Vendor: Google

Exam Code: Professional-Security-Operations-Engineer

Exam Name: Professional Security Operations Engineer

Version: DEMO

QUESTION 1
You are reviewing the security analyst team's playbook action process. Currently, security analysts navigate to the Playbooks tab in Google Security Operations (SecOps) for each alert and manually run steps assigned to a user. You need to present all actions from alerts awaiting user input in one location for the analyst to execute. What should you do?

A. Enable approval links in the manual action and display them as clickable links to the user in a HTML widget in the Default Case View tab.
B. Add a general insight in your playbook to display manual action details to the user.
C. Use the Pending Actions widget in the Default Case View in settings.
D. Create an Alert View with the playbook that incorporates the Pending Actions widget.

Answer: C
Explanation:
The correct approach is to use the Pending Actions widget in the Default Case View. This widget consolidates all manual playbook actions that require analyst input, allowing them to be executed from a single location. This streamlines the workflow, reduces manual navigation, and ensures analysts don't miss pending steps across multiple alerts.

QUESTION 2
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 log time zone issue. You want to fix this problem. What should you do?

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

Answer: B
Explanation:
The correct fix is to create a parser extension to correct the time zone. Parser extensions let you adjust specific fields, such as timestamps, without modifying the default parser. This resolves ingestion delays caused by time zone mismatches while maintaining the integrity and upgrade compatibility of the default parser.

QUESTION 3
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?

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

Explanation:
The most efficient method is to run a UDM search and use aggregations on process-related UDM fields. This allows you to quickly identify the most common processes and applications across all servers, providing accurate data to establish baselines and exclusion lists without relying only on alerts or dashboards.

QUESTION 4
You work for an organization that uses Security Command Center (SCC) with Event Threat Detection (ETD) enabled. You need to enable ETD detections for data exfiltration attempts from designated sensitive Cloud Storage buckets and BigQuery datasets. You want to minimize Cloud Logging costs. What should you do?

A. Enable "data read" audit logs only for the designated sensitive Cloud Storage buckets and BigQuery datasets.
B. Enable "data read" and "data write" audit logs only for the designated sensitive Cloud Storage buckets and BigQuery datasets.
C. Enable "data read" and "data write" audit logs for all Cloud Storage buckets and BigQuery datasets throughout the organization.
D. Enable VPC Flow Logs for the VPC networks containing resources that access the sensitive Cloud Storage buckets and BigQuery datasets.

Answer: A
Explanation:
To detect data exfiltration attempts from sensitive Cloud Storage buckets and BigQuery datasets using ETD, you only need “data read” audit logs. These logs capture access and read events (which indicate potential exfiltration). Enabling them only for the designated sensitive resources minimizes Cloud Logging costs while still providing the necessary visibility for detections.

QUESTION 5
Your company uses Security Command Center (SCC) and Google Security Operations (SecOps). Last week, an attacker attempted to establish persistence by generating a key for an unused service account. You need to confirm that you are receiving alerts when keys are created for unused service accounts and that newly created keys are automatically deleted. You want to minimize the amount of manual effort required. What should you do?

A. Generate a YARA-L rule in Google SecOps that detects when a service account key is created. Using the built-in IDE, create a custom action in Google SecOps SOAR that deletes the service account key.
B. Use the Initial Access: Dormant Service Account Key Created finding from SCC, and ingest this finding into Google SecOps. Create a custom action in Google SecOps SOAR that is triggered on this finding. Use the built-in IDE to build code to delete the service account key.
C. Configure a Cloud Logging sink to write logs to a Pub/Sub topic that filters for the methodName: "google.iam.admin.v1.CreateServiceAccountKey" field. Create a Cloud Run function that subscribes to the Pub/Sub topic and deletes the service account key.
D. Use the Initial Access: Dormant Service Account Key Created finding from SCC, and write this finding to a Pub/Sub topic. Create a Cloud Run function that subscribes to the Pub/Sub topic and deletes the service account key.

Answer: B
Explanation:
The most efficient solution is to use the built-in SCC detection "Initial Access: Dormant Service Account Key Created", ingest the finding into Google SecOps, and automate the response with a

custom SOAR action that deletes the key. This leverages existing SCC findings for accurate detection, integrates directly with Google SecOps for centralized alerting, and minimizes manual effort by automating remediation.

QUESTION 6
Your company recently adopted Security Command Center (SCC) but is not using Google Security Operations (SecOps). Your organization has thousands of active projects. You need to detect anomalous behavior in your Google Cloud environment by windowing and aggregating data over a given time period, based on specific log events or advanced calculations. You also need to provide an interface for analysts to triage the alerts. How should you build this capability?

A. Send the logs to Cloud SQL, and run a scheduled query against these events using a Cloud Run scheduled job. Configure an aggregated log filter to stream event-driven logs to a Pub/Sub topic. Configure a trigger to send an email alert when new events are sent to this feed.
B. Sink the logs to BigQuery, and configure Cloud Run functions to execute a periodic job and generate normalized alerts in a Pub/Sub topic for findings. Use log-based metrics to generate event-driven alerts and send these alerts to the Pub/Sub topic. Write the alerts as findings using the SCC API.
C. Use log-based metrics to generate event-driven alerts for the detection scenarios. Configure a Cloud Monitoring alert policy to send email alerts to your security operations team.
D. Create a series of aggregated log sinks for each required finding, and send the normalized findings as JSON files to Cloud Storage. Use the write event to generate an alert.

Answer: B
Explanation:
The correct approach is to sink logs to BigQuery, where you can perform windowing and advanced aggregations over time. Then, use Cloud Run functions to periodically query BigQuery and generate normalized alerts published to a Pub/Sub topic. From there, alerts can be written back into SCC as findings via the SCC API, giving analysts a central interface for triage. This architecture supports large-scale environments, advanced calculations, and efficient integration with SCC.

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?

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
Explanation:
In Google SecOps, you can add a custom filter directly to the SIEM dashboard to dynamically monitor assets based on a specific asset tag. This approach is straightforward, requires no external intervention, and ensures that the dashboard updates automatically as assets with the tag change over time.

QUESTION 8

A business unit in your organization plans to use Vertex AI to develop models within Google Cloud. The security team needs to implement detective and preventative guardrails to ensure that the environment meets internal security control requirements. How should you secure this environment?

A. Implement Assured Workloads by creating a folder for the business unit and assigning the relevant control package.
B. Implement preconfigured and custom organization policies to meet the control requirements. Apply these policies to the business unit folder.
C. Create a policy bundle representing the control requirements using Rego. Implement these policies using Workload Manager. Scope this scan to the business unit folder.
D. Create a posture consisting of predefined and custom organization policies and predefined and Security Health Analytics (SHA) custom modules. Scope this posture to the business unit folder.

Answer: D
Explanation:
The correct approach is to create a posture in SCC that combines predefined and custom organization policies with predefined and custom Security Health Analytics (SHA) modules, and then scope it to the business unit folder. This ensures both preventative guardrails (organization policies) and detective guardrails (SHA findings) are enforced for the Vertex AI environment, aligning with internal security control requirements.

QUESTION 9
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
Explanation:
The best solution is to create a Cloud Monitoring notification with a metric-absence condition for each collector_id. A metric-absence alert triggers when expected ingestion metrics are missing within a defined period (e.g., five minutes), which quickly identifies silent sources or failed collectors. This provides near real-time detection of ingestion health issues in the SecOps pipeline.

QUESTION 10
A Google Security Operations (SecOps) detection rule is generating frequent false positive alerts. The rule was designed to detect suspicious Cloud Storage enumeration by triggering an alert whenever the storage.objects.list API operation is called using the api.operation UDM field. However, a legitimate backup automation tool that uses the same API, causing the rule to fire unnecessarily. You need to reduce these false positives from this trusted backup tool while still detecting potentially malicious usage. How should you modify the rule to improve its accuracy?

A. Add principal.user.email != "backup-bot@foobaa.com" to the rule condition to exclude the automation account.
B. Replace api.operation with api.service_name = "storage.googleapis.com" to narrow the detection scope.
C. Convert the rule into a multi-event rule that looks for repeated API calls across multiple buckets.
D. Adjust the rule severity to `LOW` to deprioritize alerts from automation tools.

Answer: A
Explanation:
The most accurate way to reduce false positives is to exclude the known trusted backup automation account by adding a condition such as principal.user.email != "backup-bot@foobaa.com". This keeps the rule active for all other accounts, ensuring you still detect suspicious or malicious Cloud Storage enumeration while preventing unnecessary alerts from legitimate automation.

QUESTION 11
Your company uses Google Security Operations (SecOps) Enterprise and is ingesting various logs. You need to proactively identify potentially compromised user accounts. Specifically, you need to detect when a user account downloads an unusually large volume of data compared to the user's established baseline activity. You want to detect this anomalous data access behavior using the least amount of effort. What should you do?

A. Inspect Security Command Center (SCC) default findings for data exfiltration in Google SecOps.
B. Create a log-based metric in Cloud Monitoring, and configure an alert to trigger if the data downloaded per user exceeds a predefined limit. Identify users who exceed the predefined limit in Google SecOps.
C. Develop a custom YARA-L detection rule in Google SecOps that counts download bytes per user per hour and triggers an alert if a threshold is exceeded.
D. Enable curated detection rules for User and Endpoint Behavioral Analytics (UEBA), and use the Risk Analytics dashboard in Google SecOps to identify metrics associated with the anomalous activity.

Answer: D
Explanation:
The most effective and least effort solution is to enable curated UEBA (User and Endpoint Behavioral Analytics) detection rules in Google SecOps and use the Risk Analytics dashboard. UEBA automatically establishes user baselines and detects anomalies such as unusually large data downloads, removing the need to manually define thresholds or build custom rules.

QUESTION 12
Your organization uses Security Command Center (SCC) and relies on Compute Engine instances to run business-critical workloads. SCC has flagged a particular instance for exhibiting a high volume of outbound network connections to geographically diverse and unknown IP addresses. You need to determine whether the instance has been compromised by malware. What should you do?

A. Examine the IAM roles assigned to the service account that are associated with the instance. Revoke any permissions that could have facilitated malware installation.
B. Review the Google Cloud Service Health dashboard to identify any ongoing Google Cloud platform incidents that could be causing unusual network traffic from the instance.
C. Disable and re-enable the instances' network interface and determine whether the unusual

network behavior is resolved.

D. Analyze Event Threat Detection findings. Review the events and the outbound network connections associated with the instance.

Answer: D
Explanation:
The correct action is to analyze Event Threat Detection (ETD) findings in SCC, which provide detailed insights into suspicious activities such as unusual outbound network connections. Reviewing these findings allows you to correlate the flagged activity with the instance's outbound traffic patterns, helping determine whether the instance is compromised by malware.

QUESTION 13
Your company wants to enhance its detection capabilities to prevent insider threat incidents. You need to be alerted when a privileged Google Group is modified to allow access to the general public. You need to identify and enable the optimal log source, and configure the alert. What should you do?

A. Enable Google Drive log events. Create a reporting rule that triggers when a file sharing event occurs with the visibility set to anyone with the link.
B. Enable VPC Flow Logs for the default VPC network. Configure a log-based alert in Cloud Logging to detect anomalous traffic patterns associated with Google Groups API endpoints.
C. Enable IAM Admin Activity audit logs, and export the logs to Google Security Operations (SecOps). Write a YARA-L rule in Google SecOps to capture any changes to relevant IAM policies.
D. Enable data sharing for Google Workspace Admin Audit logs, and ensure that Event Threat Detection is enabled for your organization.

Answer: D
Explanation:
To detect insider threats involving Google Group privilege modifications, you need Google Workspace Admin Audit logs, which capture group membership and sharing changes. By enabling data sharing of these logs with SCC and ensuring Event Threat Detection (ETD) is enabled, SCC will automatically generate findings for risky modifications, such as making a privileged group publicly accessible. This provides the optimal log source and automated alerting with minimal effort.

QUESTION 14
You are using Google Security Operations (SecOps) to investigate suspicious activity linked to a specific user. You want to identify all assets the user has interacted with over the past seven days to assess potential impact. Your need to understand the user's relationships to endpoints, service accounts, and cloud resources. How should you identify user-to-asset relationships in Google SecOps?

A. Use the Raw Log Scan view to group events by asset ID.
B. Query for hostnames in UDM Search and filter the results by user.
C. Generate an ingestion report to identify sources where the user appeared in the last seven days.
D. Run a retrohunt to find rule matches triggered by the user.

Answer: B
Explanation:
The correct approach is to query UDM Search for hostnames (or other asset identifiers) and filter results by the specific user. UDM normalizes logs into a common schema, allowing you to trace

the user's interactions across endpoints, service accounts, and cloud resources within the seven-day window. This provides a comprehensive view of user-to-asset relationships for impact assessment.

QUESTION 15
Your organization recently acquired a Google Security Operations (SecOps) Enterprise Plus license. Your organization is already ingesting Cloud Audit Logs, firewall logs, proxy logs and endpoint logs, but there are no threat intelligence feeds being ingested into your Google SecOps environment. You need to design and deploy a solution that alerts your team quickly if an IOC of an active breach is observed in your environment. What should you do?

A. Write, enable, and configure alerting on a custom multi-event rule.
B. Write, enable, and configure alerting on a custom single-event rule.
C. Enable and configure alerting for relevant curated detection rule sets.
D. Create and schedule a dashboard to send periodic summaries of the active breach IOCs and their associated events.

Answer: C
Explanation:
The fastest and most effective way to alert on IOCs in Google SecOps is to enable and configure curated detection rule sets. These curated rules are maintained by Google and automatically updated with the latest threat intelligence, ensuring that if an IOC from an active breach is observed in your ingested logs, your team will receive alerts without the need to manually create or maintain custom rules.

QUESTION 16
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?

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
Explanation:
On-premises firewalls cannot send logs directly to Google SecOps. The correct approach is to deploy a third-party agent (such as Bindplane or NXLog) in your on-premises environment and configure the firewalls to forward Syslog data to that agent. The agent then reliably forwards the logs to Google SecOps for ingestion.

Thank You for Trying Our Product

Braindump2go Certification Exam Features:

★ More than **99,900** Satisfied Customers Worldwide.

★ Average **99.9%** Success Rate.

★ **Free Update** to match latest and real exam scenarios.

★ **Instant Download** Access! No Setup required.

★ Questions & Answers are downloadable in **PDF** format and **VCE** test engine format.

★ Multi-Platform capabilities - **Windows, Laptop, Mac, Android, iPhone, iPod, iPad**.

★ **100%** Guaranteed Success or **100%** Money Back Guarantee.

★ **Fast**, helpful support **24x7**.

View list of all certification exams: http://www.braindump2go.com/all-products.html

10% Discount Coupon Code: **ASTR14**