DBCLOUD
EXAMS

QUESTIONS & ANSWERS

verified



Technology Provider: Google

Exam: Professional Security Operations Engineer

Number of questions in the database: 133

Exam Version: NOV.2026

Question #1Topic 1

You are responsible for identifying suspicious activity and security events at your organization. You have been asked to search in Google Security Operations (SecOps) for network traffic associated with an active HTTP backdoor that runs on TCP port 5555. You want to use the most effective approach to identify traffic originating from the server that is running the backdoor. What should you do?

A. Detect on events where network.ApplicationProtocol is HTTP.

B. Detect on events where target.port is 5555.

C. Detect on events where principal.port is 5555.

D. Detect on events where network.ip_protocol is TCP.

Correct Answer: C

Question #2Topic 1

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.

Correct Answer: C

https://dbcloud.academy/

Question #3Topic 1

Your organization uses Google Security Operations (SecOps). You discover frequent file downloads from a shared workspace within a short time window. You need to configure a rule in Google SecOps that identifies these suspicious events and assigns higher risk scores to repeated anomalies. What should you do?

A. Configure a rule that flags file download events with the highest risk score, regardless of time frame.

B. Create a frequency-based YARA-L detection rule that assigns a risk outcome score and is triggered when multiple suspicious downloads occur within a defined time frame.

C. Configure a single-event YARA-L detection rule that assigns a risk outcome score and is triggered when a user downloads a large number of files in 24 hours.

D. Enable default curated detections, and use automatic alerting for single file download events.

Correct Answer: B

Question #4Topic 1

You are implementing Google Security Operations (SecOps) at your organization. You discover that the current detection rules are too noisy. Due to the high volume of alerts, some true positives might be missed. You want to ingest additional context sources to reduce false positives in your security detections and to improve the overall positive ratio of the alerts. What should you do?

A. Ingest high-value asset (HVA) data from your configuration management database (CMDB) system to increase the priority of the alerts based on the sensitivity of the assets found in the detection rules.

B. Ingest dark web forum handlers from your threat intelligence system to match dark web principals within the detection rules.

C. Ingest IOCs from your threat intelligence system to validate the IP addresses, domains and hashes with the detection rules.

D. Ingest tactics, techniques, and procedures (TTPs) from your threat intelligence system to validate the processes and tools with the detection rules.

Correct Answer: A

https://dbcloud.academy/

Question #5Topic 1

You are developing a new detection rule in Google Security Operations (SecOps). You are defining the YARA-L logic that includes complex event, match, and condition sections. You need to develop and test the rule to ensure that the detections are accurate before the rule is migrated to production. You want to minimize impact to production processes. What should you do?

A. Develop the rule logic in the UDM search, review the search output to inform changes to filters and logic, and copy the rule into the Rules Editor.

B. Use Gemini in Google SecOps to develop the rule by providing a description of the parameters and conditions, and transfer the rule into the Rules Editor.

C. Develop the rule in the Rules Editor, define the sections the rule logic, and test the rule using the test rule feature.

D. Develop the rule in the Rules Editor, define the sections of the rule logic, and test the rule by setting it to live but not alerting. Run a YARA-L retrohunt from the rules dashboard.

Correct Answer: C

Question #6Topic 1

Your organization has recently acquired Company A, which has its own SOC and security tooling. You have already configured ingestion of Company A's security telemetry and migrated their detection rules to Google Security Operations (SecOps). You now need to enable Company A's analysts to work their cases in Google SecOps. You need to ensure that Company A's analysts: do not have access to any case data originating from outside of Company A. are able to re-purpose playbooks previously developed by your organization's employees.

You need to minimize effort to implement your solution. What is the first step you should take?

A. Acquire a second Google SecOps SOAR tenant for Company A.

B. Provision a new service account for Company A.

C. Define a new SOC role for Company A.

D. Create a Google SecOps SOAR environment for Company A.

Correct Answer: D

https://dbcloud.academy/

Question #7Topic 1

You have identified and isolated a new malware sample installed by an advanced threat group that you believe was developed specifically for an attack against your organization. You want to quickly and efficiently analyze this malware to get IOCs without alerting the threat group. What should you do?

A. Search for the threat group in Google Threat Intelligence.

B. Upload the malware to Google Threat Intelligence by using VirusTotal.

C. Upload the malware to Google Threat Intelligence by using Private Scanning.

D. Calculate the file checksum for the malware, and search for the checksum in GoogleThreat Intelligence by using VirusTotal.

Correct Answer: C

Question #8Topic 1

Your organization uses Cloud Identity as their identity provider (IdP) and is a Google Security Operations (SecOps) customer You need to grant a group of users access to the Google SecOps instance with read-only access to all resources, including detection engine rules. How should this be configured?

A. Create a Google Group and add the required users. Grant the roles/chronicle.Viewer IAM role to the group on the project associated with your Google SecOps Instance.

B. Create a Google Group and add the required users. Grant the roles/chronicle.limitedViewer IAM role to the group on the project associated with your Google SecOps instance.

C. Create a workforce identity pool at the organization level. Grant the roles/chronicle.editor IAM role to the principalSet://iam.googleapis.com/locations/global/workforcePools/POOL_ID/group/GROUP_ID principal set on the project associated with your Google SecOps instance.

D. Create a workforce identity pool at the organization level Grant the roles/chronicle.limitedViewer IAM role to the principalSet://iam.googleapis.com/locations/global/workforcePools/POOL_ID/group/GROUP_ID principal set on the project associated with your Google SecOps Instance.

Correct Answer: A

https://dbcloud.academy/