ExamsIndex
Practice Materials & Tests

DEMO VERSION

Google

Security-Operations-Engineer Exam

Google Cloud Certified - Professional Security Operations Engineer (PSOE) Exam

Exam Latest Version: 6.0

Question 1. (Single Select)

You need to augment your organization's existing Security Command Center (SCC) implementation with additional detectors. You have a list of known IoCs and would like to include external signals for this capability to ensure broad detection coverage. What should you do?

A: Create a custom posture for your organization that combines the prebuilt Event Threat Detection and Security Health Analytics (SHA) detectors.
B: Create a Security Health Analytics (SHA) custom module using the compute address resource.
C: Create an Event Threat Detection custom module using the "Configurable Bad IP" template.
D: Create a custom log sink with internal and external IP addresses from threat intelligence. Use the SCC API to generate a finding for each event.

Correct Answer: C

Explanation:

Comprehensive and Detailed 150 to 250 words of Explanation From Exact Extract Google Security Operations Engineer documents:

The correct solution is to create an Event Threat Detection (ETD) custom module. ETD is the Security Command Center (SCC) service designed to analyze logs for active threats, anomalies, and malicious behavior. The user's requirement is to use a list of known Indicators of Compromise (IoCs) and external signals, which directly aligns with the purpose of ETD.

In contrast, Security Health Analytics (SHA), mentioned in options A and B, is a posture management service. SHA custom modules are used to detect misconfigurations and vulnerabilities in resource settings, not to analyze log streams for threat activity based on IoCs.

Event Threat Detection provides pre-built templates for creating custom modules to simplify the detection engineering process. The "Configurable Bad IP" template is specifically designed for this exact use case. It allows an organization to upload and maintain a list of known malicious IP addresses (a common form of external IoC). ETD will then continuously scan relevant log sources, such as VPC Flow Logs, Cloud DNS logs, and Cloud NAT logs. If any activity to or from an IP address on this custom list is detected, ETD automatically generates a CONFIGURABLE_BAD_IP finding in Security Command Center for review and response. This approach is the native, efficient, and supported method for integrating IP-based IoCs into SCC, unlike option D which requires building a complex, manual pipeline.

(Google Cloud documentation, "Overview of Event Threat Detection custom modules"; "Using Event Threat Detection custom module templates")

Question 2. (Multi Select)

You are helping a new Google Security Operations (SecOps) customer configure access for their SOC team. The customer's Google SecOps administrators currently have access to the Google SecOps instance. The customer is reporting that the SOC team members are not getting authorized to access the instance, but they are able to authenticate to the third-party identity provider (IdP). How should you fix the issue?

Choose 2 answers

A: Link Google SecOps to a Google Cloud project with the Chronicle API.
B: Connect Google SecOps with the third-party IdP using Workforce Identity Federation.
C: Grant the appropriate data access scope to the SOC team's IdP group in IAM.
D: Grant the roles/chronicle.viewer role to the SOC team's IdP group in IAM.
E: Grant the Basic permission to the appropriate IdP groups in the Google SecOps SOAR Advanced Settings.

Correct Answer: D, E

Explanation:

Comprehensive and Detailed Explanation

This scenario describes a common configuration task where authorization is failing despite successful authentication. The problem stems from the fact that Google SecOps uses a dual-authorization model: one for the main platform (SIEM/Chronicle) and a separate one for the SOAR module. The SOC team needs both.

The prompt states admins already have access, which confirms that prerequisite steps like linking the project (Option A) and configuring Workforce Identity Federation (Option B) are already complete. The problem is specific to the new SOC team's group.

Fixing Instance Access (Option D):

The error "not getting authorized to access the instance" refers to the primary Google Cloud-level authorization. Access to the Google SecOps application itself is controlled by Google Cloud IAM roles on the linked project.1 The SOC team's group, which is federated from the third-party IdP, is represented as a principalSet in IAM. This principalSet must be granted an IAM role to allow sign-in. The roles/chronicle.viewer role is the minimum predefined role required to grant this application access.

Fixing SOAR Access (Option E):

Simply granting the IAM role (Option D) is not enough for the SOC team to perform its job. That role only gets them into the main SIEM interface. The SOAR module (for case management and playbooks) has its own internal role-based access control system. An administrator must also navigate within the SecOps platform to the SOAR Advanced Settings > Users & Groups and grant the SOC team's federated group a SOAR-specific permission, like "Basic" or "Analyst."

Both steps are required to fully "fix the issue" and provide the SOC team with functional access to the platform.

Exact Extract from Google Security Operations Documents:

Identity and Access Management: Access to a Google SecOps instance using a third-party IdP relies on Workforce Identity Federation, but authorization is configured in two distinct locations.

Google Cloud IAM: Authorization to the main SecOps instance (including the SIEM interface) is controlled by Google Cloud IAM.2 The federated identities (groups) from the third-party IdP are mapped to a principalSet. This principalSet must be granted an IAM role on the Google Cloud project linked to the SecOps instance. The roles/chronicle.viewer role is the minimum predefined role required to grant sign-in access.

Google SecOps SOAR: Authorization for the SOAR module (for case management and playbooks) is managed independently.3 An administrator must navigate to the SOAR Advanced Settings > Users & Groups and assign a SOAR-specific role (e.g., 'Basic' or 'Analyst') to the same federated IdP group.

Google Cloud Documentation: Google Security Operations > Documentation > Onboard > Configure a third-party identity provider

Google Cloud Documentation: Google Security Operations > Documentation > SOAR > SOAR Administration > Users and Groups

Question 3. (Single Select)

You are developing a playbook to respond to phishing reports from users at your company. You configured a UDM query action to identify all users who have connected to a malicious domain. You need to extract the users from the UDM query and add them as entities in an alert so the playbook can reset the password for those users. You want to minimize the effort required by the SOC analyst. What should you do?

A: Implement an Instruction action from the Flow integration that instructs the analyst to add the entities in the Google SecOps user interface.
B: Use the Create Entity action from the Siemplify integration. Use the Expression Builder to create a placeholder with the usernames in the Entities Identifier parameter.
C: Configure a manual Create Entity action from the Siemplify integration that instructs the analyst to input the Entities Identifier parameter based on the results of the action.
D: Create a case for each identified user with the user designated as the entity.

Correct Answer: B

Explanation:

Comprehensive and Detailed 150 to 250 words of Explanation From Exact Extract Google Security Operations Engineer documents:

The key requirement is to *automate* the extraction of data to *minimize analyst effort*. This is a core function of Google Security Operations SOAR (formerly Siemplify). The **Siemplify integration** provides the foundational playbook actions for case management and entity manipulation.

The **`Create Entity`** action is designed to programmatically add new entities (like users, IPs, or domains) to the active case. To make this action automatic, the playbook developer must use the **Expression Builder**. The Expression Builder is the tool used to parse the JSON output from a previous action (the UDM query) and dynamically map the results (the list of usernames) into the parameters of a subsequent action.

By using the Expression Builder to configure the `Entities Identifier` parameter of the `Create Entity` action, the playbook automatically extracts all `principal.user.userid` fields from the UDM query results and adds them to the case. These new entities can then be automatically passed to the next playbook step, such as "Reset Password."

Options A and C are incorrect because they are **manual** actions. They require an analyst to intervene, which does *not* minimize effort. Option D is incorrect as it creates multiple, unnecessary cases, flooding the queue instead of enriching the single, original phishing case.

(Google Cloud documentation, "Google SecOps SOAR Playbooks overview"; "Using the Expression Builder"; "Marketplace and Integrations")

***

Question 4. (Single Select)

Your company uses Google Security Operations (SecOps) Enterprise and is ingesting various logs. You need to proactively identify potentially compromised user accounts. Specifically, you need to detect when a user account downloads an unusually large volume of data compared to the user's established baseline activity. You want to detect this anomalous data access behavior using minimal effort. What should you do?

A: Develop a custom YARA-L detection rule in Google SecOps that counts download bytes per user per hour and triggers an alert if a threshold is exceeded.
B: Create a log-based metric in Cloud Monitoring, and configure an alert to trigger if the data downloaded per user exceeds a predefined limit. Identify users who exceed the predefined limit in Google SecOps.
C: Inspect Security Command Center (SCC) default findings for data exfiltration in Google SecOps.
D: Enable curated detection rules for User and Endpoint Behavioral Analytics (UEBA), and use the Risk Analytics dashboard in Google SecOps to identify metrics associated with the anomalous activity.

Correct Answer: D

Explanation:

Comprehensive and Detailed 150 to 250 words of Explanation From Exact Extract Google Security Operations Engineer documents:

The requirement to detect activity that is *unusual* compared to a *user's established baseline*

is the precise definition of **User and Endpoint Behavioral Analytics (UEBA)**. This is a core capability of Google Security Operations Enterprise designed to solve this exact problem with **minimal effort**.

Instead of requiring analysts to write and tune custom rules with static thresholds (like in Option A) or configure external metrics (Option B), the UEBA engine automatically models the behavior of every user and entity. By simply **enabling the curated UEBA detection rulesets**, the platform begins building these dynamic baselines from historical log data.

When a user's activity, such as data download volume, significantly deviates from their *own* normal, established baseline, a UEBA detection (e.g., `Anomalous Data Download`) is automatically generated. These anomalous findings and other risky behaviors are aggregated into a risk score for the user. Analysts can then use the **Risk Analytics dashboard** to proactively identify the highest-risk users and investigate the specific anomalous activities that contributed to their risk score. This built-in, automated approach is far superior and requires less effort than maintaining static, noisy thresholds.

(Google Cloud documentation, "User and Endpoint Behavioral Analytics (UEBA) overview"; "UEBA curated detections list"; "Using the Risk Analytics dashboard")

Question 5. (Single Select)

Your organization plans to ingest logs from an on-premises MySQL database as a new log source into its Google Security Operations (SecOps) instance. You need to create a solution that minimizes effort. What should you do?

A: Configure and deploy a Bindplane collection agent
B: Configure a third-party API feed in Google SecOps.
C: Configure direct ingestion from your Google Cloud organization.
D: Configure and deploy a Google SecOps forwarder.

Correct Answer: D

Explanation:

Comprehensive and Detailed 150 to 250 words of Explanation From Exact Extract Google

Security Operations Engineer documents:

The standard, native, and minimal-effort solution for ingesting logs from on-premises sources into Google Security Operations (SecOps) is to use the Google SecOps forwarder. The forwarder is a lightweight software component (available as a Linux binary or Docker container) that is deployed within the customer's network. It is designed to collect logs from a variety of on-premises sources and securely forward them to the SecOps platform.

The forwarder can be configured to monitor log files directly (which is a common output for a MySQL database) or to receive logs via syslog. Once the forwarder is installed and its configuration file is set up to point to the MySQL log file or syslog stream, it handles the compression, batching, and secure transmission of those logs to Google SecOps. This is the intended and most direct ingestion path for on-premises telemetry.

Option C is incorrect because the log source is on-premises, not within the Google Cloud organization. Option B (API feed) is the wrong mechanism; feeds are used for structured data like threat intelligence or alerts, not for raw telemetry logs from a database. Option A (Bindplane) is a third-party partner solution, which may involve additional configuration or licensing, and is not the native, minimal-effort tool provided directly by Google SecOps for this task.

(Google Cloud documentation, "Google SecOps data ingestion overview"; "Install and configure the SecOps forwarder")

ExamsIndex

Demo PDF Complete

Your Security-Operations-Engineer Demo (5 Questions)

Get the Complete Version

Full Questions with Detailed Explanations

Interactive Web-Based Exams Available

To get 50% off, use Coupon Code: OCT50

https://examsindex.com/exam/security-operations-engineer