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, and infrastructure. This individual uses Google Cloud resources 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 and threat intelligence for detection and response.

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

Section 1: Platform operations (~14% of the exam)

1.1 Enhancing detection and response. Considerations include:

- Prioritizing telemetry sources (e.g., Security Command Center [SCC], Google Security Operations [SecOps], GTI, Cloud IDS) to detect incidents or misconfigurations within an enterprise environment
- Integrating multiple tools (e.g., SCC, Google SecOps, GTI, Cloud IDS, downstream third-party system) in the security architecture to enhance detection capabilities
- Justifying the use of tools with overlapping capabilities based on a set of requirements
- Evaluating the effectiveness of existing tools to identify gaps in coverage and mitigate potential threats
- Evaluating automation and cloud-based tools to enhance existing detection and response processes

1.2 Configuring access. Considerations include:

- Configuring user and service account authentication to security tools (e.g., SCC, Google SecOps)
- Configuring user and service account authorization for feature access using IAM roles and permissions

- Configuring user and service account authorization for data access using IAM roles and permissions
- Configuring and analyzing audit logs (e.g., Cloud Audit Logs, data access logs) for the solution
- Configuring API access for automations within security tools (e.g., service accounts, API keys, SCC, Google SecOps, GTI)
- Provisioning identities using Workforce Identity Federation

Section 2: Data management (~14% of the exam)

2.1 Ingesting logs for security tooling. Considerations include:

- Determining approaches for data ingestion within security tools (e.g., SCC, Google SecOps)
- Configuring an ingestion tool or features within security tools (e.g., SCC, Google SecOps)
- Assessing required logs for detection and response, including automated sources, within security tools (e.g., SCC Event Threat Detection, 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 Identifying 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, Active Directory organizational context)
- Evaluating event and entity data matches for enrichment by using aliasing fields

Section 3: Threat hunting (~19% 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
- Investigating the network, endpoints, and services to identify threat patterns or indicators of compromise (IOCs) using Google Cloud tools (e.g., Logs Explorer, Log Analytics, BigQuery, Google SecOps)

- Collaborating with the incident response team to identify active threats in the environment
- Developing hypotheses based on behavior, threat intel, posture, and incident data (e.g., SCC, GTI)

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, SCC toxic combinations)
- Analyzing entity risk score to identify anomalous behavior
- Comparing and performing retrohunt of historical event data with newly enriched logs (e.g., Google SecOps rules engine, BigQuery, Cloud Logging)
- Searching proactively for underlying threats using threat intelligence (e.g., GTI, detection rules)

Section 4: Detection engineering (~22% 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 reference lists) 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, curated detection rules)
- Designing detection rules to discover posture or risk profile changes within the environment (e.g., SCC Security Health Analytics [SHA], SCC posture management, 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, dashboards)
- Assessing how to use entity/context data within detection rules to improve their accuracy (e.g., Google SecOps entity graph)
- Configuring SCC Event Threat Detection custom detectors for IOCs

4.2 Leveraging threat intelligence for detection. Considerations include:

- Scoring alerts based on the risk level of IOCs
- Using latest IOCs to search within ingested security telemetry
- Measuring the frequency of repetitive alerts to identify and reduce false positives

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 security tooling (e.g., SCC, Google SecOps)
- Analyzing the scope of the incident using security tooling (e.g., Logs Explorer, Log Analytics, BigQuery, Cloud Logging, Cloud Monitoring)
- 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., Hash, IP, URL, Binaries) (GTI)
- Performing root cause analysis using security tools (e.g., SCC, Google SecOps SIEM)

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 (e.g., Google SecOps SOAR)
- Implementing mechanisms to notify analysts and stakeholders of incidents

5.3 Implementing the case management lifecycle. Considerations include:

- Assigning cases into appropriate response stages
- Implementing efficient workflows for case escalation
- Assessing the effectiveness of case handoffs

Section 6: Observability (~10% of the exam)

6.1 Developing and maintaining dashboards and reports to provide insights. Considerations include:

- Identifying key security analytics (e.g., metrics, KPIs, trends)
- Implementing dashboards to visualize security telemetry, ingestion metrics, detections, alerts, and IOCs (e.g., Google SecOps SOAR, SIEM, Looker Studio)
- Generating and customizing reports (e.g., Google SecOps SOAR, SIEM)

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)
- Configuring silent source detection