Responding to and Managing an Incident

IDENTIFYING INCIDENTS · TWO-PHASE LIFECYCLE · DISCOVERY SERVICES · RECOVERY SERVICES · EVENT-DRIVEN AUTOMATION · BEST PRACTICES

STUDY & REVIEW

01 MUST KNOW

if you remember five things, remember these

01 **What it is: incident response** is a set of information security policies and procedures you use to **identify, contain, and eliminate** cyberattacks. The goal is to quickly detect and halt attacks, which minimizes damage and helps prevent future attacks of the same type.

02 **Not every event is an incident:** an **event** is any observed occurrence; an **incident** needs immediate analysis and remediation. A remote login (traveler on a VPN), a failing-but-still-operational drive, or a *denied* access attempt are events worth watching — not necessarily incidents to remedy right now.

03 **Two phases: Phase 1 — discovery and recognition** (identification, logging, categorization → notification and escalation → investigation and diagnosis). **Phase 2 — resolution and recovery** (forensic isolation → stage a fix → deploy the fix → incident closure). Automate wherever possible; rehearse in staging.

04 **Detect vs. remediate services: discovery/recognition** → Trusted Advisor, CloudWatch, Amazon Inspector, GuardDuty, Shield, AWS Config. **Resolution/recovery** → Systems Manager, CloudFormation, Amazon SNS, Step Functions, Lambda. These lists are not exhaustive.

05 **Event-driven automation:** a **detective mechanism invokes a responsive mechanism** to remediate automatically and cut time-to-value. **Lambda, SNS, and Step Functions** are the event-driven response services — e.g., EventBridge catches a `cloudtrail:StopLogging` event and invokes a Lambda function to restart logging.

02 KEY TERMS

TERM	DEFINITION
Incident response	A set of information security policies and procedures used to identify, contain, and eliminate cyberattacks
Event vs. incident	An event is any observed occurrence; an incident is an event that needs immediate analysis and remediation — not all events are incidents
Discovery and recognition	Phase 1: identification, logging, and categorization; notification and escalation; investigation and diagnosis
Resolution and recovery	Phase 2: forensic isolation, staging a fix, deploying the fix, and incident closure
Escalation	Handing an incident to a more experienced or specialized employee when the current responder cannot resolve it
Forensic isolation	Isolating an affected component and deep-diving to find the issue, often by capturing a disk image or as-is OS configuration
Finding	An Amazon Inspector record that describes a vulnerability, identifies the affected resource, rates its severity, and gives remediation guidance
DDoS attack	A malicious attempt to disrupt normal traffic by overwhelming a target or its infrastructure with a flood of internet traffic
Event-driven response	A program written to respond to actions generated by the user or system — a detective mechanism invokes a responsive one
Runbook	An easy-to-follow document detailing the steps to take to respond to and recover from an incident
Game day	A simulated incident-response event, run in a safe (staging) environment with key staff and management, used to fine-tune the process

TERM	DEFINITION
Hot swapping	Removing or plugging in components while the power remains switched on

03 THE INCIDENT RESPONSE LIFECYCLE

Phase 1 discovery & recognition → Phase 2 resolution & recovery

01 Identify · log · categorize → 02 Notify · escalate → 03 Investigate · diagnose → 04 Forensic isolation → 05 Stage · deploy fix → 06 Incident closure

04 DISCOVERY & RECOGNITION SERVICES

detect and identify an attack

SERVICE	WHAT IT DOES	REMEMBER
Trusted Advisor	Inspects your environment against best practices and recommends fixes that close security gaps	Checks vary by Support plan
CloudWatch	Displays metrics for every AWS service you use; alarms watch metrics and send notifications	Monitoring & alarms
Amazon Inspector	Continuously scans EC2 instances and ECR container images for vulnerabilities; creates a **finding**	Vulnerability management
Amazon GuardDuty	Threat-intelligence feeds + ML detect unexpected or malicious activity in your account	Continuous threat detection
AWS Shield	Automatic protection from common DDoS attacks; Shield Advanced adds detection/mitigation/response	DDoS protection
AWS Config	Inventories resources and records configuration changes; notifies and can remediate	Config monitoring & inventory

05 RESOLUTION & RECOVERY SERVICES

contain, remediate, and recover

SERVICE	WHAT IT DOES	REMEMBER
Systems Manager	Visibility and control; unified view of operational data; keeps instances in a defined state	Ops, automation & patching
CloudFormation	Provisions resources from a template; can rebuild a staging env in an isolated (forensic) VPC	Infrastructure as code
Amazon SNS	Instantly sends/receives notifications to apps, users, devices; can invoke Lambda	Notifications — event-driven
Step Functions	Low-code visual workflows that coordinate a multi-step response	Orchestration — event-driven
AWS Lambda	Serverless, **stateless** code that runs on demand in response to events	Compute — event-driven

06 BEST PRACTICES: PREPARE VS. REHEARSE

preparation minimizes disruption

PREPARE & PRE-POSITION

before an incident happens

- Identify key personnel, external resources, and tooling
- Develop IR plans and easy-to-follow runbooks
- Pre-provision access and pre-deploy tools into AWS
- Automate containment to reduce response time and impact

REHEARSE & IMPROVE

so the plan works under pressure

- Run incident response game days for different threats
- Involve key staff and management
- Document root cause to prevent recurrence
- Feed lessons learned back into the process

07 EXAM TRAPS

where the knowledge check gets you

- × “Any anomaly is an incident that needs immediate remediation.” — No. Not all events are incidents: a remote login (traveler on an approved VPN), a failing-but-operational drive, or a *denied* access attempt are events to monitor, not necessarily incidents to remedy now.
- × “Escalation means notifying the customer.” — Escalation is handing the incident to a **more experienced or specialized employee** when the current responder can't resolve it themselves.
- × “GuardDuty scans your instances for software vulnerabilities.” — That is **Amazon Inspector** (scans EC2 + ECR images, creates findings). **GuardDuty** uses threat-intel feeds and ML to spot malicious activity and account-behavior anomalies.
- × “AWS Config and CloudTrail do the same thing.” — **Config** is continuous monitoring/assessment that inventories resources and records configuration changes; **CloudTrail** captures API calls and provides *no* resource inventory.
- × “You need a paid plan for any DDoS protection.” — Building on AWS gives **automatic** protection against common DDoS attacks; **Shield Advanced** is the add-on for extra detection, mitigation, and response.
- × “Lambda functions keep state between runs.” — Lambda functions are **stateless**, with no affinity to the underlying infrastructure, so Lambda can rapidly launch as many copies as the incoming event rate needs.
- × “In event-driven response, the detective mechanism does the remediation.” — The **detective mechanism invokes a separate responsive mechanism**; e.g., EventBridge detects `cloudtrail:StopLogging` and invokes a Lambda function to remediate.
- × “Trusted Advisor gives every check on every plan.” — Basic/Developer get core security checks and all service-quota checks; only Business, Enterprise On-Ramp, and Enterprise plans unlock **all** checks plus Support API and CLI access.

08 SELF-QUIZ

answers are upside-down below

Q1 In information security, what is the term for the set of policies and procedures used to identify, contain, and eliminate cyberattacks?

Q2 What are the two phases of incident response, in order?

Q3 Which continuous monitoring and assessment service gives you an inventory of your AWS resources and records changes to their configuration?

Q4 Which vulnerability management service continuously scans EC2 instances and ECR container images and produces a finding?

Q5 Which service uses threat-intelligence feeds and machine learning to identify unexpected or potentially malicious activity in your account?

Q6 Which service automatically protects your AWS applications against distributed denial-of-service attacks?

Q7 Which monitoring service automatically displays metrics for every AWS service you use and lets you set alarms that send notifications?

Q8 Name the three AWS services the module calls event-driven response services.

Q9 Which service uses a template to recreate a staging environment inside an isolated, or forensic, VPC?

Q10 Rehearsing your incident response with simulated events that involve key staff and management is known as running what?

ANSWER KEY (rotate the page)

Q1 incident response **Q2** discovery and recognition, then resolution and recovery **Q3** AWS Config **Q4** Amazon Inspector **Q5** Amazon GuardDuty **Q6** AWS Shield **Q7** Amazon CloudWatch **Q8** AWS Lambda, Amazon SNS, and AWS Step Functions **Q9** AWS CloudFormation **Q10** incident response game days