# Security-Operations-Engineer試験準備、Security-Operations-Engineerサンプル問題集

JPexam.com - 模擬試験場

VMware | VCP-510 | VMware Certified Professional on VSphere 5

| マークした | 回答した | 番号 | 条目 |
|---|---|---|---|
| □ | | 1. | Click the Exhibit button. An administrator has deployed a new virtual machine on an ESXi 5.x hos... |
| □ | | 2. | An administrator notices that when a virtual machine is placed into a resource pool, a warning in... |
| □ | | 3. | An administrator views the Fault Tolerance pane of the Summary tab of a virtual machine and fin... |
| □ | | 4. | Which two conditions prevent the application of a host profile to an ESXi 5.x host? (Choose two.) |
| □ | | 5. | An administrator is editing the IP allocation policy for a vApp. Which three options are available? ... |
| □ | | 6. | ACME Junkmail Incorporated has been utilizing templates in their environment. They are running... |
| □ | | 7. | What are three valid objects to place in a vApp? (Choose three.) |
| □ | | 8. | Which three Storage I/O Control conditions might trigger the Non-VI workload detected on the dat... |
| □ | | 9. | An administrator has just finished deploying a vApp for a web service. What three options are av... |
| □ | | 10. | An administrator is working to implement Storage Profiles in their environment. Which two ways ... |
| □ | | 11. | Which VMware solution uses the security of a vSphere implementation and provides linked-clon... |
| □ | | 12. | Which two conditions will prevent a virtual machine from being successfully migrated using Stor... |
| □ | | 13. | Under which two conditions can vStorage APIs for Array Integration (VAAI) provide a performance... |
| □ | | 14. | An administrator is enabling Enhanced vMotion Compatibility (EVC) in a DRS cluster. The admin... |
| □ | | 15. | Which two conditions must exist on all hosts in the cluster if Enhanced vMotion Compatibility (EV... |
| □ | | 16. | Users are experiencing performance issues when updating their database hosted on a virtual ... |
| □ | | 17. | An administrator takes a vSphere snapshot of a virtual machine and applies an OS update. After ... |
| □ | | 18. | An administrator has created a virtual machine that will be accessed from a public kiosk. Manag... |
| □ | | 19. | What are three true statements about quiescing virtual machine snapshots? (Choose three.) |
| □ | | 20. | An administrator has deployed vCenter Data Recovery and wants the largest possible de-duplic... |
| □ | | 21. | An administrator has recently upgraded their Update Manager infrastructure to vSphere 5.x. Seve... |
| □ | | 22. | An administrator is using Update Manager 5.x to update virtual appliances in a vSphere environ... |
| □ | | 23. | An administrator is working to update the hosts and virtual machines in a vSphere 5.x deployme... |
| □ | | 24. | An administrator selects the Profile Compliance tab of an vSphere cluster, then selects Check C... |

最短時間でSecurity-Operations-Engineer試験に合格し、関連する認定資格を取得する場合、当社のSecurity-Operations-Engineerトレーニング資料を選択することは、すべての人々の利益になります。あなたのSecurity-Operations-Engineer試験に合格し、想像を超える最短時間で関連する認定資格を取得することが非常に簡単になることを確認できます。ウェブからSecurity-Operations-Engineer認定トレーニング資料の手順を知ることができます。また、Security-Operations-Engineer試験問題のデモを無料でダウンロードして、支払い前に確認することもできます。

## Google Security-Operations-Engineer 認定試験の出題範囲：

| トピック | 出題範囲 |
|---|---|
| トピック 1 | • 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. |
| トピック 2 | • 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. |
| トピック 3 | • 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. |

|  |  |
|---|---|
| トピック 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. |

**>> Security-Operations-Engineer試験準備 <<**

## Google Security-Operations-Engineer試験の準備方法｜一番優秀なSecurity-Operations-Engineer試験準備試験｜最高のGoogle Cloud Certified - Professional Security Operations Engineer (PSOE) Examサンプル問題集

あなたの利益を保障するために、あなたのSecurity-Operations-Engineer問題集を購入した後、我々はSecurity-Operations-Engineer対策の一年間の無料更新を提供します。我々の専門家たちは毎日更新を検査していますから、この一年間で、もし更新があったら、更新したSecurity-Operations-Engineer問題集は自動的にあなたのメールアドレスに送られます。我々PassTestはあなたの持っている商品は最新的のを保証しています。

## Google Cloud Certified - Professional Security Operations Engineer (PSOE) Exam 認定 Security-Operations-Engineer 試験問題 (Q28-Q33):

**質問 # 28**
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. Modify the UI settings to correct the time zone.
- C. Create a parser extension to correct the time zone.
- D. Create a custom parser to correct the time zone.

**正解：C**

解説：
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.

**質問 # 29**
You are a SOC analyst at an organization that uses Google Security Operations (SecOps). You are investigating suspicious activity in your organization's environment. Alerts in Google SecOps indicate repeated PowerShell activity on a set of endpoints. Outbound connections are made to a domain that does not appear in your threat intelligence feeds. The activity occurs across multiple systems and user accounts. You need to search across impacted systems and user identities to identify the malicious user and understand the scope of the compromise. What should you do?

- A. Perform a raw log search for the suspicious domain string, and manually pivot to related user activity.
- B. Use the Behavioral Analytics dashboard in Risk Analytics to identify abnormal IP-based activity and high-risk user behavior.
- C. Use the User Sign-In Overview dashboard to monitor authentication trends and anomalies across all users.
- D. Perform a YARA-L 2.0 search to correlate activity across impacted systems and users.

**正解：D**

解説：

The most effective approach is to perform a YARA-L 2.0 search that correlates activity across impacted systems and user identities. YARA-L rules can link PowerShell execution events, outbound connections, and user activity, enabling you to identify the malicious user and the scope of the compromise efficiently, rather than relying on manual log searches or only analyzing authentication trends.

**質問 # 30**

You are using Google Security Operations (SecOps) to investigate suspicious activity linked to a specific user. You want to identify all assets the user has interacted with over the past seven days to assess potential impact. You need to understand the user's relationships to endpoints, service accounts, and cloud resources.

How should you identify user-to-asset relationships in Google SecOps?

- A. Use the Raw Log Scan view to group events by asset ID.
- B. Generate an ingestion report to identify sources where the user appeared in the last seven days.
- C. Query for hostnames in UDM Search and filter the results by user.
- D. Run a retrohunt to find rule matches triggered by the user.

**正解：C**

**解説：**

Comprehensive and Detailed 150 to 250 words of Explanation From Exact Extract Google Security Operations Engineer documents:

The primary investigation tool for exploring relationships and historical activity in Google Security Operations is the UDM (Universal Data Model) search. The platform's curated views, such as the "User View," are built on top of this search capability.

To find all assets a user has interacted with, an analyst would perform a UDM search for the specific user (e.g., principal.user.userid = "suspicious_user") over the specified time range. The search results will include all UDM events associated with that user. Within these events, the analyst can examine all populated asset fields, such as principal.asset.hostname, principal.ip, target.resource.name, and target.user.userid (for interactions with service accounts).

This UDM search allows the analyst to pivot from the user entity to all related asset entities, directly answering the question of "what assets the user has interacted with." While the wording of Option A is slightly backward (it's more efficient to query for the user and find the hostnames), it is the only option that correctly identifies the UDM search as the tool used to find user-to-asset (hostname) relationships. Options B (Retrohunt), C (Raw Log Scan), and D (Ingestion Report) are incorrect tools for this investigative task.

(Reference: Google Cloud documentation, "Google SecOps UM Search overview"; "Investigate a user"; " Universal Data Model noun list")

**質問 # 31**

You have identified a new threat actor group that has several IOCs in Google Threat Intelligence.

You want to use some of these IOCs in several detection rules in Google Security Operations (SecOps) to help identify suspicious activity. You want to use the most effective approach. What should you do?

- A. Save the IOCs in a new collection in Google Threat Intelligence. Share this list with other members of the security team to facilitate their searches and rule creation.
- B. Add the IOCs to a new or existing reference list, and update the YARA-L logic of detection rules to include the reference list.
- C. Identify the detection rules that apply to the new IOCs, and update the YARA-L logic to reference the threat actor group.
- D. Configure a new data feed in Google SecOps that includes the IOCs. Update the YARA-L logic to reference the new IOCs against applicable UDM fields.

**正解：B**

**解説：**

The most effective approach is to add the IOCs to a reference list in Google SecOps and then update the YARA-L logic of your detection rules to reference that list. This centralizes the IOCs for reuse across multiple rules, simplifies maintenance, and ensures consistency in detection logic without duplicating IOC entries in multiple places.

**質問 # 32**

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. 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.
- B. 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.
- C. Configure a detection rule in SIEM Rules & Detections to include logic to capture the event fields for each case with the relevant stage metrics.
- D. 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.

**正解：B**

解説：
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")

### 質問 # 33

......

ンロードできますSecurity-Operations-Engineer資格認定試験

- Security-Operations-Engineer学習関連題 □ Security-Operations-Engineer再テスト □ Security-Operations-Engineer テストトレーニング □ □ www.goshiken.com □を開き、“ Security-Operations-Engineer ”を入力して、無料でダウンロードしてくださいSecurity-Operations-Engineer試験勉強書
- Security-Operations-Engineer試験の準備方法丨素敵なSecurity-Operations-Engineer試験準備試験丨有難いGoogle Cloud Certified - Professional Security Operations Engineer (PSOE) Examサンプル問題集 □ URL ☀ www.xhs1991.com □☀□をコピーして開き、➠ Security-Operations-Engineer □を検索して無料でダウンロードしてくださいSecurity-Operations-Engineer的中率
- Security-Operations-Engineer合格率 □ Security-Operations-Engineer資格認定試験 □ Security-Operations-Engineer学習範囲 □ ➠ www.goshiken.com □で{ Security-Operations-Engineer }を検索して、無料で簡単にダウンロードできますSecurity-Operations-Engineer日本語対策問題集
- 試験の準備方法-最新のSecurity-Operations-Engineer試験準備試験-有難いSecurity-Operations-Engineerサンプル問題集 □ 今すぐ▹ www.mogiexam.com◃を開き、“ Security-Operations-Engineer ”を検索して無料でダウンロードしてくださいSecurity-Operations-Engineer再テスト
- 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, 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, 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, lwiyo.com, github.com, Disposable vapes