered security services
- Enabling Threat Detection & Response layer of services at scale
- Adding automated response & remediation

- New Trust Center: https://aws.amazon.com/trust-center/

AWS services to secure your cloud environment

Amazon Detective
Amazon GuardDuty
AWS Organizations
Amazon Inspector
Amazon Macie
AWS Security Hub

Centralize threat detection and monitoring

Improve security posture assessment

Optimize vulnerability management

Streamline root cause analysis

Improve sensitive data discovery

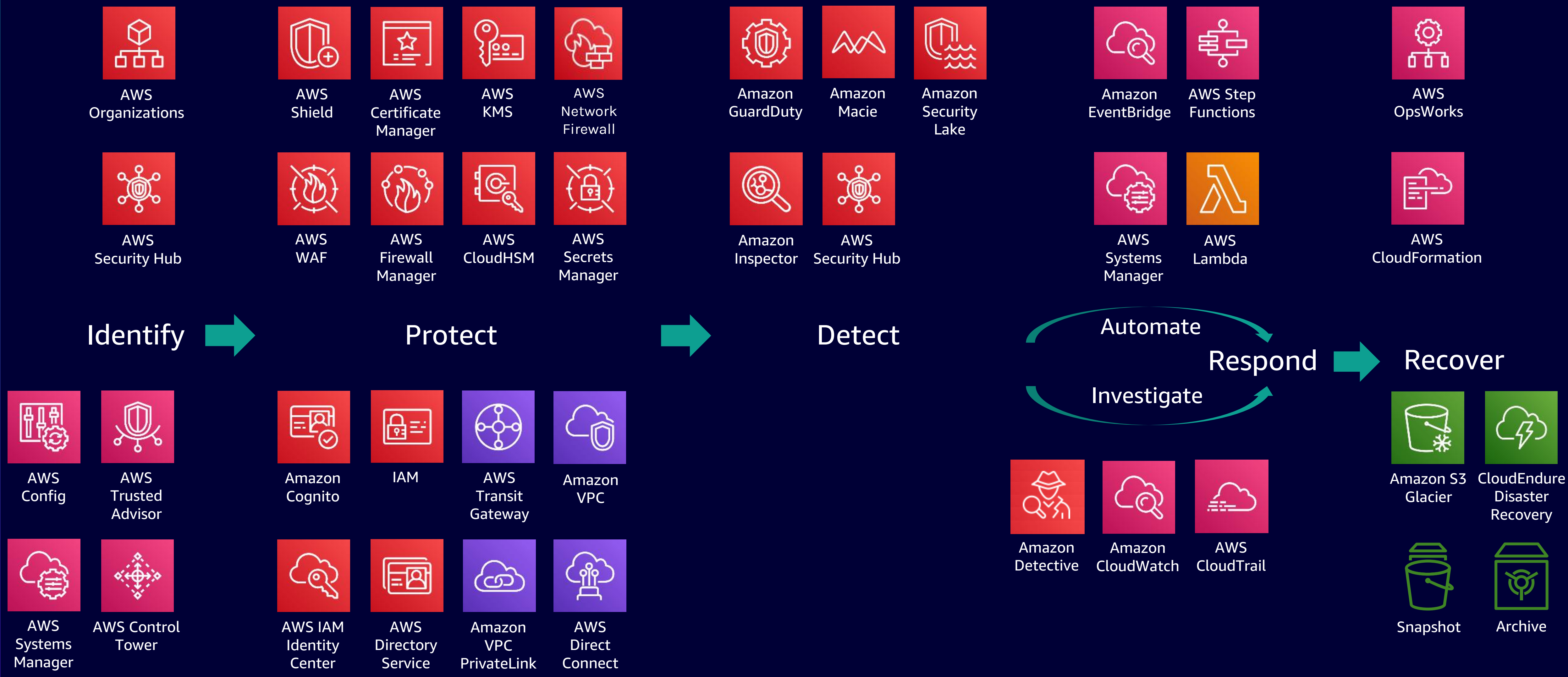
Initiate and route workflows to existing systems

Prioritize critical findings

Automate remediation

Scale deployments

AWS foundational and layered security services



AWS Organizations

AWS Security Hub

AWS Config

AWS Trusted Advisor

AWS Systems Manager

AWS Control Tower

Identify

AWS Shield

AWS Certificate Manager

AWS KMS

AWS Network Firewall

AWS WAF

AWS Firewall Manager

AWS CloudHSM

AWS Secrets Manager

Protect

Amazon Cognito

IAM

AWS Transit Gateway

Amazon VPC

AWS IAM Identity Center

AWS Directory Service

Amazon VPC PrivateLink

AWS Direct Connect

Amazon GuardDuty

Amazon Macie

Amazon Security Lake

Amazon Inspector

AWS Security Hub

Detect

Amazon EventBridge

AWS Step Functions

AWS Systems Manager

AWS Lambda

Automate

Respond

Investigate

Amazon Detective

Amazon CloudWatch

AWS CloudTrail

AWS OpsWorks

AWS CloudFormation

Recover

Amazon S3 Glacier

CloudEndure Disaster Recovery

Snapshot

Archive

How do I enable threat detection at scale?

Scalable and centralized management

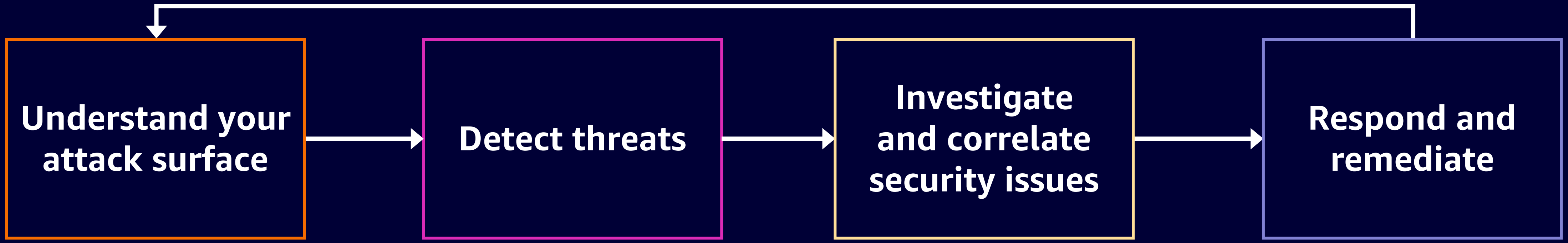
BUILT-IN INTEGRATION WITH AWS ORGANIZATIONS

Administrator / member setup

- Designate a centralized delegated administrator
- Add all member accounts
- Auto-enable services on all member accounts

Continuous security monitoring for AWS

Continuous improvement of your AWS security posture



Understand your attack surface

Detect threats

Investigate and correlate security issues

Respond and remediate

Amazon Inspector:
CVE scans and OS-level configurations

Amazon Macie:
Data classification

AWS Security Hub:
Resource and account-level configurations

NIST CSF function:
IDENTIFY

Amazon GuardDuty:
Automated intelligent threat detection

NIST CSF function:
DETECT

Amazon Detective:
Security investigations

AWS Security Hub:
Alert aggregation

NIST CSF function:
DETECT

AWS Security Hub:
Automated response and remediation runbooks and ITSM or "taking action" integrations

NIST CSF function:
RESPOND

NIST CSF functions covered by other AWS services: PROTECT – AWS identity, crypto, and edge protection services; RECOVER – AWS backup services

Amazon Inspector

AUTOMATED AND CONTINUOUS VULNERABILITY MANAGEMENT AT SCALE

Gain centralized visibility

- Environment coverage
- High impact findings
- Resources by finding severity

One-click continuous monitoring

- Automatic discovery of resources
- Monitors throughout the resource life-cycle

Prioritize with contextualized scoring

- Inspector Risk score
- Security metrics
- Customized views

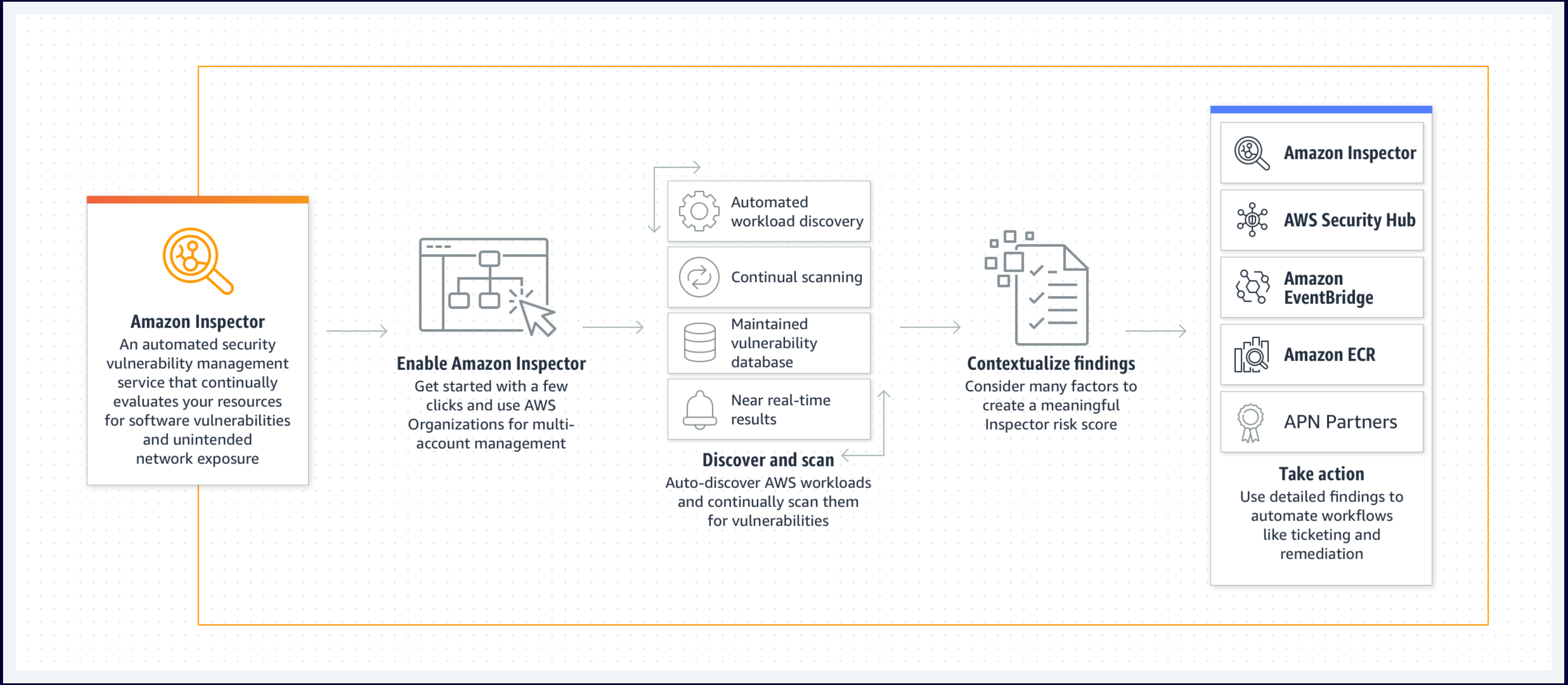
Centrally manage at scale

- AWS Organizations
- Package vulnerability, Network reachability
- Environment coverage

Automate and take actions

- Management APIs
- Detailed findings in Eventbridge
- Security Hub integration

Amazon Inspector – How it works



Amazon Inspector
An automated security vulnerability management service that continually evaluates your resources for software vulnerabilities and unintended network exposure

Enable Amazon Inspector
Get started with a few clicks and use AWS Organizations for multi-account management

- Automated workload discovery
- Continual scanning
- Maintained vulnerability database
- Near real-time results

Discover and scan
Auto-discover AWS workloads and continually scan them for vulnerabilities

Contextualize findings
Consider many factors to create a meaningful Inspector risk score

- Amazon Inspector
- AWS Security Hub
- Amazon EventBridge
- Amazon ECR
- APN Partners

Take action
Use detailed findings to automate workflows like ticketing and remediation

Continuous discovery and scanning

- Automatically discover workloads and continually scan them for vulnerabilities across your organization

  - *Automatic Discovery - Amazon Inspector automatically discovers all eligible resources and begins continuous scans of those resources for software vulnerabilities and unintended network exposure.*

  - *Continuous scanning - Amazon Inspector employs its own, purpose-built scanning engine to monitor your resources for software vulnerabilities or open network paths that can result in compromised workloads, malicious use or resources, or unauthorized access to your data.*

- Amazon Inspector monitors your environment throughout the life-cycle of your resources by running scans in response to events such as after the installation of a new application or patch.

Support for Lambda functions

Amazon Inspector identifies software vulnerabilities (CVEs) in application package dependencies used in the Lambda function code and associated layers.

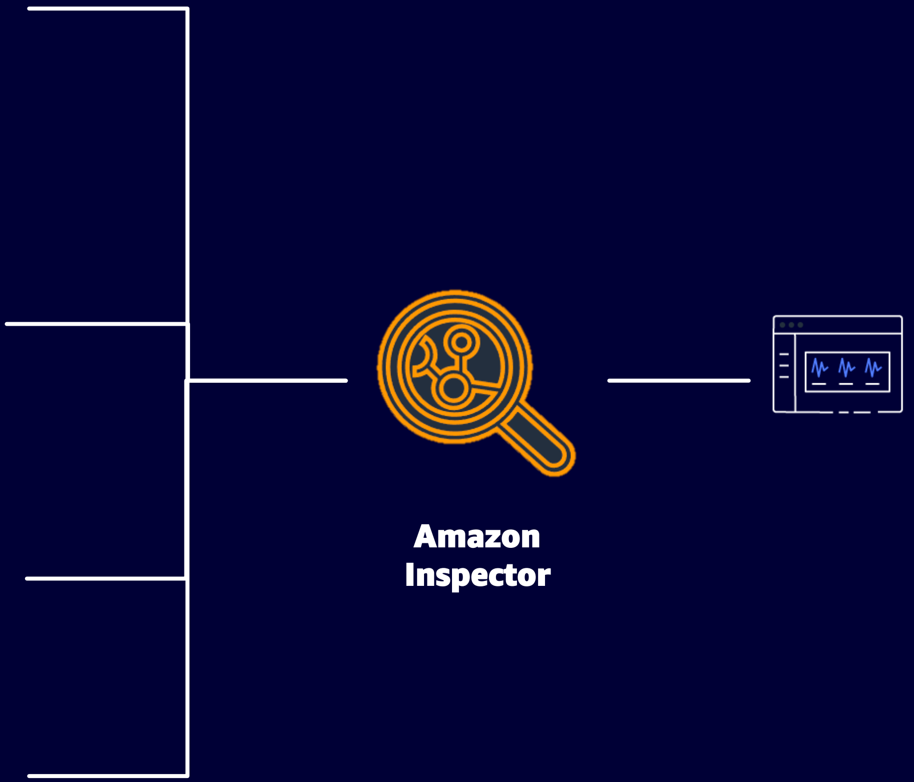
Simplified one-click enablement and Multi-account support with AWS Organization

Automated discovery and continuous monitoring of all functions

- ✓Automated discovery upon deployment
- ✓ Continuous scanning based on:
    - ✓Updates to the function
    - ✓New CVEs being published
- ✓No agents needed

Easy prioritization and remediation with exploitability and Fixed-in package details

Automation through integration with Amazon EventBridge



A single pane of glass for vulnerabilities across all resources

- ✓ Lambda functions
- ✓ EC2 instances
- ✓ Container images in ECR

Note: Automated exclusion of stale functions that have not been invoked in 90 days plus manual tag based exclusion available

Prioritized and contextualized scoring

- Drive efficiency and accuracy with the Amazon Inspector risk score for prioritized, contextualized, and actionable results.

- *Amazon Inspector score - The Inspector risk score is a highly contextualized score that is generated for each finding by correlating common vulnerabilities and exposures (CVE) information with network reachability results, and exploitability data.*

- *Vendor score*
  - *Software package vulnerability scoring - Amazon Inspector uses the NVD/CVSS score as the basis of severity scoring for software package vulnerabilities.*
  - *Network Reachability scoring - Amazon Inspector uses the NVD/CVSS score as the basis of severity scoring for software package vulnerabilities. The NVD/CVSS score is the vulnerability severity score published by the NVD and is defined by the CVSS.*

- Amazon Inspector examines the security metrics that compose the National Vulnerability Database (NVD) base score for the vulnerability and adjusts them according your compute environment.

Amazon Macie

- *Discover and protect your sensitive data at scale*

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

Amazon Macie - Gain visibility and evaluate

- Provides customers visibility into S3 bucket inventory
    - Number of buckets
    - Storage size
    - Object count
    - Automated sensitive data discovery
- Monitors changes to S3 bucket policies
    - Publicly accessible
    - Unencrypted
    - Shared outside of the account
    - Replicated to external accounts

Across multiple accounts and automatically includes new buckets

AWS Security Hub

CONTINUOUS SECURITY ASSESSMENT & AUTOMATED RESPONSE LAYER

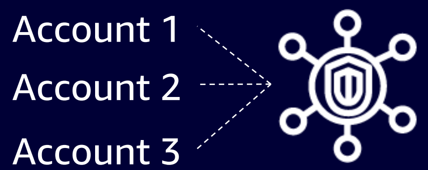
Centrally view & manage security alerts & automate security checks

Save time with aggregated findings

Improve security posture with automated checks

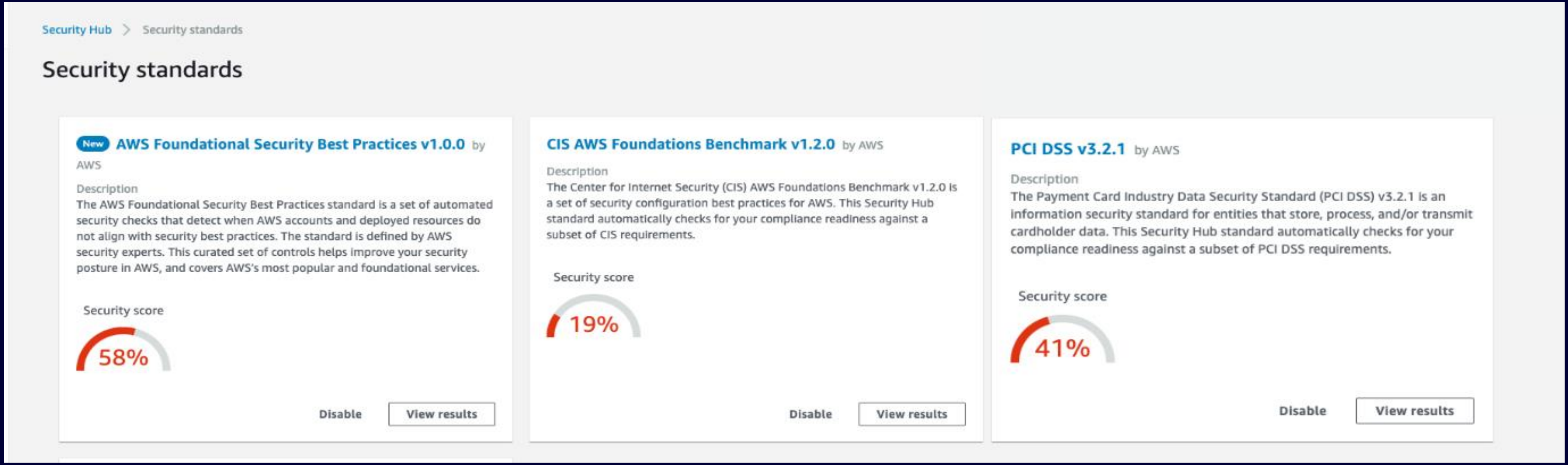
Curated security best practices

Seamless integration w/ standardized findings format


Account 1
Account 2
Account 3

Multi-account support

Automated security & compliance checks



Security Hub > Security standards

Security standards

New 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
58%

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
19%

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.

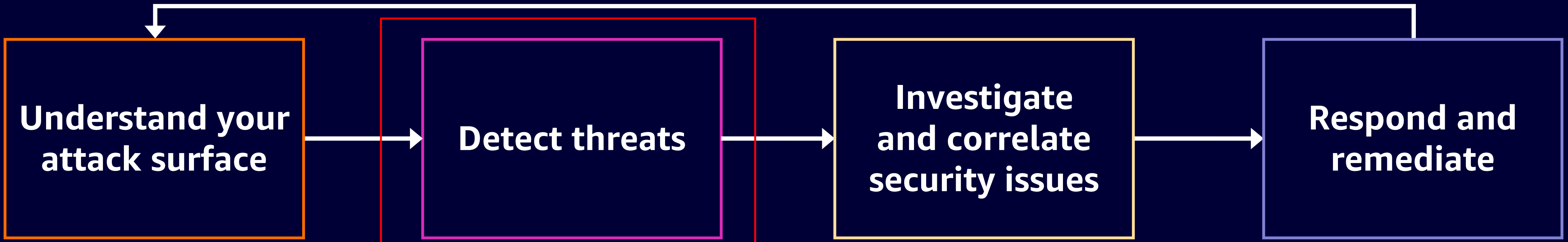
Security score
41%

Disable | View results

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

Continuous security monitoring for AWS

Continuous improvement of your AWS security posture



Understand your attack surface

Detect threats

Investigate and correlate security issues

Respond and remediate

Amazon Inspector: CVE scans and OS-level configurations

Amazon Macie: Data classification

AWS Security Hub: Resource and account-level configurations

NIST CSF function: IDENTIFY

Amazon GuardDuty: Automated intelligent threat detection

NIST CSF function: DETECT

Amazon Detective: Security investigations

AWS Security Hub: Alert aggregation

NIST CSF function: DETECT

AWS Security Hub: Automated response and remediation runbooks and ITSM or “taking action” integrations

NIST CSF function: RESPOND

NIST CSF functions covered by other AWS services: PROTECT – AWS identity, crypto, and edge protection services; RECOVER – AWS backup services

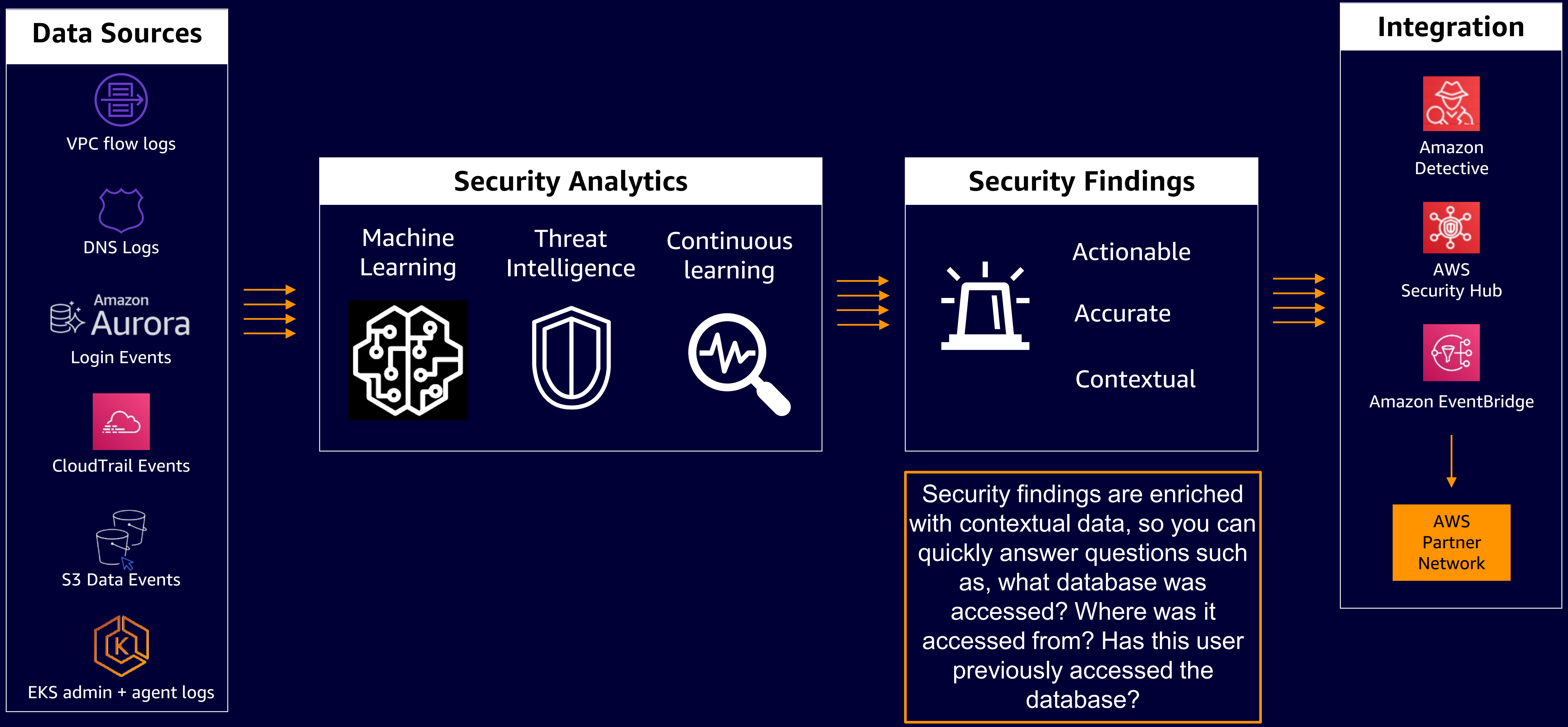
Amazon GuardDuty

FOUNDATIONAL THREAT DETECTION & MONITORING LAYER

Protect your AWS accounts, workloads, and data with intelligent threat detection and continuous monitoring

- One-click activation with no performance impact
- Continuous monitoring of AWS accounts and resources
- Global coverage with regional results
- Detect known & unknown threats
- Enterprise-wide consolidation & management

How GuardDuty works



Data Sources

VPC flow logs

DNS Logs

Amazon Aurora Login Events

CloudTrail Events

S3 Data Events

EKS admin + agent logs

Security Analytics

Machine Learning

Threat Intelligence

Continuous learning

Security Findings

Actionable

Accurate

Contextual

Security findings are enriched with contextual data, so you can quickly answer questions such as, what database was accessed? Where was it accessed from? Has this user previously accessed the database?

Integration

Amazon Detective

AWS Security Hub

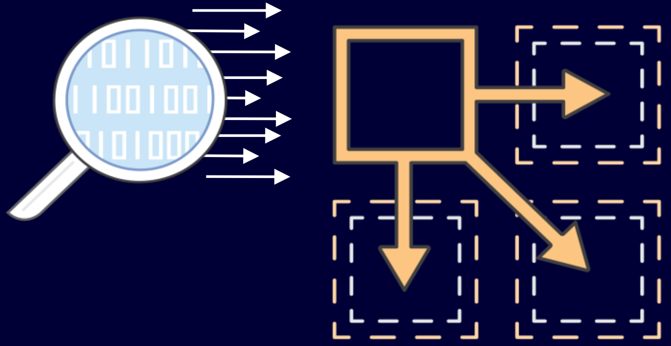
Amazon EventBridge

AWS Partner Network

What can GuardDuty detect?

DETECTING KNOWN THREATS USING THREAT INTELLIGENCE

- GuardDuty leverages threat intelligence from various sources
  - AWS security intel
  - AWS partners CrowdStrike and Proofpoint
  - Customer-provided threat intel

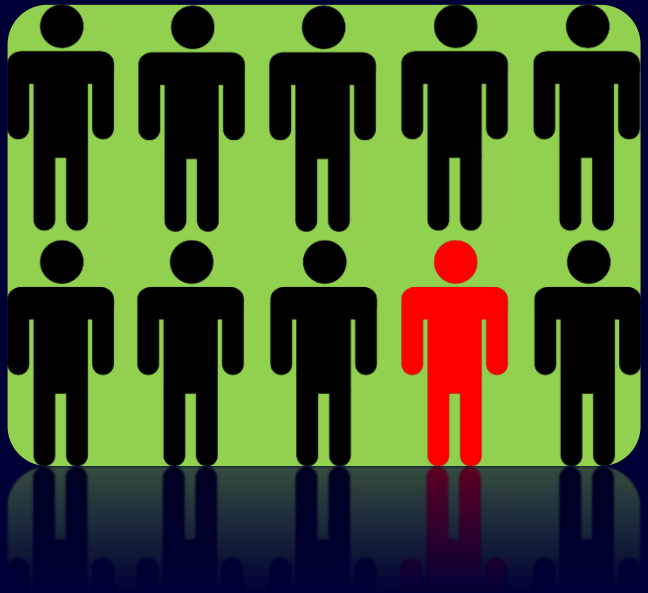


- Threat intelligence enables GuardDuty to identify the following
  - Known malware-infected hosts
  - Anonymizing proxies
  - Sites hosting malware and hacker tools
  - Cryptocurrency mining pools and wallets

What can GuardDuty detect?

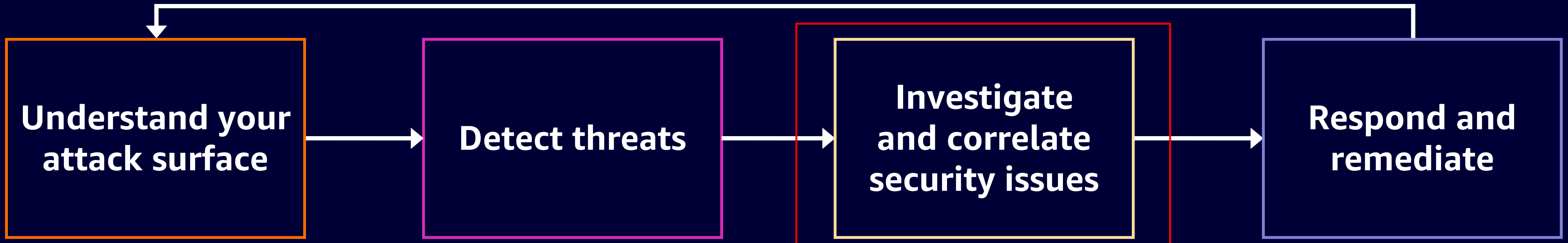
UNKNOWN THREATS USING MACHINE LEARNING

- Algorithms to detect unusual behavior
  - Inspecting signal patterns for heuristics
  - Profiling the normal and looking at deviations
  - Machine learning classifiers



Continuous security monitoring for AWS

Continuous improvement of your AWS security posture



Understand your attack surface

Detect threats

Investigate and correlate security issues

Respond and remediate

Amazon Inspector:
CVE scans and OS-level configurations

Amazon Macie:
Data classification

AWS Security Hub:
Resource and account-level configurations

NIST CSF function:
IDENTIFY

Amazon GuardDuty:
Automated intelligent threat detection

NIST CSF function:
DETECT

Amazon Detective:
Security investigations

AWS Security Hub:
Alert aggregation

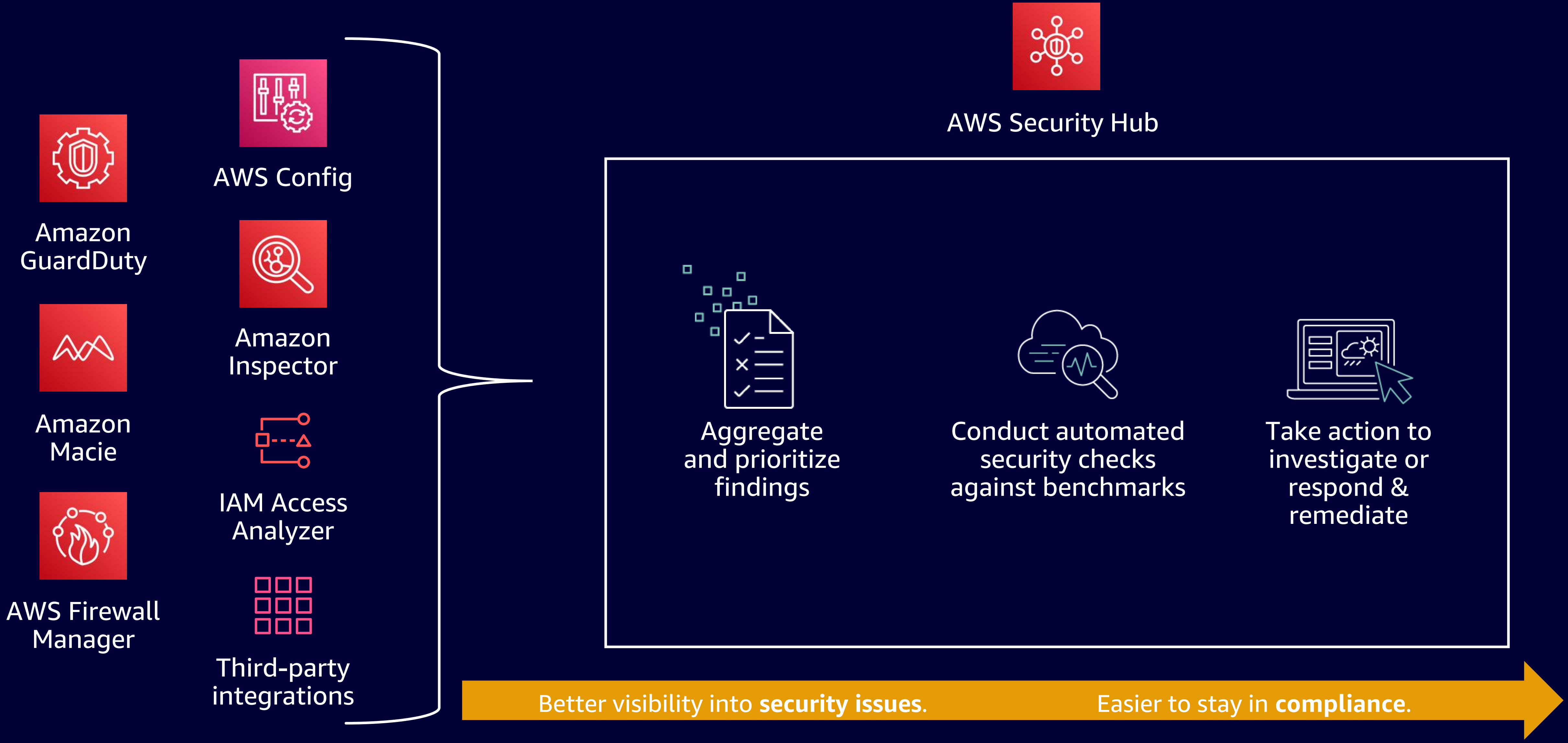
NIST CSF function:
DETECT

AWS Security Hub:
Automated response and remediation runbooks and ITSM or “taking action” integrations

NIST CSF function:
RESPOND

NIST CSF functions covered by other AWS services: PROTECT – AWS identity, crypto, and edge protection services; RECOVER – AWS backup services

How AWS Security Hub works



Amazon GuardDuty
Amazon Macie
AWS Firewall Manager
AWS Config
Amazon Inspector
IAM Access Analyzer
Third-party integrations
AWS Security Hub
Aggregate and prioritize findings
Conduct automated security checks against benchmarks
Take action to investigate or respond & remediate
Better visibility into **security issues**.
Easier to stay in **compliance**.

Simple and Scalable Security Monitoring

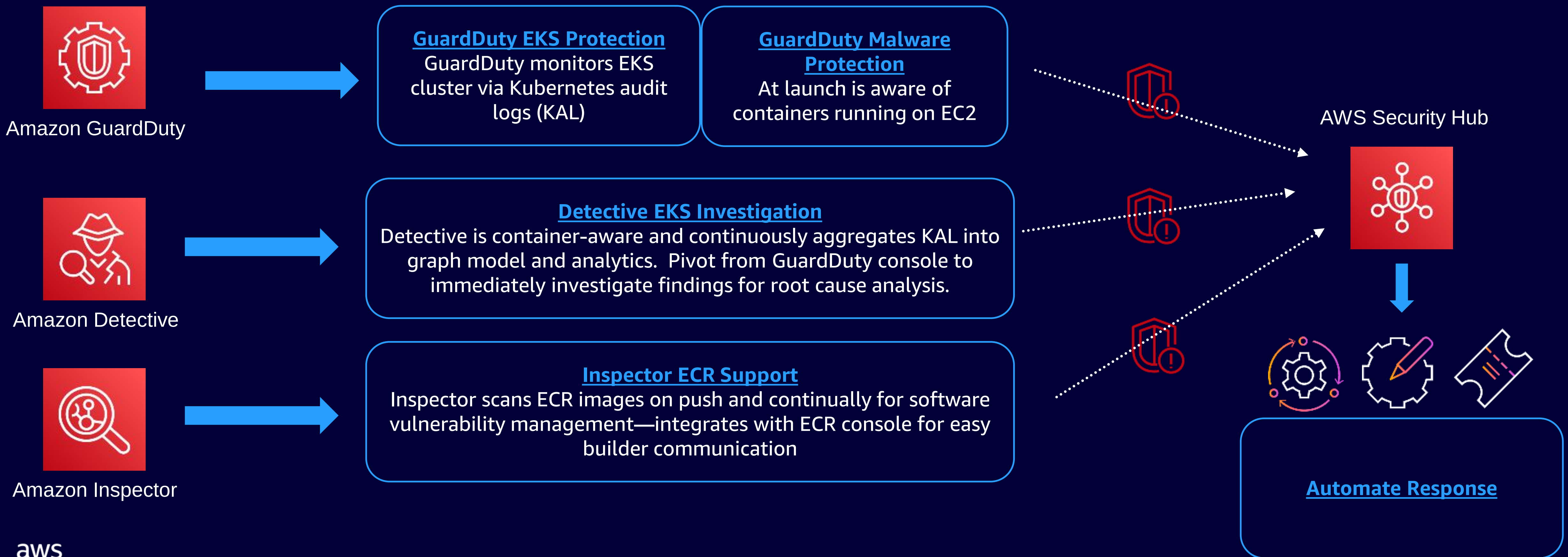
Scale existing services

Simple and easy deployment

AWS Orgs assures environment-wide enablement

Continuous monitoring

Centralization of security findings scales and automates operations



GuardDuty EKS Protection
GuardDuty monitors EKS cluster via Kubernetes audit logs (KAL)

GuardDuty Malware Protection
At launch is aware of containers running on EC2

Detective EKS Investigation
Detective is container-aware and continuously aggregates KAL into graph model and analytics. Pivot from GuardDuty console to immediately investigate findings for root cause analysis.

Inspector ECR Support
Inspector scans ECR images on push and continually for software vulnerability management—integrates with ECR console for easy builder communication

Automate Response

Amazon Detective

INVESTIGATIVE LAYER

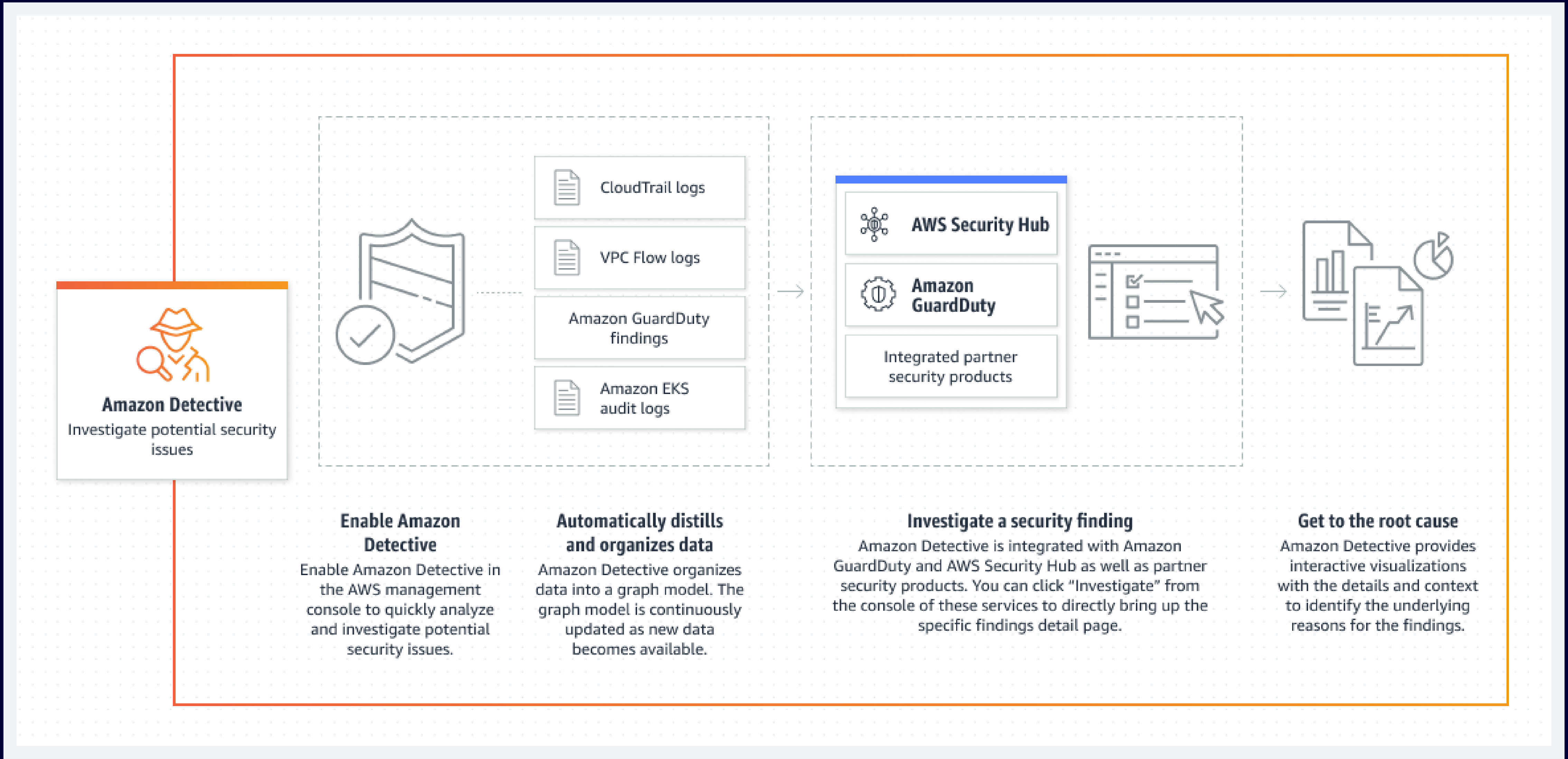
Quickly analyze, investigate, and identify root cause of security issues

Built-in data collection

Automated analysis

Visual insights

How Amazon Detective works



Amazon Detective

Investigate potential security issues

CloudTrail logs

VPC Flow logs

Amazon GuardDuty findings

Amazon EKS audit logs

AWS Security Hub

Amazon GuardDuty

Integrated partner security products

Enable Amazon Detective

Enable Amazon Detective in the AWS management console to quickly analyze and investigate potential security issues.

Automatically distills and organizes data

Amazon Detective organizes data into a graph model. The graph model is continuously updated as new data becomes available.

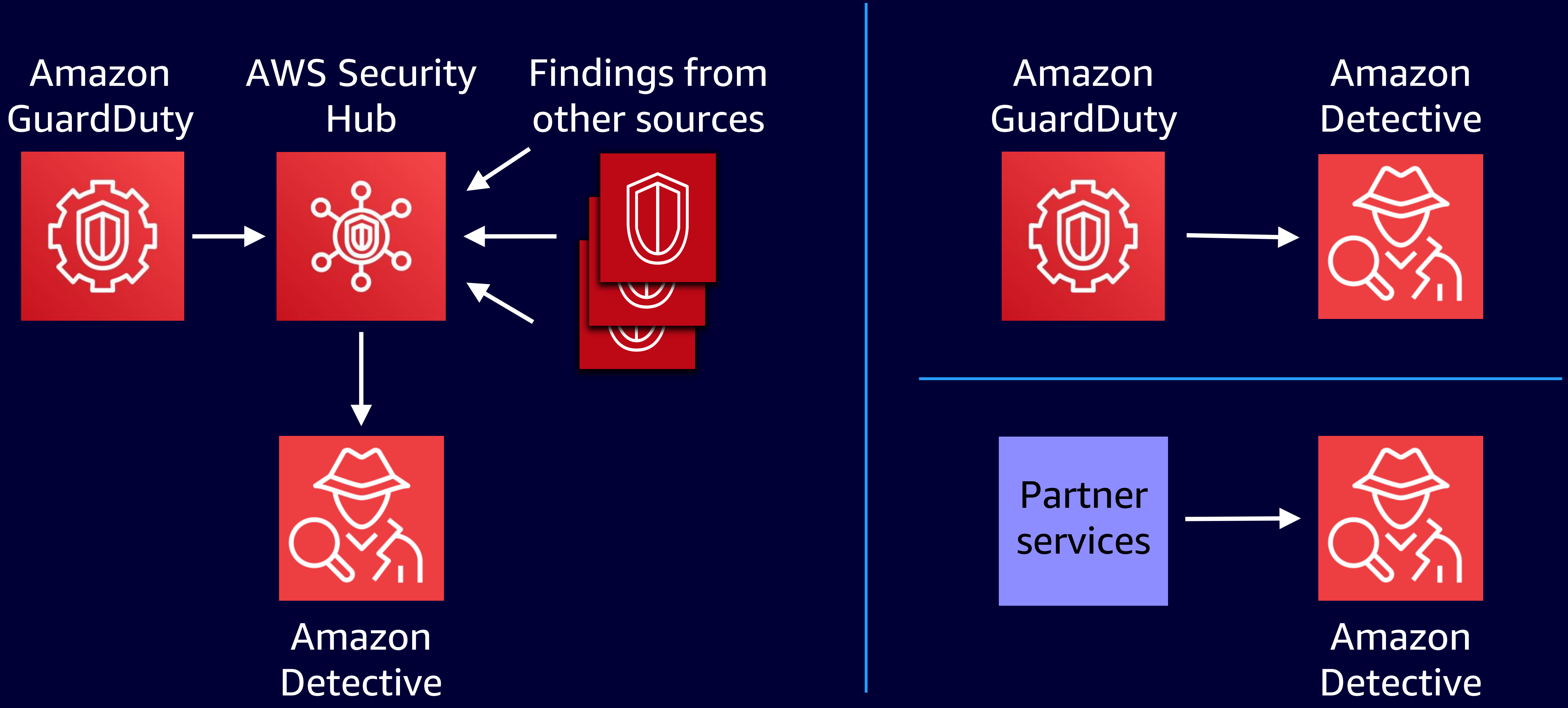
Investigate a security finding

Amazon Detective is integrated with Amazon GuardDuty and AWS Security Hub as well as partner security products. You can click "Investigate" from the console of these services to directly bring up the specific findings detail page.

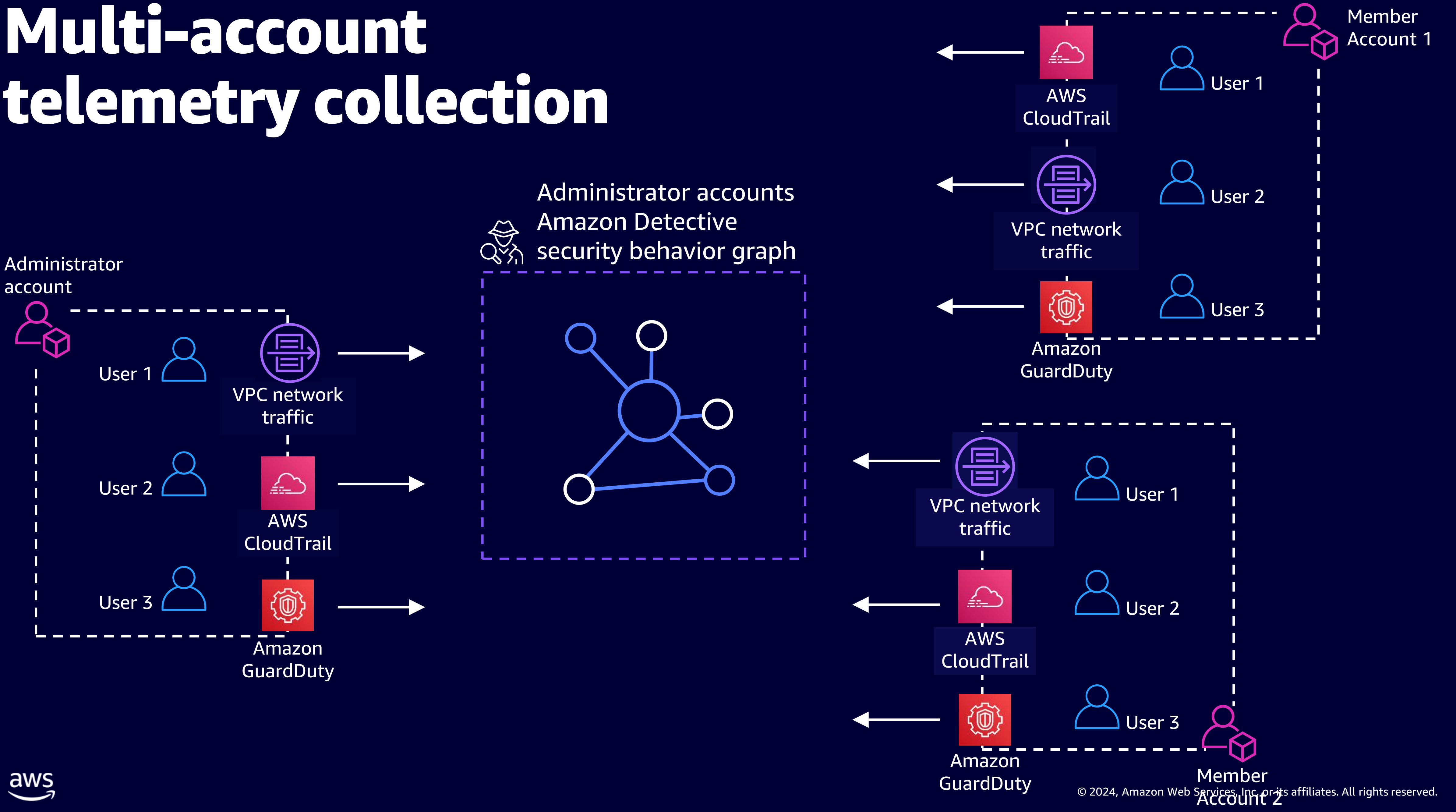
Get to the root cause

Amazon Detective provides interactive visualizations with the details and context to identify the underlying reasons for the findings.

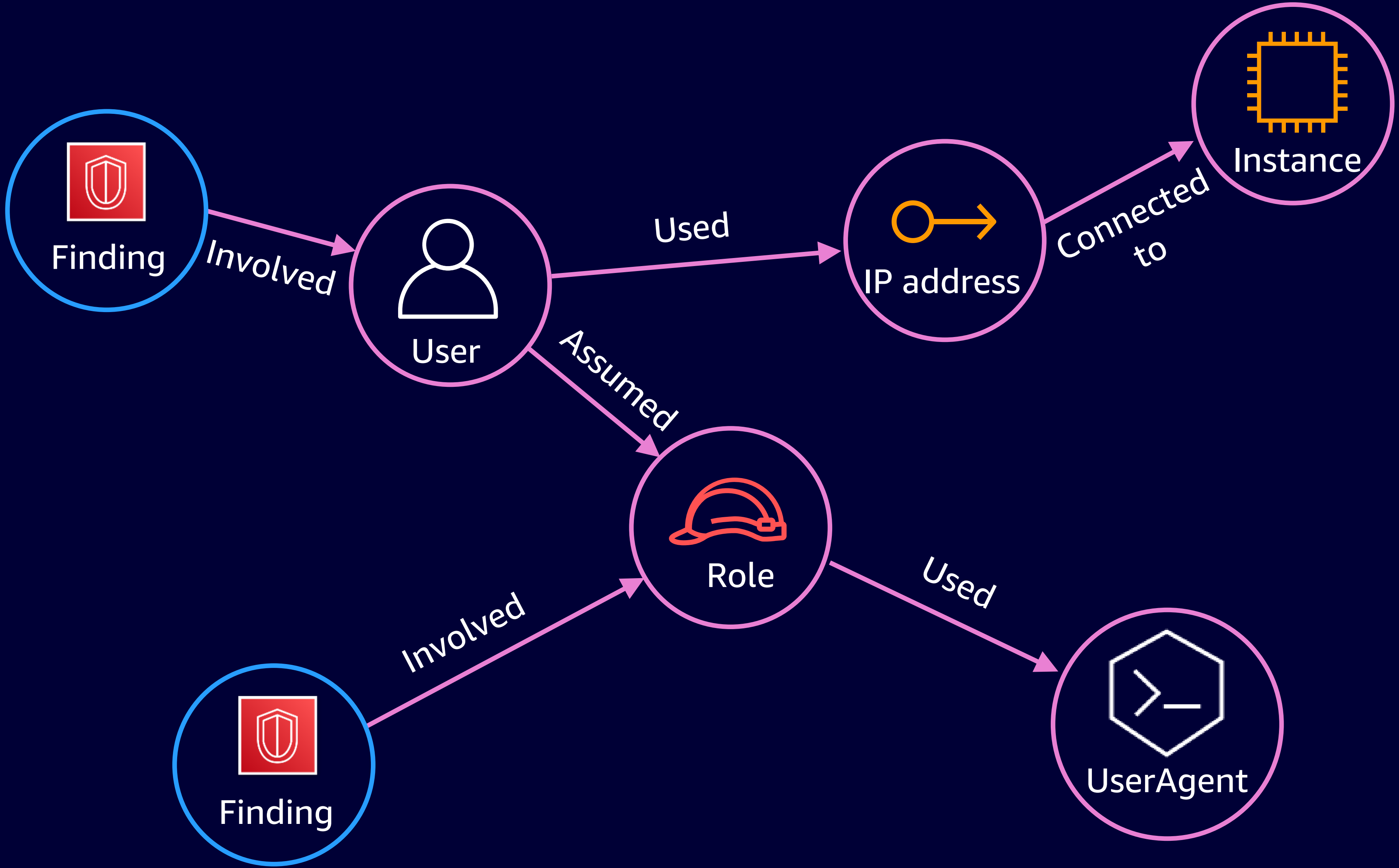
Amazon Detective usage flow



Multi-account telemetry collection



Security behavior graph



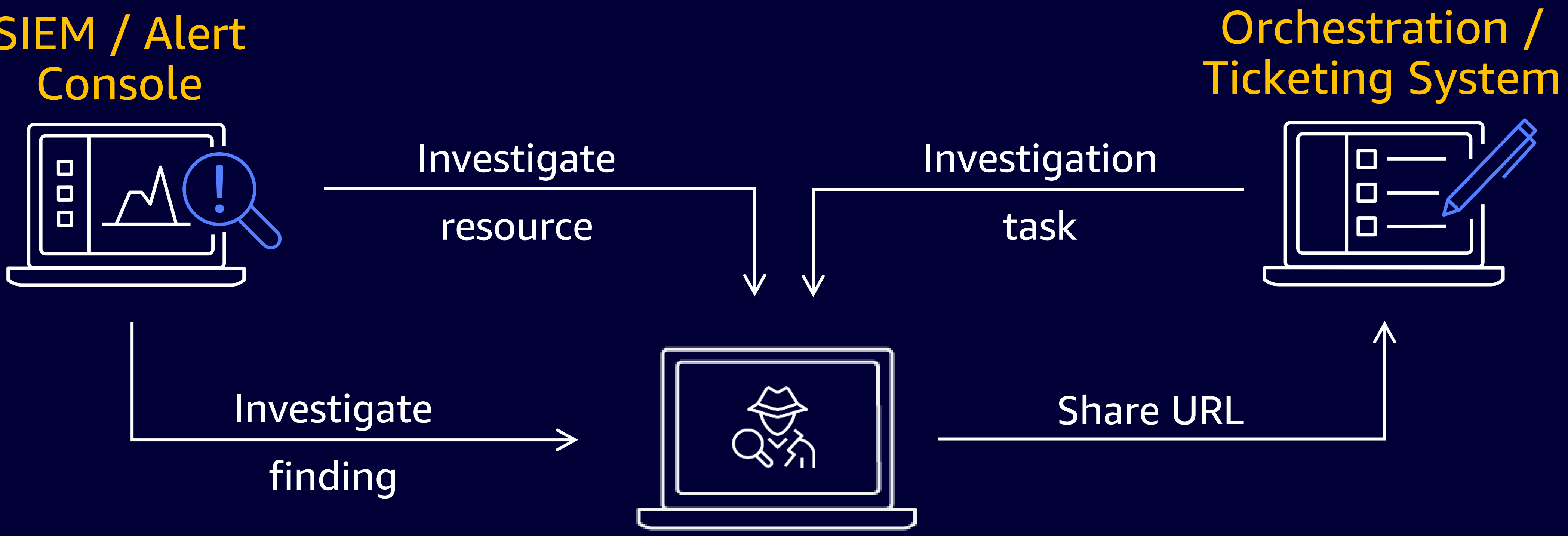
Amazon Detective EKS Support

- **Amazon Detective** security investigations for Amazon Elastic Kubernetes Service (Amazon EKS) clusters to quickly analyze, investigate, and identify the root-cause of malicious or suspicious behavior that represents potential threats to container workloads.

➡ Review Amazon EKS specific activity, such as pod volume patterns and container service user activity, including divergent behavior within and across EKS clusters

➡ Investigate security findings with their EKS clusters, such as cryptocurrency mining, unintentional admin privilege exposure, container misconfigurations that allow access to underlying EC2 nodes, or behavioral patterns common to compromised container clusters.

Amazon Detective workflow integration



SIEM / Alert Console

Orchestration / Ticketing System

Investigate resource

Investigation task

Investigate finding

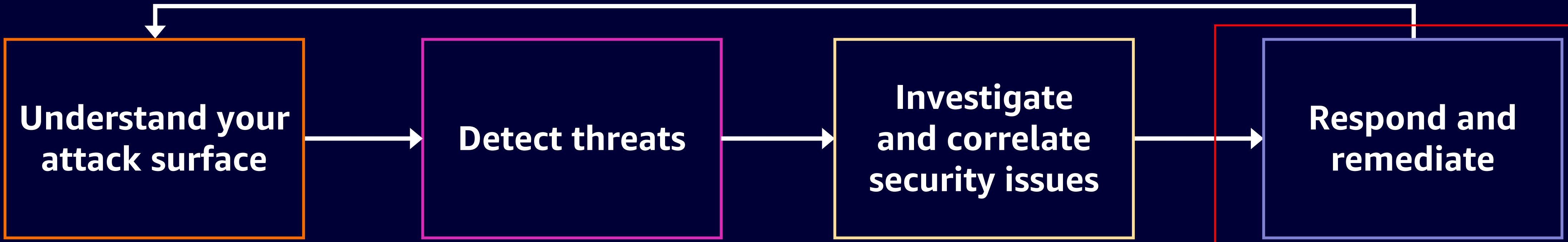
Share URL

Amazon Detective

- Allows multi-account enablement with no data sources to configure
- Decreases complexity and increases efficiency of your AWS security investigations
- Is graph-based with purpose-built model
- Enables multiple personas on your security team to look back at findings for up to 1 year
- Records analytic baselines for common types of activity
- Is integrated tightly with GuardDuty to start deep investigations on findings with one click

Continuous security monitoring for AWS

Continuous improvement of your AWS security posture


Understand your attack surface
Detect threats
Investigate and correlate security issues
Respond and remediate

Amazon Inspector:
CVE scans and OS-level configurations
Amazon Macie:
Data classification
AWS Security Hub:
Resource and account-level configurations

NIST CSF function:
IDENTIFY

Amazon GuardDuty:
Automated intelligent threat detection

NIST CSF function:
DETECT

Amazon Detective:
Security investigations
AWS Security Hub:
Alert aggregation

NIST CSF function:
DETECT

AWS Security Hub:
Automated response and remediation runbooks and ITSM or “taking action” integrations

NIST CSF function:
RESPOND

NIST CSF functions covered by other AWS services: PROTECT – AWS identity, crypto, and edge protection services; RECOVER – AWS backup services

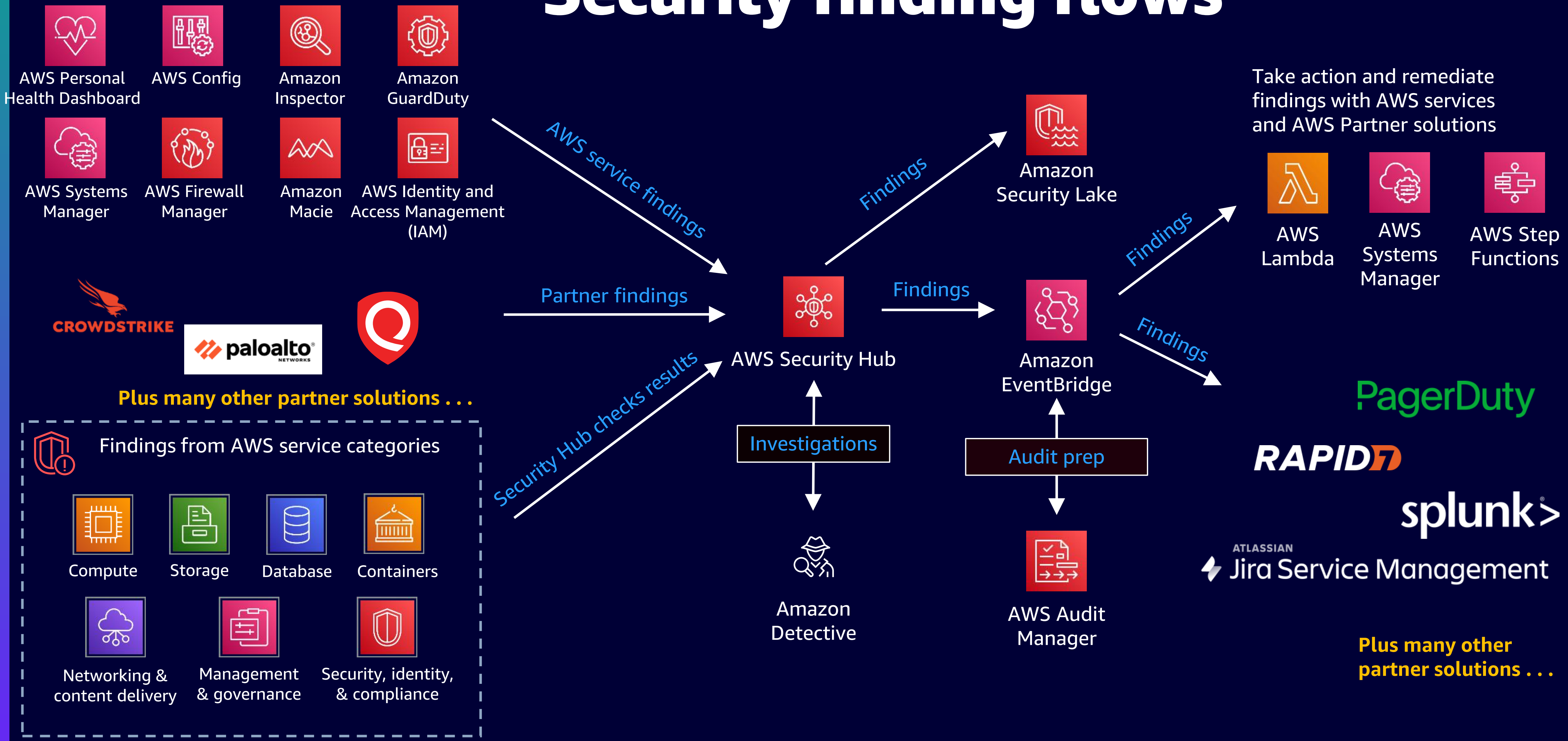
Security Hub as a central dashboard

Centralize across accounts and prioritize findings without needing to normalize

View security and compliance posture against key standards

Take automated action on findings through Amazon Eventbridge

Security finding flows



AWS Personal Health Dashboard

AWS Config

Amazon Inspector

Amazon GuardDuty

AWS Systems Manager

AWS Firewall Manager

Amazon Macie

AWS Identity and Access Management (IAM)

CROWDSTRIKE

paloalto NETWORKS

Plus many other partner solutions . . .

Findings from AWS service categories

Compute

Storage

Database

Containers

Networking & content delivery

Management & governance

Security, identity, & compliance

AWS service findings

Partner findings

Security Hub checks results

AWS Security Hub

Findings

Amazon Security Lake

Findings

Amazon EventBridge

Investigations

Amazon Detective

Audit prep

AWS Audit Manager

Take action and remediate findings with AWS services and AWS Partner solutions

Findings

AWS Lambda

AWS Systems Manager

AWS Step Functions

Findings

PagerDuty

RAPID7

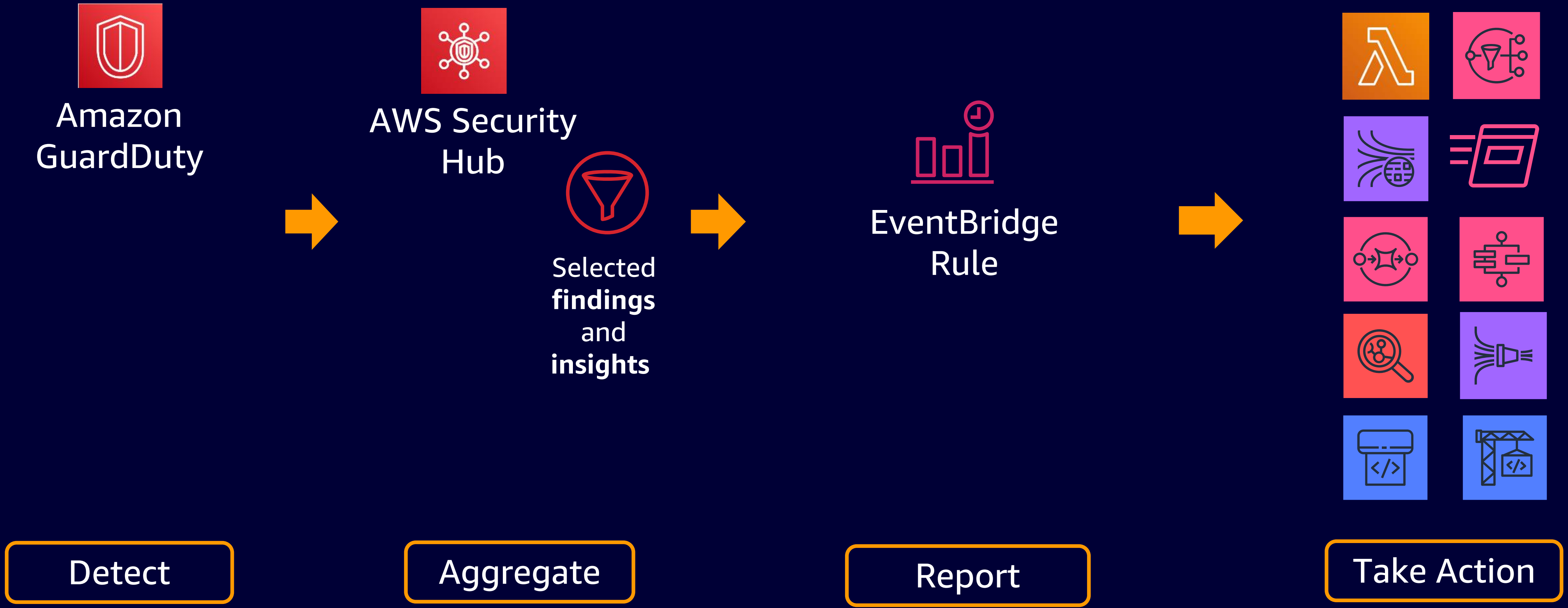
splunk>

ATLASSIAN Jira Service Management

Plus many other partner solutions . . .

aws

Acting on findings



Amazon GuardDuty

AWS Security Hub

Selected **findings** and **insights**

EventBridge Rule

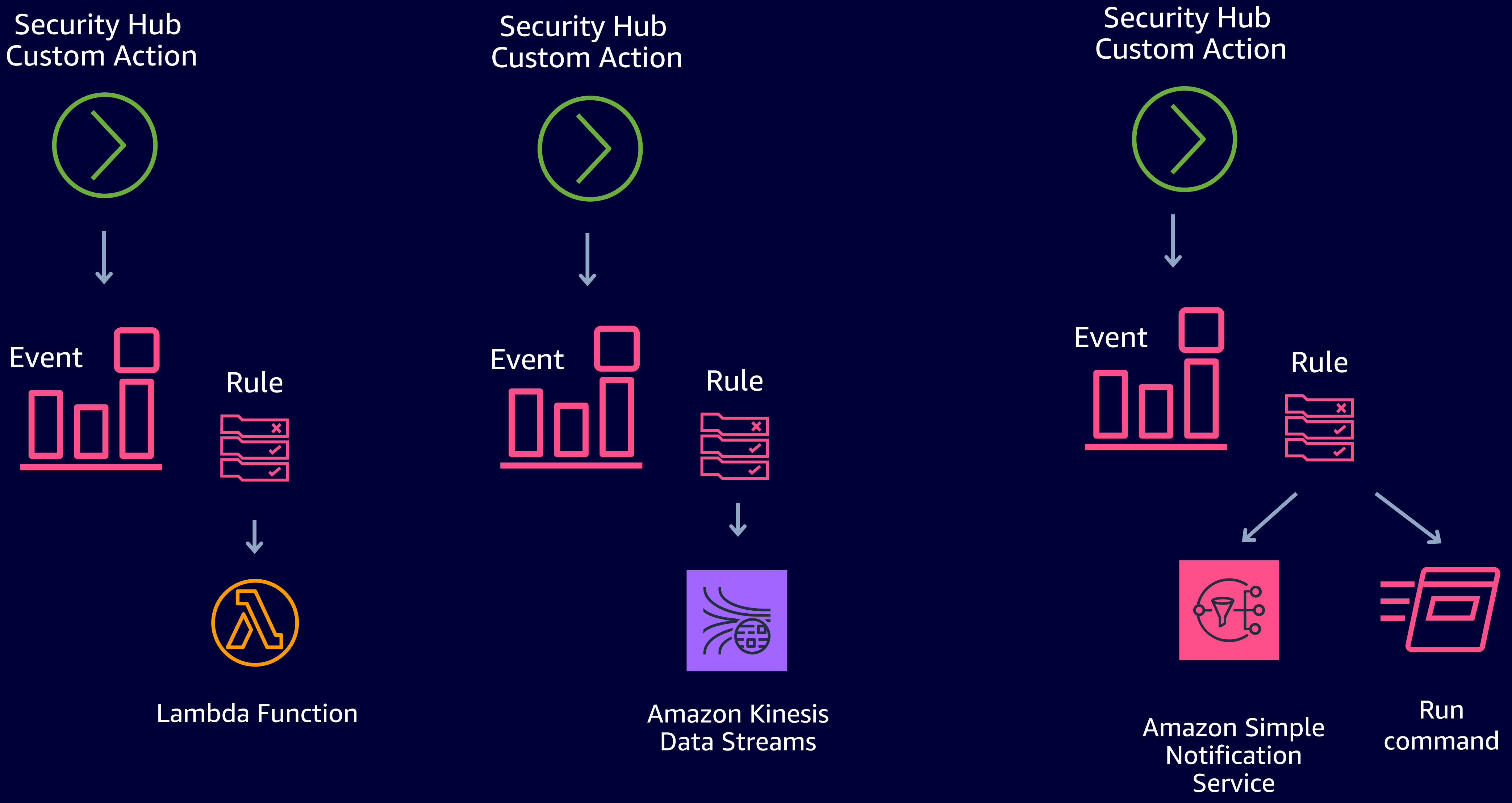
Detect

Aggregate

Report

Take Action

Use Security Hub Custom Actions to trigger automation



Security Hub Custom Action

Event

Rule

Lambda Function

Security Hub Custom Action

Event

Rule

Amazon Kinesis Data Streams

Security Hub Custom Action

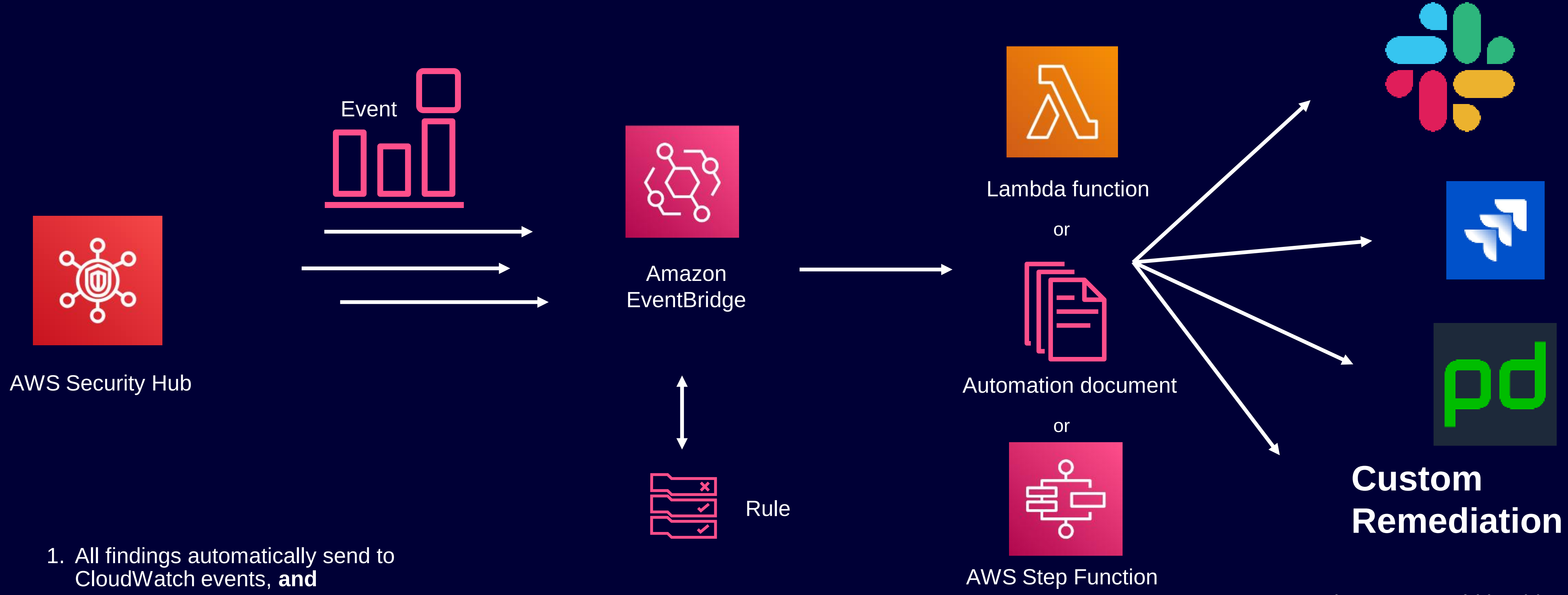
Event

Rule

Amazon Simple Notification Service

Run command

Customizable response and remediation actions



1. All findings automatically send to CloudWatch events, **and**

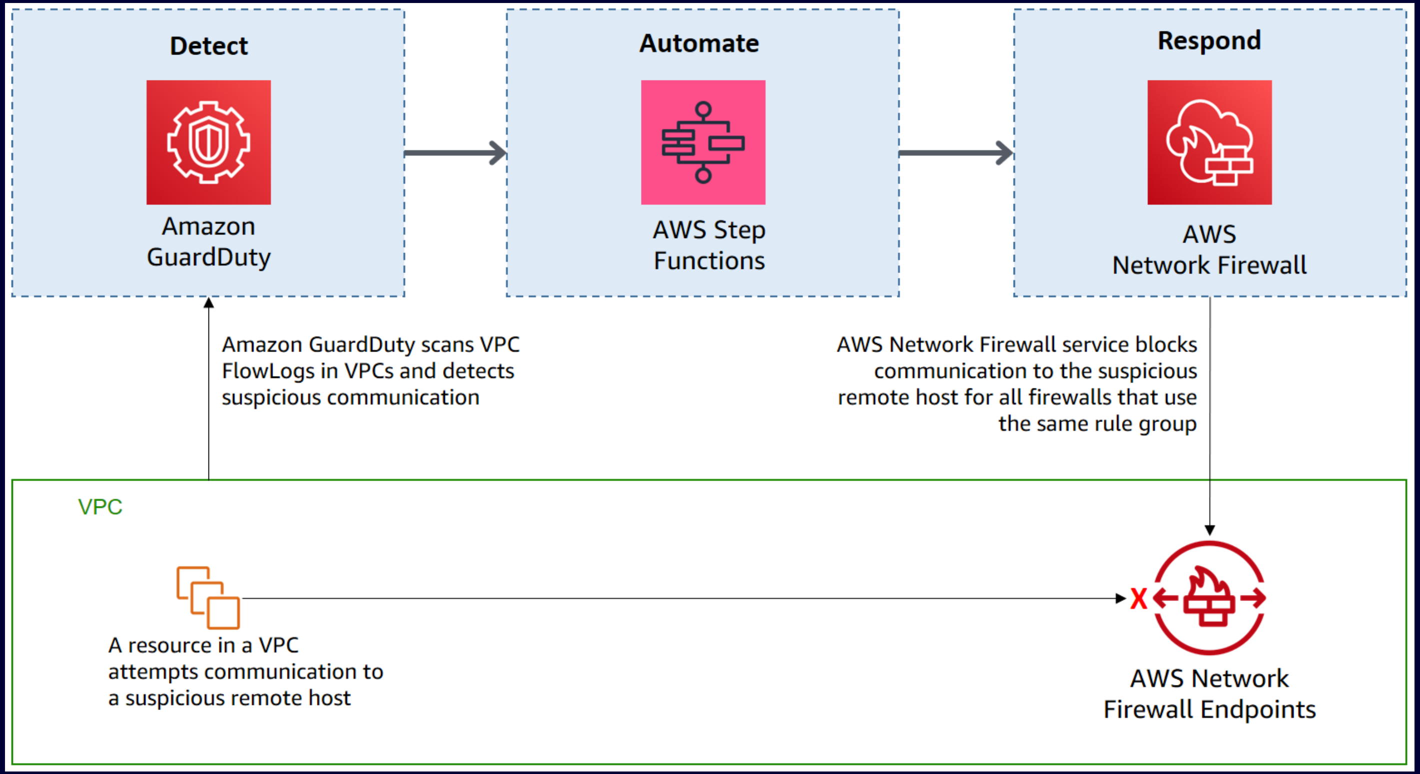
2. Security Hub user can select findings in the console and take a custom action on them. These findings are sent to CloudWatch decorated with a custom action ID

3. User creates Amazon CloudWatch Events rules to look for certain findings associated with a custom action ID or findings with specific characteristics.

4. The rule defines a target, typically a Lambda function, Step Function, or Automation document

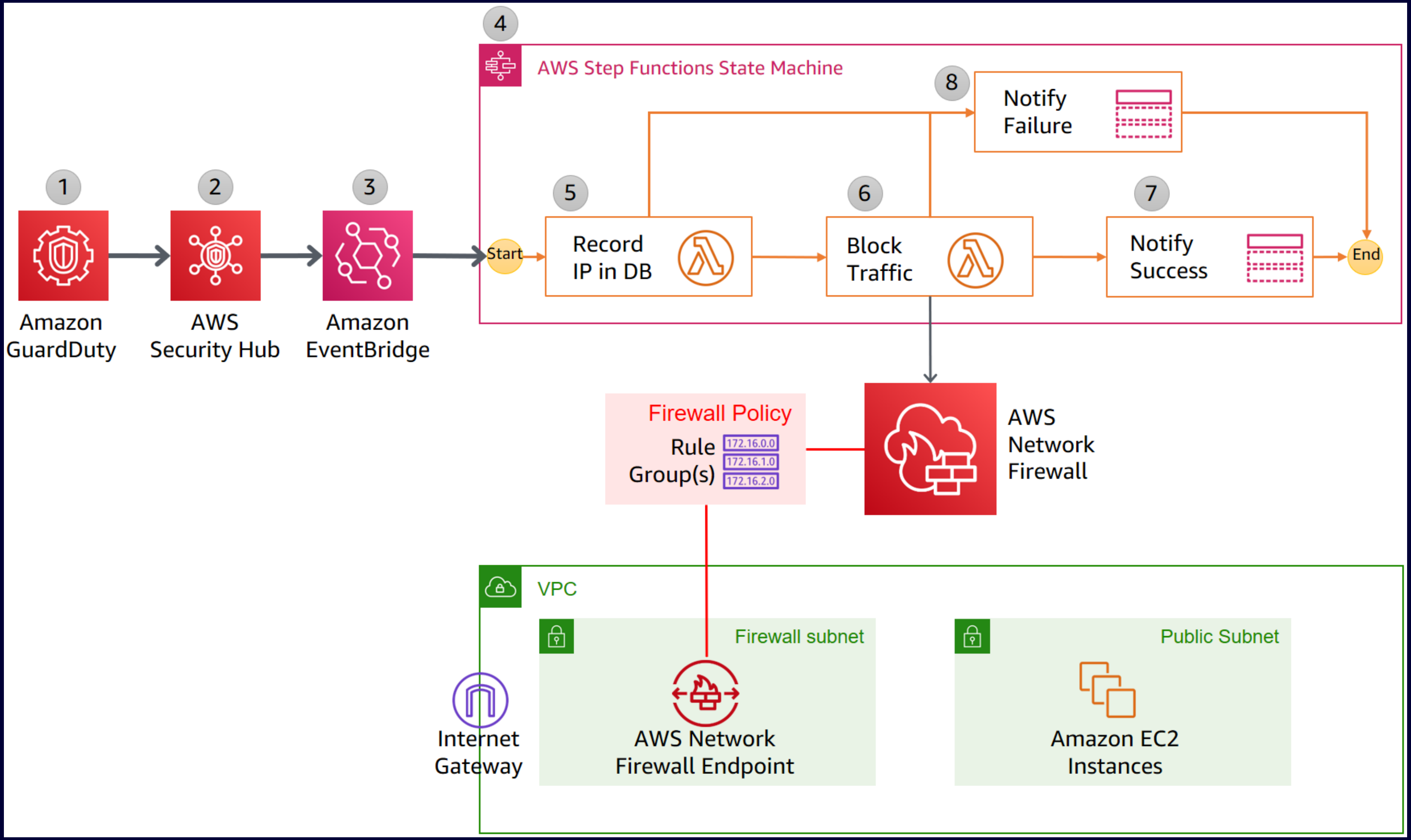
5. The target could be things like a chat, ticketing, on-call management, SOAR platform, or custom remediation playbook

Automated detection & response

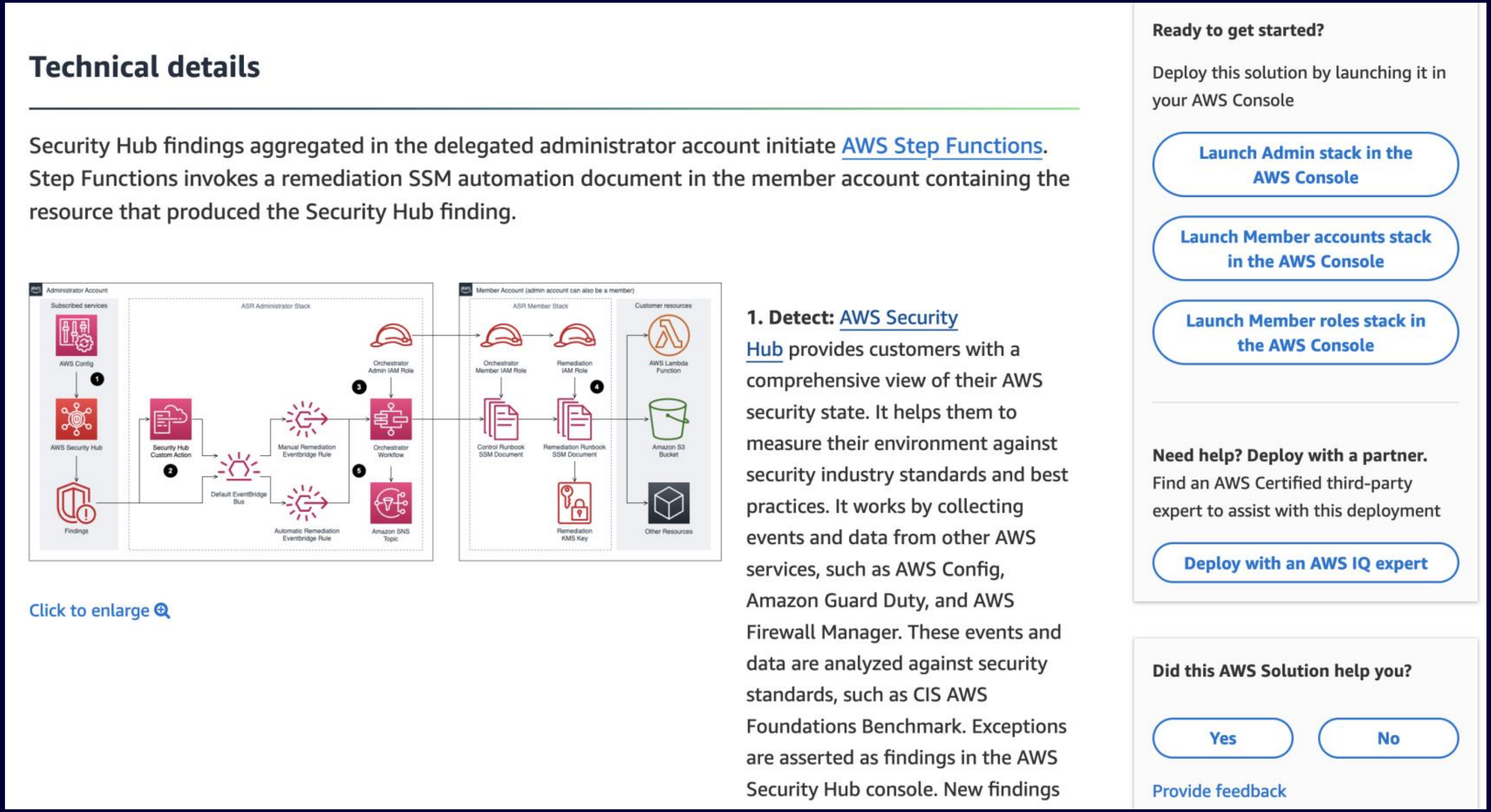

Detect
Amazon GuardDuty
Automate
AWS Step Functions
Respond
AWS Network Firewall
Amazon GuardDuty scans VPC FlowLogs in VPCs and detects suspicious communication
AWS Network Firewall service blocks communication to the suspicious remote host for all firewalls that use the same rule group
VPC
A resource in a VPC attempts communication to a suspicious remote host
X
AWS Network Firewall Endpoints

- Blocking traffic to and from suspicious remote hosts, for example to IP addresses associated with known command and control servers for botnets.
- GuardDuty detection of unintended communication with remote hosts triggers a series of steps, including blocking of network traffic to those hosts by using Network Firewall, and notification of security operators.

Customizable response and remediation actions



Automated security response on AWS



Technical details

Security Hub findings aggregated in the delegated administrator account initiate AWS Step Functions. Step Functions invokes a remediation SSM automation document in the member account containing the resource that produced the Security Hub finding.

1. **Detect:** AWS Security Hub provides customers with a comprehensive view of their AWS security state. It helps them to measure their environment against security industry standards and best practices. It works by collecting events and data from other AWS services, such as AWS Config, Amazon Guard Duty, and AWS Firewall Manager. These events and data are analyzed against security standards, such as CIS AWS Foundations Benchmark. Exceptions are asserted as findings in the AWS Security Hub console. New findings

Ready to get started?

Deploy this solution by launching it in your AWS Console

Launch Admin stack in the AWS Console
Launch Member accounts stack in the AWS Console
Launch Member roles stack in the AWS Console

Need help? Deploy with a partner.
Find an AWS Certified third-party expert to assist with this deployment

Did this AWS Solution help you?

https://aws.amazon.com/solutions/implementations/automated-security-response-on-aws//

Centralized management of your security data

Preview

Amazon Security Lake

AUTOMATICALLY CENTRALIZE SECURITY DATA INTO A PURPOSE-BUILT DATA LAKE IN A FEW CLICKS

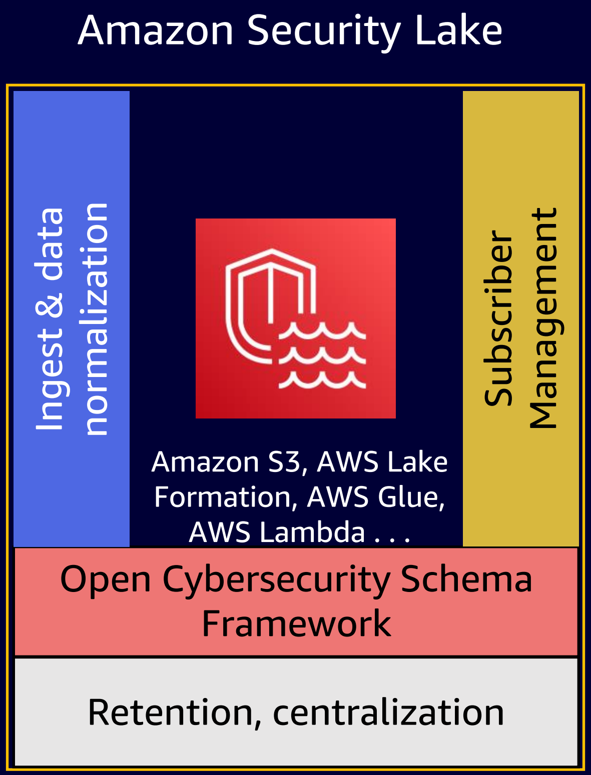
Centralize data automatically from cloud, on premises, and custom security sources across regions

Optimize and manage security data for more efficient storage and query performance

Normalize data to an industry standard to easily share and use with multiple analytics tools

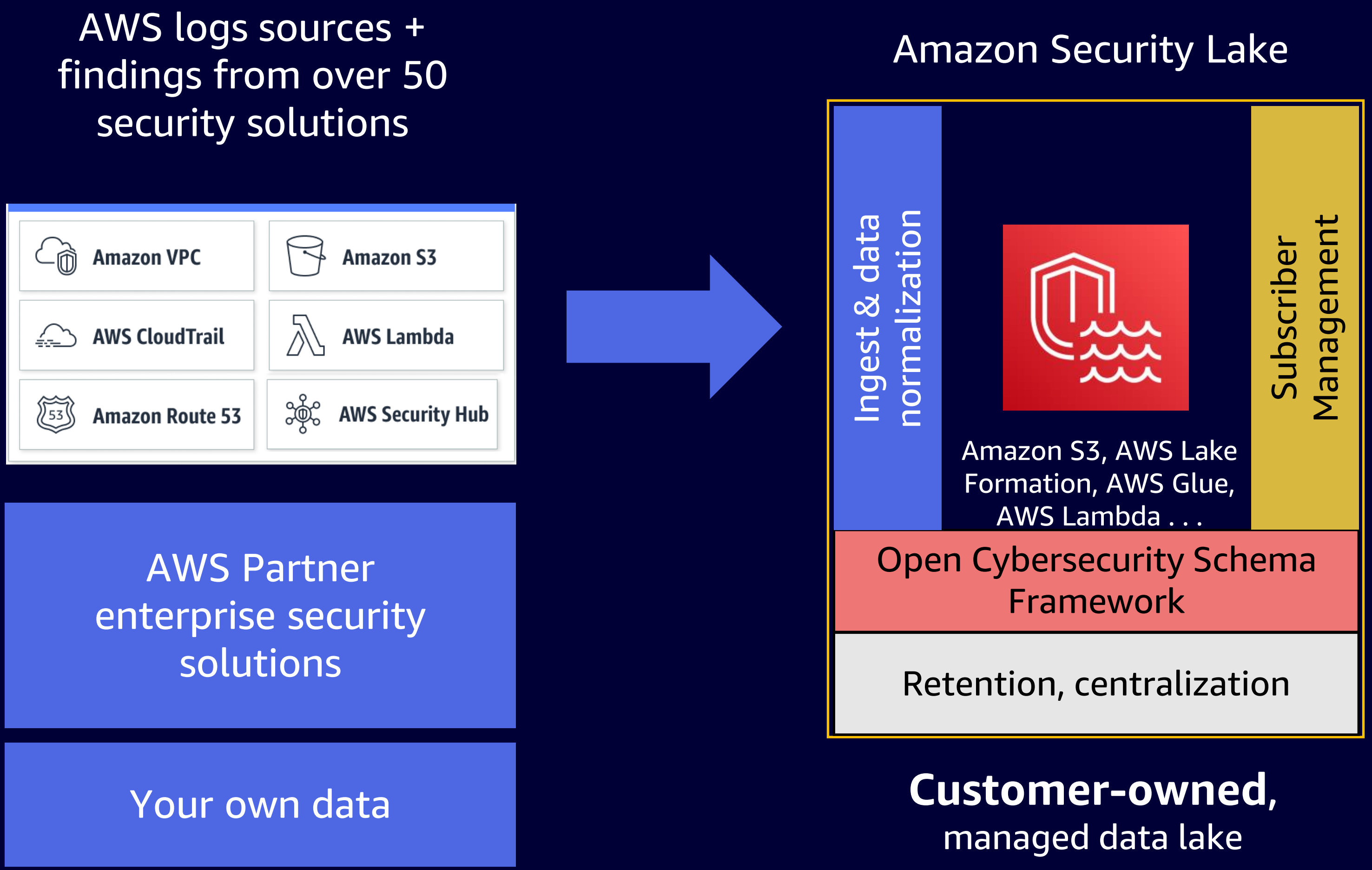
Analyze using your preferred analytics tools while retaining control and ownership of your security data

How it works


Amazon Security Lake
Ingest & data normalization
Subscriber Management
Amazon S3, AWS Lake Formation, AWS Glue, AWS Lambda . . .
Open Cybersecurity Schema Framework
Retention, centralization

Customer-owned,
managed data lake

How it works



AWS logs sources + findings from over 50 security solutions

AWS Partner enterprise security solutions

Your own data

Amazon Security Lake

Ingest & data normalization

Amazon S3, AWS Lake Formation, AWS Glue, AWS Lambda . . .

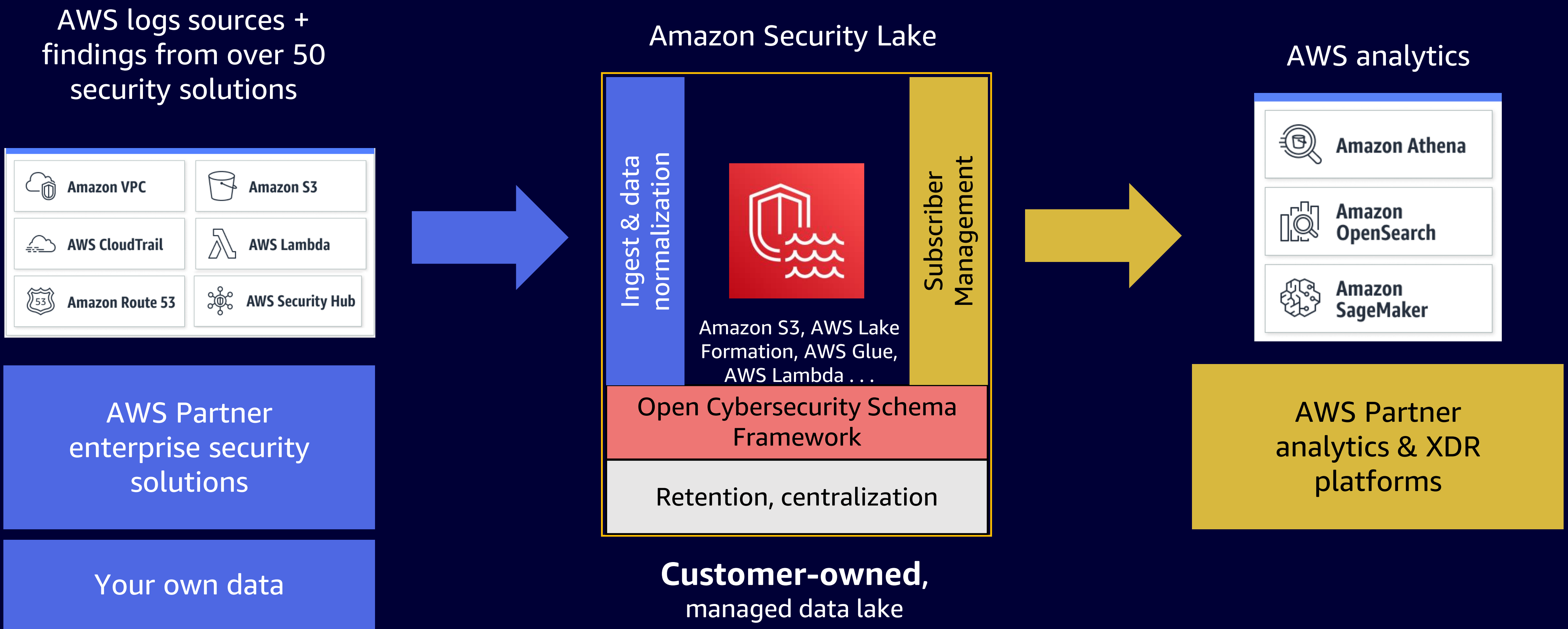
Subscriber Management

Open Cybersecurity Schema Framework

Retention, centralization

Customer-owned,
managed data lake

How it works



AWS logs sources + findings from over 50 security solutions

Amazon VPC

Amazon S3

AWS CloudTrail

AWS Lambda

Amazon Route 53

AWS Security Hub

AWS Partner enterprise security solutions

Your own data

Amazon Security Lake

Ingest & data normalization

Subscriber Management

Amazon S3, AWS Lake Formation, AWS Glue, AWS Lambda . . .

Open Cybersecurity Schema Framework

Retention, centralization

Customer-owned,
managed data lake

AWS analytics

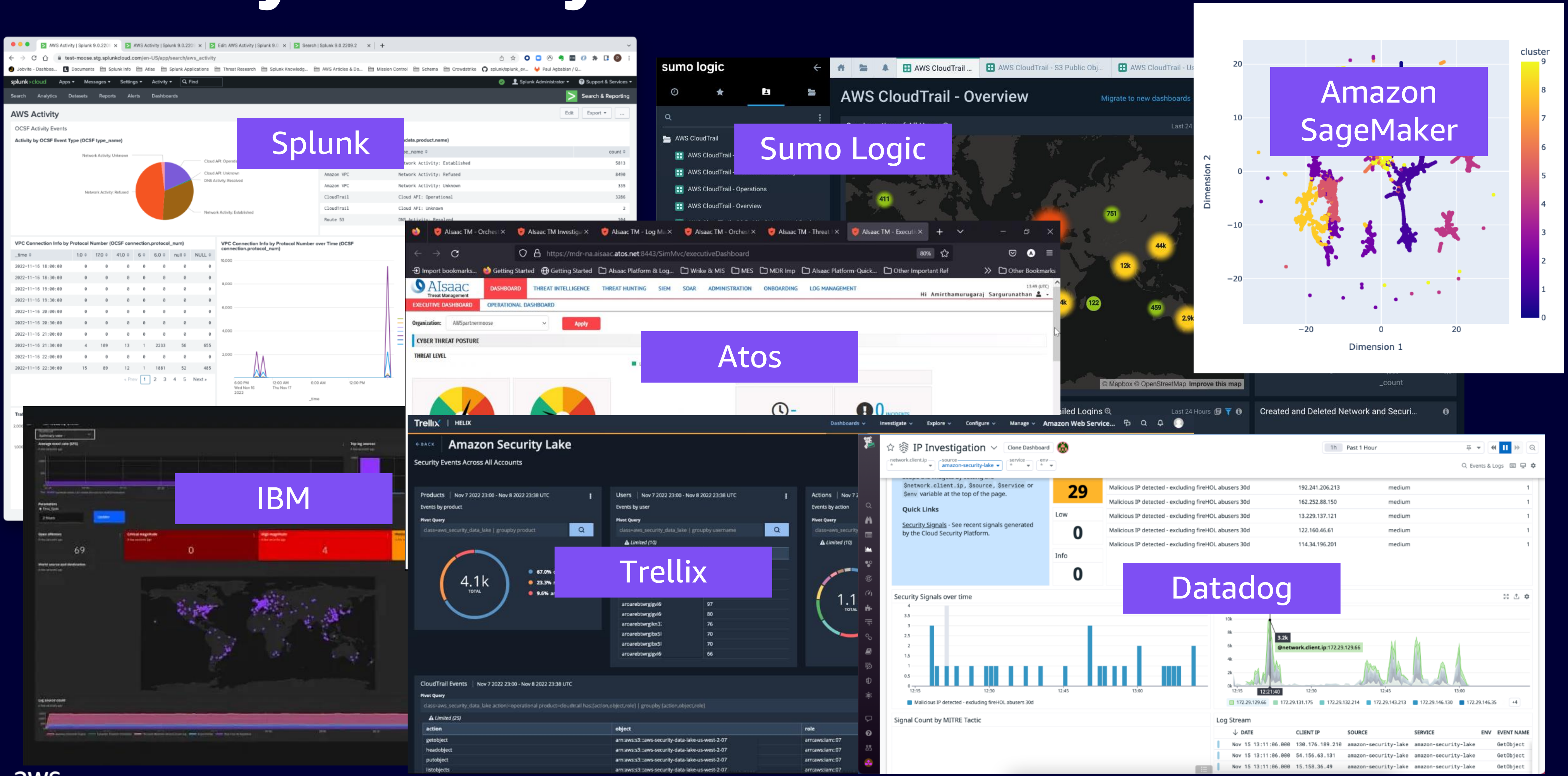
Amazon Athena

Amazon OpenSearch

Amazon SageMaker

AWS Partner analytics & XDR platforms

Choose your analytics



© 2024, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Layer Threat Detection and Response Services

ADVANCED THREAT DETECTION AND RESPONSE ON AWS

Security tools natively available in AWS

Reduce the burden for the security team

Centralized & scalable deployment with a click of a button

Thank you!

Jason Rylands