# ShopNimbus Cloud Security Project – Week 4 Deliverable

**Detection, Response & Recovery: Logging & Monitoring Implementation**

Project ID: shopnimbus-security-group7

## 1. Objective

This report outlines the configuration and verification of Google Cloud logging, monitoring, and alerting controls implemented to enhance the detection, response, and recovery capabilities of the ShopNimbus project. The implementation complies with NIST and CIS benchmarks for audit and event management.

## 2. Environment Setup

|  |  |
| --- | --- |
| Component | Value |
| Project ID | shopnimbus-security-group7 |
| Primary Region | us-central1 |
| Billing | Enabled |
| Enabled APIs | logging, monitoring, securitycenter, bigquery, cloudkms, cloudasset |

## 3. Implementation Steps

|  |  |  |
| --- | --- | --- |
| Step | Command | Purpose / Result |
| Enable Required APIs | gcloud services enable logging.googleapis.com monitoring.googleapis.com securitycenter.googleapis.com bigquery.googleapis.com cloudkms.googleapis.com cloudasset.googleapis.com | Activates all required GCP APIs. |
| Create BigQuery Dataset | bq --location=US mk --dataset scc\_logs | Creates dataset for centralized log exports. |
| Create Log Sink | gcloud logging sinks create scc\_findings\_sink bigquery.googleapis.com/projects/shopnimbus-security-group7/datasets/scc\_logs --log-filter='resource.type="security\_center\_source" OR logName:"cloudaudit.googleapis.com/activity"' | Exports SCC and audit logs to BigQuery. |
| Create IAM Policy Change Metric | gcloud logging metrics create iam\_policy\_changes --description='Detect IAM policy changes' --log-filter='protoPayload.methodName="SetIamPolicy"' | Tracks IAM SetIamPolicy changes for detection. |
| Create Alert Policy | gcloud alpha monitoring policies create --display-name='IAM Policy Change Alert' --condition-display-name='IAM Policy Change Detected' --condition-filter='resource.type="global" AND metric.type="logging.googleapis.com/user/iam\_policy\_changes"' --if='> 0' --duration='0s' --trigger-count=1 --combiner='OR' | Creates alert for IAM policy change events. |

## 4. Verification & Evidence Commands

|  |  |
| --- | --- |
| Verification Command | Expected Output |
| gcloud logging sinks list --format='table(name, destination, filter)' | Displays scc\_findings\_sink linked to BigQuery scc\_logs |
| bq show shopnimbus-security-group7:scc\_logs | Dataset exists; service account writer confirmed |
| gcloud logging metrics list --format='table(name, description)' | iam\_policy\_changes metric listed |
| gcloud alpha monitoring policies list --format='table(displayName, enabled)' | IAM Policy Change Alert shows True |
| gcloud asset list --project=shopnimbus-security-group7 --limit=5 | Lists BigQuery dataset, KMS keys, and project assets |

## 5. Screenshot Evidence

• Logging sink output (scc\_findings\_sink)  
• BigQuery dataset (scc\_logs)  
• IAM Policy Metric  
• Alert Policy Verification  
• Asset List Output

## 6. Compliance Mapping

- NIST PR.AC-4: Access permissions monitored.  
- NIST PR.DS-5: Data-at-rest protection via KMS.  
- NIST DE.CM-1: Continuous event monitoring.  
- CIS 8.2 / 8.6: Centralized logging and alerting.  
- PCI DSS 10.x: Logging of security events.

## 7. Notes & Lessons Learned

Alert policies require valid resource types such as 'global' for custom log metrics. IAM role changes are now detected and logged in near real-time. The project achieved end-to-end integration of Security Command Center, BigQuery, and Cloud Logging.