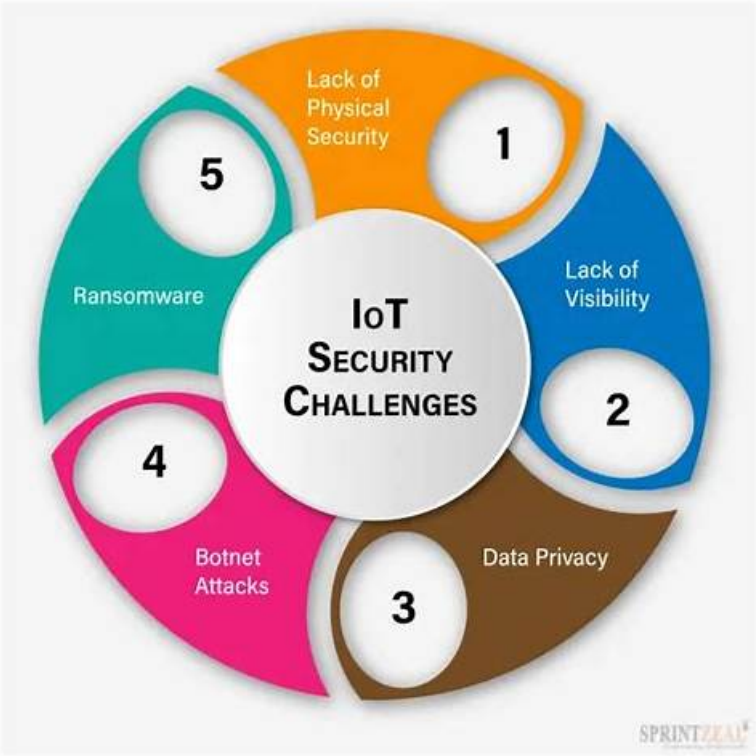
# One of the Best Ways to Prepare For the Security-Operations-Engineer




BTW, DOWNLOAD part of SurePassExams Security-Operations-Engineer dumps from Cloud Storage: https://drive.google.com/open?id=1WtWejOCFug41SSPZY7O4KOcjro3M03MR

SurePassExams provides with actual Google Security-Operations-Engineer exam dumps in PDF format. You can easily download and use Google Cloud Certified - Professional Security Operations Engineer (PSOE) Exam (Security-Operations-Engineer) PDF dumps on laptops, tablets, and smartphones. Our real Google Cloud Certified - Professional Security Operations Engineer (PSOE) Exam (Security-Operations-Engineer) dumps PDF is useful for applicants who don't have enough time to prepare for the examination. If you are a busy individual, you can use Google Security-Operations-Engineer PDF dumps on the go and save time.

## Google Security-Operations-Engineer Exam Syllabus Topics:

| Topic | Details |
|---|---|
| Topic 1 | • Platform Operations: This section of the exam measures the skills of Cloud Security Engineers and covers the configuration and management of security platforms in enterprise environments. It focuses on integrating and optimizing tools such as Security Command Center (SCC), Google SecOps, GTI, and Cloud IDS to improve detection and response capabilities. Candidates are assessed on their ability to configure authentication, authorization, and API access, manage audit logs, and provision identities using Workforce Identity Federation to enhance access control and visibility across cloud systems. |
| Topic 2 | • Threat Hunting: This section of the exam measures the skills of Cyber Threat Hunters and emphasizes proactive identification of threats across cloud and hybrid environments. It tests the ability to create and execute advanced queries, analyze user and network behaviors, and develop hypotheses based on incident data and threat intelligence. Candidates are expected to leverage Google Cloud tools like BigQuery, Logs Explorer, and Google SecOps to discover indicators of compromise (IOCs) and collaborate with incident response teams to uncover hidden or ongoing attacks. |

| | |
|---|---|
| Topic 3 | • Incident Response: This section of the exam measures the skills of Incident Response Managers and assesses expertise in containing, investigating, and resolving security incidents. It includes evidence collection, forensic analysis, collaboration across engineering teams, and isolation of affected systems. Candidates are evaluated on their ability to design and execute automated playbooks, prioritize response steps, integrate orchestration tools, and manage case lifecycles efficiently to streamline escalation and resolution processes. |



## 100% Pass Google Security-Operations-Engineer - Marvelous Reliable Google Cloud Certified - Professional Security Operations Engineer (PSOE) Exam Study Notes

Great concentrative progress has been made by our company, who aims at further cooperation with our candidates in the way of using our Security-Operations-Engineer exam engine as their study tool. Owing to the devotion of our professional research team and responsible working staff, our Security-Operations-Engineer Training Materials have received wide recognition and now, with more people joining in the Security-Operations-Engineer exam army, we has become the top-raking Security-Operations-Engineer learning guide provider in the international market.

## Google Cloud Certified - Professional Security Operations Engineer (PSOE) Exam Sample Questions (Q45-Q50):

**NEW QUESTION # 45**
You have discovered that a server that hosts an internal web application has been accidentally exposed to the internet for 48 hours. Logging is enabled on the server. You want to use Google Security Operations (SecOps) to run a UDM search against the server logs to identify whether there have been any successful exploitations against it. What event field search should you use?

- A. Perform a search for antimalware or endpoint security events by using the product_event_type UDM field.
- B. Perform a search for sign-on activity for user accounts that are not expected on the server by using the principal.user.userid UDM field.
- C. Perform a search for process launches and commands that are rarely seen by using the metadata.event_type UDM field.
- D. Perform a search for network traffic where the principal is rarely seen by using the principal.ip UDM field.

**Answer: C**

Explanation:
To check for successful exploitations, you need to look for abnormal process launches and commands that indicate post-exploitation activity. In Google SecOps UDM, this is done by searching with the metadata.event_type field, which classifies events such as process execution.
Unusual or rarely seen processes provide strong indicators of compromise.

**NEW QUESTION # 46**
Your company works with an external Managed Service Provider (MSP) that requires its users to have the ability to list findings from Security Command Center (SCC) using the Google Cloud SDK. You need to configure the required access for the managed service provider while minimizing your involvement in their external user lifecycle management processes. What should you do?

- A. Create a workload identity pool in a SCC project. Grant the MSP user the permission to impersonate a service account from this pool, and grant the service account the appropriate IAM role at the organization level.
- B. Create a user account in your Cloud Identity instance using a subdomain indicating they are external to your organization. Grant this user account the appropriate IAM role at the organization level.
- C. Create a workforce identity pool and federate with the identity provider (IdP) of the managed service provider. Grant users of the MSP the appropriate IAM role at the organization level.
- D. Create a service account in a SCC project. Grant the MSP user permission to impersonate this account. Grant this service account the appropriate IAM role at the organization level.

**Answer: C**

Explanation:
The best solution is to create a Workforce Identity Pool and federate with the MSP's IdP. This allows the MSP's users to authenticate with their own identity provider while receiving the necessary IAM roles in your environment. It minimizes your lifecycle management overhead since you don't need to create or manage individual external user accounts, while still providing secure, role-based access to SCC findings.

**NEW QUESTION # 47**
You are implementing Google Security Operations (SecOps) for your organization. Your organization has their own threat intelligence feed that has been ingested to Google SecOps by using a native integration with a Malware Information Sharing Platform (MISP). You are working on the following detection rule to leverage the command and control (C2) indicators that were ingested into the entity graph.
What code should you add in the detection rule to filter for the domain IOCS?

- A. $ioc.graph.metadata.entity_type = "D0MAIN_NAME"
  $ioc.graph.metadata.source_type = MDERIVED_CONTEXT"
- B. $ioc.graph.metadata.entity_type = "DOMAIN_NAME"
  Sioc.graph.metadata.source_type = "GLOBAL_CONTEXT"
- C. $ioc.graph.metadata.entity_type = ,'D0MAIN_NAME*'
  $ioc.graph.metadata.source type = "source type unspecified"
- D. $ioc.graph.metadata.entity_type = MDOMAIN_NAME"
  $ioc.graph.metadata.scurce_type = "ElfeITYj