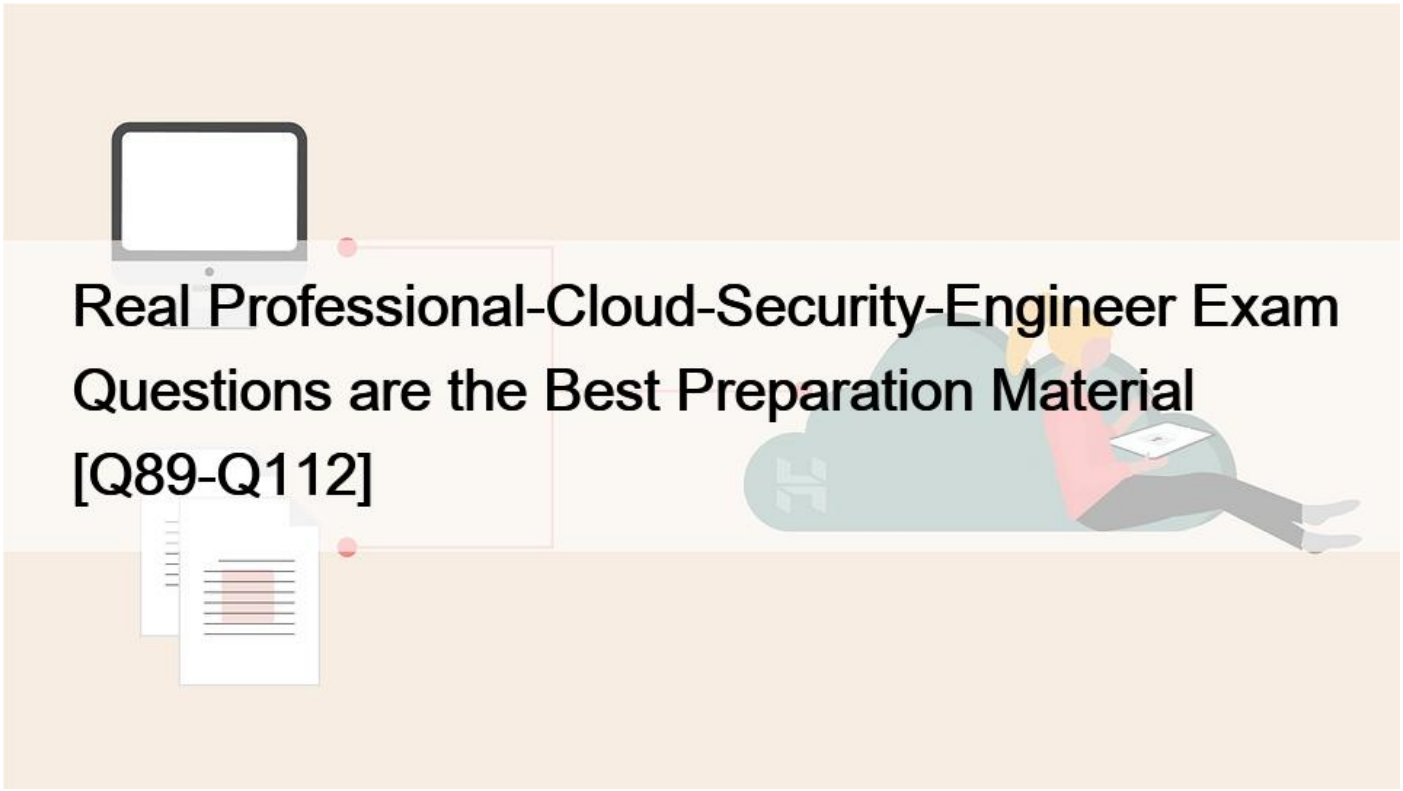
Real Professional-Cloud-Security-Engineer Exam Questions are the Best Preparation Material [Q89-Q112



Real Professional-Cloud-Security-Engineer Exam Questions are the Best Preparation Material
Practice on 2024 LATEST Professional-Cloud-Security-Engineer Exam Updated 235 Questions

QUESTION 89

Your team creates an ingress firewall rule to allow SSH access from their corporate IP range to a specific bastion host on Compute Engine. Your team wants to make sure that this firewall rule cannot be used by unauthorized engineers who may otherwise have access to manage VMs in the development environment. What should your team do to meet this requirement?
* Create the firewall rule with a target of a network tag. Centrally manage access to the tag.
* Create the firewall rule with a target of a service account. Centrally manage access to the service account.
* Create the firewall rule in a Shared VPC with a target of a network tag.
* Create the firewall rule in a Shared VPC with a target of a specific subnet.

A is not correct because the network tag value can be inferred by examining the Firewall Rule or VM metadata.

B is correct because access to the Service Account is required to use a firewall rule with a target of a Service Account.

C is not correct because the target network tag value can be inferred by examining the Firewall Rule or VM metadata.

D is not correct because the target subnet value can be inferred by examining the Firewall Rule or VM metadata.

https://cloud.google.com/vpc/docs/firewalls#service-accounts-vs-tags

QUESTION 90

Your organization is rolling out a new continuous integration and delivery (CI/CD) process to deploy infrastructure and applications in Google Cloud Many teams will use their own instances of the CI/CD workflow It will run on Google Kubernetes Engine (GKE) The CI/CD pipelines must be designed to securely access Google Cloud APIs What should you do?
* * 1 Create a dedicated service account for the CI/CD pipelines

* 2 Run the deployment pipelines in a dedicated nodes pool in the GKE cluster

* 3 Use the service account that you created as identity for the nodes in the pool to authenticate to the Google Cloud APIs
* * 1 Create service accounts for each deployment pipeline

* 2 Generate private keys for the service accounts

* 3 Securely store the private keys as Kubernetes secrets accessible only by the pods that run the specific deploy pipeline
* * 1 Create individual service accounts (or each deployment pipeline

* 2 Add an identifier for the pipeline in the service account naming convention

* 3 Ensure each pipeline runs on dedicated pods

* 4 Use workload identity to map a deployment pipeline pod with a service account
* * 1 Create two service accounts one for the infrastructure and one for the application deployment

* 2 Use workload identities to let the pods run the two pipelines and authenticate with the service accounts

* 3 Run the infrastructure and application pipelines in separate namespaces

QUESTION 91

You are migrating an application into the cloud The application will need to read data from a Cloud Storage bucket. Due to local regulatory requirements, you need to hold the key material used for encryption fully under your control and you require a valid rationale for accessing the key material.

What should you do?
* Encrypt the data in the Cloud Storage bucket by using Customer Managed Encryption Keys. Configure an 1AM deny policy for unauthorized groups
* Encrypt the data in the Cloud Storage bucket by using Customer Managed Encryption Keys backed by a Cloud Hardware Security Module (HSM). Enable data access logs.
* Generate a key in your on-premises environment and store it in a Hardware Security Module (HSM) that is managed on-premises Use this key as an external key in the Cloud Key Management Service (KMS). Activate Key Access Justifications (KAJ) and set the external key system to reject unauthorized accesses.
* Generate a key in your on-premises environment to encrypt the data before you upload the data to the Cloud Storage bucket Upload the key to the Cloud Key Management Service (KMS). Activate Key Access Justifications (KAJ) and have the external key system reject unauthorized accesses.
By generating a key in your on-premises environment and storing it in an HSM that you manage, you’re ensuring that the key material is fully under your control. Using the key as an external key in Cloud KMS allows you to use the key with Google Cloud services without having the key stored on Google Cloud. Activating Key Access Justifications (KAJ) provides a reason every time the key is accessed, and you can configure the external key system to reject unauthorized access attempts.

QUESTION 92

A customer wants to make it convenient for their mobile workforce to access a CRM web interface that is hosted on Google Cloud Platform (GCP). The CRM can only be accessed by someone on the corporate network. The customer wants to make it available over the internet. Your team requires an authentication layer in front of the application that supports two-factor authentication Which GCP product should the customer implement to meet these requirements?
* Cloud Identity-Aware Proxy
* Cloud Armor
* Cloud Endpoints
* Cloud VPN
Explanation

Cloud IAP is integrated with Google Sign-in which Multi-factor authentication can be enabled.https://cloud.google.com/iap/docs/concepts-overview

QUESTION 93

Your organization wants to be continuously evaluated against CIS Google Cloud Computing Foundations Benchmark v1 3 0 (CIS Google Cloud Foundation 1 3). Some of the controls are irrelevant to your organization and must be disregarded in evaluation. You need to create an automated system or process to ensure that only the relevant controls are evaluated.

What should you do?
* Mark all security findings that are irrelevant with a tag and a value that indicates a security exception Select all marked findings and mute them on the console every time they appear Activate Security Command Center (SCC) Premium.
* Activate Security Command Center (SCC) Premium Create a rule to mute the security findings in SCC so they are not evaluated.
* Download all findings from Security Command Center (SCC) to a CSV file Mark the findings that are part of CIS Google Cloud Foundation 1 3 in the file Ignore the entries that are irrelevant and out of scope for the company.
* Ask an external audit company to provide independent reports including needed CIS benchmarks. In the scope of the audit clarify that some of the controls are not needed and must be disregarded.

QUESTION 94

You are part of a security team investigating a compromised service account key. You need to audit which new resources were created by the service account.

What should you do?
* Query Data Access logs.
* Query Admin Activity logs.
* Query Access Transparency logs.
* Query Stackdriver Monitoring Workspace.
Explanation

Admin activity logs are always created to log entries for API calls or other actions that modify the configuration or metadata of resources. For example, these logs record when users create VM instances or change Identity and Access Management permissions.

QUESTION 95

You want to evaluate GCP for PCI compliance. You need to identify Google’s inherent controls.

Which document should you review to find the information?
* Google Cloud Platform: Customer Responsibility Matrix
* PCI DSS Requirements and Security Assessment Procedures
* PCI SSC Cloud Computing Guidelines
* Product documentation for Compute Engine
https://cloud.google.com/files/PCI_DSS_Shared_Responsibility_GCP_v32.pdf

https://services.google.com/fh/files/misc/gcp_pci_shared_responsibility_matrix_aug_2021.pdf

QUESTION 96

Your team needs to prevent users from creating projects in the organization. Only the DevOps team should be allowed to create projects on behalf of the requester.

Which two tasks should your team perform to handle this request? (Choose two.)
* Remove all users from the Project Creator role at the organizational level.
* Create an Organization Policy constraint, and apply it at the organizational level.
* Grant the Project Editor role at the organizational level to a designated group of users.
* Add a designated group of users to the Project Creator role at the organizational level.
* Grant the billing account creator role to the designated DevOps team.
Explanation

https://cloud.google.com/resource-manager/docs/organization-policy/org-policy-constraints

QUESTION 97

You need to follow Google-recommended practices to leverage envelope encryption and encrypt data at the application layer.

What should you do?
* Generate a data encryption key (DEK) locally to encrypt the data, and generate a new key encryption key (KEK) in Cloud KMS to encrypt the DEK. Store both the encrypted data and the encrypted DEK.
* Generate a data encryption key (DEK) locally to encrypt the data, and generate a new key encryption key (KEK) in Cloud KMS to encrypt the DEK. Store both the encrypted data and the KEK.
* Generate a new data encryption key (DEK) in Cloud KMS to encrypt the data, and generate a key encryption key (KEK) locally to encrypt the key. Store both the encrypted data and the encrypted DEK.
* Generate a new data encryption key (DEK) in Cloud KMS to encrypt the data, and generate a key encryption key (KEK) locally to encrypt the key. Store both the encrypted data and the KEK.
Explanation/Reference: https://cloud.google.com/kms/docs/envelope-encryption

QUESTION 98

Your Google Cloud organization allows for administrative capabilities to be distributed to each team through provision of a Google Cloud project with Owner role (roles/ owner). The organization contains thousands of Google Cloud Projects Security Command Center Premium has surfaced multiple cpen_myscl_port findings. You are enforcing the guardrails and need to prevent these types of common misconfigurations.

What should you do?
* Create a firewall rule for each virtual private cloud (VPC) to deny traffic from 0 0 0 0/0 with priority 0.
* Create a hierarchical firewall policy configured at the organization to deny all connections from 0 0 0 0/0.
* Create a Google Cloud Armor security policy to deny traffic from 0 0 0 0/0.

* Create a hierarchical firewall policy configured at the organization to allow connections only from internal IP ranges

QUESTION 99

You are in charge of migrating a legacy application from your company datacenters to GCP before the current maintenance contract expires. You do not know what ports the application is using and no documentation is available for you to check. You want to complete the migration without putting your environment at risk.

What should you do?
* Migrate the application into an isolated project using a “Lift & Shift” approach. Enable all internal TCP traffic using VPC Firewall rules. Use VPC Flow logs to determine what traffic should be allowed for the application to work properly.
* Migrate the application into an isolated project using a “Lift & Shift” approach in a custom network. Disable all traffic within the VPC and look at the Firewall logs to determine what traffic should be allowed for the application to work properly.
* Refactor the application into a micro-services architecture in a GKE cluster. Disable all traffic from outside the cluster using Firewall Rules. Use VPC Flow logs to determine what traffic should be allowed for the application to work properly.
* Refactor the application into a micro-services architecture hosted in Cloud Functions in an isolated project.

Disable all traffic from outside your project using Firewall Rules. Use VPC Flow logs to determine what traffic should be allowed for the application to work properly.

QUESTION 100

You have been tasked with configuring Security Command Center for your organization’s Google Cloud environment. Your security team needs to receive alerts of potential crypto mining in the organization’s compute environment and alerts for common Google Cloud misconfigurations that impact security. Which Security Command Center features should you use to configure these alerts? (Choose two.)
* Event Threat Detection
* Container Threat Detection
* Security Health Analytics
* Cloud Data Loss Prevention
* Google Cloud Armor
https://cloud.google.com/security-command-center/docs/concepts-event-threat-detection-overview Event Threat Detection is a built-in service for the Security Command Center Premium tier that continuously monitors your organization and identifies threats within your systems in near-real time.
https://cloud.google.com/security-command-center/docs/concepts-security-sources#security-health-analytics

QUESTION 101

Your organization is using Active Directory and wants to configure Security Assertion Markup Language (SAML). You must set up and enforce single sign-on (SSO) for all users.

What should you do?
* 1. Manage SAML profile assignments.

* 2. Enable OpenID Connect (OIDC) in your Active Directory (AD) tenant.

* 3. Verify the domain.
* 1. Create a new SAML profile.

* 2. Upload the X.509 certificate.

* 3. Enable the change password URL.

* 4. Configure Entity ID and ACS URL in your IdP.
* 1- Create a new SAML profile.

* 2. Populate the sign-in and sign-out page URLs.

* 3. Upload the X.509 certificate.

* 4. Configure Entity ID and ACS URL in your IdP
* 1. Configure prerequisites for OpenID Connect (OIDC) in your Active Directory (AD) tenant

* 2. Verify the AD domain.

* 3. Decide which users should use SAML.

* 4. Assign the pre-configured profile to the select organizational units (OUs) and groups.
When configuring SAML-based Single Sign-On (SSO) in an organization that’s using Active Directory, the general steps would involve setting up a SAML profile, specifying the necessary URLs for sign-in and sign-out processes, uploading an X.509 certificate for secure communication, and setting up the Entity ID and Assertion Consumer Service (ACS) URL in the Identity Provider (which in this case would be Active Directory).

QUESTION 102

Your organization wants to be compliant with the General Data Protection Regulation (GDPR) on Google Cloud You must implement data residency and operational sovereignty in the EU.

What should you do?

Choose 2 answers
* Limit the physical location of a new resource with the Organization Policy Service resource locations constraint.”
* Use Cloud IDS to get east-west and north-south traffic visibility in the EU to monitor intra-VPC and mter-VPC communication.
* Limit Google personnel access based on predefined attributes such as their citizenship or geographic location by using Key Access Justifications
* Use identity federation to limit access to Google Cloud resources from non-EU entities.
* Use VPC Flow Logs to monitor intra-VPC and inter-VPC traffic in the EU.
https://cloud.google.com/architecture/framework/security/data-residency-sovereignty#manage_your_operational_sovereignty

QUESTION 103

A customer has 300 engineers. The company wants to grant different levels of access and efficiently manage IAM permissions between users in the development and production environment projects.

Which two steps should the company take to meet these requirements? (Choose two.)
* Create a project with multiple VPC networks for each environment.
* Create a folder for each development and production environment.
* Create a Google Group for the Engineering team, and assign permissions at the folder level.
* Create an Organizational Policy constraint for each folder environment.
* Create projects for each environment, and grant IAM rights to each engineering user.

QUESTION 104

You are the security admin of your company. Your development team creates multiple GCP projects under the “implementation” folder for several dev, staging, and production workloads. You want to prevent data exfiltration by malicious insiders or compromised code by setting up a security perimeter. However, you do not want to restrict communication between the projects.

What should you do?
* Use a Shared VPC to enable communication between all projects, and use firewall rules to prevent data exfiltration.
* Create access levels in Access Context Manager to prevent data exfiltration, and use a shared VPC for communication between projects.
* Use an infrastructure-as-code software tool to set up a single service perimeter and to deploy a Cloud Function that monitors the “implementation” folder via Stackdriver and Cloud Pub/Sub. When the function notices that a new project is added to the folder, it executes Terraform to add the new project to the associated perimeter.
* Use an infrastructure-as-code software tool to set up three different service perimeters for dev, staging, and prod and to deploy a Cloud Function that monitors the “implementation” folder via Stackdriver and Cloud Pub/Sub. When the function notices that a new project is added to the folder, it executes Terraform to add the new project to the respective perimeter.
https://cloud.google.com/vpc-service-controls/docs/overview#benefits

https://github.com/terraform-google-modules/terraform-google-vpc-service-controls/tree/master/examples/automatic_folder

QUESTION 105

You want to limit the images that can be used as the source for boot disks. These images will be stored in a dedicated project.

What should you do?
* Use the Organization Policy Service to create a compute.trustedimageProjects constraint on the organization level. List the trusted project as the whitelist in an allow operation.
* Use the Organization Policy Service to create a compute.trustedimageProjects constraint on the organization level. List the trusted projects as the exceptions in a deny operation.
* In Resource Manager, edit the project permissions for the trusted project. Add the organization as member with the role: Compute Image User.
* In Resource Manager, edit the organization permissions. Add the project ID as member with the role: Compute Image User.

QUESTION 106

Your organization recently deployed a new application on Google Kubernetes Engine. You need to deploy a solution to protect the application. The solution has the following requirements:

Scans must run at least once per week

Must be able to detect cross-site scripting vulnerabilities

Must be able to authenticate using Google accounts

Which solution should you use?
* Google Cloud Armor
* Web Security Scanner
* Security Health Analytics

* Container Threat Detection

QUESTION 107

A DevOps team will create a new container to run on Google Kubernetes Engine. As the application will be internet-facing, they want to minimize the attack surface of the container.

What should they do?
* Use Cloud Build to build the container images.
* Build small containers using small base images.
* Delete non-used versions from Container Registry.
* Use a Continuous Delivery tool to deploy the application.
https://cloud.google.com/solutions/best-practices-for-building-containers

QUESTION 108

You are a consultant for an organization that is considering migrating their data from its private cloud to Google Cloud. The organization’s compliance team is not familiar with Google Cloud and needs guidance on how compliance requirements will be met on Google Cloud. One specific compliance requirement is for customer data at rest to reside within specific geographic boundaries. Which option should you recommend for the organization to meet their data residency requirements on Google Cloud?
* Organization Policy Service constraints
* Shielded VM instances
* Access control lists
* Geolocation access controls
* Google Cloud Armor
https://cloud.google.com/resource-manager/docs/organization-policy/using-constraints#list-constraint

QUESTION 109

You will create a new Service Account that should be able to list the Compute Engine instances in the project. You want to follow Google-recommended practices.

What should you do?
* Create an Instance Template, and allow the Service Account Read Only access for the Compute Engine Access Scope.
* Create a custom role with the permission compute.instances.list and grant the Service Account this role.
* Give the Service Account the role of Compute Viewer, and use the new Service Account for all instances.
* Give the Service Account the role of Project Viewer, and use the new Service Account for all instances.
https://cloud.google.com/compute/docs/access/iam

QUESTION 110

An organization is moving applications to Google Cloud while maintaining a few mission-critical applications on-premises. The organization must transfer the data at a bandwidth of at least 50 Gbps. What should they use to ensure secure continued connectivity between sites?
* Dedicated Interconnect
* Cloud Router
* Cloud VPN
* Partner Interconnect
Reference:

https://cloud.google.com/network-connectivity/docs/interconnect/concepts/overview

QUESTION 111

Your organization wants full control of the keys used to encrypt data at rest in their Google Cloud environments. Keys must be generated and stored outside of Google and integrate with many Google Services including BigQuery.

What should you do?
* Create a Cloud Key Management Service (KMS) key with imported key material Wrap the key for protection during import. Import the key generated on a trusted system in Cloud KMS.
* Create a KMS key that is stored on a Google managed FIPS 140-2 level 3 Hardware Security Module (HSM) Manage the Identity and Access Management (IAM) permissions settings, and set up the key rotation period.
* Use Cloud External Key Management (EKM) that integrates with an external Hardware Security Module (HSM) system from supported vendors.
* Use customer-supplied encryption keys (CSEK) with keys generated on trusted external systems Provide the raw CSEK as part of the API call.
Cloud EKM allows you to use encryption keys that are stored and managed in a third-party key management system deployed outside of Google’s infrastructure. This gives your organization full control over the keys used to encrypt data at rest in Google Cloud environments, including BigQuery.

QUESTION 112

You need to connect your organization’s on-premises network with an existing Google Cloud environment that includes one Shared VPC with two subnets named Production and Non-Production. You are required to:

Use a private transport link.

Configure access to Google Cloud APIs through private API endpoints originating from on-premises environments.

Ensure that Google Cloud APIs are only consumed via VPC Service Controls.

What should you do?
* 1. Set up a Cloud VPN link between the on-premises environment and Google Cloud.

2. Configure private access using the restricted googleapis.com domains in on-premises DNS configurations.
* 1. Set up a Partner Interconnect link between the on-premises environment and Google Cloud.

2. Configure private access using the private.googleapis.com domains in on-premises DNS configurations.
* 1. Set up a Direct Peering link between the on-premises environment and Google Cloud.

2. Configure private access for both VPC subnets.
* 1. Set up a Dedicated Interconnect link between the on-premises environment and Google Cloud.

2. Configure private access using the restricted.googleapis.com domains in on-premises DNS configurations.
Explanation

restricted.googleapis.com (199.36.153.4/30) only provides access to Cloud and Developer APIs that support VPC Service Controls. VPC Service Controls are enforced for these services

https://cloud.google.com/vpc/docs/configure-private-google-access-hybrid

Authentic Professional-Cloud-Security-Engineer Exam Dumps PDF - Jun-2024 Updated:
https://www.test4engine.com/Professional-Cloud-Security-Engineer_exam-latest-braindumps.html]