Google
GCP-PSOE
Google Professional Security Operations Engineer

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 company has deployed two on-premises firewalls. You need to configure the firewalls to send logs to Google Security Operations (SecOps) using Syslog. What should you do?
Response:

A. Pull the firewall logs by using a Google SecOps feed integration.
B. Set the Google SecOps URL instance as the Syslog destination.
C. Deploy a third-party agent (e.g Bindplane, NXLog) on your on-premises environment, and set the agent as the Syslog destination.
D. Deploy a Google Ops Agent on your on-premises environment, and set the agent as the Syslog destination.

Answer: C

Question: 2

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?
Response:

A. Use the UDM lookup feature to identify relevant process-related UDM fields and values.
B. Run a UDM search, and review aggregations for relevant process-related UDM fields.
C. Review the Google SecOps SIEM Rules & Detections, and identify the most common processes appearing in alerts that are marked as false positives.
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: B

Question: 3

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 2 answers
Response:

A. Review the architecture of the tool to identify the cloud provider that hosts the tool.
B. Review the documentation to identify if default parsers exist for the tool, and determine whether the logs are supported and able to be ingested.
C. Identify the tool in the Google SecOps Marketplace, and verify support for the necessary actions in the workflow.
D. 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.
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: B,C

Question: 4

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.)
Response:

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: 5

You are responsible for identifying suspicious activity and security events in your organization's environment. You discover that some detection rules are being triggered for internal IP addresses in the 192.0.2.0/8 subnet that are causing false positive alerts.
You want to improve these detection rules. What should you add to the YARA-L detection rules?
Response:

A. net.ip_in_range_cidr(all Se.principal.ip, "192.0.2.0/8")
B. net.ip_in_range_cidr(any Se.principal.ip, "192.0.2.0/8")
C. not net.ip_in_range_cidr(all Se.principal.ip, "192.0.2.0/8")
D. not net.ip_in_range_cidr(any Se.principal.ip, "192.0.2.0/8")

Answer: D

Question: 6

You are conducting a proactive threat hunt in Google Security Operations (SecOps). You observe multiple login events with the same principal.user.userid field that originate from different countries within a short time window.
You need to validate whether the account has been compromised. What should you do?
Response:

A. Use the entity graph to correlate the user's risk score with linked assets, and review any active alerts.
B. Perform a YARA-L 2.0 search for login events and their associated principal.location.country field. Use an outcome field to aggregate the number of failed logins.
C. Perform a UDM search for login events, and pivot to group results by user and country of origin.
D. Run a YARA-L retrohunt rule that detects users who are logging in from multiple regions using multiple entity contexts.

Answer: C

Question: 7

Your organization is a Google Security Operations (SecOps) customer and monitors critical assets using a SIEM dashboard. You need to dynamically monitor the assets based on a specific asset tag. What should you do?
Response:

A. Ask Cloud Customer Care to add a custom filter to the dashboard.
B. Add a custom filter to the dashboard.
C. Copy an existing dashboard and add a custom filter.

D. Export the dashboard configuration to a file, modify the file to add a custom filter, and import the file into Google SecOps.

Answer: B

Question: 8

You are a security engineer at a managed security service provider (MSSP) that is onboarding to Google Security Operations (SecOps). You need to ensure that cases for each customer are logically separated. How should you configure this logical separation?
Response:

A. In Google SecOps SOAR settings, create a new environment for each customer.
B. In Google SecOps SOAR settings, create a role for each customer.
C. In Google SecOps SOAR settings, create a permissions group for each customer.
D. In Google SecOps Playbooks, create a playbook for each customer.

Answer: A

Question: 9

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?
Response:

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

Answer: C

Question: 10

You are responsible for selecting and prioritizing potential sources of data to integrate with Google Security Operations (SecOps). Your company has recently started using several Google Cloud services to increase security in its Google Cloud organization.
You need to determine which logs should be ingested into Google SecOps to reduce the effort required to write detections. What should you do?
Response:

A. Ingest Google Cloud Armor logs by using Cloud Logging.
B. Deploy a Bindplane agent to ingest event logs from Compute Engine VMs that provide endpoint visibility.
C. Integrate Security Command Center (SCC) into Google SecOps to ingest logs originating from the Google Cloud services.
D. Use Google Threat Intelligence to gain insight about threat group behavior and support threat hunting activities.

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/