# GCP-SOE-B Exam Flashcards & Valid Braindumps GCP-SOE-B Questions


P.S. Free 2026 Google GCP-SOE-B dumps are available on Google Drive shared by Lead1Pass: https://drive.google.com/open?id=1pDjGXiSDLSE0l2sgqPCR7hb0FrXzZB44

All kinds of exams are changing with dynamic society because the requirements are changing all the time. To keep up with the newest regulations of the GCP-SOE-B exam, our experts keep their eyes focusing on it. Our GCP-SOE-B practice materials are updating according to the precise of the real exam. Our GCP-SOE-B Test Prep can help you to conquer all difficulties you may encounter. In other words, we will be your best helper. We are sure that GCP-SOE-B will help you pass the exam and get a good grade.

## Google GCP-SOE-B Exam Syllabus Topics:

| Section | Weight | Objectives |
|---|---|---|
| Topic 1: Incident Response | 20-25% | - Evidence collection and preservation<br>- Post-incident reporting<br>- Forensic analysis techniques<br>- Root cause analysis<br>- Incident classification and prioritization |
| Topic 2: Detection Engineering | 25-30% | - Log source integration and correlation<br>- Threat hunting methodologies<br>- SIEM platform usage (Chronicle, Splunk, etc.)<br>- False positive management<br>- Designing and implementing detection rules |
| Topic 3: Foundations of Security Operations | 15-20% | - Building a security operations center (SOC)<br>- Understanding MITRE ATT&CK framework<br>- Logging and monitoring infrastructure<br>- Security operations concepts and lifecycle |
| Topic 4: Threat Intelligence | 15-20% | - Indicator of compromise (IOC) analysis<br>- Intelligence-driven defense<br>- Threat intelligence sources and feeds<br>- Threat actor profiling |
| Topic 5: Google Cloud Security Operations | 15-20% | - Google Cloud logging and monitoring (Cloud Logging, Cloud Monitoring)<br>- Security Command Center integration<br>- Automation with SOAR capabilities<br>- Cloud-native threat detection<br>- SIEM integration with Google Cloud services |

**>> GCP-SOE-B Exam Flashcards <<**

# Pass Guaranteed Quiz Professional Google - GCP-SOE-B - Security Operations Engineer (Beta) Exam Flashcards

At present, Google certification exam is the most popular test. Have you obtained Google exam certificate? For example, have you taken Google GCP-SOE-B certification exam? If not, you should take action as soon as possible. The certificate is very important, so you must get GCP-SOE-B certificate. Here I would like to tell you how to effectively prepare for Google GCP-SOE-B exam and pass the test first time to get the certificate.

## Google Security Operations Engineer (Beta) Sample Questions (Q49-Q54):

**NEW QUESTION # 49**
Your company uses Security Command Center (SCC) and Google Security Operations (SecOps). Last week, an attacker attempted to establish persistence by generating a key for an unused service account. You need to confirm that you are receiving alerts when keys are created for unused service accounts and that newly created keys are automatically deleted. You want to minimize the amount of manual effort required. What should you do?

- A. Use the Initial Access: Dormant Service Account Key Created finding from SCC, and write this finding to a Pub/Sub topic. Create a Cloud Run function that subscribes to the Pub/Sub topic and deletes the service account key.
- B. Configure a Cloud Logging sink to write logs to a Pub/Sub topic that filters for the methodName: "google.iam.admin.v1.CreateServiceAccountKey" field. Create a Cloud Run function that subscribes to the Pub/Sub topic and deletes the service account key.
- C. Generate a YARA-L rule in Google SecOps that detects when a service account key is created. Using the built-in IDE, create a custom action in Google SecOps SOAR that deletes the service account key.
- D. Use the Initial Access: Dormant Service Account Key Created finding from SCC, and ingest this finding into Google SecOps. Create a custom action in Google SecOps SOAR that is triggered on this finding. Use the built-in IDE to build code to delete the service account key.

**Answer: D**

**NEW QUESTION # 50**
Which approach BEST improves detection of compromised service accounts in Google Cloud?

- A. Baseline service account behavior and alert on deviations
- B. Disabling all service accounts You are managing the integration of Security Command Center (SCC) with downstream tooling.
- C. Monitoring VM uptime
- D. Alerting on login failures only

**Answer: A**

**NEW QUESTION # 51**
Your organization's Google Security Operations (SecOps) tenant is ingesting a vendor's firewall logs in its default JSON format using the Google-provided parser for that log. The vendor recently released a patch that introduces a new field and renames an existing field in the logs. The parser does not recognize these two fields and they remain available only in the raw logs, while the rest of the log is parsed normally. You need to resolve this logging issue as soon as possible while minimizing the overall change management impact. What should you do?

- A. Use the web interface-based custom parser feature in Google SecOps to copy the parser, and modify it to map both fields to UDM.
- B. Use the Extract Additional Fields tool in Google SecOps to convert the raw log entries to additional fields.
- C. Deploy a third-party data pipeline management tool to ingest the logs, and transform the updated fields into fields supported by the default parser.
- D. Write a code snippet, and deploy it in a parser extension to map both fields to UDM.

**Answer: B**

**NEW QUESTION # 52**
Which Google Cloud security feature MOST helps enforce the principle of least privilege at scale?

- A. IAM predefined roles and conditional IAM policies
- B. Binary Authorization
- C. Cloud NAT
- D. VPC Firewall Rules

**Answer: A**

**NEW QUESTION # 53**
You are working with your company's analyst team to automate the investigation of phishing alerts ingested directly into Google Security Operations (SecOps) SOAR from an email inbox.
The analyst team currently uses a SIEM query to search for related information. You need to design a solution to automatically include the query results in the Google SecOps case without writing any new code. What should you do?

- A. Add a widget to the Default Case View in Google SecOps SOAR that allows the analyst team to query directly from the widget.
- B. Modify the detection rule in the SIEM to include the query results as part of the detection.
- C. Add an action to the playbook that runs the SIEM query and returns the results.
- D. Create a custom action in Google SecOps IDE that runs the SIEM query from a playbook through an API call and returns the results.

**Answer: C**

**NEW QUESTION # 54**
.....

The client only needs 20-30 hours to learn our GCP-SOE-B learning questions and then they can attend the test. Most people may devote their main energy and time to their jobs, learning or other important things and can't spare much time to prepare for the GCP-SOE-B test. But if clients buy our GCP-SOE-B Training Materials they can not only do their jobs or learning well but also pass the GCP-SOE-B test smoothly and easily because they only need to spare little time to learn and prepare for the GCP-SOE-B test.

- GCP-SOE-B Exam Braindumps - GCP-SOE-B Origination Questions - GCP-SOE-B Study Guide □ The page for free download of ➽ GCP-SOE-B □ on ▹ www.prep4sures.top ◃ will open immediately □Useful GCP-SOE-B Dumps
- www.4shared.com, disqus.com, disqus.com, www.slideshare.net, fortunetelleroracle.com, divisionmidway.org, hanson.net, www.slideshare.net, savee.com, gettr.com, Disposable vapes

What's more, part of that Lead1Pass GCP-SOE-B dumps now are free: https://drive.google.com/open?id=1pDjGXiSDLSE0l2sgqPCR7hb0FrXzZB44