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

You are planning log onboarding for a Google Security Operations (SecOps) SIEM deployment in a cloud-heavy enterprise environment. The detection engineering team is requesting log sources that support visibility into:
- User identity behavior
- Lateral movement
- Privilege escalation attempts
You need to determine which telemetry sources are ingested first. Which log source should you prioritize?

A. IAM logs
B. EDR logs
C. Network firewall logs
D. Cloud access security broker (CASB) logs

Answer: A

Question: 2

You have detected a suspicious access pattern in your Google Cloud environment using Google Security Operations (SecOps). In this pattern, a service account performs a sensitive IAM operation and within 15 minutes, a script is executed on an internal server that initiates an outbound network connection.
You need to create a solution that effectively detects this type of chained behavior, correlates the activity by the same user or service account, and ensures that detections do not fire on unrelated single events. Which detection strategy should you use?

A. Use a single-event YARA-L rule that matches on process creation and network activity from the same internal host.
B. Create a suppression rule to ignore frequent IAM operations unless a network IOC match also occurs.
C. Build a multi-event YARA-L rule with a 15-minute time window and use the principal.user.userid identity field to correlate the IAM API call with the process execution event.
D. Use the SecOps entity graph to monitor service account behavior and trigger alerts when high-severity nodes are linked.

Answer: C

Question: 3

Your organization recently onboarded Google Security Operations (SecOps) and configured an EDR integration in SOAR. After reviewing recent malware incidents, you determine that analysts are spending excessive time isolating infected endpoints, even with the existing EDR isolation capabilities. You want to create a new SOAR playbook that uses the most effective and direct approach. What should you do?

A. Create a playbook to automatically block malicious IP addresses and isolate network communication.
B. Develop a playbook to automatically trigger endpoint isolation when a malware alert is generated.
C. Configure a playbook to automatically send a notification to the affected user with instructions on how to remediate the malware.
D. Deploy SOAR Remote Agent to the endpoints, and configure the host to execute a PowerShell script that disables network adapters to isolate it from the network.

Answer: B

Question: 4

You are a security operations engineer in an enterprise that uses Google Security Operations (SecOps). Your organization recently faced a cybersecurity breach. You need to increase the threat analytics as quickly as possible. What should you do?

A. Enable curated detections to identify threats.
B. Design YARA-L detection rules based on Google SecOps Marketplace use cases.
C. Develop YARA-L detection rules that focus on threat intelligence.
D. Ingest data from a threat intelligence platform (TIP) into Google SecOps.

Answer: A

Question: 5

You scheduled a Google Security Operations (SecOps) report to export results to a BigQuery dataset in your Google Cloud project. The report executes successfully in Google SecOps, but no data appears in the dataset.
You confirmed that the dataset exists. How should you address this export failure?

A. Grant the Google SecOps service account the roles/iam.serviceAccountUser IAM role to itself.
B. Set a retention period for the BigQuery export.
C. Grant the user account that scheduled the report the roles/bigquery.dataEditor IAM role on the project.
D. Grant the Google SecOps service account the roles/bigquery.dataEditor IAM role on the dataset.

Answer: D

Question: 6

You are responsible for developing and configuring data ingestion in Google Security Operations (SecOps) for your organization. Your organization is using a prebuilt parser to parse a complex but stable and common log source. The parser is working correctly.
However, your organization now wants you to change the configuration to parse additional fields from the raw logs and map them to UDM fields. What should you do?

A. Design and develop a custom parser.
B. Apply any pending updates to the prebuilt parser.
C. Implement a parser extension on top of the prebuilt parser.
D. Implement middleware to modify the underlying data structure.

Answer: C

Question: 7

Your company recently started pulling JSON logs from a third-party system into Google Security Operations (SecOps). You noticed that some fields are missing, and you want to parse them into UDM fields as quickly as possible. What should you do?

A. Configure auto extraction to add the additional fields.
B. Create parser extensions using the no-code approach.
C. Create parser extensions using the code snippet approach.
D. Submit a parser improvement request to Cloud Customer Care.

Answer: B

Question: 8

Your team wants to improve Google Security Operations (SecOps) detection rules by integrating threat intelligence from the Applied Threat Intelligence (ATI) Fusion Feed. You need to automatically prioritize and respond to high-risk IOCs based on their threat context. What should you do?

A. Configure YARA-L detection rules to match IOCs only if they appear in the ATI Fusion Feed with a priority of “high” or “critical.”
B. Apply retrohunt to all IOC matches in the past 30 days to automatically adjust threat levels based on ATI confidence scores.
C. Use IOC rule templates from managed rule sets in Google SecOps that ingest and correlate with the ATI Fusion Feed in real time.
D. Assign an auto-escalation level to any rule using ATI indicators by configuring global IOC thresholds.

Answer: A

Question: 9

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?

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: 10

You are managing a Google Security Operations (SecOps) implementation for a regional customer. Your customer informs you that logs are appearing in the platform after a consistent six-hour delay.
After some research, you determine that there is a time zone issue in the raw logs. You want to fix this problem. What should you do?

A. Create a parser extension to correct the time zone.
B. Modify the default parser and include a default time zone.
C. Create a custom parser to correct the time zone.
D. Modify the Google SecOps UI settings to correct the time zone.

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/