Google Cloud Security Command Center (SCC) – GSP1124

Author: Mustafa Dukureh
Date: November 9, 2025
Program: Google Security Operations Engineer Path

Introduction

This report summarizes the Google Cloud Security Command Center (SCC) lab (GSP1124), completed as part of the Google Security Operations Engineer learning path. The lab provided hands-on experience using SCC to detect, analyze, and mitigate cloud security risks within a Google Cloud environment. SCC serves as a unified risk management platform that combines cloud security posture management with security operations to enhance visibility, compliance, and response time.

Objectives

The objectives of this lab were to: - Explore the Security Command Center interface and its key features. - Configure SCC settings at the project level. - Analyze and remediate security misconfigurations and vulnerabilities. - Utilize Security Health Analytics (SHA) to enable and test modules. - Apply mute rules to filter out non-critical findings. - Investigate and resolve high-severity vulnerabilities such as open SSH and RDP ports.

Setup and Configuration

The lab environment consisted of a temporary Qwiklabs project configured with default networks and resources. Cloud Shell was activated to manage configurations, and Security Command Center was enabled to scan and report findings. Key SCC services such as Security Health Analytics, Web Security Scanner, and Event Threat Detection were available for configuration at the project level.

Key Findings and Analysis

The SCC dashboard identified multiple misconfigurations primarily associated with the default VPC network. Findings included open SSH and RDP ports accessible from any IP address, disabled VPC Flow Logs, and missing Private Google Access configurations. Each finding was assigned a severity level ranging from Low to High. High-severity findings were prioritized for remediation to strengthen network security posture.

Security Health Analytics Configuration

Within the SCC settings, the Security Health Analytics module was used to detect configuration issues across Google Cloud resources. The module 'VPC_FLOW_LOGS_SETTINGS_NOT_RECOMMENDED' was enabled to ensure that subnetworks had proper flow logging. This module continuously evaluates configurations and flags non-compliant resources. Enabling this feature improved the visibility and audit readiness of the cloud environment.

Mitigation Actions

Findings were addressed based on severity. High-severity vulnerabilities, such as open SSH and RDP ports, were resolved by restricting access to Google-managed IP ranges (35.235.240.0/20) to ensure secure Identity Aware Proxy (IAP) connections. Additional findings related to disabled flow logs and missing Private Google Access were muted for the test environment to avoid false positives during analysis.

Outcomes and Lessons Learned

By completing this lab, a deeper understanding of Google Cloud’s built-in security capabilities was achieved. The Security Command Center provided centralized visibility into cloud assets, real-time risk analysis, and proactive threat detection. Using Security Health Analytics and automated risk scoring helped prioritize fixes and streamline response efforts. The exercise also reinforced best practices in managing security posture, compliance standards, and network access control.

Conclusion

This lab successfully demonstrated how Google Cloud’s Security Command Center Enterprise can identify, prioritize, and remediate security risks across cloud environments. Through this hands-on experience, Mustafa Dukureh gained practical expertise in configuring SCC modules, analyzing vulnerabilities, and enhancing cloud security posture management. These skills align with the responsibilities of a Security Operations Engineer and are directly applicable to enterprise-level cloud security management.