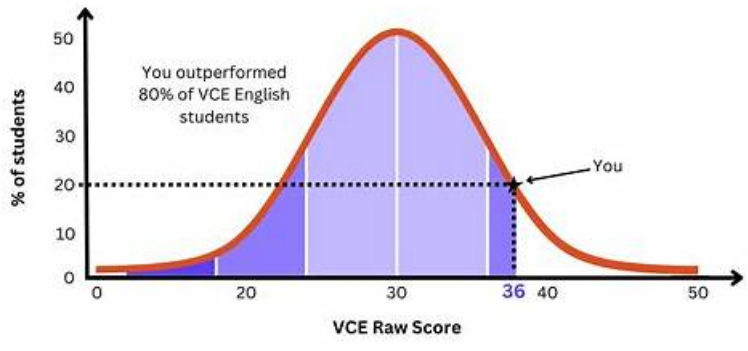
Test Security-Operations-Engineer Questions Vce, Test Security-Operations-Engineer Result



BTW, DOWNLOAD part of PrepAwayETE Security-Operations-Engineer dumps from Cloud Storage: https://drive.google.com/open?id=1KsyzMwyfpN193-ebqIOKAAFd5-6rpAvG

You can take advantage of several perks if you buy PrepAwayETE's bundle package of Google Security-Operations-Engineer dumps. The bundle package is cost-effective and includes all three formats of Google Cloud Certified - Professional Security Operations Engineer (PSOE) Exam exam preparation material Google Security-Operations-Engineer PDF Dumps Questions Answers, and Google Security-Operations-Engineer Practice Test software (online and offline). Google Security-Operations-Engineer Dumps are worth trying while preparing for the exam. You will be sure of what Google Security-Operations-Engineer exam questions will be asked in the exam.

Google Security-Operations-Engineer Exam Syllabus Topics:

Topic	Details
Topic 1	• Monitoring and Reporting: This section of the exam measures the skills of Security Operations Center (SOC) Analysts and covers building dashboards, generating reports, and maintaining health monitoring systems. It focuses on identifying key performance indicators (KPIs), visualizing telemetry data, and configuring alerts using tools like Google SecOps, Cloud Monitoring, and Looker Studio. Candidates are assessed on their ability to centralize metrics, detect anomalies, and maintain continuous visibility of system health and operational performance.
Topic 2	• 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 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	• 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.

Topic 5	• 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.

Test Security-Operations-Engineer Result - Latest Security-Operations-Engineer Exam Tips

It is acknowledged that high-quality service after sales plays a vital role in enhancing the quality of our Security-Operations-Engineer learning engine. Therefore, we, as a leader in the field specializing in the Security-Operations-Engineer exam material especially focus on the service after sales. In order to provide the top service on our Security-Operations-Engineer training prep, our customer agents will work 24/7. So if you have any doubts about the Security-Operations-Engineerstudy guide, you can contact us by email or the Internet at any time you like.

Google Cloud Certified - Professional Security Operations Engineer (PSOE) Exam Sample Questions (Q76-Q81):

NEW QUESTION # 76
You received an alert from Container Threat Detection that an added binary has been executed in a business critical workload. You need to investigate and respond to this incident. What should you do? (Choose two.)

- A. Review the finding, quarantine the cluster containing the running pod, and delete the running pod to prevent further compromise.
- B. Notify the workload owner. Follow the response playbook, and ask the threat hunting team to identify the root cause of the incident.
- C. Silence the alert in the Security Command Center (SCC) console, as the alert is a low severity finding.
- D. Review the finding, investigate the pod and related resources, and research the related attack and response methods.
- E. Keep the cluster and pod running, and investigate the behavior to determine whether the activity is malicious.

Answer: B,D

Explanation:
The correct response involves both notifying the workload owner and following the response playbook to ensure coordinated incident handling, and reviewing the finding while investigating the pod and related resources to understand the attack and determine the appropriate remediation. This approach ensures proper communication, structured incident response, and thorough technical investigation without prematurely deleting or silencing critical evidence.

NEW QUESTION # 77
Your organization's Google Security Operations (SecOps) tenant is ingesting a vendor's firewall logs in its default JSON format using the Google-provided parser for that log. The vendor recently released a patch that introduces a new field and renames an existing field in the logs. The parser does not recognize these two fields and they remain available only in the raw logs, while the rest of the log is parsed normally. You need to resolve this logging issue as soon as possible while minimizing the overall change management impact. What should you do?

- A. Use the web interface-based custom parser feature in Google SecOps to copy the parser, and modify it to map both fields to UDM.
- B. Deploy a third-party data pipeline management tool to ingest the logs, and transform the updated fields into fields supported by the default parser.
- C. Use the Extract Additional Fields tool in Google SecOps to convert the raw log entries to additional fields.
- D. Write a code snippet, and deploy it in a parser extension to map both fields to UDM.

Answer: C

Explanation:
The quickest and lowest-impact solution is to use the Extract Additional Fields tool in Google SecOps. This allows you to map the new and renamed fields from the raw logs into UDM fields without modifying the default parser or deploying custom code, ensuring the logs are fully parsed and available for downstream detections.

NEW QUESTION # 78
An organization detects a successful login to a Google Cloud IAM user from an unfamiliar country, followed by the creation of multiple new service account keys within minutes. No malware alerts are triggered. What is the MOST appropriate immediate action?

- A. Revoke active credentials, disable the compromised identity, and initiate an incident response
- B. Wait for evidence of data access
- C. Rotate only the affected user's password
- D. Disable the service accounts and continue monitorin

Answer: A

Explanation:
Rapid creation of service account keys after anomalous login strongly indicates identity compromise. Immediate containment is required to prevent persistence and escalation.

NEW QUESTION # 79
You are a SOC manager guiding an implementation of your existing incident response plan (IRP) into Google Security Operations (SecOps). You need to capture time duration data for each of the case stages. You want your solution to minimize maintenance overhead. What should you do?

- A. Configure Case Stages in the Google SecOps SOAR settings, and use the Change Case Stage action in your playbooks that captures time metrics when the stage changes.
- B. Configure a detection rule in SIEM Rules & Detections to include logic to capture the event fields for each case with the relevant stage metrics.
- C. Create a Google SecOps dashboard that displays specific actions that have been run, identifies which stage a case is in, and calculates the time elapsed since the start of the case.
- D. Write a job in the IDE that runs frequently to check the progress of each case and updates the notes with timestamps to reflect when these changes were identified.

Answer: A

Explanation:
This requirement is a core, out-of-the-box feature of the Google SecOps SOAR platform. The solution with the minimal maintenance overhead is always the native, built-in one. The platform is designed to measure SOC KPIs (like MTTR) by tracking Case Stages.
A SOC manager first defines their organization's incident response stages (e.g., "Triage," "Investigation," "Remediation") in the SOAR settings. Then, as playbooks are built, the Change Case Stage action is added to the workflow. When a playbook runs, it triggers this action, and the SOAR platform automatically timestamps the exact moment a case transitions from one stage to the next.
This creates the precise time-duration data needed for metrics. This data is then automatically available for the built-in dashboards and reporting tools (as mentioned in Option A, which is the result of Option B). Option D (custom IDE job) and Option C (detection rule) are incorrect, high-maintenance, and non-standard ways to accomplish a task that is a fundamental feature of the SOAR platform.
(Reference: Google Cloud documentation, "Google SecOps SOAR overview"; "Get insights from dashboards and reports"; "Manage playbooks")

NEW QUESTION # 80
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. Ingest data from a threat intelligence platform (TIP) into Google SecOps.

- B. Enable curated detections to identify threats.
- C. Develop YARA-L detection rules that focus on threat intelligence.
- D. Design YARA-L detection rules based on Google SecOps Marketplace use cases.

Answer: B

Explanation:
The fastest way to increase threat analytics in Google SecOps after a breach is to enable curated detections. These are prebuilt, continuously updated detection rules maintained by Google that provide immediate coverage against a wide range of threats, requiring no custom development and delivering quick improvements in visibility and response.

NEW QUESTION # 81
.....

You will receive a registration code and download instructions via email. We will be happy to assist you with any questions regarding our products. Our Google Cloud Certified - Professional Security Operations Engineer (PSOE) Exam (Security-Operations-Engineer) practice exam software helps to prepare applicants to practice time management, problem-solving, and all other tasks on the standardized exam and lets them check their scores. The Google Cloud Certified - Professional Security Operations Engineer (PSOE) Exam (Security-Operations-Engineer) practice test results help students to evaluate their performance and determine their readiness without difficulty.