

AWS Incident Response Playbook Template

Version: 1.0

Author: Javier Pulido - <https://thehiddenport.dev> (<https://thehiddenport.dev>)

Use Case: Cloud-native environments (AWS), ISO 27001 aligned

Phase 1: Preparation

- ☐ Define roles (Incident Commander, Comms Lead, IR Engineer)
 - ☐ Ensure CloudTrail is enabled and stored securely
 - ☐ Enable GuardDuty, Security Hub, AWS Config
 - ☐ Set up pre-authorized SSM automation scripts for memory acquisition
 - ☐ Create IAM roles with least privilege for forensic access
 - ☐ Document critical assets (production accounts, regions, services)
-

Phase 2: Detection and Analysis

- ☐ Trigger: Security Hub finding or GuardDuty alert
 - ☐ Correlate with CloudTrail logs
 - ☐ Identify affected resources (EC2, IAM, S3, etc.)
 - ☐ Use `aws config` to trace change initiator
 - ☐ Tag incident in Security Hub with `WorkflowStatus: IN_PROGRESS`
 - ☐ Capture volatile data via SSM (AVML, netstat, ps)
-

Phase 3: Containment

- ☐ Isolate compromised EC2 via Security Group update
 - ☐ Revoke temporary credentials if compromised
 - ☐ Suspend affected IAM users
 - ☐ Disable automation roles if abused
-

Phase 4: Eradication and Recovery

- ☐ Patch vulnerable components
 - ☐ Rotate secrets/keys
 - ☐ Re-image compromised workloads (if necessary)
 - ☐ Restore from known-good backups
-

Phase 5: Lessons Learned

- ☐ Host a post-mortem with all involved
 - ☐ Document root cause and timeline
 - ☐ Update playbook based on this incident
 - ☐ Share a debrief with stakeholders (non-technical summary)
 - ☐ Mark Security Hub finding as `RESOLVED`
-

Appendix

- **Contact Matrix** (IR lead, CISO, platform lead)
 - **Tooling Links** (AVML, Volatility, SSM commands)
 - **EventBridge Rule Example**
 - **Slack Response Workflow**
-

For more templates and examples, visit <https://thehiddenport.dev>.