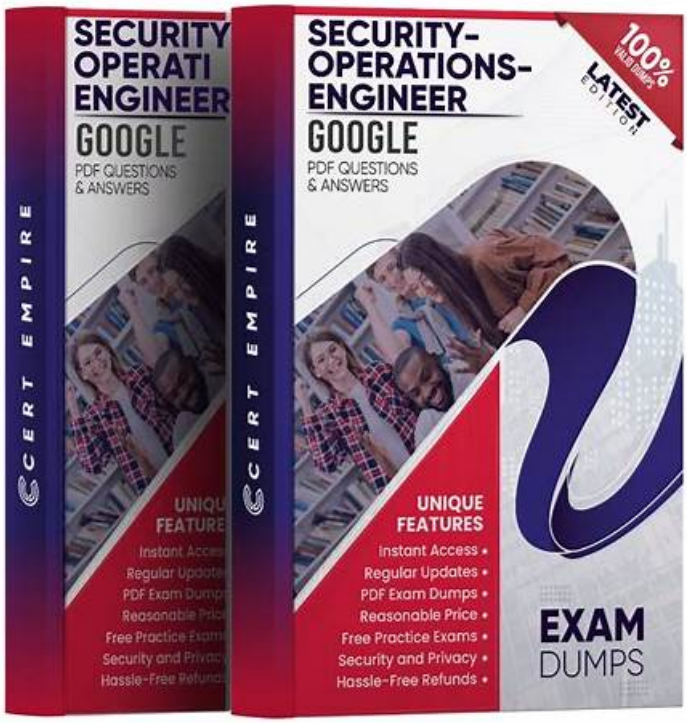
Free Google Security-Operations-Engineer Exam Questions, Security-Operations-Engineer Training Questions



P.S. Free & New Security-Operations-Engineer dumps are available on Google Drive shared by ValidDumps: https://drive.google.com/open?id=1FdJhIyHWAHEB5C2Nrm_0eNoiUhzfDqPa

Our Security-Operations-Engineer study materials can have such a high pass rate, and it is the result of step by step that all members uphold the concept of customer first. If you use a trial version of Security-Operations-Engineer training prep, you can find that our study materials have such a high passing rate and so many users support it. After using the trial version, we believe that you will be willing to choose Security-Operations-Engineer Exam Questions.

Google Security-Operations-Engineer Exam Syllabus Topics:

Section	Weight	Objectives
Detection engineering	22%	- Develop detection rules (YARA-L, Sigma) - Optimize detection logic and reduce false positives - Implement threat intelligence into detections - Manage detection lifecycle
Observability	10%	- Design monitoring and alerting strategies - Report security posture and risks - Analyze telemetry and metrics - Improve security visibility
Platform operations	14%	- Manage access and permissions - Configure Security Command Center - Manage Google Security Operations platform - Monitor platform health and performance
Threat hunting	19%	- Document and share findings - Use threat intelligence in hunting - Analyze anomalies and behaviors - Design and execute threat hunts

Data management	14%	- Validate data quality and completeness - Manage data retention and storage - Ingest and normalize logs and data - Implement Unified Data Model (UDM)
Incident response	21%	- Develop and use response playbooks - Contain and eradicate threats - Investigate security incidents - Automate response workflows

High-efficient Security-Operations-Engineer Training materials are helpful Exam Questions - ValidDumps

At the fork in the road, we always face many choices. When we choose job, job are also choosing us. Today's era is a time of fierce competition. Our Security-Operations-Engineer exam question can make you stand out in the competition. Why is that? The answer is that you get the certificate. What certificate? Certificates are certifying that you have passed various qualifying examinations. Watch carefully you will find that more and more people are willing to invest time and energy on the Security-Operations-Engineer Exam, because the exam is not achieved overnight, so many people are trying to find a suitable way.

Google Cloud Certified - Professional Security Operations Engineer (PSOE) Exam Sample Questions (Q35-Q40):

NEW QUESTION # 35
Your company's SOC recently responded to a ransomware incident that began with the execution of a malicious document. EDR tools contained the initial infection. However, multiple privileged service accounts continued to exhibit anomalous behavior, including credential dumping and scheduled task creation. You need to design an automated playbook in Google Security Operations (SecOps) SOAR to minimize dwell time and accelerate containment for future similar attacks. Which action should you take in your Google SecOps SOAR playbook to support containment and escalation?

- A. Create an external API call to VirusTotal to submit hashes from forensic artifacts.
- B. Add a YARA-L rule that sends an alert when a document is executed using a scripting engine such as wscript.exe.
- C. Configure a step that revokes OAuth tokens and suspends sessions for high-privilege accounts based on entity risk.
- D. Add an approval step that requires an analyst to validate the alert before executing a containment action.

Answer: C

Explanation:
To minimize dwell time and contain privileged account abuse in ransomware incidents, the SOAR playbook should revoke OAuth tokens and suspend sessions for high-privilege accounts based on entity risk. This action directly disrupts attacker persistence and lateral movement while automated escalation ensures timely response, reducing reliance on manual intervention.

NEW QUESTION # 36
You are using Google Security Operations (SecOps) to investigate suspicious activity linked to a specific user. You want to identify all assets the user has interacted with over the past seven days to assess potential impact. You need to understand the user's relationships to endpoints, service accounts, and cloud resources.
How should you identify user-to-asset relationships in Google SecOps?

- A. Run a retrohunt to find rule matches triggered by the user.
- B. Query for hostnames in UDM Search and filter the results by user.
- C. Generate an ingestion report to identify sources where the user appeared in the last seven days.
- D. Use the Raw Log Scan view to group events by asset ID.

Answer: B

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

documents:
The primary investigation tool for exploring relationships and historical activity in Google Security Operations is the UDM (Universal Data Model) search. The platform's curated views, such as the "User View," are built on top of this search capability.
To find all assets a user has interacted with, an analyst would perform a UDM search for the specific user (e.
g., principal.user.userid = "suspicious_user") over the specified time range. The search results will include all UDM events associated with that user. Within these events, the analyst can examine all populated asset fields, such as principal.asset.hostname, principal.ip, target.resource.name, and target.user.userid (for interactions with service accounts).
This UDM search allows the analyst to pivot from the user entity to all related asset entities, directly answering the question of "what assets the user has interacted with." While the wording of Option A is slightly backward (it's more efficient to query for the user and find the hostnames), it is the only option that correctly identifies the UDM search as the tool used to find user-to-asset (hostname) relationships. Options B (Retrohunt), C (Raw Log Scan), and D (Ingestion Report) are incorrect tools for this investigative task.
(Reference: Google Cloud documentation, "Google SecOps UM Search overview"; "Investigate a user"; " Universal Data Model noun list")

NEW QUESTION # 37
You are using Google Security Operations (SecOps) to identify and report a repetitive sequence of brute force SSH login attempts on a Compute Engine image that did not result in a successful login. You need to gain visibility into this activity while minimizing impact on your ingestion quota.
Which log type should you ingest into Google SecOps?

- A. Cloud IDS logs
- B. VPC Flow Logs
- C. Security Command Center Premium (SCCP) findings
- D. Cloud Audit Logs

Answer: B

Explanation:
VPC Flow Logs provide network-level visibility into traffic such as repetitive SSH connection attempts, regardless of login success. Ingesting VPC Flow Logs lets you identify brute force patterns while minimizing ingestion volume, since you don't need full authentication logs or Cloud Audit Logs for unsuccessful login attempts. This approach gives you the necessary insight into SSH brute force activity without high log ingestion costs.

NEW QUESTION # 38
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 Security Health Analytics (SHA) custom module using the compute address resource.
- B. Create a custom posture for your organization that combines the prebuilt Event Threat Detection and Security Health Analytics (SHA) detectors.
- 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.

Answer: C

Explanation:
The correct approach is to create an Event Threat Detection (ETD) custom module using the
"Configurable Bad IP" template. This allows you to ingest known IOCs, including external threat intelligence signals, and generate detections when these IOCs are observed in your environment, augmenting SCC's built-in detection capabilities.

NEW QUESTION # 39
You received an alert from Container Threat Detection that an added binary has been executed in a business critical workload. You need to investigate and respond to this incident. What should you do? (Choose two.)

- A. Keep the cluster and pod running, and investigate the behavior to determine whether the activity is malicious.

- B. Notify the workload owner. Follow the response playbook, and ask the threat hunting team to identify the root cause of the incident.
- C. Silence the alert in the Security Command Center (SCC) console, as the alert is a low severity finding.
- D. Review the finding, quarantine the cluster containing the running pod, and delete the running pod to prevent further compromise.
- E. Review the finding, investigate the pod and related resources, and research the related attack and response methods.

Answer: B,E

Explanation:
The correct response involves both notifying the workload owner and following the response playbook to ensure coordinated incident handling, and reviewing the finding while investigating the pod and related resources to understand the attack and determine the appropriate remediation. This approach ensures proper communication, structured incident response, and thorough technical investigation without prematurely deleting or silencing critical evidence.

NEW QUESTION # 40
.....

Based on the research results of the examination questions over the years, the experts give more detailed explanations of the contents of the frequently examined contents and difficult-to-understand contents, and made appropriate simplifications for infrequently examined contents. Security-Operations-Engineer test questions make it possible for students to focus on the important content which greatly shortens the students' learning time. With Security-Operations-Engineer Exam Torrent, you will no longer learn blindly but in a targeted way. With Security-Operations-Engineer exam guide, you only need to spend 20-30 hours to study and you can successfully pass the exam. You will no longer worry about your exam because of bad study materials. If you decide to choose and practice our Security-Operations-Engineer test questions, our life will be even more exciting.

Operations-Engineer Pattern □ [www.prep4sures.top] is best website to obtain □ Security-Operations-Engineer □ for free download □Security-Operations-Engineer Preparation Store

- ehoroskop.net, sakovaa.alboompro.com, fortunetelleroracle.com, scalar.usc.edu, qiita.com, emmaklewis.sites.gettysburg.edu, writeablog.net, estar.jp, www.grepmed.com, dorahacks.io, Disposable vapes

BONUS!!! Download part of ValidDumps Security-Operations-Engineer dumps for free: https://drive.google.com/open?id=1FdJhIyHWAHEB5C2Nrm_0eNoiUhzfDqPa