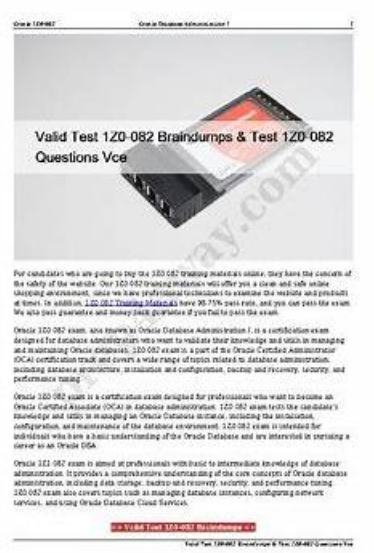
Security-Operations-Engineer Valid Test Vce Free - Security-Operations-Engineer Pdf Demo Download



If you buy our Security-Operations-Engineer training quiz, you will find three different versions are available on our test platform. According to your need, you can choose the suitable version of our Security-Operations-Engineer exam questions for you. The three different versions of our Security-Operations-Engineer Study Materials include the PDF version, the software version and the online version. We can promise that the three different versions are equipment with the high quality for you to pass the exam.

The Google Security-Operations-Engineer desktop practice exam software is customizable and suits the learning needs of candidates. A free demo of the Google Cloud Certified - Professional Security Operations Engineer (PSOE) Exam (Security-Operations-Engineer) desktop software is available for sampling purposes. You can change Google Security-Operations-Engineer Practice Exam's conditions such as duration and the number of questions. This simulator creates a Google Cloud Certified - Professional Security Operations Engineer (PSOE) Exam (Security-Operations-Engineer) real exam environment that helps you to get familiar with the original test.

>> Security-Operations-Engineer Valid Test Vce Free <<

Security-Operations-Engineer Pdf Demo Download, Security-Operations-Engineer Minimum Pass Score

TrainingQuiz is also offering 90 days free Security-Operations-Engineer updates. You can update your Security-Operations-

Engineer study material for one year from the date of purchase. The Security-Operations-Engineer updated package will include all the past questions from the past papers. You can pass the Security-Operations-Engineer exam easily with the help of the PDF dumps included in the package. It will have all the questions that you should cover for the Security-Operations-Engineer Security-Operations-Engineer exam. If you are facing any issues with the products you have, then you can always contact our 24/7 support to get assistance.

Google Cloud Certified - Professional Security Operations Engineer (PSOE) Exam Sample Questions (Q24-Q29):

NEW QUESTION # 24
Your organization has recently onboarded to Google Cloud with Security Command Center Enterprise (SCCE) and is now integrating it with your organization's SOC. You want to automate the response process within SCCE and integrate with the existing SOC ticketing system. You want to use the most efficient solution. How should you implement this functionality?

- A. Use the SCC notifications feed to send alerts to Pub/Sub. Ingest these feeds using the relevant SIEM connector.
- B. Configure the SCC notifications feed to send alerts to a Cloud Storage bucket. Create a Dataflow job to read the new files, extract the relevant information, and send the information to the SOC ticketing system.
- C. Evaluate each event within the SCC console. Create a ticket for each finding in the ticketing system, and include the remediation steps.
- D. Disable the generic posture finding playbook in Google Security Operations (SecOps) SOAR and enable the playbook for the ticketing system. Add a step in your Google SecOps SOAR playbook to generate a ticket based on the event type.

Answer: D

Explanation:
Comprehensive and Detailed Explanation
The correct answer is Option C. The prompt asks for the most efficient and automated solution for handling SCCE findings and integrating with a ticketing system. This is the primary use case for Google Security Operations SOAR.
The native workflow is as follows:
* SCCE detects a finding.
* The finding is automatically ingested into Google SecOps SIEM, which creates an alert.
* The alert is automatically sent to SecOps SOAR, which creates a case.
* The SOAR case automatically triggers a playbook.
Option C describes this process perfectly. An administrator would disable the default playbook and enable a specific playbook that uses a pre-built integration (from the Marketplace) for the organization's ticketing system (e.g., ServiceNow, Jira). This playbook would contain an automated step to generate a ticket, thus fulfilling the requirement efficiently.
Option B is a manual process. Options A and D describe complex, custom-built data engineering pipelines, which are far less efficient than using the built-in SOAR capabilities.
Exact Extract from Google Security Operations Documents:
SOAR Playbooks and Integrations: Google SecOps SOAR is designed to automate and orchestrate responses to alerts. When an alert from a source like Security Command Center (SCC) is ingested and creates a case, it can be configured to automatically trigger a playbook.
Ticketing Integration: A common playbook use case is integration with an external ticketing system. Using a pre-built integration from the SOAR Marketplace, an administrator can add a step to the playbook (e.g., Create Ticket). This action will automatically generate a ticket in the external system and populate it with details from the alert, such as the finding, the affected resources, and the recommended remediation steps.
This provides a seamless, automated workflow from detection to ticketing.
References:
Google Cloud Documentation: Google Security Operations > Documentation > SOAR > Use cases > Case Management Google Cloud Documentation: Google Security Operations > Documentation > SOAR > Marketplace integrations

NEW QUESTION # 25
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.

```
rule ioc_domain_C2 {
  meta:
    author = "Google Cloud Security"
    description = "Detect DNS events that indicate communication to a C2 domain"

  events:
    $dns.metadata.event_type = "NETWORK_DNS"
    $dns.network.dns.questions.name =$dns_query
    $ioc.graph.metadata.product_name = "MISP"

    << Add code>>

    $ioc.graph.metadata.threat.summary = "C2 domains"
    $ioc.graph.entity.hostname = $dns_query

   match:
     $dns_query over 5m

   condition:
     $dns and $ioc
}
```

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 = "DOMAIN_NAME"
  Sioc.graph.metadata.source_type = "GLOBAL_CONTEXT"
- C. $ioc.graph.metadata.entity_type = "D0MAIN_NAME"
  $ioc.graph.metadata.source_type = MDERIVED_CONTEXT"
- D. $ioc.graph.metadata.entity_type = MDOMAIN_NAME"
  $ioc.graph.metadata.scurce_type = "ElfelTYj