AWS Detective

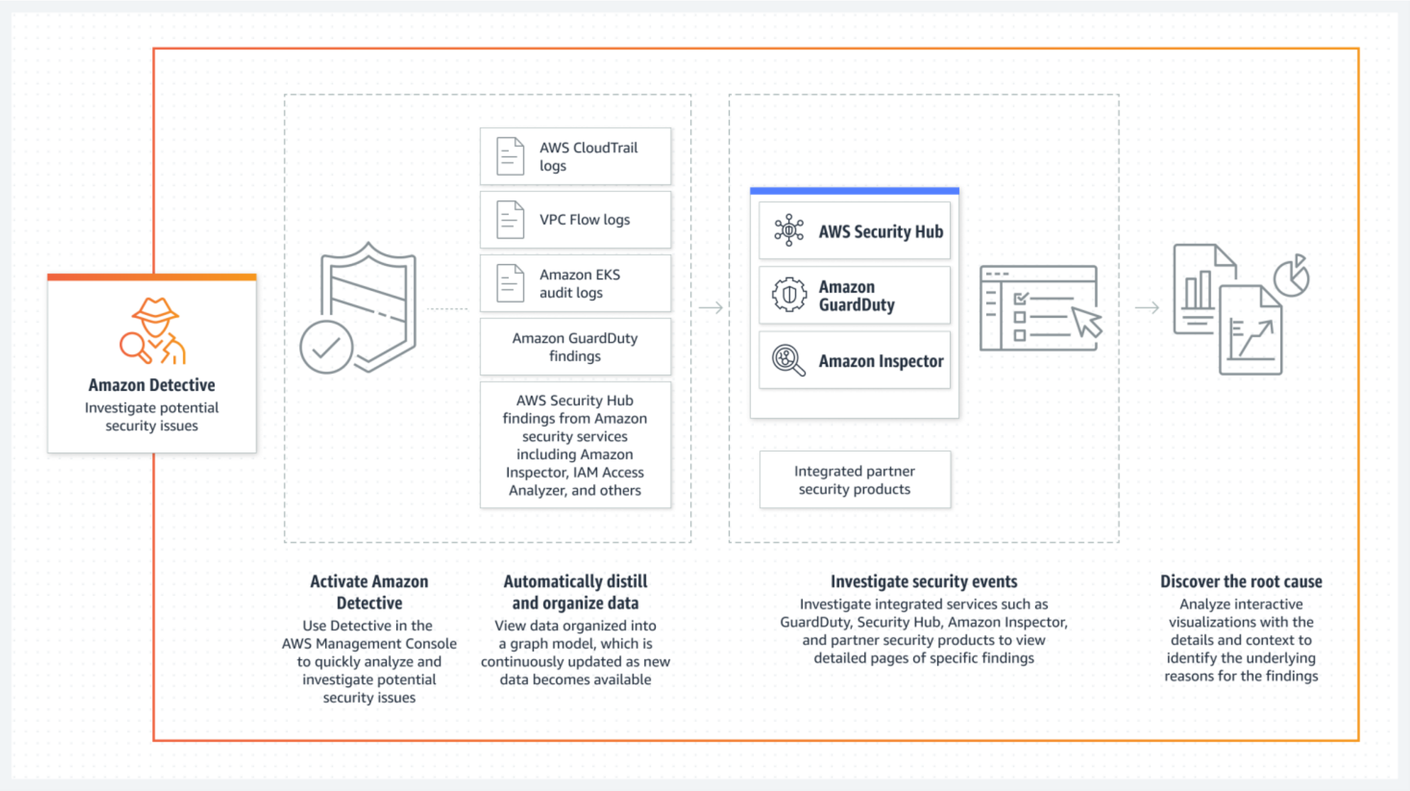
PRESENTATION BY:
S.SURESH
CLOUDSIKSHA

AWS Detective

Amazon Detective makes it easy to analyze, investigate, and quickly identify the cause of a potential security threat or suspicious activity

Amazon Detective automatically collects historical data from your AWS resources and uses machine learning, statistical analysis, and chart theory to create a linked dataset that enables you to conduct faster and more efficient security audits

AWS Detective


Amazon Detective
Investigate potential security issues
AWS CloudTrail logs
VPC Flow logs
Amazon EKS audit logs
Amazon GuardDuty findings
AWS Security Hub findings from Amazon security services including Amazon Inspector, IAM Access Analyzer, and others
AWS Security Hub
Amazon GuardDuty
Amazon Inspector
Integrated partner security products

Activate Amazon Detective
Use Detective in the AWS Management Console to quickly analyze and investigate potential security issues

Automatically distill and organize data
View data organized into a graph model, which is continuously updated as new data becomes available

Investigate security events
Investigate integrated services such as GuardDuty, Security Hub, Amazon Inspector, and partner security products to view detailed pages of specific findings

Discover the root cause
Analyze interactive visualizations with the details and context to identify the underlying reasons for the findings

Benefits of AWS Detective

Using Amazon Detective's ready-made data aggregations, summaries, and contexts, you can quickly analyze and determine the nature and scope of potential security problems

Amazon Detective holds aggregated data for up to a year and makes it available through a series of visualizations that show changes in the type and extent of activity in a selected time window and links these changes to safety findings

Data Sources

With Amazon Detective, customers can view summaries and analytics data on AWS CloudTrail events and VPC flow logs. For customers who have Amazon GuardDuty enabled, Detective also processes the findings from Amazon GuardDuty. It is integrated with AWS Inspector as well as Security Hub

Difference between Detective & GuardDuty

Amazon GuardDuty is a threat detection service that continuously monitors and protects your AWS accounts and workloads for malicious and unauthorized behavior

Amazon Detective simplifies the process of investigating security outcomes and determining the root cause. Amazon Detective analyzes trillions of events from multiple data sources, such as: B. Findings from PC Flow-Logs, AWS CloudTrail Logs and Amazon GuardDuty, and automatically creates a diagram model that gives you a unified, interactive view of your resources

Investigative Phase

Triage

- In the triage phase, you determine whether you believe the activity is a true positive (genuine malicious activity) or false positive (not malicious or hi-risk activity).

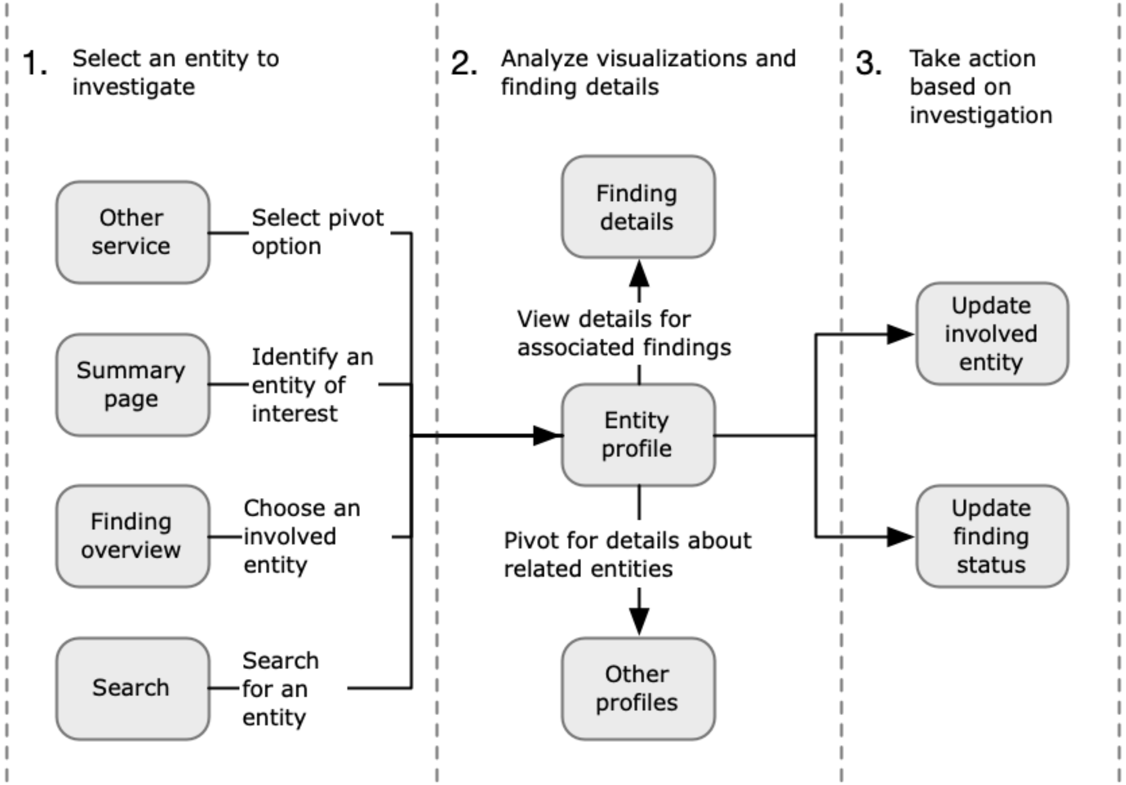
Scoping

- During the scoping phase, analysts determine the extent of the malicious or high-risk activity and the underlying cause

Response

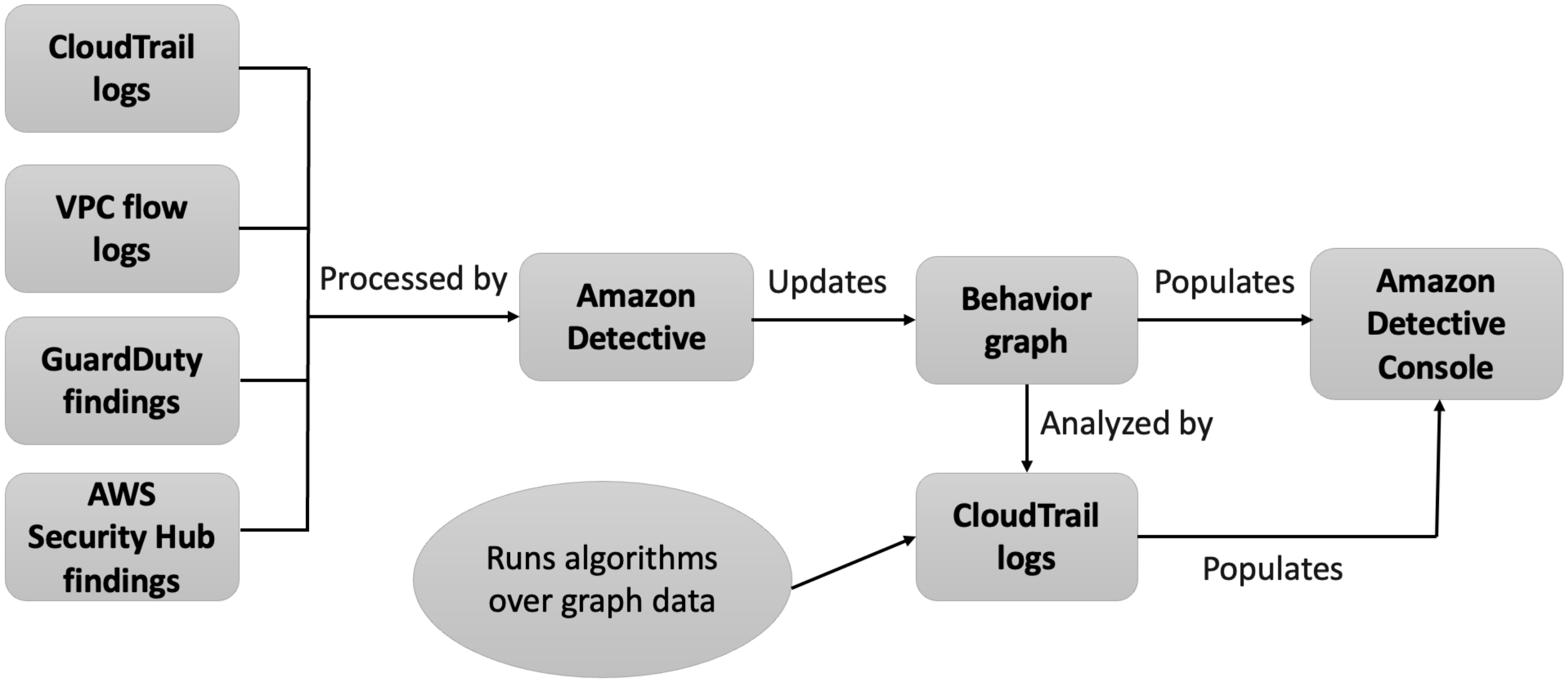
- The final step is to respond to the attack in order to stop the attack, minimize the damage, and prevent a similar attack from happening again

Investigation Flow



1. Select an entity to investigate
2. Analyze visualizations and finding details
3. Take action based on investigation
Other service
Select pivot option
Summary page
Identify an entity of interest
Finding overview
Choose an involved entity
Search
Search for an entity
Finding details
View details for associated findings
Entity profile
Pivot for details about related entities
Other profiles
Update involved entity
Update finding status

Processing Source Data



CloudTrail logs

VPC flow logs

GuardDuty findings

AWS Security Hub findings

Processed by

Amazon Detective

Updates

Behavior graph

Populates

Amazon Detective Console

Analyzed by

Runs algorithms over graph data

CloudTrail logs

Populates

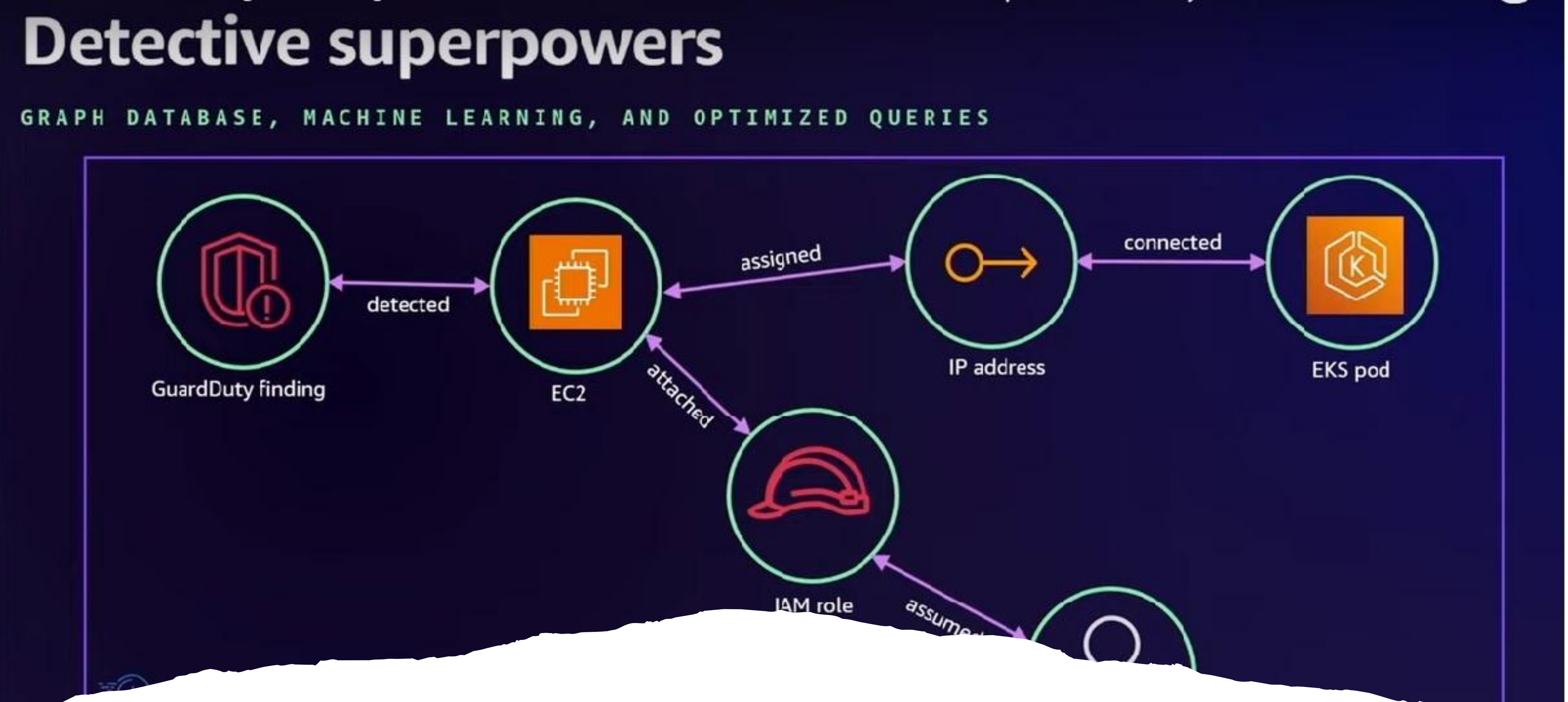
Finding Groups

Amazon Detective finding groups enable you to examine multiple activities as they relate to a single security compromise event

You can analyze the root cause for high severity GuardDuty findings using finding groups

When security findings are investigated in isolation, it can lead to a misinterpretation of their significance and difficulty in finding the root cause

Amazon Detective addresses this problem by applying a graph analysis technique that infers relationships between findings and entities, and groups them together



Detective superpowers

GRAPH DATABASE, MACHINE LEARNING, AND OPTIMIZED QUERIES

GuardDuty finding

detected

EC2

assigned

IP address

connected

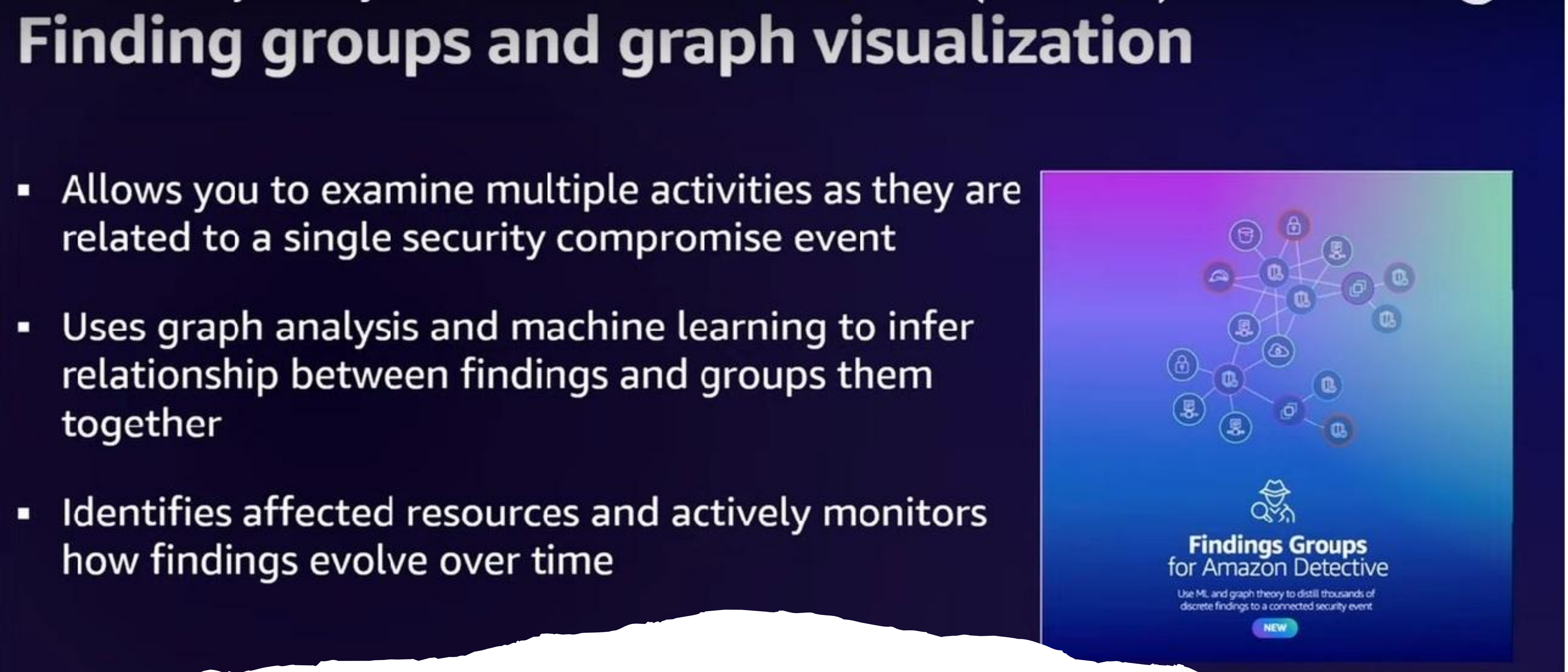
EKS pod

attached

IAM role

assumed

Detective Linkages



Finding groups and graph visualization

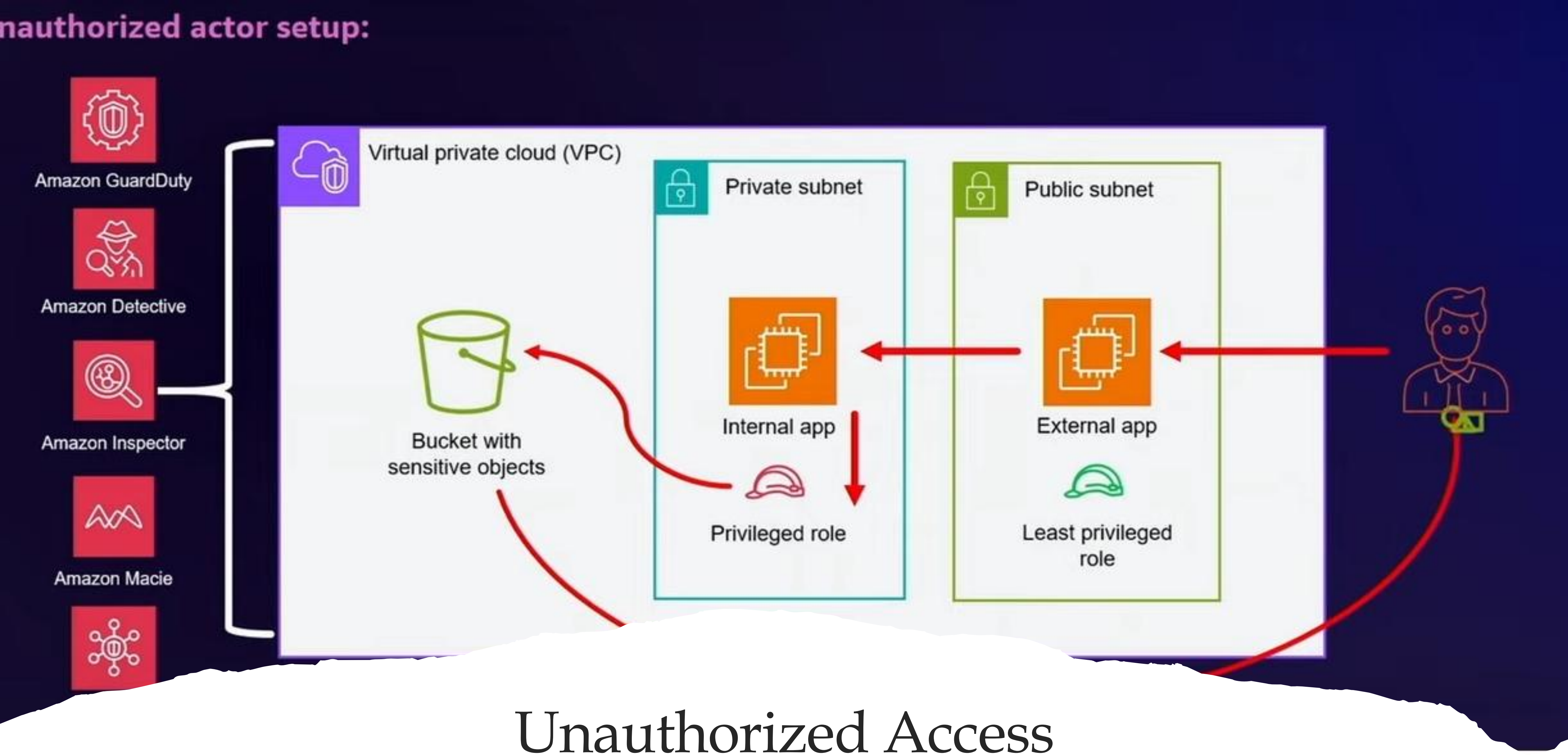
- Allows you to examine multiple activities as they are related to a single security compromise event
- Uses graph analysis and machine learning to infer relationship between findings and groups them together
- Identifies affected resources and actively monitors how findings evolve over time

Findings Groups
for Amazon Detective

Use ML and graph theory to distill thousands of discrete findings to a connected security event

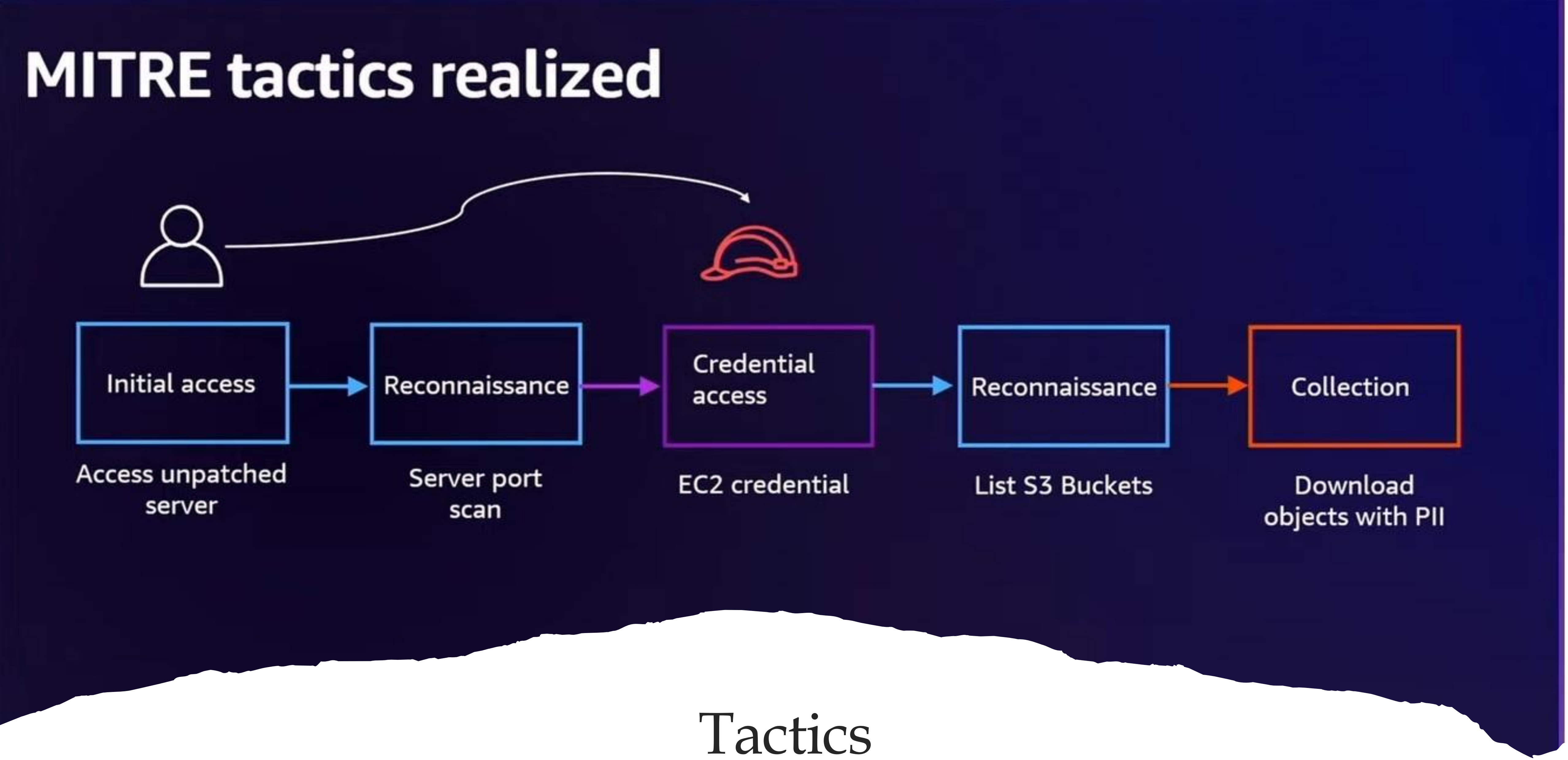
NEW

Detective Visualization



nauthorized actor setup:

Unauthorized Access



MITRE tactics realized

Initial access → Reconnaissance → Credential access → Reconnaissance → Collection

Access unpatched server

Server port scan

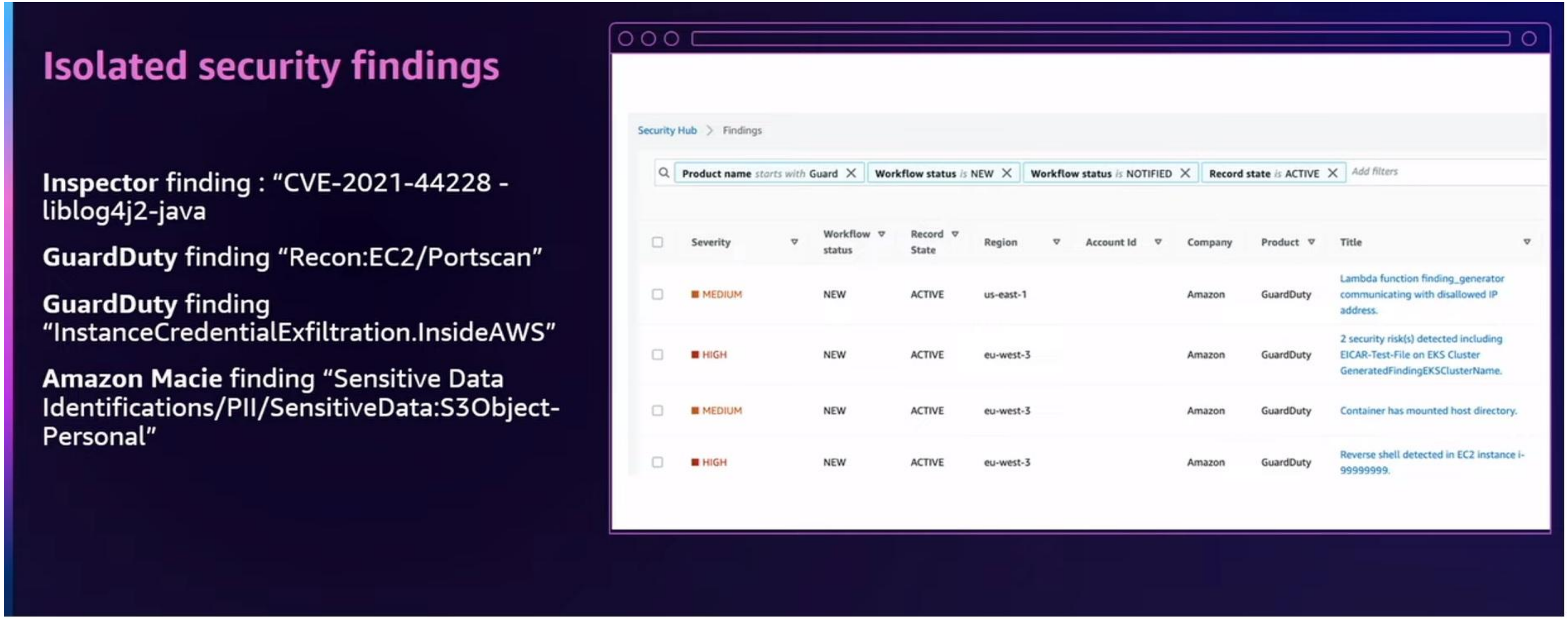
EC2 credential

List S3 Buckets

Download objects with PII

Tactics

Isolated security Findings



Isolated security findings

Inspector finding : “CVE-2021-44228 - liblog4j2-java

GuardDuty finding “Recon:EC2/Portscan”

GuardDuty finding “InstanceCredentialExfiltration.InsideAWS”

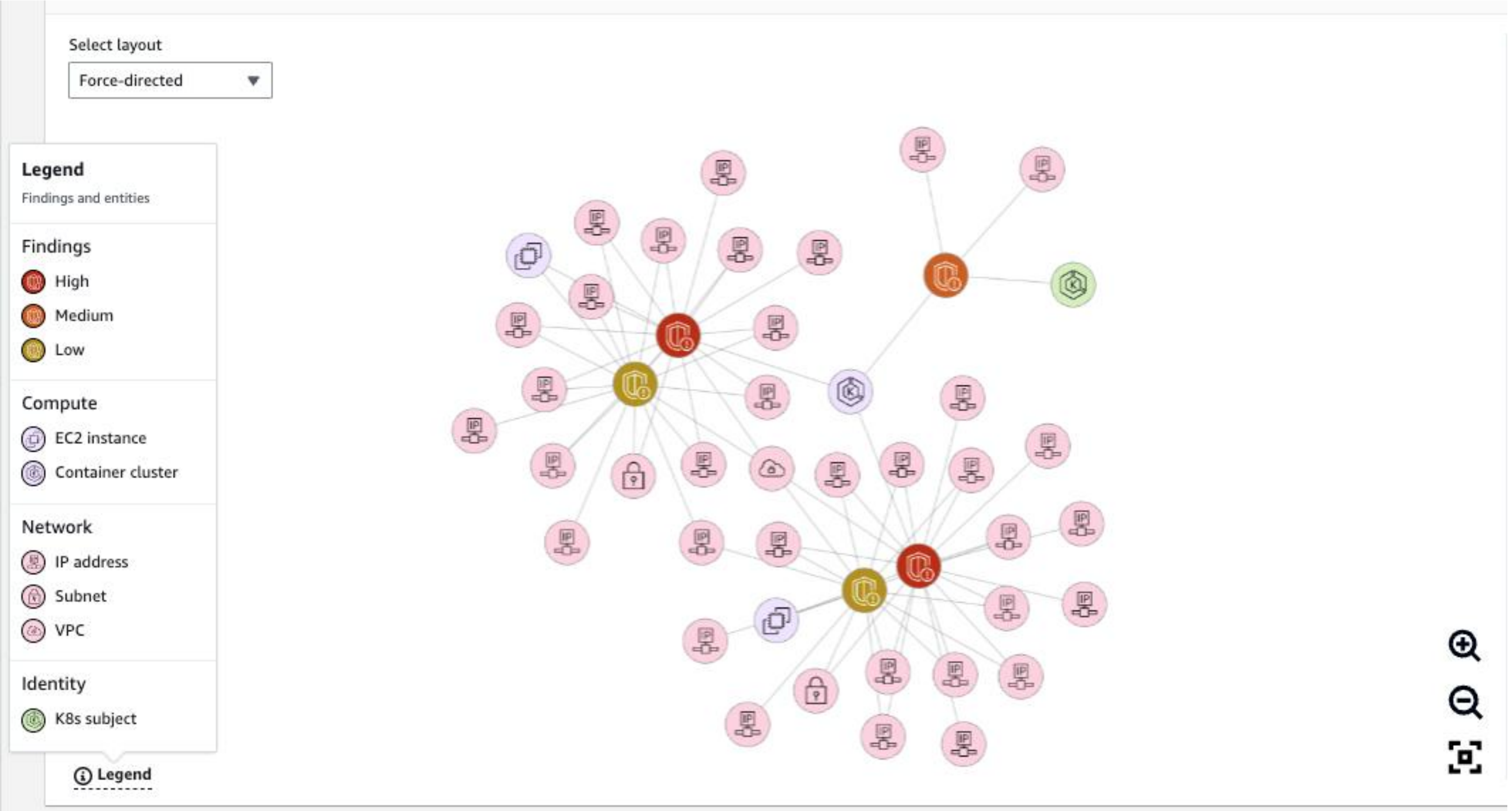
Amazon Macie finding “Sensitive Data Identifications/PII/SensitiveData:S3Object-Personal”

Security Hub > Findings

Product name *starts with* Guard ✕ | Workflow status *is* NEW ✕ | Workflow status *is* NOTIFIED ✕ | Record state *is* ACTIVE ✕ | *Add filters*

□	Severity	Workflow status	Record State	Region	Account Id	Company	Product	Title
□	MEDIUM	NEW	ACTIVE	us-east-1		Amazon	GuardDuty	Lambda function finding_generator communicating with disallowed IP address.
□	HIGH	NEW	ACTIVE	eu-west-3		Amazon	GuardDuty	2 security risk(s) detected including EICAR-Test-File on EKS Cluster GeneratedFindingEKSClusterName.
□	MEDIUM	NEW	ACTIVE	eu-west-3		Amazon	GuardDuty	Container has mounted host directory.
□	HIGH	NEW	ACTIVE	eu-west-3		Amazon	GuardDuty	Reverse shell detected in EC2 instance i-99999999.

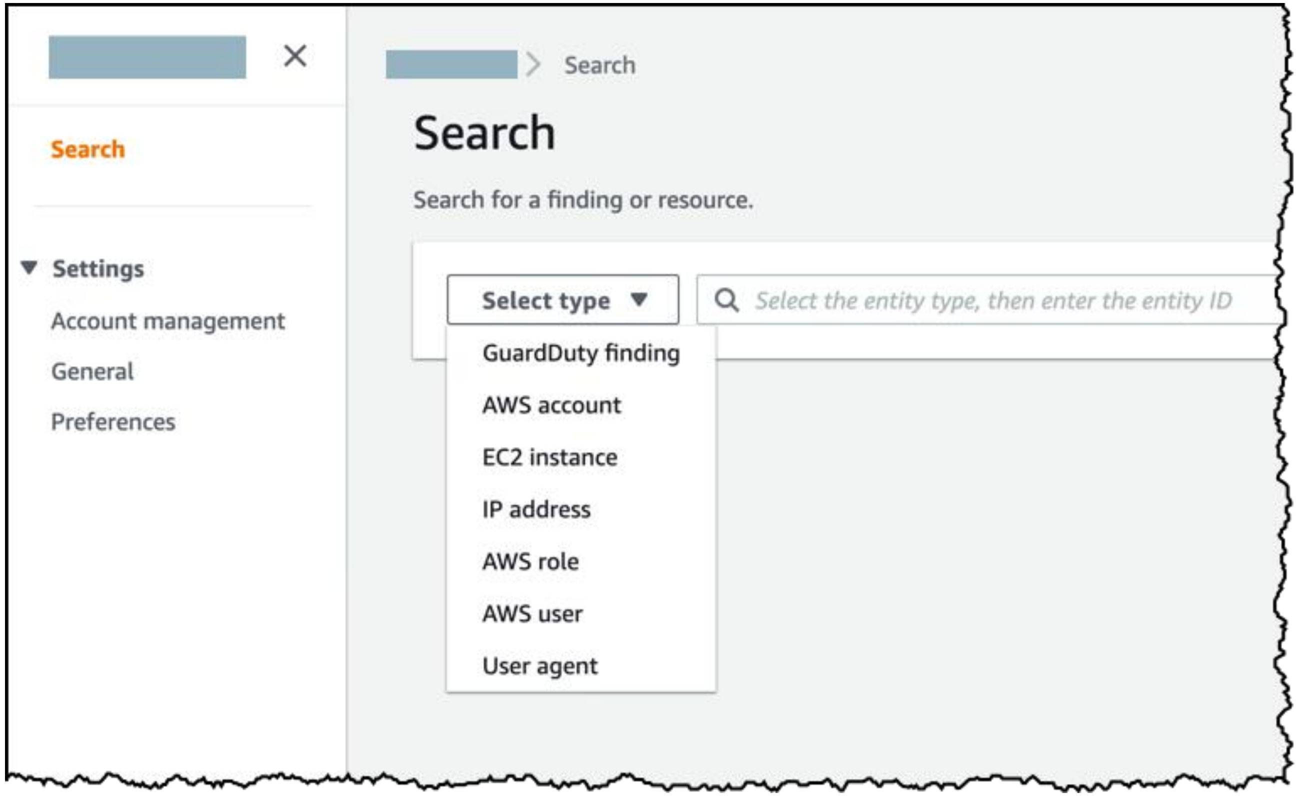
Investigation – Finding Groups



Select layout

Force-directed ▼

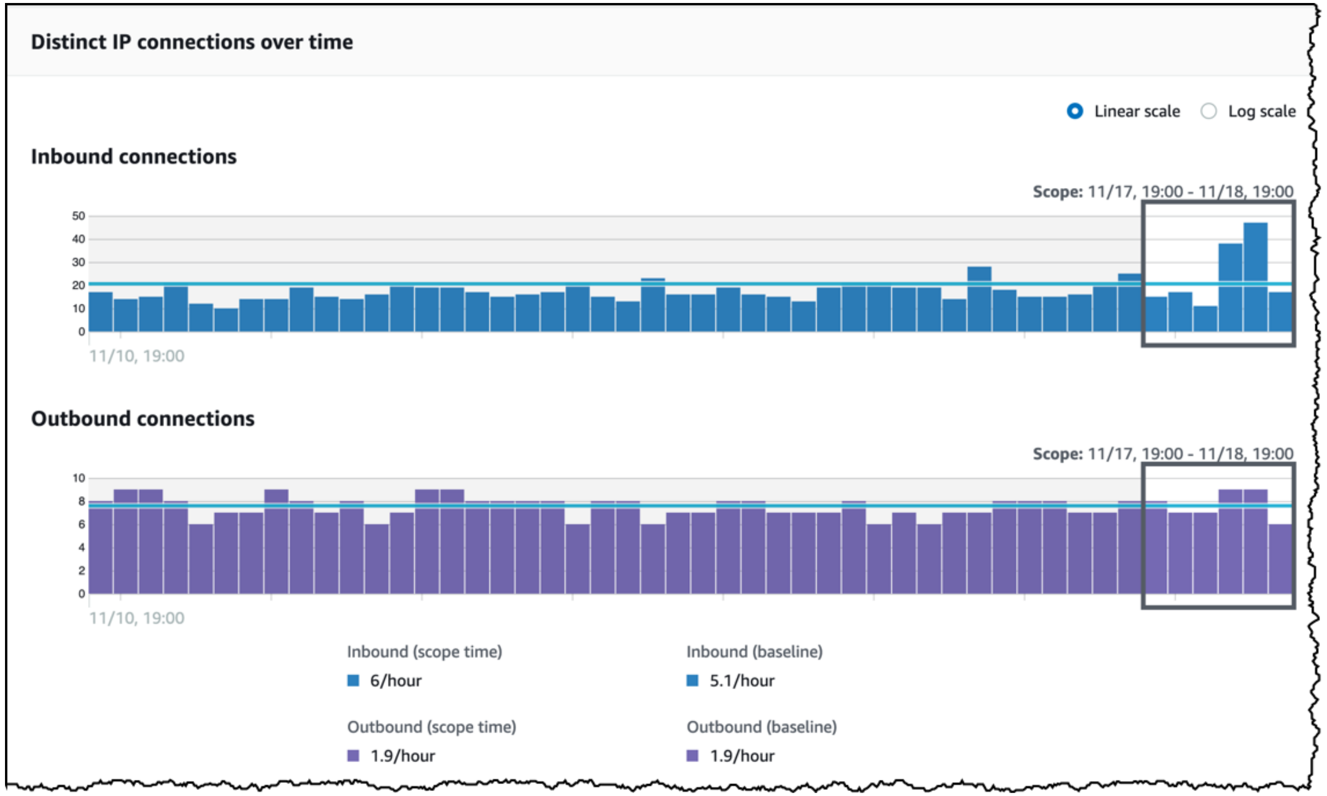
AWS Detective - Findings



Search

Search for a finding or resource.

AWS Detective - Findings



Distinct IP connections over time

● Linear scale ○ Log scale

Inbound connections

Scope: 11/17, 19:00 - 11/18, 19:00

Outbound connections

Scope: 11/17, 19:00 - 11/18, 19:00

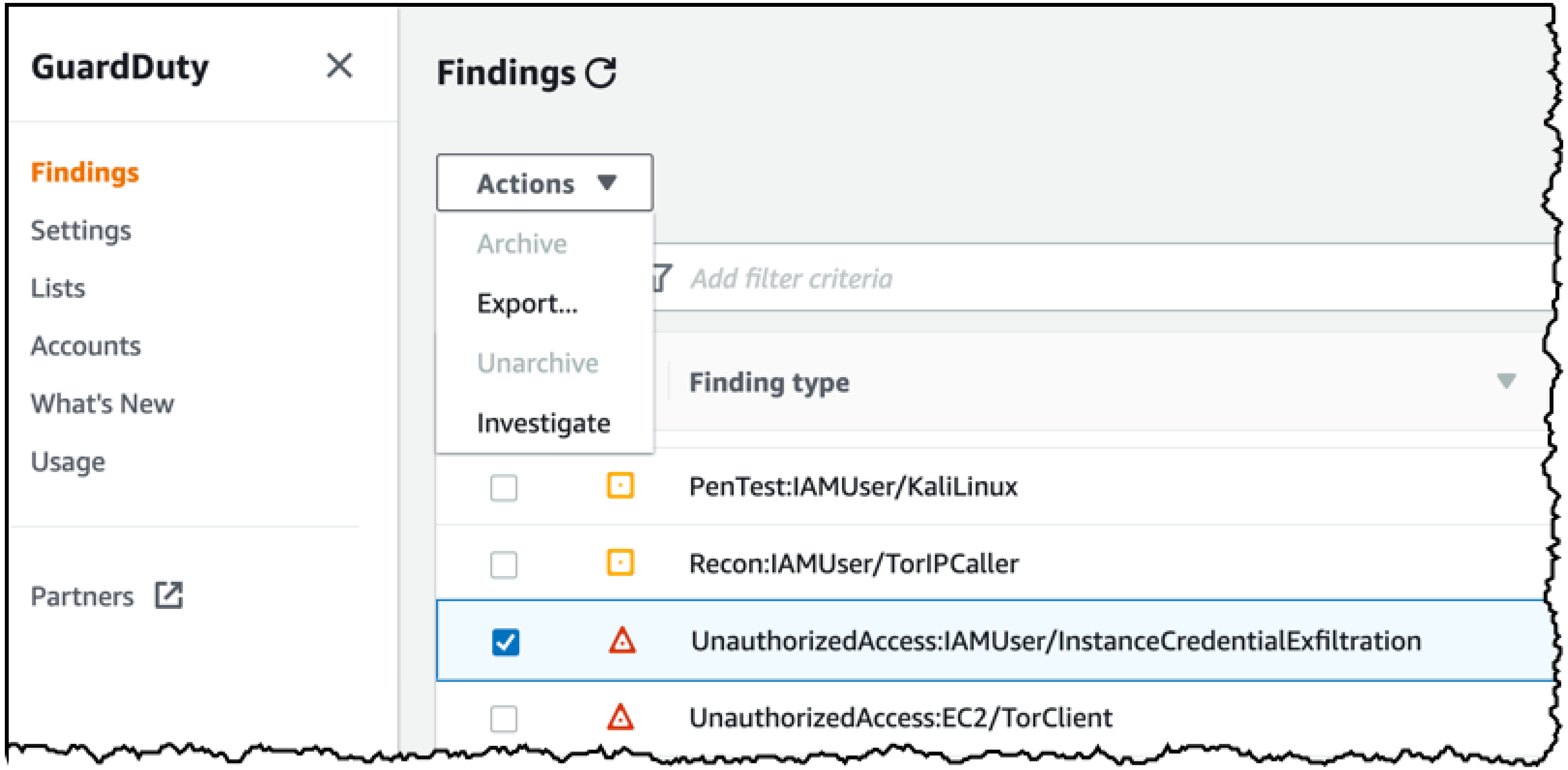
Inbound (scope time)
■ 6/hour

Inbound (baseline)
■ 5.1/hour

Outbound (scope time)
■ 1.9/hour

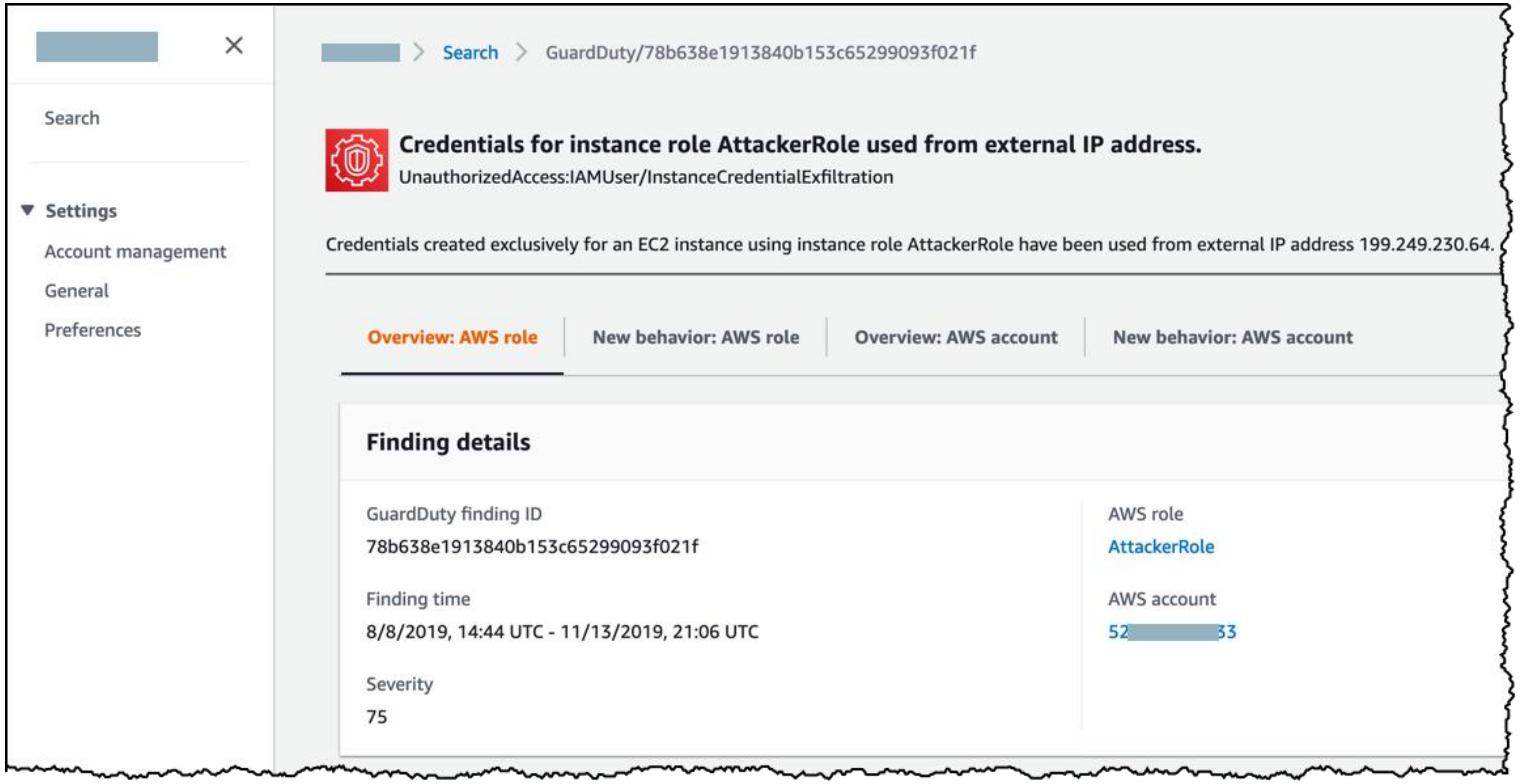
Outbound (baseline)
■ 1.9/hour

Detective & Guard Duty



		Finding type
□		PenTest:IAMUser/KaliLinux
□		Recon:IAMUser/TorIPCaller
☑	⚠	UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration
□	⚠	UnauthorizedAccess:EC2/TorClient

Attack Details



[redacted] > Search > GuardDuty/78b638e1913840b153c65299093f021f

Credentials for instance role AttackerRole used from external IP address.
UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration

Credentials created exclusively for an EC2 instance using instance role AttackerRole have been used from external IP address 199.249.230.64.

Finding details

GuardDuty finding ID
78b638e1913840b153c65299093f021f

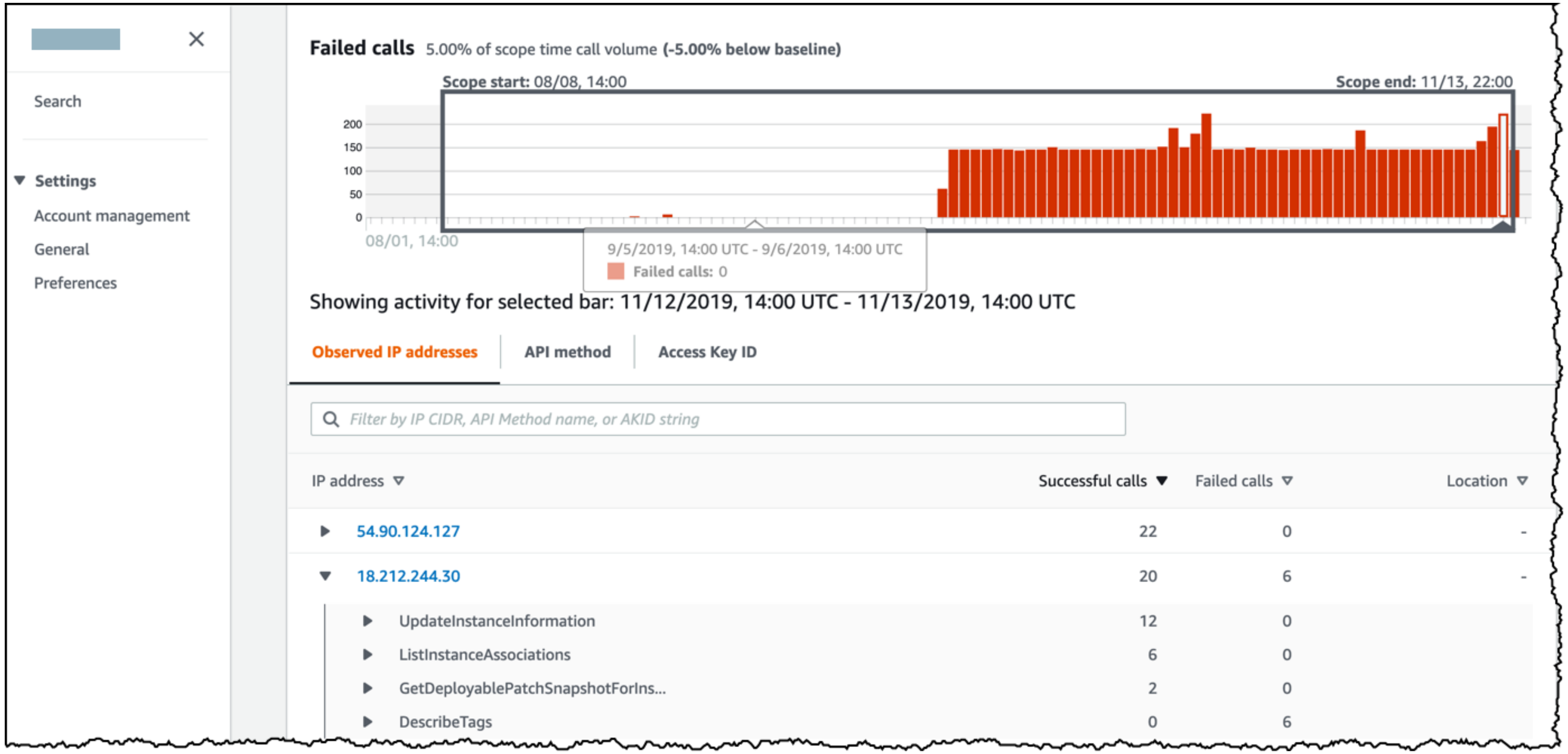
Finding time
8/8/2019, 14:44 UTC - 11/13/2019, 21:06 UTC

Severity
75

AWS role
AttackerRole

AWS account
52[redacted]33

Failed API Calls



Failed calls 5.00% of scope time call volume **(-5.00% below baseline)**

Scope start: 08/08, 14:00

Scope end: 11/13, 22:00

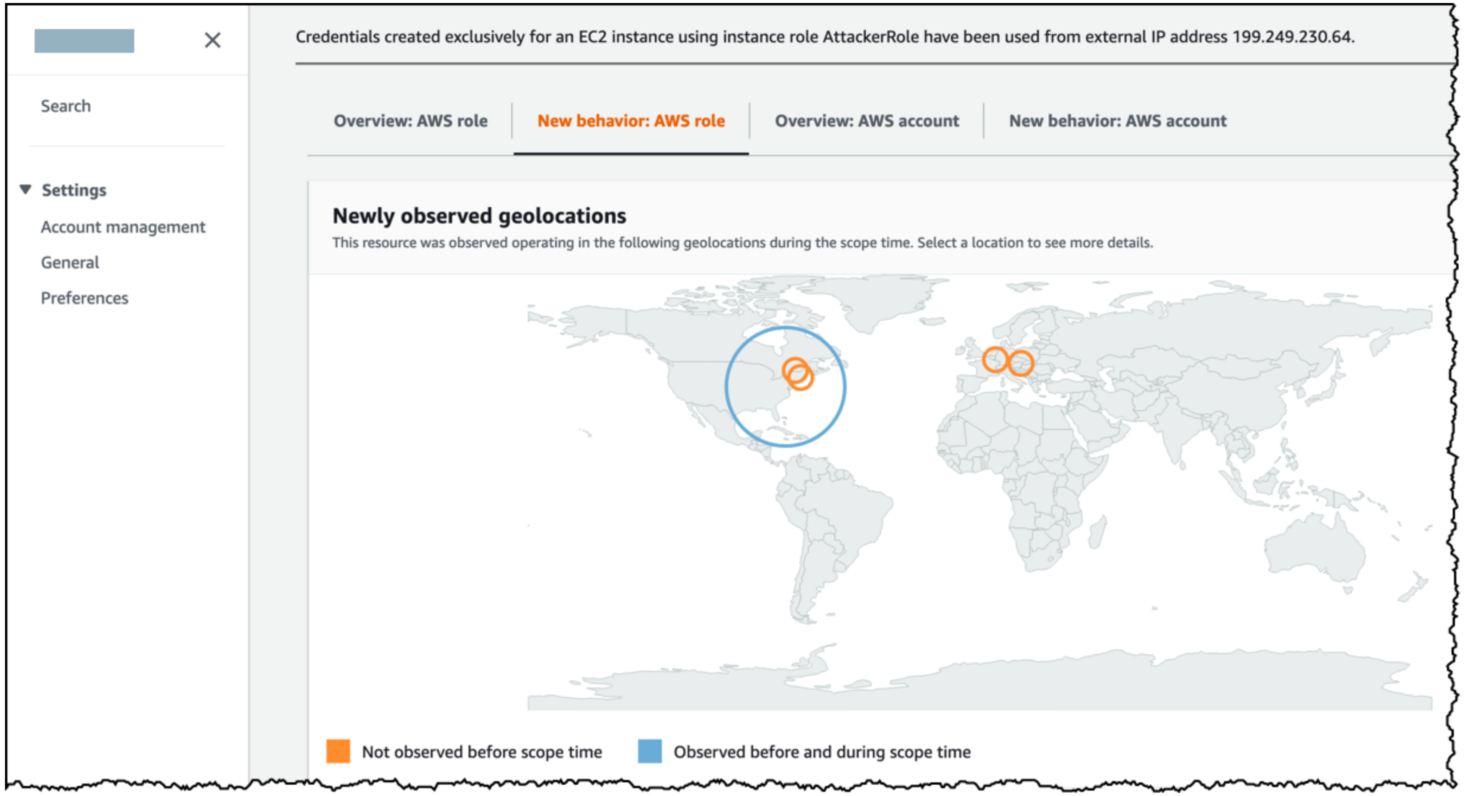
9/5/2019, 14:00 UTC - 9/6/2019, 14:00 UTC

Failed calls: 0

Showing activity for selected bar: 11/12/2019, 14:00 UTC - 11/13/2019, 14:00 UTC

IP address ▽	Successful calls ▼	Failed calls ▽	Location ▽
▶ 54.90.124.127	22	0	-
▼ 18.212.244.30	20	6	-
▶ UpdateInstanceInformation	12	0	
▶ ListInstanceAssociations	6	0	
▶ GetDeployablePatchSnapshotForIns...	2	0	
▶ DescribeTags	0	6	

Location



Credentials created exclusively for an EC2 instance using instance role AttackerRole have been used from external IP address 199.249.230.64.

Newly observed geolocations

This resource was observed operating in the following geolocations during the scope time. Select a location to see more details.

🟧 Not observed before scope time 🟦 Observed before and during scope time

Thank you