Professional Cloud Security Engineer

1. Your team needs to make sure that a Compute Engine instance does not have access to the internet or to any Google APIs or services.
Which two settings must remain disabled to meet these requirements? (Choose two.)

- [ ] A. Public IP
- [ ] B. IP Forwarding
- [ ] C. Private Google Access
- [ ] D. Static routes
- [ ] E. IAM Network User Role

Answer(s): A C

---

2. Which two implied firewall rules are defined on a VPC network? (Choose two.)

- [ ] A. A rule that allows all outbound connections
- [ ] B. A rule that denies all inbound connections
- [ ] C. A rule that blocks all inbound port 25 connections
- [ ] D. A rule that blocks all outbound connections
- [ ] E. A rule that allows all inbound port 80 connections

Answer(s): A B

---

3. A customer needs an alternative to storing their plain text secrets in their source-code management (SCM) system.

How should the customer achieve this using Google Cloud Platform?

A. Use Cloud Source Repositories, and store secrets in Cloud SQL.

B. Encrypt the secrets with a Customer-Managed Encryption Key (CMEK), and store them in Cloud Storage.

C. Run the Cloud Data Loss Prevention API to scan the secrets, and store them in Cloud SQL.

D. Deploy the SCM to a Compute Engine VM with local SSDs, and enable preemptible VMs.

Answer(s): B

---

4. Your team wants to centrally manage GCP IAM permissions from their on-premises Active Directory Service. Your team wants to manage permissions by AD group membership.
What should your team do to meet these requirements?

A. Set up Cloud Directory Sync to sync groups, and set IAM permissions on the groups.

B. Set up SAML 2.0 Single Sign-On (SSO), and assign IAM permissions to the groups.

C. Use the Cloud Identity and Access Management API to create groups and IAM permissions from Active Directory.

D. Use the Admin SDK to create groups and assign IAM permissions from Active Directory.

Answer(s): A

---

5. When creating a secure container image, which two items should you incorporate into the build if possible? (Choose two.)

- [ ] A. Ensure that the app does not run as PID 1.
- [ ] B. Package a single app as a container.
- [ ] C. Remove any unnecessary tools not needed by the app.

- [ ] D. Use public container images as a base image for the app.
- [ ] E. Use many container image layers to hide sensitive information.

Answer(s): B C

---

6. A customer needs to launch a 3-tier internal web application on Google Cloud Platform (GCP). The customer's internal compliance requirements dictate that end-user access may only be allowed if the traffic seems to originate from a specific known good CIDR. The customer accepts the risk that their application will only have SYN flood DDoS protection. They want to use GCP's native SYN flood protection.
Which product should be used to meet these requirements?

A. Cloud Armor

B. VPC Firewall Rules

C. Cloud Identity and Access Management

D. Cloud CDN

Answer(s): A

---

7. A company is running workloads in a dedicated server room. They must only be accessed from within the private company network. You need to connect to these workloads from Compute Engine instances within a Google Cloud Platform project.
Which two approaches can you take to meet the requirements? (Choose two.)

- [ ] A. Configure the project with Cloud VPN.
- [ ] B. Configure the project with Shared VPC.
- [ ] C. Configure the project with Cloud Interconnect.
- [ ] D. Configure the project with VPC peering.
- [ ] E. Configure all Compute Engine instances with Private Access.

Answer(s): A C

---

8. A customer implements Cloud Identity-Aware Proxy for their ERP system hosted on Compute Engine. Their security team wants to add a security layer so that the ERP systems only accept traffic from Cloud Identity- Aware Proxy.
What should the customer do to meet these requirements?

A. Make sure that the ERP system can validate the JWT assertion in the HTTP requests.

B. Make sure that the ERP system can validate the identity headers in the HTTP requests.

C. Make sure that the ERP system can validate the x-forwarded-for headers in the HTTP requests.

D. Make sure that the ERP system can validate the user's unique identifier headers in the HTTP requests.

Answer(s): A

---

9. A company has been running their application on Compute Engine. A bug in the application allowed a malicious user to repeatedly execute a script that results in the Compute Engine instance crashing. Although the bug has been fixed, you want to get notified in case this hack re-occurs.
What should you do?

A. Create an Alerting Policy in Stackdriver using a Process Health condition, checking that the number of executions of the script remains below the desired threshold. Enable notifications.

B. Create an Alerting Policy in Stackdriver using the CPU usage metric. Set the threshold to 80% to be notified when the CPU usage goes above this 80%.

C. Log every execution of the script to Stackdriver Logging. Create a User-defined metric in Stackdriver Logging on the logs, and create a Stackdriver Dashboard displaying the metric.

D. Log every execution of the script to Stackdriver Logging. Configure BigQuery as a log sink, and create a BigQuery scheduled query to count the number of executions in a specific timeframe.

Answer(s): A

---

10. Your team needs to obtain a unified log view of all development cloud projects in your SIEM. The development projects are under the NONPROD organization folder with the test and pre-production projects. The development projects share the ABC-BILLING billing account with the rest of the organization.
Which logging export strategy should you use to meet the requirements?

A. 1. Export logs to a Cloud Pub/Sub topic with folders/NONPROD parent and includeChildren property set to True in a dedicated SIEM project.2. Subscribe SIEM to the topic.

B. 1. Create a Cloud Storage sink with billingAccounts/ABC-BILLING parent and includeChildren property set to False in a dedicated SIEM project.2. Process Cloud Storage objects in SIEM.

C. 1. Export logs in each dev project to a Cloud Pub/Sub topic in a dedicated SIEM project.2. Subscribe SIEM to the topic.

D. 1. Create a Cloud Storage sink with a publicly shared Cloud Storage bucket in each project.2. Process Cloud Storage objects in SIEM.

Answer(s): C

---

11. A customer needs to prevent attackers from hijacking their domain/IP and redirecting users to a malicious site through a man-in-the-middle attack.
Which solution should this customer use?

A. VPC Flow Logs

B. Cloud Armor

C. DNS Security Extensions

D. Cloud Identity-Aware Proxy

Answer(s): C

---

12. A customer deploys an application to App Engine and needs to check for Open Web Application Security Project (OWASP) vulnerabilities.
Which service should be used to accomplish this?

A. Cloud Armor

B. Google Cloud Audit Logs

C. Cloud Security Scanner

D. Forseti Security

Answer(s): C

---

13. A customer's data science group wants to use Google Cloud Platform (GCP) for their analytics workloads. Company policy dictates that all data must be company-owned and all user authentications must go through their own Security Assertion Markup Language (SAML) 2.0 Identity Provider (IdP). The Infrastructure Operations Systems Engineer was trying to set up Cloud Identity for the customer and realized that their domain was already being used by G Suite.
How should you best advise the Systems Engineer to proceed with the least disruption?

A. Contact Google Support and initiate the Domain Contestation Process to use the domain name in your new Cloud Identity domain.

B. Register a new domain name, and use that for the new Cloud Identity domain.

C. Ask Google to provision the data science manager's account as a Super Administrator in the existing domain.

D. Ask customer's management to discover any other uses of Google managed services, and work with the existing Super Administrator.

Answer(s): D

---

14. A business unit at a multinational corporation signs up for GCP and starts moving workloads into GCP. The business unit creates a Cloud Identity domain with an organizational resource that has hundreds of projects.
Your team becomes aware of this and wants to take over managing permissions and auditing the domain resources.
Which type of access should your team grant to meet this requirement?

A. Organization Administrator

B. Security Reviewer

C. Organization Role Administrator

D. Organization Policy Administrator

Answer(s): C

---

15. An application running on a Compute Engine instance needs to read data from a Cloud Storage bucket. Your team does not allow Cloud Storage buckets to be globally readable and wants to ensure the principle of least privilege.
Which option meets the requirement of your team?

A. Create a Cloud Storage ACL that allows read-only access from the Compute Engine instance's IP address and allows the application to read from the bucket without credentials.

B. Use a service account with read-only access to the Cloud Storage bucket, and store the credentials to the service account in the config of the application on the Compute Engine instance.

C. Use a service account with read-only access to the Cloud Storage bucket to retrieve the credentials from the instance metadata.

D. Encrypt the data in the Cloud Storage bucket using Cloud KMS, and allow the application to decrypt the data with the KMS key.

Answer(s): C

---

16. An organization's typical network and security review consists of analyzing application transit routes, request handling, and firewall rules. They want to enable their developer teams to deploy new applications without the overhead of this full review.
How should you advise this organization?

A. Use Forseti with Firewall filters to catch any unwanted configurations in production.

B. Mandate use of infrastructure as code and provide static analysis in the CI/CD pipelines to enforce policies.

C. Route all VPC traffic through customer-managed routers to detect malicious patterns in production.

D. All production applications will run on-premises. Allow developers free rein in GCP as their dev and QA platforms.

Answer(s): B

---

17. An employer wants to track how bonus compensations have changed over time to identify employee outliers and correct earning disparities. This task must be performed without exposing the sensitive compensation data for any individual and must be reversible to identify the outlier.
Which Cloud Data Loss Prevention API technique should you use to accomplish this?

A. Generalization

B. Redaction

C. CryptoHashConfig

D. CryptoReplaceFfxFpeConfig

Answer(s): D

---

18. An organization adopts Google Cloud Platform (GCP) for application hosting services and needs guidance on setting up password requirements for their Cloud Identity account. The organization has a password policy requirement that corporate employee passwords must have a minimum number of characters.
Which Cloud Identity password guidelines can the organization use to inform their new requirements?

A. Set the minimum length for passwords to be 8 characters.

B. Set the minimum length for passwords to be 10 characters.

C. Set the minimum length for passwords to be 12 characters.

D. Set the minimum length for passwords to be 6 characters.

Answer(s): A

---

19. You need to follow Google-recommended practices to leverage envelope encryption and encrypt data at the application layer.
What should you do?

A. 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.

B. 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.

C. 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.

D. 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.

Answer(s): A

---

20. How should a customer reliably deliver Stackdriver logs from GCP to their on-premises SIEM system?

A. Send all logs to the SIEM system via an existing protocol such as syslog.

B. Configure every project to export all their logs to a common BigQuery DataSet, which will be queried by the SIEM system.

C. Configure Organizational Log Sinks to export logs to a Cloud Pub/Sub Topic, which will be sent to the SIEM via Dataflow.

D. Build a connector for the SIEM to query for all logs in real time from the GCP RESTful JSON APIs.

Answer(s): C
