Professional-Cloud-Security-Engineer新版題庫上線 & Professional-Cloud-Security-Engineer題庫

從Google Drive中免費下載最新的KaoGuTi Professional-Cloud-Security-Engineer PDF版考試題庫：https://drive.google.com/open?id=1AWG5yUY7ifMJkBvEQcovua7t4OJ-mTXW

如果你正在為如何通過Professional-Cloud-Security-Engineer考試而煩惱，這是沒有必要，通過最新的考試要點來提供覆蓋率很廣的Google Professional-Cloud-Security-Engineer擬真試題，幫助考生做好充足的考前準備。KaoGuTi的目的在于如何提供可以確保考生通過認證的高品質題庫，我們的Professional-Cloud-Security-Engineer考試練習題和答案準確性高，問題覆蓋面大，不斷的更新和整編出高通過率的Google Professional-Cloud-Security-Engineer題庫，這也是我們對所有的考生提供的保障。

Google的Professional-Cloud-Security-Engineer認證考試是為有雲安全經驗並且希望增強其技能和知識的專業人士而設計的。這個認證考試非常適合安全專業人員、雲架構師和IT專業人員，他們負責在GCP上設計、實施和管理雲安全解決方案。通過獲得這個認證，專業人士可以展示他們在雲安全方面的專業知識，增強自己的職業前景。

Google Professional-Cloud-Security-Engineer 考試是對雲安全專業人員和工程師的一項具有挑戰性和價值的認證。它衡量候選人設計和實施安全的 Google Cloud Platform 解決方案的能力，並提供職業發展和更高薪酬的機會。該認證被業界領袖所認可，有助於組織識別熟練和知識豐富的雲安全專業人員和工程師。

>> Professional-Cloud-Security-Engineer新版題庫上線 <<

Professional-Cloud-Security-Engineer題庫， Professional-Cloud-Security-Engineer認證考試解析

我受不了現在的生活和工作了，想做別的工作。你現在有這樣的想法嗎？但是，怎樣才能做更好的工作呢？你喜歡IT嗎？想通過IT來證明自己的實力嗎？如果你想從事IT方面的工作，那麼參加IT認定考試，取得認證資格是非常有必要的。你現在要做的就是參加被普遍認可的、有價值的IT資格考試。從而打開你職業生涯的新的大門。關於Google的Professional-Cloud-Security-Engineer考試，你一定不陌生吧。取得這個資格可以讓你在找工作的時候得到一份助力。什麼？沒有信心參加這個考試嗎？沒關係，你可以使用KaoGuTi的Professional-Cloud-Security-Engineer考試資料。

Google Professional-Cloud-Security-Engineer考試是一項具有挑戰性的考試，需要大量的準備和學習。候選人應該對基於雲的基礎設施和安全最佳實踐有深刻的了解。他們還應該有在基於雲的環境中設計和實施安全解決方案的經驗。通過考試的候選人將獲得一個由全球組織認可的Google Cloud Certified-專業雲安全工程師認證。此認證證明候選人具備必要的技能和知識，能夠在Google Cloud平台上保護基於雲的基礎設施。

最新的 Google Cloud Certified Professional-Cloud-Security-Engineer 免費考試真題 (Q263-Q268):

問題 #263
You are setting up a new Cloud Storage bucket in your environment that is encrypted with a customer managed encryption key (CMEK). The CMEK is stored in Cloud Key Management Service (KMS). in project
"pr j -a", and the Cloud Storage bucket will use project "prj-b". The key is backed by a Cloud Hardware Security Module (HSM)

and resides in the region europe-west3. Your storage bucket will be located in the region europe-west1. When you create the bucket, you cannot access the key. and you need to troubleshoot why.
What has caused the access issue?

- A. The CMEK is in a different region than the Cloud Storage bucket.
- B. A firewall rule prevents the key from being accessible.
- C. Cloud HSM does not support Cloud Storage
- D. The CMEK is in a different project than the Cloud Storage bucket

答案：A

解題說明：
When you use a customer-managed encryption key (CMEK) to secure a Cloud Storage bucket, the key and the bucket must be located in the same region. In this case, the key is in europe-west3 and the bucket is in europe-west1, which is why you're unable to access the key.

問題 #264
You are on your company's development team. You noticed that your web application hosted in staging on GKE dynamically includes user data in web pages without first properly validating the inputted data. This could allow an attacker to execute gibberish commands and display arbitrary content in a victim user's browser in a production environment.
How should you prevent and fix this vulnerability?

- A. Use Web Security Scanner to validate the usage of an outdated library in the code, and then use a secured version of the included library.
- B. Set up an HTTPS load balancer, and then use Cloud Armor for the production environment to prevent the potential XSS attack.
- C. Use Cloud IAP based on IP address or end-user device attributes to prevent and fix the vulnerability.
- D. Use Web Security Scanner in staging to simulate an XSS injection attack, and then use a templating system that supports contextual auto-escaping.

答案：D

解題說明：
Explanation
There is mention about simulating in Web Security Scanner. "Web Security Scanner cross-site scripting (XSS) injection testing *simulates* an injection attack by inserting a benign test string into user-editable fields and then performing various user actions."
https://cloud.google.com/security-command-center/docs/how-to-remediate-web-security-scanner-findings#xss

問題 #265
You are troubleshooting access denied errors between Compute Engine instances connected to a Shared VPC and BigQuery datasets. The datasets reside in a project protected by a VPC Service Controls perimeter. What should you do?

- A. Create a service perimeter between the service project where the Compute Engine instances reside and the host project that contains the Shared VPC.
- B. Add the service project where the Compute Engine instances reside to the service perimeter.
- C. Add the host project containing the Shared VPC to the service perimeter.
- D. Create a perimeter bridge between the service project where the Compute Engine instances reside and the perimeter that contains the protected BigQuery datasets.

答案：C

問題 #266
Your company recently published a security policy to minimize the usage of service account keys. On- premises Windows-based applications are interacting with Google Cloud APIs. You need to implement Workload Identity Federation (WIF) with your identity provider on-premises.
What should you do?

- A. Set up a workload identity pool with your corporate Active Directory Federation Service (ADFS) Let all principals in the

pool impersonate the Google Cloud service account.

- B. Set up a workload identity pool with your corporate Active Directory Federation Service (ADFS) Configure a rule to let principals in the pool impersonate the Google Cloud service account.
- C. Set up a workload identity pool with an OpenID Connect (OIDC) service on the same machine Let all principals in the pool impersonate the Google Cloud service account.
- D. Set up a workload identity pool with an OpenID Connect (OIDC) service on the name machine Configure a rule to let principals in the pool impersonate the Google Cloud service account.

答案：B

解題說明：
To minimize the usage of service account keys and implement Workload Identity Federation (WIF) with your on-premises identity provider, you can use a workload identity pool integrated with your corporate Active Directory Federation Service (ADFS). This setup allows your on-premises Windows-based applications to authenticate to Google Cloud APIs without using long-lived service account keys.
* Set Up a Workload Identity Pool:
* In the Google Cloud Console, go to IAM & Admin > Workload Identity Federation.
* Create a new workload identity pool.
* Configure the pool to trust your corporate ADFS by specifying the federation provider details.
* Create a Workload Identity Provider:
* Within the created pool, set up a new provider for ADFS.
* Configure the provider with the necessary details such as the issuer URL and credentials.
* Configure Impersonation Rules:
* Set up rules to allow principals in the workload identity pool to impersonate specific Google Cloud service accounts.
* This is done by specifying the identity provider and the conditions under which the service accounts can be impersonated.
* Update Applications:
* Modify your on-premises applications to use the configured ADFS authentication to obtain tokens.
* These tokens can then be exchanged for Google Cloud access tokens to interact with Google Cloud APIs securely.
By setting up the workload identity pool and configuring impersonation rules, you achieve secure authentication without needing to distribute and manage service account keys.
References:
* Workload Identity Federation Documentation
* Federating On-Premises Identities to Workload Identity Federation

問題 #267
Your organization must follow the Payment Card Industry Data Security Standard (PCI DSS). To prepare for an audit, you must detect deviations at an infrastructure-as-a-service level in your Google Cloud landing zone.
What should you do?

- A. Create an Assured Workloads folder in your Google Cloud organization. Migrate existing projects into the folder and monitor for deviations in the PCI DSS.
- B. Create a data profile covering all payment-relevant data types. Configure Data Discovery and a risk analysis job in Google Cloud Sensitive Data Protection to analyze findings.
- C. Activate Security Command Center Premium. Use the Compliance Monitoring product to filter findings that may not be PCI DSS compliant.
- D. Use the Google Cloud Compliance Reports Manager to download the latest version of the PCI DSS report. Analyze the report to detect deviations.

答案：C

解題說明：
To ensure compliance with the Payment Card Industry Data Security Standard (PCI DSS) at the infrastructure- as-a-service (IaaS) level within Google Cloud, it's essential to have continuous monitoring and assessment tools that can detect deviations from compliance requirements.
* Option A: Creating data profiles and configuring Data Discovery jobs in Google Cloud Sensitive Data Protection focuses on identifying and analyzing sensitive data but does not directly address infrastructure compliance monitoring.
* Option B: Downloading the latest PCI DSS report from the Compliance Reports Manager provides a static compliance report but does not offer real-time detection of deviations within your specific environment.
* Option C: Utilizing Assured Workloads helps in creating environments that meet specific compliance requirements, but migrating existing projects into such folders does not actively detect deviations; it primarily ensures that new workloads comply with

predefined policies.
* Option D: Activating Security Command Center (SCC) Premium and leveraging its Compliance Monitoring capabilities allows for continuous assessment of your Google Cloud environment against PCI DSS requirements. SCC can identify misconfigurations, vulnerabilities, and compliance violations in real-time, providing actionable insights to address any issues promptly.
Therefore, Option D is the most effective approach to detect deviations at the IaaS level in preparation for a PCI DSS audit.
References:
* Security Command Center Overview
* Security Command Center Compliance Monitoring

問題 #268
.....