

Professional Security Operations Engineer

Certification exam guide

A Google Cloud Certified Professional Security Operations Engineer detects, monitors, analyzes, investigates, and responds to security threats against workloads, endpoints, identities, and infrastructure. This individual uses Google Cloud capabilities to protect an enterprise environment and is proficient in writing detection rules, log prioritization and ingestion, orchestration, and response automation. Further, this individual has experience leveraging posture, threat intelligence, and artificial intelligence (AI) for detection and response.

Recommended experience: 3+ years of security industry experience including 1+ years using Google Cloud security tooling

This exam assesses your knowledge of performing tasks in Google Security Operations (SecOps), Security Command Center (SCC), and Google Threat Intelligence (GTI). For more information on these platforms, please refer to the [Google SecOps documentation](#), [SCC documentation](#), and [GTI documentation](#).

Section 1: Platform operations (~12% of the exam)

1.1 Enhancing detection and response. Considerations include:

- Prioritizing telemetry sources (e.g., Security Command Center [SCC], Google Threat Intelligence [GTI], Cloud Logging, and Chrome Enterprise) to detect incidents or misconfigurations within an enterprise environment
- Integrating and maintaining prebuilt security tools from Google SecOps Content Hub in the security architecture to enhance detection and response capabilities
- Justifying the operational use of tools with complementary capabilities (e.g., Cloud Logging, SCC built-in detectors, and Google SecOps rules) based on detection coverage requirements
- Evaluating the effectiveness of existing tools to identify gaps in coverage and mitigate potential threats
- Enhancing existing detection and response processes using AI, automation, and cloud-based tools

- Conducting searches in the platform (e.g., Unified Data Model [UDM] and stats searches)
- Evaluating the effectiveness of surfaced Indicators of Compromise (IOCs) and tactics, techniques, and procedures (TTPs) (e.g., GTI and Google SecOps)
- Integrating GTI IOCs and TTPs appropriate for the specific use case

1.2 Configuring access for human and non-human identities. Considerations include:

- Configuring authentication to Google Cloud security tools (e.g., SCC, Google SecOps, and Model Context Protocol [MCP])
- Configuring authorization for feature access using Identity and Access Management (IAM) roles and permissions
- Configuring authorization for data access using IAM roles and conditions
- Configuring and analyzing audit logs (e.g., Cloud Audit Logs and data access logs) for the solution
- Configuring API access for automations within Google Cloud security tools (e.g., service accounts, API keys, SCC, Google SecOps, GTI, and MCP)
- Provisioning identities using Workforce Identity Federation

Section 2: Data management (~18% of the exam)

2.1 Ingesting logs for security tooling. Considerations include:

- Architecting and configuring data ingestion pipelines from security tools (e.g., configuring Bindplane to collect Microsoft Windows Event logs and route them to Google SecOps or configuring direct ingestion of SCC findings into Google SecOps)
- Assessing required logs for detection and response, including automated sources, within Google Cloud security tools (e.g., SCC Event Threat Detection [ETD], Google SecOps)
- Evaluating parsers for data ingestion in Google SecOps
- Configuring parser modifications or extensions in Google SecOps
- Evaluating data normalization techniques from log sources in Google SecOps
- Evaluating new labels for data ingestion
- Managing log and ingestion costs

2.2 Implementing a baseline of user, asset, and entity context. Considerations include:

- Identifying relevant threat intelligence information in the enterprise environment
- Differentiating event and entity data log sources (e.g., Cloud Audit Logs and identity provider telemetry)
- Evaluating event and entity data matches for enrichment by using aliasing fields

- Ingesting GTI or third-party IOCs into the Entity Context Graph
- Configuring and using GTI capabilities (e.g., threat hunting, LiveHunt, Digital Threat Monitoring [DTM], Google Insights, and URL Scanning)
- Configuring GTI capabilities (e.g., threat hunting, LiveHunt, and Digital Threat Monitoring [DTM])

Section 3: Threat hunting (~18% of the exam)

3.1 Performing threat hunting across environments. Considerations include:

- Developing queries to search across environment logs to identify anomalous activity
- Analyzing user behavior to identify anomalous activity (e.g., stats queries)
- Investigating the network, endpoints, and services to identify threat patterns or IOCs using Google Cloud tools (e.g., Logs Explorer, BigQuery, and Google SecOps)
- Collaborating with the incident response team to identify active threats in the environment
- Developing hypotheses based on behavior, threat intelligence, attack path exposures, and incident data (e.g., SCC, Google SecOps, and GTI)
- Prompting AI using natural language to conduct threat hunting
- Evaluating the use cases for searching within the SCC security graph or the Google SecOps Entity Context Graph (e.g., enumeration of assets, sensitive data classifications, and known resource vulnerabilities)

3.2 Leveraging threat intelligence for threat hunting. Considerations include:

- Searching for IOCs within historical logs
- Identifying new attack patterns and techniques in real time using threat intelligence and risk assessments (e.g., GTI, detection rules, and SCC toxic combinations)
- Analyzing entity risk score to identify anomalous behavior
- Comparing and performing a retrohunt of historical event data with newly enriched logs (e.g., Google SecOps rules engine, BigQuery, and Cloud Logging)
- Searching proactively for underlying threats using threat intelligence (e.g., GTI and detection rules)
- Analyzing the results of the Triage and Investigation Agent

Section 4: Detection engineering (~21% of the exam)

4.1 Developing and implementing mechanisms to detect risks and identify threats.

Considerations include:

- Reconciling threat intelligence with user and asset activity
- Analyzing logs and events to identify anomalous activity
- Assessing suspicious behavior patterns by using detection rules and searches across various timelines
- Designing detection rules that use risk values (e.g., Google SecOps data tables) to identify threats matching risk profiles
- Discovering anomalous behavior of assets or users, and assigning risk values to the detections (e.g., Google SecOps Risk Analytics and curated detection rules)
- Designing detection rules to discover posture, AI infrastructure risks, or risk profile changes within the environment (e.g., Compliance Manager and Google SecOps)
- Configuring SCC tooling (e.g., Web Security Scanner) to send run-time vulnerabilities to Google SecOps
- Identifying new or low-prevalence processes, domains, and IP addresses that do not appear in threat intelligence sources using various methods (e.g., writing YARA-L rules and dashboards)
- Assessing how to use entity and context data (e.g., Cloud Asset Inventory and threat intelligence) within detection rules to improve their accuracy and dynamic risk scoring
- Configuring SCC threat detectors (e.g., ETD, Cloud Run Threat Detection, Container Threat Detection, and Virtual Machine Threat Detection)
- Analyzing detection coverage based on MITRE ATT&CK
- Writing composite detections (e.g., discovering activity correlations over longer time periods)
- Prompting AI using natural language to create detection rules

4.2 Leveraging threat intelligence for detection. Considerations include:

- Scoring alerts based on the risk level of IOCs
- Using the latest IOCs to search within ingested security telemetry
- Measuring the frequency of repetitive alerts to identify and reduce false positives
- Configuring detection rules based on GTI TTPs and IOCs as applicable for the use case
- Using Applied Threat Intelligence (ATI) to understand threat exposure (e.g., Emerging Threats Center and curated detections)

Section 5: Incident response (~21% of the exam)

5.1 Containing and investigating security incidents. Considerations include:

- Collecting evidence on the scope of the incident, including forensic images and artifacts
- Observing and analyzing alerts related to the incident using Google Cloud security tooling (e.g., SCC and Google SecOps)
- Analyzing the scope and severity of the incident using Google Cloud security tooling, environment posture, and vulnerability context (e.g., Cloud Logging, Google SecOps, Compliance Manager, and Vulnerability Assessment for Google Cloud)
- Collaborating with other engineering teams for detection and long-term remediation efforts
- Isolating affected services and processes to prevent further damage and spread of attack
- Analyzing identified artifacts based on forensic analysis (e.g., hashes, IP addresses, URLs, binaries, and GTI)
- Performing root cause analysis using Google Cloud security tools (e.g., SCC and Google SecOps security information and event management [SIEM])
- Responding to the alerts produced by GTI (e.g., DTM)
- Using AI capabilities for investigation (e.g., Triage and Investigation Agent and the Gemini Summary widget in Google SecOps Security Orchestration, Automation, and Response [SOAR])

5.2 Building, implementing, and using response playbooks. Considerations include:

- Determining the appropriate response steps for automation
- Prioritizing high-value enrichments based on threat profiles
- Evaluating appropriate integrations to be leveraged by playbooks
- Designing new processes in response to newly identified attack patterns from recent incidents
- Recommending new orchestrations and automation playbooks based on gaps in the current implementation
- Implementing playbook mechanisms to update relevant findings in other systems (e.g., SCC)
- Implementing playbook mechanisms to notify analysts and stakeholders of incidents
- Implementing playbooks to invoke the Triage and Investigation Agent
- Creating custom transformers and logical operators

- 5.3 Implementing the case management lifecycle. Considerations include:
- Capturing relevant metrics throughout the entire case lifecycle (e.g., tagging, Service Level Agreements [SLAs], stages, and closure reasons)
 - Implementing efficient workflows for case escalation

Section 6: Observability (~12% of the exam)

- 6.1 Developing and maintaining dashboards to provide insights. Considerations include:
- Identifying key security analytics (e.g., metrics, key performance indicators [KPIs], and trends)
 - Implementing dashboards to visualize security telemetry, ingestion metrics, detections, alerts, and IOCs (e.g., Google SecOps SOAR and Google SecOps SIEM)
 - Generating reports (e.g., Google SecOps SOAR, Google SecOps SIEM, GTI, and SCC)
- 6.2 Configuring health monitoring and alerting. Considerations include:
- Identifying important metrics for health monitoring and alerts
 - Creating dashboards that centralize metrics
 - Creating alerts with thresholds for specific metrics
 - Configuring notifications using Google Cloud tools (e.g., Cloud Monitoring)
 - Identifying health issues using Google Cloud tools (e.g., Cloud Logging, Gemini Cloud Assist)
 - Configuring silent source detection