Pass2Certify.com
Prepare, Practice, & Pass.

Google

GCP-SOE-B

ExamName: Security Operations Engineer (Beta)

Exam Version: 6.0

Questions & Answers Sample PDF

(Preview content before you buy)

Check the full version using the link below.

https://pass2certify.com/exam/gcp-soe-b

Unlock Full Features:

Stay Updated: 90 days of free exam updates
Zero Risk: 30-day money-back policy
Instant Access: Download right after purchase
Always Here: 24/7 customer support team

Question 1. (Multi Select)

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 UDM search across the logs for domains with geolocations that were first seen in the last 30 days.
B: Perform a UDM search across the logs for domains with low prevalence that were first seen in the last 30 days.
C: Perform a raw log search across the logs for domains with low prevalence that were first seen in the last 30 days.
D: 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.
E: 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.

Answer: B, D

Question 2. (Single Select)

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: Customize the Close Case dialog and add the five DLP event types as root cause options.
B: Customize the Case Name format to include the DLP event type.
C: 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.
D: 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.

Answer: A

Question 3. (Single Select)

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: Install the Google Rapid Response integration from the Google SecOps Marketplace. Gather information about the findings from the appropriate server.
B: 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.
C: 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.
D: 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.

Answer: B

Question 4. (Single Select)

You are an incident responder at your organization using Google Security Operations (SecOps) for monitonng 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 firewall integration to submit the IP address to a network block list to inhibit internet access from that machine.
B: Deploy emergency patches, and reboot the server to remove malicious persistence.
C: Use the EDR integration to quarantine the compromised asset.
D: Use VirusTotal to enrich the IP address and retrieve the domain. Add the domain to the proxy block list.

Answer: C

Question 5. (Single Select)

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 notification in Cloud Monitoring using a metric- absence condition based on sample policy for each collector_id.
B: Create a Google SecOps SIEM dashboard to show the ingestion metrics 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 Looker dashboard that queries the BigQuery ingestion metrics schema for each log_type and collector_id.

Answer: A

Need more info? Check the link below:

https://pass2certify.com/exam/gcp-soe-b

Thanks for Being a Valued Pass2Certify User!

Guaranteed Success Pass Every Exam with Pass2Certify.

Save $15 instantly with promo code

SAVEFAST

Sales: sales@pass2certify.com

Support: support@pass2certify.com