Google Security-Operations-Engineer Fragen und Antworten, Google Cloud Certified - Professional Security Operations Engineer (PSOE) Exam Prüfungsfragen

Als ein Mitglied der IT-Branche, machen Sie sich noch Sorgen um die Google Security-Operations-Engineer IT-Zertifizierungsprüfungen? Es ist nicht so leicht, die Google Security-Operations-Engineer IT-Zertifizierungsprüfung, die Ihre relevanten Fachkenntnisse und Fähigkeiten überprüft, zu bestehen. Für die Kandidaten, die sich zum ersten Mal an der Google Security-Operations-Engineer IT-Zertifizierungsprüfung beteiligen, ist ein zielgerichtetes Schulungsprogramm von großer Notwendigkeit. Zertpruefung stellt den Kandidaten die zielgerichteten Programme, die Simulationsprüfung, zielgerichtete Lernhilfe und die Prüfungsfragen und Antworten, die 95% der realen Prüfung ähnlich sind, zur Verfügung. Schicken Sie doch schnell Zertpruefung in den Warenkorb.

Das IT-Expertenteam von Zertpruefung haben eine kurzfristige Schulungsmethode nach ihren Kenntnissen und Erfahrungen bearbeitet. Diese Dumps könne Ihnen effektiv helfen, in kurzer Zeit den erwarteten Effekt zu erzielen, besonders für diejenigen, die arbeiten und zuleich lernen. Zertpruefung kann Ihnen viel Zeit und Energir ersparen. Wählen Sie Zertpruefung und Sie werden Ihre wünschten Schulungsmaterialien zur Google Security-Operations-Engineer Zertifizierungsprüfung bekommen.

>> Security-Operations-Engineer Fragen&Antworten <<

Security-Operations-Engineer Der beste Partner bei Ihrer Vorbereitung der Google Cloud Certified - Professional Security Operations Engineer (PSOE) Exam

Es ist unnötig für Sie, zu viel Zeit eine Prüfung vorzubereiten. Kaufen Sie bitte Google Security-Operations-Engineer Dumps von Zertpruefung. Mit diesen Dumps können Sie wissen, wie Google Security-Operations-Engineer Prüfung hocheffektiv vorzubereiten. Das ist ein seltenes Gerät, das Ihnen helfen, sehr einfach die Google Security-Operations-Engineer Prüfung zu bestehen. Sie werden bereuen, dass Sie diese Chance verlieren. So handeln Sie bitte schnell damit.

Google Cloud Certified - Professional Security Operations Engineer (PSOE) Exam Security-Operations-Engineer Prüfungsfragen mit Lösungen (Q88-Q93):

88. Frage
Your organization recently implemented Google Security Operations (SecOps). You need to create a solution that allows the security team to monitor data ingestion into Google SecOps in real time. You also need to configure a solution that automatically sends a notification if one of the data sources stops ingesting data. You need to minimize the cost of these configurations.
What should you do?

- A. Create Looker dashboards to visualize the data ingestion, and configure an alerting policy in Looker to send a notification

in case of failure.

- B. Create Looker dashboards to visualize the data ingestion, and configure an alerting policy in Cloud Monitoring to send a notification in case of failure.
- C. Use Google SecOps SIEM dashboards to visualize the data ingestion and configure an alerting policy in Cloud Logging to send a notification in case of failure.
- D. Use Google SecOps SIEM dashboards to visualize the data ingestion, and configure an alerting policy in Cloud Monitoring to send a notification in case of failure.

Antwort: D

Begründung:
The most cost-effective and efficient solution is to use Google SecOps SIEM dashboards to monitor data ingestion in real time and configure an alerting policy in Cloud Monitoring to send notifications if a data source stops ingesting. This leverages existing Google-managed services without requiring additional visualization or monitoring tools, minimizing both cost and maintenance overhead.

89. Frage
Your organization uses Cloud Identity as their identity provider (IdP) and is a Google Security Operations (SecOps) customer You need to grant a group of users access to the Google SecOps instance with read-only access to all resources, including detection engine rules. How should this be configured?

- A. Create a workforce identity pool at the organization level Grant the roles/chronicle.limitedViewer IAM role to the principalSet://iam.googleapis.com/locations/global/workforcePools/POOL_ID/group/GROUP_ID principal set on the project associated with your Google SecOps Instance.
- B. Create a workforce identity pool at the organization level. Grant the roles/chronicle.editor IAM role to the principalSet://iam.googleapis.com/locations/global/workforcePools/POOL_ID/group/GROUP_ID principal set on the project associated with your Google SecOps instance.
- C. Create a Google Group and add the required users. Grant the roles/chronicle.Viewer IAM role to the group on the project associated with your Google SecOps Instance.
- D. Create a Google Group and add the required users. Grant the roles/chronicle.limitedViewer IAM role to the group on the project associated with your Google SecOps instance.

Antwort: C

Begründung:
To grant read-only access to all Google SecOps resources, including detection engine rules, you assign the roles/chronicle.Viewer IAM role. The correct method is to create a Google Group, add the required users, and grant this role to the group at the project level tied to your Google SecOps instance. This ensures consistent, least-privilege access management through Cloud Identity.

90. Frage
You are managing the integration of Security Command Center (SCC) with downstream tooling.
You need to pull security findings from SCC and import those findings as part of Google Security Operations (SecOps) SOAR actions. You need to configure the connection between SCC and Google SecOps. What should you do?

- A. Create a Pub/Sub topic with a NotificationConfig object and a push subscription for the desired finding types. Create a new Google SecOps service account in the Google Cloud project, and grant this service account the appropriate IAM roles to read from this subscription. Export the credentials from IAM and import the credentials into Google SecOps SOAR.
- B. Install the Google Rapid Response integration from the Google SecOps Marketplace. Gather information about the findings from the appropriate server.
- C. Install the SCC integration from the Google SecOps Marketplace. Grant the SCC API the appropriate IAM roles to integrate with the Google SecOps instance. Configure this integration using a generated API key scoped to the SCC API.
- D. Create a Pub/Sub topic with a NotificationConfig object and a push subscription for the desired finding types. Grant the Google SecOps service account the appropriate IAM roles to read from this subscription.

Antwort: C

Begründung:
The proper way to integrate SCC findings into Google SecOps SOAR is to install the SCC integration from the Google SecOps Marketplace. You must grant the SCC API the appropriate IAM roles so that Google SecOps can access the findings, and configure the integration using a generated API key scoped to the SCC API. This approach provides a managed, secure, and

supported method for importing SCC findings into SecOps actions.

91. Frage
Your organization uses the curated detection rule set in Google Security Operations (SecOps) for high priority network indicators. You are finding a vast number of false positives coming from your on-premises proxy servers. You need to reduce the number of alerts. What should you do?

- A. Configure a rule exclusion for the principal.ip field.
- B. Configure a rule exclusion for the target.domain field.
- C. Configure a rule exclusion for the network.asset.ip field.
- D. Configure a rule exclusion for the target.ip field.

Antwort: A

Begründung:
Comprehensive and Detailed Explanation
The correct solution is Option B. This is a common false positive tuning scenario.
The "high priority network indicators" rule set triggers when it sees a connection to or from a known- malicious IP or domain. The problem states the false positives are coming from the on-premises proxy servers.
This implies that the proxy server itself is initiating traffic that matches these indicators. This is often benign, legitimate behavior, such as:
* Resolving a user-requested malicious domain via DNS to check its category.
* Performing an HTTP HEAD request to a malicious URL to scan it.
* Fetching its own threat intelligence or filter updates.
In all these cases, the source of the network connection is the proxy server. In the Unified Data Model (UDM), the source IP of an event is stored in the principal.ip field.
To eliminate these false positives, you must create a rule exclusion (or add a not condition to the rule) that tells the detection engine to ignore any events where the principal.ip is the IP address of your trusted proxy servers. This will not affect the rule's ability to catch a workstation behind the proxy (whose IP would be the principal.ip) connecting through the proxy to a malicious target.ip.
Exact Extract from Google Security Operations Documents:
Curated detection exclusions: Curated detections can be tuned by creating exclusions to reduce false positives from known-benign activity. You can create exclusions based on any UDM field.
Tuning Network Detections: A common source of false positives for network indicator rules is trusted network infrastructure, such as proxies or DNS servers. This equipment may generate traffic to malicious domains or IPs as part of its normal operation (e.g., DNS resolution, content filtering lookups). In this scenario, the traffic originates from the infrastructure device itself. To filter this noise, create an exclusion where the principal.ip field matches the IP address (or IP range) of the trusted proxy server. This prevents the rule from firing on the proxy's administrative traffic while preserving its ability to detect threats from end-user systems.
References:
Google Cloud Documentation: Google Security Operations > Documentation > Detections > Curated detections > Tune curated detections with exclusions Google Cloud Documentation: Google Security Operations > Documentation > Detections > Overview of the YARA-L 2.0 language

92. Frage
You are threat hunting for an advanced threat group known for targeted, novel attacks by deploying campaign-specific infrastructure. You want to develop detections based on the threat group's behaviors so you can effectively detect whether the threat group has attacked your organization. What should you do?

- A. Search for the threat actor in Google Threat Intelligence, export the IOCs associated with the threat actor into a Google Security Operations (SecOps) list, and develop detections that reference this list.
- B. Find intelligence reports in Google Threat Intelligence that relate to the threat actor, identify their behavior in previous campaigns, and use the past behavior to design detections in Google Security Operations (SecOps).
- C. Identify exposed technologies and products used by your organization, and develop detections to search for signs of exploitation.
- D. Search for the threat actor in Google Threat Intelligence, review the threat actor's tactics, techniques, and procedures (TTPs), and design detections based on the TTPs in Google Security Operations (SecOps).

Antwort: D

Begründung:

The most effective approach is to search for the threat actor in Google Threat Intelligence, review their tactics, techniques, and procedures (TTPs), and design detections based on those TTPs in Google SecOps. Since advanced groups often use novel, campaign-specific infrastructure, IOC- based detection is insufficient. TTP-based detection captures the underlying attacker behaviors, increasing resilience against evolving tactics.

93. Frage
.....

Bereiten Sie jetzt auf Google Security-Operations-Engineer Prüfung? Wenn ja, sind Sie sicherlich ein Mensch mit Ambition. Wir Zertpruefung bemühen uns darum, den Menschen wie Ihnen zu helfen, Ihr Ziel zu erreichen. Die Simulierte-Prüfungssoftware der Google Security-Operations-Engineer von uns enthält große Menge von Prüfungsaufgaben. Wenn Sie unsere Produkte gekauft haben, können Sie noch einjährige kostenlose Aktualisierung der Google Security-Operations-Engineer genießen. Benutzen Sie unsere Software! Dann gibt es gar kein Problem bei des Bestehens der Google Security-Operations-Engineer Prüfung!

Security-Operations-Engineer Prüfung: https://www.zertpruefung.de/Security-Operations-Engineer_exam.html

Google Security-Operations-Engineer Fragen&Antworten Unser Unternehmen ist sehr bekannt für Ihr großes Verantwortungsbewusstsein, Während man sich um die Krams im alltäglichen Leben kümmert, zerbricht man sich noch den Kopf, die Security-Operations-Engineer Prüfung zu bestehen, warauf warten Sie noch, Wir wünschen Ihnen viel Erfolg bei der Google Security-Operations-Engineer Prüfung, Als weltweiter Führer im Bereich der Security-Operations-Engineer Übungswerkstätte, sind wir determiniert, unseren Kunden einen verständlichen Service anzubieten und einen integrierten Service aufzubauen.

Aber der Propst meinte doch zu erkennen, daß es einen hohen Security-Operations-Engineer Schulungsangebot Berg hinaufging, Was krümmete denn ich mich so gleich einem Wurme?Wir sehen nicht, wie seine Wege führen!

Unser Unternehmen ist sehr bekannt für Ihr großes Verantwortungsbewusstsein, Während man sich um die Krams im alltäglichen Leben kümmert, zerbricht man sich noch den Kopf, die Security-Operations-Engineer Prüfung zu bestehen, warauf warten Sie noch?

Security-Operations-Engineer Schulungsmaterialien & Security-Operations-Engineer Dumps Prüfung & Security-Operations-Engineer Studienguide

Wir wünschen Ihnen viel Erfolg bei der Google Security-Operations-Engineer Prüfung, Als weltweiter Führer im Bereich der Security-Operations-Engineer Übungswerkstätte, sind wir determiniert, unseren Kunden Security-Operations-Engineer einen verständlichen Service anzubieten und einen integrierten Service aufzubauen.

Regelmäßiges Update garantiert hohe Genauigkeit der Prüfungsfragen.

- Security-Operations-Engineer Examsfragen □ Security-Operations-Engineer Prüfungs-Guide □ Security-Operations-Engineer Prüfungs-Guide □ Öffnen Sie die Webseite ➥ www.zertpruefung.ch □ und suchen Sie nach kostenloser Download von ➠ Security-Operations-Engineer □ □Security-Operations-Engineer Testing Engine
- Security-Operations-Engineer Vorbereitungsfragen □ Security-Operations-Engineer Antworten ❤ Security-Operations-Engineer Vorbereitungsfragen □ Suchen Sie jetzt auf ➽ www.itzert.com □ nach 《 Security-Operations-Engineer 》 und laden Sie es kostenlos herunter □Security-Operations-Engineer Examengine
- Security-Operations-Engineer Kostenlos Downloden □ Security-Operations-Engineer Antworten □ Security-Operations-Engineer Vorbereitungsfragen □ Suchen Sie auf ➤ www.itzert.com □ nach kostenlosem Download von □ Security-Operations-Engineer □ ⧖Security-Operations-Engineer Lernhilfe
- Google Security-Operations-Engineer Quiz - Security-Operations-Engineer Studienanleitung - Security-Operations-Engineer Trainingsmaterialien □ Suchen Sie jetzt auf " www.itzert.com " nach ✔ Security-Operations-Engineer □✔□ um den kostenlosen Download zu erhalten □Security-Operations-Engineer Antworten
- Security-Operations-Engineer Der beste Partner bei Ihrer Vorbereitung der Google Cloud Certified - Professional Security Operations Engineer (PSOE) Exam □ Sie müssen nur zu ➽ www.echtefrage.top □ gehen um nach kostenloser Download von { Security-Operations-Engineer } zu suchen □Security-Operations-Engineer Prüfungs-Guide
- Security-Operations-Engineer Trainingsmaterialien: Google Cloud Certified - Professional Security Operations Engineer (PSOE) Exam - Security-Operations-Engineer Lernmittel - Google Security-Operations-Engineer Quiz □ Öffnen Sie die Website ➤ www.itzert.com □ Suchen Sie " Security-Operations-Engineer " Kostenloser Download □Security-Operations-Engineer Schulungsangebot
- Security-Operations-Engineer Schulungsmaterialien - Security-Operations-Engineer Dumps Prüfung - Security-Operations-Engineer Studienguide □ Erhalten Sie den kostenlosen Download von □ Security-Operations-Engineer □ mühelos über { www.itzert.com } □Security-Operations-Engineer Exam

- Security-Operations-Engineer Prüfungsmaterialien □ Security-Operations-Engineer Dumps □ Security-Operations-Engineer Online Prüfung ↩ Öffnen Sie die Webseite （ www.itzert.com ） und suchen Sie nach kostenloser Download von 【 Security-Operations-Engineer 】 □Security-Operations-Engineer Prüfung
- Security-Operations-Engineer Trainingsmaterialien: Google Cloud Certified - Professional Security Operations Engineer (PSOE) Exam - Security-Operations-Engineer Lernmittel - Google Security-Operations-Engineer Quiz □ Öffnen Sie die Webseite ➡ www.examfragen.de □□□ und suchen Sie nach kostenloser Download von （ Security-Operations-Engineer ） □Security-Operations-Engineer Lernhilfe
- Security-Operations-Engineer Übungsfragen: Google Cloud Certified - Professional Security Operations Engineer (PSOE) Exam - Security-Operations-Engineer Dateien Prüfungsunterlagen □ Suchen Sie einfach auf ⇛ www.itzert.com ⇚ nach kostenloser Download von ➤ Security-Operations-Engineer □ □Security-Operations-Engineer Prüfungsmaterialien
- Security-Operations-Engineer Prüfungsinformationen □ Security-Operations-Engineer Vorbereitungsfragen □ Security-Operations-Engineer Kostenlos Downloden □ Erhalten Sie den kostenlosen Download von 《 Security-Operations-Engineer 》 mühelos über ➠ www.itzert.com □ □Security-Operations-Engineer Online Test
- www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, internsoft.com, 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, myportal.utt.edu.tt, confengine.com, prosperaedge.com, 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, coursewingsportal.com, www.skudci.com, www.stes.tyc.edu.tw, Disposable vapes