GCP-SOE-B試験の準備方法｜最新のGCP-SOE-Bテスト模擬問題集試験｜ハイパスレートのSecurity Operations Engineer (Beta)受験資料更新版

これらの2つの特性により、GCP-SOE-Bガイドトレントを使用するほぼすべての候補者が一度にテストに合格できることがわかります。これは自己決定ではありません。統計によると、当社のGCP-SOE-Bガイドトレントは98％～99％の高い合格率を達成しており、これは他のすべてをかなり上回る程度です。同時に、GCP-SOE-Bテストトレントが毎日更新されるかどうかを確認する専門スタッフがいます。メールでお問い合わせいただく場合でも、オンラインでお問い合わせいただく場合でも、できるだけ早く問題を解決できるようサポートいたします。心配する必要はまったくありません。

Google GCP-SOE-B Exam Syllabus Topics:

Section	Weight	Objectives
Topic 1: Threat Intelligence	15-20%	- Indicator of compromise (IOC) analysis - Intelligence-driven defense - Threat actor profiling - Threat intelligence sources and feeds
Topic 2: Detection Engineering	25-30%	- Designing and implementing detection rules - Log source integration and correlation - Threat hunting methodologies - False positive management - SIEM platform usage (Chronicle, Splunk, etc.)
Topic 3: Google Cloud Security Operations	15-20%	- Google Cloud logging and monitoring (Cloud Logging, Cloud Monitoring) - SIEM integration with Google Cloud services - Security Command Center integration - Automation with SOAR capabilities - Cloud-native threat detection
Topic 4: Incident Response	20-25%	- Incident classification and prioritization - Evidence collection and preservation - Forensic analysis techniques - Post-incident reporting - Root cause analysis
Topic 5: Foundations of Security Operations	15-20%	- Security operations concepts and lifecycle - Understanding MITRE ATT&CK framework - Logging and monitoring infrastructure - Building a security operations center (SOC)

>> GCP-SOE-Bテスト模擬問題集 <<

認定する-更新するGCP-SOE-Bテスト模擬問題集試験-試験の準備方法GCP-SOE-B受験資料更新版

Pass4TestのGoogleのGCP-SOE-B試験トレーニング資料を利用すれば、認定試験に合格するのは簡単になります。うちのGoogleのGCP-SOE-B試験トレーニング資料は豊富な経験を持っている専門家が長年の研究を通じて開発されたものです。Pass4Testの学習教材は君の初めての試しでGoogleのGCP-SOE-B認定試験に合格するのに助けます。

Google Security Operations Engineer (Beta) 認定 GCP-SOE-B 試験問題 (Q74-Q79):

質問 # 74
You are responsible for managing threat intelligence and IOC lists in your organization. You have compiled a list of IOCS from recent incidents. You want to quickly and efficiently share the IOCs with other teams for collaboration and integration into their operational processes. What should you do?

- A. Create a new threat graph in Google Threat Intelligence, and share the graph with the other teams.
- B. Add the IOCs to a collection in Google Threat Intelligence, and share the collection with the other teams.
- C. Export the IOCS from Google Threat Intelligence in CSV or JSON format, and email the file to the other teams.
- D. Create a list in Google Security Operations (SecOps), and grant the required access to the other teams.

正解：D

質問 # 75
Your company uses Google Security Operations (SecOps) Enterprise and is ingesting various logs. You need to proactively identify potentially compromised user accounts. Specifically, you need to detect when a user account downloads an unusually large volume of data compared to the user's established baseline activity. You want to detect this anomalous data access behavior using the least amount of effort. What should you do?

- A. Enable curated detection rules for User and Endpoint Behavioral Analytics (UEBA), and use the Risk Analytics dashboard in Google SecOps to identify metrics associated with the anomalous activity.
- B. Develop a custom YARA-L detection rule in Google SecOps that counts download bytes per user per hour and triggers an alert if a threshold is exceeded.
- C. Inspect Security Command Center (SCC) default findings for data exfiltration in Google SecOps.
- D. Create a log-based metric in Cloud Monitoring, and configure an alert to trigger if the data downloaded per user exceeds a predefined limit. Identify users who exceed the predefined limit in Google SecOps.

正解：A

質問 # 76
Your organization has recently onboarded to Google Cloud with Security Command Center Enterprise (SCCE) and is now integrating it with your organization's SO You want to automate the response process and integrate with the existing SOW ticketing system. 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 use Pub/Sub for alerts. Create a Cloud Run function to trigger when an event arrives in the topic and generate a ticket by calling the API endpoint in the SOC ticketing system.
- C. 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.
- D. Evaluate each event within the SCC console. Create a ticket for each finding in the ticketing system, and include the remediation steps.

正解：B

質問 # 77
Your organization uses Google Security Operations (SecOps). You need to identify the most commonly occurring processes and

applications across your organization's large number of servers so you can implement baselines and exclusion lists on a regular basis. You want to use the most efficient approach. What should you do?

- A. Generate a Google SecOps SIEM dashboard based on relevant UDM fields, such as processes, that provides the counts for process names and files.
- B. Run a UDM search, and review aggregations for relevant process-related UDM fields.
- C. Use the UDM lookup feature to identify relevant process- related UDM fields and values.
- D. Review the Google SecOps SIEM Rules & Detections, and identify the most common processes appearing in alerts that are marked as false positives.

正解：B

質問 # 78
You are ingesting and parsing logs from an SSO provider and an on-premises appliance using Google Security Operations (SecOps). Users are tagged as "restricted" by an internal process. Restrictions last five days from the most recent flagging time. You need to create a rule to detect when restricted users log into the appliance. Your solution must be quickly implemented and easily maintained. What should you do?

- A. Ingest the user flags as custom enrichment data using a feed. Use a multi-event detection rule to find logins from users flagged in the entity graph.
- B. Use a Google SecOps SOAR global context value to store a list of flagged users with their corresponding time to live values. Use a SOAR job to dynamically build and deploy a new version of the detection rule with the updated list of flagged users.
- C. Store the identifiers of the flagged users in the detection rule logic. Actively monitor for newly flagged users, and add them to the detection rule logic.
- D. Store the flagged users in a data table column with their corresponding time to live values in a second column. Use row-based comparisons in your detection rule.

正解：A

質問 # 79
.....

- GCP-SOE-Bコンポーネント □ GCP-SOE-B試験勉強書 □ GCP-SOE-Bクラムメディア □ □ www.goshiken.com □サイトにて最新▸ GCP-SOE-B ◂問題集をダウンロードGCP-SOE-B学習体験談
- 試験の準備方法-便利なGCP-SOE-Bテスト模擬問題集試験-100％合格率のGCP-SOE-B受験資料更新版 □⇛ www.passtest.jp ⇚を開いて➠ GCP-SOE-B □を検索し、試験資料を無料でダウンロードしてくださいGCP-SOE-B復習時間
- GCP-SOE-B最新な問題集 □ GCP-SOE-B的中率 □ GCP-SOE-B最新な問題集 □ □ www.goshiken.com □で使える無料オンライン版《 GCP-SOE-B 》 の試験問題GCP-SOE-B復習時間
- GCP-SOE-Bクラムメディア □ GCP-SOE-B試験復習 □ GCP-SOE-B最新問題 □ 時間限定無料で使える⇛ GCP-SOE-B ⇚の試験問題は➽ www.passtest.jp □サイトで検索GCP-SOE-B学習体験談
- 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, 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, 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, Disposable vapes