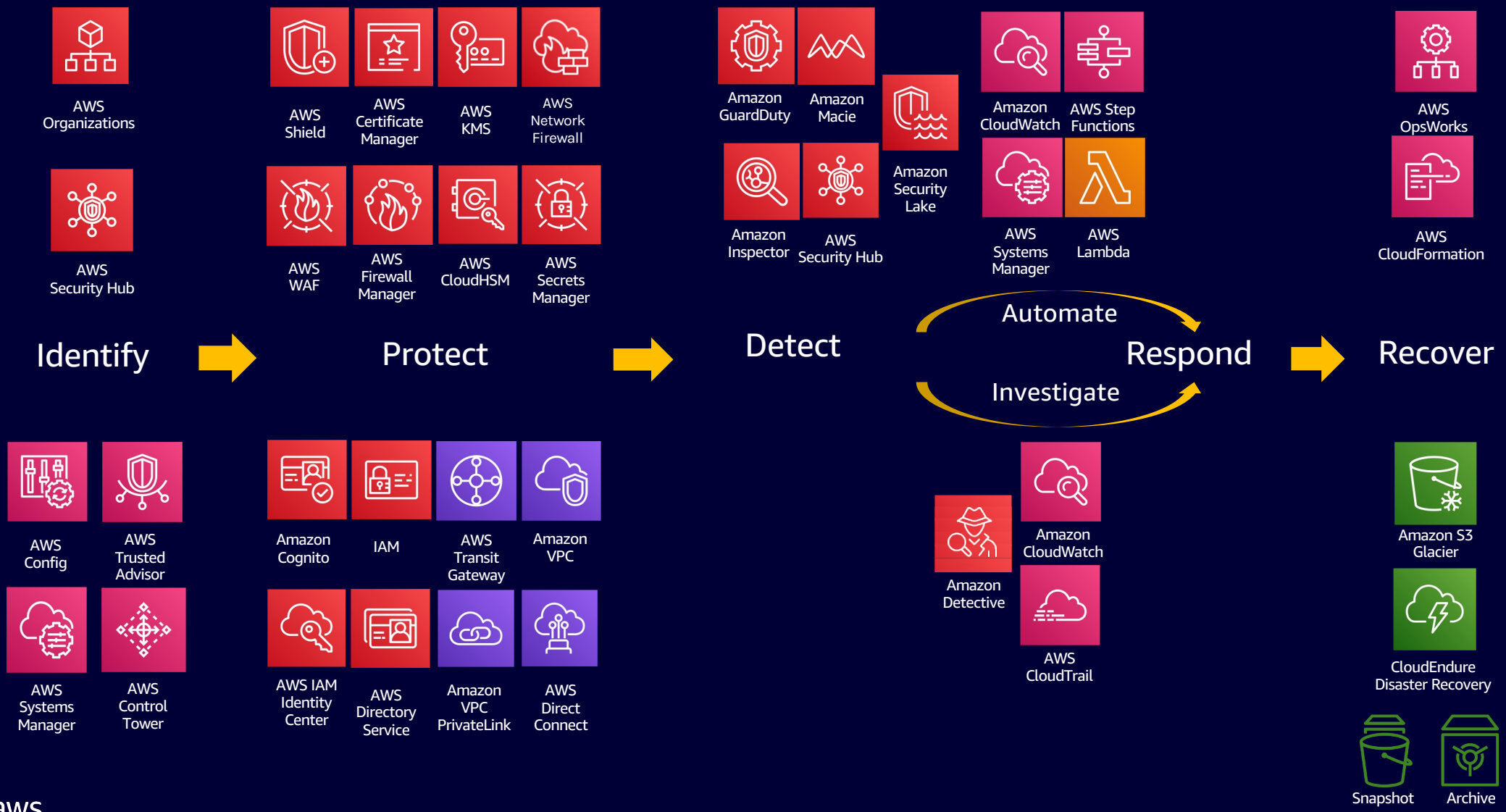
Layering AWS security services to automate incident response

Doug Pardue
Sr. Solutions Architect

Agenda

- AWS layered security services portfolio
- Enabling Threat Detection & Response layer of services at scale
- Adding automated response & remediation
- Best practices to follow

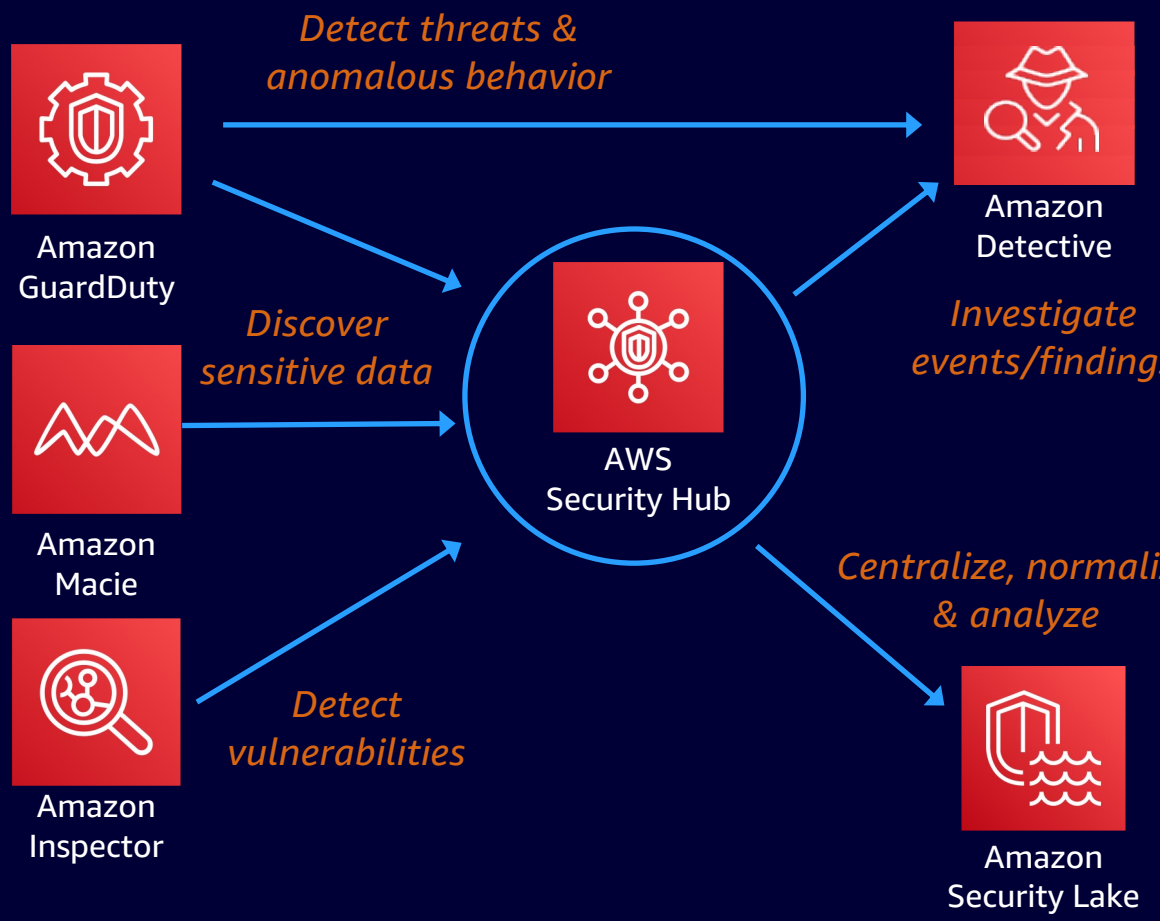
AWS foundational and layered security services



Threat detection, monitoring, and response

Security Monitoring and Threat Detection

Integrated with AWS Workloads in an AWS Account, along with identities and network activity



How do I enable threat detection at scale?

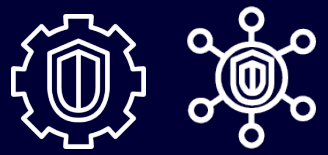
Scalable and centralized management

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

Amazon GuardDuty

FOUNDATIONAL THREAT DETECTION & MONITORING LAYER

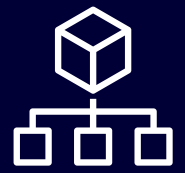
Protect your AWS accounts, workloads, and data with intelligent threat detection and continuous monitoring

One-click activation with no performance impact

Continuous monitoring of AWS accounts and resources

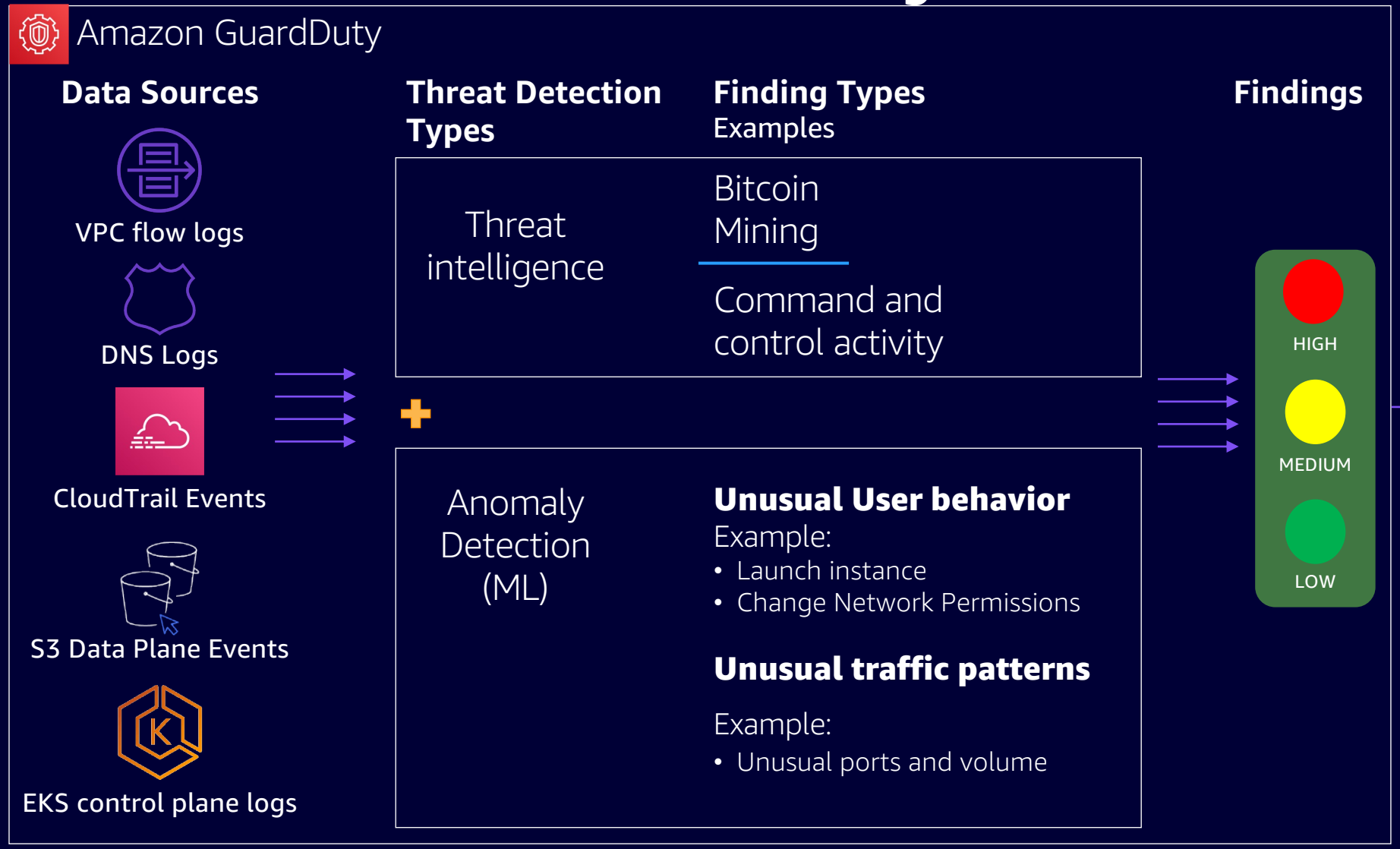
Global coverage with regional results

Detect known & unknown threats



Enterprise-wide consolidation & management

How Amazon GuardDuty works



An Expansion of GuardDuty

Data Sources

- VPC flow logs
- DNS Logs
- Amazon Aurora Login Events
- CloudTrail Events
- S3 Data Plane Events
- EKS control plane logs

Security Analytics

Machine Learning

Threat Intelligence

Continuous learning

Incorporating new machine learning techniques that model RDS login activity to accurately detect suspicious logins to RDS databases

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

GuardDuty Malware Protection

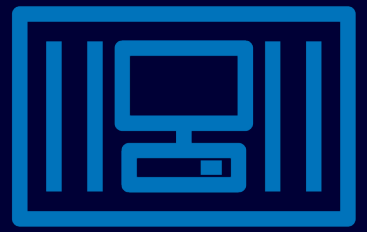
DELIVERS AGENTLESS DETECTION OF MALWARE ON AWS WORKLOADS

Single-click organization-wide malicious file detection

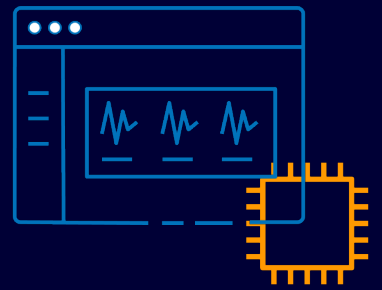
Centralized monitoring, automation, and investigation

Contextualized findings to validate suspicious behavior

No agents to install, update, or maintain



Container aware

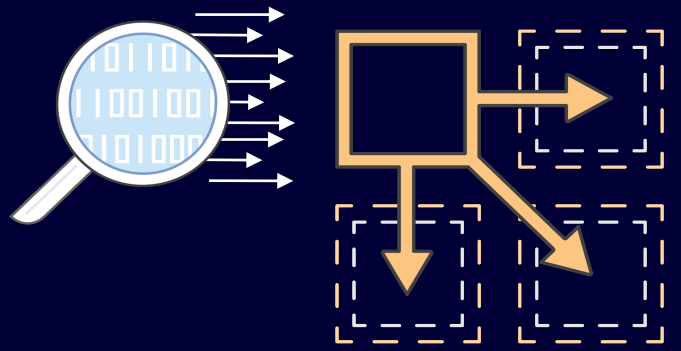


No performance impact or hidden Amazon EC2 costs for scanning

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



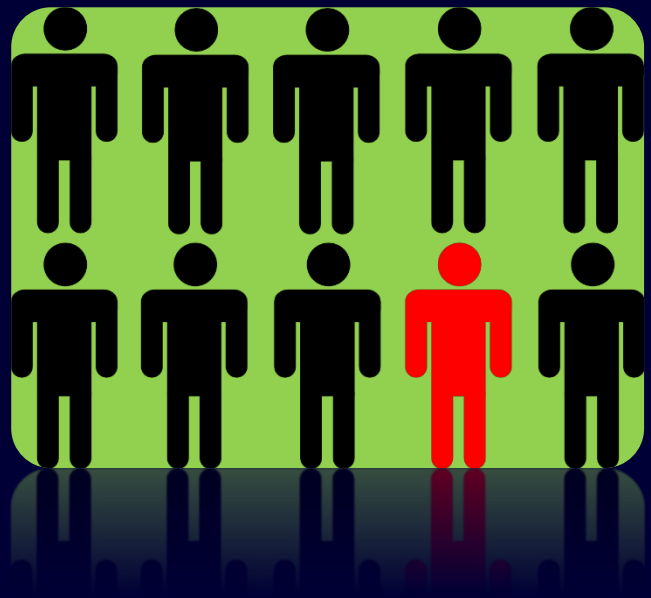
- Threat intelligence enables GuardDuty to identify the following
  - Known malware-infected hosts
  - Anonymizing proxies
  - Sites hosting malware and hacker tools
  - Cryptocurrency mining pools and wallets

aws

What can GuardDuty detect?

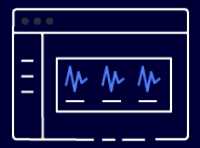
UNKNOWN THREATS USING MACHINE LEARNING

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



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

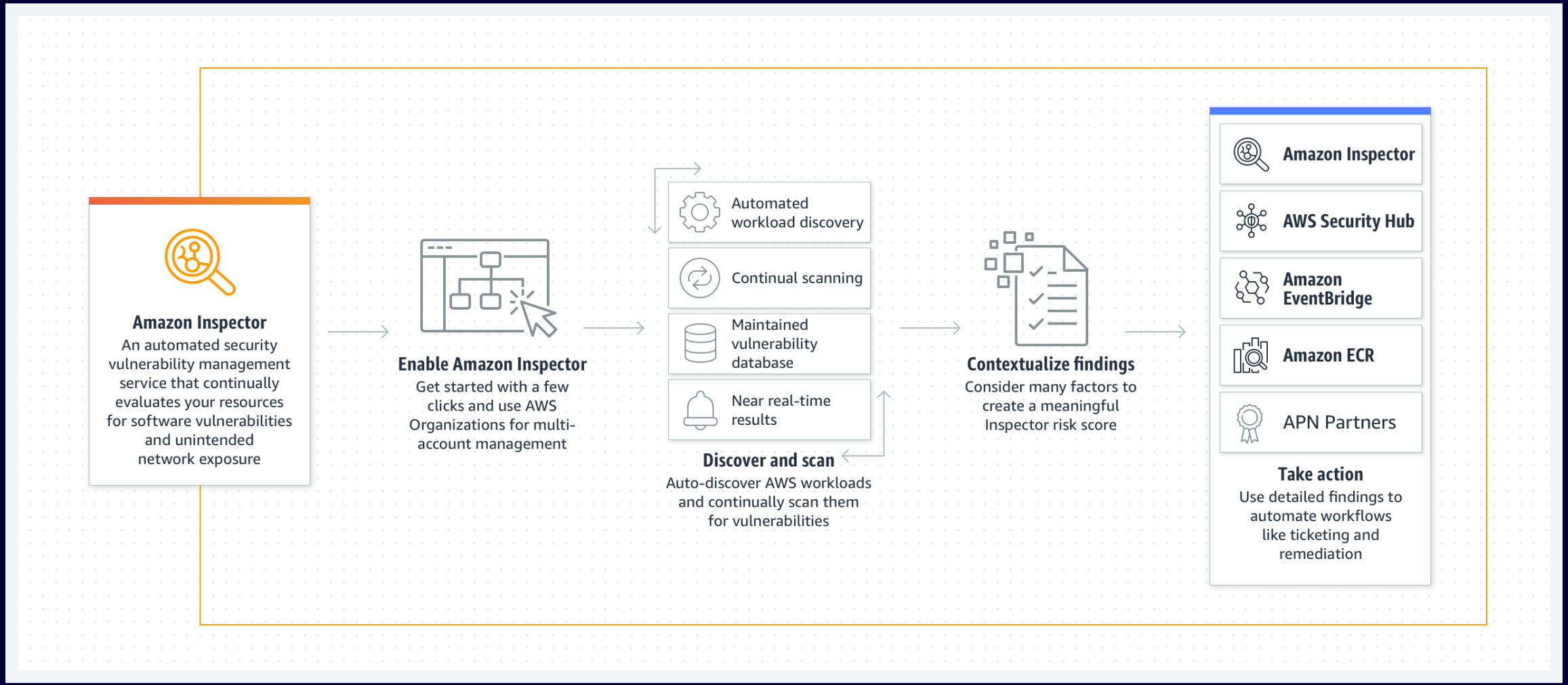
Centrally manage at scale

- 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

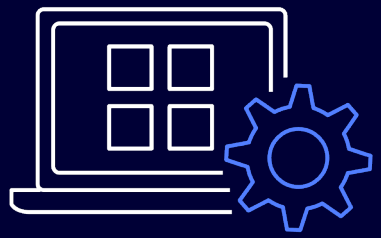


Amazon Detective

INVESTIGATIVE LAYER

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

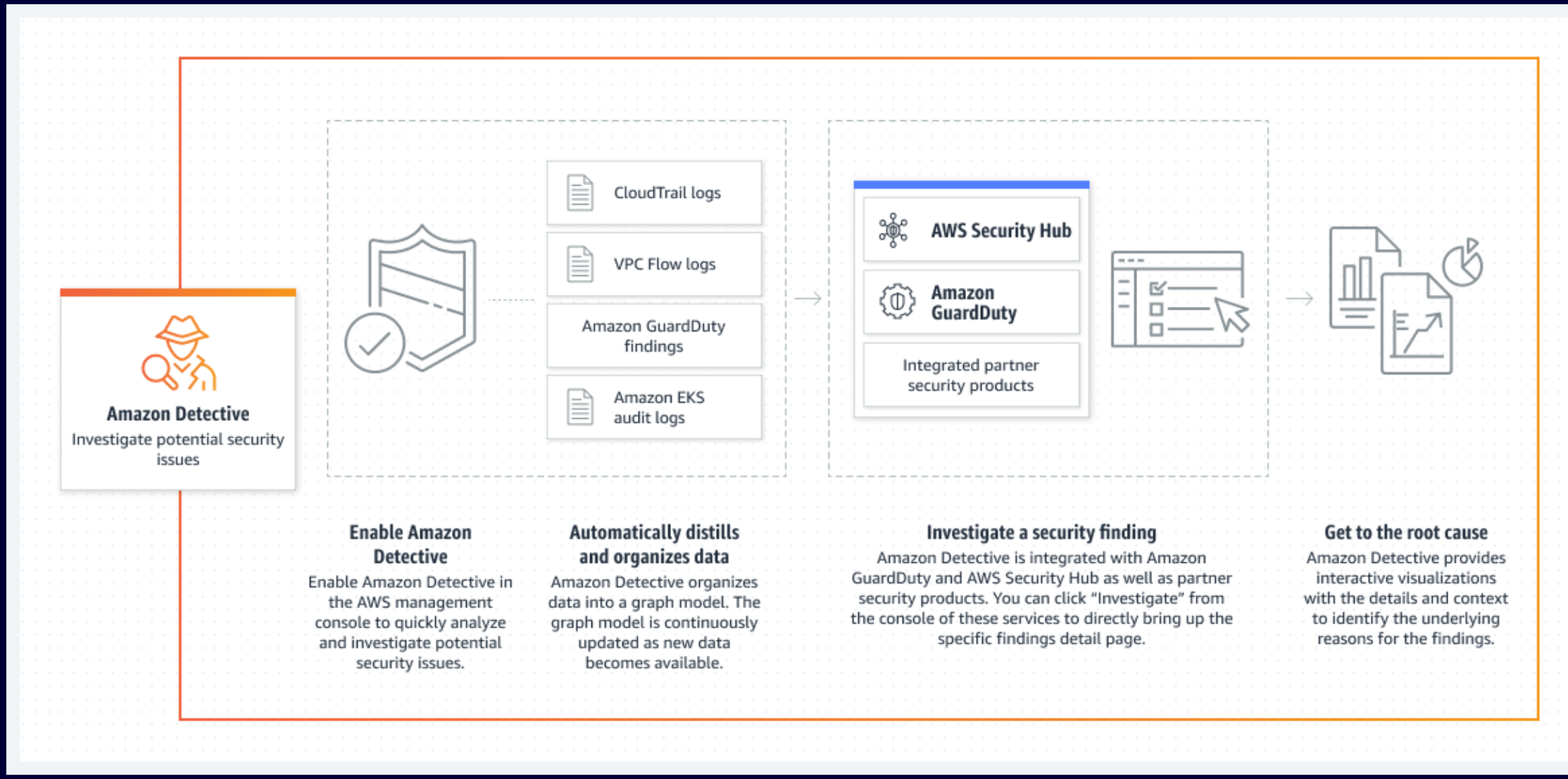
Built-in data collection



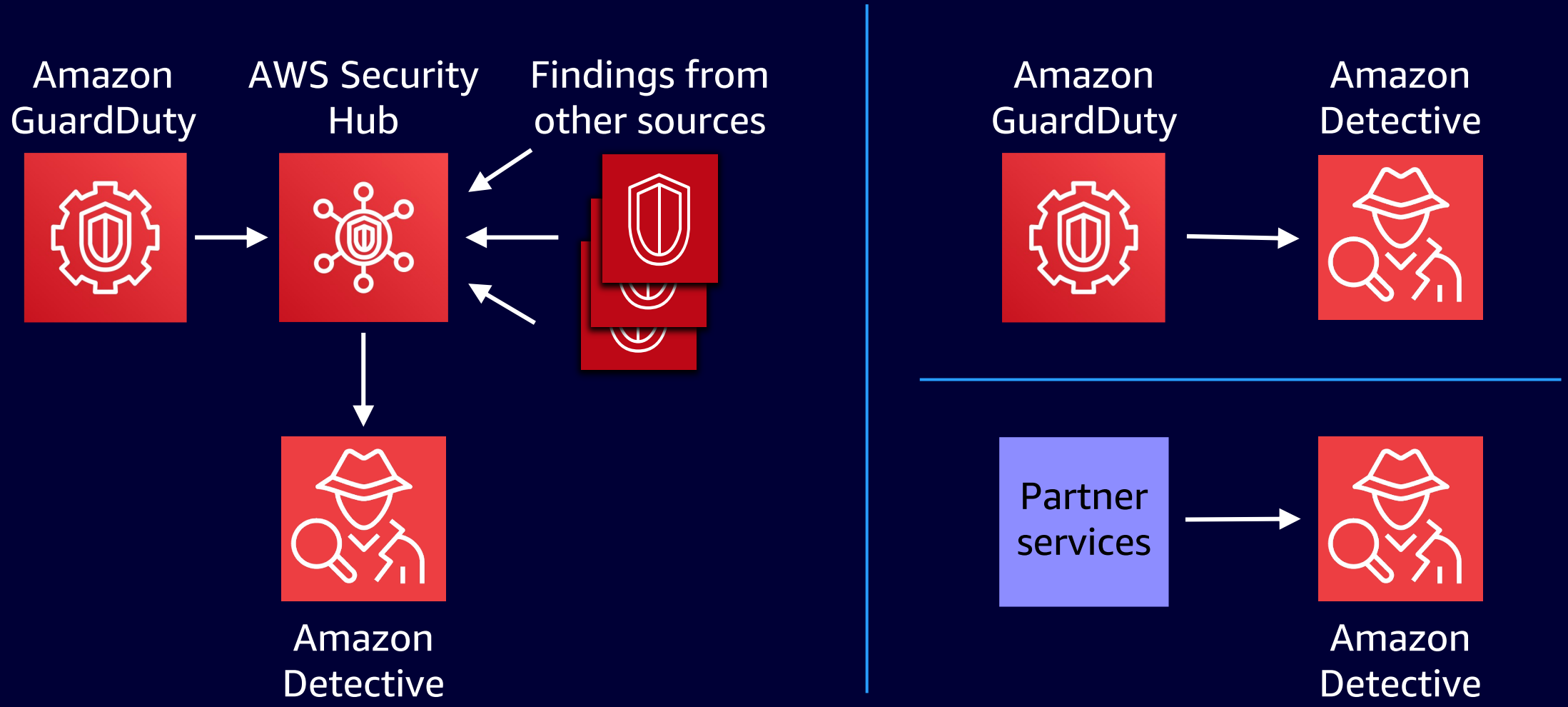
Automated analysis

Visual insights

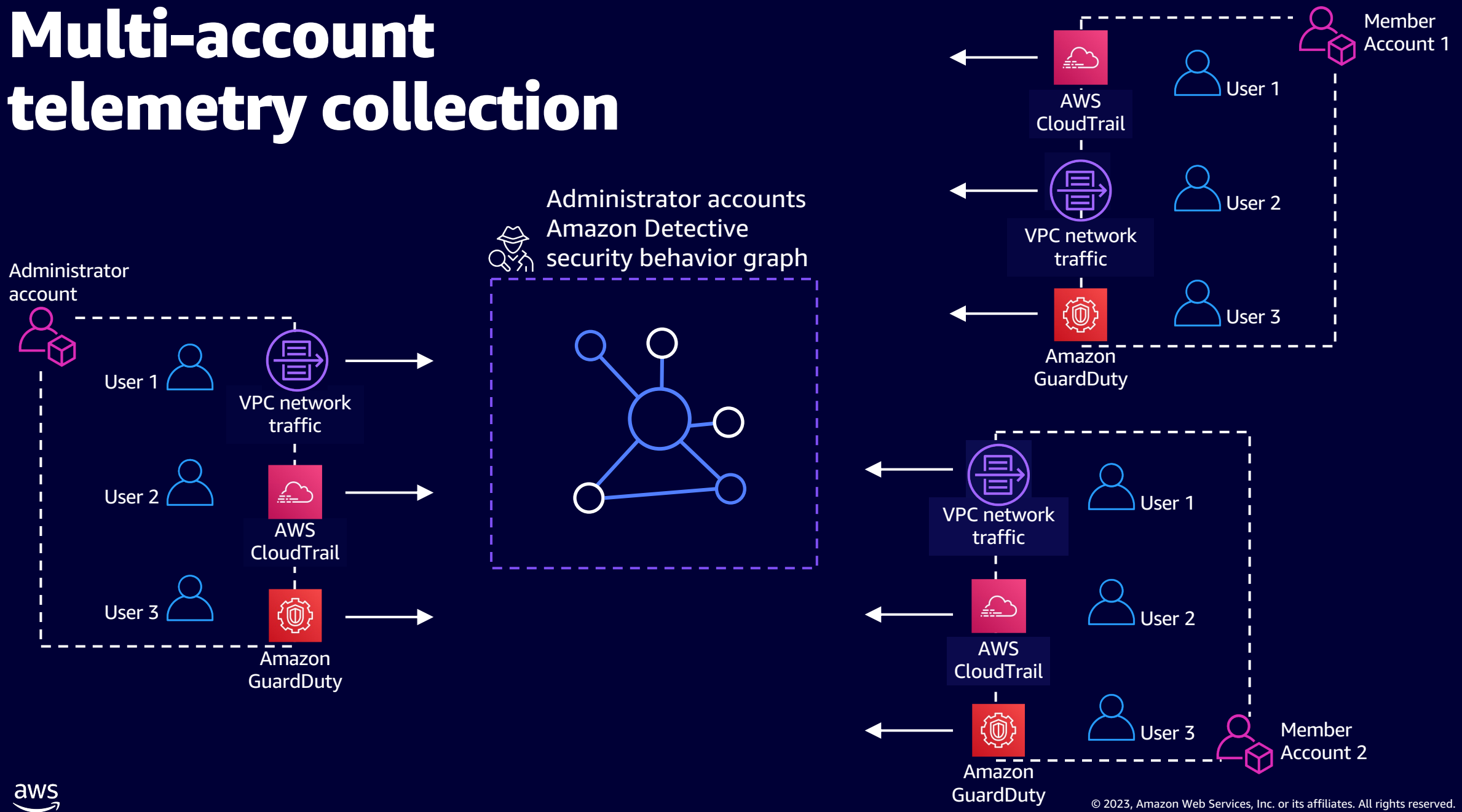
How Amazon Detective works



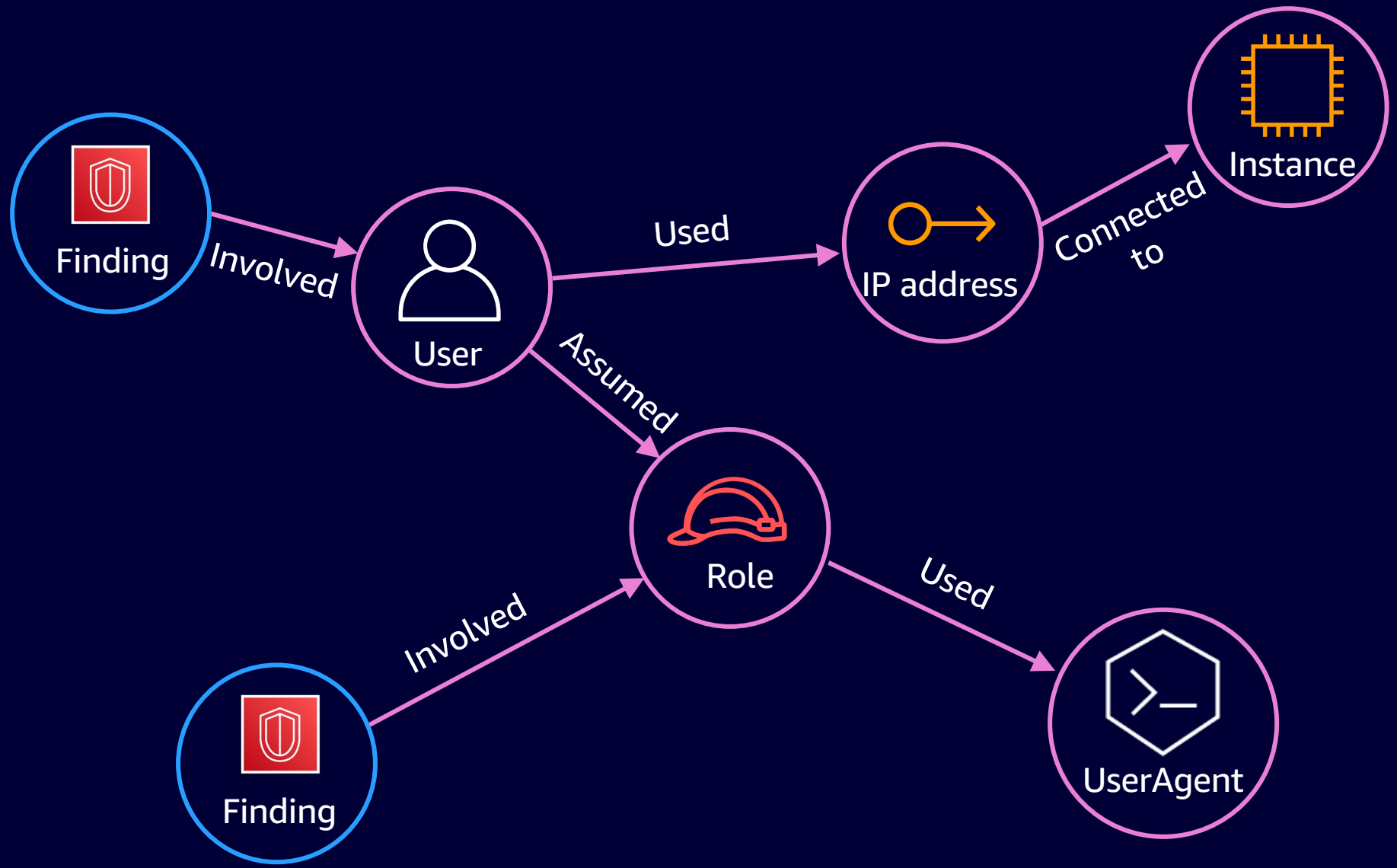
Amazon Detective usage flow



Multi-account telemetry collection



Security behavior graph



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

How do I monitor & respond to threats at scale?

AWS Security Hub

CONTINUOUS SECURITY ASSESSMENT & AUTOMATED RESPONSE LAYER

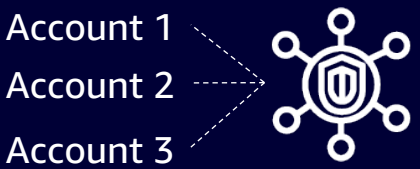
Centrally view & manage security alerts & automate security checks

Save time with aggregated findings

Improve security posture with automated checks

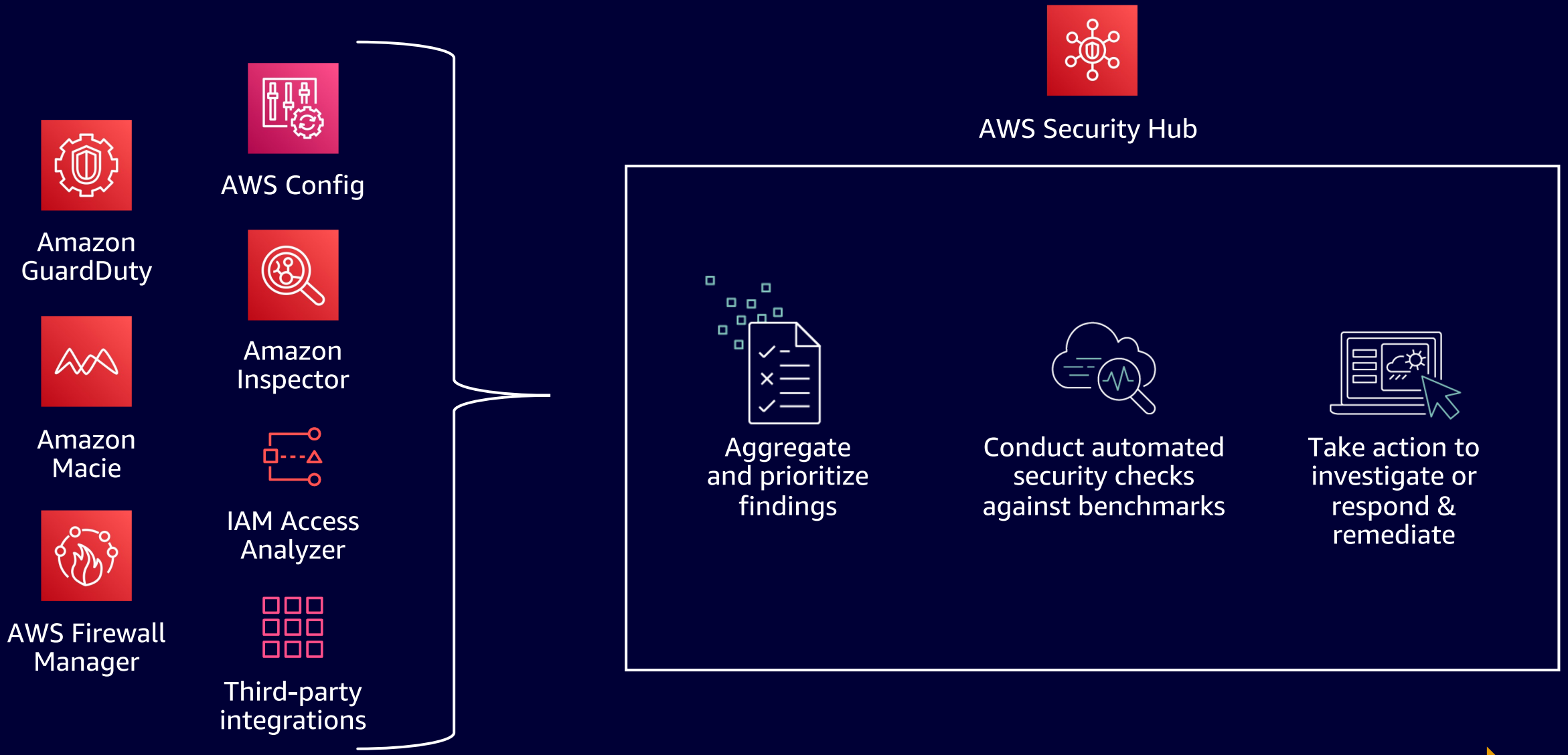
Curated security best practices

Seamless integration w/ standardized findings format



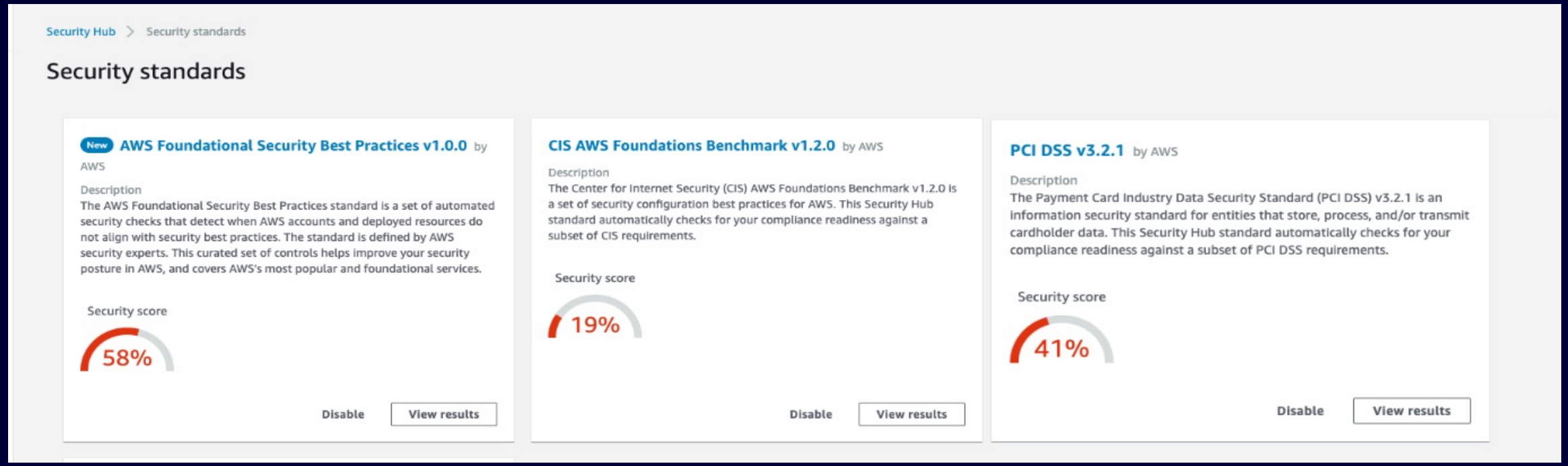
Multi-account support

How AWS Security Hub works



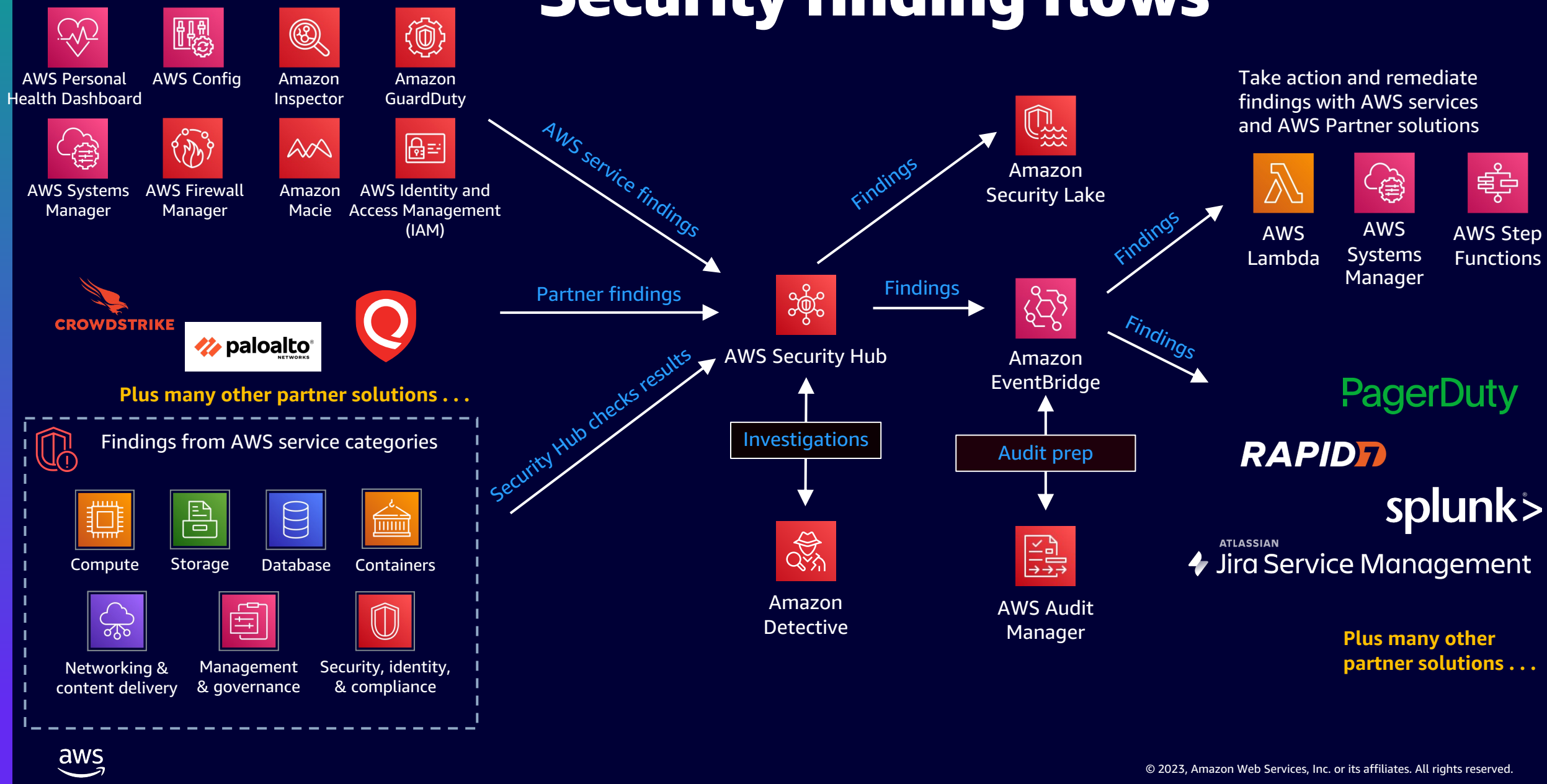
Better visibility into **security issues**. Easier to stay in **compliance**.

Automated security & compliance checks



- 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.

Security finding flows



Security Hub as a central dashboard

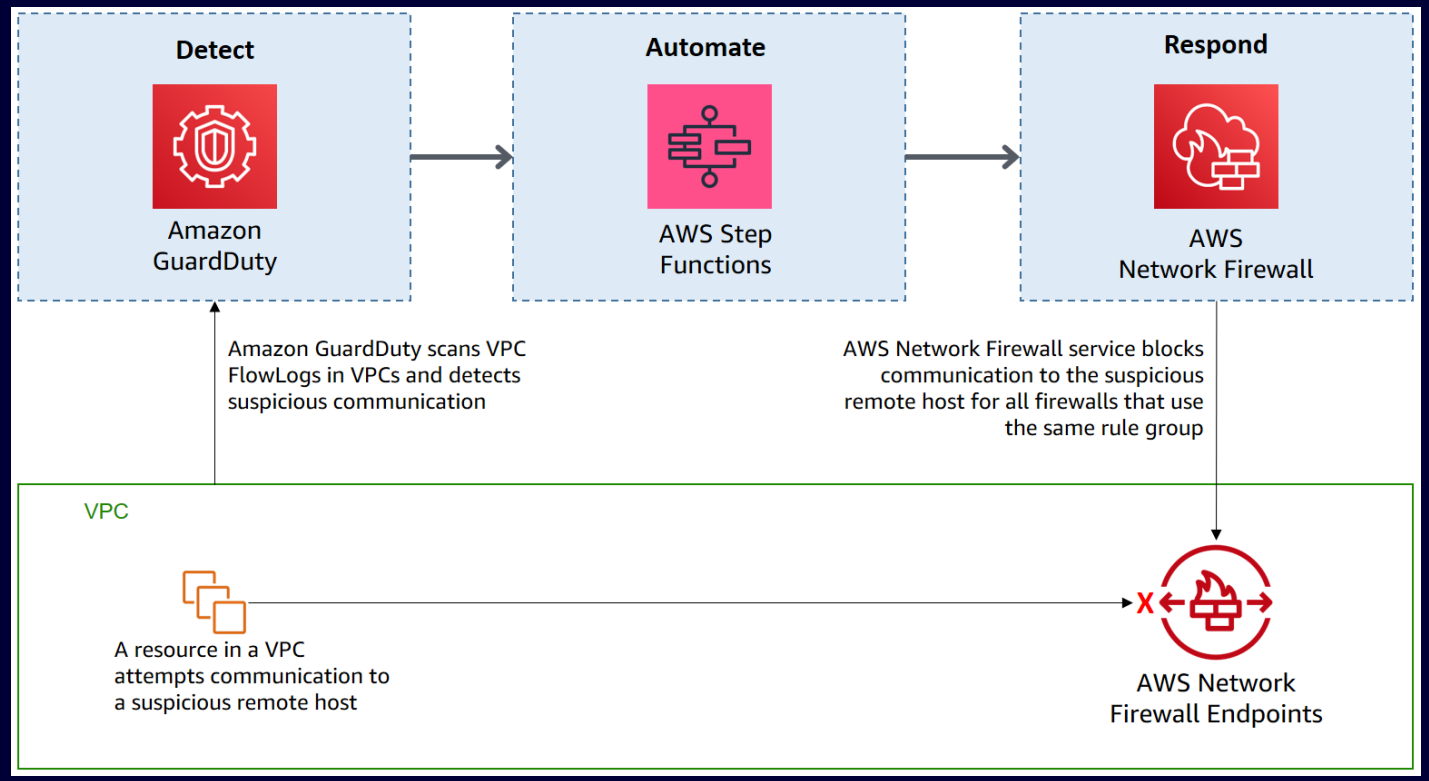
Centralize across accounts and prioritize findings without needing to normalize

View security and compliance posture against key standards

Take automated action on findings through CloudWatch Events

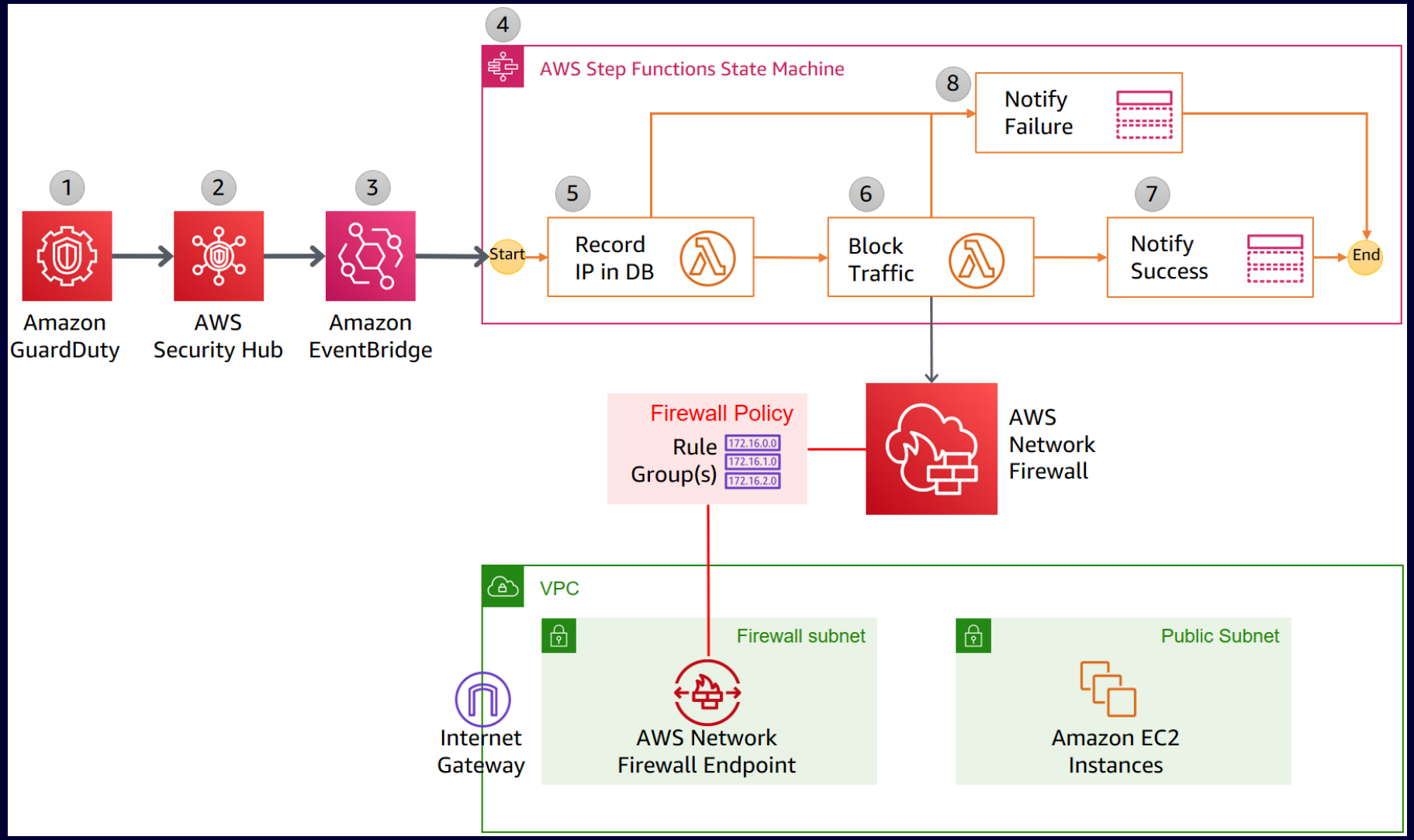
How do I automate response & remediation?

Automated detection & response

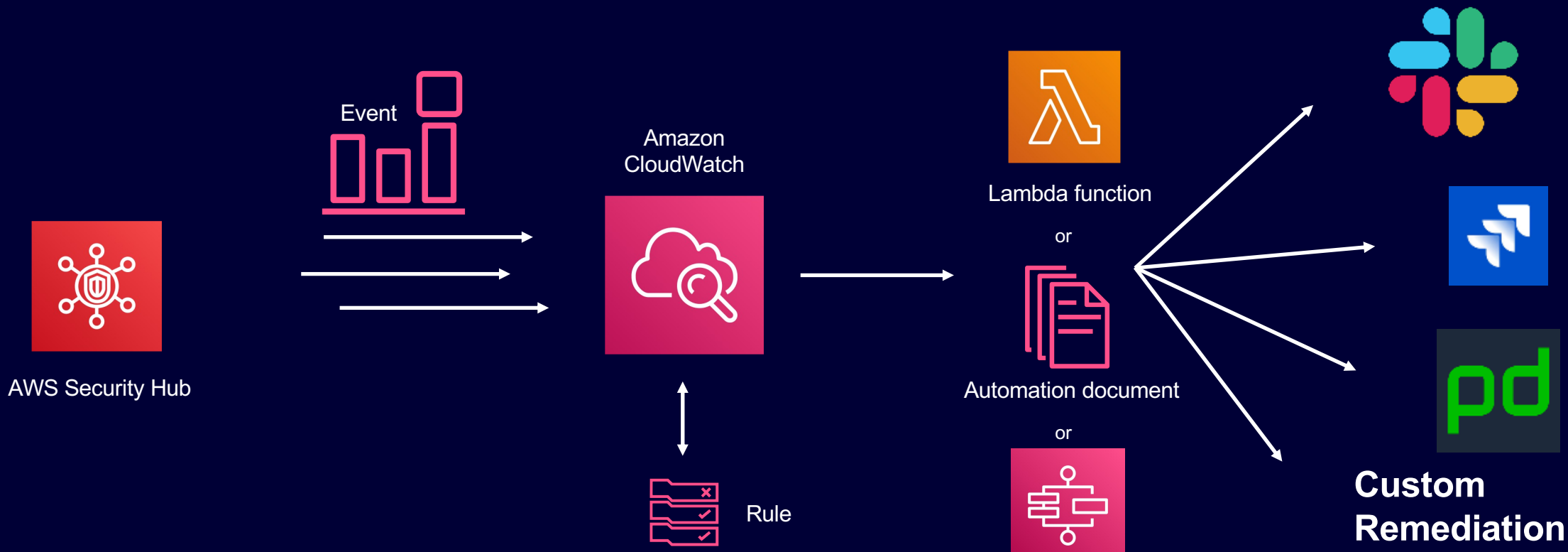


- Blocking traffic to and from suspicious remote hosts, for example to IP addresses associated with known command and control servers for botnets.
- GuardDuty detection of unintended communication with remote hosts triggers a series of steps, including blocking of network traffic to those hosts by using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

Customizable response and remediation actions



Customizable response and remediation actions



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

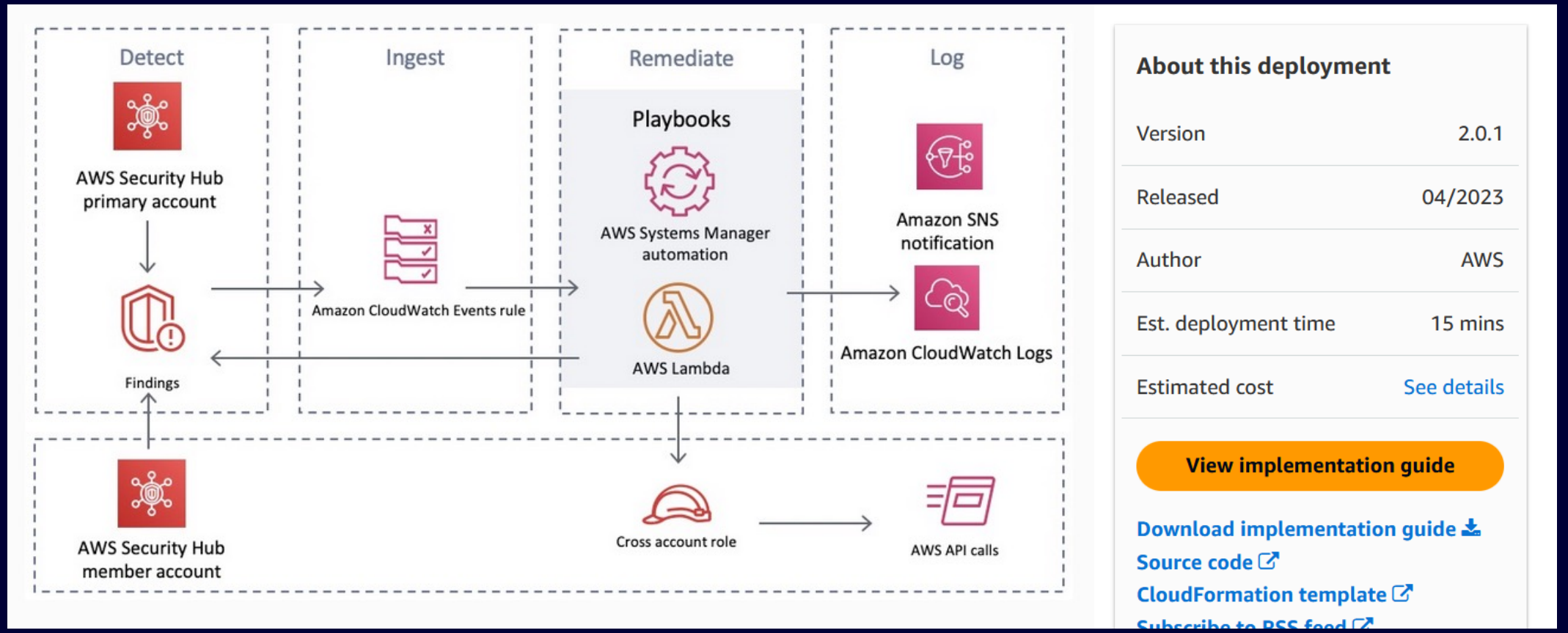
2. Security Hub user can select findings in the console and take a custom action on them. These findings are sent to CloudWatch decorated with a custom action ID

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

AWS Security Hub Automated Response and Remediation solution architecture



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

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!

Doug Pardue

Sr. Solutions Architect
wdpardue@amazon.com