# ShopNimbus Incident Response Playbook — Project shopnimbus-security-group7

## 1. Purpose and Scope

This Incident Response Playbook outlines the procedures, roles, and responsibilities for detecting, analyzing, containing, eradicating, and recovering from cybersecurity incidents within the ShopNimbus Google Cloud Platform (GCP) environment. The project ‘shopnimbus-security-group7’ integrates Google Cloud Security Command Center (SCC), Cloud Logging, and BigQuery to ensure visibility and rapid response to potential threats. The playbook applies to all components within the ShopNimbus 3-tier architecture, including Web, Application, and Database tiers, and aligns with NIST SP 800-61 incident response principles.

## 2. Roles and Responsibilities

|  |  |
| --- | --- |
| Role | Responsibility |
| Security Lead / Incident Commander | Oversees the entire incident response process, coordinates communication, and authorizes containment actions. |
| Cloud Administrator | Implements technical containment, gathers forensic evidence, and restores affected systems. |
| SOC Analyst | Monitors Security Command Center (SCC) and Cloud Logging alerts, performs initial triage and classification. |
| Compliance Officer | Ensures regulatory and documentation requirements are fulfilled after incident resolution. |
| Communications Officer | Handles external and internal notifications and status reporting to stakeholders. |

## 3. Incident Response Phases

### 3.1 Identification

Detection begins with continuous monitoring through Cloud Logging, SCC, and BigQuery exports. The Security Command Center (SCC) aggregates findings from sources such as IAM, Firewall, and Cloud Asset Inventory. Example command used for verification:  
gcloud scc findings list projects/shopnimbus-security-group7 --location=global --source=- --limit=5  
  
Indicators of compromise may include repeated failed SSH login attempts, unexpected IAM role changes, or exposure of a public storage bucket. The SOC analyst reviews SCC dashboards and log exports to confirm anomalies.

### 3.2 Containment

Once an incident is confirmed, immediate containment is prioritized to prevent further damage. Containment actions may include revoking compromised credentials, applying restrictive firewall rules, or suspending affected service accounts (e.g., web-sa, app-sa, or db-sa). Containment commands may involve disabling access tokens or modifying IAM bindings via gcloud CLI.

### 3.3 Eradication

After containment, the root cause is identified and removed. This may involve deleting malicious scripts, patching vulnerable instances, or rotating encryption keys managed in Cloud KMS. Logs stored in the BigQuery dataset (scc\_logs) are used to trace incident origin. Eradication efforts ensure the environment is free from persistent threats or backdoors.

### 3.4 Recovery

System restoration begins after confirming that vulnerabilities have been remediated. Cloud resources are re-enabled under stricter IAM controls. Recovery procedures include re-deploying clean images, restoring data from verified backups, and reapplying monitoring policies. Service account permissions (e.g., service-363546819737@gcp-sa-logging.iam.gserviceaccount.com) are revalidated to ensure least-privilege access. Post-recovery validation ensures business continuity and confirms successful mitigation.

### 3.5 Lessons Learned

Following recovery, the incident response team conducts a debriefing to document lessons learned and preventive actions. SCC findings, logs, and response times are analyzed to improve detection accuracy and reduce mean time to respond (MTTR). Recommendations may include refining alert thresholds, tightening IAM policies, or expanding log retention.

## 4. Communication Plan

All incident communication follows a structured hierarchy to ensure timely updates and avoid misinformation. The Security Lead coordinates internal escalation, while the Communications Officer manages external notifications. Critical incidents are reported to stakeholders within one hour of confirmation. Communication channels include email, Slack (internal team), and Google Cloud alerting notifications (if enabled).

## 5. Example Scenario — Failed SSH Attempts

Scenario: Multiple failed SSH attempts detected on a Compute Engine instance hosting the Web Tier.  
  
1. SCC and Cloud Logging detect repeated 'FAILED LOGIN' entries.  
2. The SOC Analyst validates findings in BigQuery dataset (scc\_logs).  
3. Security Lead declares a security incident.  
4. Cloud Administrator applies a temporary firewall rule to block the attacking IP.  
5. IAM policies reviewed for unauthorized access.  
6. Instance snapshot taken for forensic analysis.  
7. Root cause: Unrestricted SSH access (0.0.0.0/0) in firewall configuration.  
8. Fix: Restrict SSH to trusted IPs and rotate service account credentials.

## 6. Evidence Tracking Table

|  |  |  |  |
| --- | --- | --- | --- |
| Evidence Item | Source / Command | Verified By | Date / Time |
| Enabled SCC APIs | gcloud services list --enabled | grep securitycenter | SOC Analyst | 9/9/205 |
| SCC Findings Output | gcloud scc findings list --project=shopnimbus-security-group7 | SOC Analyst | 10/9/2025 |
| BigQuery Log Dataset | bq ls scc\_logs | Cloud Admin | 12/9/2025 |
| Firewall Containment Action | gcloud compute firewall-rules update | Security Lead | 01/9/2025 |
| Incident Summary Report | Compiled via Cloud Shell logs and SCC dashboard | Compliance Officer | 03/9/2025 |

## 7. Conclusion

This playbook provides a structured and repeatable process for incident response within the ShopNimbus GCP environment. By leveraging Google Cloud Security Command Center, Cloud Logging, and BigQuery integrations, the project achieves real-time threat visibility and actionable response capabilities. The procedures ensure minimal downtime, maintain compliance, and promote continuous improvement in cybersecurity operations.