SureTorrent Offer The Google Security-Operations-Engineer Exam Questions In Three Versions

Professional Cloud Security Engineer.prepaway.premium.exa... - Custom Exam - ETE Player
□ Mark
Question 57 of 93 (Exam A, Q42)
Previous
Next
Review
Show Answer
Show List
Save Session
End Exam

A DevOps team will create a new container to run on Google Kubernetes Engine. As the application will be internet-facing, they want to minimize the attack surface of the container.

What should they do?

○ A. Use Cloud Build to build the container images.
○ B. Build small containers using small base images.
○ C. Delete non-used versions from Container Registry.
○ D. Use a Continuous Delivery tool to deploy the application.

What's more, part of that SureTorrent Security-Operations-Engineer dumps now are free: https://drive.google.com/open?id=16Tz7ClMnRoaAPkMl-D0WXFwa6F-dzDjV

Three versions are available for Security-Operations-Engineer study materials, so that you can get the version you want according to your own needs. Security-Operations-Engineer PDF version is printable, and you can study anytime and anyplace. Security-Operations-Engineer Online test engine is convenient and easy to learn, it supports all web browsers, and you can use in your phone, Android and IOS both ok. One of outstanding features of Security-Operations-Engineer Online soft test engine is that it has testing history and performance review, and you can have a general review of what you have learned before next training. Security-Operations-Engineer Soft test engine can be used in more than 200 computers, and you use this version in your computer, and it supports MS operating system.

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	• 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.
Topic 3	• 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 4	- 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.

>> Security-Operations-Engineer Valid Exam Online <<

Security-Operations-Engineer Valid Exam Online Exam Pass Once Try | Security-Operations-Engineer: Google Cloud Certified - Professional Security Operations Engineer (PSOE) Exam

We believe that every customer pays most attention to quality when he is shopping. Only high-quality goods can meet the needs of every customer better. And our Security-Operations-Engineer study materials have such high quality, because its hit rate of test questions is extremely high. Perhaps you will find in the examination that a lot of questions you have seen many times in our Security-Operations-Engineer Study Materials. In addition, the passing rate is the best test for quality of study materials. And we can be very proud to tell you that the passing rate of our Security-Operations-Engineer study materials is almost 100 %.

Google Cloud Certified - Professional Security Operations Engineer (PSOE) Exam Sample Questions (Q22-Q27):

NEW QUESTION # 22
You scheduled a Google Security Operations (SecOps) report to export results to a BigQuery dataset in your Google Cloud project. The report executes successfully in Google SecOps, but no data appears in the dataset.
You confirmed that the dataset exists. How should you address this export failure?

- A. Grant the user account that scheduled the report the roles/bigquery.dataEditor IAM role on the project.
- B. Set a retention period for the BigQuery export.
- C. Grant the Google SecOps service account the roles/bigquery.dataEditor IAM role on the dataset.
- D. Grant the Google SecOps service account the roles/iam.serviceAccountUser IAM role to itself.

Answer: C

Explanation:
This is a standard Identity and Access Management (IAM) permission issue. When Google Security Operations (SecOps) exports data, it uses its own service account (often named service-<project_number>@gcp-sa-bigquerydatatransfer.iam.gserviceaccount.com or a similar SecOps-specific principal) to perform the write operation. The user account that schedules the report (Option C) is only relevant for the scheduling action, not for the data transfer itself. For the export to succeed, the Google SecOps service account principal must have explicit permission to write data into the target BigQuery dataset.
The predefined IAM role roles/bigquery.dataEditor grants the necessary permissions to create, update, and delete tables and table data within a dataset. By granting this role to the Google SecOps service account on the specific dataset, you authorize the service to write the report results and populate the tables. Option A (serviceAccountUser) is incorrect as it's used for service account impersonation, not for granting data access.
Option B (retention period) is a data lifecycle setting and has no impact on the ability to write new data. The most common cause for this exact scenario-a successful job run with no data appearing-is that the service account lacks the required bigquery.dataEditor permissions on the destination dataset.
(Reference: Google Cloud documentation, "Troubleshoot transfer configurations"; "Control access to resources with IAM"; "BigQuery predefined IAM roles")

NEW QUESTION # 23
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. 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.
- C. Perform a UDM search across the logs for domains with low prevalence that were first seen in the last 30 days.
- D. Perform a UDM search across the logs for domains with geolocations that were first seen in the last 30 days.
- E. Perform a raw log search across the logs for domains with low prevalence that were first seen in the last 30 days.

Answer: B,C

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 # 24
Your organization recently conducted a penetration test on their environment. You have been tasked with identifying a successful attack chain. The required log sources have been ingested into Google Security Operations (SecOps). You discover anomalous outbound traffic to external domains. You suspect that the finding is a communication to a command and control (C2) infrastructure. You need to identify the least common network communications over the last 14 days. What should you do?

- A. Perform a Google SecOps SIEM raw log search that looks for low rolling prevalence domains with NETWORK_CONNECTION or NETWORK_HTTP in the firewall and proxy logs over the last 14 days.
- B. Perform a Google SecOps SIEM UDM search that looks for NETWORK_CONNECTION or NETWORK_HTTP events with low rolling prevalence for principal domains over the last 14 days.
- C. Perform a Google SecOps SIEM UDM search that looks for NETWORK_CONNECTION or NETWORK_HTTP events with low rolling prevalence for target domains over the last 14 days.
- D. Perform a Google SecOps SOAR search that looks for cases with low rolling prevalence of NETWORK_CONNECTION or NETWORK_HTTP events over the last 14 days.

Answer: C

Explanation:
To identify rare network communications that could indicate C2 activity, you should run a Google SecOps SIEM UDM search for NETWORK_CONNECTION or NETWORK_HTTP events and filter for low rolling prevalence on target domains over the past 14 days. This approach highlights unusual outbound communications to external domains that are least common in your environment, aligning with C2 detection best practices.

NEW QUESTION # 25
You are investigating whether an advanced persistent threat (APT) actor has operated in your organization's environment undetected. You have received threat intelligence that includes:
* A SHA256 hash for a malicious DLL
* A known command and control (C2) domain
* A behavior pattern where rundll32.exe spawns powershell.exe with obfuscated arguments Your Google Security Operations (SecOps) instance includes logs from EDR, DNS, and Windows Sysmon.
However, you have recently discovered that process hashes are not reliably captured across all endpoints due to an inconsistent Sysmon configuration. You need to use Google SecOps to develop a detection mechanism that identifies the associated activities.
What should you do?

- A. Write a multi-event YARA-L detection rule that correlates the process relationship and hash, and run a retrohunt based on this rule.
- B. Build a data table that contains the hash and domain, and link the list to a high-frequency rule for near real-time alerting.

- C. Use Google SecOps search to identify recent uses of rundll32.exe, and tag affected assets for watchlisting.
- D. Create a single-event YARA-L detection rule based on the file hash, and run the rule against historical and incoming telemetry to detect the DLL execution.

Answer: B

Explanation:
The core of this problem is the unreliable data quality for the file hash. A robust detection strategy cannot depend on an unreliable data point. Options B and C are weak because they create a dependency on the SHA256 hash, which the prompt states is "not reliably captured." This would lead to missed detections.
Option A is far too broad and would generate massive noise.
The best detection engineering practice is to use the reliable IoCs in a flexible and high-performance manner.
The domain is a reliable IoC (from DNS logs), and the hash is still a valuable IoC, even if it's only intermittently available.
The standard Google SecOps method for this is to create a List (referred to here as a "data table") containing both static IoCs: the hash and the domain. An engineer can then write a single, efficient YARA-L rule that references this list. This rule would trigger if either a PROCESS_LAUNCH event is seen with a hash in the list or a NETWORK_DNS event is seen with a domain in the list (e.g., (event.principal.process.file.sha256 in
%ioc_list) or (event.network.dns.question.name in %ioc_list)). This creates a resilient detection mechanism that provides two opportunities to identify the threat, successfully working around the unreliable data problem.
(Reference: Google Cloud documentation, "YARA-L 2.0 language syntax"; "Using Lists in rules"; "Detection engineering overview")

NEW QUESTION # 26
A SOC team notices repeated outbound HTTPS connections from a Compute Engine instance to an external IP every 60 seconds. CPU usage is normal and no malware signatures trigger. What is the BEST next analytical step?

- A. Power off the instance
- B. Notify executive leadership
- C. Identify the process and service account generating the traffic
- D. Block the destination IP immediately

Answer: C

Explanation:
Understanding what is generating the traffic and under which identity is essential before containment.

NEW QUESTION # 27
......

Our technology and our staff are the most professional. What are the Security-Operations-Engineer practice materials worthy of your choice, I hope you spend a little time to find out. First of all, after you make a decision, you can start using our Security-Operations-Engineer Exam Questions soon. We will send you an email within five to ten minutes after your payment is successful. You can choose any version of Security-Operations-Engineer study guide, as long as you find it appropriate.

Exam Security-Operations-Engineer Question: https://www.suretorrent.com/Security-Operations-Engineer-exam-guide-torrent.html

- Security-Operations-Engineer Training Materials □ Security-Operations-Engineer Latest Exam Price □ Security-Operations-Engineer Latest Exam Price □ Go to website ▷ www.examcollectionpass.com ◁ open and search for 「Security-Operations-Engineer」 to download for free □Security-Operations-Engineer Testing Center
- Security-Operations-Engineer Latest Demo □ Security-Operations-Engineer Interactive EBook □ Security-Operations-Engineer Latest Practice Materials □ Search for □ Security-Operations-Engineer □ and download it for free immediately on ☀ www.pdfvce.com □☀□ □Valid Security-Operations-Engineer Exam Bootcamp
- Reliable Security-Operations-Engineer Test Sample □ Security-Operations-Engineer Exam Training □ Real Security-Operations-Engineer Torrent □ Search on 《 www.troytecdumps.com 》 for ⇒ Security-Operations-Engineer ⇐ to obtain exam materials for free download □Security-Operations-Engineer Frenquent Update
- Latest Security-Operations-Engineer Test Sample □ Online Security-Operations-Engineer Test □ Security-Operations-Engineer Latest Demo □ Immediately open “www.pdfvce.com” and search for ▶ Security-Operations-Engineer ◀ to obtain a free download □Reliable Security-Operations-Engineer Mock Test
- Security-Operations-Engineer Testing Center □ Reliable Security-Operations-Engineer Mock Test □ Real Security-

Operations-Engineer Torrent □ Download ✔ Security-Operations-Engineer □✔□ for free by simply searching on ▹ www.troytecdumps.com ◃ □Real Security-Operations-Engineer Torrent

- Google - Latest Security-Operations-Engineer - Google Cloud Certified - Professional Security Operations Engineer (PSOE) Exam Valid Exam Online □ Search for □ Security-Operations-Engineer □ on " www.pdfvce.com " immediately to obtain a free download □Security-Operations-Engineer Latest Exam Price
- Pass Guaranteed Reliable Google - Security-Operations-Engineer - Google Cloud Certified - Professional Security Operations Engineer (PSOE) Exam Valid Exam Online □ Go to website ➥ www.vceengine.com □ open and search for { Security-Operations-Engineer } to download for free □Security-Operations-Engineer Latest Exam Price
- Latest Security-Operations-Engineer Test Sample □ Valid Security-Operations-Engineer Study Materials □ Security-Operations-Engineer Interactive EBook □ Search for 「 Security-Operations-Engineer 」 and download exam materials for free through 【 www.pdfvce.com 】 □Security-Operations-Engineer Latest Exam Price
- Security-Operations-Engineer Testing Center □ Security-Operations-Engineer Frenquent Update □ Security-Operations-Engineer Latest Demo □ 《 www.practicevce.com 》 is best website to obtain □ Security-Operations-Engineer □ for free download □Latest Security-Operations-Engineer Test Blueprint
- Security-Operations-Engineer Study Materials - Security-Operations-Engineer Exam Preparatory - Security-Operations-Engineer Practice Test □ Enter ▹ www.pdfvce.com ◃ and search for □ Security-Operations-Engineer □ to download for free □Real Security-Operations-Engineer Torrent
- Security-Operations-Engineer Practice Tests □ Security-Operations-Engineer Frenquent Update □ Valid Security-Operations-Engineer Exam Bootcamp □ Search for ⇛ Security-Operations-Engineer ⇚ and obtain a free download on ➠ www.vce4dumps.com □ □Reliable Security-Operations-Engineer Test Prep
- www.stes.tyc.edu.tw, myportal.utt.edu.tt, rabonystudywork.com, www.stes.tyc.edu.tw, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, www.stes.tyc.edu.tw, bbs.netcnnet.net, estudiasonline.com, Disposable vapes

DOWNLOAD the newest SureTorrent Security-Operations-Engineer PDF dumps from Cloud Storage for free: https://drive.google.com/open?id=16Tz7ClMnRoaAPkMl-D0WXFwa6F-dzDjV