Hot Security-Operations-Engineer Questions - Security-Operations-Engineer Valid Test Question

Our Security-Operations-Engineer real exam has three packages, which meets your different demands. They are PDF version, online test engine and windows software of the Security-Operations-Engineer learning guide. The contents are all identical. But the displays are totally different and you may choose the right one according to your interest and hobbies. Every version of our Security-Operations-Engineer Real Exam is worthy and affordable for you to purchase. Let us fight for our bright future. You are bound to win if you are persistent.

Google Security-Operations-Engineer Exam Syllabus Topics:

Topic	Details
Topic 1	• Platform Operations: This section of the exam measures the skills of Cloud Security Engineers and covers the configuration and management of security platforms in enterprise environments. It focuses on integrating and optimizing tools such as Security Command Center (SCC), Google SecOps, GTI, and Cloud IDS to improve detection and response capabilities. Candidates are assessed on their ability to configure authentication, authorization, and API access, manage audit logs, and provision identities using Workforce Identity Federation to enhance access control and visibility across cloud systems.
Topic 2	• Incident Response: This section of the exam measures the skills of Incident Response Managers and assesses expertise in containing, investigating, and resolving security incidents. It includes evidence collection, forensic analysis, collaboration across engineering teams, and isolation of affected systems. Candidates are evaluated on their ability to design and execute automated playbooks, prioritize response steps, integrate orchestration tools, and manage case lifecycles efficiently to streamline escalation and resolution processes.
Topic 3	• Detection Engineering: This section of the exam measures the skills of Detection Engineers and focuses on developing and fine-tuning detection mechanisms for risk identification. It involves designing and implementing detection rules, assigning risk values, and leveraging tools like Google SecOps Risk Analytics and SCC for posture management. Candidates learn to utilize threat intelligence for alert scoring, reduce false positives, and improve rule accuracy by integrating contextual and entity-based data, ensuring strong coverage against potential threats.

>> Hot Security-Operations-Engineer Questions <<

Security-Operations-Engineer Valid Test Question & Security-Operations-Engineer Latest Braindumps Ppt

Our Security-Operations-Engineer exam questions are compiled by experts and approved by authorized personnel and boost varied function so that you can learn Security-Operations-Engineer test torrent conveniently and efficiently. We provide free download and

tryout before your purchase. Our Security-Operations-Engineer exam questions just need students to spend 20 to 30 hours practicing on the platform which provides simulation problems, can let them have the confidence to pass the Security-Operations-Engineer Exam, so little time great convenience for some workers. It must be your best tool to pass your Security-Operations-Engineer exam and achieve your target.

Google Cloud Certified - Professional Security Operations Engineer (PSOE) Exam Sample Questions (Q141-Q146):

NEW QUESTION # 141
Your organization is a Google Security Operations (SecOps) customer. The compliance team requires a weekly export of case resolutions and SLA metrics of high and critical severity cases over the past week. The compliance team's post-processing scripts require this data to be formatted as tabular data in CSV files, zipped, and delivered to their email each Monday morning. What should you do?

- A. Use statistics in search, and configure a Google SecOps SOAR job to format and send the report.
- B. Generate a report in SOAR Reports, and schedule delivery of the report.
- C. Build a detection rule with outcomes, and configure a Google SecOps SOAR job to format and send the report.
- D. Build an Advanced Report in SOAR Reports, and schedule delivery of the report.

Answer: D

Explanation:
Comprehensive and Detailed Explanation
The correct solution is Option C. Google SecOps SOAR has a specific feature designed for this exact use case: Advanced Reports. The standard "SOAR Reports" (Option A) are pre-canned dashboard-style reports (e.g., Management - SOC Status). However, the "Advanced Reports" feature (built on Looker) provides a powerful, flexible interface for building highly customized, tabular reports based on case data. This allows an administrator to specifically query for case resolutions and SLA metrics, and filter them by priority = High OR Critical.
Most importantly, the Advanced Reports feature has a built-in scheduler. This scheduler can be configured to run the report at a specific cadence (e.g., "Weekly on Monday at 9:00 AM"), send it to a list of email recipients, and attach the data in the required format, including CSV and as a zipped file.
Option B is incorrect because detection rules create alerts, they don't report on case metrics. Option D is incorrect because it mixes the SIEM search function with a SOAR job, which is an overly complex and unnecessary way to query case data that is already structured within the SOAR module.
Exact Extract from Google Security Operations Documents:
Explore advanced SOAR reports: The default advanced SOAR reports are a set of dashboards and reports to help track SOC performance, case handling, analyst workload, and automation efficiency. These reports provide both high-level and detailed insights across your environments.1 SLA Monitoring: Use Triage Time and SLA Met flag to monitor SLA compliance and improve case handling.
Manage advanced reports: You can create, edit, duplicate, share, download, and delete advanced reports.
Schedule a report:
* Select the report you want to schedule.
* Select the Scheduler tab and click Add.
* In the New Schedule dialog, click the Enable toggle to turn on scheduling and enter the required information (e.g., weekly, Monday, email recipients).
* You can select the delivery format, including CSV and ZIP attachments.
References:
Google Cloud Documentation: Google Security Operations > Documentation > Monitor and report > SOAR reports > Use Looker Explores in SOAR reports (Advanced Reports) Google Cloud Documentation: Google Security Operations > Documentation > Monitor and report > SOAR reports > Explore SOAR reports

NEW QUESTION # 142
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.)

- A. 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.
- B. Perform a raw log search across the logs for domains with low prevalence that were first seen in the last 30 days.
- C. Perform a UDM search across the logs for domains with geolocations 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. Perform a UDM search across the logs for domains with low prevalence that were first seen in the last 30 days.

Answer: D,E

Explanation:
Running a UDM search for low-prevalence domains first seen in the last 30 days helps uncover potentially anomalous or malicious domains, since attackers often use newly registered or rarely seen domains for C2 or exfiltration.
Using the Risk Analytics dashboard allows you to identify domains with higher normalized risk scores. Drilling into those entities helps validate whether they are new, rare, or potentially tied to malicious activity.

NEW QUESTION # 143
You are implementing Google Security Operations (SecOps) for your organization. Your organization has their own threat intelligence feed that has been ingested to Google SecOps by using a native integration with a Malware Information Sharing Platform (MISP). You are working on the following detection rule to leverage the command and control (C2) indicators that were ingested into the entity graph.
What code should you add in the detection rule to filter for the domain IOCS?

- A. $ioc.graph.metadata.entity_type = "DOMAIN_NAME"
  Sioc.graph.metadata.source_type = "GLOBAL_CONTEXT"
- B. $ioc.graph.metadata.entity_type = "D0MAIN_NAME"
  $ioc.graph.metadata.source_type = MDERIVED_CONTEXT"
- C. $ioc.graph.metadata.entity_type = MDOMAIN_NAME"
  $ioc.graph.metadata.scurce_type = "ElfeITYj