# Week 3 – Threat Identification and Protection Implementation Report

\*\*Project ID:\*\* shopnimbus-security-group7

\*\*Organization:\*\* ShopNimbus Cybersecurity Implementation Project

## 1. Overview

This report documents the configuration and verification steps carried out in Week 3 of the ShopNimbus Cybersecurity Project. The objective for this phase was to establish centralized threat identification and protection mechanisms through Security Command Center (SCC), Cloud Logging, BigQuery integration, and IAM-based access control. All configurations comply with CIS and NIST PR.DS / PR.AC security controls as well as PCI DSS and GDPR standards.

## 2. IAM Policy Document

The IAM policy document defines access control rules, roles, and permissions assigned to each service account tier within the ShopNimbus secure cloud architecture. These roles follow the principle of least privilege, granting only necessary access required for each system component.

|  |  |  |  |
| --- | --- | --- | --- |
| Service Account | Role | Description | Scope |
| web-sa@shopnimbus-security-group7.iam.gserviceaccount.com | roles/compute.viewer | Read-only compute engine viewer access | Web Tier |
| app-sa@shopnimbus-security-group7.iam.gserviceaccount.com | roles/cloudsql.client | SQL client connection access | Application Tier |
| database-sa@shopnimbus-security-group7.iam.gserviceaccount.com | roles/cloudkms.cryptoKeyEncrypterDecrypter | Encrypt/decrypt access through KMS | Database Tier |
| service-363546819737@gcp-sa-logging.iam.gserviceaccount.com | roles/bigquery.dataEditor | Log export and write access to scc\_logs dataset | Central Logging |
| editors@shopnimbus-security-group7 | roles/owner | Full administrative privileges | Project Level |

## 3. Service Account Configuration

Three service accounts were created for each architectural tier (Web, App, DB) using the commands below. Each was granted only the minimal role necessary to perform its assigned function.

Commands executed:  
gcloud iam service-accounts create web-sa --display-name="Web Tier Service Account"  
gcloud iam service-accounts create app-sa --display-name="App Tier Service Account"  
gcloud iam service-accounts create database-sa --display-name="Database Tier Service Account"

## 4. VPC Firewall Rules List

The VPC firewall rules restrict traffic following the defense-in-depth model from the ShopNimbus secure architecture diagram. External access is limited to HTTPS (TCP 443) for the web tier, while internal communication is restricted to approved subnets.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Rule Name | Direction | Allowed | Source Range | Target Tag | Purpose |
| allow-https-web | INGRESS | tcp:443 | 0.0.0.0/0 | web-tier | Allow HTTPS traffic to web server |
| allow-internal-db | INGRESS | tcp:3306 | 10.0.0.0/8 | db-tier | Permit internal App ↔ DB communication |
| deny-all-else | INGRESS | none | 0.0.0.0/0 | all | Default deny rule enforcing least privilege |

Command reference:  
gcloud compute firewall-rules list --format="table(name,direction,allowed,sourceRanges,targetTags)"

## 5. Consolidated Policy Documentation

This section summarizes all IAM, service account, and firewall configurations in a single, readable policy table for verification and audit tracking.

|  |  |  |
| --- | --- | --- |
| Policy Component | Configuration Command | Verification Status |
| IAM Role Assignment | gcloud projects get-iam-policy shopnimbus-security-group7 --format='table(bindings.role, bindings.members)' | Verified |
| Service Account Creation | gcloud iam service-accounts list | Active |
| Firewall Rule Setup | gcloud compute firewall-rules list | Configured |
| Logging Sink Verification | gcloud logging sinks list | Active |
| BigQuery Dataset Access | bq show shopnimbus-security-group7:scc\_logs | Accessible |

## 6. Compliance Mapping

- CIS Control 8.2: Enable and collect detailed audit logs.  
- NIST PR.DS-5: Data-at-rest is protected through KMS encryption.  
- NIST PR.AC-4: Access permissions are managed using IAM roles.  
- NIST DE.CM-1: Continuous monitoring of network and cloud activity enabled via Logging and SCC.

## 7. Proof of Implementation

Screenshots are required for submission showing verification outputs for:  
1. Asset list (gcloud asset list)  
2. Logging sink (gcloud logging sinks list)  
3. BigQuery dataset (bq show scc\_logs)  
4. IAM policy roles  
5. Firewall rules configuration