

Google.GCP-SOE-B.v2026-10-16.q30

Exam Code:	GCP-SOE-B
Exam Name:	Security Operations Engineer (Beta)
Certification Provider:	Google
Free Question Number:	30
Version:	v2026-10-16
# of views:	115
# of Questions views:	300
https://www.freeqas.com/qa/Google/GCP-SOE-B/Google.GCP-SOE-B.v2026-10-16.q30.html	

NEW QUESTION: 1

Which approach BEST improves detection of compromised service accounts in Google Cloud?

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

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 2

Which Google Cloud security feature MOST helps enforce the principle of least privilege at scale?

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

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 3

Your company requires PCI DSS v4.0 compliance for its cardholder data environment (CDE) in Google Cloud. You use a Security Command Center (SCC) security posture deployment based on the PCI DSS v4.0 template to monitor for configuration drift. This posture generates a finding indicating that a Compute Engine VM within the CDE scope has been configured with an external IP address. You need to take an immediate action to

remediate the compliance drift identified by this specific SCC posture finding. What should you do?

- A.** Navigate to the underlying Security Health Analytics (SHA) finding for PUBLIC_IP_ADDRESS on the VM, and mark this finding as fixed.
- B.** Reconfigure the network interface settings for the VM to explicitly remove the assigned external IP address.
- C.** Enable and enforce the constraints/compute.vmExternallpAccess organization policy constraint at the project level for the project where the VM resides.
- D.** Remove the CDE-specific tag from the VM to exclude the tag from this particular PCI DSS posture evaluation scan.

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 4

You are an incident response engineer at an organization that uses Google Security Operations (SecOps). You recently started monitoring IOCS in Applied Threat Intelligence using YARA-L rules. You have discovered that there are more false positive alerts than expected, which is causing noise for the SOC team. You need to reduce the number of false positive alerts. What should you do?

- A.** Configure alert grouping for the most repetitive alerts.
- B.** Create a playbook that automatically tunes the IOC source if its indicator confidence score (IC- Score) is between 60% and 80%.
- C.** Modify the YARA-L rules to use an indicator confidence score (IC-Score) of 60% and above.
- D.** Implement curated detections instead of custom YARA-L rules.

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 5

Your company is adopting a multi-cloud environment. You need to configure comprehensive monitoring of threats using Google Security Operations (SecOps). You want to start identifying threats as soon as possible. What should you do?

- A.** Use Gemini to generate YARA-L rules for multi-cloud use cases.
- B.** Use curated detections from the Cloud Threats category to monitor your cloud environment.
- C.** Ask Cloud Customer Care to provide a set of rules recommended by Google to monitor your company's cloud environment.
- D.** Use curated detections for Applied Threat Intelligence to monitor your company's cloud environment.

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 6

You are responsible for monitoring the ingestion of critical Windows server logs to Google Security Operations (SecOps) by using the Bindplane agent. You want to receive an immediate notification when no logs have been ingested for over 30 minutes. You want to use the most efficient notification solution. What should you do?

- A.** Create a new YARA-L rule in Google SecOps SIEM to detect the absence of logs from the server within a 30-minute window.
- B.** Create a new alert policy in Cloud Monitoring that triggers a notification based on the absence of logs from the server's hostname.
- C.** Configure a Bindplane agent to send a heartbeat signal to Google SecOps every 15 minutes, and create an alert if two heartbeats are missed.
- D.** Configure the Windows server to send an email notification if there is an error in the Bindplane process.

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 7

You are investigating an alert in Google Security Operations (SecOps). You want to view previous enrichment attributes and relevant historical cases for an entity using the fewest number of steps. What should you do?

- A.** Initiate a SIEM Search to query the entity.
- B.** Initiate a SOAR Search to query the entity.
- C.** Select the entity identifier in the Entity Highlights widget to open Entity Explorer.
- D.** Select View Details for the entity in the Entity Highlights widget.

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 8

Your organization recently implemented Google Security Operations (SecOps) with Applied Threat Intelligence enabled. You were notified by the networking team about potentially anomalous communications to external domains in the last 30 days. You plan to start your threat hunting by looking at communications to external domains. You are ingesting the following logs into Google SecOps:

- Firewall logs
- Proxy logs
- DNS logs
- DHCP logs

What should you do? (Choose two.)

- A.** Perform a raw log search across the logs for domains with low prevalence that were first seen in the last 30 days.
- B.** Perform a UDM search across the logs for domains with geolocations that were first seen in the last 30 days.

- C.** Navigate to the IOC Matches page and filter based on domain type over the last 30 days. Look for the first seen and last seen timestamps for the reported domains. Investigate these domains using the IOC drilldown link.
- D.** Perform a UDM search across the logs for domains with low prevalence that were first seen in the last 30 days.
- E.** Identify the domains with the higher normalized risk in Risk Analytics. Drill down into those entities to determine their prevalence and if they were first seen in the last 30 days.
- Answer: D,E ([LEAVE A REPLY](#))**

NEW QUESTION: 9

You have been tasked with creating a YARA-L detection rule in Google Security Operations (SecOps). The rule should identify when an internal host initiates a network connection to an external IP address that the Applied Threat Intelligence Fusion Feed associates with indicators attributed to a specific Advanced Persistent Threat 41 (APT41) threat group. You need to ensure that the external IP address is flagged if it has a documented relationship to other APT41 indicators within the Fusion Feed. How should you configure this YARA-L rule?

- A.** Configure the rule to detect outbound network connections to the external IP address. Create a Google SecOps SOAR playbook that queries the Fusion Feed to determine if the IP address has an APT41 relationship.
- B.** Configure the rule to trigger when the external IP address from the network connection event matches an entry in a manually pre-curated reference list of all APT41-related IP addresses.
- C.** Configure the rule to establish a join between the live network connection event and Fusion Feed data for the common external IP address. Filter the joined Fusion Feed data for explicit associations with the APT41 threat group or related indicators.
- D.** Configure the rule to check whether the external IP address from the network connection event has a high confidence score across any enabled threat intelligence feed.

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 10

Your organization recently implemented Google Security Operations (SecOps). You need to create a solution that allows the security team to monitor data ingestion into Google SecOps in real time. You also need to configure a solution that automatically sends a notification if one of the data sources stops ingesting data. You need to minimize the cost of these configurations.

What should you do?

- A.** Create Looker dashboards to visualize the data ingestion, and configure an alerting policy in Cloud Monitoring to send a notification in case of failure.
- B.** Use Google SecOps SIEM dashboards to visualize the data ingestion, and configure an alerting policy in Cloud Monitoring to send a notification in case of failure.

C. Create Looker dashboards to visualize the data ingestion, and configure an alerting policy in Looker to send a notification in case of failure.

D. Use Google SecOps SIEM dashboards to visualize the data ingestion and configure an alerting policy in Cloud Logging to send a notification in case of failure.

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 11

You work for a large international company that has several Compute Engine instances running in production. You need to configure monitoring and alerting for Compute Engine instances tagged with compliance-pci that have an external IP address assigned. What should you do?

A. Use the PUBLIC_IP_ADDRESS Security Health Analytics (SHA) detector to identify Compute Engine instances with external IP addresses. Determine whether the compliance-pci tag exists on the instances.

B. Deploy the compute.vmExternalIpAccess organization policy constraint to prevent specific projects or folders with the compliance-pci tag from creating Compute Engine instances with external IP addresses.

C. Create a custom Security Health Analytics (SHA) module. Configure the detection logic to scan Cloud Asset Inventory data for compute.googleapis.com/Instance assets, and Search for the compliance-pci tag.

D. Create a custom Event Threat Detection module that alerts when a Compute Engine instance with the compliance-pci tag is assigned an external IP address.

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 12

You have noticed that a Google Security Operations (SecOps) detection rule that detects excessive network connections is triggering too frequently and creating too many false positive alerts. You want to improve the rule to reduce the noise without reducing the effectiveness of the rule. What change to the detection rule should you implement?

A. Include a 10 minute timeframe for the same source and destination of network connections in the YARA-L match: section to aggregate the alerts.

B. Assign a risk score in the YARA-L outcome: section to prioritize alerts more effectively in the alert queue.

C. Add a threshold in the YARA-L condition: section to ensure that the rule only alerts after a certain number of connections.

D. Update the YARA-L events: section to exclude the most common IP addresses involved in the network connection alerts to reduce the number of alerts.

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 13

You are receiving security alerts from multiple connectors in your Google Security Operations (SecOps) instance. You need to identify which IP address entities are internal to your network and label each entity with its specific network name. This network name will be used as the trigger for the playbook. What should you do?

- A.** Enrich the IP address entities as the initial step of the playbook.
- B.** Configure each network in the Google SecOps SOAR settings.
- C.** Modify the entity attribute in the alert overview.
- D.** Create an outcome variable in the rule to assign the network name.

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 14

You need to pull security findings from SCC and import those findings as part of Google Security Operations (SecOps) SOAR actions. You need to configure the connection between SCC and Google SecOps. What should you do?

- A.** Create a Pub/Sub topic with a NotificationConfig object and a push subscription for the desired finding types. Create a new Google SecOps service account in the Google Cloud project, and grant this service account the appropriate IAM roles to read from this subscription. Export the credentials from IAM and import the credentials into Google SecOps SOAR.
- B.** Create a Pub/Sub topic with a NotificationConfig object and a push subscription for the desired finding types. Grant the Google SecOps service account the appropriate IAM roles to read from this subscription.
- C.** Install the Google Rapid Response integration from the Google SecOps Marketplace. Gather information about the findings from the appropriate server.
- D.** Install the SCC integration from the Google SecOps Marketplace. Grant the SCC API the appropriate IAM roles to integrate with the Google SecOps instance. Configure this integration using a generated API key scoped to the SCC API.

Answer: ([SHOW ANSWER](#)**)**

NEW QUESTION: 15

Your organization uses Google Security Operations (SecOps) for security analysis and investigation. Your organization has decided that all security cases related to Data Loss Prevention (DLP) events must be categorized with a defined root cause specific to one of five DLP event types when the case is closed in Google SecOps. How should you achieve this?

- A.** Create a Google SecOps SOAR playbook that automatically assigns case tags where each tag contains the unique definition of one of the five DLP event types.
- B.** Create case tags in Google SecOps SOAR where each tag contains a unique definition of each of the five DLP event types, and have analysts assign them to cases manually.
- C.** Customize the Case Name format to include the DLP event type.

D. Customize the Close Case dialog and add the five DLP event types as root cause options.

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 16

You are an incident responder at your organization using Google Security Operations (SecOps) for monitoring and investigation. You discover that a critical production server, which handles financial transactions, shows signs of unauthorized file changes and network scanning from a suspicious IP address. You suspect that persistence mechanisms may have been installed. You need to use Google SecOps to immediately contain the threat while ensuring that forensic data remains available for investigation. What should you do first?

A. Use the EDR integration to quarantine the compromised asset.

B. Deploy emergency patches, and reboot the server to remove malicious persistence.

C. Use the firewall integration to submit the IP address to a network block list to inhibit internet access from that machine.

D. Use VirusTotal to enrich the IP address and retrieve the domain. Add the domain to the proxy block list.

Answer: **A** ([LEAVE A REPLY](#))

Valid GCP-SOE-B Dumps shared by PrepPdf.com for Helping Passing GCP-SOE-B Exam! PrepPdf.com now offer the **newest GCP-SOE-B exam dumps**, the PrepPdf.com GCP-SOE-B exam **questions have been updated** and **answers have been corrected** get the **newest** PrepPdf.com GCP-SOE-B dumps with Test Engine here:
<https://www.preppdf.com/Google/GCP-SOE-B-prepaway-exam-dumps.html> (87 Q&As Dumps, **40%OFF Special Discount: Exam-Tests**)

NEW QUESTION: 17

Your company's Google Security Operations (SecOps) instance has three roles: Tier 1, Tier 2, and Tier 3. Currently, analysts in all tiers can access all cases in Google SecOps. Your company's SOC has a new requirement to restrict access to cases assigned to the Tier 3 role from the other tiers. You need to ensure cases that are assigned to the Tier 3 role can only be accessed by Tier 3 analysts. What should you do?

A. Instruct analysts in Tier 1 and Tier 2 to create a case queue filter to exclude cases assigned to the Tier 3 role.

B. Revoke additional role access from Tier 1 and Tier 2 analysts.

C. Configure the Cross Environment Policy to allow users to move cases between environments. Move Tier 3 cases to an environment that only Tier 3 analysts can access.

D. Assign the cases to a user in the Tier 3 role.

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 18

You observe several distinct, low-severity suspicious activities associated with a single internal server. You determine that no single event is a high-confidence IO You need to create a solution that ensures ongoing and heightened scrutiny for this server. What should you do?

- A.** Add the server to a Google Security Operations (SecOps) watchlist, and monitor the watchlist closely for the next few weeks.
- B.** Create a case, isolate the server from the network, and escalate the case for forensic investigation.
- C.** Schedule a daily Google Security Operations (SecOps) report detailing all activity on this server.
- D.** Develop a YARA-L detection rule specific to this server.

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 19

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

Answer: **A** ([LEAVE A REPLY](#))

NEW QUESTION: 20

You work for an organization that uses Security Command Center (SCC) with Event Threat Detection (ETD) enabled. You need to enable ETD detections for data exfiltration attempts from designated sensitive Cloud Storage buckets and BigQuery datasets. You want to minimize Cloud Logging costs. What should you do?

- A.** Enable VPC Flow Logs for the VPC networks containing resources that access the sensitive Cloud Storage buckets and BigQuery datasets.
- B.** Enable "data read" and "data write" audit logs for all Cloud Storage buckets and BigQuery datasets throughout the organization.
- C.** Enable "data read" and "data write" audit logs only for the designated sensitive Cloud Storage buckets and BigQuery datasets.
- D.** Enable "data read" audit logs only for the designated sensitive Cloud Storage buckets and BigQuery datasets.

Answer: **D** ([LEAVE A REPLY](#))

NEW QUESTION: 21

Your company's analyst team uses a playbook to make necessary changes to external systems that are integrated with the Google Security Operations (SecOps) platform. You need to automate the task to run once every day at a specific time. You want your solution to minimize maintenance overhead. What should you do?

- A.** Use a VM to host a script that runs a playbook via an API call.
- B.** Create a Cron Scheduled Connector for this use case. Configure a playbook trigger to match the cases created by the connector that runs the playbook with the relevant actions.
- C.** Create a Google SecOps SOAR request and a playbook trigger to match the request from the user to start the playbook with the relevant actions.
- D.** Write a custom Google SecOps SOAR job in the IDE using the code from the existing playbook actions.

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 22

You are a security analyst at an organization that uses Google Security Operations (SecOps).

You notice suspicious login attempts on several user accounts. You need to determine whether these attempts are part of a coordinated attack as quickly as possible. What action should you take first?

- A.** Remove user accounts that have repeated invalid login attempts.
- B.** Use UDM Search to query historical logs for recent IOCS associated with the suspicious login attempts.
- C.** Enable default curated detections to automatically block suspicious IP addresses.
- D.** Look for correlations across impacted users in the Risk Analytics dashboard.

Answer: D ([LEAVE A REPLY](#))

NEW QUESTION: 23

An organization detects a successful login to a Google Cloud IAM user from an unfamiliar country, followed by the creation of multiple new service account keys within minutes. No malware alerts are triggered. What is the MOST appropriate immediate action?

- A.** Disable the service accounts and continue monitoring.
- B.** Revoke active credentials, disable the compromised identity, and initiate an incident response.
- C.** Rotate only the affected user's password.
- D.** Wait for evidence of data access.

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 24

Your organization is a Google Security Operations (SecOps) customer. The compliance team requires a weekly export of case resolutions and SLA metrics of high and critical

severity cases over the past week. The compliance team's post- processing scripts require this data to be formatted as tabular data in CSV files, zipped, and delivered to their email each Monday morning.

What should you do?

- A.** Generate a report in SOAR Reports, and schedule delivery of the report.
- B.** Build an Advanced Report in SOAR Reports, and schedule delivery of the report.
- C.** Use statistics in search, and configure a Google SecOps SOAR job to format and send the report.
- D.** Build a detection rule with outcomes, and configure a Google SecOps SOAR job to format and send the report.

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 25

You are ingesting and parsing logs from an SSO provider and an on-premises appliance using Google Security Operations (SecOps). Users are tagged as "restricted" by an internal process. Restrictions last five days from the most recent flagging time. You need to create a rule to detect when restricted users log into the appliance. Your solution must be quickly implemented and easily maintained. What should you do?

- A.** Store the identifiers of the flagged users in the detection rule logic. Actively monitor for newly flagged users, and add them to the detection rule logic.
- B.** Use a Google SecOps SOAR global context value to store a list of flagged users with their corresponding time to live values. Use a SOAR job to dynamically build and deploy a new version of the detection rule with the updated list of flagged users.
- C.** Ingest the user flags as custom enrichment data using a feed. Use a multi-event detection rule to find logins from users flagged in the entity graph.
- D.** Store the flagged users in a data table column with their corresponding time to live values in a second column. Use row-based comparisons in your detection rule.

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 26

You are responsible for evaluating the level of effort required to integrate a new third-party endpoint detection tool with Google Security Operations (SecOps). Your organization's leadership wants to minimize customization for the new tool for faster deployment. You need to verify that the Google SecOps SOAR and SIEM support the expected workflows for the new third-party tool.

You must recommend a tool to your leadership team as quickly as possible. What should you do? (Choose two.)

- A.** Review the documentation to identify if default parsers exist for the tool, and determine whether the logs are supported and able to be ingested.
- B.** Review the architecture of the tool to identify the cloud provider that hosts the tool.

- C. Develop a custom integration that uses Python scripts and Cloud Run functions to forward logs and orchestrate actions between the third-party tool and Google SecOps.
- D. Identify the tool in the Google SecOps Marketplace and verify support for the necessary actions in the workflow.
- E. Configure a Pub/Sub topic to ingest raw logs from the third-party tool and build custom YARA-L rules in Google SecOps to extract relevant security events.

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 27

You are implementing Google Security Operations (SecOps) with multiple log sources. You want to closely monitor the health of the ingestion pipeline's forwarders and collection agents, and detect silent sources within five minutes. What should you do?

- A. Create a Google SecOps SIEM dashboard to show the ingestion metrics for each log_type and collector_id.
- B. Create a Looker dashboard that queries the BigQuery ingestion metrics schema for each log_type and collector_id.
- C. Create an ingestion notification for health metrics in Cloud Monitoring based on the total ingested log count for each collector_id.
- D. Create a notification in Cloud Monitoring using a metric- absence condition based on sample policy for each collector_id.

Answer: D ([LEAVE A REPLY](#))

NEW QUESTION: 28

Your organization uses the curated detection rule set in Google Security Operations (SecOps) for high priority network indicators. You are finding a vast number of false positives coming from your on-premises proxy servers. You need to reduce the number of alerts. What should you do?

- A. Configure a rule exclusion for the network.asset.ip field.
- B. Configure a rule exclusion for the principal.ip field.
- C. Configure a rule exclusion for the target.ip field.
- D. Configure a rule exclusion for the target.domain field.

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 29

After resolving a confirmed security incident in Google Cloud, what action provides the GREATEST long-term security improvement?

- A. Increasing log retention
- B. Updating detections, playbooks, and IAM controls based on lessons learned
- C. Closing all related alerts
- D. Adding more analysts

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 30

Your organization uses Google Security Operations (SecOps). You need to identify the most commonly occurring processes and applications across your organization's large number of servers so you can implement baselines and exclusion lists on a regular basis. You want to use the most efficient approach. What should you do?

- A.** Review the Google SecOps SIEM Rules & Detections, and identify the most common processes appearing in alerts that are marked as false positives.
- B.** Use the UDM lookup feature to identify relevant process- related UDM fields and values.
- C.** Run a UDM search, and review aggregations for relevant process-related UDM fields.
- D.** Generate a Google SecOps SIEM dashboard based on relevant UDM fields, such as processes, that provides the counts for process names and files.

Answer: ([SHOW ANSWER](#))

Valid GCP-SOE-B Dumps shared by PrepPdf.com for Helping Passing GCP-SOE-B Exam! PrepPdf.com now offer the **newest GCP-SOE-B exam dumps**, the PrepPdf.com GCP-SOE-B exam **questions have been updated** and **answers have been corrected** get the **newest** PrepPdf.com GCP-SOE-B dumps with Test Engine here:
<https://www.preppdf.com/Google/GCP-SOE-B-prepaway-exam-dumps.html> (87 Q&As Dumps, **40%OFF** Special Discount: **Exam-Tests**)