

AWS re:Invent

NOV. 28 – DEC. 2, 2022 | LAS VEGAS, NV

SEC209-R

Continuous innovation in AWS Threat Detection and Monitoring services

Himanshu Verma

Sr. Manager Worldwide Security Specialist

Ryan Holland

Sr. Manager Amazon GuardDuty



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Topics we will cover

Overview of AWS Threat Detection & Monitoring Service portfolio

New features and key capabilities

Demo overview

Q&A

Continuously integrated security



Integrate AWS security services to achieve continuous threat detection, optimized route workflows, and minimal remediation time



Empower SecOps and DevOps teams to unify visibility and automate responses to help them achieve operational excellence in cloud security

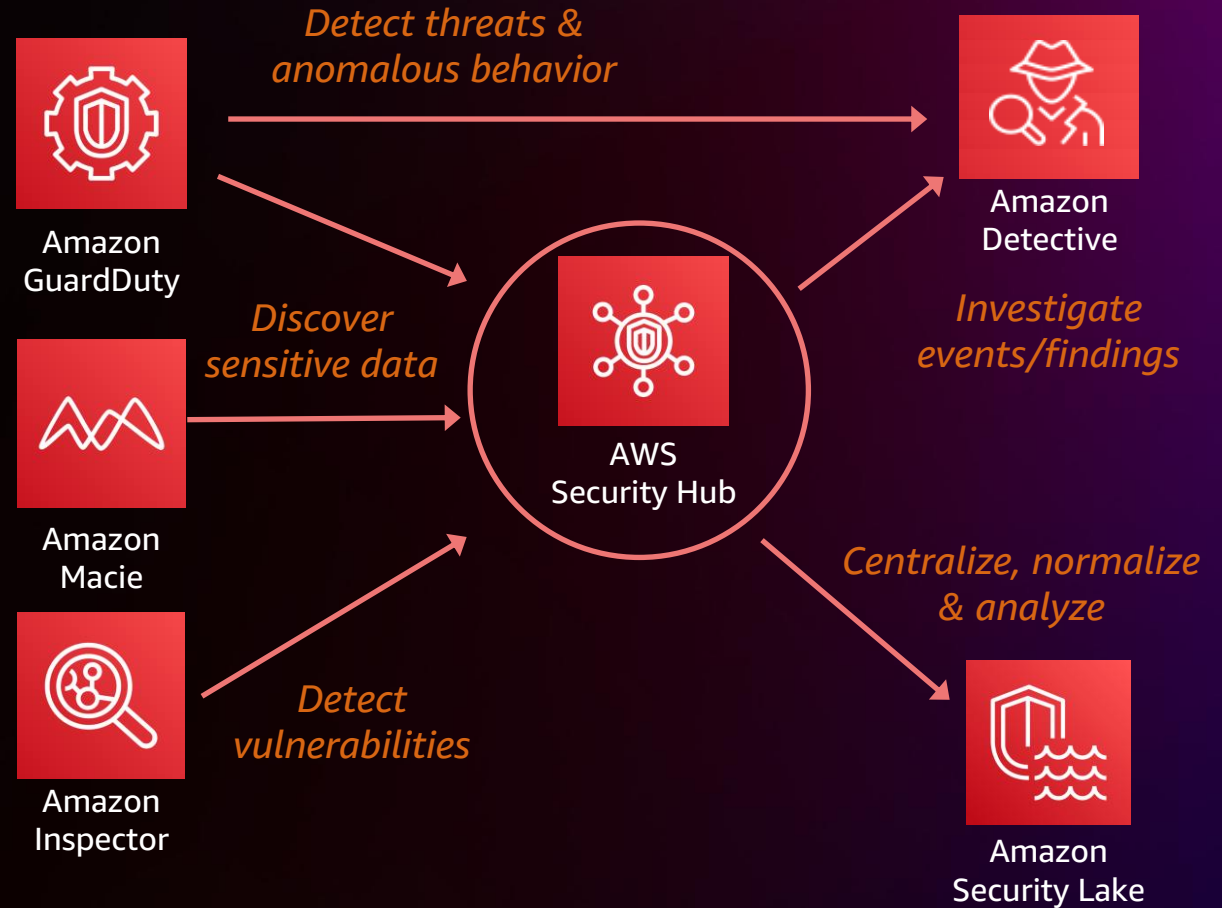
Threat detection, monitoring, and response



Security Monitoring and Threat Detection

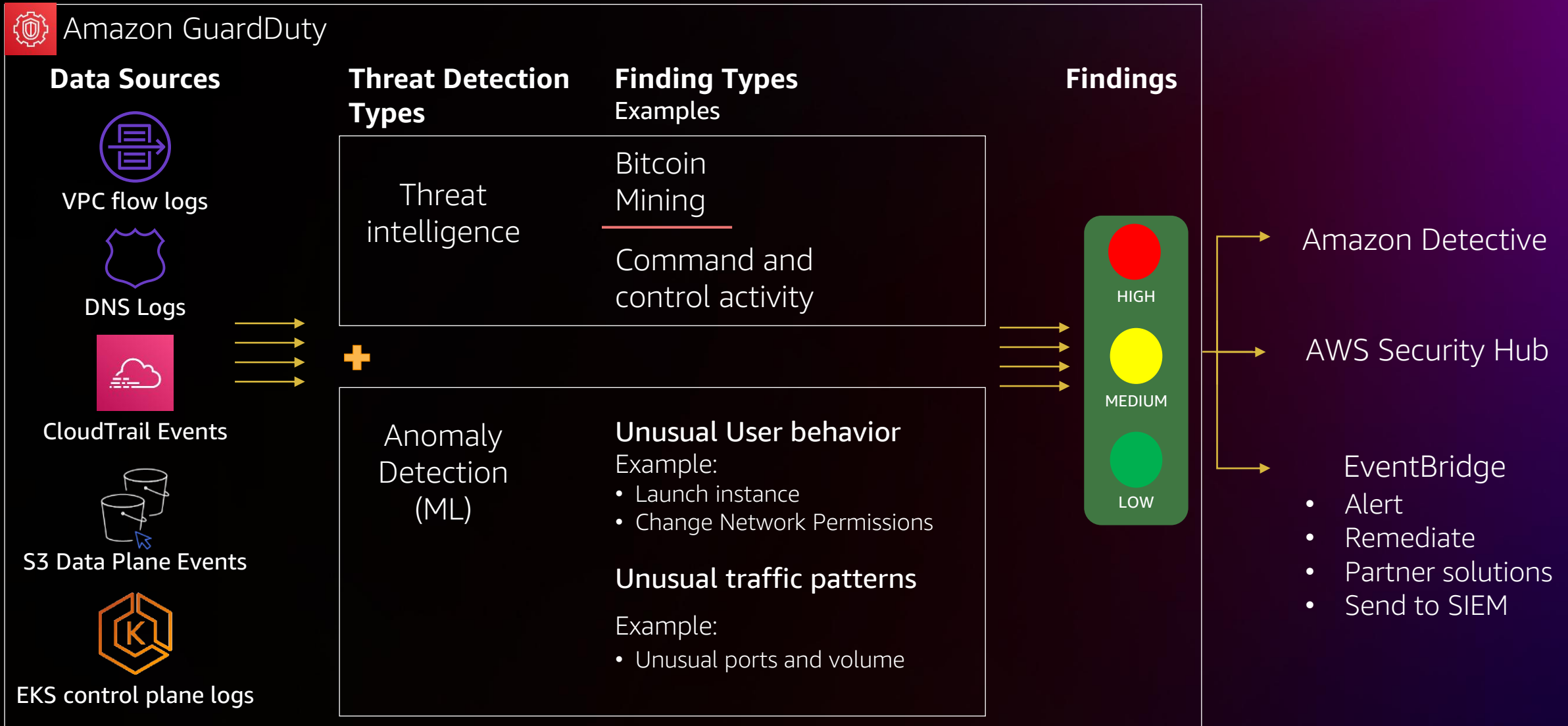


Integrated with AWS Workloads in an AWS Account, along with identities and network activity

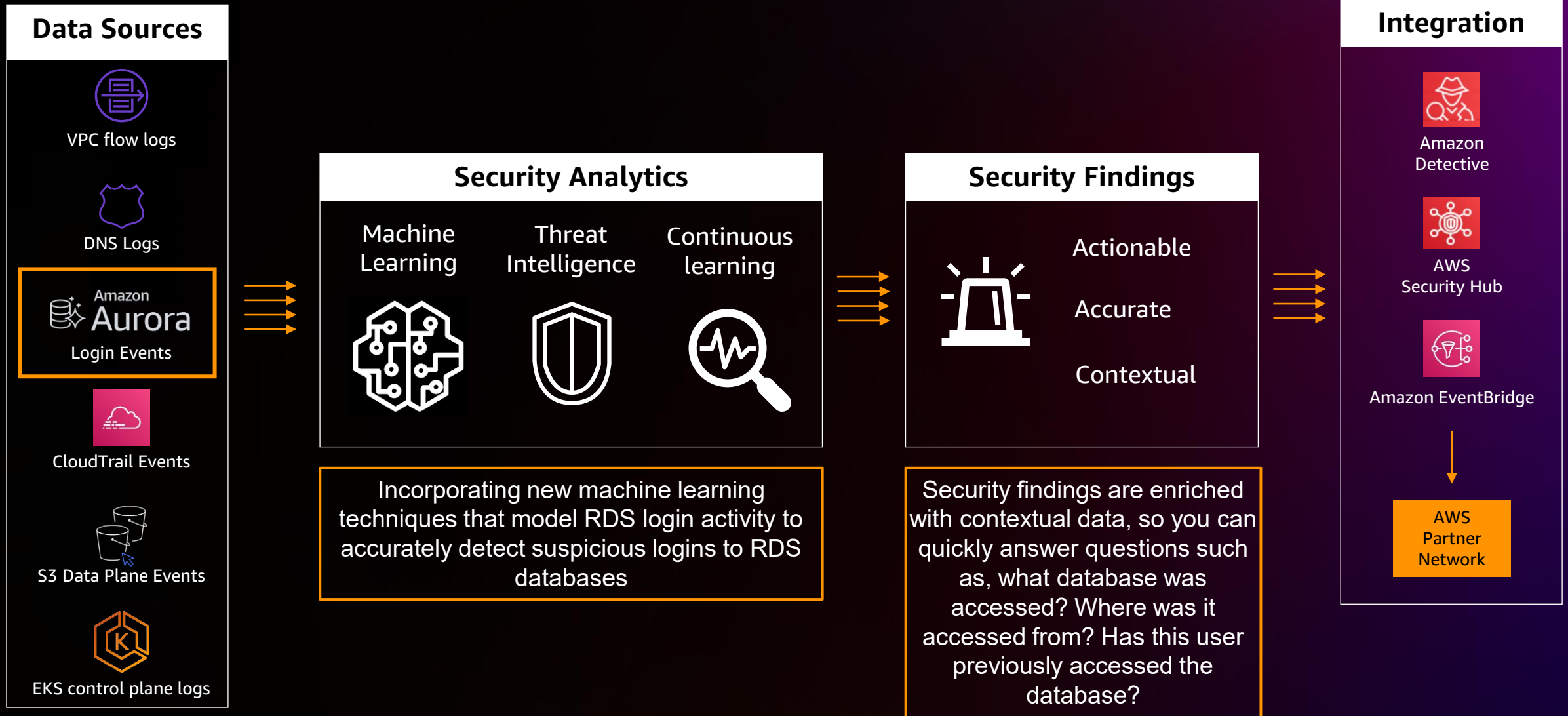


Detection of threats and suspicious events













How Amazon GuardDuty works



An Expansion of GuardDuty



Context to quickly investigate and respond

CredentialAccess:RDS/AnomalousBehavior.SuccessfulLogin 		
Finding ID: F7d67b5x97d4d4b9ac3162b0689be6e5		
 Unusual successful login by GeneratedFindingUserName observed on RDS instance GeneratedFindingDBInstanceid. Learn More		
Investigate with Detective		
Overview		
Severity	HIGH	
Region	us-east-1	
Count	1	
Account ID	507368004552	
Resource ID	GeneratedFindingDBInstanceid	
Created at	11-06-2022 14:24:26 (2 days ago)	
Updated at	11-06-2022 14:24:26 (2 days ago)	
Unusual behavior		
User name	GeneratedFindingUserName (Login count: 1 successful, 0 failed, 0 incomplete connections)	
ASN	GeneratedFindingAsnOrg (Login count: 10 successful, 0 failed, 0 incomplete connections)	
Application name	GeneratedFindingApplicationName (Login count: 1 successful, 0 failed, 0 incomplete connections)	
Database name	GeneratedFindingDatabaseName (Login count: 1 successful, 0 failed, 0 incomplete connections)	
Resource affected		
Resource role	TARGET	
Resource type	RDSDBInstance	
RDS DB instance details		
DB instance identifier	GeneratedFindingDBInstanceid	
Engine	GeneratedFindingEngine	
Engine version	13.6	
DB cluster identifier	GeneratedFindingDBClusterid	
DB instance ARN	arn:aws:rds:us-east-1:123456789000:db:GeneratedFindingDBInstanceid	
RDS DB user details		
User	GeneratedFindingUserName	
Application	GeneratedFindingApplicationName	
Database	GeneratedFindingDatabaseName	
SSL	GeneratedFindingSSLValue	
Auth method	GeneratedFindingAuthMethod	
Action		
Action type	RDS_LOGIN_ATTEMPT	
First seen	11-06-2022 14:24:26 (2 days ago)	
Last seen	11-06-2022 14:24:26 (2 days ago)	
Actor		
IP address	1.2.3.4	
Location		
City	GeneratedFindingCityName	
Country	GeneratedFindingCountryName	
Organization		
Asn	0	
Asn org	GeneratedFindingAsnOrg	
Isp	GeneratedFindingIsp	
Org	GeneratedFindingOrg	
Additional information		
Sample	true	

Finding name indicates whether the anomalous behavior was a successful or failed login

Unusual behavior section allows you to quickly see what suspicious behavior triggered the alert, including user, database, and application names, and the ASN the database was accessed from

Resource section provides details on the database, and the user that accessed it

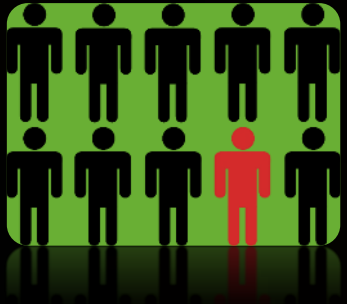
Actor section provides details on the IP address that the database was accessed from, including country, and ASN

GuardDuty S3 Protection

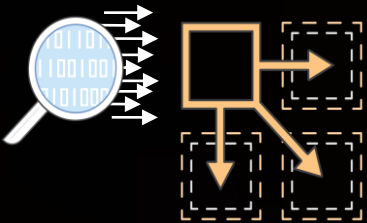


NEW MACHINE LEARNING CAPABILITIES AND THREAT DETECTIONS

The new machine learning approach can more accurately identify malicious activity associated with **known attack tactics**, including **data discovery**, **tampering**, and **exfiltration**.



This new capability continuously models S3 data plane API invocations (e.g. GET, PUT, and DELETE) within an account, **incorporating probabilistic predictions** to more accurately alert on **highly suspicious** user access to data stored in S3 buckets, such as requests coming from an **unusual geo-location**, or **unusually high volumes of API calls** consistent with attempts to exfiltrate data.



GuardDuty's S3 protection includes **19 managed threat detections** tailored to help protect your data stored in S3. These threat detections are available to customers that have enabled S3 protection in GuardDuty.

GuardDuty for EKS Finding Types

Policy

- Exposed dashboard
- Admin access to default service account
- Anonymous access granted

Malicious access

- Data discovery, exfiltration, or modification from:
 - Tor
 - Successful anonymous access
 - Malicious IPs

Suspicious behavior

- Execution in Kubernetes system pod
- Container with sensitive mount
- Privilege container

- GuardDuty immediately begins to analyze Kubernetes data sources from your Amazon EKS clusters and monitors them for malicious and suspicious activity.

GuardDuty aligns findings using the MITRE ATT&CK framework

Credential Access

Defense Evasion

Discovery

Impact

Privilege Escalation

Policy

Execution

Persistence



Amazon GuardDuty Malware Protection

GuardDuty Malware Protection – a fully managed malware detection service supports detection of malicious software by scanning Amazon Elastic Block Storage (EBS) and container workloads running on Amazon EC2.

- ➔ **Detects malware** (trojans, worms, rootkits, crypto miners, bots, etc.) and generates a new finding in GuardDuty
- ➔ Scans **Elastic Block Storage (EBS)** for malware on Amazon EC2 instance and container workloads that are exhibiting suspicious behavior

- *Automatic* - malware scanning triggered on GuardDuty findings
- *Agentless* - no security software required to install or maintain

NEW

Amazon GuardDuty EKS runtime monitoring

Lightweight, fully managed security agent that monitors on-host operating system-level behavior

Provide visibility into the activity of the containers themselves and the EC2 host they run on

Detect early signs of an attack like suspicious script executions or communications with a C&C server

Integrated to Amazon Detective to make it easier to investigate and find root cause



Container runtime threat detection

DETECT THREATS TO CONTAINERS BY MONITORING OPERATING SYSTEM-LEVEL BEHAVIOR

Improved Safety

Detects suspicious script executions, which is an early sign of an attack

Identifies specific containers trying to communicate with a command & control server

High Performance

Lightweight, fully managed security agent

Integrates with EKS for automated resource discovery and agent deployment

More Visibility

Detects malicious activity earlier in attack cycle

Monitors on-host OS-level behavior, such as file access, process execution, and network connections



EKS Runtime Monitoring

Threat Intel Findings

- Applies threat intelligence to IP and DNS requests.

Privilege Escalation

- RunC Container Escapes
- CGroup agent modification
- Host directory mounts
- Userfaultfd usage
- Containers accessing docker socket

Suspicious behavior

- Execution of new binaries or scripts in running containers.
- LD_Preload function hijacks
- Memory marked as executable
- New kernel modules

- EKS integration allows for 1-Click deployment and AWS Organizations integration
- Findings include Pod details as well as detailed process metadata
- Existing GuardDuty backend VPC Flow Log and DNS monitoring in event of agent failures

GuardDuty aligns findings using the MITRE ATT&CK framework

Credential Access

Defense Evasion

Discovery

Impact

Privilege Escalation

Policy

Execution

Persistence



Investigate events



Amazon Detective Use Case Benefits

INVESTIGATE ISSUES FASTER AND WITH LESS EFFORT



1) Finding / Alert triage

Accelerate triage and avoid unnecessary escalations



2) Incident Investigation

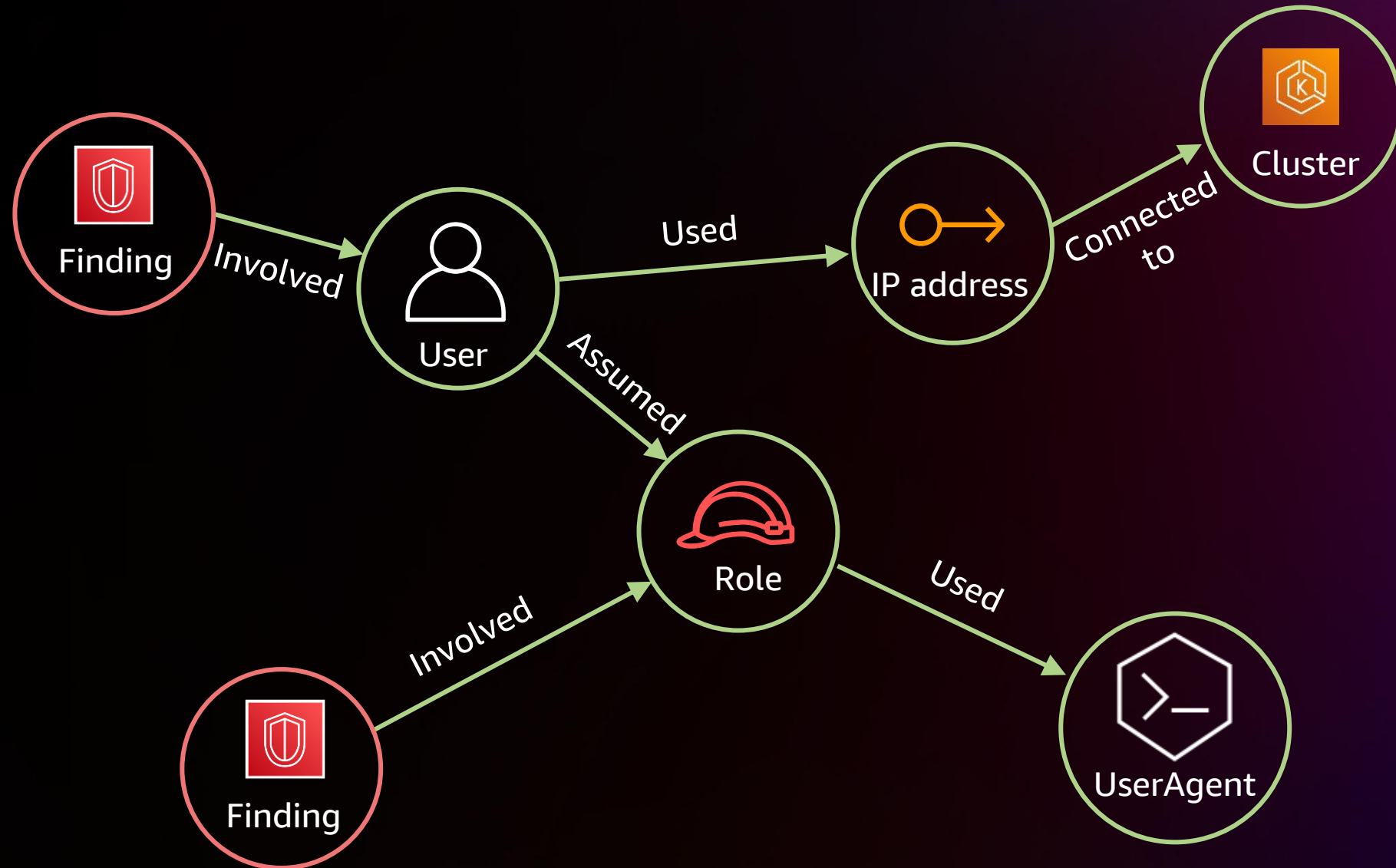
Improve context and surface correlated behavior



3) Threat Hunting

Simplify data collection, aggregation and pivoting

Amazon Detective – Security behavior graph



Amazon Detective support for EKS

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.

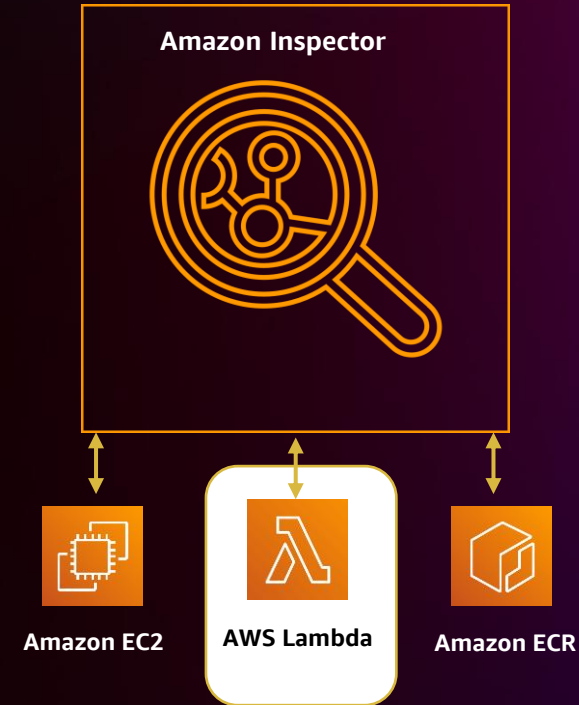
- ➡ Review **Amazon EKS** specific activity, such as **pod volume patterns** and **container service user activity**, including divergent behavior within and across EKS clusters
- ➡ **Investigate** security findings with their **EKS clusters**, such as cryptocurrency mining, unintentional **admin privilege exposure**, container **misconfigurations** that allow access to underlying EC2 nodes, or behavioral patterns common to **compromised** container clusters.

Manage vulnerabilities



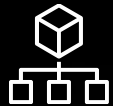
What is Amazon Inspector?

Amazon Inspector is an automated vulnerability management service that **continually** scans workloads for software vulnerabilities and unintended network exposure



Added support for Lambda functions

With this expanded capability, Amazon Inspector now 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



**Amazon
Inspector**



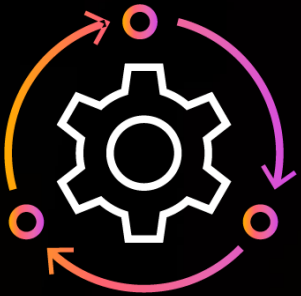
A single pane of glass for vulnerabilities across all resources

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



Continuous monitoring with automated response & remediation

Security Hub – response & remediation



Enable **automated remediation** for high-severity configuration findings



Use **custom actions** to invoke runbooks for automated response



Use **partner integrations** to consolidate and normalize security findings



Integrate with **ticketing and workflow** tools

Centralized management of your security data



Amazon Security Lake

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



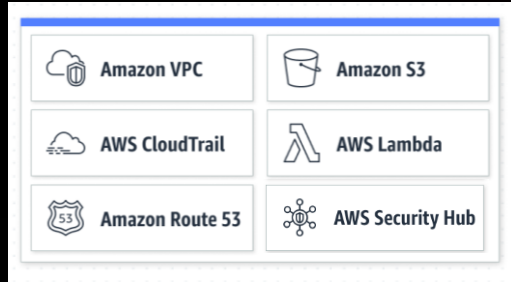
Centralize data automatically from cloud, on-premises, and custom security sources across AWS Regions

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

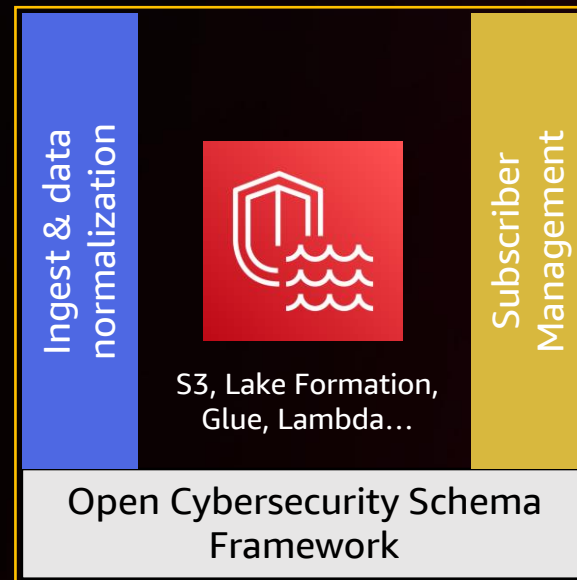


AWS logs sources +
finding from over 50
security solutions



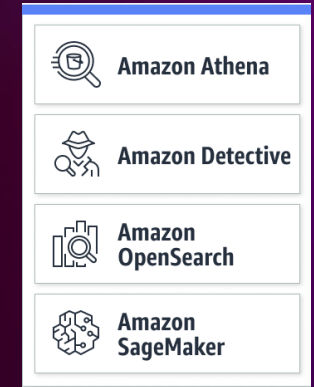
Enterprise security
solutions

Amazon Security Lake

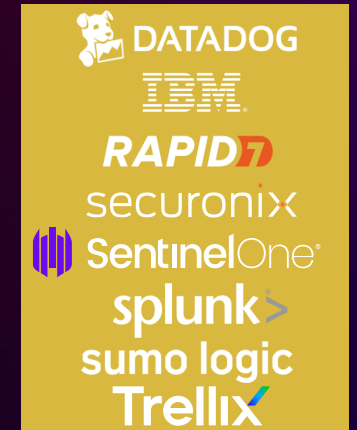


Customer owned,
managed data lake

Customers can use
any analytics



AWS security and
analytics



Analytics & XDR
Platforms

Amazon Security Lake Partners



Getting Started – AWS Organizations

- Security Lake works with AWS Organizations
- Define the delegated admin account in your organization

Security, Identity and Compliance

Amazon Security Lake

Automatically centralize all your security data with a few clicks

Get Started with Amazon Security Lake

Easily enable features for all Regions and all accounts
Automatically collect log data from your AWS resources

Get started



AWS Organizations

Delegate administration to another account

lorem ipsum

Delegate

☒ VulnMngmntTeam (Account 022245678912)
Delegated administrator: Inspector

☐ SecOpsCent (Account 012345678912)
Delegated administrator: GuardDuty

☐ I want to enter a different account

Getting Started – Collect everything

Everything on by default

Multi-Region enablement

All accounts of your organization

Select log and event sources

All selected data is ingested into your data lake.

☒ All log and event sources
Turn on everything: CloudTrail, VPC, WAF, and DNS.

☐ Specific log and event sources
Select which sources you would like to turn on.

Select Regions [Info](#)

Selected Regions will contribute their data to your data lake.

☒ All Regions - *recommended*
Enable all Regions and any new Regions

☐ Specific Regions
Specify which Regions to enable

☐ This Region (us-east-1)
Enable this Region only

► Encryption settings

Select accounts

All selected accounts will contribute their data to your data lake.

☒ All accounts
Enable all accounts in my organization.
☒ Enable all new accounts

☐ Specific accounts
Decide which accounts to include
☒ Enable all new accounts that adhere.

☐ This account
Only enable this account for now.

Getting Started – Centralization and Retention

One or multiple
central Regions

Define storage
class transitions

Amazon Security Lake > Enable Amazon Security Lake

Step 1
[Define collection objective](#)

Step 2
Define target objective

Step 3
[Review and create](#)

Define target objective [Info](#)

Define target objective

Select Rollup Region-optional

All data from contributing Regions reside in the rollup Region. You can create multiple rollup Regions, which is useful for aligning to GDPR requirements and data tenancy.

Select Rollup Region	Select contributing Regions	Replication role ARN	
US East (N. Virginia) ▼	Choose contributin... ▼		Remove
	US West (Oregon) ✕		

[Add rollup region](#)

You can add 0 more tags.

Set storage classes - optional

Amazon Security Lake uses standard S3 storage classes. You can define when you want the data to transition between storage classes, and if you want the data to expire.

Choose storage class	Retention period	
Standard-IA ▼	30	Remove

[Add transition](#)

Cancel Previous **Next**

Done!

You can immediately query your data

Data

Data source

AwsDataCatalog

Database

amazon_security_lake_glue_db_us_east_1

Tables and views

Filter tables and views

▼ Tables (5)

amazon_security_lake_table_us_east_1_cloud_trail

amazon_security_lake_table_us_east_1_myendpointprocessdata

amazon_security_lake_table_us_east_1_route53

amazon_security_lake_table_us_east_1_sh_findings

amazon_security_lake_table_us_east_1_vpc_flow

Amazon Athena > Query editor

Editor

Recent queries

Saved queries

Settings

Workgroup

primary

>

Query 20

Query 21

```
1 SELECT start_time,
2     end_time,
3     src_endpoint.interface_uid,
4     connection_info.direction,
5     src_endpoint.ip,
6     dst_endpoint.ip,
7     src_endpoint.port,
8     dst_endpoint.port,
9     traffic.packets,
10    traffic.bytes
11 FROM "amazon_security_lake_glue_db_us_east_1".
12      "amazon_security_lake_table_us_east_1_vpc_flow"
13 WHERE ( src_endpoint.ip = '172.31.73.28' AND dst_endpoint.ip = '172.31.71.151' )
14        OR ( src_endpoint.ip = '172.31.71.151' AND dst_endpoint.ip = '172.31.73.28' )
15 ORDER BY start_time ASC
16 LIMIT 100
```

Results (100+)

Copy

Download results

Search rows

#	start_time	end_time	interface_uid	direction	ip	ip	port	port
1	1669577323000	1669577325000	eni-0bd9d6778b3871f25	egress	172.31.71.151	172.31.73.28	40672	2049
2	1669577323000	1669577325000		Ingress	172.31.73.28	172.31.71.151	2049	40672
3	1669577358000	1669577360000		Ingress	172.31.71.151	172.31.73.28	40672	2049



Summary: Simple and Scalable Security Monitoring

Scale existing services

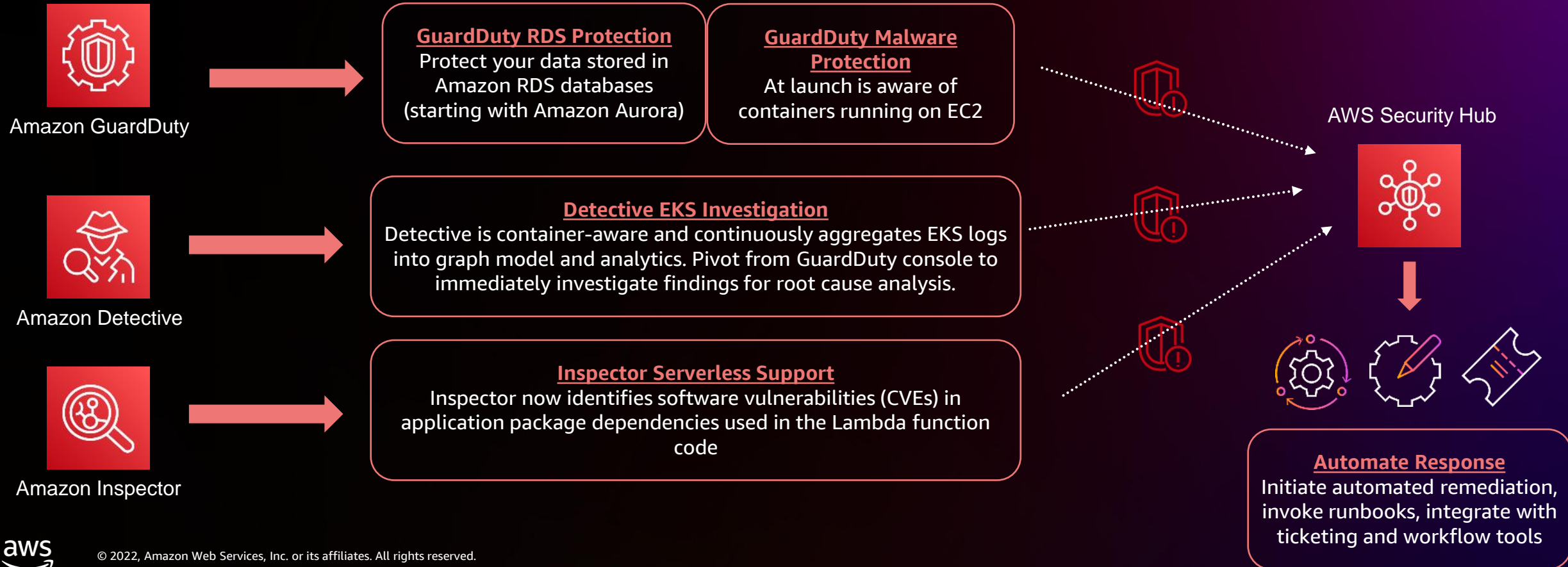
Customers use same console, findings, and experience

Simple and easy deployment

One-click enables container support
AWS Orgs assures environment-wide enablement
(new customers have support on by default)

Continuous monitoring

Centralization of security findings
scales and automates operations



Thank you!



Please complete the session survey in the **mobile app**

