Security-Operations-Engineer Exam Bootcamp & Security-Operations-Engineer Latest Dumps & Security-Operations-Engineer Study Materials

AI SECURITY ENGINEER

MINI BOOTCAMP

→ 15 Eylül | Yapay Zekaya Genel Bakış

→ 17 Eylül | Siber Güvenliğe Genel Bakış

→ 22 Eylül | OWASP Web Top-10

→ 24 Eylül | Deep Learning Temelleri (Uygulamalı)

→ 29 Eylül | Deep Learning ile Siber Güvenlik Uygulaması Geliştirmek

→ 1 Ekim | OWASP Machine Learning Security

P.S. Free 2026 Google Security-Operations-Engineer dumps are available on Google Drive shared by ActualPDF: https://drive.google.com/open?id=1ZlvlArKg0fiEK_WBFETadd0EWRmoKW2h

Desktop Google Security-Operations-Engineer Practice Exam Software is a one-of-a-kind and very effective software developed to assist applicants in preparing for the Security-Operations-Engineer certification test. The Desktop Security-Operations-Engineer Practice Exam Software that we provide includes a self-assessment feature that enables you to test your knowledge by taking simulated tests and evaluating the results. You can acquire a sense of the Security-Operations-Engineer software by downloading a free trial version before deciding whether to buy it.

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	• Threat Hunting: This section of the exam measures the skills of Cyber Threat Hunters and emphasizes proactive identification of threats across cloud and hybrid environments. It tests the ability to create and execute advanced queries, analyze user and network behaviors, and develop hypotheses based on incident data and threat intelligence. Candidates are expected to leverage Google Cloud tools like BigQuery, Logs Explorer, and Google SecOps to discover indicators of compromise (IOCs) and collaborate with incident response teams to uncover hidden or ongoing attacks.

Topic 3	- 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 4	- Data Management: This section of the exam measures the skills of Security Analysts and focuses on effective data ingestion, log management, and context enrichment for threat detection and response. It evaluates candidates on setting up ingestion pipelines, configuring parsers, managing data normalization, and handling costs associated with large-scale logging. Additionally, candidates demonstrate their ability to establish baselines for user, asset, and entity behavior by correlating event data and integrating relevant threat intelligence for more accurate monitoring.

>> Security-Operations-Engineer Passing Score <<

Your Investment with ActualPDF Google Security-Operations-Engineer Exam Questions is Secured

With our Security-Operations-Engineer practice materials, you don't need to spend a lot of time and effort on reviewing and preparing. For everyone, time is precious. Office workers and mothers are very busy at work and home; students may have studies or other things. Using Security-Operations-Engineer guide torrent, you only need to spend a small amount of time to master the core key knowledge to pass the Security-Operations-Engineer Exam and get a Security-Operations-Engineercertificate. It is proved that if you spend 20 to 30 hours to study our Security-Operations-Engineer exam questions, it is easy for you to pass the Security-Operations-Engineer exam.

Google Cloud Certified - Professional Security Operations Engineer (PSOE) Exam Sample Questions (Q123-Q128):

NEW QUESTION # 123
You recently joined a company that uses Google Security Operations (SecOps) with Applied Threat Intelligence enabled. You have alert fatigue from a recent red team exercise, and you want to reduce the amount of time spent sifting through noise. You need to filter out IoCs that you suspect were generated due to the exercise. What should you do?

- A. Navigate to the IOC Matches page. Review IoCs with an Indicator Confidence Score (IC-Score) label >= 80%.
- B. Navigate to the IOC Matches page. Identify and mute the IoCs from the red team exercise.
- C. Filter IoCs with an ingestion time that matches the time period of the red team exercise.
- D. Ask Gemini to provide a list of IoCs from the red team exercise.

Answer: B

Explanation:
The IOC Matches page is the central location in Google Security Operations (SecOps) for reviewing all IoCs that have been automatically correlated against your organization's UDM data. This page is populated by the Applied Threat Intelligence service, which includes feeds from Google, Mandiant, and VirusTotal.
When security exercises (like red teaming or penetration testing) are conducted, they often use known malicious tools or infrastructure that will correctly trigger IoC matches, creating "noise" and contributing to alert fatigue. The platform provides a specific function to manage this: muting.
An analyst can navigate to the IOC Matches page, use filters (such as time, as mentioned in Option B) to identify the specific IoCs associated with the red team exercise, and then select the Mute action for those IoCs. Muting is the correct operational procedure for suppressing known-benign or exercise-related IoCs.
This action prevents them from appearing in the main view and contributing to noise, while preserving the historical record of the match. Option D is a prioritization technique, not a suppression one.
(Reference: Google Cloud documentation, "View IoCs using Applied Threat Intelligence"; "View alerts and IoCs"; "Mute or unmute IoC") Here is the formatted answer as requested.

NEW QUESTION # 124

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 custom parser to correct the time zone.
- C. Modify the UI settings to correct the time zone.
- D. Create a parser extension to correct the time zone.

Answer: D

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.

NEW QUESTION # 125

You are the lead engineer on your organization's incident response team. You are running CrowdStrike Falcon and SentinelOne to protect the Windows devices in different regions of your organization. You are ingesting the following logs into Google Security Operations (SecOps):

- Azure AD Directory Audit (AZURE_AD_AUDIT)
- Crowdstrike Falcon (CS_EDR)
- Microsoft Sysmon (WINDOWS_SYSMON)
- SentinelOne (SENTINEL_EDR)
- Windows Event (WINEVTLOG)

You notice that a high volume of ransomware incidents are impacting your team's SLAs. You need to automate the response to ransomware on Windows devices. How should you automate the detection and containment of ransomware incidents? (Choose two.)

- A. Enable the Risk Analytics for User and Endpoint Behavioral Analytics (UEBA) category in curated detections to detect peer group-based anomalous behavior and suspicious actions.
- B. Install a SOAR remote agent on each Windows device for endpoint containment actions. Create a playbook to contain impacted Windows devices based on curated detections.
- C. Install SOAR EDR jobs to execute remote endpoint containment actions. Create a playbook to contain impacted Windows devices based on curated detections.
- D. Enable the Windows Threats category in curated detections to detect the latest Windows threats.
- E. Install SOAR EDR integrations for endpoint containment actions. Create a playbook to contain impacted Windows devices based on curated detections.

Answer: D,E

Explanation:

Enabling the Windows Threats category in curated detections ensures that the latest ransomware and other Windows-specific threats are automatically detected without creating custom rules, improving detection speed.

Installing SOAR EDR integrations allows automated containment actions (e.g., isolating impacted endpoints). Creating a playbook based on these curated detections automates response to ransomware incidents, reducing SLA impact and manual effort.

NEW QUESTION # 126

You are configuring a new integration in Google Security Operations (SecOps) to perform enrichment actions in playbooks. This enrichment technology is located in a private data center that does not allow inbound network connections. You need to connect your Google SecOps instance to the integration. What should you do?

- A. Create a forwarder in the private data center. Configure an instance of the integration to run on the forwarder.
- B. Query the enrichment source in the private data center and upload the results to the case wall in Google SecOps.
- C. Create a remote agent in the private data center. Configure an instance of the integration to run on a remote agent in Google SecOps.

- D. Create a network route in Google Cloud to the private data center.

Answer: C

Explanation:
The correct approach is to create a remote agent in the private data center and configure the integration to run on that agent. Remote agents can initiate outbound connections to Google SecOps, enabling playbook enrichment without requiring inbound network access, which adheres to the private data center's network restrictions.

NEW QUESTION # 127
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 = ,'D0MAIN_NAME*'
  $ioc.graph.metadata.source type = "source type unspecified"
- B. $ioc.graph.metadata.entity_type = MDOMAIN_NAME"
  $ioc.graph.metadata.scurce_type = "ElfelTYj