AWS Incident Response Playbook Template

Incident Response Playbook Overview

This template provides a structured outline for detecting, investigating, and responding to security incidents in AWS. It assumes limited team size and leverages AWS-native services.

Triage Checklist

Item	Status
Confirm GuardDuty/Security Hub finding	☐
Review AWS Config changes	☐
Determine scope of access or compromise	☐
Log incident in internal tracking system	☐
Check IAM activity via CloudTrail	☐

Isolation Actions

- Isolate instances using security group modifications or move to a quarantine subnet
- Remove affected users' permissions temporarily
- Detach public-facing interfaces or load balancers where applicable

Evidence Collection

EBS Snapshots

- Identify attached volumes with `describe-instances`
- Create snapshots for each volume
- Tag with incident ID and timestamp

Memory Dump (Linux EC2)

- Trigger AVML dump via SSM command
- Store result in versioned, write-only S3 bucket
- Encrypt at rest with SSE-S3 or KMS

Retrieve Instance Metadata

- Use SSM to run: `curl http://169.254.169.254/latest/meta-data/`
- Save output to secure S3 bucket
- Include as part of forensic report

Cold Storage for Evidence

- Use S3 Glacier or Deep Archive for long-term storage
- Apply Object Lock (Governance or Compliance mode)
- Tag evidence with:
  - Case ID
  - Analyst name
  - Acquisition date

Post-Incident Analysis

- Conduct internal review with involved stakeholders
- Identify control failures and response delays
- Determine if playbooks or detections require updates

Reporting Template

Unset

```
### Incident Summary


-   Case ID: IR-YYYY-NNN

-   Date Detected:

-   Source: (e.g., GuardDuty, Security Hub, Internal report)

-   Initial Scope:

-   Impact Assessment:

-   Responder(s):


### Timeline


| Time (UTC) | Event                        |

| ---------- | ---------------------------- |

| 09:12      | GuardDuty alert triggered    |

| 09:15      | Instance isolated via SSM    |


### Root Cause Analysis

### Remediation Actions

### Recommendations

### Lessons Learned
```

Response Log Table

Action Taken	By Who	When (UTC)	Signature
Example: EC2 snapshot created	Alice Morgan	2025-04-30 10:34	A.M. (digital)

Final Checks

Item	Completed
IAM credentials rotated	☐
Affected services redeployed / sanitized	☐
Findings documented in Security Hub	☐
Evidence backed up to S3 Glacier	☐

Note: Adapt this playbook to your environment. Test it in advance. Incident response is a skill — rehearse it regularly.