Comprehensive Implementation Guide: PRJ-GCP-SEC-089

1. Project Overview

This project, **PRJ-GCP-SEC-089**, delivers a **comprehensive, cloud-native security and compliance solution** specifically tailored for Google Cloud Platform (GCP) environments. It is designed to move an organization from a fragmented, reactive security posture to a unified, proactive, and automated defense-in-depth strategy. The solution is built upon four foundational GCP security services:

1. **Security Command Center (SCC):** Serves as the central security and risk management platform, providing unified visibility into security findings, asset inventory, and compliance posture across the entire GCP organization.
2. **Chronicle SIEM (Google SecOps):** Ingests high-fidelity security data, including SCC findings, for advanced threat detection, high-speed security analytics, and threat hunting at petabyte scale, leveraging Google's global threat intelligence.
3. **VPC Service Controls (VPC SC):** Establishes a robust **data perimeter** to prevent unauthorized movement of sensitive data, mitigating the risk of data exfiltration from services like Cloud Storage, BigQuery, and Cloud SQL.
4. **Cloud Armor:** Provides a critical layer of defense at the network edge, offering Web Application Firewall (WAF) capabilities and Distributed Denial of Service (DDoS) protection for applications fronted by GCP Load Balancers.

The integration of these services ensures continuous security monitoring, automated compliance reporting, and a strong defense against both internal and external threats, making the GCP environment production-ready and compliant with stringent regulatory requirements.

2. Business Context

Implementing a robust cloud security architecture is not merely a technical requirement but a critical business imperative that delivers quantifiable value through risk mitigation, cost savings, and efficiency gains.

The Challenge of Fragmented Security

Modern GCP environments often suffer from **fragmented security monitoring and threat detection**. Security teams are forced to manually correlate alerts across disparate services, leading

to delayed response times and increased Mean Time To Detect (MTTD) and Mean Time To Respond (MTTR). This manual, reactive approach is unsustainable against sophisticated, fast-moving threats.

Quantified Business Value and ROI

The PRJ-GCP-SEC-089 solution directly addresses these challenges, providing a clear return on investment (ROI) through the following mechanisms:

Feature	Business Value	ROI/Efficiency Gain
Unified Security Posture (SCC)	Provides a single, consolidated view of all security findings, asset inventory, and compliance status across the organization.	**Efficiency Gain:** Reduces operational overhead by an estimated **30-40%** by eliminating context switching and manual data correlation across multiple security tools.
Advanced Threat Intelligence (Chronicle)	Enables the detection of advanced, zero-day threats and sophisticated attack campaigns using Google's global threat intelligence and high-speed analytics.	**Risk Mitigation:** Reduces the probability of a catastrophic data breach, which can cost millions. Proactive detection reduces MTTR, saving an estimated $100k-$**500k** per major incident in response costs.
Automated Compliance Reporting	Continuous assessment and reporting against industry benchmarks (e.g., CIS) and regulatory standards.	**Cost Savings:** Cuts down on manual audit preparation time by **50-70%**, freeing up compliance and security personnel for higher-value tasks.
Data Exfiltration Prevention (VPC SC)	Establishes a security boundary around sensitive services, preventing unauthorized data movement.	**Risk Mitigation:** Protects against insider threats and compromised credentials, directly mitigating the most severe financial and reputational risks associated with data loss.
Cost Effective Cloud-Native Tools	Utilizes GCP-native security services, minimizing the need for expensive, third-party security tools and their associated integration costs.	**Cost Savings:** Optimizes cloud security spending by leveraging existing platform capabilities, resulting in a lower Total Cost of Ownership (TCO) for the security stack.

Risk Mitigation Focus

The implemented controls are specifically designed to mitigate critical cloud security risks:

- **Threat Detection and Response:** Automated detection and response to security incidents and active threats through the SCC-to-Chronicle pipeline.
- **Misconfigurations:** Continuous scanning for and remediation of security misconfigurations in GCP resources, which are a leading cause of cloud breaches.
- **Unauthorized Access:** Enforcement of least-privilege access and strong authentication mechanisms, coupled with the VPC SC perimeter to enforce access boundaries.

- **Data Exfiltration:** VPC Service Controls establish a non-bypassable data perimeter to prevent unauthorized movement of sensitive data to external projects or public internet destinations.
- **Compliance Violations:** Proactive identification and reporting of compliance gaps against defined frameworks, ensuring continuous adherence to regulatory mandates.

3. GRC Mapping

This solution is engineered to align with key Governance, Risk, and Compliance (GRC) requirements, ensuring a strong, auditable, and defensible security foundation. The architecture directly supports multiple international and industry-specific compliance frameworks.

Compliance Frameworks and Control Mapping

Framework	Alignment Focus	Control Implementation
Google Cloud Security Foundations	Adherence to Google's security blueprint and best practices for cloud architecture.	SCC provides continuous assessment against the Google Cloud Security Health Check.
NIST Cybersecurity Framework (CSF)	Supports all five core functions of the framework.	**Identify** (SCC Asset Inventory), **Protect** (VPC SC, Cloud Armor), **Detect** (SCC, Chronicle SIEM), **Respond** (Chronicle SOAR capabilities), and **Recover**.
ISO/IEC 27001:2022	Information Security Management System (ISMS) controls.	Specifically addresses controls like **A.8.23** (Vulnerability management via SCC Vulnerability Manager) and **A.5.24** (Incident management via Chronicle SIEM/SOAR).
CIS Google Cloud Platform Foundation Benchmark	Continuous assessment and reporting against security configuration best practices.	SCC's Compliance dashboard provides automated, continuous assessment against the CIS benchmark, reporting on deviations and providing remediation steps.
SOC 2 (Service Organization Control 2)	Trust Services Criteria (Security, Availability, Processing Integrity, Confidentiality, Privacy).	**CC7.2** (System monitoring) and **CC7.3** (Security events) are directly supported by the SCC-Chronicle SIEM integration, providing real-time, centralized logging and monitoring.

Regulatory Alignment

The technical controls implemented by this project directly address requirements from major global regulations:

Regulation	Relevant Section	Control Implementation
GDPR (General Data Protection Regulation)	Article 32 (Security measures), Article 33 (Breach notification)	**VPC Service Controls** ensure data locality and prevent unauthorized data transfers (Article 32). **Chronicle SIEM** provides the necessary incident detection and logging for timely breach notification (Article 33).
HIPAA (Health Insurance Portability and Accountability Act)	§ 164.308(a)(1) (Security management), § 164.312(b) (Audit controls)	**Comprehensive logging and monitoring** via Chronicle SIEM and **strong access controls** enforced by VPC SC and IAM ensure the confidentiality, integrity, and availability of Protected Health Information (PHI).
PCI DSS (Payment Card Industry Data Security Standard)	Requirement 10 (Monitoring), Requirement 11 (Testing)	**Continuous monitoring** (SCC/Chronicle) and **vulnerability scanning** (SCC) ensure the security of the Cardholder Data Environment (CDE). **Cloud Armor** helps meet WAF requirements.

Audit Evidence Generation

The integrated system automatically generates the following artifacts, which serve as crucial evidence during internal and external audits:

- **Security Findings and Vulnerability Reports:** Detailed, exportable reports from SCC, including asset-level findings and vulnerability scan results.
- **Threat Detection Alerts and Incidents:** Comprehensive incident timelines and alert details managed within Chronicle SIEM, demonstrating effective threat response.
- **Compliance Posture Assessments:** Snapshot and continuous reports generated by SCC's Compliance dashboard against frameworks like CIS and NIST.
- **Security Event Logs:** High-fidelity, long-term security event logs ingested and retained in Chronicle SIEM, providing an immutable audit trail.

4. Prerequisites

Before beginning the deployment, ensure the following accounts, tools, permissions, and setup steps are completed.

Accounts and Permissions

1. **GCP Project:** A dedicated GCP project (e.g., `prj-sec-089`) must be created to host the security components and configurations.
2. **Organization/Folder Level Access:** To enable the full capabilities of SCC Premium Tier, the deploying user must have the `securitycenter.admin` role at the **Organization** or **Folder** level.

3. **Project-Level Permissions:** The deploying user must have the following IAM roles on the target project:
    - `roles/owner` or `roles/editor` (for initial setup).
    - `roles/serviceusage.serviceUsageAdmin` (to enable APIs).
    - `roles/pubsub.admin` (to create topics and manage IAM).
    - `roles/accesscontextmanager.policyAdmin` (to manage VPC Service Controls).
    - `roles/compute.securityAdmin` (to manage Cloud Armor policies).

Required Tools

1. **Google Cloud SDK (`gcloud` CLI):** The command-line interface must be installed, configured, and authenticated.

```
# Install gcloud CLI (if not already installed)
# Follow official Google Cloud documentation for installation.

# Authenticate and set application default credentials
gcloud auth login
gcloud auth application-default login

# Set the target project ID for all subsequent commands
export PROJECT_ID="PRJ-GCP-SEC-089"
gcloud config set project $PROJECT_ID
```

Enabled APIs

The following GCP APIs must be enabled in the target project to support the deployment:

- `securitycenter.googleapis.com` (Security Command Center)
- `cloudasset.googleapis.com` (Cloud Asset Inventory)
- `pubsub.googleapis.com` (Pub/Sub for data export)
- `compute.googleapis.com` (Compute Engine, required for VPC Service Controls and Cloud Armor)
- `accesscontextmanager.googleapis.com` (Access Context Manager, required for VPC Service Controls)

5. Architecture Overview

The solution employs a **hub-and-spoke security model** where the security components are centrally managed and deployed to protect distributed workloads.

Central Security Hub (SCC & Chronicle):

- **Security Command Center (SCC):** Acts as the central **security findings aggregator**. It continuously scans all connected GCP resources for vulnerabilities, misconfigurations, and threats.
- **Continuous Export Pipeline:** SCC findings are immediately exported via a **Pub/Sub topic** to ensure real-time data transfer.
- **Chronicle SIEM:** Ingests the Pub/Sub stream, providing the **long-term retention, advanced correlation, and threat hunting** capabilities that SCC does not offer natively. This separation of concerns allows SCC to focus on detection and Chronicle to focus on analysis and response.

Defense-in-Depth Layers (VPC SC & Cloud Armor):

- **VPC Service Controls (VPC SC):** This is the **data perimeter layer**. It creates a logical security boundary around sensitive services (e.g., GCS, BigQuery) within the project, preventing any unauthorized access or data exfiltration attempts, even from compromised credentials.
- **Cloud Armor:** This is the **network edge protection layer**. It sits in front of public-facing applications (via Load Balancers) to filter malicious traffic, providing WAF rules (e.g., SQLi, XSS protection) and L3/L4 DDoS mitigation.

This layered approach ensures that security is enforced at multiple points: the asset level (SCC), the data access level (VPC SC), the network edge (Cloud Armor), and the analysis/response level (Chronicle SIEM).

6. Step-by-Step Implementation

The following steps provide detailed, actionable instructions for deploying the core components of the PRJ-GCP-SEC-089 solution.

Step 6.1: Enable Security Command Center (SCC)

SCC must be enabled at the appropriate level (Organization or Project) to begin asset inventory and finding generation.

1. **Set Project Context and Enable API:**

```
# Set the target project ID (Ensure this is done in the Prerequisites step)
export PROJECT_ID="PRJ-GCP-SEC-089"
gcloud config set project $PROJECT_ID

# Enable the Security Command Center API
gcloud services enable securitycenter.googleapis.com
```

2. **Activate SCC at the Project Level (Standard Tier):** For the Standard Tier, activation is done at the project level. This is sufficient for basic asset inventory and vulnerability scanning.

```
gcloud scc settings set-project-service-account $PROJECT_ID
```

Note on Premium Tier: For full features (e.g., Event Threat Detection, Container Threat Detection), SCC Premium must be enabled at the **Organization** or **Folder** level, typically via the GCP Console, as it requires higher-level permissions.

Step 6.2: Configure Continuous Export to Chronicle SIEM

This step sets up the real-time data pipeline from SCC to Chronicle SIEM using a Pub/Sub topic.

1. **Define Variables and Create Pub/Sub Topic:**

```
# Define variables for the export
export PUBSUB_TOPIC="scc-findings-export"
# Example filter: Export only ACTIVE findings with HIGH or CRITICAL severity
export EXPORT_FILTER="state=\"ACTIVE\" AND (severity=\"HIGH\" OR
severity=\"CRITICAL\")"

# Create a Pub/Sub topic for SCC findings
gcloud pubsub topics create $PUBSUB_TOPIC
```

2. **Grant Publish Permissions to SCC Service Account:** The SCC service account needs permission to publish findings to the newly created topic.

```
# Get the SCC service account for the organization/project
# Note: The format of the service account depends on whether SCC is enabled at Org
or Project level.
export SCC_SA=$(gcloud scc settings describe --format="value(serviceAccount)")

# Grant the SCC service account permission to publish to the topic
gcloud pubsub topics add-iam-policy-binding $PUBSUB_TOPIC \
    --member="serviceAccount:$SCC_SA" \
    --role="roles/pubsub.publisher"
```

3. **Create the Continuous Export Configuration:** This command creates the actual export rule within SCC. **Replace `YOUR_ORGANIZATION_ID` with your actual organization ID.**

```
gcloud scc settings create-export $PUBSUB_TOPIC \
    --organization=YOUR_ORGANIZATION_ID \
    --description="Export High/Critical Findings to Chronicle" \
    --filter=$EXPORT_FILTER \
    --pubsub-topic="projects/$PROJECT_ID/topics/$PUBSUB_TOPIC"
```

4. **Chronicle SIEM Ingestion Configuration (Conceptual):** The final step is external to the `gcloud` CLI and must be performed in the Chronicle SIEM console:
    - Navigate to the **Chronicle Settings** or **Data Ingestion** section.
    - Create a new **GCP Pub/Sub feed**.
    - Specify the full topic path: `projects/PRJ-GCP-SEC-089/topics/scc-findings-export`.
    - Chronicle will automatically begin ingesting and parsing the SCC findings for analysis.

Step 6.3: Implement VPC Service Controls Perimeter

This step creates a security perimeter to protect sensitive data services.

1. **Define Variables and Get Policy ID:**

```
# Define variables
export PERIMETER_NAME="prj_sec_089_perimeter"
# Get the Access Context Manager Policy ID (usually a number)
export POLICY_ID=$(gcloud access-context-manager policies list --
format="value(name)")
```

2. **Create the Service Perimeter:** This example creates a perimeter protecting Cloud Storage and BigQuery, restricting access to resources within the `PRJ-GCP-SEC-089` project.

```
gcloud access-context-manager perimeters create $PERIMETER_NAME \
    --policy=$POLICY_ID \
    --perimeter-type=regular \
    --resources="projects/$PROJECT_ID" \
    --restricted-
services="storage.googleapis.com,bigquery.googleapis.com,cloudsql.googleapis.com" \
    --title="Security Perimeter for PRJ-GCP-SEC-089"
```

3. **Configure Access Levels (Optional but Recommended):** To allow legitimate access from outside the perimeter (e.g., corporate network, CI/CD pipelines), you must define and add Access Levels.

```
# Example: Adding an existing Access Level named 'corp_network_access'
# gcloud access-context-manager perimeters update $PERIMETER_NAME \
#     --add-access-levels="corp_network_access"
```

Step 6.4: Configure Cloud Armor Policy

This step deploys a Web Application Firewall (WAF) policy to protect a public-facing application.

1. **Define Variables:**

```
export ARMOR_POLICY_NAME="web-app-waf-policy"
export BACKEND_SERVICE_NAME="web-app-backend" # Replace with your actual backend service name
```

2. **Create the Cloud Armor Security Policy:**

```
gcloud compute security-policies create $ARMOR_POLICY_NAME \
    --description="WAF and DDoS protection for web application"
```

3. **Add WAF Rules (Example: SQL Injection Protection):** Cloud Armor uses preconfigured WAF rules (WAF Expression Sets).

```
gcloud compute security-policies rules create 1000 \
    --security-policy $ARMOR_POLICY_NAME \
    --expression "evaluatePreconfiguredExpr('sqli-canary')" \
    --action "deny-403" \
    --description "Block SQL Injection attempts" \
    --priority 1000

# Add a rule for XSS protection
gcloud compute security-policies rules create 1001 \
    --security-policy $ARMOR_POLICY_NAME \
    --expression "evaluatePreconfiguredExpr('xss-canary')" \
    --action "deny-403" \
    --description "Block Cross-Site Scripting attempts" \
    --priority 1001
```

4. **Attach the Policy to a Backend Service:** The policy must be attached to the target backend service (e.g., a Load Balancer's backend).

```
# gcloud compute backend-services update $BACKEND_SERVICE_NAME \
#     --security-policy $ARMOR_POLICY_NAME
```

7. Validation & Testing

A rigorous validation process is essential to confirm that all security controls are correctly deployed and functioning as intended.

7.1. SCC and Chronicle Pipeline Validation

Test Case	Action	Expected Result
SCC Activation	Navigate to the SCC dashboard in the GCP Console.	Assets from the project should be inventoried, and initial findings (e.g., misconfigurations) should be visible.
Continuous Export Test	Manually create a high-severity misconfiguration (e.g., create a GCS bucket with public access).	A new message should appear in the `scc-findings-export` Pub/Sub topic within minutes.
Chronicle Ingestion	Check the Chronicle SIEM console (Raw Log view or UDM Search) for the ingested SCC finding.	The finding should be present, parsed into the Unified Data Model (UDM), and correlated with other events.

7.2. VPC Service Controls Validation

The primary test for VPC SC is to confirm that the data perimeter successfully blocks unauthorized access.

Test Case	Action	Expected Result
Data Exfiltration Block	From a VM **outside** the perimeter (e.g., a different project or local machine without the correct Access Level), attempt to copy data from a protected GCS bucket in `PRJ-GCP-SEC-089`.	The operation should be blocked with a `403 Policy Violation` error message.
Internal Access Allowed	From a VM **inside** the perimeter, attempt to copy data from the same protected GCS bucket.	The operation should succeed, confirming that authorized access within the perimeter is maintained.

7.3. Cloud Armor Validation

This test confirms the WAF rules are actively protecting the application.

Test Case	Action	Expected Result
SQL Injection Block	Attempt to access the protected application URL with a known malicious payload in a query parameter (e.g., `?id=1' OR '1'='1`).	The request should be denied with a **403 Forbidden** response, and the Cloud Armor logs should show a rule match for `sqli-canary`.
XSS Block	Attempt to access the protected application URL with a known XSS payload (e.g., `?q=<script>alert(1)</script>`).	The request should be denied with a **403 Forbidden** response, and the Cloud Armor logs should show a rule match for `xss-canary`.

8. Troubleshooting

Common issues encountered during the deployment and their resolutions.

Issue	Potential Cause	Resolution
SCC Findings Not Exporting	1. Incorrect Pub/Sub IAM permissions. 2. Incorrect export filter. 3. SCC not fully activated.	1. Verify the SCC service account (`SCC_SA`) has the `roles/pubsub.publisher` role on the topic. 2. Check the `EXPORT_FILTER` syntax for errors. 3. Ensure SCC is fully enabled at the correct level (Org/Folder/Project).
VPC SC Blocking Legitimate Traffic	1. The Access Level is too restrictive or missing. 2. A required service is missing from the perimeter's `allowed-services` list.	1. Review the VPC SC dry-run logs to identify the blocked request. Adjust the Access Level to include the source IP/identity. 2. Add the necessary service (e.g., `cloudbuild.googleapis.com`) to the perimeter's `allowed-services` .
Cloud Armor Policy Not Applied	The policy is not correctly attached to the Load Balancer's backend service.	Verify the `gcloud compute backend-services update` command was executed successfully and the `security-policy` field on the backend service is set to `web-app-waf-policy` .
Chronicle Ingestion Failure	The Pub/Sub feed in Chronicle is misconfigured or the topic path is incorrect.	Double-check the full topic path (`projects/PROJECT_ID/topics/TOPIC_NAME`) in the Chronicle SIEM console feed configuration. Ensure the Chronicle service account has `roles/pubsub.subscriber` on the topic.
`gcloud` Command Permission Denied	The authenticated user lacks the necessary IAM roles for the specific resource (e.g., `roles/accesscontextmanager.policyAdmin`).	Verify the user's IAM roles against the Prerequisites section. Use `gcloud auth list` and `gcloud config get-value project` to confirm the correct identity and project are active.

9. Cost Optimization

Optimizing costs while maintaining a strong security posture is crucial. The following tips focus on reducing the operational expenses of the deployed services.

- **SCC Tier Selection:**
  - **Action:** Start with the **Standard Tier** for basic asset inventory and security health checks.
  - **Benefit:** Only upgrade to **Premium Tier** for advanced services like Event Threat Detection and Vulnerability Manager when the business need justifies the higher cost. Carefully evaluate which assets require Premium protection.

- **Chronicle Data Ingestion Filtering:**
  - **Action:** Use a highly restrictive `EXPORT_FILTER` for the SCC Continuous Export (as demonstrated in Step 6.2) to send only high-value, actionable findings (e.g., `CRITICAL` and `HIGH` severity) to Chronicle.
  - **Benefit:** Reduces the volume of data ingested by Chronicle, directly impacting ingestion costs, which are often volume-based. Avoid sending low-severity, informational findings that can be reviewed in SCC directly.
- **VPC Service Controls Dry-Run Mode:**
  - **Action:** Utilize the VPC SC **dry-run mode** extensively before enforcing the perimeter.
  - **Benefit:** Prevents unexpected service disruptions and costly downtime by identifying all policy violations *before* they impact production traffic, saving significant operational cost.
- **Resource Sizing for Custom Tools:**
  - **Action:** Ensure that any underlying Compute Engine resources used for custom security tooling or response functions are appropriately sized (e.g., using E2 or N2 machines) and utilize **Committed Use Discounts (CUDs)** where possible for predictable workloads.
- **Cloud Armor Policy Granularity:**
  - **Action:** Consolidate multiple, similar rules into a single, more complex rule using logical operators where possible.
  - **Benefit:** While Cloud Armor is generally cost-effective, optimizing rule count and complexity can slightly reduce processing overhead and simplify management.

10. Security Best Practices

Beyond the core deployment, maintaining a robust security posture requires continuous adherence to best practices and operational discipline.

1. **Principle of Least Privilege (PoLP) Enforcement:**
   - **Practice:** Ensure the SCC service account, the Chronicle service account, and all human operators have only the minimum required IAM roles to perform their functions. For example, the SCC service account only needs `roles/pubsub.publisher` on the export topic, not `roles/pubsub.admin`.
   - **Action:** Regularly audit IAM bindings using the **IAM Recommender** to identify and remove overly permissive roles.
2. **Software Supply Chain Security with Binary Authorization:**
   - **Practice:** For containerized workloads (e.g., GKE, Cloud Run), enforce **Binary Authorization**.
   - **Action:** Configure attestors and policies to ensure that only signed, trusted container images that have passed vulnerability scanning and quality gates are allowed to be

deployed to production environments, mitigating supply chain risks like the use of compromised base images.

3. **Regular Review and Alert Tuning:**
    - **Practice:** Security is not a "set-it-and-forget-it" task. The effectiveness of the SCC-Chronicle pipeline depends on the quality of the alerts.
    - **Action:** Schedule **monthly reviews** of SCC findings and Chronicle alerts. Tune the SCC export filter and Chronicle detection rules to reduce false positives and ensure that high-fidelity, actionable alerts are prioritized.
4. **Use Organization Policy Constraints for Global Enforcement:**
    - **Practice:** Enforce security best practices globally across all projects using **Organization Policies**.
    - **Action:** Implement constraints such as `constraints/compute.disableGuestAttributesAccess` (to prevent metadata theft) or `constraints/compute.vmExternalIpAccess` (to disable public IP addresses on VMs) to enforce a baseline security standard that complements the project-specific controls deployed here.
5. **Data Access Logging and Monitoring:**
    - **Practice:** Ensure that **Data Access Logs** (Admin Read, Data Read, Data Write) are enabled for all sensitive services (e.g., BigQuery, Cloud Storage) and are being ingested into Chronicle SIEM.
    - **Action:** This provides the necessary audit trail to detect and investigate data exfiltration attempts that may be blocked by VPC SC, allowing for a full post-incident analysis.

Cleanup

To fully dismantle the deployed security components and avoid future charges, execute the following commands in reverse order of deployment.

```
# 1. Delete Cloud Armor Policy
gcloud compute security-policies delete $ARMOR_POLICY_NAME --quiet

# 2. Delete VPC Service Controls Perimeter
# Note: Ensure you use the correct POLICY_ID from the deployment step
gcloud access-context-manager perimeters delete $PERIMETER_NAME --policy=$POLICY_ID --
quiet

# 3. Delete SCC Continuous Export
# Note: You need the export ID, which is the Pub/Sub topic name in this case
# Replace YOUR_ORGANIZATION_ID with your actual organization ID
gcloud scc settings delete-export $PUBSUB_TOPIC --organization=YOUR_ORGANIZATION_ID --
quiet

# 4. Delete Pub/Sub Topic
gcloud pubsub topics delete $PUBSUB_TOPIC --quiet

# 5. Deactivate SCC (Optional - if no longer needed in the project)
# gcloud services disable securitycenter.googleapis.com
```

Project Name: `prj-gcp-sec-089` **Author:** Manus AI **Date:** January 26, 2026