

AWS Cloud Security Foundations (AWS-CSF)

Lecture 10

Responding to and Managing an Incident

Prepared by
Dr. Ibrahim Gomaa

Lecture 10: Responding to and Managing an Incident

Topics

- Identifying an incident
- AWS services that support the discovery and recognition phase
- AWS services that support the resolution and recovery phase
- Best practices and new trends for handling an incident

Identifying an incident

Incident recognition and response

- Is a set of information security policies and procedures that you can use to identify, contain, and eliminate cyberattacks
- Enables an organization to quickly detect and halt attacks
- Helps you to minimize damage and prevent future attacks

Recognizing incidents

Not all events are incidents in need of immediate remedy.

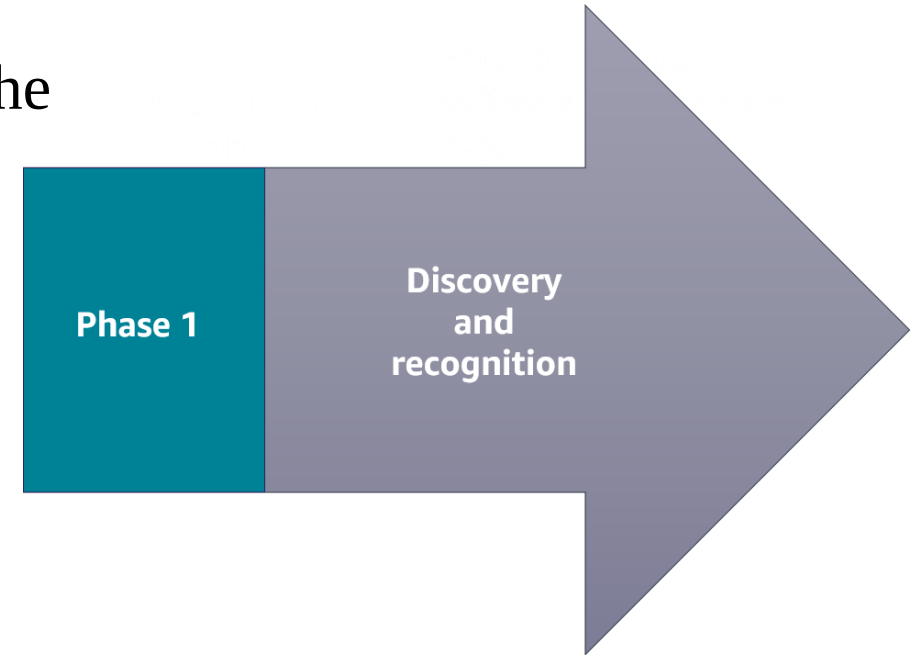
Let's take a look at a few examples of such events:

- Logging in from a remote location
- Failing hard drive that is still fully operational
- Employee trying to access resources that they shouldn't access

Phase 1: Discovery and recognition

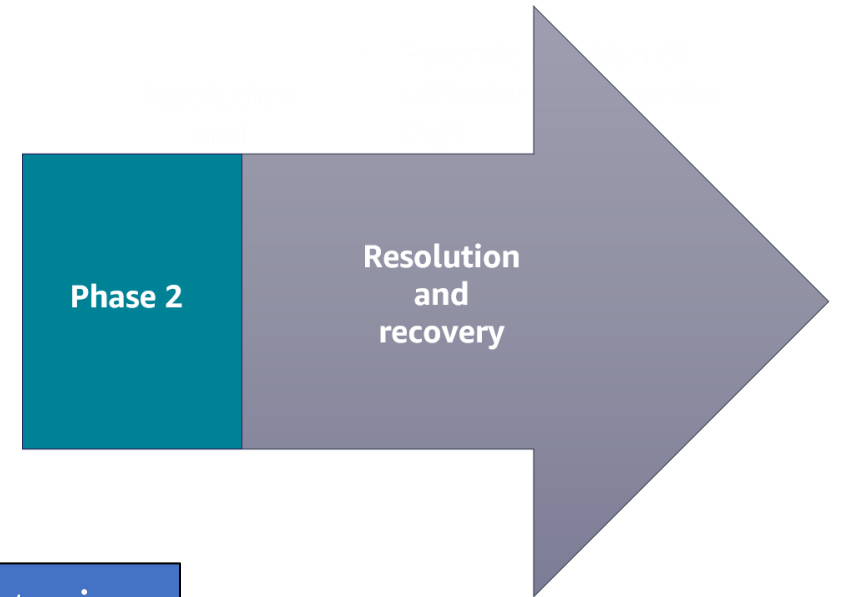
Incident response has two phases. The first phase is the *discovery and recognition phase*

- Incident identification, logging, and categorization
- Incident notification and escalation
- Investigation and diagnosis



Phase 2: Resolution and recovery

- Forensic isolation (if software, reproduce the bug)
- Stage a fix: Reproduce the issue, apply a fix, and test
- Deploy the fix: Push any new infrastructure as code, or any new application code to production
- Incident closure: Resolve the incident



Automate these processes wherever possible, and run game days in staging (safe) environments to fine-tune your corporate-wide incident response process.

AWS services that support the discovery and recognition phase

Discovery and recognition phase



AWS Trusted
Advisor



Amazon
CloudWatch



Amazon
Inspector



Amazon
GuardDuty



AWS Shield



AWS Config

AWS Trusted Advisor

- Draws upon best practices learned from serving hundreds of thousands of AWS customers
- Inspects your AWS environment, and then makes recommendations when opportunities exist to improve performance and help close security gaps



AWS Trusted
Advisor

Amazon CloudWatch

- Provides a reliable, scalable, and flexible monitoring solution that you can start using within minutes
- Automatically displays metrics about every AWS service that you use
- Provides the ability to create alarms that watch metrics and send notifications



Amazon
CloudWatch

Amazon Inspector

- Is a vulnerability management service that continuously scans your AWS workloads for vulnerabilities
- Automatically discovers and scans Amazon Elastic Compute Cloud (Amazon EC2) instances and container images that reside in Amazon Elastic Container Registry (Amazon ECR)
- Creates a finding when it discovers a vulnerability or network issue



Amazon
Inspector

Amazon GuardDuty

- Is a continuous security monitoring service
- Identifies unexpected and potentially unauthorized or malicious activity
- Uses threat intelligence feeds: such as lists of malicious IP addresses and domains, and machine learning to identify unexpected and potentially unauthorized and malicious activity within your AWS environment, For example, GuardDuty can detect compromised EC2 instances serving malware or mining bitcoin



Amazon
GuardDuty

AWS Shield

- Automatically protects an enterprise network from a distributed denial of service (DDoS) attack
- Offers the AWS Shield Advanced managed threat protection service to improve your security posture with additional DDoS detection, mitigation, and response capabilities



AWS Shield

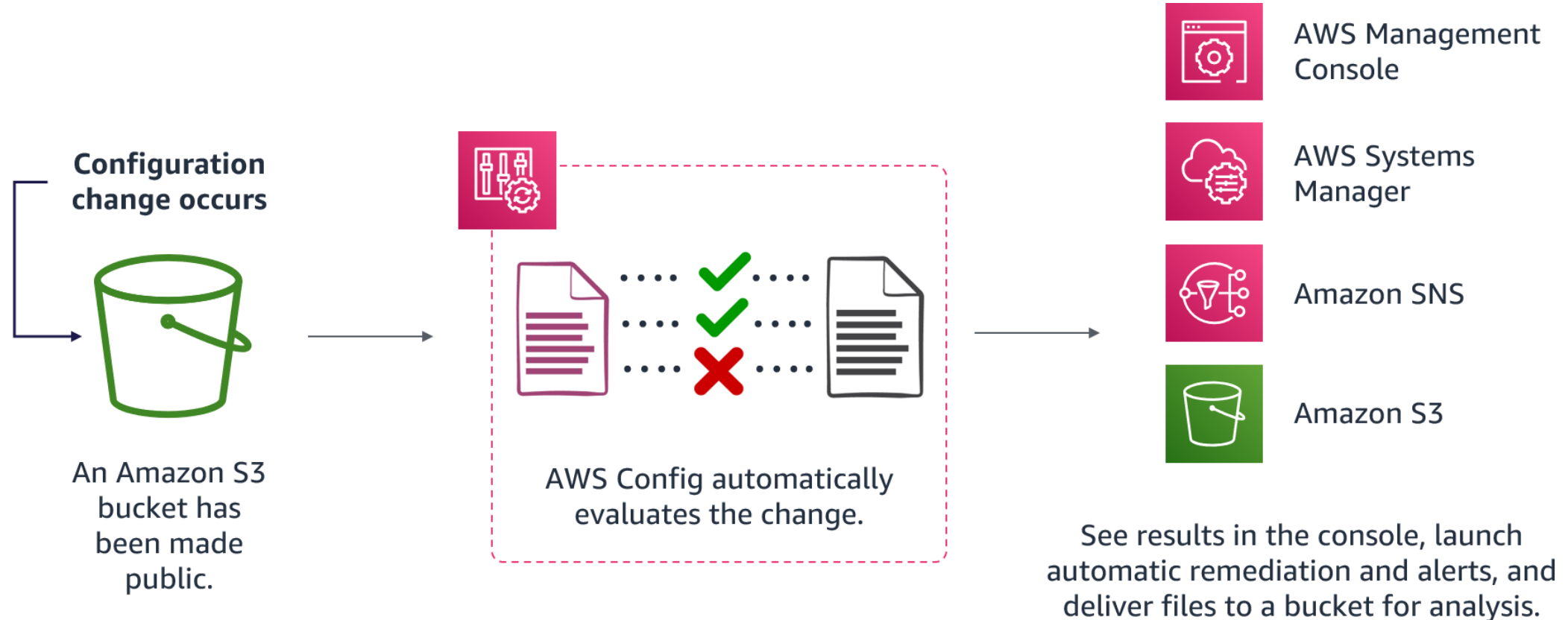
AWS Config

- Is a continuous monitoring and assessment service
- Provides the ability to view current and historic configurations of a resource and use this information to troubleshoot outages
- Sends notifications when changes occur
- Integrates with other AWS services to remediate issues



AWS Config

Evaluating AWS Config rules



AWS services that support the resolution and recovery phase

AWS services that support the resolution and recovery phase

Resolution and recovery



AWS Systems
Manager



AWS
CloudFormation

Event-driven responses

is a computer program that is written to respond to actions generated by the user or the system.



Amazon Simple
Notification Service
(Amazon SNS)



AWS Step Functions



AWS Lambda

AWS Systems Manager

- Gives you visibility and control of your infrastructure on AWS
- Provides a unified user interface so that you can view operational data from multiple AWS services
- Provides the ability to group resources by application and view operational data for monitoring and troubleshooting
- Helps you to keep your instances in their defined state and perform on-demand changes, such as updating applications or running shell scripts



AWS Systems
Manager

AWS CloudFormation

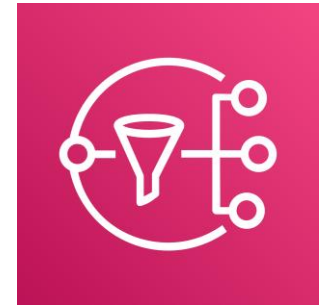
- Helps you model and set up your AWS resources so that you can spend less time managing those resources and more time focusing on your applications that run in AWS
- Provides the ability to create a template that describes all the AWS resources that you want
- Can be used to re-create a staging environment inside an isolated, or forensic, virtual private cloud (VPC)



AWS
CloudFormation

Amazon Simple Notification Service (Amazon SNS)

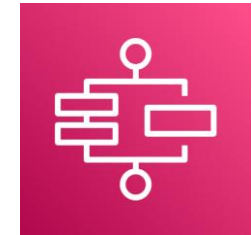
- Is an event-driven web service that provides the ability for applications, end users, and devices to instantly send and receive notifications from the cloud



Amazon Simple
Notification Service
(Amazon SNS)

AWS Step Functions

- Is a visual workflow service that developers use to build distributed applications, and automate IT and business processes
- Provides the ability to create event-driven workflows to manage failures, retries, parallelization, service integrations, and observability so that developers can focus on higher value business logic



AWS Step Functions

When an enterprise experiences abnormalities, implementing Step Functions can help you to create complex business logic in event-driven workflows that connect services, systems, or people within minutes

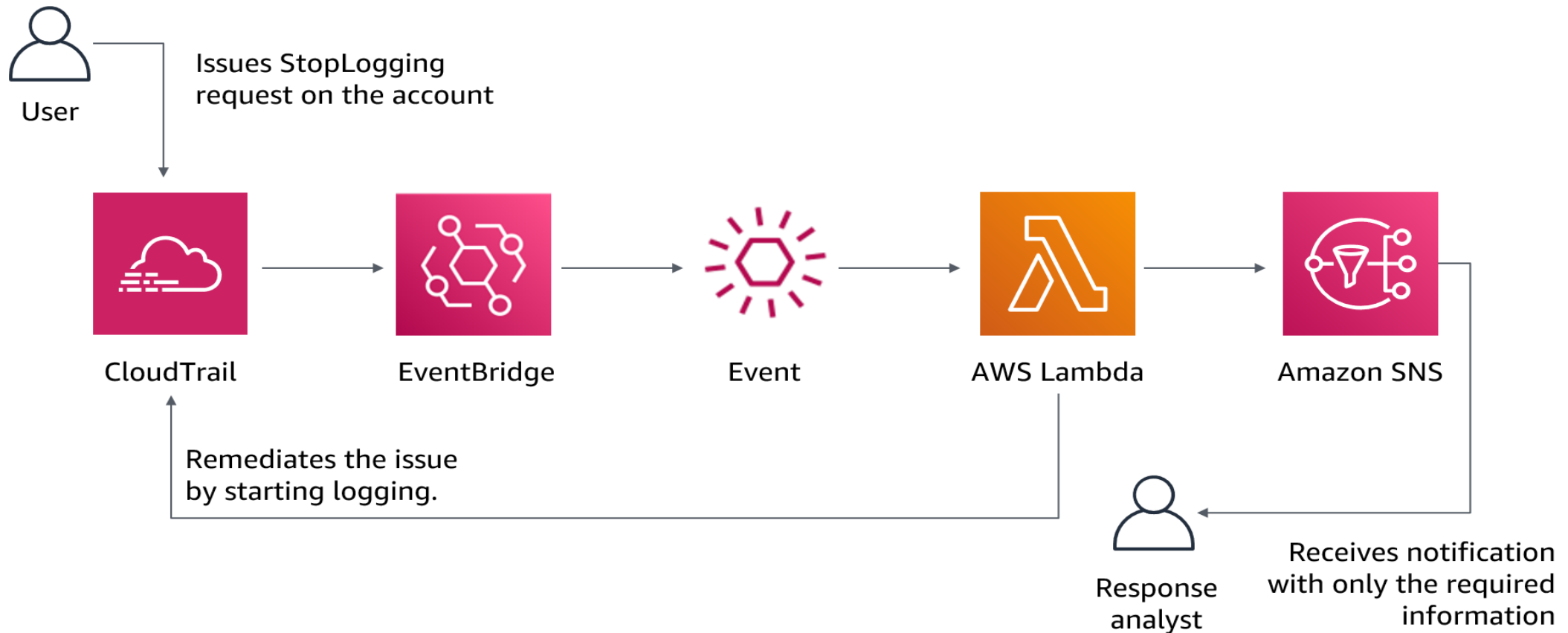
AWS Lambda

- Is a serverless, event-driven compute service that provides the ability to run code on demand without provisioning or managing servers
- Lambda functions are stateless



AWS Lambda

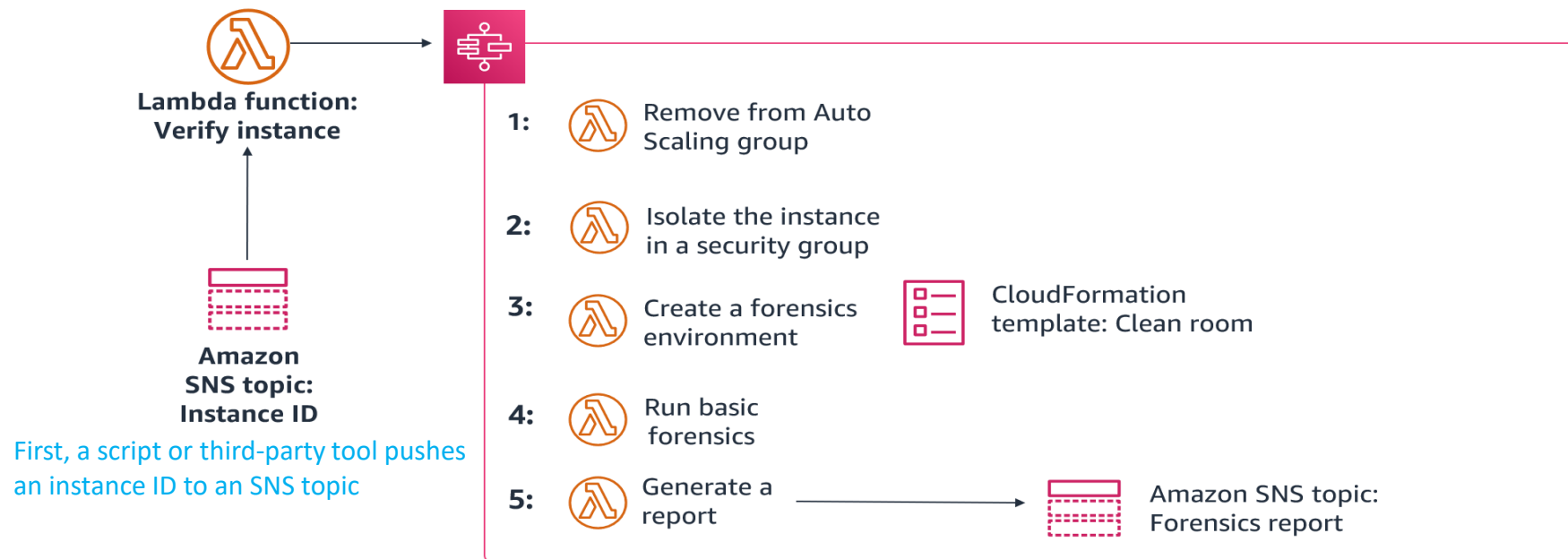
Lambda for incident response



Working together for incident response

an example of how to use [Step Functions](#), [Lambda](#), [CloudFormation](#), and [Amazon SNS](#) to remediate a compromised instance.

Then, a Lambda function verifies the ID and, if compromised, initiates the following Step Functions workflow:



Best practices and new trends for handling an incident

Industry best practices for handling incidents

- Identify key personnel, external resources, and tooling.
- Automate containment capabilities.
- Develop incident response plans.
- Pre-provision access and tools.
- Run incident response game days.



New trends for handling incidents

Agentic AI-Powered Investigation (AI-Native IR)

AWS has introduced AI agents within the AWS Security Incident Response service that automatically gather and analyze evidence.

- **Automated Context Gathering:** When a case is created, the AI agent automatically queries AWS CloudTrail, IAM configurations, Amazon EC2 details, and Cost Explorer to build a timeline and identify indicators of compromise (IoCs).
- **Operational Intelligence:** The agent identifies suspicious patterns—such as unauthorized API calls or unusual resource consumption—and presents actionable summaries within minutes

New trends for handling incidents

AWS Security Incident Response (Dedicated Service)

This service centralizes incident handling to tackle alert fatigue and fragmentation across multiple accounts.

- **Intelligent Auto-Triage:** The service filters out noise, with the capability to suppress 99% of non-critical findings, allowing teams to focus on high-priority alerts.
- **Cross-Account Collaboration:** It enables centralized coordination for multi-account environments and provides a "single pane of glass" for visibility.

New trends for handling incidents

"Containment-as-Code" and Automated Remediation

The trend is to immediately isolate compromised resources using automated playbooks.

- **Systems Manager Integration:** Security Incident Response uses AWS Systems Manager to trigger automated containment, such as removing security groups or creating snapshots of compromised instances.
- **Pre-approved Actions:** Organizations can define and automate remediation steps for common scenarios, such as credential compromises or data exfiltration attempts.

New trends for handling incidents

Shift to Proactive and "Always-On" Support

- **AWS Incident Detection & Response (IDR):** This premium service offers a 5-minute response time from engineers for critical, business-impacting events, extending beyond automated alerts.
- **Proactive Engagement:** IMEs (Incident Management Engineers) monitor specific workloads 24x7, initiating collaboration if an anomaly is detected.

New trends for handling incidents

Focus on Post-Incident "Lessons Learned"

- **Automated Reporting:** The new "CloudWatch Investigations" feature allows users to automatically generate reports that include a full incident timeline, impact assessment, and recommended actions, simplifying post-incident reviews.
- **Continuous Improvement:** The service analyzes false positives to refine auto-triage rules and update suppression rules for GuardDuty and Security Hub.

Thanks