Number: Professional Cloud Security Engineer
Passing Score: 800
Time Limit: 120
File Version: 7.0

Certification: Professional Cloud Security Engineer
Certification Full Name: Professional Cloud Security Engineer

Exam A

QUESTION 1
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

Correct Answer: A
Section:

QUESTION 2
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.

Correct Answer: A, C
Section:
Explanation:
A) IPsec VPN tunels: https://cloud.google.com/network-connectivity/docs/vpn/concepts/overview
Interconnect https://cloud.google.com/network-connectivity/docs/interconnect/concepts/dedicated-overview

QUESTION 3
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.

Correct Answer: A
Section:
Explanation:

Use Cryptographic Verification If there is a risk of IAP being turned off or bypassed, your app can check to make sure the identity information it receives is valid. This uses a third web request header added by IAP, called X-Goog-IAP-JWT-Assertion. The value of the header is a cryptographically signed object that also contains the user identity data. Your application can verify the digital signature and use the data provided in this object to be certain that it was provided by IAP without alteration.

QUESTION 4
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.

Correct Answer: A
Section:

QUESTION 5
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.

Correct Answer: C
Section:
Explanation:
'Your team needs to obtain a unified log view of all development cloud projects in your SIEM' - This means we are ONLY interested in development projects. 'The development projects are under the NONPROD organization folder with the test and pre-production projects' - We will need to filter out development from others i.e test and pre-prod. 'The development projects share the ABC-BILLING billing account with the rest of the organization.' - This is unnecessary information.

QUESTION 6
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

Correct Answer: C

Section:
Explanation:
DNSSEC --- use a DNS registrar that supports DNSSEC, and enable it. DNSSEC digitally signs DNS communication, making it more difficult (but not impossible) for hackers to intercept and spoof. Domain Name System Security Extensions (DNSSEC) adds security to the Domain Name System (DNS) protocol by enabling DNS responses to be validated. Having a trustworthy Domain Name System (DNS) that translates a domain name like www.example.com into its associated IP address is an increasingly important building block of today's web-based applications. Attackers can hijack this process of domain/IP lookup and redirect users to a malicious site through DNS hijacking and man-in-the-middle attacks. DNSSEC helps mitigate the risk of such attacks by cryptographically signing DNS records. As a result, it prevents attackers from issuing fake DNS responses that may misdirect browsers to nefarious websites. https://cloud.google.com/blog/products/gcp/dnssec-now-available-in-cloud-dns

QUESTION 7
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

Correct Answer: C
Section:
Explanation:
Web Security Scanner supports categories in the OWASP Top Ten, a document that ranks and provides remediation guidance for the top 10 most critical web application security risks, as determined by the Open Web Application Security Project (OWASP). https://cloud.google.com/security-command-center/docs/concepts-web-security-scanner-overview#detectors_and_compliance

QUESTION 8
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.

Correct Answer: D
Section:
Explanation:
https://support.google.com/cloudidentity/answer/7389973

QUESTION 9
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

Correct Answer: C
Section:
Explanation:
Here are the permissions available to organizationRoleAdmin
iam.roles.create
iam.roles.delete
iam.roles.undelete
iam.roles.get
iam.roles.list
iam.roles.update
resourcemanager.projects.get
resourcemanager.projects.getIamPolicy
resourcemanager.projects.list
resourcemanager.organizations.get
resourcemanager.organizations.getIamPolicy
There are sufficient as per least privilege policy. You can do user management as well as auditing.
https://cloud.google.com/iam/docs/understanding-custom-roles

QUESTION 10
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.

Correct Answer: C
Section:
Explanation:
If the environment variable GOOGLE_APPLICATION_CREDENTIALS is set, ADC uses the service account key or configuration file that the variable points to. If the environment variable GOOGLE_APPLICATION_CREDENTIALS isn't set, ADC uses the service account that is attached to the resource that is running your code. https://cloud.google.com/docs/authentication/production#passing_the_path_to_the_service_account_key_in_code

QUESTION 11
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.

Correct Answer: B
Section:
Explanation:
https://cloud.google.com/recommender/docs/tutorial-iac

QUESTION 12
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

Correct Answer: D
Section:
Explanation:
De-identifying sensitive data Cloud Data Loss Prevention (DLP) can de-identify sensitive data in text content, including text stored in container structures such as tables. De-identification is the process of removing identifying information from data. The API detects sensitive data such as personally identifiable information (PII), and then uses a de-identification transformation to mask, delete, or otherwise obscure the data. For example, de-identification techniques can include any of the following: Masking sensitive data by partially or fully replacing characters with a symbol, such as an asterisk (*) or hash (#). Replacing each instance of sensitive data with a token, or surrogate, string. Encrypting and replacing sensitive data using a randomly generated or pre-determined key. When you de-identify data using the CryptoReplaceFfxFpeConfig or CryptoDeterministicConfig infoType transformations, you can re-identify that data, as long as you have the CryptoKey used to originally de-identify the data. https://cloud.google.com/dlp/docs/deidentify-sensitive-data

QUESTION 13
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.

Correct Answer: A
Section:
Explanation:
Default password length is 8 characters. https://support.google.com/cloudidentity/answer/33319?hl=en
https://support.google.com/cloudidentity/answer/139399?hl=en#:~:text=It%20can%20be%20between%208,decide%20to%20change%20their%20password.

QUESTION 14
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.

Correct Answer: A
Section:
Explanation:
Envelope Encryption: https://cloud.google.com/kms/docs/envelope-encryption

Here are best practices for managing DEKs:
-Generate DEKs locally.
-When stored, always ensure DEKs are encrypted at rest.
- For easy access, store the DEK near the data that it encrypts.
The DEK is encrypted (also known as wrapped) by a key encryption key (KEK). The process of encrypting a key with another key is known as envelope encryption.
Here are best practices for managing KEKs:
-Store KEKs centrally. (KMS)
-Set the granularity of the DEKs they encrypt based on their use case. For example, consider a workload that requires multiple DEKs to encrypt the workload's data chunks. You could use a single KEK to wrap all DEKs that are responsible for that workload's encryption.
-Rotate keys regularly, and also after a suspected incident.

QUESTION 15
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.

Correct Answer: C
Section:
Explanation:
Scenarios for exporting Cloud Logging data: Splunk This scenario shows how to export selected logs from Cloud Logging to Pub/Sub for ingestion into Splunk. Splunk is a security information and event management (SIEM) solution that supports several ways of ingesting data, such as receiving streaming data out of Google Cloud through Splunk HTTP Event Collector (HEC) or by fetching data from Google Cloud APIs through Splunk Add-on for Google Cloud. Using the Pub/Sub to Splunk Dataflow template, you can natively forward logs and events from a Pub/Sub topic into Splunk HEC. If Splunk HEC is not available in your Splunk deployment, you can use the Add-on to collect the logs and events from the Pub/Sub topic. https://cloud.google.com/solutions/exporting-stackdriver-logging-for-splunk

QUESTION 16
In order to meet PCI DSS requirements, a customer wants to ensure that all outbound traffic is authorized.
Which two cloud offerings meet this requirement without additional compensating controls? (Choose two.)

A. App Engine
B. Cloud Functions
C. Compute Engine
D. Google Kubernetes Engine
E. Cloud Storage

Correct Answer: C, D
Section:
Explanation:
App Engine ingress firewall rules are available, but egress rules are not currently available. Per requirements 1.2.1 and 1.3.4, you must ensure that all outbound traffic is authorized. SAQ A-EP and SAQ D--type merchants must provide compensating controls or use a different Google Cloud product. Compute Engine and GKE are the preferred alternatives. https://cloud.google.com/solutions/pci-dss-compliance-in-gcp

QUESTION 17
A website design company recently migrated all customer sites to App Engine. Some sites are still in progress and should only be visible to customers and company employees from any location.
Which solution will restrict access to the in-progress sites?

A. Upload an .htaccess file containing the customer and employee user accounts to App Engine.

B. Create an App Engine firewall rule that allows access from the customer and employee networks and denies all other traffic.
C. Enable Cloud Identity-Aware Proxy (IAP), and allow access to a Google Group that contains the customer and employee user accounts.
D. Use Cloud VPN to create a VPN connection between the relevant on-premises networks and the company's GCP Virtual Private Cloud (VPC) network.

Correct Answer: C
Section:
Explanation:
https://cloud.google.com/iap/docs/concepts-overview#when_to_use_iap

QUESTION 18
When working with agents in a support center via online chat, an organization's customers often share pictures of their documents with personally identifiable information (PII). The organization that owns the support center is concerned that the PII is being stored in their databases as part of the regular chat logs they retain for review by internal or external analysts for customer service trend analysis.
Which Google Cloud solution should the organization use to help resolve this concern for the customer while still maintaining data utility?

A. Use Cloud Key Management Service (KMS) to encrypt the PII data shared by customers before storing it for analysis.
B. Use Object Lifecycle Management to make sure that all chat records with PII in them are discarded and not saved for analysis.
C. Use the image inspection and redaction actions of the DLP API to redact PII from the images before storing them for analysis.
D. Use the generalization and bucketing actions of the DLP API solution to redact PII from the texts before storing them for analysis.

Correct Answer: C
Section:
Explanation:
https://cloud.google.com/dlp/docs/concepts-image-redaction

QUESTION 19
A company's application is deployed with a user-managed Service Account key. You want to use Google- recommended practices to rotate the key.
What should you do?

A. Open Cloud Shell and run gcloud iam service-accounts enable-auto-rotate --iam- account=IAM_ACCOUNT.
B. Open Cloud Shell and run gcloud iam service-accounts keys rotate --iam- account=IAM_ACCOUNT --key=NEW_KEY.
C. Create a new key, and use the new key in the application. Delete the old key from the Service Account.
D. Create a new key, and use the new key in the application. Store the old key on the system as a backup key.

Correct Answer: C
Section:
Explanation:
You can rotate a key by creating a new key, updating applications to use the new key, and deleting the old key. Use the serviceAccount.keys.create() method and serviceAccount.keys.delete() method together to automate the rotation.

QUESTION 20
Your team needs to configure their Google Cloud Platform (GCP) environment so they can centralize the control over networking resources like firewall rules, subnets, and routes. They also have an on-premises environment where resources need access back to the GCP resources through a private VPN connection. The networking resources will need to be controlled by the network security team.
Which type of networking design should your team use to meet these requirements?

A. Shared VPC Network with a host project and service projects
B. Grant Compute Admin role to the networking team for each engineering project
C. VPC peering between all engineering projects using a hub and spoke model

D. Cloud VPN Gateway between all engineering projects using a hub and spoke model

Correct Answer: A
Section:
Explanation:
Use Shared VPC to connect to a common VPC network. Resources in those projects can communicate with each other securely and efficiently across project boundaries using internal IPs. You can manage shared network resources, such as subnets, routes, and firewalls, from a central host project, enabling you to apply and enforce consistent network policies across the projects.

QUESTION 21
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?

A. 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.
B. 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.
C. In Resource Manager, edit the project permissions for the trusted project. Add the organization as member with the role: Compute Image User.
D. In Resource Manager, edit the organization permissions. Add the project ID as member with the role: Compute Image User.

Correct Answer: B
Section:
Explanation:
Reference: https://cloud.google.com/compute/docs/images/restricting-image-access

QUESTION 22
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.)

A. Remove all users from the Project Creator role at the organizational level.
B. Create an Organization Policy constraint, and apply it at the organizational level.
C. Grant the Project Editor role at the organizational level to a designated group of users.
D. Add a designated group of users to the Project Creator role at the organizational level.
E. Grant the billing account creator role to the designated DevOps team.

Correct Answer: A, D
Section:
Explanation:
https://cloud.google.com/resource-manager/docs/organization-policy/org-policy-constraints

QUESTION 23
A customer deployed an application on Compute Engine that takes advantage of the elastic nature of cloud computing.
How can you work with Infrastructure Operations Engineers to best ensure that Windows Compute Engine VMs are up to date with all the latest OS patches?

A. Build new base images when patches are available, and use a CI/CD pipeline to rebuild VMs, deploying incrementally.
B. Federate a Domain Controller into Compute Engine, and roll out weekly patches via Group Policy Object.
C. Use Deployment Manager to provision updated VMs into new serving Instance Groups (IGs).
D. Reboot all VMs during the weekly maintenance window and allow the StartUp Script to download the latest patches from the internet.

Correct Answer: A
Section:

Explanation:
Compute Engine doesn't automatically update the OS or the software on your deployed instances. You will need to patch or update your deployed Compute Engine instances when necessary. However, in the cloud it is not recommended that you patch or update individual running instances. Instead it is best to patch the image that was used to launch the instance and then replace each affected instance with a new copy.

QUESTION 24
Your team needs to make sure that their backend database can only be accessed by the frontend application and no other instances on the network.
How should your team design this network?

A. Create an ingress firewall rule to allow access only from the application to the database using firewall tags.
B. Create a different subnet for the frontend application and database to ensure network isolation.
C. Create two VPC networks, and connect the two networks using Cloud VPN gateways to ensure network isolation.
D. Create two VPC networks, and connect the two networks using VPC peering to ensure network isolation.

Correct Answer: A
Section:
Explanation:
'However, even though it is possible to uses tags for target filtering in this manner, we recommend that you use service accounts where possible. Target tags are not access-controlled and can be changed by someone with the instanceAdmin role while VMs are in service. Service accounts are access-controlled, meaning that a specific user must be explicitly authorized to use a service account. There can only be one service account per instance, whereas there can be multiple tags. Also, service accounts assigned to a VM can only be changed when the VM is stopped'

QUESTION 25
An organization receives an increasing number of phishing emails.
Which method should be used to protect employee credentials in this situation?

A. Multifactor Authentication
B. A strict password policy
C. Captcha on login pages
D. Encrypted emails

Correct Answer: A
Section:
Explanation:
https://cloud.google.com/blog/products/g-suite/7-ways-admins-can-help-secure-accounts-against-phishing-g-suite
https://www.duocircle.com/content/email-security-services/email-security-in-cryptography#:~:text=Customer%20Login-,Email%20Security%20In%20Cryptography%20Is%20One%20Of%20The%20Most,Measures%20To%20Prevent%20Phishing%20Attempts&text=Cybercriminals%20love%20emails%20the%20most,networks%20all%20over%20the%20world.

QUESTION 26
A customer is collaborating with another company to build an application on Compute Engine. The customer is building the application tier in their GCP Organization, and the other company is building the storage tier in a different GCP Organization. This is a 3-tier web application. Communication between portions of the application must not traverse the public internet by any means.
Which connectivity option should be implemented?

A. VPC peering
B. Cloud VPN
C. Cloud Interconnect
D. Shared VPC

Correct Answer: A

Section:
Explanation:
Peering two VPCs does permit traffic to flow between the two shared networks, but it's only bi-directional. Peered VPC networks remain administratively separate.

QUESTION 27
Your team wants to make sure Compute Engine instances running in your production project do not have public IP addresses. The frontend application Compute Engine instances will require public IPs. The product engineers have the Editor role to modify resources. Your team wants to enforce this requirement.
How should your team meet these requirements?

A. Enable Private Access on the VPC network in the production project.
B. Remove the Editor role and grant the Compute Admin IAM role to the engineers.
C. Set up an organization policy to only permit public IPs for the front-end Compute Engine instances.
D. Set up a VPC network with two subnets: one with public IPs and one without public IPs.

Correct Answer: C
Section:
Explanation:
https://cloud.google.com/resource-manager/docs/organization-policy/org-policy-constraints#constraints-for-specific-services

QUESTION 28
Which two security characteristics are related to the use of VPC peering to connect two VPC networks? (Choose two.)

A. Central management of routes, firewalls, and VPNs for peered networks
B. Non-transitive peered networks; where only directly peered networks can communicate
C. Ability to peer networks that belong to different Google Cloud Platform organizations
D. Firewall rules that can be created with a tag from one peered network to another peered network
E. Ability to share specific subnets across peered networks

Correct Answer: B, C
Section:
Explanation:
https://cloud.google.com/vpc/docs/vpc-peering#key_properties

QUESTION 29
A patch for a vulnerability has been released, and a DevOps team needs to update their running containers in Google Kubernetes Engine (GKE).
How should the DevOps team accomplish this?

A. Use Puppet or Chef to push out the patch to the running container.
B. Verify that auto upgrade is enabled; if so, Google will upgrade the nodes in a GKE cluster.
C. Update the application code or apply a patch, build a new image, and redeploy it.
D. Configure containers to automatically upgrade when the base image is available in Container Registry.

Correct Answer: C
Section:
Explanation:
https://cloud.google.com/containers/security
Containers are meant to be immutable, so you deploy a new image in order to make changes. You can simplify patch management by rebuilding your images regularly, so the patch is picked up the next time a container is deployed. Get the full picture of your environment with regular image security reviews.

QUESTION 30
A company is running their webshop on Google Kubernetes Engine and wants to analyze customer transactions in BigQuery. You need to ensure that no credit card numbers are stored in BigQuery
What should you do?

A. Create a BigQuery view with regular expressions matching credit card numbers to query and delete affected rows.
B. Use the Cloud Data Loss Prevention API to redact related infoTypes before data is ingested into BigQuery.
C. Leverage Security Command Center to scan for the assets of type Credit Card Number in BigQuery.
D. Enable Cloud Identity-Aware Proxy to filter out credit card numbers before storing the logs in BigQuery.

Correct Answer: B
Section:
Explanation:
https://cloud.google.com/bigquery/docs/scan-with-dlp
Cloud Data Loss Prevention API allows to detect and redact or remove sensitive data before the comments or reviews are published. Cloud DLP will read information from BigQuery, Cloud Storage or Datastore and scan it for sensitive data.

QUESTION 31
A customer wants to deploy a large number of 3-tier web applications on Compute Engine.
How should the customer ensure authenticated network separation between the different tiers of the application?

A. Run each tier in its own Project, and segregate using Project labels.
B. Run each tier with a different Service Account (SA), and use SA-based firewall rules.
C. Run each tier in its own subnet, and use subnet-based firewall rules.
D. Run each tier with its own VM tags, and use tag-based firewall rules.

Correct Answer: B
Section:
Explanation:
'Isolate VMs using service accounts when possible' 'even though it is possible to uses tags for target filtering in this manner, we recommend that you use service accounts where possible. Target tags are not access-controlled and can be changed by someone with the instanceAdmin role while VMs are in service. Service accounts are access-controlled, meaning that a specific user must be explicitly authorized to use a service account. There can only be one service account per instance, whereas there can be multiple tags. Also, service accounts assigned to a VM can only be changed when the VM is stopped.' https://cloud.google.com/solutions/best-practices-vpc-design#isolate-vms-service-accounts

QUESTION 32
A manager wants to start retaining security event logs for 2 years while minimizing costs. You write a filter to select the appropriate log entries.
Where should you export the logs?

A. BigQuery datasets
B. Cloud Storage buckets
C. StackDriver logging
D. Cloud Pub/Sub topics

Correct Answer: B
Section:

QUESTION 33
For compliance reasons, an organization needs to ensure that in-scope PCI Kubernetes Pods reside on ''in- scope'' Nodes only. These Nodes can only contain the ''in-scope'' Pods.
How should the organization achieve this objective?

A. Add a nodeSelector field to the pod configuration to only use the Nodes labeled inscope: true.
B. Create a node pool with the label inscope: true and a Pod Security Policy that only allows the Pods to run on Nodes with that label.
C. Place a taint on the Nodes with the label inscope: true and effect NoSchedule and a toleration to match in the Pod configuration.
D. Run all in-scope Pods in the namespace ''in-scope-pci''.

Correct Answer: A
Section:
Explanation:
nodeSelector is the simplest recommended form of node selection constraint. You can add the nodeSelector field to your Pod specification and specify the node labels you want the target node to have. Kubernetes only schedules the Pod onto nodes that have each of the labels you specify. => https://kubernetes.io/docs/concepts/scheduling-eviction/assign-pod-node/#nodeselector Tolerations are applied to pods. Tolerations allow the scheduler to schedule pods with matching taints. Tolerations allow scheduling but don't guarantee scheduling: the scheduler also evaluates other parameters as part of its function. => https://kubernetes.io/docs/concepts/scheduling-eviction/taint-and-toleration/

QUESTION 34
In an effort for your company messaging app to comply with FIPS 140-2, a decision was made to use GCP compute and network services. The messaging app architecture includes a Managed Instance Group (MIG) that controls a cluster of Compute Engine instances. The instances use Local SSDs for data caching and UDP for instance-to-instance communications. The app development team is willing to make any changes necessary to comply with the standard
Which options should you recommend to meet the requirements?

A. Encrypt all cache storage and VM-to-VM communication using the BoringCrypto module.
B. Set Disk Encryption on the Instance Template used by the MIG to customer-managed key and use BoringSSL for all data transit between instances.
C. Change the app instance-to-instance communications from UDP to TCP and enable BoringSSL on clients' TLS connections.
D. Set Disk Encryption on the Instance Template used by the MIG to Google-managed Key and use BoringSSL library on all instance-to-instance communications.

Correct Answer: A
Section:
Explanation:
https://cloud.google.com/security/compliance/fips-140-2-validated
Google Cloud Platform uses a FIPS 140-2 validated encryption module called BoringCrypto (certificate 3318) in our production environment. This means that both data in transit to the customer and between data centers, and data at rest are encrypted using FIPS 140-2 validated encryption. The module that achieved FIPS 140-2 validation is part of our BoringSSL library.

QUESTION 35
A customer has an analytics workload running on Compute Engine that should have limited internet access.
Your team created an egress firewall rule to deny (priority 1000) all traffic to the internet.
The Compute Engine instances now need to reach out to the public repository to get security updates. What should your team do?

A. Create an egress firewall rule to allow traffic to the CIDR range of the repository with a priority greater than 1000.
B. Create an egress firewall rule to allow traffic to the CIDR range of the repository with a priority less than 1000.
C. Create an egress firewall rule to allow traffic to the hostname of the repository with a priority greater than 1000.
D. Create an egress firewall rule to allow traffic to the hostname of the repository with a priority less than 1000.

Correct Answer: B
Section:
Explanation:
https://cloud.google.com/vpc/docs/firewalls#priority_order_for_firewall_rules

QUESTION 36

You want data on Compute Engine disks to be encrypted at rest with keys managed by Cloud Key Management Service (KMS). Cloud Identity and Access Management (IAM) permissions to these keys must be managed in a grouped way because the permissions should be the same for all keys.
What should you do?

A. Create a single KeyRing for all persistent disks and all Keys in this KeyRing. Manage the IAM permissions at the Key level.
B. Create a single KeyRing for all persistent disks and all Keys in this KeyRing. Manage the IAM permissions at the KeyRing level.
C. Create a KeyRing per persistent disk, with each KeyRing containing a single Key. Manage the IAM permissions at the Key level.
D. Create a KeyRing per persistent disk, with each KeyRing containing a single Key. Manage the IAM permissions at the KeyRing level.

Correct Answer: B
Section:
Explanation:
https://cloud.netapp.com/blog/gcp-cvo-blg-how-to-use-google-cloud-encryption-with-a-persistent-disk

QUESTION 37
A company is backing up application logs to a Cloud Storage bucket shared with both analysts and the administrator. Analysts should only have access to logs that do not contain any personally identifiable information (PII). Log files containing PII should be stored in another bucket that is only accessible by the administrator.
What should you do?

A. Use Cloud Pub/Sub and Cloud Functions to trigger a Data Loss Prevention scan every time a file is uploaded to the shared bucket. If the scan detects PII, have the function move into a Cloud Storage bucket only accessible by the administrator.
B. Upload the logs to both the shared bucket and the bucket only accessible by the administrator. Create a job trigger using the Cloud Data Loss Prevention API. Configure the trigger to delete any files from the shared bucket that contain PII.
C. On the bucket shared with both the analysts and the administrator, configure Object Lifecycle Management to delete objects that contain any PII.
D. On the bucket shared with both the analysts and the administrator, configure a Cloud Storage Trigger that is only triggered when PII data is uploaded. Use Cloud Functions to capture the trigger and delete such files.

Correct Answer: A
Section:
Explanation:
https://codelabs.developers.google.com/codelabs/cloud-storage-dlp-functions#0 https://www.youtube.com/watch?v=0TmO1f-Ox40

QUESTION 38
A customer terminates an engineer and needs to make sure the engineer's Google account is automatically deprovisioned.
What should the customer do?

A. Use the Cloud SDK with their directory service to remove their IAM permissions in Cloud Identity.
B. Use the Cloud SDK with their directory service to provision and deprovision users from Cloud Identity.
C. Configure Cloud Directory Sync with their directory service to provision and deprovision users from Cloud Identity.
D. Configure Cloud Directory Sync with their directory service to remove their IAM permissions in Cloud Identity.

Correct Answer: C
Section:
Explanation:
https://cloud.google.com/identity/solutions/automate-user-provisioning#cloud_identity_automated_provisioning
'Cloud Identity has a catalog of automated provisioning connectors, which act as a bridge between Cloud Identity and third-party cloud apps.'

QUESTION 39
An organization is evaluating the use of Google Cloud Platform (GCP) for certain IT workloads. A well- established directory service is used to manage user identities and lifecycle management. This directory service must

continue for the organization to use as the ''source of truth'' directory for identities.
Which solution meets the organization's requirements?

A. Google Cloud Directory Sync (GCDS)
B. Cloud Identity
C. Security Assertion Markup Language (SAML)
D. Pub/Sub

Correct Answer: A
Section:
Explanation:
With Google Cloud Directory Sync (GCDS), you can synchronize the data in your Google Account with your Microsoft Active Directory or LDAP server. GCDS doesn't migrate any content (such as email messages, calendar events, or files) to your Google Account. You use GCDS to synchronize your Google users, groups, and shared contacts to match the information in your LDAP server.
https://support.google.com/a/answer/106368?hl=en

QUESTION 40
Which international compliance standard provides guidelines for information security controls applicable to the provision and use of cloud services?

A. ISO 27001
B. ISO 27002
C. ISO 27017
D. ISO 27018

Correct Answer: C
Section:
Explanation:
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.
https://cloud.google.com/security/compliance/iso-27017

QUESTION 41
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?

A. Create an Instance Template, and allow the Service Account Read Only access for the Compute Engine Access Scope.
B. Create a custom role with the permission compute.instances.list and grant the Service Account this role.
C. Give the Service Account the role of Compute Viewer, and use the new Service Account for all instances.
D. Give the Service Account the role of Project Viewer, and use the new Service Account for all instances.

Correct Answer: B
Section:
Explanation:
https://cloud.google.com/compute/docs/access/iam

QUESTION 42
In a shared security responsibility model for IaaS, which two layers of the stack does the customer share responsibility for? (Choose two.)

A. Hardware

B. Network Security
C. Storage Encryption
D. Access Policies
E. Boot

Correct Answer: B, D
Section:
Explanation:
https://cloud.google.com/blog/products/containers-kubernetes/exploring-container-security-the-shared-responsibility-model-in-gke-container-security-shared-responsibility-model-gke

QUESTION 43
An organization is starting to move its infrastructure from its on-premises environment to Google Cloud Platform (GCP). The first step the organization wants to take is to migrate its ongoing data backup and disaster recovery solutions to GCP. The organization's on-premises production environment is going to be the next phase for migration to GCP. Stable networking connectivity between the on-premises environment and GCP is also being implemented.
Which GCP solution should the organization use?

A. BigQuery using a data pipeline job with continuous updates via Cloud VPN
B. Cloud Storage using a scheduled task and gsutil via Cloud Interconnect
C. Compute Engines Virtual Machines using Persistent Disk via Cloud Interconnect
D. Cloud Datastore using regularly scheduled batch upload jobs via Cloud VPN

Correct Answer: B
Section:
Explanation:
https://cloud.google.com/solutions/dr-scenarios-for-data#production_environment_is_on-premises
https://medium.com/@pvergadia/cold-disaster-recovery-on-google-cloud-for-applications-running-on-premises-114b31933d02

QUESTION 44
What are the steps to encrypt data using envelope encryption?

A. Generate a data encryption key (DEK) locally. Use a key encryption key (KEK) to wrap the DEK. Encrypt data with the KEK. Store the encrypted data and the wrapped KEK.
B. Generate a key encryption key (KEK) locally. Use the KEK to generate a data encryption key (DEK). Encrypt data with the DEK. Store the encrypted data and the wrapped DEK.
C. Generate a data encryption key (DEK) locally. Encrypt data with the DEK. Use a key encryption key (KEK) to wrap the DEK. Store the encrypted data and the wrapped DEK.
D. Generate a key encryption key (KEK) locally. Generate a data encryption key (DEK) locally. Encrypt data with the KEK. Store the encrypted data and the wrapped DEK.

Correct Answer: C
Section:
Explanation:
The process of encrypting data is to generate a DEK locally, encrypt data with the DEK, use a KEK to wrap the DEK, and then store the encrypted data and the wrapped DEK. The KEK never leaves Cloud KMS.
https://cloud.google.com/kms/docs/envelope-encryption#how_to_encrypt_data_using_envelope_encryption

QUESTION 45
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?

A. Cloud Identity-Aware Proxy
B. Cloud Armor

C. Cloud Endpoints
D. Cloud VPN

Correct Answer: A
Section:
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 46
Your company is storing sensitive data in Cloud Storage. You want a key generated on-premises to be used in the encryption process.
What should you do?

A. Use the Cloud Key Management Service to manage a data encryption key (DEK).
B. Use the Cloud Key Management Service to manage a key encryption key (KEK).
C. Use customer-supplied encryption keys to manage the data encryption key (DEK).
D. Use customer-supplied encryption keys to manage the key encryption key (KEK).

Correct Answer: C
Section:
Explanation:
This is a Customer-supplied encryption keys (CSEK). We generate our own encryption key and manage it on-premises. A KEK never leaves Cloud KMS.There is no KEK or KMS on-premises. Encryption at rest by default, with various key management options https://cloud.google.com/security/encryption-at-rest

QUESTION 47
Last week, a company deployed a new App Engine application that writes logs to BigQuery. No other workloads are running in the project. You need to validate that all data written to BigQuery was done using the App Engine Default Service Account.
What should you do?

A. 1. Use StackDriver Logging and filter on BigQuery Insert Jobs. 2. Click on the email address in line with the App Engine Default Service Account in the authentication field. 3. Click Hide Matching Entries. 4. Make sure the resulting list is empty.
B. 1. Use StackDriver Logging and filter on BigQuery Insert Jobs. 2. Click on the email address in line with the App Engine Default Service Account in the authentication field. 3. Click Show Matching Entries. 4. Make sure the resulting list is empty.
C. 1. In BigQuery, select the related dataset. 2. Make sure the App Engine Default Service Account is the only account that can write to the dataset.
D. 1. Go to the IAM section on the project. 2. Validate that the App Engine Default Service Account is the only account that has a role that can write to BigQuery.

Correct Answer: A
Section:

QUESTION 48
Your team wants to limit users with administrative privileges at the organization level.
Which two roles should your team restrict? (Choose two.)

A. Organization Administrator
B. Super Admin
C. GKE Cluster Admin
D. Compute Admin
E. Organization Role Viewer

Correct Answer: A, B
Section:

QUESTION 49
An organization's security and risk management teams are concerned about where their responsibility lies for certain production workloads they are running in Google Cloud Platform (GCP), and where Google's responsibility lies. They are mostly running workloads using Google Cloud's Platform-as-a-Service (PaaS) offerings, including App Engine primarily.
Which one of these areas in the technology stack would they need to focus on as their primary responsibility when using App Engine?

A. Configuring and monitoring VPC Flow Logs
B. Defending against XSS and SQLi attacks
C. Manage the latest updates and security patches for the Guest OS
D. Encrypting all stored data

Correct Answer: B
Section:
Explanation:
in PaaS the customer is responsible for web app security, deployment, usage, access policy, and content. https://cloud.google.com/architecture/framework/security/shared-responsibility-shared-fate

QUESTION 50
An engineering team is launching a web application that will be public on the internet. The web application is hosted in multiple GCP regions and will be directed to the respective backend based on the URL request.
Your team wants to avoid exposing the application directly on the internet and wants to deny traffic from a specific list of malicious IP addresses
Which solution should your team implement to meet these requirements?

A. Cloud Armor
B. Network Load Balancing
C. SSL Proxy Load Balancing
D. NAT Gateway

Correct Answer: A
Section:
Explanation:
https://cloud.google.com/armor/docs/security-policy-overview#edge-security

QUESTION 51
A customer is running an analytics workload on Google Cloud Platform (GCP) where Compute Engine instances are accessing data stored on Cloud Storage. Your team wants to make sure that this workload will not be able to access, or be accessed from, the internet.
Which two strategies should your team use to meet these requirements? (Choose two.)

A. Configure Private Google Access on the Compute Engine subnet
B. Avoid assigning public IP addresses to the Compute Engine cluster.
C. Make sure that the Compute Engine cluster is running on a separate subnet.
D. Turn off IP forwarding on the Compute Engine instances in the cluster.
E. Configure a Cloud NAT gateway.

Correct Answer: A, B
Section:

QUESTION 52

A customer wants to run a batch processing system on VMs and store the output files in a Cloud Storage bucket. The networking and security teams have decided that no VMs may reach the public internet.
How should this be accomplished?

A. Create a firewall rule to block internet traffic from the VM.
B. Provision a NAT Gateway to access the Cloud Storage API endpoint.
C. Enable Private Google Access on the VPC.
D. Mount a Cloud Storage bucket as a local filesystem on every VM.

Correct Answer: C
Section:
Explanation:
https://cloud.google.com/vpc/docs/private-google-access

QUESTION 53
As adoption of the Cloud Data Loss Prevention (DLP) API grows within the company, you need to optimize usage to reduce cost. DLP target data is stored in Cloud Storage and BigQuery. The location and region are identified as a suffix in the resource name.
Which cost reduction options should you recommend?

A. Set appropriate rowsLimit value on BigQuery data hosted outside the US and set appropriate bytesLimitPerFile value on multiregional Cloud Storage buckets.
B. Set appropriate rowsLimit value on BigQuery data hosted outside the US, and minimize transformation units on multiregional Cloud Storage buckets.
C. Use rowsLimit and bytesLimitPerFile to sample data and use CloudStorageRegexFileSet to limit scans.
D. Use FindingLimits and TimespanContfig to sample data and minimize transformation units.

Correct Answer: C
Section:
Explanation:
https://cloud.google.com/dlp/docs/inspecting-storage#sampling https://cloud.google.com/dlp/docs/best-practices-costs#limit_scans_of_files_in_to_only_relevant_files

QUESTION 54
Your team uses a service account to authenticate data transfers from a given Compute Engine virtual machine instance of to a specified Cloud Storage bucket. An engineer accidentally deletes the service account, which breaks application functionality. You want to recover the application as quickly as possible without compromising security.
What should you do?

A. Temporarily disable authentication on the Cloud Storage bucket.
B. Use the undelete command to recover the deleted service account.
C. Create a new service account with the same name as the deleted service account.
D. Update the permissions of another existing service account and supply those credentials to the applications.

Correct Answer: B
Section:
Explanation:
https://cloud.google.com/iam/docs/reference/rest/v1/projects.serviceAccounts/undelete

QUESTION 55
You are the Security Admin in your company. You want to synchronize all security groups that have an email address from your LDAP directory in Cloud IAM.
What should you do?

A. Configure Google Cloud Directory Sync to sync security groups using LDAP search rules that have ''user email address'' as the attribute to facilitate one-way sync.

B. Configure Google Cloud Directory Sync to sync security groups using LDAP search rules that have ''user email address'' as the attribute to facilitate bidirectional sync.
C. Use a management tool to sync the subset based on the email address attribute. Create a group in the Google domain. A group created in a Google domain will automatically have an explicit Google Cloud Identity and Access Management (IAM) role.
D. Use a management tool to sync the subset based on group object class attribute. Create a group in the Google domain. A group created in a Google domain will automatically have an explicit Google Cloud Identity and Access Management (IAM) role.

Correct Answer: A
Section:
Explanation:
search rules that have 'user email address' as the attribute to facilitate one-way sync. Reference Links: https://support.google.com/a/answer/6126589?hl=en

QUESTION 56
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?

A. Query Data Access logs.
B. Query Admin Activity logs.
C. Query Access Transparency logs.
D. Query Stackdriver Monitoring Workspace.

Correct Answer: B
Section:
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 57
You have an application where the frontend is deployed on a managed instance group in subnet A and the data layer is stored on a mysql Compute Engine virtual machine (VM) in subnet B on the same VPC. Subnet A and Subnet B hold several other Compute Engine VMs. You only want to allow thee application frontend to access the data in the application's mysql instance on port 3306.
What should you do?

A. Configure an ingress firewall rule that allows communication from the src IP range of subnet A to the tag 'data-tag' that is applied to the mysql Compute Engine VM on port 3306.
B. Configure an ingress firewall rule that allows communication from the frontend's unique service account to the unique service account of the mysql Compute Engine VM on port 3306.
C. Configure a network tag 'fe-tag' to be applied to all instances in subnet A and a network tag 'data-tag' to be applied to all instances in subnet B. Then configure an egress firewall rule that allows communication from Compute Engine VMs tagged with data-tag to destination Compute Engine VMs tagged fe-tag.
D. Configure a network tag 'fe-tag' to be applied to all instances in subnet A and a network tag 'data-tag' to be applied to all instances in subnet B. Then configure an ingress firewall rule that allows communication from Compute Engine VMs tagged with fe-tag to destination Compute Engine VMs tagged with data-tag.

Correct Answer: B
Section:
Explanation:
https://cloud.google.com/sql/docs/mysql/sql-proxy#using-a-service-account

QUESTION 58
Your company operates an application instance group that is currently deployed behind a Google Cloud load balancer in us-central-1 and is configured to use the Standard Tier network. The infrastructure team wants to expand to a second Google Cloud region, us-east-2. You need to set up a single external IP address to distribute new requests to the instance groups in both regions.
What should you do?

A. Change the load balancer backend configuration to use network endpoint groups instead of instance groups.
B. Change the load balancer frontend configuration to use the Premium Tier network, and add the new instance group.
C. Create a new load balancer in us-east-2 using the Standard Tier network, and assign a static external IP address.
D. Create a Cloud VPN connection between the two regions, and enable Google Private Access.

Correct Answer: B
Section:
Explanation:
https://cloud.google.com/load-balancing/docs/choosing-load-balancer#global-regional

QUESTION 59
You are the security admin of your company. You have 3,000 objects in your Cloud Storage bucket. You do not want to manage access to each object individually. You also do not want the uploader of an object to always have full control of the object. However, you want to use Cloud Audit Logs to manage access to your bucket.
What should you do?

A. Set up an ACL with OWNER permission to a scope of allUsers.
B. Set up an ACL with READER permission to a scope of allUsers.
C. Set up a default bucket ACL and manage access for users using IAM.
D. Set up Uniform bucket-level access on the Cloud Storage bucket and manage access for users using IAM.

Correct Answer: D
Section:
Explanation:
https://cloud.google.com/storage/docs/uniform-bucket-level-access#enabled

QUESTION 60
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?

A. Use a Shared VPC to enable communication between all projects, and use firewall rules to prevent data exfiltration.
B. Create access levels in Access Context Manager to prevent data exfiltration, and use a shared VPC for communication between projects.
C. 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.
D. 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.

Correct Answer: C
Section:
Explanation:
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 61
You need to provide a corporate user account in Google Cloud for each of your developers and operational staff who need direct access to GCP resources. Corporate policy requires you to maintain the user identity in a third-party identity management provider and leverage single sign-on. You learn that a significant number of users are using their corporate domain email addresses for personal Google accounts, and you need to follow Google recommended practices to convert existing unmanaged users to managed accounts.
Which two actions should you take? (Choose two.)

A. Use Google Cloud Directory Sync to synchronize your local identity management system to Cloud Identity.
B. Use the Google Admin console to view which managed users are using a personal account for their recovery email.
C. Add users to your managed Google account and force users to change the email addresses associated with their personal accounts.
D. Use the Transfer Tool for Unmanaged Users (TTUU) to find users with conflicting accounts and ask them to transfer their personal Google accounts.
E. Send an email to all of your employees and ask those users with corporate email addresses for personal Google accounts to delete the personal accounts immediately.

Correct Answer: A, D
Section:
Explanation:
https://cloud.google.com/architecture/identity/migrating-consumer-accounts#initiating_a_transfer

QUESTION 62
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 Cloud IAP based on IP address or end-user device attributes to prevent and fix the vulnerability.
B. Set up an HTTPS load balancer, and then use Cloud Armor for the production environment to prevent the potential XSS attack.
C. 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.
D. Use Web Security Scanner in staging to simulate an XSS injection attack, and then use a templating system that supports contextual auto-escaping.

Correct Answer: D
Section:
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

QUESTION 63
You are part of a security team that wants to ensure that a Cloud Storage bucket in Project A can only be readable from Project B. You also want to ensure that data in the Cloud Storage bucket cannot be accessed from or copied to Cloud Storage buckets outside the network, even if the user has the correct credentials.
What should you do?

A. Enable VPC Service Controls, create a perimeter with Project A and B, and include Cloud Storage service.
B. Enable Domain Restricted Sharing Organization Policy and Bucket Policy Only on the Cloud Storage bucket.
C. Enable Private Access in Project A and B networks with strict firewall rules to allow communication between the networks.
D. Enable VPC Peering between Project A and B networks with strict firewall rules to allow communication between the networks.

Correct Answer: A
Section:
Explanation:
https://cloud.google.com/vpc-service-controls/docs/overview#isolate

QUESTION 64
You are responsible for protecting highly sensitive data in BigQuery. Your operations teams need access to this data, but given privacy regulations, you want to ensure that they cannot read the sensitive fields such as email addresses and first names. These specific sensitive fields should only be available on a need-to-know basis to the HR team. What should you do?

A. Perform data masking with the DLP API and store that data in BigQuery for later use.
B. Perform data redaction with the DLP API and store that data in BigQuery for later use.
C. Perform data inspection with the DLP API and store that data in BigQuery for later use.
D. Perform tokenization for Pseudonymization with the DLP API and store that data in BigQuery for later use.

Correct Answer: D
Section:
Explanation:
Pseudonymization is a de-identification technique that replaces sensitive data values with cryptographically generated tokens. Pseudonymization is widely used in industries like finance and healthcare to help reduce the risk of data in use, narrow compliance scope, and minimize the exposure of sensitive data to systems while preserving data utility and accuracy.
https://cloud.google.com/dlp/docs/pseudonymization

QUESTION 65
You are a Security Administrator at your organization. You need to restrict service account creation capability within production environments. You want to accomplish this centrally across the organization. What should you do?

A. Use Identity and Access Management (IAM) to restrict access of all users and service accounts that have access to the production environment.
B. Use organization policy constraints/iam.disableServiceAccountKeyCreation boolean to disable the creation of new service accounts.
C. Use organization policy constraints/iam.disableServiceAccountKeyUpload boolean to disable the creation of new service accounts.
D. Use organization policy constraints/iam.disableServiceAccountCreation boolean to disable the creation of new service accounts.

Correct Answer: D
Section:
Explanation:
You can use the iam.disableServiceAccountCreation boolean constraint to disable the creation of new service accounts. This allows you to centralize management of service accounts while not restricting the other permissions your developers have on projects. https://cloud.google.com/resource-manager/docs/organization-policy/restricting-service-accounts#disable_service_account_creation

QUESTION 66
You are the project owner for a regulated workload that runs in a project you own and manage as an Identity and Access Management (IAM) admin. For an upcoming audit, you need to provide access reviews evidence. Which tool should you use?

A. Policy Troubleshooter
B. Policy Analyzer
C. IAM Recommender
D. Policy Simulator

Correct Answer: B
Section:
Explanation:
https://cloud.google.com/policy-intelligence/docs/policy-analyzer-overview
Policy Analyzer lets you find out which principals (for example, users, service accounts, groups, and domains) have what access to which Google Cloud resources based on your IAM allow policies.

QUESTION 67
Your organization has implemented synchronization and SAML federation between Cloud Identity and Microsoft Active Directory. You want to reduce the risk of Google Cloud user accounts being compromised. What should you do?

A. Create a Cloud Identity password policy with strong password settings, and configure 2-Step Verification with security keys in the Google Admin console.
B. Create a Cloud Identity password policy with strong password settings, and configure 2-Step Verification with verification codes via text or phone call in the Google Admin console.

C. Create an Active Directory domain password policy with strong password settings, and configure post-SSO (single sign-on) 2-Step Verification with security keys in the Google Admin console.
D. Create an Active Directory domain password policy with strong password settings, and configure post-SSO (single sign-on) 2-Step Verification with verification codes via text or phone call in the Google Admin console.

Correct Answer: C
Section:
Explanation:
'We recommend against using text messages. The National Institute of Standards and Technology (NIST) no longer recommends SMS-based 2SV due to the hijacking risk from state-sponsored entities.'

QUESTION 68
You have been tasked with implementing external web application protection against common web application attacks for a public application on Google Cloud. You want to validate these policy changes before they are enforced. What service should you use?

A. Google Cloud Armor's preconfigured rules in preview mode
B. Prepopulated VPC firewall rules in monitor mode
C. The inherent protections of Google Front End (GFE)
D. Cloud Load Balancing firewall rules
E. VPC Service Controls in dry run mode

Correct Answer: A
Section:
Explanation:
You can preview the effects of a rule without enforcing it. In preview mode, actions are noted in Cloud Monitoring. You can choose to preview individual rules in a security policy, or you can preview every rule in the policy.
https://cloud.google.com/armor/docs/security-policy-overview#preview_mode

QUESTION 69
You are asked to recommend a solution to store and retrieve sensitive configuration data from an application that runs on Compute Engine. Which option should you recommend?

A. Cloud Key Management Service
B. Compute Engine guest attributes
C. Compute Engine custom metadata
D. Secret Manager

Correct Answer: D
Section:
Explanation:
Secret Manager is a secure and convenient storage system for API keys, passwords, certificates, and other sensitive data. Secret Manager provides a central place and single source of truth to manage, access, and audit secrets across Google Cloud. https://cloud.google.com/secret-manager

QUESTION 70
You need to implement an encryption at-rest strategy that reduces key management complexity for non-sensitive data and protects sensitive data while providing the flexibility of controlling the key residency and rotation schedule. FIPS 140-2 L1 compliance is required for all data types. What should you do?

A. Encrypt non-sensitive data and sensitive data with Cloud External Key Manager.
B. Encrypt non-sensitive data and sensitive data with Cloud Key Management Service
C. Encrypt non-sensitive data with Google default encryption, and encrypt sensitive data with Cloud External Key Manager.
D. Encrypt non-sensitive data with Google default encryption, and encrypt sensitive data with Cloud Key Management Service.

Correct Answer: D
Section:
Explanation:
Google uses a common cryptographic library, Tink, which incorporates our FIPS 140-2 Level 1 validated module, BoringCrypto, to implement encryption consistently across almost all Google Cloud products. To provideflexibility of controlling the key residency and rotation schedule, use google provided key for non-sensitive and encrypt sensitive data with Cloud Key Management Service

QUESTION 71
Your company wants to determine what products they can build to help customers improve their credit scores depending on their age range. To achieve this, you need to join user information in the company's banking app with customers' credit score data received from a third party. While using this raw data will allow you to complete this task, it exposes sensitive data, which could be propagated into new systems.
This risk needs to be addressed using de-identification and tokenization with Cloud Data Loss Prevention while maintaining the referential integrity across the database. Which cryptographic token format should you use to meet these requirements?

A. Deterministic encryption
B. Secure, key-based hashes
C. Format-preserving encryption
D. Cryptographic hashing

Correct Answer: A
Section:
Explanation:
''This encryption method is reversible, which helps to maintain referential integrity across your database and has no character-set limitations.'' https://cloud.google.com/blog/products/identity-security/take-charge-of-your-data-how-tokenization-makes-data-usable-without-sacrificing-privacy
https://cloud.google.com/dlp/docs/pseudonymization
FPE provides fewer security guarantees compared to other deterministic encryption methods such as AES-SIV. For these reasons, Google strongly recommends using deterministic encryption with AES-SIV instead of FPE for all security sensitive use cases. Other methods like deterministic encryption using AES-SIV provide these stronger security guarantees and are recommended for tokenization use cases unless length and character set preservation are strict requirements---for example, for backward compatibility with a legacy data system.

QUESTION 72
An office manager at your small startup company is responsible for matching payments to invoices and creating billing alerts. For compliance reasons, the office manager is only permitted to have the Identity and Access Management (IAM) permissions necessary for these tasks. Which two IAM roles should the office manager have? (Choose two.)

A. Organization Administrator
B. Project Creator
C. Billing Account Viewer
D. Billing Account Costs Manager
E. Billing Account User

Correct Answer: C, D
Section:
Explanation:
https://cloud.google.com/billing/docs/how-to/billing-access#overview-of-cloud-billing-roles-in-cloud-iam
Billing Account Costs Manager (roles/billing.costsManager)
- Manage budgets and view and export cost information of billing accounts (but not pricing information)
Billing Account Viewer (roles/billing.viewer)
- View billing account cost information and transactions.

QUESTION 73
You are designing a new governance model for your organization's secrets that are stored in Secret Manager. Currently, secrets for Production and Non-Production applications are stored and accessed using service accounts.

Your proposed solution must:
Provide granular access to secrets
Give you control over the rotation schedules for the encryption keys that wrap your secrets
Maintain environment separation
Provide ease of management
Which approach should you take?

A. 1. Use separate Google Cloud projects to store Production and Non-Production secrets. 2. Enforce access control to secrets using project-level identity and Access Management (IAM) bindings. 3. Use customer-managed encryption keys to encrypt secrets.
B. 1. Use a single Google Cloud project to store both Production and Non-Production secrets. 2. Enforce access control to secrets using secret-level Identity and Access Management (IAM) bindings. 3. Use Google-managed encryption keys to encrypt secrets.
C. 1. Use separate Google Cloud projects to store Production and Non-Production secrets. 2. Enforce access control to secrets using secret-level Identity and Access Management (IAM) bindings. 3. Use Google-managed encryption keys to encrypt secrets.
D. 1. Use a single Google Cloud project to store both Production and Non-Production secrets. 2. Enforce access control to secrets using project-level Identity and Access Management (IAM) bindings. 3. Use customer-managed encryption keys to encrypt secrets.

Correct Answer: A
Section:
Explanation:
Provide granular access to secrets: 2.Enforce access control to secrets using project-level identity and Access Management (IAM) bindings. Give you control over the rotation schedules for the encryption keys that wrap your secrets: 3. Use customer-managed encryption keys to encrypt secrets. Maintain environment separation: 1. Use separate Google Cloud projects to store Production and Non-Production secrets.

QUESTION 74
You are a security engineer at a finance company. Your organization plans to store data on Google Cloud, but your leadership team is worried about the security of their highly sensitive data Specifically, your company is concerned about internal Google employees' ability to access your company's data on Google Cloud. What solution should you propose?

A. Use customer-managed encryption keys.
B. Use Google's Identity and Access Management (IAM) service to manage access controls on Google Cloud.
C. Enable Admin activity logs to monitor access to resources.
D. Enable Access Transparency logs with Access Approval requests for Google employees.

Correct Answer: D
Section:
Explanation:
https://cloud.google.com/access-transparency Access approval Explicitly approve access to your data or configurations on Google Cloud. Access Approval requests, when combined with Access Transparency logs, can be used to audit an end-to-end chain from support ticket to access request to approval, to eventual access.

QUESTION 75
Your company's new CEO recently sold two of the company's divisions. Your Director asks you to help migrate the Google Cloud projects associated with those divisions to a new organization node. Which preparation steps are necessary before this migration occurs? (Choose two.)

A. Remove all project-level custom Identity and Access Management (IAM) roles.
B. Disallow inheritance of organization policies.
C. Identify inherited Identity and Access Management (IAM) roles on projects to be migrated.
D. Create a new folder for all projects to be migrated.
E. Remove the specific migration projects from any VPC Service Controls perimeters and bridges.

Correct Answer: C

Section:
Explanation:
https://cloud.google.com/resource-manager/docs/project-migration#plan_policy
When you migrate your project, it will no longer inherit the policies from its current place in the resource hierarchy, and will be subject to the effective policy evaluation at its destination. We recommend making sure that the effective policies at the project's destination match as much as possible the policies that the project had in its source location. https://cloud.google.com/resource-manager/docs/project-migration#import_export_folders
Policy inheritance can cause unintended effects when you are migrating a project, both in the source and destination organization resources. You can mitigate this risk by creating specific folders to hold only projects for export and import, and ensuring that the same policies are inherited by the folders in both organization resources. You can also set permissions on these folders that will be inherited to the projects moved within them, helping to accelerate the project migration process.

QUESTION 76
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?

A. Organization Policy Service constraints
B. Shielded VM instances
C. Access control lists
D. Geolocation access controls
E. Google Cloud Armor

Correct Answer: A
Section:
Explanation:
https://cloud.google.com/resource-manager/docs/organization-policy/using-constraints#list-constraint

QUESTION 77
Your security team wants to reduce the risk of user-managed keys being mismanaged and compromised. To achieve this, you need to prevent developers from creating user-managed service account keys for projects in their organization. How should you enforce this?

A. Configure Secret Manager to manage service account keys.
B. Enable an organization policy to disable service accounts from being created.
C. Enable an organization policy to prevent service account keys from being created.
D. Remove the iam.serviceAccounts.getAccessToken permission from users.

Correct Answer: C
Section:
Explanation:
https://cloud.google.com/iam/docs/best-practices-for-managing-service-account-keys
'To prevent unnecessary usage of service account keys, use organization policy constraints: At the root of your organization's resource hierarchy, apply the Disable service account key creation and Disable service account key upload constraints to establish a default where service account keys are disallowed. When needed, override one of the constraints for selected projects to re-enable service account key creation or upload.'

QUESTION 78
You are responsible for managing your company's identities in Google Cloud. Your company enforces 2-Step Verification (2SV) for all users. You need to reset a user's access, but the user lost their second factor for 2SV. You want to minimize risk. What should you do?

A. On the Google Admin console, select the appropriate user account, and generate a backup code to allow the user to sign in. Ask the user to update their second factor.
B. On the Google Admin console, temporarily disable the 2SV requirements for all users. Ask the user to log in and add their new second factor to their account. Re-enable the 2SV requirement for all users.
C. On the Google Admin console, select the appropriate user account, and temporarily disable 2SV for this account Ask the user to update their second factor, and then re-enable 2SV for this account.

D. On the Google Admin console, use a super administrator account to reset the user account's credentials. Ask the user to update their credentials after their first login.

Correct Answer: A
Section:
Explanation:
https://support.google.com/a/answer/9176734
Use backup codes for account recovery If you need to recover an account, use backup codes. Accounts are still protected by 2-Step Verification, and backup codes are easy to generate.

QUESTION 79
Which Google Cloud service should you use to enforce access control policies for applications and resources?

A. Identity-Aware Proxy
B. Cloud NAT
C. Google Cloud Armor
D. Shielded VMs

Correct Answer: A
Section:
Explanation:
https://cloud.google.com/iap/docs/concepts-overview 'Use IAP when you want to enforce access control policies for applications and resources.'

QUESTION 80
You want to update your existing VPC Service Controls perimeter with a new access level. You need to avoid breaking the existing perimeter with this change, and ensure the least disruptions to users while minimizing overhead. What should you do?

A. Create an exact replica of your existing perimeter. Add your new access level to the replica. Update the original perimeter after the access level has been vetted.
B. Update your perimeter with a new access level that never matches. Update the new access level to match your desired state one condition at a time to avoid being overly permissive.
C. Enable the dry run mode on your perimeter. Add your new access level to the perimeter configuration. Update the perimeter configuration after the access level has been vetted.
D. Enable the dry run mode on your perimeter. Add your new access level to the perimeter dry run configuration. Update the perimeter configuration after the access level has been vetted.

Correct Answer: D
Section:
Explanation:
https://cloud.google.com/vpc-service-controls/docs/dry-run-mode
When using VPC Service Controls, it can be difficult to determine the impact to your environment when a service perimeter is created or modified. With dry run mode, you can better understand the impact of enabling VPC Service Controls and changes to perimeters in existing environments.

QUESTION 81
Your organization's Google Cloud VMs are deployed via an instance template that configures them with a public IP address in order to host web services for external users. The VMs reside in a service project that is attached to a host (VPC) project containing one custom Shared VPC for the VMs. You have been asked to reduce the exposure of the VMs to the internet while continuing to service external users. You have already recreated the instance template without a public IP address configuration to launch the managed instance group (MIG). What should you do?

A. Deploy a Cloud NAT Gateway in the service project for the MIG.
B. Deploy a Cloud NAT Gateway in the host (VPC) project for the MIG.
C. Deploy an external HTTP(S) load balancer in the service project with the MIG as a backend.
D. Deploy an external HTTP(S) load balancer in the host (VPC) project with the MIG as a backend.

Correct Answer: D

Section:
Explanation:
https://cloud.google.com/load-balancing/docs/https#shared-vpc
While you can create all the load balancing components and backends in the Shared VPC host project, this model does not separate network administration and service development responsibilities.

QUESTION 82
Your privacy team uses crypto-shredding (deleting encryption keys) as a strategy to delete personally identifiable information (PII). You need to implement this practice on Google Cloud while still utilizing the majority of the platform's services and minimizing operational overhead. What should you do?

A. Use client-side encryption before sending data to Google Cloud, and delete encryption keys on-premises
B. Use Cloud External Key Manager to delete specific encryption keys.
C. Use customer-managed encryption keys to delete specific encryption keys.
D. Use Google default encryption to delete specific encryption keys.

Correct Answer: C
Section:
Explanation:
https://cloud.google.com/sql/docs/mysql/cmek
'You might have situations where you want to permanently destroy data encrypted with CMEK. To do this, you destroy the customer-managed encryption key version. You can't destroy the keyring or key, but you can destroy key versions of the key.'

QUESTION 83
You need to centralize your team's logs for production projects. You want your team to be able to search and analyze the logs using Logs Explorer. What should you do?

A. Enable Cloud Monitoring workspace, and add the production projects to be monitored.
B. Use Logs Explorer at the organization level and filter for production project logs.
C. Create an aggregate org sink at the parent folder of the production projects, and set the destination to a Cloud Storage bucket.
D. Create an aggregate org sink at the parent folder of the production projects, and set the destination to a logs bucket.

Correct Answer: D
Section:
Explanation:
https://cloud.google.com/logging/docs/export/aggregated_sinks#supported-destinations
You can use aggregated sinks to route logs within or between the same organizations and folders to the following destinations: - Another Cloud Logging bucket: Log entries held in Cloud Logging log buckets.

QUESTION 84
You need to use Cloud External Key Manager to create an encryption key to encrypt specific BigQuery data at rest in Google Cloud. Which steps should you do first?

A. 1. Create or use an existing key with a unique uniform resource identifier (URI) in your Google Cloud project. 2. Grant your Google Cloud project access to a supported external key management partner system.
B. 1. Create or use an existing key with a unique uniform resource identifier (URI) in Cloud Key Management Service (Cloud KMS). 2. In Cloud KMS, grant your Google Cloud project access to use the key.
C. 1. Create or use an existing key with a unique uniform resource identifier (URI) in a supported external key management partner system. 2. In the external key management partner system, grant access for this key to use your Google Cloud project.
D. 1. Create an external key with a unique uniform resource identifier (URI) in Cloud Key Management Service (Cloud KMS). 2. In Cloud KMS, grant your Google Cloud project access to use the key.

Correct Answer: C
Section:
Explanation:
https://cloud.google.com/kms/docs/ekm#how_it_works

- First, you create or use an existing key in a supported external key management partner system. This key has a unique URI or key path.
- Next, you grant your Google Cloud project access to use the key, in the external key management partner system.
- In your Google Cloud project, you create a Cloud EKM key, using the URI or key path for the externally-managed key.

QUESTION 85
Your company's cloud security policy dictates that VM instances should not have an external IP address. You need to identify the Google Cloud service that will allow VM instances without external IP addresses to connect to the internet to update the VMs. Which service should you use?

A. Identity Aware-Proxy
B. Cloud NAT
C. TCP/UDP Load Balancing
D. Cloud DNS

Correct Answer: B
Section:
Explanation:
https://cloud.google.com/nat/docs/overview 'Cloud NAT (network address translation) lets certain resources without external IP addresses create outbound connections to the internet.'

QUESTION 86
You want to make sure that your organization's Cloud Storage buckets cannot have data publicly available to the internet. You want to enforce this across all Cloud Storage buckets. What should you do?

A. Remove Owner roles from end users, and configure Cloud Data Loss Prevention.
B. Remove Owner roles from end users, and enforce domain restricted sharing in an organization policy.
C. Configure uniform bucket-level access, and enforce domain restricted sharing in an organization policy.
D. Remove *.setIamPolicy permissions from all roles, and enforce domain restricted sharing in an organization policy.

Correct Answer: C
Section:
Explanation:
- Uniform bucket-level access: https://cloud.google.com/storage/docs/uniform-bucket-level-access#should-you-use
- Domain Restricted Sharing: https://cloud.google.com/resource-manager/docs/organization-policy/restricting-domains#public_data_sharing

QUESTION 87
Your company plans to move most of its IT infrastructure to Google Cloud. They want to leverage their existing on-premises Active Directory as an identity provider for Google Cloud. Which two steps should you take to integrate the company's on-premises Active Directory with Google Cloud and configure access management? (Choose two.)

A. Use Identity Platform to provision users and groups to Google Cloud.
B. Use Cloud Identity SAML integration to provision users and groups to Google Cloud.
C. Install Google Cloud Directory Sync and connect it to Active Directory and Cloud Identity.
D. Create Identity and Access Management (IAM) roles with permissions corresponding to each Active Directory group.
E. Create Identity and Access Management (IAM) groups with permissions corresponding to each Active Directory group.

Correct Answer: C, E
Section:
Explanation:
https://cloud.google.com/architecture/identity/federating-gcp-with-active-directory-synchronizing-user-accounts?hl=en
https://cloud.google.com/architecture/identity/federating-gcp-with-active-directory-synchronizing-user-accounts?hl=en#deciding_where_to_deploy_gcds

QUESTION 88
You are in charge of creating a new Google Cloud organization for your company. Which two actions should you take when creating the super administrator accounts? (Choose two.)

A. Create an access level in the Google Admin console to prevent super admin from logging in to Google Cloud.
B. Disable any Identity and Access Management (IAM) roles for super admin at the organization level in the Google Cloud Console.
C. Use a physical token to secure the super admin credentials with multi-factor authentication (MFA).
D. Use a private connection to create the super admin accounts to avoid sending your credentials over the Internet.
E. Provide non-privileged identities to the super admin users for their day-to-day activities.

Correct Answer: C, E
Section:
Explanation:
https://cloud.google.com/resource-manager/docs/super-admin-best-practices#discourage_super_admin_account_usage
- Use a security key or other physical authentication device to enforce two-step verification - Give super admins a separate account that requires a separate login

QUESTION 89
You are deploying a web application hosted on Compute Engine. A business requirement mandates that application logs are preserved for 12years and data is kept within European boundaries. You want to implement a storage solution that minimizes overhead and is cost-effective. What should you do?

A. Create a Cloud Storage bucket to store your logs in the EUROPE-WEST1 region. Modify your application code to ship logs directly to your bucket for increased efficiency.
B. Configure your Compute Engine instances to use the Google Cloud's operations suite Cloud Logging agent to send application logs to a custom log bucket in the EUROPE-WEST1 region with a custom retention of 12 years.
C. Use a Pub/Sub topic to forward your application logs to a Cloud Storage bucket in the EUROPE-WEST1 region.
D. Configure a custom retention policy of 12 years on your Google Cloud's operations suite log bucket in the EUROPE-WEST1 region.

Correct Answer: B
Section:
Explanation:
https://youtu.be/MI4iG2GIZMA

QUESTION 90
You discovered that sensitive personally identifiable information (PII) is being ingested to your Google Cloud environment in the daily ETL process from an on-premises environment to your BigQuery datasets. You need to redact this data to obfuscate the PII, but need to re-identify it for data analytics purposes. Which components should you use in your solution? (Choose two.)

A. Secret Manager
B. Cloud Key Management Service
C. Cloud Data Loss Prevention with cryptographic hashing
D. Cloud Data Loss Prevention with automatic text redaction
E. Cloud Data Loss Prevention with deterministic encryption using AES-SIV

Correct Answer: B, E
Section:
Explanation:
B: you need KMS to store the CryptoKey https://cloud.google.com/dlp/docs/reference/rest/v2/projects.deidentifyTemplates#crypt
E: for the de-identity you need to use CryptoReplaceFfxFpeConfig or CryptoDeterministicConfig https://cloud.google.com/dlp/docs/reference/rest/v2/projects.deidentifyTemplates#cryptodeterministicconfig
https://cloud.google.com/dlp/docs/deidentify-sensitive-data

QUESTION 91

You are working with a client that is concerned about control of their encryption keys for sensitive data. The client does not want to store encryption keys at rest in the same cloud service provider (CSP) as the data that the keys are encrypting. Which Google Cloud encryption solutions should you recommend to this client? (Choose two.)

A. Customer-supplied encryption keys.
B. Google default encryption
C. Secret Manager
D. Cloud External Key Manager
E. Customer-managed encryption keys

Correct Answer: A, D
Section:

QUESTION 92
You are implementing data protection by design and in accordance with GDPR requirements. As part of design reviews, you are told that you need to manage the encryption key for a solution that includes workloads for Compute Engine, Google Kubernetes Engine, Cloud Storage, BigQuery, and Pub/Sub. Which option should you choose for this implementation?

A. Cloud External Key Manager
B. Customer-managed encryption keys
C. Customer-supplied encryption keys
D. Google default encryption

Correct Answer: B
Section:
Explanation:
https://cloud.google.com/kms/docs/using-other-products#cmek_integrations https://cloud.google.com/kms/docs/using-other-products#cmek_integrations CMEK is supported for all the listed google services.

QUESTION 93
Which Identity-Aware Proxy role should you grant to an Identity and Access Management (IAM) user to access HTTPS resources?

A. Security Reviewer
B. lAP-Secured Tunnel User
C. lAP-Secured Web App User
D. Service Broker Operator

Correct Answer: C
Section:
Explanation:
IAP-Secured Tunnel User: Grants access to tunnel resources that use IAP. IAP-Secured Web App User: Access HTTPS resources which use Identity-Aware Proxy, Grants access to App Engine, Cloud Run, and Compute Engine resources.
https://cloud.google.com/iap/docs/managing-access#roles

QUESTION 94
You need to audit the network segmentation for your Google Cloud footprint. You currently operate Production and Non-Production infrastructure-as-a-service (IaaS) environments. All your VM instances are deployed without any service account customization.
After observing the traffic in your custom network, you notice that all instances can communicate freely -- despite tag-based VPC firewall rules in place to segment traffic properly -- with a priority of 1000. What are the most likely reasons for this behavior?

A. All VM instances are missing the respective network tags.
B. All VM instances are residing in the same network subnet.
C. All VM instances are configured with the same network route.
D. A VPC firewall rule is allowing traffic between source/targets based on the same service account with priority 999.
E. A VPC firewall rule is allowing traffic between source/targets based on the same service account with priority 1001.

Correct Answer: A, D
Section:

QUESTION 95
You are creating a new infrastructure CI/CD pipeline to deploy hundreds of ephemeral projects in your Google Cloud organization to enable your users to interact with Google Cloud. You want to restrict the use of the default networks in your organization while following Google-recommended best practices. What should you do?

A. Enable the constraints/compute.skipDefaultNetworkCreation organization policy constraint at the organization level.
B. Create a cron job to trigger a daily Cloud Function to automatically delete all default networks for each project.
C. Grant your users the IAM Owner role at the organization level. Create a VPC Service Controls perimeter around the project that restricts the compute.googleapis.com API.
D. Only allow your users to use your CI/CD pipeline with a predefined set of infrastructure templates they can deploy to skip the creation of the default networks.

Correct Answer: A
Section:
Explanation:
Enable the constraints/compute.skipDefaultNetworkCreation organization policy constraint at the organization level.
https://cloud.google.com/resource-manager/docs/organization-policy/org-policy-constraints - constraints/compute.skipDefaultNetworkCreation This boolean constraint skips the creation of the default network and related resources during Google Cloud Platform Project resource creation where this constraint is set to True. By default, a default network and supporting resources are automatically created when creating a Project resource.

QUESTION 96
You are a security administrator at your company and are responsible for managing access controls (identification, authentication, and authorization) on Google Cloud. Which Google-recommended best practices should you follow when configuring authentication and authorization? (Choose two.)

A. Use Google default encryption.
B. Manually add users to Google Cloud.
C. Provision users with basic roles using Google's Identity and Access Management (IAM) service.
D. Use SSO/SAML integration with Cloud Identity for user authentication and user lifecycle management.
E. Provide granular access with predefined roles.

Correct Answer: D, E
Section:
Explanation:
https://cloud.google.com/iam/docs/using-iam-securely#least_privilege Basic roles include thousands of permissions across all Google Cloud services. In production environments, do not grant basic roles unless there is no alternative. Instead, grant the most limited predefined roles or custom roles that meet your needs.

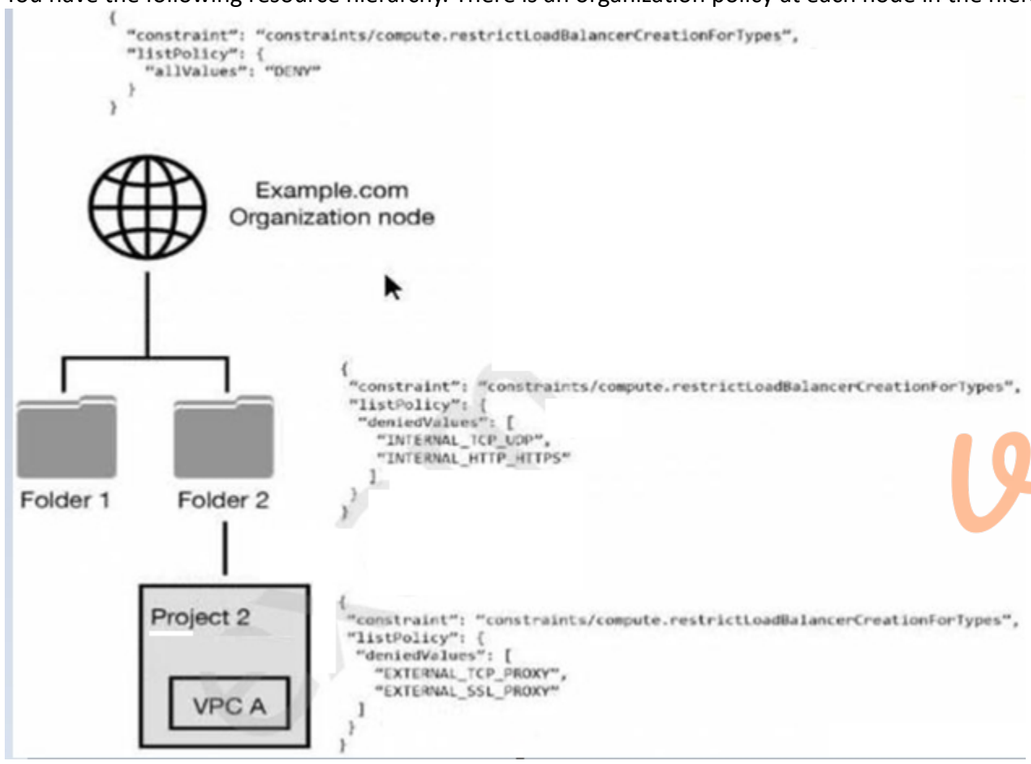
QUESTION 97
You have been tasked with inspecting IP packet data for invalid or malicious content. What should you do?

A. Use Packet Mirroring to mirror traffic to and from particular VM instances. Perform inspection using security software that analyzes the mirrored traffic.
B. Enable VPC Flow Logs for all subnets in the VPC. Perform inspection on the Flow Logs data using Cloud Logging.
C. Configure the Fluentd agent on each VM Instance within the VPC. Perform inspection on the log data using Cloud Logging.

D. Configure Google Cloud Armor access logs to perform inspection on the log data.

Correct Answer: A
Section:
Explanation:
https://cloud.google.com/vpc/docs/packet-mirroring
Packet Mirroring clones the traffic of specified instances in your Virtual Private Cloud (VPC) network and forwards it for examination. Packet Mirroring captures all traffic and packet data, including payloads and headers.

QUESTION 98
You have the following resource hierarchy. There is an organization policy at each node in the hierarchy as shown. Which load balancer types are denied in VPC A?



A. All load balancer types are denied in accordance with the global node's policy.
B. INTERNAL_TCP_UDP, INTERNAL_HTTP_HTTPS is denied in accordance with the folder's policy.
C. EXTERNAL_TCP_PROXY, EXTERNAL_SSL_PROXY are denied in accordance with the project's policy.
D. EXTERNAL_TCP_PROXY, EXTERNAL_SSL_PROXY, INTERNAL_TCP_UDP, and INTERNAL_HTTP_HTTPS are denied in accordance with the folder and project's policies.

Correct Answer: D
Section:

QUESTION 99
Your security team wants to implement a defense-in-depth approach to protect sensitive data stored in a Cloud Storage bucket. Your team has the following requirements:
The Cloud Storage bucket in Project A can only be readable from Project B.
The Cloud Storage bucket in Project A cannot be accessed from outside the network.
Data in the Cloud Storage bucket cannot be copied to an external Cloud Storage bucket.
What should the security team do?

A. Enable domain restricted sharing in an organization policy, and enable uniform bucket-level access on the Cloud Storage bucket.
B. Enable VPC Service Controls, create a perimeter around Projects A and B. and include the Cloud Storage API in the Service Perimeter configuration.
C. Enable Private Access in both Project A and B's networks with strict firewall rules that allow communication between the networks.
D. Enable VPC Peering between Project A and B's networks with strict firewall rules that allow communication between the networks.

Correct Answer: B
Section:
Explanation:
VPC Peering is between organizations not between Projects in an organization. That is Shared VPC. In this case, both projects are in same organization so having VPC Service Controls around both projects with necessary rules should be fine.
https://cloud.google.com/vpc-service-controls/docs/overview

QUESTION 100
You need to create a VPC that enables your security team to control network resources such as firewall rules. How should you configure the network to allow for separation of duties for network resources?

A. Set up multiple VPC networks, and set up multi-NIC virtual appliances to connect the networks.
B. Set up VPC Network Peering, and allow developers to peer their network with a Shared VPC.
C. Set up a VPC in a project. Assign the Compute Network Admin role to the security team, and assign the Compute Admin role to the developers.
D. Set up a Shared VPC where the security team manages the firewall rules, and share the network with developers via service projects.

Correct Answer: D
Section:

QUESTION 101
You are onboarding new users into Cloud Identity and discover that some users have created consumer user accounts using the corporate domain name. How should you manage these consumer user accounts with Cloud Identity?

A. Use Google Cloud Directory Sync to convert the unmanaged user accounts.
B. Create a new managed user account for each consumer user account.
C. Use the transfer tool for unmanaged user accounts.
D. Configure single sign-on using a customer's third-party provider.

Correct Answer: C
Section:
Explanation:
https://support.google.com/a/answer/6178640?hl=en
The transfer tool enables you to see what unmanaged users exist, and then invite those unmanaged users to the domain.

QUESTION 102
You have created an OS image that is hardened per your organization's security standards and is being stored in a project managed by the security team. As a Google Cloud administrator, you need to make sure all VMs in your Google Cloud organization can only use that specific OS image while minimizing operational overhead. What should you do? (Choose two.)

A. Grant users the compuce.imageUser role in their own projects.
B. Grant users the compuce.imageUser role in the OS image project.
C. Store the image in every project that is spun up in your organization.
D. Set up an image access organization policy constraint, and list the security team managed project in the projects allow list.
E. Remove VM instance creation permission from users of the projects, and only allow you and your team to create VM instances.

Correct Answer: B, D
Section:
Explanation:
https://cloud.google.com/resource-manager/docs/organization-policy/org-policy-constraints - constraints/compute.trustedImageProjects
This list constraint defines the set of projects that can be used for image storage and disk instantiation for Compute Engine. If this constraint is active, only images from trusted projects will be allowed as the source for boot disks for new instances.

QUESTION 103
You're developing the incident response plan for your company. You need to define the access strategy that your DevOps team will use when reviewing and investigating a deployment issue in your Google Cloud environment. There are two main requirements:
Least-privilege access must be enforced at all times.
The DevOps team must be able to access the required resources only during the deployment issue.
How should you grant access while following Google-recommended best practices?

A. Assign the Project Viewer Identity and Access Management (IAM) role to the DevOps team.
B. Create a custom IAM role with limited list/view permissions, and assign it to the DevOps team.
C. Create a service account, and grant it the Project Owner IAM role. Give the Service Account User Role on this service account to the DevOps team.
D. Create a service account, and grant it limited list/view permissions. Give the Service Account User Role on this service account to the DevOps team.

Correct Answer: D
Section:

QUESTION 104
You are working with a client who plans to migrate their data to Google Cloud. You are responsible for recommending an encryption service to manage their encrypted keys. You have the following requirements:
The master key must be rotated at least once every 45days.
The solution that stores the master key must be FIPS 140-2 Level 3 validated.
The master key must be stored in multiple regions within the US for redundancy.
Which solution meets these requirements?

A. Customer-managed encryption keys with Cloud Key Management Service
B. Customer-managed encryption keys with Cloud HSM
C. Customer-supplied encryption keys
D. Google-managed encryption keys

Correct Answer: B
Section:
Explanation:
https://cloud.google.com/docs/security/key-management-deep-dive https://cloud.google.com/kms/docs/faq

QUESTION 105
You manage your organization's Security Operations Center (SOC). You currently monitor and detect network traffic anomalies in your VPCs based on network logs. However, you want to explore your environment using network payloads and headers. Which Google Cloud product should you use?

A. Cloud IDS
B. VPC Service Controls logs
C. VPC Flow Logs
D. Google Cloud Armor
E. Packet Mirroring

Correct Answer: E
Section:
Explanation:
https://cloud.google.com/vpc/docs/packet-mirroring
Packet Mirroring clones the traffic of specified instances in your Virtual Private Cloud (VPC) network and forwards it for examination. Packet Mirroring captures all traffic and packet data, including payloads and headers.

QUESTION 106
You are consulting with a client that requires end-to-end encryption of application data (including data in transit, data in use, and data at rest) within Google Cloud. Which options should you utilize to accomplish this? (Choose two.)

A. External Key Manager
B. Customer-supplied encryption keys
C. Hardware Security Module
D. Confidential Computing and Istio
E. Client-side encryption

Correct Answer: D, E
Section:
Explanation:
Google Cloud customers with additional requirements for encryption of data over WAN can choose to implement further protections for data as it moves from a user to an application, or virtual machine to virtual machine. These protections include IPSec tunnels, Gmail S/MIME, managed SSL certificates, and Istio. https://cloud.google.com/docs/security/encryption-in-transit

QUESTION 107
You need to enforce a security policy in your Google Cloud organization that prevents users from exposing objects in their buckets externally. There are currently no buckets in your organization. Which solution should you implement proactively to achieve this goal with the least operational overhead?

A. Create an hourly cron job to run a Cloud Function that finds public buckets and makes them private.
B. Enable the constraints/storage.publicAccessPrevention constraint at the organization level.
C. Enable the constraints/storage.uniformBucketLevelAccess constraint at the organization level.
D. Create a VPC Service Controls perimeter that protects the storage.googleapis.com service in your projects that contains buckets. Add any new project that contains a bucket to the perimeter.

Correct Answer: B
Section:
Explanation:
https://cloud.google.com/storage/docs/public-access-prevention
Public access prevention protects Cloud Storage buckets and objects from being accidentally exposed to the public. If your bucket is contained within an organization, you can enforce public access prevention by using the organization policy constraint storage.publicAccessPrevention at the project, folder, or organization level.

QUESTION 108
Your company requires the security and network engineering teams to identify all network anomalies and be able to capture payloads within VPCs. Which method should you use?

A. Define an organization policy constraint.
B. Configure packet mirroring policies.
C. Enable VPC Flow Logs on the subnet.
D. Monitor and analyze Cloud Audit Logs.

Correct Answer: B
Section:

Explanation:
https://cloud.google.com/vpc/docs/packet-mirroring
Packet Mirroring clones the traffic of specified instances in your Virtual Private Cloud (VPC) network and forwards it for examination. Packet Mirroring captures all traffic and packet data, including payloads and headers.

QUESTION 109
Your company is moving to Google Cloud. You plan to sync your users first by using Google Cloud Directory Sync (GCDS). Some employees have already created Google Cloud accounts by using their company email addresses that were created outside of GCDS. You must create your users on Cloud Identity.
What should you do?

A. Configure GCDS and use GCDS search rules lo sync these users.
B. Use the transfer tool to migrate unmanaged users.
C. Write a custom script to identify existing Google Cloud users and call the Admin SDK Directory API to transfer their account.
D. Configure GCDS and use GCDS exclusion rules to ensure users are not suspended.

Correct Answer: D
Section:

QUESTION 110
Your organization is using GitHub Actions as a continuous integration and delivery (Cl/CD) platform. You must enable access to Google Cloud resources from the Cl/CD pipelines in the most secure way.
What should you do?

A. Create a service account key and add it to the GitHub pipeline configuration file.
B. Create a service account key and add it to the GitHub repository content.
C. Configure a Google Kubernetes Engine cluster that uses Workload Identity to supply credentials to GitHub.
D. Configure workload identity federation to use GitHub as an identity pool provider.

Correct Answer: D
Section:

QUESTION 111
Your company must follow industry specific regulations. Therefore, you need to enforce customer-managed encryption keys (CMEK) for all new Cloud Storage resources in the organization called org1.
What command should you execute?

A. * organization policy: constraints/gcp.restrictStorageNonCraekServices * binding at: orgl * policy type: deny * policy value: storage.gcogleapis.com
B. * organization policy: constraints/gcp.restrictHonCmekServices * binding at: orgl * policy type: deny * policy value: storage.googleapis.com
C. * organization policy:constraints/gcp.restrictStorageNonCraekServices * binding at: orgl * policy type: allow * policy value: all supported services
D. * organization policy: constramts/gcp.restrictNonCmekServices * binding at: orgl * policy type: allow * policy value: storage.googleapis.com

Correct Answer: A
Section:

QUESTION 112
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?

A. Create a firewall rule for each virtual private cloud (VPC) to deny traffic from 0 0 0 0/0 with priority 0.

B. Create a hierarchical firewall policy configured at the organization to deny all connections from 0 0 0 0/0.
C. Create a Google Cloud Armor security policy to deny traffic from 0 0 0 0/0.
D. Create a hierarchical firewall policy configured at the organization to allow connections only from internal IP ranges

Correct Answer: B
Section:

QUESTION 113
Your organization must comply with the regulation to keep instance logging data within Europe. Your workloads will be hosted in the Netherlands in region europe-west4 in a new project. You must configure Cloud Logging to keep your data in the country.
What should you do?

A. Configure the organization policy constraint gcp.resourceLocations to europe-west4.
B. Set the logging storage region to eurcpe-west4 by using the gcloud CLI logging settings update.
C. Create a new tog bucket in europe-west4. and redirect the _Def auit bucKet to the new bucket.
D. Configure log sink to export all logs into a Cloud Storage bucket in europe-west4.

Correct Answer: C
Section:

QUESTION 114
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?

A. * 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
B. * 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
C. * 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
D. * 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

Correct Answer: C
Section:

QUESTION 115
Your organization processes sensitive health information. You want to ensure that data is encrypted while in use by the virtual machines (VMs). You must create a policy that is enforced across the entire organization.
What should you do?

A. Implement an organization policy that ensures that all VM resources created across your organization use customer-managed encryption keys (CMEK) protection.
B. Implement an organization policy that ensures all VM resources created across your organization are Confidential VM instances.
C. Implement an organization policy that ensures that all VM resources created across your organization use Cloud External Key Manager (EKM) protection.
D. No action is necessary because Google encrypts data while it is in use by default.

Correct Answer: A

Section:

QUESTION 116
You are a Cloud Identity administrator for your organization. In your Google Cloud environment groups are used to manage user permissions. Each application team has a dedicated group Your team is responsible for creating these groups and the application teams can manage the team members on their own through the Google Cloud console. You must ensure that the application teams can only add users from within your organization to their groups.
What should you do?

A. Change the configuration of the relevant groups in the Google Workspace Admin console to prevent external users from being added to the group.
B. Set an Identity and Access Management (IAM) policy that includes a condition that restricts group membership to user principals that belong to your organization.
C. Define an Identity and Access Management (IAM) deny policy that denies the assignment of principals that are outside your organization to the groups in scope.
D. Export the Cloud Identity logs to BigQuery Configure an alert for external members added to groups Have the alert trigger a Cloud Function instance that removes the external members from the group.

Correct Answer: B
Section:

QUESTION 117
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?

A. 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.
B. Activate Security Command Center (SCC) Premium Create a rule to mute the security findings in SCC so they are not evaluated.
C. 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.
D. 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.

Correct Answer: B
Section:

QUESTION 118
You are routing all your internet facing traffic from Google Cloud through your on-premises internet connection. You want to accomplish this goal securely and with the highest bandwidth possible.
What should you do?

A. Create an HA VPN connection to Google Cloud Replace the default 0 0 0 0/0 route.
B. Create a routing VM in Compute Engine Configure the default route with the VM as the next hop.
C. Configure Cloud Interconnect with HA VPN Replace the default 0 0 0 0/0 route to an on-premises destination.
D. Configure Cloud Interconnect and route traffic through an on-premises firewall.

Correct Answer: D
Section:

QUESTION 119
Your organization is transitioning to Google Cloud You want to ensure that only trusted container images are deployed on Google Kubernetes Engine (GKE) clusters in a project. The containers must be deployed from a centrally managed. Container Registry and signed by a trusted authority.
What should you do?
Choose 2 answers

A. Configure the Binary Authorization policy with respective attestations for the project.
B. Create a custom organization policy constraint to enforce Binary Authorization for Google Kubernetes Engine (GKE).
C. Enable Container Threat Detection in the Security Command Center (SCC) for the project.
D. Configure the trusted image organization policy constraint for the project.
E. Enable Pod Security standards and set them to Restricted.

Correct Answer: A, D
Section:

QUESTION 120
Your organization uses Google Workspace Enterprise Edition tor authentication. You are concerned about employees leaving their laptops unattended for extended periods of time after authenticating into Google Cloud. You must prevent malicious people from using an employee's unattended laptop to modify their environment.
What should you do?

A. Create a policy that requires employees to not leave their sessions open for long durations.
B. Review and disable unnecessary Google Cloud APIs.
C. Require strong passwords and 2SV through a security token or Google authenticate.
D. Set the session length timeout for Google Cloud services to a shorter duration.

Correct Answer: D
Section:

QUESTION 121
You are migrating an on-premises data warehouse to BigQuery Cloud SQL, and Cloud Storage. You need to configure security services in the data warehouse. Your company compliance policies mandate that the data warehouse must:
* Protect data at rest with full lifecycle management on cryptographic keys
* Implement a separate key management provider from data management
* Provide visibility into all encryption key requests
What services should be included in the data warehouse implementation?
Choose 2 answers

A. Customer-managed encryption keys
B. Customer-Supplied Encryption Keys
C. Key Access Justifications
D. Access Transparency and Approval
E. Cloud External Key Manager

Correct Answer: C, E
Section:

QUESTION 122
You are auditing all your Google Cloud resources in the production project. You want to identity all principals who can change firewall rules.
What should you do?

A. Use Policy Analyzer lo query the permissions compute, firewalls, create of compute, firewalls. Create of compute,firewalls.delete.
B. Reference the Security Health Analytics - Firewall Vulnerability Findings in the Security Command Center.

C. Use Policy Analyzer to query the permissions compute, firewalls, get of compute, firewalls, list.
D. Use Firewall Insights to understand your firewall rules usage patterns.

Correct Answer: A
Section:

QUESTION 123
You manage one of your organization's Google Cloud projects (Project A). AVPC Service Control (SC) perimeter is blocking API access requests to this project including Pub/Sub. A resource running under a service account in another project (Project B) needs to collect messages from a Pub/Sub topic in your project Project B is not included in a VPC SC perimeter. You need to provide access from Project B to the Pub/Sub topic in Project A using the principle of least
Privilege.
What should you do?

A. Configure an ingress policy for the perimeter in Project A and allow access for the service account in Project B to collect messages.
B. Create an access level that allows a developer in Project B to subscribe to the Pub/Sub topic that is located in Project A.
C. Create a perimeter bridge between Project A and Project B to allow the required communication between both projects.
D. Remove the Pub/Sub API from the list of restricted services in the perimeter configuration for Project A.

Correct Answer: A
Section:

QUESTION 124
You run applications on Cloud Run. You already enabled container analysis for vulnerability scanning. However, you are concerned about the lack of control on the applications that are deployed. You must ensure that only trusted container images are deployed on Cloud Run.
What should you do?
Choose 2 answers

A. Enable Binary Authorization on the existing Kubernetes cluster.
B. Set the organization policy constraint constraints/run. allowedBinaryAuthorizationPolicie to the list of allowed Binary Authorization policy names.
C. Set the organization policy constraint constraints/compute.trustedimageProjects to the list of protects that contain the trusted container images.
D. Enable Binary Authorization on the existing Cloud Run service.
E. Use Cloud Run breakglass to deploy an image that meets the Binary Authorization policy by default.

Correct Answer: B, D
Section:

QUESTION 125
You have a highly sensitive BigQuery workload that contains personally identifiable information (Pll) that you want to ensure is not accessible from the internet. To prevent data exfiltration only requests from authorized IP addresses are allowed to query your BigQuery tables.
What should you do?

A. Use service perimeter and create an access level based on the authorized source IP address as the condition.
B. Use Google Cloud Armor security policies defining an allowlist of authorized IP addresses at the global HTTPS load balancer.
C. Use the Restrict allowed Google Cloud APIs and services organization policy constraint along with Cloud Data Loss Prevention (DLP).
D. Use the Restrict Resource service usage organization policy constraint along with Cloud Data Loss Prevention (DLP).

Correct Answer: A

Section:

QUESTION 126
Your organization is moving virtual machines (VMs) to Google Cloud. You must ensure that operating system images that are used across your projects are trusted and meet your security requirements.
What should you do?

A. Implement an organization policy to enforce that boot disks can only be created from images that come from the trusted image project.
B. Create a Cloud Function that is automatically triggered when a new virtual machine is created from the trusted image repository Verify that the image is not deprecated.
C. Implement an organization policy constraint that enables the Shielded VM service on all projects to enforce the trusted image repository usage.
D. Automate a security scanner that verifies that no common vulnerabilities and exposures (CVEs) are present in your trusted image repository.

Correct Answer: D
Section:

QUESTION 127
You define central security controls in your Google Cloud environment for one of the folders in your organization you set an organizational policy to deny the assignment of external IP addresses to VMs. Two days later you receive an alert about a new VM with an external IP address under that folder.
What could have caused this alert?

A. The VM was created with a static external IP address that was reserved in the project before the organizational policy rule was set.
B. The organizational policy constraint wasn't properly enforced and is running in 'dry run mode.
C. At project level, the organizational policy control has been overwritten with an 'allow' value.
D. The policy constraint on the folder level does not have any effect because of an allow' value for that constraint on the organizational level.

Correct Answer: A
Section:

QUESTION 128
You are using Security Command Center (SCC) to protect your workloads and receive alerts for suspected security breaches at your company. You need to detect cryptocurrency mining software.
Which SCC service should you use?

A. Container Threat Detection
B. Web Security Scanner
C. Rapid Vulnerability Detection
D. Virtual Machine Threat Detection

Correct Answer: D
Section:

QUESTION 129
Your DevOps team uses Packer to build Compute Engine images by using this process:
1 Create an ephemeral Compute Engine VM.
2 Copy a binary from a Cloud Storage bucket to the VM's file system.
3 Update the VM's package manager.
4 Install external packages from the internet onto the VM.
Your security team just enabled the organizational policy. consrraints/compure.vnExtemallpAccess. to restrict the usage of public IP Addresses on VMs. In response your DevOps team updated their scripts to remove public IP addresses on the Compute Engine VMs however the build pipeline is failing due to connectivity issues.
What should you do?

Choose 2 answers

A. Provision a Cloud NAT instance in the same VPC and region as the Compute Engine VM
B. Provision an HTTP load balancer with the VM in an unmanaged instance group to allow inbound connections from the internet to your VM.
C. Update the VPC routes to allow traffic to and from the internet.
D. Provision a Cloud VPN tunnel in the same VPC and region as the Compute Engine VM.
E. Enable Private Google Access on the subnet that the Compute Engine VM is deployed within.

Correct Answer: A, E
Section:

QUESTION 130
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) Configure a rule to let 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) Let all 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 name machine Configure a rule to let 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 same machine Let all principals in the pool impersonate the Google Cloud service account.

Correct Answer: A
Section:

QUESTION 131
You have stored company approved compute images in a single Google Cloud project that is used as an image repository. This project is protected with VPC Service Controls and exists in the perimeter along with other projects in your organization. This lets other projects deploy images from the image repository project. A team requires deploying a third-party disk image that is stored in an external Google Cloud organization. You need to grant read access to the disk image so that it can be deployed into the perimeter.
What should you do?

A. * 1 Update the perimeter * 2 Configure the egressTo field to set identity Type to any_identity. * 3 Configure the egressFrom field to include the external Google Cloud project number as an allowed resource and the serviceName to compute. googleapis. com.
B. * Allow the external project by using the organizational policy constraints/compute.trustedlmageProjects.
C. * 1 Update the perimeter * 2 Configure the egressTo field to include the external Google Cloud project number as an allowed resource and the serviceName to compute. googleapis. com. * 3 Configure the egressFrom field to set identity Type to any_idestity.
D. * 1 Update the perimeter * 2 Configure the ingressFrcm field to set identityType to an-y_identity. * 3 Configure the ingressTo field to include the external Google Cloud project number as an allowed resource and the serviceName to compute.googleapis -com.

Correct Answer: A
Section:

QUESTION 132
Your organization recently activated the Security Command Center {SCO standard tier. There are a few Cloud Storage buckets that were accidentally made accessible to the public. You need to investigate the impact of the incident and remediate it.
What should you do?

A. * 1 Remove the Identity and Access Management (IAM) granting access to allusers from the buckets * 2 Apply the organization policy storage. unifromBucketLevelAccess to prevent regressions * 3 Query the data access

logs to report on unauthorized access

B. * 1 Change bucket permissions to limit access * 2 Query the data access audit logs for any unauthorized access to the buckets * 3 After the misconfiguration is corrected mute the finding in the Security Command Center
C. * 1 Change permissions to limit access for authorized users * 2 Enforce a VPC Service Controls perimeter around all the production projects to immediately stop any unauthorized access * 3 Review the administrator activity audit logs to report on any unauthorized access
D. * 1 Change the bucket permissions to limit access * 2 Query the buckets usage logs to report on unauthorized access to the data * 3 Enforce the organization policy storage.publicAccessPrevention to avoid regressions

Correct Answer: B
Section:

QUESTION 133
Your organization uses the top-tier folder to separate application environments (prod and dev). The developers need to see all application development audit logs but they are not permitted to review production logs. Your security team can review all logs in production and development environments. You must grant Identity and Access Management (IAM) roles at the right resource level tor the developers and security team while you ensure least privilege.
What should you do?

A. * 1 Grant logging, viewer rote to the security team at the organization resource level. * 2 Grant logging, viewer rote to the developer team at the folder resource level that contains all the dev projects.
B. * 1 Grant logging. viewer rote to the security team at the organization resource level. * 2 Grant logging. admin role to the developer team at the organization resource level.
C. * 1 Grant logging.admin role to the security team at the organization resource level. * 2 Grant logging. viewer rote to the developer team at the folder resource level that contains all the dev projects.
D. * 1 Grant logging.admin role to the security team at the organization resource level. * 2 Grant logging.admin role to the developer team at the organization resource level.

Correct Answer: A
Section:

QUESTION 134
Your organization s customers must scan and upload the contract and their driver license into a web portal in Cloud Storage. You must remove all personally identifiable information (Pll) from files that are older than 12 months. Also you must archive the anonymized files for retention purposes.
What should you do?

A. Set a time to live (TTL) of 12 months for the files in the Cloud Storage bucket that removes PH and moves the files to the archive storage class.
B. Create a Cloud Data Loss Prevention (DLP) inspection job that de-identifies Pll in files created more than 12 months ago and archives them to another Cloud Storage bucket. Delete the original files.
C. Schedule a Cloud Key Management Service (KMS) rotation period of 12 months for the encryption keys of the Cloud Storage files containing Pll to de-identify them Delete the original keys.
D. Configure the Autoclass feature of the Cloud Storage bucket to de-identify Pll Archive the files that are older than 12 months Delete the original files.

Correct Answer: B
Section:

QUESTION 135
After completing a security vulnerability assessment, you learned that cloud administrators leave Google Cloud CLI sessions open for days. You need to reduce the risk of attackers who might exploit these open sessions by setting these sessions to the minimum duration.
What should you do?

A. Set the session duration for the Google session control to one hour.
B. Set the reauthentication frequency (or the Google Cloud Session Control to one hour.
C. Set the organization policy constraint constraints/iam.allowServiceAccountCredentialLifetimeExtension to one hour.
D. Set the organization policy constraint constraints/iam. serviceAccountKeyExpiryHours to one hour and inheritFromParent to false.

Correct Answer: B

Section:

QUESTION 136
Your application is deployed as a highly available cross-region solution behind a global external HTTP(S) load balancer. You notice significant spikes in traffic from multiple IP addresses but it is unknown whether the IPs are malicious. You are concerned about your application's availability. You want to limit traffic from these clients over a specified time interval.
What should you do?

A. Configure a rate_based_ban action by using Google Cloud Armor and set the ban_duration_sec parameter to the specified time interval.
B. Configure a deny action by using Google Cloud Armor to deny the clients that issued too many requests over the specified time interval.
C. Configure a throttle action by using Google Cloud Armor to limit the number of requests per client over a specified time interval.
D. Configure a firewall rule in your VPC to throttle traffic from the identified IP addresses.

Correct Answer: C
Section:

QUESTION 137
You have numerous private virtual machines on Google Cloud. You occasionally need to manage the servers through Secure Socket Shell (SSH) from a remote location. You want to configure remote access to the servers in a manner that optimizes security and cost efficiency.
What should you do?

A. Create a site-to-site VPN from your corporate network to Google Cloud.
B. Configure server instances with public IP addresses Create a firewall rule to only allow traffic from your corporate IPs.
C. Create a firewall rule to allow access from the Identity-Aware Proxy (IAP) IP range Grant the role of an IAP- secured Tunnel User to the administrators.
D. Create a jump host instance with public IP Manage the instances by connecting through the jump host.

Correct Answer: C
Section:

QUESTION 138
Your organization has on-premises hosts that need to access Google Cloud APIs You must enforce private connectivity between these hosts minimize costs and optimize for operational efficiency
What should you do?

A. Route all on-premises traffic to Google Cloud through an IPsec VPN tunnel to a VPC with Private Google Access enabled.
B. Set up VPC peering between the hosts on-premises and the VPC through the internet.
C. Enforce a security policy that mandates all applications to encrypt data with a Cloud Key Management. Service (KMS) key before you send it over the network.
D. Route all on-premises traffic to Google Cloud through a dedicated or Partner interconnect to a VPC with Private Google Access enabled.

Correct Answer: D
Section:

QUESTION 139
Your organization s record data exists in Cloud Storage. You must retain all record data for at least seven years This policy must be permanent.
What should you do?

A. * 1 Identify buckets with record data * 2 Apply a retention policy and set it to retain for seven years * 3 Monitor the bucket by using log-based alerts to ensure that no modifications to the retention policy occurs
B. * 1 Identify buckets with record data * 2 Apply a retention policy and set it to retain for seven years * 3 Remove any Identity and Access Management (IAM) roles that contain the storage buckets update permission
C. * 1 Identify buckets with record data * 2 Enable the bucket policy only to ensure that data is retained * 3 Enable bucket lock

D. * 1 Identify buckets with record data * 2 Apply a retention policy and set it to retain for seven years * 3 Enable bucket lock

Correct Answer: D
Section:

QUESTION 140
Your organization wants to protect all workloads that run on Compute Engine VM to ensure that the instances weren't compromised by boot-level or kernel-level malware. Also, you need to ensure that data in use on the VM cannot be read by the underlying host system by using a hardware-based solution.
What should you do?

A. * 1 Use Google Shielded VM including secure boot Virtual Trusted Platform Module (vTPM) and integrity monitoring * 2 Create a Cloud Run function to check for the VM settings generate metrics and run the function regularly
B. * 1 Activate Virtual Machine Threat Detection in Security Command Center (SCO Premium * 2 Monitor the findings in SCC
C. * 1 Use Google Shielded VM including secure boot Virtual Trusted Platform Module (vTPM) and integrity monitoring * 2 Activate Confidential Computing * 3 Enforce these actions by using organization policies
D. * 1 Use secure hardened images from the Google Cloud Marketplace * 2 When deploying the images activate the Confidential Computing option * 3 Enforce the use of the correct images and Confidential Computing by using organization policies

Correct Answer: C
Section: