Google
GCP-SOE-B
Security Operations Engineer (Beta)

For More Information – Visit link below:
https://www.examsempire.com/

Product Version

1. **Up to Date products, reliable and verified.**
2. **Questions and Answers in PDF Format.**

Latest Version: 6.0

Question: 1

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: 2

You are a SOC manager at an organization that recently implemented Google Security Operations (SecOps). You need to monitor your organization's data ingestion health in Google SecOps. Data is ingested with Bindplane collection agents. You want to configure the following:
- Receive a notification when data sources go silent within 15 minutes.
- Visualize ingestion throughput and parsing errors. What should you do?

A. Configure notifications in Cloud Monitoring when ingestion sources become silent in Bindplane. Monitor and visualize Google SecOps data ingestion metrics using Bindplane Observability Pipeline (OP).
B. Configure silent source notifications for Google SecOps collection agents in Cloud Monitoring. Create a Cloud Monitoring dashboard to visualize data ingestion metrics.
C. Configure silent source alerts based on rule detections for anomalous data ingestion activity in Risk Analytics. Monitor and visualize the alert metrics in the Risk Analytics dashboard.
D. Configure automated scheduled delivery of an ingestion health report in the Data Ingestion and Health dashboard. Monitor and visualize data ingestion metrics in this dashboard.

Answer: B

Question: 3

You are threat hunting for an advanced threat group known for targeted, novel attacks by deploying campaign-specific infrastructure. You want to develop detections based on the threat group's behaviors

so you can effectively detect whether the threat group has attacked your organization. What should you do?

A. Identify exposed technologies and products used by your organization, and develop detections to search for signs of exploitation.
B. Find intelligence reports in Google Threat Intelligence that relate to the threat actor, identify their behavior in previous campaigns, and use the past behavior to design detections in Google Security Operations (SecOps).
C. Search for the threat actor in Google Threat Intelligence, export the IOCs associated with the threat actor into a Google Security Operations (SecOps) list, and develop detections that reference this list.
D. Search for the threat actor in Google Threat Intelligence, review the threat actor's tactics, techniques, and procedures (TTPs), and design detections based on the TTPs in Google Security Operations (SecOps).

Answer: D

Question: 4

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

Answer: D

Question: 5

You are a senior SOC analyst in your organization. You are receiving alerts of traffic to a command and control (C2) IP address. You want to use Google Security Operations (SecOps) to investigate the IP address associated with the C2 IP address. What should you do?

A. Use Google SecOps SOAR Search to run a playbook designed to investigate the suspicious IP address and identify related outbound and inbound traffic.
B. Use Google SecOps SOAR Search to identify the cases where the suspicious IP address exists.

C. Conduct a Google SecOps SIEM Search that uses src.ip and target.ip to identify outbound and inbound traffic associated with the suspicious IP address.
D. Use Google SecOps SIEM Search to query against the grouped ip field, and use the enriched field from the suspicious events to identify related activity.

Answer: C

Question: 6

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

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

Answer: C

Question: 7

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: 8

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

Thank You for Trying Our Product

Special 16 USD Discount Coupon: NSZUBG3X

Email: support@examsempire.com

Check our Customer Testimonials and ratings available on every product page.

Visit our website.

https://examsempire.com/