Google Professional Cloud Security Engineer

Question #1

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

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

Hide Solution Discussion 34
Correct Answer: AC

Question #2

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

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

Hide Solution Discussion 10
Correct Answer: AB

Community vote distribution
AB (100%)

Question #3

A customer needs an alternative to storing their plain text secrets in their source-code management (SCM) system.
How should the customer achieve this using Google Cloud Platform?

A. Use Cloud Source Repositories, and store secrets in Cloud SQL.
B. Encrypt the secrets with a Customer-Managed Encryption Key (CMEK), and store them in Cloud Storage.
C. Run the Cloud Data Loss Prevention API to scan the secrets, and store them in Cloud SQL.
D. Deploy the SCM to a Compute Engine VM with local SSDs, and enable preemptible VMs.

Hide Solution Discussion 13

Correct Answer: B

Question #4

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

A. Set up Cloud Directory Sync to sync groups, and set IAM permissions on the groups.
B. Set up SAML 2.0 Single Sign-On (SSO), and assign IAM permissions to the groups.
C. Use the Cloud Identity and Access Management API to create groups and IAM permissions from Active Directory.
D. Use the Admin SDK to create groups and assign IAM permissions from Active Directory.

Hide Solution Discussion 26
Correct Answer: A

Question #5

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

A. Ensure that the app does not run as PID 1.
B. Package a single app as a container.
C. Remove any unnecessary tools not needed by the app.
D. Use public container images as a base image for the app.
E. Use many container image layers to hide sensitive information.

Hide Solution Discussion 16
Correct Answer: BC

Question #6

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

A. Cloud Armor
B. VPC Firewall Rules
C. Cloud Identity and Access Management
D. Cloud CDN

Hide Solution Discussion 32
Correct Answer: B

Reason:

- ***VPC Firewall Rules:*** *These rules allow you to control incoming and outgoing traffic to your Virtual Private Cloud (VPC) network. You can create rules that specifically allow traffic only from the "known good CIDR" while blocking all other traffic. This directly enforces the compliance requirement. VPC firewalls also offer basic DDoS protection against SYN floods.*

Here's why the other options are not the best fit:

- ***Cloud Armor:*** *While Cloud Armor is a powerful tool for web application security and DDoS protection, it's primarily designed to protect against external threats and application-layer attacks. It's less focused on controlling access based on simple CIDR rules.*
- ***Cloud Identity and Access Management (IAM):*** *IAM is about managing user identities and permissions within your GCP projects, not network-level access control.*
- ***Cloud CDN:*** *Cloud CDN is for caching content closer to users for faster delivery. It doesn't directly address the requirement of restricting access based on source IP address.*

In summary: *VPC Firewall Rules provide the most direct and effective way to restrict access to your internal web application based on the specified CIDR, while also providing the basic SYN flood protection required.*

Question #7

A company is running workloads in a dedicated server room. They must only be accessed from within the private company network. You need to connect to these workloads from Compute Engine instances within a Google Cloud Platform project.

Which two approaches can you take to meet the requirements? (Choose two.)

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

Hide Solution Discussion 18
Correct Answer: AC

Question #8

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

A. Make sure that the ERP system can validate the JWT assertion in the HTTP requests.
B. Make sure that the ERP system can validate the identity headers in the HTTP requests.
C. Make sure that the ERP system can validate the x-forwarded-for headers in the HTTP requests.
D. Make sure that the ERP system can validate the user's unique identifier headers in the HTTP requests.

Hide Solution Discussion 10
Correct Answer: A

Reason:

- ***How IAP works:*** *When a user tries to access an application protected by IAP, they are redirected to the IAP service. IAP authenticates the user and, if successful, issues a signed JSON Web Token (JWT) containing information about the authenticated user. This JWT is then passed along with the request to the application.*

- ***Validating the JWT:*** *By configuring the ERP system to validate the JWT assertion in the incoming HTTP requests, you ensure that only requests that have been authenticated and authorized by IAP are allowed. This adds the extra security layer the security team desires.*

Here's why the other options are not the best fit:

- ***Identity headers:*** *While IAP might include identity information in headers, relying solely on them is less secure than validating the signed JWT. Headers can be potentially modified in transit.*
- ***x-forwarded-for headers:*** *These headers indicate the original client IP address, but don't guarantee the request originated from IAP.*
- ***User's unique identifier headers:*** *Similar to identity headers, these can be spoofed and are not as secure as JWT validation.*

In summary: *JWT validation provides the most secure and reliable way to ensure that only traffic originating from IAP, and thus authenticated by it, can reach the ERP system.*

Question #9

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

A. Create an Alerting Policy in Stackdriver using a Process Health condition, checking that the number of executions of the script remains below the desired threshold. Enable notifications.
B. Create an Alerting Policy in Stackdriver using the CPU usage metric. Set the threshold to 80% to be notified when the CPU usage goes above this 80%.
C. Log every execution of the script to Stackdriver Logging. Create a User-defined metric in Stackdriver Logging on the logs, and create a Stackdriver Dashboard displaying the metric.
D. Log every execution of the script to Stackdriver Logging. Configure BigQuery as a log sink, and create a BigQuery scheduled query to count the number of executions in a specific timeframe.

Hide Solution Discussion 29
Correct Answer: A

Question #10

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

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

B. 1. Create a Cloud Storage sink with billingAccounts/ABC-BILLING parent and includeChildren property set to False in a dedicated SIEM project. 2. Process Cloud Storage objects in SIEM.
C. 1. Export logs in each dev project to a Cloud Pub/Sub topic in a dedicated SIEM project. 2. Subscribe SIEM to the topic.
D. 1. Create a Cloud Storage sink with a publicly shared Cloud Storage bucket in each project. 2. Process Cloud Storage objects in SIEM.

Hide Solution Discussion 40
Correct Answer: A

Question #11

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

A. VPC Flow Logs
B. Cloud Armor
C. DNS Security Extensions
D. Cloud Identity-Aware Proxy

Hide Solution Discussion 16
Correct Answer: C

Question #12

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

A. Cloud Armor
B. Google Cloud Audit Logs
C. Web Security Scanner
D. Anomaly Detection

Hide Solution Discussion 5
Correct Answer: C

Question #13

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

A. Contact Google Support and initiate the Domain Contestation Process to use the domain name in your new Cloud Identity domain.
B. Register a new domain name, and use that for the new Cloud Identity domain.

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

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

Reason:

Least Disruptive: *This option avoids any changes to the existing G Suite domain, minimizing disruption to users and existing services.*

- ***Centralized Management:*** *By working with the existing Super Administrator, the Systems Engineer can ensure that the data science group's Cloud Identity setup aligns with the company's overall Google Workspace environment. This can simplify user management and access control.*
- ***Potential Cost Savings:*** *If the company is already using G Suite, they might be able to leverage existing licenses or discounts for Cloud Identity, potentially saving costs.*
- ***Collaboration:*** *This approach fosters collaboration between different teams within the company, ensuring a unified and consistent approach to identity management.*

Here's why the other options are not as ideal:

- ***Domain Contestation:*** *This process can be complex, time-consuming, and may not be successful. It also introduces unnecessary risk and disruption to the existing G Suite setup.*
- ***Registering a New Domain:*** *While this is an option, it creates a separate identity domain for the data science group, potentially leading to management overhead and inconsistencies.*
- ***Provisioning a New Super Administrator:*** *This could disrupt existing administrative roles and responsibilities within the G Suite domain.*

In summary: *Collaborating with the existing G Suite administrator and leveraging the existing domain is the most efficient, least disruptive, and potentially cost-effective solution for the data science group's Cloud Identity needs.*

Hide Solution Discussion 29
Correct Answer: D

Question #14

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

A. Organization Administrator
B. Security Reviewer
C. Organization Role Administrator
D. Organization Policy Administrator

Hide Solution Discussion 37
Correct Answer: A

Question #15

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

A. Create a Cloud Storage ACL that allows read-only access from the Compute Engine instance's IP address and allows the application to read from the bucket without credentials.
B. Use a service account with read-only access to the Cloud Storage bucket, and store the credentials to the service account in the config of the application on the Compute Engine instance.
C. Use a service account with read-only access to the Cloud Storage bucket to retrieve the credentials from the instance metadata.
D. Encrypt the data in the Cloud Storage bucket using Cloud KMS, and allow the application to decrypt the data with the KMS key.

Hide Solution Discussion 35
Correct Answer: C

Question #16

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

A. Use Forseti with Firewall filters to catch any unwanted configurations in production.
B. Mandate use of infrastructure as code and provide static analysis in the CI/CD pipelines to enforce policies.
C. Route all VPC traffic through customer-managed routers to detect malicious patterns in production.
D. All production applications will run on-premises. Allow developers free rein in GCP as their dev and QA platforms.

Hide Solution Discussion 28
Correct Answer: B

Question #17

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

A. Generalization
B. Redaction
C. CryptoHashConfig
D. CryptoReplaceFfxFpeConfig

Reason:

- ***Preserves Utility While Protecting Data:*** *Format-Preserving Encryption (FPE) allows you to encrypt the compensation data in a way that retains its format (e.g., numbers stay as numbers) while still being secure. This is crucial for analysis because you can perform calculations and comparisons on the encrypted data without decrypting it.*

- ***Reversible:*** *FPE is reversible, meaning you can decrypt the data if needed to identify specific outliers and understand the underlying values driving the disparities.*

- ***Meets Other Requirements:***

    - ***Individual Privacy:*** *FPE ensures individual compensation values are protected, as they are encrypted.*
    - ***Analysis:*** *The data can still be analyzed in its encrypted form to track changes and identify outliers.*

Here's why the other options are not the best fit:

- ***Generalization:*** *This involves replacing specific values with more general ones (e.g., replacing an age with an age range). While it protects privacy, it might lose too much detail for effective outlier analysis.*
- ***Redaction:*** *This completely removes the sensitive data, making it impossible to perform any analysis or identify outliers.*
- ***CryptoHashConfig:*** *Hashing is one-way and irreversible. While it's good for data masking, it doesn't allow for analysis or reversing the process to identify the original outlier values.*

In summary: *CryptoReplaceFfxFpeConfig provides the best balance of data protection, analytical utility, and reversibility, making it the most suitable technique for this scenario.*

Hide Solution Discussion 39
Correct Answer: D

Question #18

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

A. Set the minimum length for passwords to be 8 characters.
B. Set the minimum length for passwords to be 10 characters.
C. Set the minimum length for passwords to be 12 characters.
D. Set the minimum length for passwords to be 6 characters.

Reference: https://support.google.com/cloudidentity/answer/139399?hl=en

Hide Solution Discussion 23
Correct Answer: A

Question #19

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

A. Generate a data encryption key (DEK) locally to encrypt the data, and generate a new key encryption key (KEK) in Cloud KMS to encrypt the DEK. Store both the encrypted data and the encrypted DEK.

B. Generate a data encryption key (DEK) locally to encrypt the data, and generate a new key encryption key (KEK) in Cloud KMS to encrypt the DEK. Store both the encrypted data and the KEK.

C. Generate a new data encryption key (DEK) in Cloud KMS to encrypt the data, and generate a key encryption key (KEK) locally to encrypt the key. Store both the encrypted data and the encrypted DEK.

D. Generate a new data encryption key (DEK) in Cloud KMS to encrypt the data, and generate a key encryption key (KEK) locally to encrypt the key. Store both the encrypted data and the KEK.

Reason:

- ***Data Encryption Key (DEK) Generated Locally:***
  - *Generating the DEK locally ensures that the key used to encrypt the sensitive data is never directly exposed to Cloud KMS. This adds an extra layer of security by keeping the DEK within your control.*
  - *It's also more efficient to generate the DEK locally, as it avoids the overhead of interacting with Cloud KMS for every encryption operation.*
- ***Key Encryption Key (KEK) in Cloud KMS:***
  - *Cloud KMS is a secure and managed service for storing and managing encryption keys. By generating the KEK in Cloud KMS, you benefit from its robust security features, such as key rotation, access control, and audit logging.*
  - *Using Cloud KMS for the KEK allows you to leverage its key management capabilities while keeping the DEK (which directly encrypts the data) local and more secure.*
- ***Storing Encrypted DEK:***
  - *The DEK needs to be stored alongside the encrypted data so you can decrypt it later. However, it should always be stored in its encrypted form.*
  - *By encrypting the DEK with the KEK stored in Cloud KMS, you ensure that only authorized users with access to the KEK can decrypt the DEK and subsequently the data.*

Why other options are not ideal:

- ***Storing the KEK locally:*** *This defeats the purpose of using a key management service like Cloud KMS and exposes the KEK to potential compromise.*
- ***Generating the DEK in Cloud KMS:*** *While possible, it's less secure than generating it locally, as it exposes the DEK to Cloud KMS.*

In Summary: *Following these practices ensures a strong security posture for your application-layer encryption by combining the efficiency of local DEK generation with the security and management benefits of Cloud KMS for the KEK.*

Hide Solution Discussion 23
Correct Answer: A

Question #20

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

A. Send all logs to the SIEM system via an existing protocol such as syslog.
B. Configure every project to export all their logs to a common BigQuery DataSet, which will be queried by the SIEM system.
C. Configure Organizational Log Sinks to export logs to a Cloud Pub/Sub Topic, which will be sent to the SIEM via Dataflow.
D. Build a connector for the SIEM to query for all logs in real time from the GCP RESTful JSON APIs.

Hide Solution Discussion 13
Correct Answer: C

Question #21

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
E. Cloud Storage

Hide Solution Discussion 25
Correct Answer: CD

Question #22

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.

Hide Solution Discussion 10
Correct Answer: C

Question #23

When working with agents in the support center via online chat, your organization's customers often share pictures of their documents with personally identifiable information (PII). Your leadership team

is concerned that this PII is being stored as part of the regular chat logs, which are reviewed by internal or external analysts for customer service trends.
You want to resolve this concern while still maintaining data utility. What should you do?

A. Use Cloud Key Management Service to encrypt PII shared by customers before storing it for analysis.
B. Use Object Lifecycle Management to make sure that all chat records containing PII 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.

Hide Solution Discussion 5
Correct Answer: C

Question #24

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.

Hide Solution Discussion 18
Correct Answer: C

Question #25

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

Hide Solution Discussion 19
Correct Answer: A

Reference: https://cloud.google.com/docs/enterprise/best-practices-for-enterprise-organizations#centralize_network_control

Question #26

An organization is migrating from their current on-premises productivity software systems to G Suite. Some network security controls were in place that were mandated by a regulatory body in their region for their previous on-premises system. The organization's risk team wants to ensure that network security controls are maintained and effective in G Suite. A security architect supporting this migration has been asked to ensure that network security controls are in place as part of the new shared responsibility model between the organization and Google Cloud.
What solution would help meet the requirements?

A. Ensure that firewall rules are in place to meet the required controls.
B. Set up Cloud Armor to ensure that network security controls can be managed for G Suite.
C. Network security is a built-in solution and Google's Cloud responsibility for SaaS products like G Suite.
D. Set up an array of Virtual Private Cloud (VPC) networks to control network security as mandated by the relevant regulation.

Hide Solution Discussion 16
Correct Answer: C

Question #27

A customer's company has multiple business units. Each business unit operates independently, and each has their own engineering group. Your team wants visibility into all projects created within the company and wants to organize their Google Cloud Platform (GCP) projects based on different business units. Each business unit also requires separate sets of IAM permissions.
Which strategy should you use to meet these needs?

A. Create an organization node, and assign folders for each business unit.
B. Establish standalone projects for each business unit, using gmail.com accounts.
C. Assign GCP resources in a project, with a label identifying which business unit owns the resource.
D. Assign GCP resources in a VPC for each business unit to separate network access.

Hide Solution Discussion 6
Correct Answer: A

Question #28

A company has redundant mail servers in different Google Cloud Platform regions and wants to route customers to the nearest mail server based on location.
How should the company accomplish this?

A. Configure TCP Proxy Load Balancing as a global load balancing service listening on port 995.

B. Create a Network Load Balancer to listen on TCP port 995 with a forwarding rule to forward traffic based on location.
C. Use Cross-Region Load Balancing with an HTTP(S) load balancer to route traffic to the nearest region.
D. Use Cloud CDN to route the mail traffic to the closest origin mail server based on client IP address.

Reason:

- ***TCP Proxy Load Balancing*** *is designed for TCP traffic (such as email, which typically uses ports like* ***995 for POP3S****), and it is a* ***global load balancing service****. It routes traffic based on proximity to the closest backend that can handle the traffic. This means that customer requests will be routed to the nearest mail server, satisfying the requirement to direct customers based on their location.*
- ***Port 995*** *is commonly used for encrypted email traffic (POP3 over SSL/TLS). Since mail services rely on TCP for communication,* ***TCP Proxy Load Balancing*** *is the correct type of load balancer to handle this kind of traffic efficiently.*

Why the other options are less ideal:

- ***B. Create a Network Load Balancer to listen on TCP port 995 with a forwarding rule to forward traffic based on location****: Network Load Balancers are regional, not global, so they do not provide the ability to route traffic based on user location across multiple regions. It cannot route to the nearest server in different regions.*
- ***C. Use Cross-Region Load Balancing with an HTTP(S) load balancer****:* ***HTTP(S) load balancing*** *is specifically designed for HTTP/HTTPS traffic, not for TCP-based protocols like mail services (which use POP3, IMAP, or SMTP). This makes it inappropriate for email traffic.*
- ***D. Use Cloud CDN****:* ***Cloud CDN*** *is designed for serving cached content for web applications, such as static assets for websites, not for routing live TCP-based traffic like email. Cloud CDN does not support mail protocols like POP3, IMAP, or SMTP and is irrelevant in this scenario.*

Thus, ***Option A*** *is the best solution as it allows the company to use* ***TCP Proxy Load Balancing*** *to route mail traffic (on port 995) to the nearest mail server based on the customer's location.*

Hide Solution Discussion 34
Correct Answer: A

Question #29

Your team sets up a Shared VPC Network where project co-vpc-prod is the host project. Your team has configured the firewall rules, subnets, and VPN gateway on the host project. They need to enable Engineering Group A to attach a Compute Engine instance to only the 10.1.1.0/24 subnet.
What should your team grant to Engineering Group A to meet this requirement?

A. Compute Network User Role at the host project level.
B. Compute Network User Role at the subnet level.
C. Compute Shared VPC Admin Role at the host project level.
D. Compute Shared VPC Admin Role at the service project level.

Hide Solution Discussion 26
Correct Answer: B

Question #30

A company migrated their entire data/center to Google Cloud Platform. It is running thousands of instances across multiple projects managed by different departments. You want to have a historical record of what was running in Google Cloud Platform at any point in time.
What should you do?

A. Use Resource Manager on the organization level.
B. Use Forseti Security to automate inventory snapshots.
C. Use Stackdriver to create a dashboard across all projects.
D. Use Security Command Center to view all assets across the organization.

Hide Solution Discussion 34
Correct Answer: D

Question #31

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 current data backup and disaster recovery solutions to GCP for later analysis. The organization's production environment will remain on- premises for an indefinite time. The organization wants a scalable and cost-efficient solution.
Which GCP solution should the organization use?

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

Hide Solution Discussion 20
Correct Answer: B

Question #32

You are creating an internal App Engine application that needs to access a user's Google Drive on the user's behalf. Your company does not want to rely on the current user's credentials. It also wants to follow Google-recommended practices.
What should you do?

A. Create a new Service account, and give all application users the role of Service Account User.
B. Create a new Service account, and add all application users to a Google Group. Give this group the role of Service Account User.
C. Use a dedicated G Suite Admin account, and authenticate the application's operations with these G Suite credentials.
D. Create a new service account, and grant it G Suite domain-wide delegation. Have the application use it to impersonate the user.

Hide Solution Discussion 13
Correct Answer: D

Question #33

A customer wants to move their sensitive workloads to a Compute Engine-based cluster using Managed Instance Groups (MIGs). The jobs are bursty and must be completed quickly. They have a requirement to be able to control the key lifecycle.
Which boot disk encryption solution should you use on the cluster to meet this customer's requirements?

A. Customer-supplied encryption keys (CSEK)
B. Customer-managed encryption keys (CMEK) using Cloud Key Management Service (KMS)
C. Encryption by default
D. Pre-encrypting files before transferring to Google Cloud Platform (GCP) for analysis

Hide Solution Discussion 3
Correct Answer: B

Question #34

Your company is using Cloud Dataproc for its Spark and Hadoop jobs. You want to be able to create, rotate, and destroy symmetric encryption keys used for the persistent disks used by Cloud Dataproc. Keys can be stored in the cloud.
What should you do?

A. Use the Cloud Key Management Service to manage the data encryption key (DEK).
B. Use the Cloud Key Management Service to manage the 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).

Hide Solution Discussion 23
Correct Answer: B

Question #35

You are a member of the security team at an organization. Your team has a single GCP project with credit card payment processing systems alongside web applications and data processing systems. You want to reduce the scope of systems subject to PCI audit standards.
What should you do?

A. Use multi-factor authentication for admin access to the web application.
B. Use only applications certified compliant with PA-DSS.
C. Move the cardholder data environment into a separate GCP project.
D. Use VPN for all connections between your office and cloud environments.

Hide Solution Discussion 7
Correct Answer: C

Question #36

A retail customer allows users to upload comments and product reviews. The customer needs to make sure the text does not include sensitive data before the comments or reviews are published.
Which Google Cloud Service should be used to achieve this?

A. Cloud Key Management Service
B. Cloud Data Loss Prevention API
C. BigQuery
D. Web Security Scanner

Hide Solution Discussion 19
Correct Answer: B

Question #37

A company allows every employee to use Google Cloud Platform. Each department has a Google Group, with all department members as group members. If a department member creates a new project, all members of that department should automatically have read-only access to all new project resources. Members of any other department should not have access to the project. You need to configure this behavior.
What should you do to meet these requirements?

A. Create a Folder per department under the Organization. For each department's Folder, assign the Project Viewer role to the Google Group related to that department.
B. Create a Folder per department under the Organization. For each department's Folder, assign the Project Browser role to the Google Group related to that department.
C. Create a Project per department under the Organization. For each department's Project, assign the Project Viewer role to the Google Group related to that department.
D. Create a Project per department under the Organization. For each department's Project, assign the Project Browser role to the Google Group related to that department.

Hide Solution Discussion 20
Correct Answer: A

Question #38

A customer's internal security team must manage its own encryption keys for encrypting data on Cloud Storage and decides to use customer-supplied encryption keys (CSEK).
How should the team complete this task?

A. Upload the encryption key to a Cloud Storage bucket, and then upload the object to the same bucket.
B. Use the gsutil command line tool to upload the object to Cloud Storage, and specify the location of the encryption key.
C. Generate an encryption key in the Google Cloud Platform Console, and upload an object to Cloud Storage using the specified key.
D. Encrypt the object, then use the gsutil command line tool or the Google Cloud Platform Console to upload the object to Cloud Storage.

Reason:

- ***Client-Side Encryption:*** *With CSEK, you are responsible for encrypting the data before it is sent to Cloud Storage. This means you need to use your own encryption tools and keys to encrypt the object locally.*

- ***Upload the Encrypted Object:*** *Once the object is encrypted, you can upload it to Cloud Storage using the gsutil command-line tool or the Google Cloud Platform Console. You will need to provide the encryption key you used to encrypt the object during the upload process.*

- ***Cloud Storage's Role:*** *Cloud Storage stores the encrypted object and associates it with the provided encryption key. It does not have access to the actual key itself, only a wrapped version of it.*

- ***Decryption:*** *When you need to access the data, you will need to provide the same encryption key to decrypt the object.*

Why other options are incorrect:

- ***A. Upload the key to Cloud Storage:*** *You should **never** upload your raw encryption keys directly to Cloud Storage. This would compromise the security of your data.*
- ***B. gsutil with key location:*** *While gsutil is used for uploading, you don't specify the key's location. You provide the key itself during the upload.*
- ***C. Generate key in GCP Console:*** *CSEK requires you to manage your own keys; you don't generate them within Google Cloud.*

Key Security with CSEK:

- ***Key Management:*** *You are fully responsible for generating, storing, and managing your CSEK keys. This gives you maximum control but also requires careful key management practices.*
- ***Rotation:*** *Regularly rotate your encryption keys to enhance security.*
- ***Secure Storage:*** *Store your keys in a secure location, such as a hardware security module (HSM).*

By following these steps and best practices, you can effectively use CSEK to encrypt your data in Cloud Storage while maintaining complete control over your encryption keys.

Hide Solution Discussion 29
Correct Answer: B

Question #39

A customer has 300 engineers. The company wants to grant different levels of access and efficiently manage IAM permissions between users in the development and production environment projects. Which two steps should the company take to meet these requirements? (Choose two.)

A. Create a project with multiple VPC networks for each environment.
B. Create a folder for each development and production environment.
C. Create a Google Group for the Engineering team, and assign permissions at the folder level.
D. Create an Organizational Policy constraint for each folder environment.
E. Create projects for each environment, and grant IAM rights to each engineering user.

Hide Solution Discussion 16
Correct Answer: BC

Question #40

You want to evaluate your organization's Google Cloud instance for PCI compliance. You need to identify Google's inherent controls.
Which document should you review to find the information?

A. Google Cloud Platform: Customer Responsibility Matrix
B. PCI DSS Requirements and Security Assessment Procedures
C. PCI SSC Cloud Computing Guidelines
D. Product documentation for Compute Engine

Hide Solution Discussion 14
Correct Answer: A

Question #41

Your company runs a website that will store PII on Google Cloud Platform. To comply with data privacy regulations, this data can only be stored for a specific amount of time and must be fully deleted after this specific period. Data that has not yet reached the time period should not be deleted. You want to automate the process of complying with this regulation.
What should you do?

A. Store the data in a single Persistent Disk, and delete the disk at expiration time.
B. Store the data in a single BigQuery table and set the appropriate table expiration time.
C. Store the data in a single Cloud Storage bucket and configure the bucket's Time to Live.
D. Store the data in a single BigTable table and set an expiration time on the column families.

Hide Solution Discussion 20
Correct Answer: C

Question #42

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

A. Use Cloud Build to build the container images.
B. Build small containers using small base images.
C. Delete non-used versions from Container Registry.
D. Use a Continuous Delivery tool to deploy the application.

Hide Solution Discussion 26
Correct Answer: B

Question #43

While migrating your organization's infrastructure to GCP, a large number of users will need to access GCP Console. The Identity Management team already has a well-established way to manage your users and want to keep using your existing Active Directory or LDAP server along with the existing SSO password.
What should you do?

A. Manually synchronize the data in Google domain with your existing Active Directory or LDAP server.
B. Use Google Cloud Directory Sync to synchronize the data in Google domain with your existing Active Directory or LDAP server.
C. Users sign in directly to the GCP Console using the credentials from your on-premises Kerberos compliant identity provider.
D. Users sign in using OpenID (OIDC) compatible IdP, receive an authentication token, then use that token to log in to the GCP Console.

Hide Solution Discussion 9
Correct Answer: B

Question #44

Your company is using GSuite and has developed an application meant for internal usage on Google App Engine. You need to make sure that an external user cannot gain access to the application even when an employee's password has been compromised.
What should you do?

A. Enforce 2-factor authentication in GSuite for all users.
B. Configure Cloud Identity-Aware Proxy for the App Engine Application.
C. Provision user passwords using GSuite Password Sync.
D. Configure Cloud VPN between your private network and GCP.

Hide Solution Discussion 25
Correct Answer: A

Question #45

A large financial institution is moving its Big Data analytics to Google Cloud Platform. They want to have maximum control over the encryption process of data stored at rest in BigQuery.
What technique should the institution use?

A. Use Cloud Storage as a federated Data Source.
B. Use a Cloud Hardware Security Module (Cloud HSM).
C. Customer-managed encryption keys (CMEK).
D. Customer-supplied encryption keys (CSEK).

Hide Solution Discussion 20
Correct Answer: C
Reference: https://cloud.google.com/bigquery/docs/encryption-at-rest

Question #46

A company is deploying their application on Google Cloud Platform. Company policy requires long-term data to be stored using a solution that can automatically replicate data over at least two geographic places.
Which Storage solution are they allowed to use?

A. Cloud Bigtable

B. Cloud BigQuery
C. Compute Engine SSD Disk
D. Compute Engine Persistent Disk

Hide Solution Discussion 48
Correct Answer: B

Question #47

A large e-retailer is moving to Google Cloud Platform with its ecommerce website. The company wants to ensure payment information is encrypted between the customer's browser and GCP when the customers checkout online.
What should they do?

A. Configure an SSL Certificate on an L7 Load Balancer and require encryption.
B. Configure an SSL Certificate on a Network TCP Load Balancer and require encryption.
C. Configure the firewall to allow inbound traffic on port 443, and block all other inbound traffic.
D. Configure the firewall to allow outbound traffic on port 443, and block all other outbound traffic.

Hide Solution Discussion 8
Correct Answer: A

Question #48

Applications often require access to `secrets` - small pieces of sensitive data at build or run time. The administrator managing these secrets on GCP wants to keep a track of `who did what, where, and when?` within their GCP projects.
Which two log streams would provide the information that the administrator is looking for? (Choose two.)

A. Admin Activity logs
B. System Event logs
C. Data Access logs
D. VPC Flow logs
E. Agent logs

Hide Solution Discussion 8
Correct Answer: AC

Question #49

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

A. Migrate the application into an isolated project using a ƛ€Lift & Shiftƛ€ approach. Enable all internal TCP traffic using VPC Firewall rules. Use VPC Flow logs to determine what traffic should be allowed for the application to work properly.

B. Migrate the application into an isolated project using a ג€Lift & Shiftג€ approach in a custom network. Disable all traffic within the VPC and look at the Firewall logs to determine what traffic should be allowed for the application to work properly.
C. Refactor the application into a micro-services architecture in a GKE cluster. Disable all traffic from outside the cluster using Firewall Rules. Use VPC Flow logs to determine what traffic should be allowed for the application to work properly.
D. Refactor the application into a micro-services architecture hosted in Cloud Functions in an isolated project. Disable all traffic from outside your project using Firewall Rules. Use VPC Flow logs to determine what traffic should be allowed for the application to work properly.

Hide Solution Discussion 33
Correct Answer: A

Question #50

Your company has deployed an application on Compute Engine. The application is accessible by clients on port 587. You need to balance the load between the different instances running the application. The connection should be secured using TLS, and terminated by the Load Balancer. What type of Load Balancing should you use?

A. Network Load Balancing
B. HTTP(S) Load Balancing
C. TCP Proxy Load Balancing
D. SSL Proxy Load Balancing

Hide Solution Discussion 11
Correct Answer: D

Question #51

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.

Hide Solution Discussion 19
Correct Answer: A

Question #52

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.

Hide Solution Discussion 18
Correct Answer: AD

Question #53

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.

Hide Solution Discussion 29
Correct Answer: A

Question #54

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.

Hide Solution Discussion 17
Correct Answer: A

Question #55

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

Hide Solution Discussion 17
Correct Answer: A

Question #56

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

Hide Solution Discussion 18
Correct Answer: A

Question #57

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.

Hide Solution Discussion 14
Correct Answer: C

Question #58

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 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

Hide Solution Discussion 20
Correct Answer: BC

Question #59

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.

Hide Solution Discussion 27
Correct Answer: C

Question #60

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.

Hide Solution Discussion 23
Correct Answer: B

Question #61

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.

Hide Solution Discussion 26
Correct Answer: B

Question #62

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

Hide Solution Discussion 17
Correct Answer: B

Question #63

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 ز€in-scope-pciز€.

Reason:

- ***Strong Isolation:*** *Taints and tolerations in Kubernetes provide a powerful mechanism for controlling pod placement. By tainting the in-scope nodes with NoSchedule, you prevent any pods without a matching toleration from being scheduled on those nodes. This ensures that only the PCI-related pods, which have the specific toleration, can run on these dedicated nodes.*

- ***Compliance Focus:*** *This approach directly addresses the compliance requirement by guaranteeing a strict separation between in-scope and out-of-scope workloads. It creates a clear boundary and prevents accidental placement of non-compliant pods on the sensitive nodes.*

- ***Maintainability:*** *Using taints and tolerations is a declarative and maintainable way to enforce pod placement policies. The configuration is embedded within the Kubernetes resources, making it easy to manage and audit.*

Here's why the other options are not as effective:

- ***nodeSelector:*** *While nodeSelector can direct pods to specific nodes, it doesn't prevent other pods from being scheduled on those nodes if resources are available. This doesn't provide the required isolation for PCI compliance.*

- ***Node pool and Pod Security Policy:*** *This approach helps with separating workloads but might not be as granular as taints and tolerations in ensuring that only the in-scope pods run on the designated nodes.*

- ***Namespace:*** *Namespaces provide logical isolation but don't guarantee physical separation of pods onto specific nodes.*

In summary: *Using taints and tolerations provides the strongest isolation and most direct way to ensure that in-scope PCI pods are exclusively scheduled on dedicated nodes, meeting the organization's compliance requirements.*

Hide Solution Discussion 14
Correct Answer: C

Question #64

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.

Reason:

- ***FIPS 140-2 Compliance:*** *BoringCrypto is a FIPS 140-2 validated cryptographic module provided by Google. Using it for both data-at-rest (cache storage) and data-in-transit (VM-to-VM communication) ensures that your encryption meets the FIPS 140-2 standard.*

- ***Comprehensive Coverage:*** *This option addresses both data encryption needs within your messaging app architecture:*

    - ***Local SSD Encryption:*** *By using BoringCrypto to encrypt the data cached on local SSDs, you ensure the confidentiality and integrity of the data at rest.*
    - ***VM-to-VM Communication:*** *Encrypting the UDP communication between instances with BoringCrypto protects the messages exchanged between the application components.*
- ***Flexibility:*** *The application development team can integrate BoringCrypto into their application logic to encrypt the data before writing it to the cache and to encrypt/decrypt messages exchanged between instances. This provides flexibility in how the encryption is implemented within the application.*

Here's why the other options are not as suitable:

- ***Disk Encryption with CMEK/Google-managed key:*** *While disk encryption is important, it doesn't address the encryption of the VM-to-VM communication, which is also necessary for FIPS 140-2 compliance in this scenario.*
- ***Changing from UDP to TCP and enabling BoringSSL:*** *While BoringSSL is a good choice for TLS encryption, it's not FIPS 140-2 validated. Also, changing the communication protocol might have performance implications and require significant code changes.*
- ***Using BoringSSL for instance-to-instance communication:*** *As mentioned earlier, BoringSSL is not FIPS 140-2 validated, so it won't meet the compliance requirements.*

Important Note: *FIPS 140-2 compliance can be complex. It's recommended to consult with security and compliance experts to ensure that your implementation meets all the requirements of the standard.*

Hide Solution Discussion 31
Correct Answer: A

Question #65

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.

Hide Solution Discussion 21
Correct Answer: B

Question #66

**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.

Hide Solution Discussion 15
Correct Answer: B

Question #67

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.

Hide Solution Discussion 13
Correct Answer: A

Question #68

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.

Hide Solution Discussion 14
Correct Answer: C

Question #69

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

Hide Solution Discussion 24
Correct Answer: A

Question #70

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

Hide Solution Discussion 9
Correct Answer: C

Question #71

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.

Hide Solution Discussion 19
Correct Answer: B

Question #72

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

Hide Solution Discussion 13
Correct Answer: BD

Question #73

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

Hide Solution Discussion 15
Correct Answer: B

Question #74

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.

Hide Solution Discussion 7
Correct Answer: C
Reference: https://cloud.google.com/kms/docs/envelope-encryption

Question #75

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

Hide Solution Discussion 14
Correct Answer: A

Question #76

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).

Reason:

- ***Customer-Supplied Encryption Keys (CSEK):*** *CSEK allows you to generate and manage your own encryption keys outside of Google Cloud. This means you can generate the key on-premises and use it to encrypt data stored in Cloud Storage. This gives you complete control over the key lifecycle and ensures that the key never leaves your on-premises environment.*

- ***Data Encryption Key (DEK):*** *The DEK is the specific key used to encrypt and decrypt the data itself. By managing the DEK with CSEK, you ensure that the key used for encryption is generated and controlled within your own secure environment.*

Here's why the other options are not suitable:

- ***Cloud Key Management Service (Cloud KMS) for DEK/KEK:*** *While Cloud KMS is a secure and convenient way to manage keys, it doesn't allow you to use a key generated on-premises. Cloud KMS keys are generated and managed within Google Cloud.*

In summary: *To use a key generated on-premises for encrypting data in Cloud Storage, CSEK is the appropriate solution. It provides the necessary control and flexibility to integrate your on-premises key management with Google Cloud's encryption capabilities.*

Hide Solution Discussion 74
Correct Answer: C

Question #77

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 Cloud 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 Cloud 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 that the App Engine Default Service Account is the only account that can write to the dataset.
D. 1. Go to the Identity and Access Management (IAM) section of the project. 2. Validate that the App Engine Default Service Account is the only account that has a role that can write to BigQuery.

Hide Solution Discussion 8
Correct Answer: A

Question #78

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

Hide Solution Discussion 8
Correct Answer: AB

Question #79

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 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 area in the technology stack should they 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. Managing the latest updates and security patches for the Guest OS
D. Encrypting all stored data

Hide Solution Discussion 12
Correct Answer: B

Question #80

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

Hide Solution Discussion 11
Correct Answer: A

Question #81

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.

Hide Solution Discussion 27
Correct Answer: AB

Question #82

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.
D. Mount a Cloud Storage bucket as a local filesystem on every VM.

Hide Solution Discussion 52
Correct Answer: C

Question #83

As adoption of the Cloud Data Loss Prevention (Cloud DLP) API grows within your company, you need to optimize usage to reduce cost. Cloud 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.

Hide Solution Discussion 7
Correct Answer: C

Question #84

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.

Hide Solution Discussion 9
Correct Answer: B

Question #85

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.

Hide Solution Discussion 13
Correct Answer: A

Question #86

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.

Hide Solution Discussion 16
Correct Answer: B

Question #87

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 the 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.

Hide Solution Discussion 15
Correct Answer: B

Question #88

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.

Hide Solution Discussion 13
Correct Answer: B

Question #89

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.

Hide Solution Discussion 17
Correct Answer: D

Question #90

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.

Hide Solution Discussion 25
Correct Answer: C

Question #91

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.

Hide Solution Discussion 15
Correct Answer: AD

Question #92

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.

Hide Solution Discussion 19
Correct Answer: D

Question #93

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.

Hide Solution Discussion 17
Correct Answer: A

Question #94

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 Human Resources team. What should you do?

A. Perform data masking with the Cloud Data Loss Prevention API, and store that data in BigQuery for later use.
B. Perform data redaction with the Cloud Data Loss Prevention API, and store that data in BigQuery for later use.

C. Perform data inspection with the Cloud Data Loss Prevention API, and store that data in BigQuery for later use.
D. Perform tokenization for Pseudonymization with the Cloud Data Loss Prevention API, and store that data in BigQuery for later use.

Hide Solution Discussion 9
Correct Answer: D

Question #95

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.

Hide Solution Discussion 8
Correct Answer: D

Question #96

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

Hide Solution Discussion 8
Correct Answer: B

Question #97

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.

Hide Solution Discussion 10
Correct Answer: C

Question #98

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

Hide Solution Discussion 6
Correct Answer: A

Question #99

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

Hide Solution Discussion 9

Question #100

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.

Hide Solution Discussion 16
Correct Answer: D

Question #101

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

Hide Solution Discussion 21
Correct Answer: A

Question #102

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

Hide Solution Discussion 11
Correct Answer: CD

Question #103

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.

Hide Solution Discussion 9
Correct Answer: A

Question #104

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.

Hide Solution Discussion 9
Correct Answer: D

Question #105

You want to use the gcloud command-line tool to authenticate using a third-party single sign-on (SSO) SAML identity provider. Which options are necessary to ensure that authentication is supported by the third-party identity provider (IdP)? (Choose two.)

A. SSO SAML as a third-party IdP
B. Identity Platform
C. OpenID Connect

D. Identity-Aware Proxy

E. Cloud Identity

Hide Solution Discussion 26
Correct Answer: AE

Question #106

You work for a large organization where each business unit has thousands of users. You need to delegate management of access control permissions to each business unit. You have the following requirements:
☞ Each business unit manages access controls for their own projects.
☞ Each business unit manages access control permissions at scale.
☞ Business units cannot access other business units' projects.
☞ Users lose their access if they move to a different business unit or leave the company.
☞ Users and access control permissions are managed by the on-premises directory service.
What should you do? (Choose two.)

A. Use VPC Service Controls to create perimeters around each business unit's project.

B. Organize projects in folders, and assign permissions to Google groups at the folder level.

C. Group business units based on Organization Units (OUs) and manage permissions based on OUs

D. Create a project naming convention, and use Google's IAM Conditions to manage access based on the prefix of project names.

E. Use Google Cloud Directory Sync to synchronize users and group memberships in Cloud Identity.

Hide Solution Discussion 5
Correct Answer: BE

Question #107

Your organization recently deployed a new application on Google Kubernetes Engine. You need to deploy a solution to protect the application. The solution has the following requirements:
☞ Scans must run at least once per week
☞ Must be able to detect cross-site scripting vulnerabilities
☞ Must be able to authenticate using Google accounts
Which solution should you use?

A. Google Cloud Armor

B. Web Security Scanner

C. Security Health Analytics

D. Container Threat Detection

Hide Solution Discussion 6
Correct Answer: B

Question #108

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

A. Dedicated Interconnect
B. Cloud Router
C. Cloud VPN
D. Partner Interconnect

Hide Solution Discussion 6
Correct Answer: A

Question #109

Your organization has had a few recent DDoS attacks. You need to authenticate responses to domain name lookups. Which Google Cloud service should you use?

A. Cloud DNS with DNSSEC
B. Cloud NAT
C. HTTP(S) Load Balancing
D. Google Cloud Armor

Hide Solution Discussion 6
Correct Answer: A

Question #110

Your Security team believes that a former employee of your company gained unauthorized access to Google Cloud resources some time in the past 2 months by using a service account key. You need to confirm the unauthorized access and determine the user activity. What should you do?

A. Use Security Health Analytics to determine user activity.
B. Use the Cloud Monitoring console to filter audit logs by user.
C. Use the Cloud Data Loss Prevention API to query logs in Cloud Storage.
D. Use the Logs Explorer to search for user activity.

Hide Solution Discussion 9
Correct Answer: D

Question #111

Your company requires the security and network engineering teams to identify all network anomalies within and across VPCs, internal traffic from VMs to VMs, traffic between end locations on the internet and VMs, and traffic between VMs to Google Cloud services in production. 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.

Hide Solution Discussion 20
Correct Answer: B

Question #112

Your company has been creating users manually in Cloud Identity to provide access to Google Cloud resources. Due to continued growth of the environment, you want to authorize the Google Cloud Directory Sync (GCDS) instance and integrate it with your on-premises LDAP server to onboard hundreds of users. You are required to:
☞ Replicate user and group lifecycle changes from the on-premises LDAP server in Cloud Identity.
☞ Disable any manually created users in Cloud Identity.
You have already configured the LDAP search attributes to include the users and security groups in scope for Google Cloud. What should you do next to complete this solution?

A. 1. Configure the option to suspend domain users not found in LDAP. 2. Set up a recurring GCDS task.
B. 1. Configure the option to delete domain users not found in LDAP. 2. Run GCDS after user and group lifecycle changes.
C. 1. Configure the LDAP search attributes to exclude manually created Cloud Identity users not found in LDAP. 2. Set up a recurring GCDS task.
D. 1. Configure the LDAP search attributes to exclude manually created Cloud Identity users not found in LDAP. 2. Run GCDS after user and group lifecycle changes.

Hide Solution Discussion 10
Correct Answer: A

Question #113

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

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

Hide Solution Discussion 23
Correct Answer: A

Question #114

You recently joined the networking team supporting your company's Google Cloud implementation. You are tasked with familiarizing yourself with the firewall rules configuration and providing recommendations based on your networking and Google Cloud experience. What product should you

recommend to detect firewall rules that are overlapped by attributes from other firewall rules with higher or equal priority?

A. Security Command Center
B. Firewall Rules Logging
C. VPC Flow Logs
D. Firewall Insights

Hide Solution Discussion 9
Correct Answer: D

Question #115

The security operations team needs access to the security-related logs for all projects in their organization. They have the following requirements:
☞ Follow the least privilege model by having only view access to logs.
☞ Have access to Admin Activity logs.
☞ Have access to Data Access logs.
☞ Have access to Access Transparency logs.
Which Identity and Access Management (IAM) role should the security operations team be granted?

A. roles/logging.privateLogViewer
B. roles/logging.admin
C. roles/viewer
D. roles/logging.viewer

Hide Solution Discussion 13
Correct Answer: A

Question #116

You are exporting application logs to Cloud Storage. You encounter an error message that the log sinks don't support uniform bucket-level access policies. How should you resolve this error?

A. Change the access control model for the bucket
B. Update your sink with the correct bucket destination.
C. Add the roles/logging.logWriter Identity and Access Management (IAM) role to the bucket for the log sink identity.
D. Add the roles/logging.bucketWriter Identity and Access Management (IAM) role to the bucket for the log sink identity.

Hide Solution Discussion 7
Correct Answer: A

Question #117

You plan to deploy your cloud infrastructure using a CI/CD cluster hosted on Compute Engine. You want to minimize the risk of its credentials being stolen by a third party. What should you do?

A. Create a dedicated Cloud Identity user account for the cluster. Use a strong self-hosted vault solution to store the user's temporary credentials.
B. Create a dedicated Cloud Identity user account for the cluster. Enable the constraints/iam.disableServiceAccountCreation organization policy at the project level.
C. Create a custom service account for the cluster. Enable the constraints/iam.disableServiceAccountKeyCreation organization policy at the project level
D. Create a custom service account for the cluster. Enable the constraints/iam.allowServiceAccountCredentialLifetimeExtension organization policy at the project level.

Hide Solution Discussion 6
Correct Answer: C

Question #118

You need to set up two network segments: one with an untrusted subnet and the other with a trusted subnet. You want to configure a virtual appliance such as a next-generation firewall (NGFW) to inspect all traffic between the two network segments. How should you design the network to inspect the traffic?

A. 1. Set up one VPC with two subnets: one trusted and the other untrusted. 2. Configure a custom route for all traffic (0.0.0.0/0) pointed to the virtual appliance.
B. 1. Set up one VPC with two subnets: one trusted and the other untrusted. 2. Configure a custom route for all RFC1918 subnets pointed to the virtual appliance.
C. 1. Set up two VPC networks: one trusted and the other untrusted, and peer them together. 2. Configure a custom route on each network pointed to the virtual appliance.
D. 1. Set up two VPC networks: one trusted and the other untrusted. 2. Configure a virtual appliance using multiple network interfaces, with each interface connected to one of the VPC networks.

Hide Solution Discussion 11
Correct Answer: D

Question #119

You are a member of your company's security team. You have been asked to reduce your Linux bastion host external attack surface by removing all public IP addresses. Site Reliability Engineers (SREs) require access to the bastion host from public locations so they can access the internal VPC while off-site. How should you enable this access?

A. Implement Cloud VPN for the region where the bastion host lives.
B. Implement OS Login with 2-step verification for the bastion host.
C. Implement Identity-Aware Proxy TCP forwarding for the bastion host.
D. Implement Google Cloud Armor in front of the bastion host.

Hide Solution Discussion 5
Correct Answer: C

Question #120

You need to enable VPC Service Controls and allow changes to perimeters in existing environments without preventing access to resources. Which VPC Service Controls mode should you use?

A. Cloud Run
B. Native
C. Enforced
D. Dry run

Hide Solution Discussion 7
Correct Answer: D

Community vote distribution
D (100%)

Question #121

You manage your organization's Security Operations Center (SOC). You currently monitor and detect network traffic anomalies in your Google Cloud VPCs based on packet header information. However, you want the capability to explore network flows and their payload to aid investigations. Which Google Cloud product should you use?

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

Hide Solution Discussion 6
Correct Answer: D

Question #122

Your organization acquired a new workload. The Web and Application (App) servers will be running on Compute Engine in a newly created custom VPC. You are responsible for configuring a secure network communication solution that meets the following requirements:
☞ Only allows communication between the Web and App tiers.
☞ Enforces consistent network security when autoscaling the Web and App tiers.
☞ Prevents Compute Engine Instance Admins from altering network traffic.
What should you do?

A. 1. Configure all running Web and App servers with respective network tags. 2. Create an allow VPC firewall rule that specifies the target/source with respective network tags.
B. 1. Configure all running Web and App servers with respective service accounts. 2. Create an allow VPC firewall rule that specifies the target/source with respective service accounts.

C. 1. Re-deploy the Web and App servers with instance templates configured with respective network tags. 2. Create an allow VPC firewall rule that specifies the target/source with respective network tags.

D. 1. Re-deploy the Web and App servers with instance templates configured with respective service accounts. 2. Create an allow VPC firewall rule that specifies the target/source with respective service accounts.

Reason:

- ***Secure Communication and Isolation:*** *Network tags provide a way to logically group instances and apply firewall rules to them. By tagging Web servers and App servers with distinct tags (e.g., "web-tier" and "app-tier"), you can create a firewall rule that allows traffic only between those specific tags. This ensures that only the Web and App tiers can communicate with each other, isolating them from other resources in the VPC.*

- ***Consistent Security with Autoscaling:*** *Instance templates define the configuration of new instances created by autoscaling. By including the appropriate network tags in the instance templates, you ensure that any new Web or App server instances automatically inherit the correct tags and are subject to the defined firewall rules. This enforces consistent network security even when the number of instances changes dynamically.*

- ***Prevent Unauthorized Changes:*** *VPC firewall rules are managed at the project level, not the individual instance level. This means that even if someone has Compute Engine Instance Admin permissions, they cannot modify the firewall rules that govern traffic flow between the Web and App tiers. This prevents accidental or malicious changes to network security.*

Why other options are not as suitable:

- ***Option A:*** *While you can add network tags to existing instances, it's better to use instance templates for consistency and to ensure that new instances created by autoscaling inherit the correct tags.*
- ***Options B and D:*** *Service accounts are used for authentication and authorization, not for network traffic control. VPC firewall rules do not support filtering based on service accounts.*

In summary: *Using instance templates with network tags and VPC firewall rules provides a secure, consistent, and manageable solution for controlling network communication between the Web and App tiers, meeting all the specified requirements.*

Hide Solution Discussion 10
Correct Answer: D

Question #123

You need to connect your organization's on-premises network with an existing Google Cloud environment that includes one Shared VPC with two subnets named
Production and Non-Production. You are required to:
☞ Use a private transport link.
☞ Configure access to Google Cloud APIs through private API endpoints originating from on-premises environments.
☞ Ensure that Google Cloud APIs are only consumed via VPC Service Controls.
What should you do?

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

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

C. 1. Set up a Direct Peering link between the on-premises environment and Google Cloud. 2. Configure private access for both VPC subnets.

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

Hide Solution Discussion 5
Correct Answer: D

Question #124

You are working with protected health information (PHI) for an electronic health record system. The privacy officer is concerned that sensitive data is stored in the analytics system. You are tasked with anonymizing the sensitive data in a way that is not reversible. Also, the anonymized data should not preserve the character set and length. Which Google Cloud solution should you use?

A. Cloud Data Loss Prevention with deterministic encryption using AES-SIV

B. Cloud Data Loss Prevention with format-preserving encryption

C. Cloud Data Loss Prevention with cryptographic hashing

D. Cloud Data Loss Prevention with Cloud Key Management Service wrapped cryptographic keys

Hide Solution Discussion 7
Correct Answer: C

Question #125

You are setting up a CI/CD pipeline to deploy containerized applications to your production clusters on Google Kubernetes Engine (GKE). You need to prevent containers with known vulnerabilities from being deployed. You have the following requirements for your solution:
Must be cloud-native -
☞ Must be cost-efficient
☞ Minimize operational overhead
How should you accomplish this? (Choose two.)

A. Create a Cloud Build pipeline that will monitor changes to your container templates in a Cloud Source Repositories repository. Add a step to analyze Container Analysis results before allowing the build to continue.

B. Use a Cloud Function triggered by log events in Google Cloud's operations suite to automatically scan your container images in Container Registry.

C. Use a cron job on a Compute Engine instance to scan your existing repositories for known vulnerabilities and raise an alert if a non-compliant container image is found.

D. Deploy Jenkins on GKE and configure a CI/CD pipeline to deploy your containers to Container Registry. Add a step to validate your container images before deploying your container to the cluster.

E. In your CI/CD pipeline, add an attestation on your container image when no vulnerabilities have been found. Use a Binary Authorization policy to block deployments of containers with no attestation in your cluster.

Hide Solution Discussion 7
Correct Answer: AE

Question #126

Which type of load balancer should you use to maintain client IP by default while using the standard network tier?

A. SSL Proxy
B. TCP Proxy
C. Internal TCP/UDP
D. TCP/UDP Network

Hide Solution Discussion 11
Correct Answer: D

Question #127

You want to prevent users from accidentally deleting a Shared VPC host project. Which organization-level policy constraint should you enable?

A. compute.restrictSharedVpcHostProjects
B. compute.restrictXpnProjectLienRemoval
C. compute.restrictSharedVpcSubnetworks
D. compute.sharedReservationsOwnerProjects

Hide Solution Discussion 6
Correct Answer: B

Question #128

Users are reporting an outage on your public-facing application that is hosted on Compute Engine. You suspect that a recent change to your firewall rules is responsible. You need to test whether your firewall rules are working properly. What should you do?

A. Enable Firewall Rules Logging on the latest rules that were changed. Use Logs Explorer to analyze whether the rules are working correctly.
B. Connect to a bastion host in your VPC. Use a network traffic analyzer to determine at which point your requests are being blocked.
C. In a pre-production environment, disable all firewall rules individually to determine which one is blocking user traffic.
D. Enable VPC Flow Logs in your VPC. Use Logs Explorer to analyze whether the rules are working correctly.

Hide Solution Discussion 4
Correct Answer: A

Question #129

You are a security administrator at your company. Per Google-recommended best practices, you implemented the domain restricted sharing organization policy to allow only required domains to access your projects. An engineering team is now reporting that users at an external partner outside your organization domain cannot be granted access to the resources in a project. How should you make an exception for your partner's domain while following the stated best practices?

A. Turn off the domain restriction sharing organization policy. Set the policy value to "Allow All."
B. Turn off the domain restricted sharing organization policy. Provide the external partners with the required permissions using Google's Identity and Access Management (IAM) service.
C. Turn off the domain restricted sharing organization policy. Add each partner's Google Workspace customer ID to a Google group, add the Google group as an exception under the organization policy, and then turn the policy back on.
D. Turn off the domain restricted sharing organization policy. Set the policy value to "Custom." Add each external partner's Cloud Identity or Google Workspace customer ID as an exception under the organization policy, and then turn the policy back on.

Hide Solution Discussion 14
Correct Answer: D

Question #130

You plan to use a Google Cloud Armor policy to prevent common attacks such as cross-site scripting (XSS) and SQL injection (SQLi) from reaching your web application's backend. What are two requirements for using Google Cloud Armor security policies? (Choose two.)

A. The load balancer must be an external SSL proxy load balancer.
B. Google Cloud Armor Policy rules can only match on Layer 7 (L7) attributes.
C. The load balancer must use the Premium Network Service Tier.
D. The backend service's load balancing scheme must be EXTERNAL.
E. The load balancer must be an external HTTP(S) load balancer.

Hide Solution Discussion 22
Correct Answer: DE

Question #131

You perform a security assessment on a customer architecture and discover that multiple VMs have public IP addresses. After providing a recommendation to remove the public IP addresses, you are told those VMs need to communicate to external sites as part of the customer's typical operations. What should you recommend to reduce the need for public IP addresses in your customer's VMs?

A. Google Cloud Armor
B. Cloud NAT

C. Cloud Router
D. Cloud VPN

Hide Solution Discussion 2
Correct Answer: B

Question #132

You are tasked with exporting and auditing security logs for login activity events for Google Cloud console and API calls that modify configurations to Google
Cloud resources. Your export must meet the following requirements:
➢ Export related logs for all projects in the Google Cloud organization.
➢ Export logs in near real-time to an external SIEM.
What should you do? (Choose two.)

A. Create a Log Sink at the organization level with a Pub/Sub destination.
B. Create a Log Sink at the organization level with the includeChildren parameter, and set the destination to a Pub/Sub topic.
C. Enable Data Access audit logs at the organization level to apply to all projects.
D. Enable Google Workspace audit logs to be shared with Google Cloud in the Admin Console.
E. Ensure that the SIEM processes the AuthenticationInfo field in the audit log entry to gather identity information.

Hide Solution Discussion 25
Correct Answer: BC

Question #133

Your company's Chief Information Security Officer (CISO) creates a requirement that business data must be stored in specific locations due to regulatory requirements that affect the company's global expansion plans. After working on the details to implement this requirement, you determine the following:
➢ The services in scope are included in the Google Cloud Data Residency Terms.
➢ The business data remains within specific locations under the same organization.
➢ The folder structure can contain multiple data residency locations.
You plan to use the Resource Location Restriction organization policy constraint. At which level in the resource hierarchy should you set the constraint?

A. Folder
B. Resource
C. Project
D. Organization

Hide Solution Discussion 29
Correct Answer: C

Question #134

You need to set up a Cloud interconnect connection between your company's on-premises data center and VPC host network. You want to make sure that on- premises applications can only access Google APIs over the Cloud Interconnect and not through the public internet. You are required to only use APIs that are supported by VPC Service Controls to mitigate against exfiltration risk to non-supported APIs. How should you configure the network?

A. Enable Private Google Access on the regional subnets and global dynamic routing mode.
B. Set up a Private Service Connect endpoint IP address with the API bundle of "all-apis", which is advertised as a route over the Cloud interconnect connection.
C. Use private.googleapis.com to access Google APIs using a set of IP addresses only routable from within Google Cloud, which are advertised as routes over the connection.
D. Use restricted googleapis.com to access Google APIs using a set of IP addresses only routable from within Google Cloud, which are advertised as routes over the Cloud Interconnect connection.

Hide Solution Discussion 14
Correct Answer: D

Question #135

You need to implement an encryption-at-rest strategy that protects sensitive data and reduces key management complexity for non-sensitive data. Your solution has the following requirements:
☞ Schedule key rotation for sensitive data.
☞ Control which region the encryption keys for sensitive data are stored in.
☞ Minimize the latency to access encryption keys for both sensitive and non-sensitive data.
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.

Hide Solution Discussion 11
Correct Answer: D

Question #136

Your security team uses encryption keys to ensure confidentiality of user data. You want to establish a process to reduce the impact of a potentially compromised symmetric encryption key in Cloud Key Management Service (Cloud KMS).
Which steps should your team take before an incident occurs? (Choose two.)

A. Disable and revoke access to compromised keys.
B. Enable automatic key version rotation on a regular schedule.
C. Manually rotate key versions on an ad hoc schedule.
D. Limit the number of messages encrypted with each key version.
E. Disable the Cloud KMS API.

Hide Solution Discussion 13
Correct Answer: BD

Question #137

Your company's chief information security officer (CISO) is requiring business data to be stored in specific locations due to regulatory requirements that affect the company's global expansion plans. After working on a plan to implement this requirement, you determine the following:
☞ The services in scope are included in the Google Cloud data residency requirements.
☞ The business data remains within specific locations under the same organization.
☞ The folder structure can contain multiple data residency locations.
☞ The projects are aligned to specific locations.
You plan to use the Resource Location Restriction organization policy constraint with very granular control. At which level in the hierarchy should you set the constraint?

A. Organization
B. Resource
C. Project
D. Folder

Hide Solution Discussion 15
Correct Answer: C

Question #138

A database administrator notices malicious activities within their Cloud SQL instance. The database administrator wants to monitor the API calls that read the configuration or metadata of resources. Which logs should the database administrator review?

A. Admin Activity
B. System Event
C. Access Transparency
D. Data Access

Hide Solution Discussion 6
Correct Answer: D

Question #139

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

A. Upload the logs to both the shared bucket and the bucket with PII that is only accessible to the administrator. Use the Cloud Data Loss Prevention API to create a job trigger. Configure the trigger to delete any files that contain PII from the shared bucket.
B. On the shared bucket, configure Object Lifecycle Management to delete objects that contain PII.

C. On the shared bucket, configure a Cloud Storage trigger that is only triggered when PII is uploaded. Use Cloud Functions to capture the trigger and delete the files that contain PII.

D. Use Pub/Sub and Cloud Functions to trigger a Cloud Data Loss Prevention scan every time a file is uploaded to the administrator's bucket. If the scan does not detect PII, have the function move the objects into the shared Cloud Storage bucket.

Hide Solution Discussion 4
Correct Answer: D

Question #140

You work for an organization in a regulated industry that has strict data protection requirements. The organization backs up their data in the cloud. To comply with data privacy regulations, this data can only be stored for a specific length of time and must be deleted after this specific period.
You want to automate the compliance with this regulation while minimizing storage costs. What should you do?

A. Store the data in a persistent disk, and delete the disk at expiration time.

B. Store the data in a Cloud Bigtable table, and set an expiration time on the column families.

C. Store the data in a BigQuery table, and set the table's expiration time.

D. Store the data in a Cloud Storage bucket, and configure the bucket's Object Lifecycle Management feature.

Hide Solution Discussion 8
Correct Answer: D

Question #141

You have been tasked with configuring Security Command Center for your organization's Google Cloud environment. Your security team needs to receive alerts of potential crypto mining in the organization's compute environment and alerts for common Google Cloud misconfigurations that impact security. Which Security Command Center features should you use to configure these alerts? (Choose two.)

A. Event Threat Detection

B. Container Threat Detection

C. Security Health Analytics

D. Cloud Data Loss Prevention

E. Google Cloud Armor

Hide Solution Discussion 8
Correct Answer: AC

Question #142

You have noticed an increased number of phishing attacks across your enterprise user accounts. You want to implement the Google 2-Step Verification (2SV) option that uses a cryptographic signature to authenticate a user and verify the URL of the login page. Which Google 2SV option should you use?

A. Titan Security Keys

B. Google prompt
C. Google Authenticator app
D. Cloud HSM keys

Hide Solution Discussion 9
Correct Answer: A

Question #143

Your organization hosts a financial services application running on Compute Engine instances for a third-party company. The third-party company's servers that will consume the application also run on Compute Engine in a separate Google Cloud organization. You need to configure a secure network connection between the Compute Engine instances. You have the following requirements:
☞ The network connection must be encrypted.
☞ The communication between servers must be over private IP addresses.
What should you do?

A. Configure a Cloud VPN connection between your organization's VPC network and the third party's that is controlled by VPC firewall rules.
B. Configure a VPC peering connection between your organization's VPC network and the third party's that is controlled by VPC firewall rules.
C. Configure a VPC Service Controls perimeter around your Compute Engine instances, and provide access to the third party via an access level.
D. Configure an Apigee proxy that exposes your Compute Engine-hosted application as an API, and is encrypted with TLS which allows access only to the third party.

Hide Solution Discussion 26
Correct Answer: B

Question #144

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.

Hide Solution Discussion 36
Correct Answer: CE

Question #145

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

Hide Solution Discussion 6
Correct Answer: A

Question #146

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.

Hide Solution Discussion 6
Correct Answer: C

Question #147

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.

Hide Solution Discussion 4
Correct Answer: A

Question #148

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

Hide Solution Discussion 3
Correct Answer: A

Question #149

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.

Hide Solution Discussion 5
Correct Answer: D

Question #150

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.

Hide Solution Discussion 25
Correct Answer: C

Question #151

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.

Hide Solution Discussion 5
Correct Answer: C

Question #152

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.

Hide Solution Discussion 10
Correct Answer: D

Question #153

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.

Hide Solution Discussion 6
Correct Answer: C

Question #154

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

Hide Solution Discussion 5
Correct Answer: B

Question #155

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.

Hide Solution Discussion 5
Correct Answer: C

Question #156

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.

Hide Solution Discussion 23
Correct Answer: CD

Question #157

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.

Hide Solution Discussion 9
Correct Answer: CE

Question #158

You are deploying a web application hosted on Compute Engine. A business requirement mandates that application logs are preserved for 12 years 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.

Hide Solution Discussion 20
Correct Answer: A

Question #159

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

Hide Solution Discussion 13
Correct Answer: BE

Question #160

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

Hide Solution Discussion 8
Correct Answer: AD

Question #161

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

Hide Solution Discussion 28
Correct Answer: B

Question #162

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

A. Security Reviewer

B. IAP-Secured Tunnel User

C. IAP-Secured Web App User

D. Service Broker Operator

Hide Solution Discussion 9
Correct Answer: C

Question #163

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.

Hide Solution Discussion 24
Correct Answer: AD

Question #164

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.

Hide Solution Discussion 6
Correct Answer: A

Question #165

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.

Hide Solution Discussion 6

Correct Answer: DE

Question #166

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.

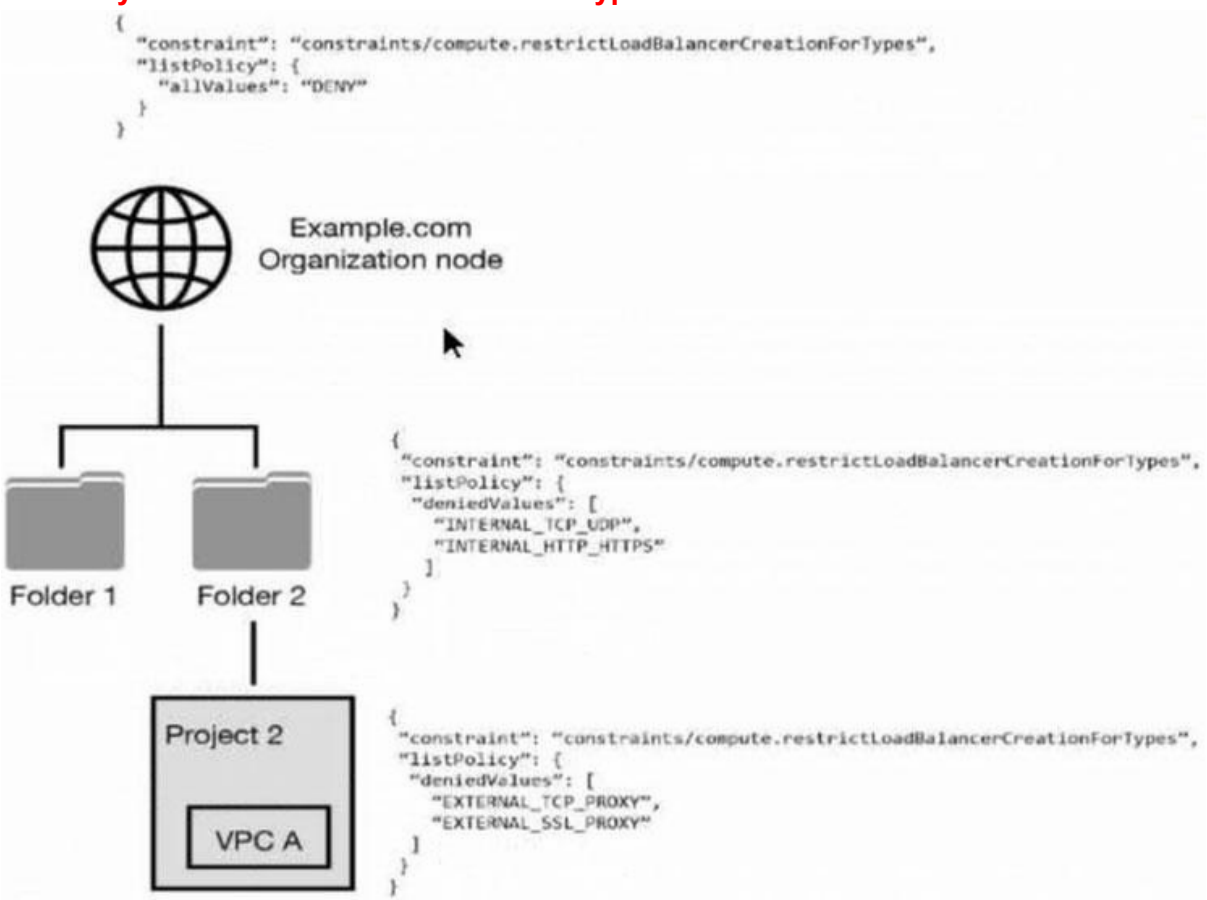
D. Configure Google Cloud Armor access logs to perform inspection on the log data.

Hide Solution Discussion 6

Correct Answer: A

Question #167

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.

Hide Solution Discussion 18
Correct Answer: A

Question #168

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.

Hide Solution Discussion 7
Correct Answer: B

Question #169

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.

Hide Solution Discussion 5
Correct Answer: D

Question #170

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.

Reason:

- ***Designed for this scenario:*** *The transfer tool in Cloud Identity is specifically created to address the situation where users have existing consumer accounts (like Gmail) with the corporate domain. It provides a streamlined process to convert these unmanaged accounts into managed Cloud Identity accounts.*
- ***Preserves data and access:*** *This tool allows users to transfer their existing data and access to the managed account, minimizing disruption and ensuring a smooth transition.*
- ***Centralized management:*** *By converting these accounts, you bring them under your organization's control within Cloud Identity. This enables centralized management of user identities, access policies, and security settings.*

Why other options are less suitable:

- ***Use Google Cloud Directory Sync to convert the unmanaged user accounts.*** *Directory Sync is primarily used for synchronizing users from on-premises directories (like Active Directory) to Cloud Identity. It's not the ideal tool for converting existing consumer accounts.*
- ***Create a new managed user account for each consumer user account.*** *This would result in duplicate accounts for the same user, leading to confusion and potential data inconsistencies. It's not an efficient or recommended approach.*
- ***Configure single sign-on using a customer's third-party provider.*** *While SSO is valuable for centralized authentication, it doesn't address the core issue of unmanaged consumer accounts using the corporate domain.*

The transfer tool offers the most direct and effective way to manage consumer user accounts with Cloud Identity, ensuring a smooth transition and centralized control.

Hide Solution Discussion 7
Correct Answer: C

Question #171

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 compute.imageUser role in their own projects.
B. Grant users the compute.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 project's allow list.

E. Remove VM instance creation permission from users of the projects, and only allow you and your team to create VM instances.

Hide Solution Discussion 12
Correct Answer: BD

Question #172

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.

Hide Solution Discussion 26
Correct Answer: D

Question #173

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 45 days.
☞ 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

Hide Solution Discussion 13
Correct Answer: B

Question #174

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

Hide Solution Discussion 11
Correct Answer: E

Question #175

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

Solution Discussion 14
Correct Answer: DE

Question #176

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.

Hide Solution Discussion 8
Correct Answer: B

Question #177

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.

Hide Solution Discussion 7
Correct Answer: B

Question #178

**An organization 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?**

A. Cryptographic hashing
B. Redaction
C. Format-preserving encryption
D. Generalization

Hide Solution Discussion 10
Correct Answer: C

Community vote distribution

Question #179

You need to set up a Cloud Interconnect connection between your company's on-premises data center and VPC host network. You want to make sure that on-premises applications can only access Google APIs over the Cloud Interconnect and not through the public internet. You are required to only use APIs that are supported by VPC Service Controls to mitigate against exfiltration risk to non-supported APIs. How should you configure the network?

A. Enable Private Google Access on the regional subnets and global dynamic routing mode.
B. Create a CNAME to map *.googleapis.com to restricted.googleapis.com, and create A records for restricted.googleapis.com mapped to 199.36.153.8/30.
C. Use private.googleapis.com to access Google APIs using a set of IP addresses only routable from within Google Cloud, which are advertised as routes over the connection.
D. Use restricted googleapis.com to access Google APIs using a set of IP addresses only routable from within Google Cloud, which are advertised as routes over the Cloud Interconnect connection.

Hide Solution Discussion 4
Correct Answer: D

Question #180

**Your organization develops software involved in many open source projects and is concerned about software supply chain threats. You need to deliver provenance for the build to demonstrate the software is untampered.
What should you do?**

A. 1. Hire an external auditor to review and provide provenance.
   2. Define the scope and conditions.
   3. Get support from the Security department or representative.
   4. Publish the attestation to your public web page.

B. 1. Review the software process.
2. Generate private and public key pairs and use Pretty Good Privacy (PGP) protocols to sign the output software artifacts together with a file containing the address of your enterprise and point of contact.
3. Publish the PGP signed attestation to your public web page.

C. 1. Publish the software code on GitHub as open source.
2. Establish a bug bounty program, and encourage the open source community to review, report, and fix the vulnerabilities.

D. 1. Generate Supply Chain Levels for Software Artifacts (SLSA) level 3 assurance by using Cloud Build.
2. View the build provenance in the Security insights side panel within the Google Cloud console.

Hide Solution Discussion 5
Correct Answer: D

Question #181

Your organization operates Virtual Machines (VMs) with only private IPs in the Virtual Private Cloud (VPC) with internet access through Cloud NAT. Everyday, you must patch all VMs with critical OS updates and provide summary reports.
What should you do?

A. Validate that the egress firewall rules allow any outgoing traffic. Log in to each VM and execute OS specific update commands. Configure the Cloud Scheduler job to update with critical patches daily for daily updates.

B. Copy the latest patches to the Cloud Storage bucket. Log in to each VM, download the patches from the bucket, and install them.

C. Assign public IPs to VMs. Validate that the egress firewall rules allow any outgoing traffic. Log in to each VM, and configure a daily cron job to enable for OS updates at night during low activity periods.

D. Ensure that VM Manager is installed and running on the VMs. In the OS patch management service, configure the patch jobs to update with critical patches dally.

Hide Solution Discussion 7
Correct Answer: D

Question #182

For compliance reporting purposes, the internal audit department needs you to provide the list of virtual machines (VMs) that have critical operating system (OS) security updates available, but not installed. You must provide this list every six months, and you want to perform this task quickly.
What should you do?

A. Run a Security Command Center security scan on all VMs to extract a list of VMs with critical OS vulnerabilities every six months.

B. Run a gcloud CLI command from the Command Line Interface (CLI) to extract the VM's OS version information every six months.

C. Ensure that the Cloud Logging agent is installed on all VMs, and extract the OS last update log date every six months.

D. Ensure the OS Config agent is installed on all VMs and extract the patch status dashboard every six months.

Hide Solution Discussion 8

Correct Answer: D

Question #183

Your company conducts clinical trials and needs to analyze the results of a recent study that are stored in BigQuery. The interval when the medicine was taken contains start and stop dates. The interval data is critical to the analysis, but specific dates may identify a particular batch and introduce bias. You need to obfuscate the start and end dates for each row and preserve the interval data. What should you do?

A. Use date shifting with the context set to the unique ID of the test subject.

B. Extract the date using TimePartConfig from each date field and append a random month and year.

C. Use bucketing to shift values to a predetermined date based on the initial value.

D. Use the FFX mode of format preserving encryption (FPE) and maintain data consistency.

Reason:

- ***Date Shifting:*** *Date shifting involves adding or subtracting a consistent time interval (e.g., days, weeks, months) from each date in a dataset. This preserves the relative difference between dates (the interval) while masking the actual dates.*

- ***Contextual Shifting:*** *By setting the context to the unique ID of the test subject, you ensure that the same shift is applied to all dates related to that individual. This maintains the integrity of the interval data within each subject's records.*

- ***Preserving Intervals:*** *This technique is crucial for your analysis because it allows you to study the time intervals between medicine intake without revealing the actual dates, which could introduce bias or compromise patient privacy.*

- ***Example:*** *If Subject A took medicine from January 1st to January 10th, and you apply a 30-day shift, the obfuscated data would show they took it from February 1st to February 10th. The 10-day interval is preserved, but the actual dates are masked.*

Why other options are less suitable:

- ***B. TimePartConfig and random date:*** *This approach would destroy the interval information, as you're essentially creating random dates.*
- ***C. Bucketing:*** *Bucketing groups dates into predefined ranges, which might not be granular enough for your analysis and could still reveal potential patterns.*
- ***D. Format-Preserving Encryption (FPE):*** *While FPE can obfuscate data while maintaining its format, it might not be the most practical for date shifting and preserving intervals across multiple related dates.*

In summary: *Date shifting with a context set to the unique ID of the test subject provides the most effective way to obfuscate dates in your clinical trial data while preserving the critical interval information needed for your analysis. This approach balances data privacy with the needs of your research.*

Hide Solution Discussion 5

Correct Answer: A

Question #184

You have a highly sensitive BigQuery workload that contains personally identifiable information (PII) 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 Resource Service Usage organization policy constraint along with Cloud Data Loss Prevention (DLP).
D. Use the Restrict allowed Google Cloud APIs and services organization policy constraint along with Cloud Data Loss Prevention (DLP).

Reason:

***Option A (Correct)**: Using a **service perimeter** with **VPC Service Controls** is designed to protect resources like BigQuery from unauthorized access, especially from the public internet. A service perimeter allows you to restrict the access of certain APIs and services to only authorized networks or IP addresses. By creating an **access level** based on the authorized source IP addresses, you can ensure that only requests from those specific IP addresses can query your BigQuery tables. This is a standard practice for securing sensitive data like PII in BigQuery.*

- ***Option B (Incorrect)**: **Google Cloud Armor** is a security service used to protect applications from attacks and apply IP-based restrictions, but it is not designed to protect resources such as BigQuery that operate at the API level. Cloud Armor is typically applied at the level of HTTP(S) load balancers, so it doesn't directly restrict access to BigQuery.*
- ***Option C (Incorrect)**: The **Restrict Resource Service Usage** organization policy constraint is used to limit which Google Cloud resources can be used by your organization, but it doesn't directly address controlling access based on IP addresses. Cloud Data Loss Prevention (DLP) is for scanning and detecting sensitive data, but it won't prevent access from unauthorized IPs.*
- ***Option D (Incorrect)**: The **Restrict allowed Google Cloud APIs and services** constraint limits which APIs and services can be used, but it doesn't restrict access based on IP addresses. Cloud DLP again helps with identifying and protecting sensitive data but does not enforce network-level security.*

*In summary, **A** directly addresses the requirement to restrict access to BigQuery based on authorized IP addresses, ensuring data security for highly sensitive workloads.*

Hide Solution Discussion 6
Correct Answer: A

Question #185

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. Implement an organization policy constraint that enables the Shielded VM service on all projects to enforce the trusted image repository usage.
C. 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.
D. Automate a security scanner that verifies that no common vulnerabilities and exposures (CVEs) are present in your trusted image repository.

Hide Solution Discussion 9
Correct Answer: A

Question #186

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. Allow the external project by using the organizational policy, constraints/compute.trustedImageProjects.
B. 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 identityType to ANY_IDENTITY.
C. 1. Update the perimeter.
2. Configure the ingressFrom field to set identityType to ANY_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.
D. 1. Update the perimeter.
2. Configure the egressTo field to set identityType 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.

Hide Solution Discussion 12
Correct Answer: B

Question #187

A service account key has been publicly exposed on multiple public code repositories. After reviewing the logs, you notice that the keys were used to generate short-lived credentials. You need to immediately remove access with the service account.
What should you do?

A. Delete the compromised service account.
B. Disable the compromised service account key.
C. Wait until the service account credentials expire automatically.
D. Rotate the compromised service account key.

Hide Solution Discussion 10
Correct Answer: A

Question #188

A company is using Google Kubernetes Engine (GKE) with container images of a mission-critical application. The company wants to scan the images for known security issues and securely share the report with the security team without exposing them outside Google Cloud.
What should you do?

A. 1. Enable Container Threat Detection in the Security Command Center Premium tier.
   2. Upgrade all clusters that are not on a supported version of GKE to the latest possible GKE version.
   3. View and share the results from the Security Command Center.
B. 1. Use an open source tool in Cloud Build to scan the images.
   2. Upload reports to publicly accessible buckets in Cloud Storage by using gsutil.
   3. Share the scan report link with your security department.
C. 1. Enable vulnerability scanning in the Artifact Registry settings.
   2. Use Cloud Build to build the images.
   3. Push the images to the Artifact Registry for automatic scanning.
   4. View the reports in the Artifact Registry.
D. 1. Get a GitHub subscription.
   2. Build the images in Cloud Build and store them in GitHub for automatic scanning.
   3. Download the report from GitHub and share with the Security Team.

Hide Solution Discussion 10
Correct Answer: C

Question #189

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

D. Configure a deny action by using Google Cloud Armor to deny the clients that issued too many requests over the specified time interval.

Hide Solution Discussion 5
Correct Answer: A

Question #190

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

A. 1. Create a new SAML profile.
2. Populate the sign-in and sign-out page URLs.
3. Upload the X.509 certificate.
4. Configure Entity ID and ACS URL in your IdP.

B. 1. Configure prerequisites for OpenID Connect (OIDC) in your Active Directory (AD) tenant.
2. Verify the AD domain.
3. Decide which users should use SAML.
4. Assign the pre-configured profile to the select organizational units (OUs) and groups.

C. 1. Create a new SAML profile.
2. Upload the X.509 certificate.
3. Enable the change password URL.
4. Configure Entity ID and ACS URL in your IdP.

D. 1. Manage SAML profile assignments.
2. Enable OpenID Connect (OIDC) in your Active Directory (AD) tenant.
3. Verify the domain.

Hide Solution Discussion 3
Correct Answer: A

Community vote distribution
A (100%)

Question #191

Employees at your company use their personal computers to access your organization's Google Cloud console. You need to ensure that users can only access the Google Cloud console from their corporate-issued devices and verify that they have a valid enterprise certificate.
What should you do?

A. Implement an Access Policy in BeyondCorp Enterprise to verify the device certificate. Create an access binding with the access policy just created.

B. Implement a VPC firewall policy. Activate packet inspection and create an allow rule to validate and verify the device certificate.

C. Implement an organization policy to verify the certificate from the access context.

D. Implement an Identity and Access Management (IAM) conditional policy to verify the device certificate.

Hide Solution Discussion 7
Correct Answer: A

Question #192 IMP

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 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.
B. 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.
C. 1. Create individual service accounts for 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 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.

Hide Solution Discussion 6
Correct Answer: A

Question #193

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 (PII) 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 PII and moves the files to the archive storage class.
B. Create a Cloud Data loss Prevention (DLP) inspection job that de-identifies PII in files created more than 12 months ago and archives them to another Cloud Storage bucket. Delete the original files.

C. Configure the Autoclass feature of the Cloud Storage bucket to de-identify PII. Archive the files that are older than 12 months. Delete the original files.
D. Schedule a Cloud Key Management Service (KMS) rotation period of 12 months for the encryption keys of the Cloud Storage files containing PII to de-identify them. Delete the original keys.

Hide Solution Discussion 5
Correct Answer: B

Question #194

You plan to synchronize identities to Cloud Identity from a third-party identity provider (IdP). You discovered that some employees used their corporate email address to set up consumer accounts to access Google services. You need to ensure that the organization has control over the configuration, security, and lifecycle of these consumer accounts.
What should you do? (Choose two.)

A. Mandate that those corporate employees delete their unmanaged consumer accounts.
B. Reconcile accounts that exist in Cloud Identity but not in the third-party IdP.
C. Evict the unmanaged consumer accounts in the third-party IdP before you sync identities.
D. Use Google Cloud Directory Sync (GCDS) to migrate the unmanaged consumer accounts' emails as user aliases.
E. Use the transfer tool to invite those corporate employees to transfer their unmanaged consumer accounts to the corporate domain.

Hide Solution Discussion 12
Correct Answer: B

Question #195

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

A. Use Policy Analyzer to query the permissions compute.firewalls.get or compute.firewalls.list.
B. Use Firewall Insights to understand your firewall rules usage patterns.
C. Reference the Security Health Analytics – Firewall Vulnerability Findings in the Security Command Center.
D. Use Policy Analyzer to query the permissions compute.firewalls.create or compute.firewalls.update or compute.firewalls.delete.

Hide Solution Discussion 7
Correct Answer: D

Question #196

Your organization previously stored files in Cloud Storage by using Google Managed Encryption Keys (GMEK), but has recently updated the internal policy to require Customer Managed Encryption Keys (CMEK). You need to re-encrypt the files quickly and efficiently with minimal cost.
What should you do?

A. Reupload the files to the same Cloud Storage bucket specifying a key file by using gsutil.
B. Encrypt the files locally, and then use gsutil to upload the files to a new bucket.
C. Copy the files to a new bucket with CMEK enabled in a secondary region.
D. Change the encryption type on the bucket to CMEK, and rewrite the objects.

Hide Solution Discussion 9
Correct Answer: D

Question #197

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 two.)

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

Reason:

- ***A. Enable Binary Authorization on the existing Cloud Run service.*** *This directly addresses your need to ensure only trusted container images are deployed. Binary Authorization acts as a gatekeeper, blocking any deployments that don't meet your defined criteria. You can configure it to require attestations like vulnerability scan results or approvals from specific authorities.*

- ***B. Set the organization policy constraint constraints/run.allowedBinaryAuthorizationPolicies to the list of allowed Binary Authorization policy names.*** *This enforces your Binary Authorization policy at the organizational level, preventing developers from bypassing it. It ensures that all Cloud Run deployments across your organization adhere to your security standards.*

Why the other options are not as effective:

- ***C. Enable Binary Authorization on the existing Kubernetes cluster.*** *While Binary Authorization can be used with GKE, it's not relevant for Cloud Run, which is a serverless platform.*
- ***D. Use Cloud Run breakglass.*** *Breakglass is designed for emergency situations where you need to bypass security controls temporarily. It shouldn't be used as a standard deployment mechanism.*
- ***E. Set the organization policy constraint constraints/compute.trustedImageProjects.*** *This constraint is specifically for Compute Engine, not Cloud Run.*

In summary: *By enabling Binary Authorization on your Cloud Run service and enforcing it with an organization policy, you establish a robust and automated security control that ensures only trusted container images are deployed. This significantly improves the security of your Cloud Run applications.*

Hide Solution Discussion 12
Correct Answer: AB

Question #198

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. Set up VPC peering between the hosts on-premises and the VPC through the internet.
B. Route all on-premises traffic to Google Cloud through an IPsec VPN tunnel to a VPC with Private Google Access enabled.
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.

Hide Solution Discussion 7
Correct Answer: B

Question #199

As part of your organization's zero trust strategy, you use Identity-Aware Proxy (IAP) to protect multiple applications. You need to ingest logs into a Security Information and Event Management (SIEM) system so that you are alerted to possible intrusions.
Which logs should you analyze?

A. Data Access audit logs
B. Policy Denied audit logs
C. Cloud Identity user log events
D. Admin Activity audit logs

Hide Solution Discussion 8
Correct Answer: A

Question #200

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 poli-cy:constraints/gcp.restrictStorageNonCmekServices
• binding at: org1
• policy type: allow
• policy value: all supported services
B. • organization policy: con-straints/gcp.restrictNonCmekServices
• binding at: org1
• policy type: deny
• policy value: storage.googleapis.com
C. • organization policy: con-straints/gcp.restrictStorageNonCmekServices
• binding at: org1

• policy type: deny
• policy value: storage.googleapis.com

D. • organization policy: con-straints/gcp.restrictNonCmekServices
• binding at: org1
• policy type: allow
• policy value: storage.googleapis.com

Hide Solution Discussion 9
Correct Answer: B

Question #201

Your company's Google Cloud organization has about 200 projects and 1,500 virtual machines. There is no uniform strategy for logs and events management, which reduces visibility for your security operations team. You need to design a logs management solution that provides visibility and allows the security team to view the environment's configuration.
What should you do?

A. 1. Create a dedicated log sink for each project that is in scope.
2. Use a BigQuery dataset with time partitioning enabled as a destination of the log sinks.
3. Deploy alerts based on log metrics in every project.
4. Grant the role "Monitoring Viewer" to the security operations team in each project.

B. 1. Create one log sink at the organization level that includes all the child resources.
2. Use as destination a Pub/Sub topic to ingest the logs into the security information and event. management (SIEM) on-premises, and ensure that the right team can access the SIEM.
3. Grant the Viewer role at organization level to the security operations team.

C. 1. Enable network logs and data access logs for all resources in the "Production" folder.
2. Do not create log sinks to avoid unnecessary costs and latency.
3. Grant the roles "Logs Viewer" and "Browser" at project level to the security operations team.

D. 1. Create one sink for the "Production" folder that includes child resources and one sink for the logs ingested at the organization level that excludes child resources.
2. As destination, use a log bucket with a minimum retention period of 90 days in a project that can be accessed by the security team.
3. Grant the security operations team the role of Security Reviewer at organization level.

Hide Solution Discussion 8
Correct Answer: B

Question #202

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 OPEN_MYSQL_PORT findings. You are enforcing the guardrails and need to prevent these types of common misconfigurations.
What should you do?

A. Create a hierarchical firewall policy configured at the organization to deny all connections from 0.0.0.0/0.

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

C. Create a Google Cloud Armor security policy to deny traffic from 0.0.0.0/0.

D. Create a firewall rule for each virtual private cloud (VPC) to deny traffic from 0.0.0.0/0 with priority 0.

Hide Solution Discussion 16
Correct Answer: B

Question #203

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. Configure log sink to export all logs into a Cloud Storage bucket in europe-west4.

C. Create a new log bucket in europe-west4, and redirect the _Default bucket to the new bucket.

D. Set the logging storage region to europe-west4 by using the gcloud CLI logging settings update.

Reason:

- ***Log Buckets and Locations:*** *Cloud Logging uses "log buckets" to store log data. By default, a project has a "_Default" log bucket. You can create new log buckets in specific regions to control where your log data is stored.*

- ***Data Residency:*** *To comply with data residency regulations, you need to ensure that the log bucket storing your data is located in Europe. Creating a new log bucket in europe-west4 (Netherlands) achieves this.*

- ***Redirecting the _Default Bucket:*** *By redirecting the _Default bucket to your new Europe-based bucket, you ensure that all logs generated by resources in your project are automatically routed to the compliant location.*

Why other options are not as effective:

- ***A. gcp.resourceLocations organization policy:*** *This policy restricts the creation of resources to specific regions, but it doesn't change the location of existing resources or redirect log flows.*
- ***B. Log sink to Cloud Storage:*** *While exporting logs to Cloud Storage can be useful for long-term storage and analysis, it doesn't directly address the requirement of keeping logs within Europe for compliance. You would still need to ensure the Cloud Storage bucket is in the appropriate location.*
- ***D. gcloud CLI logging settings update:*** *This command is used to configure logging settings at the project level, but it doesn't allow you to change the storage location of the _Default log bucket.*

In summary: *Creating a new log bucket in the desired European region and redirecting the _Default bucket to it is the most direct and effective way to ensure that your logging data remains within Europe for compliance purposes.***

Hide Solution Discussion 21

Correct Answer: C

Question #204

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

Hide Solution Discussion 4
Correct Answer: A

Question #205

You are running applications outside Google Cloud that need access to Google Cloud resources. You are using workload identity federation to grant external identities Identity and Access Management (IAM) roles to eliminate the maintenance and security burden associated with service account keys. You must protect against attempts to spoof another user's identity and gain unauthorized access to Google Cloud resources.
What should you do? (Choose two.)

A. Enable data access logs for IAM APIs.
B. Limit the number of external identities that can impersonate a service account.
C. Use a dedicated project to manage workload identity pools and providers.
D. Use immutable attributes in attribute mappings.
E. Limit the resources that a service account can access.

Hide Solution Discussion 7
Correct Answer: CD

Question #206

You manage a BigQuery analytical data warehouse in your organization. You want to keep data for all your customers in a common table while you also restrict query access based on rows and columns permissions. Non-query operations should not be supported.
What should you do? (Choose two.)

A. Create row-level access policies to restrict the result data when you run queries with the filter expression set to TRUE.
B. Configure column-level encryption by using Authenticated Encryption with Associated Data (AEAD) functions with Cloud Key Management Service (KMS) to control access to columns at query runtime.
C. Create row-level access policies to restrict the result data when you run queries with the filter expression set to FALSE.
D. Configure dynamic data masking rules to control access to columns at query runtime.

E. Create column-level policy tags to control access to columns at query runtime.

Hide Solution Discussion 8
Correct Answer: CE

Question #207

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, constraints/ compute.vmExternalIpAccess, 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 two.)

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

Hide Solution Discussion 6
Correct Answer: BC

Question #208

Your organization recently activated the Security Command Center (SCC) 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 all Users from the buckets.
   2. Apply the organization policy storage.uniformBucketLevelAccess to prevent regressions.
   3. Query the data access logs to report on unauthorized access.
B. 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.
C. 1. Change the bucket permissions to limit access.
   2. Query the bucket's usage logs to report on unauthorized access to the data.
   3. Enforce the organization policy storage.publicAccessPrevention to avoid regressions.
D. 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.

Hide Solution Discussion 5
Correct Answer: C

Question #209

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 two.)

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

Hide Solution Discussion 16
Correct Answer: BE

Question #210

Your company uses Google Cloud and has publicly exposed network assets. You want to discover the assets and perform a security audit on these assets by using a software tool in the least amount of time.
What should you do?

A. Run a platform security scanner on all instances in the organization.
B. Identify all external assets by using Cloud Asset Inventory, and then run a network security scanner against them.
C. Contact a Google approved security vendor to perform the audit.
D. Notify Google about the pending audit, and wait for confirmation before performing the scan.

Hide Solution Discussion 6
Correct Answer: B

Question #211

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

A. Limit the physical location of a new resource with the Organization Policy Service "resource locations constraint."
B. Use Cloud IDS to get east-west and north-south traffic visibility in the EU to monitor intra-VPC and inter-VPC communication.

C. Limit Google personnel access based on predefined attributes such as their citizenship or geographic location by using Key Access Justifications.

D. Use identity federation to limit access to Google Cloud resources from non-EU entities.

E. Use VPC Flow Logs to monitor intra-VPC and inter-VPC traffic in the EU.

Hide Solution Discussion 10
Correct Answer: AC

Question #212

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 to 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.

Hide Solution Discussion 8
Correct Answer: B

Question #213

Your organization is using GitHub Actions as a continuous integration and delivery (CI/CD) platform. You must enable access to Google Cloud resources from the CI/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.

Hide Solution Discussion 4
Correct Answer: D

Question #214

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.

Hide Solution Discussion 4
Correct Answer: B

Question #215

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.

Hide Solution Discussion 19
Correct Answer: A

Question #216

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.

Hide Solution Discussion 8
Correct Answer: B

Question #217

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.

Hide Solution Discussion 9
Correct Answer: D

Question #218

Your organization uses Google Workspace Enterprise Edition for 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 authenticator.
D. Set the session length timeout for Google Cloud services to a shorter duration.

Hide Solution Discussion 5
Correct Answer: D

Question #219

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 two.)

A. Customer-managed encryption keys
B. Customer-Supplied Encryption Keys
C. Key Access Justifications

D. Access Transparency and Approval

E. Cloud External Key Manager

Hide Solution Discussion 10
Correct Answer: CE

Question #220

You manage one of your organization's Google Cloud projects (Project A). A VPC 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.

Hide Solution Discussion 15
Correct Answer: A

Question #221

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. A 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.

Hide Solution Discussion 21
Correct Answer: C

Question #222

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 same 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.

Hide Solution Discussion 5
Correct Answer: A

Question #223

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 for 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.

Hide Solution Discussion 15
Correct Answer: B

Question #224

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.

Hide Solution Discussion 6
Correct Answer: C

Question #225

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.

Hide Solution Discussion 4
Correct Answer: D

Question #226

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 (SCC) 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.

Hide Solution Discussion 6
Correct Answer: C

Question #227

You are migrating your users to Google Cloud. There are cookie replay attacks with Google web and Google Cloud CLI SDK sessions on endpoint devices. You need to reduce the risk of these threats. What should you do? (Choose two.)

A. Configure Google session control to a shorter duration.
B. Set an organizational policy for OAuth 2.0 access token with a shorter duration.
C. Set a reauthentication policy for Google Cloud services to a shorter duration.
D. Configure a third-party identity provider with session management.
E. Enforce Security Key Authentication with 2SV.

Hide Solution Discussion 13
Correct Answer: AE

Question #228

You manage a mission-critical workload for your organization, which is in a highly regulated industry. The workload uses Compute Engine VMs to analyze and process the sensitive data after it is uploaded to Cloud Storage from the endpoint computers. Your compliance team has detected that this workload does not meet the data protection requirements for sensitive data. You need to meet these requirements:
• Manage the data encryption key (DEK) outside the Google Cloud boundary.
• Maintain full control of encryption keys through a third-party provider.
• Encrypt the sensitive data before uploading it to Cloud Storage.
• Decrypt the sensitive data during processing in the Compute Engine VMs.
• Encrypt the sensitive data in memory while in use in the Compute Engine VMs.
What should you do? (Choose two.)

A. Configure Customer Managed Encryption Keys to encrypt the sensitive data before it is uploaded to Cloud Storage, and decrypt the sensitive data after it is downloaded into your VMs.
B. Configure Cloud External Key Manager to encrypt the sensitive data before it is uploaded to Cloud Storage, and decrypt the sensitive data after it is downloaded into your VMs.
C. Create Confidential VMs to access the sensitive data.
D. Migrate the Compute Engine VMs to Confidential VMs to access the sensitive data.
E. Create a VPC Service Controls service perimeter across your existing Compute Engine VMs and Cloud Storage buckets.

Hide Solution Discussion 21
Correct Answer: BC

Question #229

Your organization wants to be General Data Protection Regulation (GDPR) compliant. You want to ensure that your DevOps teams can only create Google Cloud resources in the Europe regions. What should you do?

A. Use Identity-Aware Proxy (IAP) with Access Context Manager to restrict the location of Google Cloud resources.

B. Use the org policy constraint 'Google Cloud Platform – Resource Location Restriction' on your Google Cloud organization node.

C. Use the org policy constraint 'Restrict Resource Service Usage' on your Google Cloud organization node.

D. Use Identity and Access Management (IAM) custom roles to ensure that your DevOps team can only create resources in the Europe regions.

Hide Solution Discussion 10
Correct Answer: B

Question #230

For data residency requirements, you want your secrets in Google Clouds Secret Manager to only have payloads in europe-west1 and europe-west4. Your secrets must be highly available in both regions.
What should you do?

A. Create your secret with a user managed replication policy, and choose only compliant locations.

B. Create your secret with an automatic replication policy, and choose only compliant locations.

C. Create two secrets by using Terraform, one in europe-west1 and the other in europe-west4.

D. Create your secret with an automatic replication policy, and create an organizational policy to deny secret creation in non-compliant locations.

Hide Solution Discussion 7
Correct Answer: A

Question #231

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

A. Encrypt the data in the Cloud Storage bucket by using Customer Managed Encryption Keys. Configure an IAM deny policy for unauthorized groups.

B. Generate a key in your on-premises environment to encrypt the data before you upload the data to the Cloud Storage bucket. Upload the key to the Cloud Key Management Service (KMS). Activate Key Access Justifications (KAJ) and have the external key system reject unauthorized accesses.

C. Encrypt the data in the Cloud Storage bucket by using Customer Managed Encryption Keys backed by a Cloud Hardware Security Module (HSM). Enable data access logs.

D. Generate a key in your on-premises environment and store it in a Hardware Security Module (HSM) that is managed on-premises. Use this key as an external key in the Cloud Key Management Service (KMS). Activate Key Access Justifications (KAJ) and set the external key system to reject unauthorized accesses.

Hide Solution Discussion 7
Correct Answer: D

Question #232

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 for the developers and security team while you ensure least privilege.
What should you do?

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

Hide Solution Discussion 3
Correct Answer: A

Question #233

You manage a fleet of virtual machines (VMs) in your organization. You have encountered issues with lack of patching in many VMs. You need to automate regular patching in your VMs and view the patch management data across multiple projects.
What should you do? (Choose two.)

A. View patch management data in VM Manager by using OS patch management.
B. View patch management data in Artifact Registry.
C. View patch management data in a Security Command Center dashboard.
D. Deploy patches with Security Command Genter by using Rapid Vulnerability Detection.
E. Deploy patches with VM Manager by using OS patch management.

Hide Solution Discussion 9
Correct Answer: CE

Community vote distribution

Question #234

Your organization uses BigQuery to process highly sensitive, structured datasets. Following the "need to know" principle, you need to create the Identity and Access Management (IAM) design to meet the needs of these users:
• Business user: must access curated reports.
• Data engineer: must administrate the data lifecycle in the platform.
• Security operator: must review user activity on the data platform.

What should you do?

A. Configure data access log for BigQuery services, and grant Project Viewer role to security operator.
B. Set row-based access control based on the “region” column, and filter the record from the United States for data engineers.
C. Create curated tables in a separate dataset and assign the role roles/bigquery.dataViewer.
D. Generate a CSV data file based on the business user's needs, and send the data to their email addresses.

Hide Solution Discussion 8
Correct Answer: C

Question #235

You are setting up a new Cloud Storage bucket in your environment that is encrypted with a customer managed encryption key (CMEK). The CMEK is stored in Cloud Key Management Service (KMS), in project “prj-a”, and the Cloud Storage bucket will use project “prj-b”. The key is backed by a Cloud Hardware Security Module (HSM) and resides in the region europe-west3. Your storage bucket will be located in the region europe-west1. When you create the bucket, you cannot access the key, and you need to troubleshoot why.
What has caused the access issue?

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

Reason:

- ***Option D (Correct)**: **Cloud Key Management Service (KMS) keys**, including those backed by a **Cloud Hardware Security Module (HSM)**, must reside in the same region as the Google Cloud resource that uses them, in this case, the Cloud Storage bucket. The key is located in **europe-west3**, while the storage bucket is in **europe-west1**. Since they are in different regions, Cloud Storage cannot access the CMEK, causing the access issue.*
- ***Option A (Incorrect)**: **Firewall rules** in Google Cloud do not apply to Cloud KMS or Cloud Storage interactions. Cloud KMS keys are managed within Google Cloud, and access to them is controlled by IAM policies, not firewall rules.*
- ***Option B (Incorrect)**: **Cloud HSM** does support **Cloud Storage** when used with **CMEK**. Cloud HSM is a secure method to manage encryption keys, but the issue in this scenario is not about support but about the key and bucket being in different regions.*
- ***Option C (Incorrect)**: While the CMEK is in a different project (project "prj-a") than the Cloud Storage bucket (project "prj-b"), Google Cloud supports cross-project use of keys as long as the appropriate IAM permissions are granted. This would not cause an access issue if permissions were configured correctly.*

Summary:

*The access issue is caused by the **CMEK and Cloud Storage bucket being in different regions** (Option D). To resolve this, either move the key to the same region as the bucket or create a bucket in the same region as the key (both should be in **europe-west1** or **europe-west3**).*

Hide Solution Discussion 8
Correct Answer: D

Question #236

You are deploying regulated workloads on Google Cloud. The regulation has data residency and data access requirements. It also requires that support is provided from the same geographical location as where the data resides.
What should you do?

A. Enable Access Transparency Logging.
B. Deploy Assured Workloads.
C. Deploy resources only to regions permitted by data residency requirements.
D. Use Data Access logging and Access Transparency logging to confirm that no users are accessing data from another region.

Hide Solution Discussion 4
Correct Answer: B

Question #237

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

A. Use customer-supplied encryption keys (CSEK) with keys generated on trusted external systems. Provide the raw CSEK as part of the API call.
B. Create a KMS key that is stored on a Google managed FIPS 140-2 level 3 Hardware Security Module (HSM). Manage the Identity and Access Management (IAM) permissions settings, and set up the key rotation period.
C. Use Cloud External Key Management (EKM) that integrates with an external Hardware Security Module (HSM) system from supported vendors.
D. Create a Cloud Key Management Service (KMS) key with imported key material. Wrap the key for protection during import. Import the key generated on a trusted system in Cloud KMS.

Hide Solution Discussion 6
Correct Answer: C

Question #238

Your company is concerned about unauthorized parties gaining access to the Google Cloud environment by using a fake login page. You must implement a solution to protect against person-in-the-middle attacks.
Which security measure should you use?

A. Security key
B. Google prompt

C. Text message or phone call code

D. Google Authenticator application

Hide Solution Discussion 5

Correct Answer: A

Question #239

You control network traffic for a folder in your Google Cloud environment. Your folder includes multiple projects and Virtual Private Cloud (VPC) networks. You want to enforce on the folder level that egress connections are limited only to IP range 10.58.5.0/24 and only from the VPC network "dev-vpc". You want to minimize implementation and maintenance effort.
What should you do?

A. 1. Leave the network configuration of the VMs in scope unchanged.
2. Create a new project including a new VPC network "new-vpc".
3. Deploy a network appliance in "new-vpc" to filter access requests and only allow egress connections from "dev-vpc" to 10.58.5.0/24.

B. 1. Leave the network configuration of the VMs in scope unchanged.
2. Enable Cloud NAT for "dev-vpc" and restrict the target range in Cloud NAT to 10.58.5.0/24.

C. 1. Attach external IP addresses to the VMs in scope.
2. Define and apply a hierarchical firewall policy on folder level to deny all egress connections and to allow egress to IP range 10.58.5.0/24 from network dev-vpc.

D. 1. Attach external IP addresses to the VMs in scope.
2. Configure a VPC Firewall rule in "dev-vpc" that allows egress connectivity to IP range 10.58.5.0/24 for all source addresses in this network.

Reason:

- ***Hierarchical Firewall Policies:*** *These policies allow you to define firewall rules at the folder level, which are then automatically inherited by all projects and VPC networks within that folder. This centralized control ensures consistent enforcement of your egress traffic restrictions across the entire environment.*

- ***Least Privilege:*** *By default, the hierarchical firewall policy denies all egress connections. You then create a specific allow rule for traffic originating from the "dev-vpc" network and destined for the 10.58.5.0/24 IP range. This least privilege approach enhances security by blocking all other egress traffic.*

- ***Reduced Management Overhead:*** *You don't need to configure individual firewall rules for each VPC network or VM. This significantly simplifies implementation and maintenance, especially in a dynamic environment with multiple projects and networks.*

- ***Flexibility:*** *You can easily update the hierarchical firewall policy at the folder level to modify the egress restrictions as your requirements change.*

Why other options are not as suitable:

- ***A. Network appliance:*** *Deploying a network appliance adds complexity and operational overhead. It also introduces a potential single point of failure.*
- ***B. Cloud NAT:*** *Cloud NAT is primarily used to provide internet access to VMs in private subnets. While you can restrict the target IP range with Cloud NAT, it's not the most efficient or direct way to achieve your goal.*
- ***D. VPC Firewall rule:*** *Configuring VPC Firewall rules individually for each network is less efficient and doesn't provide the centralized control and ease of management that hierarchical firewall policies offer.*

By using hierarchical firewall policies, you can effectively and efficiently enforce your egress traffic restrictions at the folder level, minimizing effort and maximizing security.

Hide Solution Discussion 11
Correct Answer: B

Question #240

Your customer has an on-premises Public Key Infrastructure (PKI) with a certificate authority (CA). You need to issue certificates for many HTTP load balancer frontends. The on-premises PKI should be minimally affected due to many manual processes, and the solution needs to scale.
What should you do?

A. Use Certificate Manager to issue Google managed public certificates and configure it at HTTP the load balancers in your infrastructure as code (IaC).
B. Use a subordinate CA in the Google Certificate Authority Service from the on-premises PKI system to issue certificates for the load balancers.
C. Use Certificate Manager to import certificates issued from on-premises PKI and for the frontends. Leverage the gcloud tool for importing.
D. Use the web applications with PKCS12 certificates issued from subordinate CA based on OpenSSL on-premises. Use the gcloud tool for importing. Use the External TCP/UDP Network load balancer instead of an external HTTP Load Balancer.

Hide Solution Discussion 5
Correct Answer: B

Community vote distribution
B (78%)
C (22%)

Question #241

You are developing a new application that uses exclusively Compute Engine VMs. Once a day, this application will execute five different batch jobs. Each of the batch jobs requires a dedicated set of permissions on Google Cloud resources outside of your application. You need to design a secure access concept for the batch jobs that adheres to the least-privilege principle.
What should you do?

A. 1. Create a general service account “g-sa” to orchestrate the batch jobs.
2. Create one service account per batch job ‘b-sa-[1-5]’. Grant only the permissions required to run the individual batch jobs to the service accounts and generate service account keys for each of these service accounts.

3. Store the service account keys in Secret Manager. Grant g-sa access to Secret Manager and run the batch jobs with the permissions of b-sa-[1-5].

B. 1. Create a general service account “g-sa” to execute the batch jobs.
2. Grant the permissions required to execute the batch jobs to g-sa.
3. Execute the batch jobs with the permissions granted to g-sa.

C. 1. Create a workload identity pool and configure workload identity pool providers for each batch job.
2. Assign the workload identity user role to each of the identities configured in the providers.
3. Create one service account per batch job “b-sa-[1-5]”, and grant only the permissions required to run the individual batch jobs to the service accounts.
4. Generate credential configuration files for each of the providers. Use these files to execute the batch jobs with the permissions of b-sa-[1-5].

D. 1. Create a general service account “g-sa” to orchestrate the batch jobs.
2. Create one service account per batch job “b-sa-[1-5]”, and grant only the permissions required to run the individual batch jobs to the service accounts.
3. Grant the Service Account Token Creator role to g-sa. Use g-sa to obtain short-lived access tokens for b-sa-[1-5] and to execute the batch jobs with the permissions of b-sa-[1-5].

Hide Solution Discussion 4
Correct Answer: D

Question #242

Your Google Cloud environment has one organization node, one folder named “Apps”, and several projects within that folder. The organizational node enforces the constraints/iam.allowedPolicyMemberDomains organization policy, which allows members from the terramearth.com organization. The “Apps” folder enforces the constraints/iam.allowedPolicyMemberDomains organization policy, which allows members from the flowlogistic.com organization. It also has the inheritFromParent: false property. You attempt to grant access to a project in the “Apps” folder to the user testuser@terramearth.com.
What is the result of your action and why?

A. The action succeeds because members from both organizations, terramearth.com or flowlogistic.com, are allowed on projects in the “Apps” folder.

B. The action succeeds and the new member is successfully added to the project's Identity and Access Management (IAM) policy because all policies are inherited by underlying folders and projects.

C. The action fails because a constraints/iam.allowedPolicyMemberDomains organization policy must be defined on the current project to deactivate the constraint temporarily.

D. The action fails because a constraints/iam.allowedPolicyMemberDomains organization policy is in place and only members from the flowlogistic.com organization are allowed.

Hide Solution Discussion 4
Correct Answer: D

Question #243

An administrative application is running on a virtual machine (VM) in a managed group at port 5601 inside a Virtual Private Cloud (VPC) instance without access to the internet currently. You want to

expose the web interface at port 5601 to users and enforce authentication and authorization Google credentials.
What should you do?

A. Configure the bastion host with OS Login enabled and allow connection to port 5601 at VPC firewall. Log in to the bastion host from the Google Cloud console by using SSH-in-browser and then to the web application.
B. Modify the VPC routing with the default route point to the default internet gateway. Modify the VPC Firewall rule to allow access from the internet 0.0.0.0/0 to port 5601 on the application instance.
C. Configure Secure Shell Access (SSH) bastion host in a public network, and allow only the bastion host to connect to the application on port 5601. Use a bastion host as a jump host to connect to the application.
D. Configure an HTTP Load Balancing instance that points to the managed group with Identity-Aware Proxy (IAP) protection with Google credentials. Modify the VPC firewall to allow access from IAP network range.

Hide Solution Discussion 5
Correct Answer: D

Question #244

Your company's users access data in a BigQuery table. You want to ensure they can only access the data during working hours. What should you do?

A. Assign a BigQuery Data Viewer role along with an IAM condition that limits the access to specified working hours.
B. Run a gsutil script that assigns a BigQuery Data Viewer role, and remove it only during the specified working hours.
C. Assign a BigQuery Data Viewer role to a service account that adds and removes the users daily during the specified working hours.
D. Configure Cloud Scheduler so that it triggers a Cloud Functions instance that modifies the organizational policy constraint for BigQuery during the specified working hours.

Hide Solution Discussion 8
Correct Answer: A

Question #245

You have placed several Compute Engine instances in a private subnet. You want to allow these instances to access Google Cloud services, like Cloud Storage, without traversing the internet. What should you do?

A. Enable Private Google Access for the private subnet.
B. Configure Private Service Connect for the private subnet's Virtual Private Cloud (VPC) and allocate an IP range for the Compute Engine instances.
C. Reserve and assign static external IP addresses for the Compute Engine instances.
D. Create a Cloud NAT gateway for the region where the private subnet is configured.

Hide Solution Discussion 2
Correct Answer: A

Question #246

Your organization relies heavily on Cloud Run for its containerized applications. You utilize Cloud Build for image creation, Artifact Registry for image storage, and Cloud Run for deployment. You must ensure that containers with vulnerabilities rated above a common vulnerability scoring system (CVSS) score of "medium" are not deployed to production. What should you do?

A. Implement vulnerability scanning as part of the Cloud Build process. If any medium or higher vulnerabilities are detected, manually rebuild the image with updated components.
B. Perform manual vulnerability checks post-build, but before Cloud Run deployment. Implement a manual security-engineer-driven remediation process.
C. Configure Binary Authorization on Cloud Run to enforce image signatures. Create policies to allow deployment only for images passing a defined vulnerability threshold.
D. Utilize a vulnerability scanner during the Cloud Build stage and set Artifact Registry permissions to block images containing vulnerabilities above "medium."

Hide Solution Discussion 2
Correct Answer: C

Question #247

You run a web application on top of Cloud Run that is exposed to the internet with an Application Load Balancer. You want to ensure that only privileged users from your organization can access the application. The proposed solution must support browser access with single sign-on. What should you do?

A. Change Cloud Run configuration to require authentication. Assign the role of Cloud Run Invoker to the group of privileged users.
B. Create a group of privileged users in Cloud Identity. Assign the role of Cloud Run User to the group directly on the Cloud Run service.
C. Change the Ingress Control configuration of Cloud Run to internal and create firewall rules to allow only access from known IP addresses.
D. Activate Identity-Aware Proxy (IAP) on the Application Load Balancer backend. Assign the role of IAP-secured Web App User to the group of privileged users.

Hide Solution Discussion 3
Correct Answer: D

Question #248

During a routine security review, your team discovered a suspicious login attempt to impersonate a highly privileged but regularly used service account by an unknown IP address. You need to effectively investigate in order to respond to this potential security incident. What should you do?

A. Enable Cloud Audit Logs for the resources that the service account interacts with. Review the logs for further evidence of unauthorized activity.
B. Review Cloud Audit Logs for activity related to the service account. Focus on the time period of the suspicious login attempt.
C. Run a vulnerability scan to identify potentially exploitable weaknesses in systems that use the service account.
D. Check Event Threat Detection in Security Command Center for any related alerts. Cross-reference your findings with Cloud Audit Logs.

Hide Solution Discussion 3
Correct Answer: D

Question #249

Your organization has an operational image classification model running on a managed AI service on Google Cloud. You are in a configuration review with stakeholders and must describe the security responsibilities for the image classification model. What should you do?

A. Explain that using platform-as-a-service (PaaS) transfers security concerns to Google. Describe the need for strict API usage limits to protect against unexpected usage and billing spikes.
B. Explain the security aspects of the code that transforms user-uploaded images using Google's service. Define Cloud IAM for fine-grained access control within the development team.
C. Explain Google's shared responsibility model. Focus the configuration review on Identity and Access Management (IAM) permissions, secure data upload/download procedures, and monitoring logs for any potential malicious activity.
D. Explain the development of custom network firewalls around the image classification service for deep intrusion detection and prevention. Describe vulnerability scanning tools for known vulnerabilities.

Hide Solution Discussion 2
Correct Answer: C

Question #250

You are managing data in your organization's Cloud Storage buckets and are required to retain objects. To reduce storage costs, you must automatically downgrade the storage class of objects older than 365 days to Coldline storage. What should you do?

A. Use Cloud Asset Inventory to generate a report of the configuration of all storage buckets. Examine the Lifecycle management policy settings and ensure that they are set correctly.
B. Set up a CloudRun Job with Cloud Scheduler to execute a script that searches for and removes flies older than 365 days from your Cloud Storage.
C. Enable the Autoclass feature to manage all aspects of bucket storage classes.
D. Define a lifecycle policy JSON with an action on SetStorageClass to COLDLINE with an age condition of 365 and matchStorageClass STANDARD.

Hide Solution Discussion 3

Correct Answer: D ___

Question #251

Your organization has a centralized identity provider that is used to manage human and machine access. You want to leverage this existing identity management system to enable on-premises applications to access Google Cloud without hard coded credentials. What should you do?

A. Enable Secure Web Proxy. Create a proxy subnet for each region that Secure Web Proxy will be deployed. Deploy an SSL certificate to Certificate Manager. Create a Secure Web Proxy policy and rules that allow access to Google Cloud services.

B. Enable Workforce Identity Federation. Create a workforce identity pool and specify the on-premises identity provider as a workforce identity pool provider. Create an attribute mapping to map the on-premises identity provider token to a Google STS token. Create an IAM binding that binds the required role(s) to the external identity by specifying the project ID, workload identity pool, and attribute that should be matched.

C. Enable Identity-Aware Proxy (IAP). Configure IAP by specifying the groups and service accounts that should have access to the application. Grant these identities the IAP-secured web app user role.

D. Enable Workload Identity Federation. Create a workload identity pool and specify the on-premises identity provider as a workload identity pool provider. Create an attribute mapping to map the on-premises identity provider token to a Google STS token. Create a service account with the necessary permissions for the workload. Grant the external identity the Workload Identity user role on the service account.

Reason:

- ***Workload Identity Federation*** *allows you to securely and scalably integrate your on-premises or external identity providers with Google Cloud without hard-coding credentials into your applications or services. It enables non-Google Cloud workloads to access Google Cloud resources by exchanging tokens from your external identity provider for Google Cloud credentials, using* ***Google's Security Token Service (STS)****.*
- *This solution works well for both* ***human and machine access*** *by using tokens from your existing centralized identity provider. You create a* ***workload identity pool*** *and* ***provider****, which ensures that the system uses your existing identity management to authenticate and authorize access without storing long-lived credentials.*
- ***Attribute mapping*** *ensures that the identity information from your on-premises identity provider is correctly mapped to Google's token system, and the* ***Workload Identity User role*** *on the service account gives the required permissions for the external workload to access Google Cloud resources.*

Why the other options are less ideal:

- ***A. Enable Secure Web Proxy****: Secure Web Proxy provides a way to control access between on-premises applications and the internet, but it is not relevant to identity management and does not solve the problem of avoiding hard-coded credentials.*
- ***B. Enable Workforce Identity Federation****: This option is focused on managing* ***human user identities*** *(employees) rather than* ***workloads*** *or machine access. Workforce Identity Federation allows for external user authentication but does not address machine access, which is critical in this scenario.*

- ***C. Enable Identity-Aware Proxy (IAP)****: IAP is used to secure access to applications running on Google Cloud by enforcing identity-based access controls. However, it is designed for securing web applications and services, not for federating on-premises machine identities to access Google Cloud services.*

*Thus, **Option D** is the correct choice because **Workload Identity Federation** directly addresses the need for enabling **machine and human access** from on-premises to Google Cloud without hard-coded credentials, using your existing centralized identity management system.*

Hide Solution Discussion 4
Correct Answer: D

Question #252

Your organization is migrating a sensitive data processing workflow from on-premises infrastructure to Google Cloud. This workflow involves the collection, storage, and analysis of customer information that includes personally identifiable information (PII). You need to design security measures to mitigate the risk of data exfiltration in this new cloud environment. What should you do?

A. Encrypt all sensitive data in transit and at rest. Establish secure communication channels by using TLS and HTTPS protocols.
B. Implement a Cloud DLP solution to scan and identify sensitive information, and apply redaction or masking techniques to the PII. Integrate VPC SC with your network security controls to block potential data exfiltration attempts.
C. Restrict all outbound network traffic from cloud resources. Implement rigorous access controls and logging for all sensitive data and the systems that process the data.
D. Rely on employee expertise to prevent accidental data exfiltration incidents.

Hide Solution Discussion 2
Correct Answer: B

Community vote distribution
B (100%)

Question #253

Your organization is building a chatbot that is powered by generative AI to deliver automated conversations with internal employees. You must ensure that no data with personally identifiable information (PII) is communicated through the chatbot. What should you do?

A. Encrypt data at rest for both input and output by using Cloud KMS, and apply least privilege access to the encryption keys.
B. Discover and transform PII data in both input and output by using the Cloud Data Loss Prevention (Cloud DLP) API.
C. Prevent PII data exfiltration by using VPC-SC to create a safe scope around your chatbot.
D. Scan both input and output by using data encryption tools from the Google Cloud Marketplace.

Hide Solution Discussion 2
Correct Answer: B

Community vote distribution
B (100%)

Question #254

Your organization has applications that run in multiple clouds. The applications require access to a Google Cloud resource running in your project. You must use short-lived access credentials to maintain security across the clouds. What should you do?

A. Create a managed workload identity. Bind an attested identity to the Compute Engine workload.
B. Create a service account key. Download the key to each application that requires access to the Google Cloud resource.
C. Create a workload identity pool with a workload identity provider for each external cloud. Set up a service account and add an IAM binding for impersonation.
D. Create a VPC firewall rule for ingress traffic with an allowlist of the IP ranges of the external cloud applications.

Reason:

Workload Identity Pool: *This allows you to securely connect your external cloud environments to Google Cloud, enabling them to access resources using short-lived credentials.*

- ***Workload Identity Provider:*** *By creating a workload identity provider for each external cloud, you can integrate them seamlessly with Google Cloud's identity and access management system.*
- ***Service Account:*** *Setting up a service account with the necessary permissions provides a secure way for your external cloud applications to access the Google Cloud resource.*
- ***IAM Binding:*** *Adding an IAM binding for impersonation allows the service account to assume the identity of users or other service accounts within your Google Cloud organization, providing granular control over access.*

Why other options are less suitable:

- ***Create a managed workload identity. Bind an attested identity to the Compute Engine workload:*** *While managed workload identities can be used for certain scenarios, they might not be the most suitable solution for accessing Google Cloud resources from multiple external clouds.*
- ***Create a service account key. Download the key to each application that requires access to the Google Cloud resource:*** *This approach involves sharing the service account key with multiple applications, which can be a security risk.*
- ***Create a VPC firewall rule for ingress traffic with an allowlist of the IP ranges of the external cloud applications:*** *This option focuses on controlling network traffic, but it doesn't address the issue of providing secure access to Google Cloud resources using short-lived credentials.*

In conclusion, using a workload identity pool with a workload identity provider, service account, and IAM binding for impersonation provides the most secure and efficient way for your applications running in multiple clouds to access a Google Cloud resource using short-lived credentials.

Hide Solution Discussion 4
Correct Answer: C

Question #255

Your organization's financial modeling application is already deployed on Google Cloud. The application processes large amounts of sensitive customer financial data. Application code is old and

poorly understood by your current software engineers. Recent threat modeling exercises have highlighted the potential risk of sophisticated side-channel attacks against the application while the application is running. You need to further harden the Google Cloud solution to mitigate the risk of these side-channel attacks, ensuring maximum protection for the confidentiality of financial data during processing, while minimizing application problems. What should you do?

A. Enforce stricter access controls for Compute Engine instances by using service accounts, least privilege IAM policies, and limit network access.
B. Implement a runtime library designed to introduce noise and timing variations into the application's execution which will disrupt side-channel attack.
C. Migrate the application to Confidential VMs to provide hardware-level encryption of memory and protect sensitive data during processing.
D. Utilize customer-managed encryption keys (CMEK) to ensure complete control over the encryption process.

Hide Solution Discussion 1
Correct Answer: C

Community vote distribution
C (100%)

Question #256

Your organization has two VPC Service Controls service perimeters, Perimeter-A and Perimeter-B, in Google Cloud. You want to allow data to be copied from a Cloud Storage bucket in Perimeter-A to another Cloud Storage bucket in Perimeter-B. You must minimize exfiltration risk, only allow required connections, and follow the principle of least privilege. What should you do?

A. Configure a perimeter bridge between Perimeter-A and Perimeter-B, and specify the Cloud Storage buckets as the resources involved.
B. Configure a perimeter bridge between the projects hosting the Cloud Storage buckets in Perimeter-A and Perimeter-B.
C. Configure an egress rule for the Cloud Storage bucket in Perimeter-A and a corresponding ingress rule in Perimeter-B.
D. Configure a bidirectional egress/ingress rule for the Cloud Storage buckets in Perimeter-A and Perimeter-B.

Reason:

Perimeter bridge: *A perimeter bridge allows you to establish a controlled connection between two VPC Service Controls perimeters, enabling data flow between them while maintaining isolation and security.*

- ***Specificity:*** *By specifying the Cloud Storage buckets as the resources involved in the perimeter bridge, you can restrict data flow to only those specific buckets, minimizing the risk of exfiltration.*
- ***Least privilege:*** *Using a perimeter bridge with specific resource definitions adheres to the principle of least privilege, as it allows only the necessary connections between the perimeters.*

Why other options are less suitable:

- ***Configure a perimeter bridge between the projects hosting the Cloud Storage buckets in Perimeter-A and Perimeter-B:*** *This approach would allow for broader data flow between the projects, potentially increasing the risk of exfiltration.*
- ***Configure an egress rule for the Cloud Storage bucket in Perimeter-A and a corresponding ingress rule in Perimeter-B:*** *While this approach can control data flow, it might not provide the same level of security and isolation as a perimeter bridge.*
- ***Configure a bidirectional egress/ingress rule for the Cloud Storage buckets in Perimeter-A and Perimeter-B:*** *This approach might be too broad and could allow for unintended data flow between the perimeters.*

In conclusion, configuring a perimeter bridge between Perimeter-A and Perimeter-B with specific resource definitions provides the most secure and controlled way to allow data to be copied between the Cloud Storage buckets while minimizing exfiltration risk and following the principle of least privilege.

Hide Solution Discussion 3
Correct Answer: A

Question #257

You are running code in Google Kubernetes Engine (GKE) containers in Google Cloud that require access to objects stored in a Cloud Storage bucket. You need to securely grant the Pods access to the bucket while minimizing management overhead. What should you do?

A. Create a service account. Grant bucket access to the Pods by using Workload Identity Federation for GKE.
B. Create a service account with keys. Store the keys in Secret Manager with a 30-day rotation schedule. Reference the keys in the Pods.
C. Create a service account with keys. Store the keys as a Kubernetes secret. Reference the keys in the Pods.
D. Create a service account with keys. Store the keys in Secret Manager. Reference the keys in the Pods.

Hide Solution Discussion 2
Correct Answer: A

Question #258

Your organization is adopting Google Cloud and wants to ensure sensitive resources are only accessible from devices within the internal on-premises corporate network. You must configure Access Context Manager to enforce this requirement. These considerations apply:
• The internal network uses IP ranges 10.100.0.0/16 and 192.168.0.0/16.
• Some employees work remotely but connect securely through a company-managed virtual private network (VPN). The VPN dynamically allocates IP addresses from the pool 172.16.0.0/20.
• Access should be restricted to a specific Google Cloud project that is contained within an existing service perimeter.
What should you do?

A. Create an access level named "Authorized Devices." Utilize the Device Policy attribute to require corporate-managed devices. Apply the access level to the Google Cloud project and instruct all employees to enroll their devices in the organization's management system.
B. Create an access level titled "Internal Network Only." Add a condition with these attributes:

• IP Subnetworks: 10.100.0.0/16, 192.168.0.0/16

• Device Policy: Require OS as Windows or macOS. Apply this access level to the sensitive Google Cloud project.

C. Create an access level titled "Corporate Access." Add a condition with the IP Subnetworks attribute, including the ranges: 10.100.0.0/16, 192.168.0.0/16, 172.16.0.0/20. Assign this access level to a service perimeter encompassing the sensitive project.

D. Create a new IAM role called "InternalAccess. Add the IP ranges 10.100.0.0/16, 192.16.0.0/16, and 172.16.0.0/20 to the role as an IAM condition. Assign this role to IAM groups corresponding to on-premises and VPN users. Grant this role the necessary permissions on the resource within this sensitive Google Cloud project.

Hide Solution Discussion 1
Correct Answer: C

Community vote distribution
C (100%)

Question #259

Your team maintains 1PB of sensitive data within BigQuery that contains personally identifiable information (PII). You need to provide access to this dataset to another team within your organization for analysis purposes. You must share the BigQuery dataset with the other team while protecting the PII. What should you do?

A. Utilize BigQuery's row-level access policies to mask PII columns based on the other team's user identities.

B. Export the BigQuery dataset to Cloud Storage. Create a VPC Service Control perimeter and allow only their team's project access to the bucket.

C. Implement data pseudonymization techniques to replace the PII fields with non-identifiable values. Grant the other team access to the pseudonymized dataset.

D. Create a filtered copy of the dataset and replace the sensitive data with hash values in a separate project. Grant the other team access to this new project.

Reason:

- ***Data pseudonymization:*** *This technique involves replacing PII fields with non-identifiable values, such as random strings or numbers. This effectively masks the sensitive data while preserving the dataset's structure and utility for analysis.*
- ***Data sharing:*** *Granting the other team access to the pseudonymized dataset allows them to perform their analysis without compromising the privacy of the individuals represented in the data.*
- ***Security and compliance:*** *Pseudonymization helps to protect the privacy of individuals and comply with data protection regulations.*

Why other options are less suitable:

- ***Utilize BigQuery's row-level access policies to mask PII columns based on the other team's user identities:*** *While row-level access policies can provide some level of control, they might not be sufficient for protecting PII in all scenarios, especially if the data needs to be shared with multiple users or teams.*

- ***Export the BigQuery dataset to Cloud Storage. Create a VPC Service Control perimeter and allow only their team's project access to the bucket:*** *This approach involves moving the data out of BigQuery, which might introduce additional security risks. Additionally, it might be more complex to manage and control access to the data.*
- ***Create a filtered copy of the dataset and replace the sensitive data with hash values in a separate project. Grant the other team access to this new project:*** *This approach might be inefficient and could introduce additional complexity.*

In conclusion, implementing data pseudonymization techniques and granting the other team access to the pseudonymized dataset provides the most secure and efficient way to share the BigQuery dataset while protecting the PII.

Hide Solution Discussion 1
Correct Answer: C

Question #260

Your organization uses Google Cloud to process large amounts of location data for analysis and visualization. The location data is potentially sensitive. You must design a solution that allows storing and processing the location data securely, minimizing data exposure risks, and adhering to both regulatory guidelines and your organization's internal data residency policies. What should you do?

A. Enable location restrictions on Compute Engine instances and virtual disk resources where the data is handled. Apply labels to tag geographic metadata for all stored data.
B. Use the Cloud Data Loss Prevention (Cloud DLP) API to scan for sensitive location data before any storage or processing. Create Cloud Storage buckets with global availability for optimal performance, relying on Cloud DLP results to filter and control data access.
C. Create regional Cloud Storage buckets with Object Lifecycle Management policies that limit data lifetime. Enable fine-grained access controls by using IAM conditions. Encrypt data with customer-managed encryption keys (CMEK) generated within specific Cloud KMS key locations.
D. Store data within BigQuery in a specified region by using dataset location configuration. Use authorized views and row-level security to enforce geographic access restrictions. Encrypt data within BigQuery tables by using customer-managed encryption keys (CMEK).

Reason:

- ***BigQuery dataset location:*** *Specifying the dataset location ensures that the data is stored within the desired region, adhering to data residency policies.*
- ***Authorized views and row-level security:*** *These features provide granular control over data access, allowing you to restrict access based on geographic location and user roles. This helps to minimize data exposure risks.*
- ***Customer-managed encryption keys (CMEK):*** *Using CMEK gives you control over the encryption keys used to protect the data within BigQuery tables, ensuring that the data is encrypted with keys stored in the desired location.*

Why other options are less suitable:

- ***Enable location restrictions on Compute Engine instances and virtual disk resources where the data is handled. Apply labels to tag geographic metadata for all stored data:*** *While these measures can provide some level of control, they might not be sufficient to ensure compliance with data residency policies and to minimize data exposure risks.*

- ***Use the Cloud Data Loss Prevention (Cloud DLP) API to scan for sensitive location data before any storage or processing. Create Cloud Storage buckets with global availability for optimal performance, relying on Cloud DLP results to filter and control data access:*** *While Cloud DLP can help identify sensitive data, using global Cloud Storage buckets might not be compliant with data residency policies.*
- ***Create regional Cloud Storage buckets with Object Lifecycle Management policies that limit data lifetime. Enable fine-grained access controls by using IAM conditions. Encrypt data with customer-managed encryption keys (CMEK) generated within specific Cloud KMS key locations:*** *This approach provides some level of control, but it might be more complex to manage and maintain compared to using BigQuery with dataset location configuration, authorized views, and row-level security.*

In conclusion, storing location data within BigQuery in a specified region, using authorized views and row-level security, and encrypting data with CMEK provides the most effective and secure solution for processing location data while adhering to regulatory guidelines and data residency policies.

Hide Solution Discussion 1
Correct Answer: D

Community vote distribution
D (100%)

Question #261

Your organization utilizes Cloud Run services within multiple projects underneath the non-production folder which requires primarily internal communication. Some services need external access to approved fully qualified domain names (FQDN) while other external traffic must be blocked. Internal applications must not be exposed. You must achieve this granular control with allowlists overriding broader restrictions only for designated VPCs. What should you do?

A. Implement a global-level allowlist rule for the necessary FQDNs within a hierarchical firewall policy. Apply this policy across all VPCs in the organization and configure Cloud NAT without any additional filtering.
B. Create a folder-level deny-all rule for outbound traffic within a hierarchical firewall policy. Define FQDN allowlist rules in separate policies and associate them with the necessary VPCs. Configure Cloud NAT for these VPCs.
C. Create a project-level deny-all rule within a hierarchical structure and apply it broadly. Override this rule with separate FQDN allowlists defined in VPC-level firewall policies associated with the relevant VPCs.
D. Configure Cloud NAT with IP-based filtering to permit outbound traffic only to the allowlist d FQDNs' IP ranges. Apply Cloud NAT uniformly to all VPCs within the organization's folder structure.

Reason:

Hierarchical firewall policy: *Using a hierarchical firewall policy allows you to establish a baseline of security rules at the folder level and then override them with more granular rules at the VPC level. This provides flexibility and control over network traffic.*

- ***Folder-level deny-all rule:*** *By implementing a deny-all rule at the folder level, you can ensure that all outbound traffic is blocked by default, except for traffic that is explicitly allowed.*

- ***FQDN allowlist rules:*** *Creating separate FQDN allowlist rules for the necessary VPCs allows you to grant specific VPCs access to approved FQDNs while denying access to other external destinations.*
- ***Cloud NAT:*** *Configuring Cloud NAT for the VPCs with FQDN allowlist rules enables these VPCs to access the internet while maintaining control over outbound traffic.*

Why other options are less suitable:

- ***Implement a global-level allowlist rule for the necessary FQDNs within a hierarchical firewall policy. Apply this policy across all VPCs in the organization and configure Cloud NAT without any additional filtering:*** *This option grants access to the specified FQDNs to all VPCs in the organization, which might not be desirable if you need to restrict access to specific VPCs.*
- ***Create a project-level deny-all rule within a hierarchical structure and apply it broadly. Override this rule with separate FQDN allowlists defined in VPC-level firewall policies associated with the relevant VPCs:*** *This option provides some level of control, but it might be more complex to manage and maintain compared to the folder-level approach.*
- ***Configure Cloud NAT with IP-based filtering to permit outbound traffic only to the allowlist d FQDNs' IP ranges. Apply Cloud NAT uniformly to all VPCs within the organization's folder structure:*** *While this option provides some control over outbound traffic, it might be less flexible than using FQDN allowlist rules, especially if the IP ranges of the FQDNs change over time.*

In conclusion, using a hierarchical firewall policy with a folder-level deny-all rule and FQDN allowlist rules at the VPC level provides the most granular and effective control over outbound traffic for Cloud Run services within your organization's folder structure.

Hide Solution Discussion 1
Correct Answer: B

Question #262

Your organization hosts a sensitive web application in Google Cloud. To protect the web application, you've set up a virtual private cloud (VPC) with dedicated subnets for the application's frontend and backend components. You must implement security controls to restrict incoming traffic, protect against web-based attacks, and monitor internal traffic. What should you do?

A. Configure Cloud Firewall to permit allow-listed traffic only, deploy Google Cloud Armor with predefined rules for blocking common web attacks, and deploy Cloud Intrusion Detection System (IDS) to detect internal traffic anomalies.
B. Configure Google Cloud Armor to allow incoming connections, configure DNS Security Extensions (DNSSEC) on Cloud DNS to secure against common web attacks, and deploy Cloud Intrusion Detection System (Cloud IDS) to detect internal traffic anomalies.
C. Configure Cloud Intrusion Detection System (Cloud IDS) to monitor incoming connections, deploy Identity-Aware Proxy (IAP) to block common web attacks, and deploy Google Cloud Armor to detect internal traffic anomalies.
D. Configure Cloud DNS to secure incoming traffic, deploy Cloud Intrusion Detection System (Cloud IDS) to detect common web attacks, and deploy Google Cloud Armor to detect internal traffic anomalies.

Reason:

Configure Cloud Firewall to permit allow-listed traffic only, deploy Google Cloud Armor with predefined rules for blocking common web attacks, and deploy Cloud Intrusion Detection System (Cloud IDS) to detect internal traffic anomalies.

Here's a breakdown of why this is the best choice:

- ***Cloud Firewall:*** *This provides a granular level of control over incoming traffic, allowing you to specify which IP addresses or networks are allowed to access your web application.*
- ***Google Cloud Armor:*** *This service offers predefined rules for blocking common web attacks, such as DDoS attacks and SQL injection. It helps to protect your web application from external threats.*
- ***Cloud Intrusion Detection System (Cloud IDS):*** *This service monitors internal traffic for signs of malicious activity, such as unauthorized access or data exfiltration. It helps to detect and respond to threats within your network.*

Why other options are less suitable:

- ***Configure Google Cloud Armor to allow incoming connections, configure DNS Security Extensions (DNSSEC) on Cloud DNS to secure against common web attacks, and deploy Cloud Intrusion Detection System (Cloud IDS) to detect internal traffic anomalies:*** *While DNSSEC can help protect against DNS attacks, it doesn't provide the same level of control over incoming traffic as Cloud Firewall.*
- ***Configure Cloud Intrusion Detection System (Cloud IDS) to monitor incoming connections, deploy Identity-Aware Proxy (IAP) to block common web attacks, and deploy Google Cloud Armor to detect internal traffic anomalies:*** *While IAP can provide additional security for your web application, it might not be sufficient for controlling incoming traffic and detecting internal threats.*
- ***Configure Cloud DNS to secure incoming traffic, deploy Cloud Intrusion Detection System (Cloud IDS) to detect common web attacks, and deploy Google Cloud Armor to detect internal traffic anomalies:*** *While Cloud DNS can help secure DNS traffic, it doesn't provide the same level of control over incoming traffic as Cloud Firewall.*

In conclusion, configuring Cloud Firewall, Google Cloud Armor, and Cloud IDS provides a comprehensive and effective solution for protecting your sensitive web application in Google Cloud by restricting incoming traffic, blocking common web attacks, and detecting internal traffic anomalies.

Hide Solution Discussion 1
Correct Answer: A

Community vote distribution
A (100%)

Question #263

Your organization relies heavily on virtual machines (VMs) in Compute Engine. Due to team growth and resource demands, VM sprawl is becoming problematic. Maintaining consistent security hardening and timely package updates poses an increasing challenge. You need to centralize VM image management and automate the enforcement of security baselines throughout the virtual machine lifecycle. What should you do?

A. Use VM Manager to automatically distribute and apply patches to YMs across your projects. Integrate VM Manager with hardened, organization-standard VM images stored in a central repository.
B. Configure the sole-tenancy feature in Compute Engine for all projects. Set up custom organization policies in Policy Controller to restrict the operating systems and image sources that teams are allowed to use.
C. Create a Cloud Build trigger to build a pipeline that generates hardened VM images. Run vulnerability scans in the pipeline, and store images with passing scans in a registry. Use instance templates pointing to this registry.

D. Activate Security Command Center Enterprise. Use VM discovery and posture management features to monitor hardening state and trigger automatic responses upon detection of issues.

Reason:

- ***VM Manager*** *provides centralized management of virtual machines (VMs) by automating the distribution of security patches, updates, and configurations across all VMs in your Google Cloud environment. It ensures that VMs stay up-to-date with the latest security hardening and package updates, addressing the challenge of managing VM sprawl.*
- ***Centralized VM image management*** *with* ***organization-standard VM images*** *stored in a central repository ensures consistency in security hardening across all VMs. By using a* ***centralized image repository****, you can maintain a standard image with hardened settings, and distribute it consistently across all new and existing VMs. This setup helps to enforce security baselines and maintain consistency throughout the VM lifecycle.*

Why the other options are less ideal:

- ***B. Sole-tenancy and Policy Controller****: While* ***sole-tenancy*** *can help with physical isolation of workloads, it is not designed to centralize VM image management or automate patching and updates.* ***Policy Controller*** *can enforce some security policies but does not automate security hardening or package updates, which is critical to address VM sprawl.*
- ***C. Cloud Build trigger and vulnerability scans****: This option involves setting up a complex* ***CI/CD pipeline*** *for generating and scanning hardened VM images. While this ensures security before deployment, it doesn't provide an* ***ongoing automated mechanism*** *for patching and updating VMs throughout their lifecycle, which is necessary to prevent security issues post-deployment.*
- ***D. Security Command Center (SCC) Enterprise****: SCC Enterprise provides* ***monitoring and vulnerability detection****, but it does not offer* ***automated patch management*** *or image consistency. It's a great tool for monitoring security posture, but VM sprawl requires proactive* ***image management*** *and* ***automatic updates****, which SCC alone does not provide.*

Thus, ***Option A*** *is the best choice because it provides both centralized VM image management and automated patching, ensuring consistent security baselines and addressing the challenge of VM sprawl effectively.*

Hide Solution Discussion 3
Correct Answer: A

Community vote distribution
A (50%)
C (50%)

Question #264

Customers complain about error messages when they access your organization's website. You suspect that the web application firewall rules configured in Cloud Armor are too strict. You want to collect request logs to investigate what triggered the rules and blocked the traffic. What should you do?

A. Modify the Application Load Balancer backend and increase the tog sample rate to a higher number.
B. Enable logging in the Application Load Balancer backend and set the log level to VERBOSE in the Cloud Armor policy.

C. Change the configuration of suspicious web application firewall rules in the Cloud Armor policy to preview mode.

D. Create a log sink with a filter for togs containing redirected_by_security_policy and set a BigQuery dataset as destination.

Hide Solution Discussion 2
Correct Answer: C

Question #265

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

A. Create a data profile covering all payment relevant data types. Configure Data Discovery and a risk analysis job in Google Cloud Sensitive Data Protection to analyze findings. Gemini

B. Use the Google Cloud Compliance Reports Manager to download the latest version of the PCI DSS report Analyze the report to detect deviations.

C. Create an Assured Workloads folder in your Google Cloud organization. Migrate existing projects into the folder and monitor for deviations in the PCI DSS.

D. Activate Security Command Center Premium. Use the Compliance Monitoring product to filter findings that may not be PCI DSS compliant.

Reason:

- **Security Command Center (SCC) Premium** is designed to help organizations detect and respond to security threats, while also monitoring compliance with industry standards such as **PCI DSS**. The **Compliance Monitoring** feature in SCC Premium allows you to monitor your Google Cloud environment for compliance with PCI DSS and identify deviations at an infrastructure-as-a-service (IaaS) level.
- **SCC Premium** provides **real-time visibility** into your security posture, identifies potential misconfigurations or deviations from compliance standards, and surfaces actionable insights to address these issues. This makes it an ideal tool for preparing for a PCI DSS audit, as it directly addresses the need to detect deviations from PCI DSS compliance.

Why the other options are less ideal:

- **A. Data Discovery in Google Cloud Sensitive Data Protection**: While data discovery can help detect sensitive data types, such as payment data, it does not address the broader infrastructure-level compliance checks required for **PCI DSS**. This approach is more focused on data classification rather than overall compliance monitoring.
- **B. Google Cloud Compliance Reports Manager**: This option allows you to download a **compliance report**, but it does not provide **real-time deviation detection**. It's useful for reviewing Google's compliance with PCI DSS, but it doesn't help you actively monitor your own organization's landing zone for deviations.
- **C. Assured Workloads folder**: Assured Workloads is designed for compliance with regulations such as **FedRAMP** or **CJIS**, not PCI DSS specifically. While it offers tools to help maintain compliance for certain standards, it’s not the best choice for **actively detecting PCI DSS deviations** in an existing infrastructure.

Thus, **Option D** is the best solution as it provides **comprehensive monitoring and compliance insights** to help detect and manage PCI DSS deviations at the infrastructure level within Google Cloud.

Hide Solution Discussion 2
Correct Answer: D

Community vote distribution
D (75%)
A (25%)

Question #266

Your organization is migrating a complex application to Google Cloud. The application has multiple internal components that interact with each other across several Google Cloud projects. Security is a major concern, and you must design an authorization scheme for administrators that aligns with the principles of least privilege and separation of duties. What should you do?

A. Identify the users who will migrate the application, revoke the default user roles and assign the users with purposely created custom roles.
B. Use multiple external identity providers (IdP) configured to use different SAML profiles and federate the IdPs for each application component.
C. Configure multi-factor authentication (MFA) to enforce the use of physical tokens for all users who will migrate the application.
D. No action needed. When a Google Cloud organization is created, the appropriate permissions are automatically assigned to all users in the domain.

Hide Solution Discussion 1
Correct Answer: A

Community vote distribution
A (100%)

Question #267

Your organization operates in a highly regulated industry and needs to implement strict controls around temporary access to sensitive Google Cloud resources. You have been using Access Approval to manage this access, but your compliance team has mandated the use of a custom signing key. Additionally, they require that the key be stored in a hardware security module (HSM) located outside Google Cloud. You need to configure Access Approval to use a custom signing key that meets the compliance requirements. What should you do?

A. Create a new asymmetric signing key in Cloud Key Management System (Cloud KMS) using a supported algorithm and grant the Access Approval service account the IAM signerVerifier role on the key.
B. Export your existing Access Approval signing key as a PEM file. Upload the file to your external HSM and reconfigure Access Approval to use the key from the HSM.
C. Create a signing key in your external HSM. Integrate the HSM with Cloud External Key Manager (Cloud EKM) and make the key available within your project. Configure Access Approval to use this key.

D. Create a new asymmetric signing key in Cloud KMS and configure the key with a rotation period of 30 days. Add the corresponding public key to your external HSM.

Reason:

- ***External HSM:*** *Using an external HSM ensures that the signing key is stored in a highly secure environment outside of Google Cloud, meeting the compliance requirement.*
- ***Cloud EKM integration:*** *Integrating the HSM with Cloud EKM allows you to manage the key within your Google Cloud environment while maintaining control over the key material in the external HSM.*
- ***Custom signing key:*** *Creating a custom signing key in the HSM provides you with full control over the key generation and management process, ensuring that it meets your organization's specific requirements.*
- ***Access Approval configuration:*** *Configuring Access Approval to use the custom signing key from the HSM allows you to maintain the use of Access Approval for managing temporary access while meeting the compliance requirement for using a custom signing key stored in an external HSM.*

Why other options are less suitable:

- ***Create a new asymmetric signing key in Cloud KMS using a supported algorithm and grant the Access Approval service account the IAM signerVerifier role on the key:*** *While this option allows you to create a custom signing key, it doesn't meet the requirement of storing the key in an external HSM.*
- ***Export your existing Access Approval signing key as a PEM file. Upload the file to your external HSM and reconfigure Access Approval to use the key from the HSM:*** *This approach might not be secure, as exporting the key and uploading it to the HSM could expose the key material.*
- ***Create a new asymmetric signing key in Cloud KMS and configure the key with a rotation period of 30 days. Add the corresponding public key to your external HSM:*** *While this option provides a rotation period for the key, it doesn't address the requirement of storing the key in an external HSM.*

In conclusion, integrating a custom signing key from an external HSM with Cloud EKM and configuring Access Approval to use this key provides the most compliant and secure solution for meeting the requirements of your organization while maintaining the use of Access Approval for managing temporary access.

Hide Solution Discussion 1
Correct Answer: C

Community vote distribution
C (100%)

Question #268

Your organization has sensitive data stored in BigQuery and Cloud Storage. You need to design a solution that provides granular and flexible control authorization to read data. What should you do?

A. Deidentify sensitive fields within the dataset by using data leakage protection within the Sensitive Data Protection services.
B. Use Cloud External Key Manager (Cloud EKM) to encrypt the data in BigQuery and Cloud Storage.
C. Grant identity and access management (IAM) roles and permissions to principals.
D. Enable server-side encryption on the data in BigQuery and Cloud Storage.

Hide Solution Discussion 1
Correct Answer: C

Community vote distribution
C (100%)

Question #269

Your organization is using Security Command Center Premium as a central tool to detect and alert on security threats. You also want to alert on suspicious outbound traffic that is targeting domains of known suspicious web services. What should you do?

A. Create a DNS Server Policy in Cloud DNS and turn on logs. Attach this policy to all Virtual Private Cloud networks with internet connectivity.
B. Forward all logs to Chronicle Security Information and Event Management. Create an alert for suspicious egress traffic to the internet.
C. Create a Cloud Intrusion Detection endpoint. Connect this endpoint to all Virtual Private Cloud networks with internet connectivity.
D. Create an egress firewall policy with Threat Intelligence as the destination. Attach this policy to all Virtual Private Cloud networks with internet connectivity.

Reason:

- ***Egress firewall policy:*** *This policy allows you to control outbound traffic from your VPC networks, ensuring that only authorized traffic can leave your environment.*
- ***Threat Intelligence:*** *By setting Threat Intelligence as the destination, you can leverage Google's threat intelligence data to identify and block suspicious outbound traffic targeting known malicious domains.*
- ***Centralized management:*** *Using Security Command Center Premium, you can manage and monitor the egress firewall policy and receive alerts for any suspicious activity.*

Why other options are less suitable:

- ***Create a DNS Server Policy in Cloud DNS and turn on logs. Attach this policy to all Virtual Private Cloud networks with internet connectivity:*** *While DNS logs can provide some insights, they might not be sufficient for detecting all types of suspicious outbound traffic.*
- ***Forward all logs to Chronicle Security Information and Event Management. Create an alert for suspicious egress traffic to the internet:*** *While Chronicle can provide a comprehensive view of your security posture, it might not be the most efficient way to block suspicious outbound traffic in real time.*
- ***Create a Cloud Intrusion Detection endpoint. Connect this endpoint to all Virtual Private Cloud networks with internet connectivity:*** *Cloud Intrusion Detection is primarily designed to detect threats within your network, not to block outbound traffic.*

In conclusion, creating an egress firewall policy with Threat Intelligence as the destination provides the most effective and efficient way to detect and block suspicious outbound traffic targeting known malicious domains, while leveraging Security Command Center Premium for centralized management and monitoring.

Hide Solution Discussion 3
Correct Answer: D

Community vote distribution
B (100%)

Question #270

You work for a healthcare provider that is expanding into the cloud to store and process sensitive patient data. You must ensure the chosen Google Cloud configuration meets these strict regulatory requirements:

• Data must reside within specific geographic regions.

• Certain administrative actions on patient data require explicit approval from designated compliance officers.

• Access to patient data must be auditable.

What should you do?

A. Select a standard Google Cloud region. Restrict access to patient data based on user location and job function by using Access Context Manager. Enable both Cloud Audit Logging and Access Transparency.

B. Deploy an Assured Workloads environment in an approved region. Configure Access Approval for sensitive operations on patient data. Enable both Cloud Audit Logs and Access Transparency.

C. Deploy an Assured Workloads environment in multiple regions for redundancy. Utilize custom IAM roles with granular permissions. Isolate network-level data by using VPC Service Controls.

D. Select multiple standard Google Cloud regions for high availability. Implement Access Control Lists (ACLs) on individual storage objects containing patient data. Enable Cloud Audit Logs.

Reason:

- ***Assured Workloads*** *is designed for organizations with strict regulatory requirements, such as those in the healthcare sector. It allows you to build secure cloud environments while enforcing compliance with regulations such as HIPAA and GDPR. This is crucial for a healthcare provider dealing with sensitive patient data.*
- ***Data residency****: Assured Workloads ensures that your data remains within specified geographic regions, meeting the requirement that data must reside within specific locations.*
- ***Explicit approval for administrative actions****:* ***Access Approval*** *allows designated compliance officers to explicitly approve sensitive administrative actions (such as access to patient data), ensuring the necessary oversight and control over data access.*
- ***Auditable access****:* ***Cloud Audit Logs*** *and* ***Access Transparency*** *provide a detailed audit trail of who accessed patient data and what administrative actions were taken, fulfilling the requirement for* ***auditable access****.*

Why the other options are less ideal:

- ***A. Access Context Manager with a standard Google Cloud region****: This option can restrict access based on user location and job function, but it does not provide the necessary* ***compliance controls*** *for sensitive administrative actions (such as Access Approval) or the stringent guarantees of* ***data residency*** *that Assured Workloads provides.*
- ***C. Assured Workloads in multiple regions with VPC Service Controls****: While Assured Workloads in multiple regions may offer redundancy, it could complicate* ***data residency compliance****, as the requirement is for data to reside in* ***specific geographic regions****, not necessarily multiple regions. Additionally, VPC Service Controls help isolate network-level data but do not address the need for* ***Access Approval*** *for sensitive operations.*
- ***D. Standard regions with Access Control Lists (ACLs)****: This option does not address the specific regulatory needs, such as* ***explicit administrative approval*** *for patient data actions (Access Approval) and* ***geographically enforced data residency****, which are better handled by Assured Workloads.*

Thus, ***Option B*** *provides the most comprehensive solution for meeting the strict regulatory requirements of healthcare data storage and processing on Google Cloud.*

Hide Solution Discussion 1

Correct Answer: B

Community vote distribution
B (100%)

Question #271

You work for a multinational organization that has systems deployed across multiple cloud providers, including Google Cloud. Your organization maintains an extensive on-premises security information and event management (SIEM) system. New security compliance regulations require that relevant Google Cloud logs be integrated seamlessly with the existing SIEM to provide a unified view of security events. You need to implement a solution that exports Google Cloud logs to your on-premises SIEM by using a push-based, near real-time approach. You must prioritize fault tolerance, security, and auto scaling capabilities. In particular, you must ensure that if a log delivery fails, logs are re-sent. What should you do?

A. Create a Pub/Sub topic for log aggregation. Write a custom Python script on a Cloud Function Leverage the Cloud Logging API to periodically pull logs from Google Cloud and forward the logs to the SIEM. Schedule the Cloud Function to run twice per day.
B. Collect all logs into an organization-level aggregated log sink and send the logs to a Pub/Sub topic. Implement a primary Dataflow pipeline that consumes logs from this Pub/Sub topic and delivers the logs to the SIEM. Implement a secondary Dataflow pipeline that replays failed messages.
C. Deploy a Cloud Logging sink with a filter that routes all logs directly to a syslog endpoint. The endpoint is based on a single Compute Engine hosted on Google Cloud that routes all logs to the on-premises SIEM. Implement a Cloud Function that triggers a retry action in case of failure.
D. Utilize custom firewall rules to allow your SIEM to directly query Google Cloud logs. Implement a Cloud Function that notifies the SIEM of a failed delivery and triggers a retry action.

Hide Solution Discussion 1
Correct Answer: B

Community vote distribution
B (100%)

Question #272

You work for a global company. Due to compliance requirements, certain Compute Engine instances that reside within specific projects must be located exclusively in cloud regions within the European Union (EU). You need to ensure that existing non-compliant workloads are remediated and prevent future Compute Engine instances from being launched in restricted regions. What should you do?

A. Use a third-party configuration management tool to monitor the location of Compute Engine instances. Automatically delete or migrate non-compliant instances, including existing deployments.
B. Deploy a Security Command Center source to detect Compute Engine instances created outside the EU. Use a custom remediation function to automatically relocate the instances, run the function once a day.
C. Use organization policy constraints in Resource Manager to enforce allowed regions for Compute Engine instance creation within specific projects.

D. Set an organization policy that denies the creation of Compute Engine instances outside the EU. Apply the policy to the appropriate projects. Identify existing non-compliant instances and migrate the instances to compliant EU regions.

Hide Solution Discussion 1
Correct Answer: D

Community vote distribution
D (100%)

Question #273

You are working with developers to secure custom training jobs running on Vertex AI. For compliance reasons, all supported data types must be encrypted by key materials that reside in the Europe region and are controlled by your organization. The encryption activity must not impact the training operation in Vertex AI. What should you do?

A. Encrypt the code, training data, and metadata with Google default encryption. Use customer-managed encryption keys (CMEK) for the trained models exported to Cloud Storage buckets.
B. Encrypt the code, training data, metadata, and exported trained models with customer-managed encryption keys (CMEK).
C. Encrypt the code, training data, and exported trained models with customer-managed encryption keys (CMEK).
D. Encrypt the code, training data, and metadata with Google default encryption. Implement an organization policy that enforces a constraint to restrict the Cloud KMS location to the Europe region.

Reason:

- *The key requirement here is that all data types, including **code, training data, metadata, and trained models**, must be encrypted by **key materials that reside in the Europe region** and are controlled by your organization. This indicates the need for **customer-managed encryption keys (CMEK)**, which allows your organization to control encryption keys and their location, fulfilling the compliance requirement.*
- ***CMEK** ensures that your organization maintains control over the encryption keys, including where they are stored (in the Europe region), ensuring compliance with geographic regulations.*
- *By encrypting everything (code, data, metadata, and trained models) with **CMEK**, you maintain encryption for all parts of the training job without impacting Vertex AI's operation, as Vertex AI natively supports CMEK for managing encryption without affecting the service's functionality.*

Why the other options are less ideal:

- ***A. Encrypt the code, training data, and metadata with Google default encryption:** While Google default encryption is applied automatically, it does not give your organization direct control over the encryption keys. Additionally, the encryption keys may not necessarily be stored in the Europe region, which could violate the compliance requirement.*
- ***C. Encrypt the code, training data, and exported trained models with CMEK:** This option omits the encryption of **metadata**. Metadata may contain sensitive information, and encrypting it is crucial to meet full compliance requirements.*
- ***D. Encrypt with Google default encryption and enforce KMS location:** Google default encryption does not give you full control over the encryption keys, and simply enforcing a KMS location for future key use would not ensure compliance for all currently active keys or for encryption across all data types.*

*Thus, **Option B** provides the most comprehensive and compliant solution by using **CMEK** for all relevant data types, ensuring encryption is controlled by your organization and resides in the required region.*

Hide Solution Discussion 1
Correct Answer: B

Community vote distribution
B (100%)

Question #274

Your EU-based organization stores both Personally Identifiable Information (PII) and non-PII data in Cloud Storage buckets across multiple Google Cloud regions. EU data privacy laws require that the PII data must not be stored outside of the EU. To help meet this compliance requirement, you want to detect if Cloud Storage buckets outside of the EU contain healthcare data. What should you do?

A. Create a Sensitive Data Protection job. Specify the infoType of data to be detected and run the job across all Google Cloud Storage buckets.
B. Create a log sink with a filter on resourceLocation.currentLocations. Trigger an alert if a log message appears with a non- EUcountry.
C. Activate Security Command Center Premium. Use compliance monitoring to detect resources that do not follow the applicable healthcare regulation.
D. Enforce the gcp.resourceLocations organization policy and add "EU" in a custom rule that only applies on resources with the tag "healthcare".

Reason:

- ***Sensitive Data Protection:** This service is specifically designed to detect sensitive data within Google Cloud storage. It can identify various types of data, including PII and healthcare data.*
- ***InfoType specification:** You can configure the Sensitive Data Protection job to focus on specific infoTypes of data, such as PII or healthcare data. This helps to narrow down the scope of the scan and improve accuracy.*
- ***Comprehensive scanning:** Running the job across all Google Cloud Storage buckets ensures that you capture any potential violations of data privacy laws.*

Why other options are less suitable:

- ***Create a log sink with a filter on resourceLocation.currentLocations. Trigger an alert if a log message appears with a non- EUcountry:** While this approach can help identify resources located outside the EU, it might not be sufficient to detect all instances of PII or healthcare data.*
- ***Activate Security Command Center Premium. Use compliance monitoring to detect resources that do not follow the applicable healthcare regulation:** Security Command Center Premium can provide a comprehensive view of your security posture, but it might not be specifically designed to detect sensitive data within storage buckets.*
- ***Enforce the gcp.resourceLocations organization policy and add "EU" in a custom rule that only applies on resources with the tag "healthcare":** This approach can help restrict the creation of new resources outside the EU, but it doesn't address the issue of existing data that might be stored in non-EU regions.*

In conclusion, using Sensitive Data Protection with infoType specification and comprehensive scanning is the most effective way to detect if Cloud Storage buckets outside the EU contain healthcare data, helping you meet the compliance requirements of EU data privacy laws.

Hide Solution Discussion 1

Correct Answer: A ___

Question #275

Your organization is migrating business critical applications to Google Cloud across multiple projects. You only have the required IAM permission at the Google Cloud organization level. You want to grant project access to support engineers from two partner organizations using their existing identity provider (IdP) credentials. What should you do?

A. Create two single sign-on (SSO) profiles for the internal and partner IdPs by using SSO for Cloud Identity.
B. Create users manually by using the Google Cloud console. Assign the users to groups.
C. Create two workforce identity pools for the partner IdPs.
D. Sync user identities from their existing IdPs to Cloud Identity by using Google Cloud Directory Sync (GCDS).

Reason:

- ***Leveraging Existing Identities:*** *This approach allows support engineers from both partner organizations to access your Google Cloud projects using their existing IdP credentials. This simplifies the onboarding process and avoids the need to create and manage separate Google Cloud identities for them.*

- ***Centralized Control:*** *By creating workforce identity pools and federating them with the partner IdPs, you maintain control over access to your projects. You can define fine-grained access policies based on attributes from the partner IdPs, ensuring that support engineers only have the necessary permissions.*

- ***Scalability:*** *Workforce identity pools are designed to handle a large number of users, making this solution scalable as your needs grow and you potentially add more partner organizations.*

- ***Security:*** *This approach enhances security by leveraging the existing authentication mechanisms of the partner IdPs. You can also enforce multi-factor authentication and other security measures through the partner IdPs.*

Why other options are not as effective:

- ***Option A:*** *SSO profiles for Cloud Identity are primarily used for internal users, not for external partners.*
- ***Option B:*** *Manually creating users is time-consuming and inefficient, especially for a large number of users. It also creates an administrative overhead for managing those accounts.*
- ***Option D:*** *Syncing identities with Cloud Identity using GCDS is not ideal for temporary or external users. It creates unnecessary complexity and potential security risks.*

By creating workforce identity pools fr each partner IdP, you can efficiently grant project access to support engineers while maintaining control, security, and scalability.

Hide Solution Discussion 1
Correct Answer: C ___

Community vote distribution

D (100%)

Question #276

You are creating a secure network architecture. You must fully isolate development and production environments, and prevent any network traffic between the two environments. The network team requires that there is only one central entry point to the cloud network from the on-premises environment. What should you do?

A. Create one Virtual Private Cloud (VPC) network per environment. Add the on-premises entry point to the production VPC. Peer the VPCs with each other and create firewall rules to prevent traffic.
B. Create one shared Virtual Private Cloud (VPC) network and use it as the entry point to the cloud network. Create separate subnets per environment. Create firewall rules to prevent traffic.
C. Create one Virtual Private Cloud (VPC) network per environment. Create a VPC Service Controls perimeter per environment and add one environment VPC to each.
D. Create one Virtual Private Cloud (VPC) network per environment. Create one additional VPC for the entry point to the cloud network. Peer the entry point VPC with the environment VPCs.

Reason:

- ***Create one Virtual Private Cloud (VPC) network per environment. Add the on-premises entry point to the production VPC. Peer the VPCs with each other and create firewall rules to prevent traffic:*** *While this option creates separate environments, it doesn't provide a dedicated entry point and could make it more difficult to manage and secure network traffic.*
- ***Create one shared Virtual Private Cloud (VPC) network and use it as the entry point to the cloud network. Create separate subnets per environment. Create firewall rules to prevent traffic:*** *This option doesn't provide complete isolation between the environments, as they share the same VPC network. It might also be more difficult to manage and secure network traffic with a single VPC.*
- ***Create one Virtual Private Cloud (VPC) network per environment. Create a VPC Service Controls perimeter per environment and add one environment VPC to each:*** *While VPC Service Controls can provide additional security and compliance features, it doesn't address the requirement for a single entry point to the cloud network.*

In conclusion, creating one VPC network per environment and a dedicated entry point VPC provides the best solution for isolating the environments, enforcing a central entry point, and preventing unauthorized network traffic.

Hide Solution Discussion 4
Correct Answer: D

Community vote distribution
D (50%)
C (50%)

Question #277

You work for a large organization that is using Cloud Identity as the identity provider (IdP) on Google Cloud. Your InfoSec team has mandated the enforcement of a strong password with a length between 12 and 16 characters for all users. After configuring this requirement, users are still able to access the

Google Cloud console with passwords that are less than 12 characters. You need to fix this problem within the Admin console. What should you do?

A. Review each user's password configuration and reset existing passwords.
B. Review the organization password management setting and select Enforce password policy at the next sign-in.
C. Review each user's password configuration and select Enforce strong password.
D. Review the organization password management setting and select Enforce strong password.

Reason:

- ***Organization-wide enforcement:*** *By selecting "Enforce strong password" at the organization level, you ensure that the password policy is applied consistently to all users within your organization. This eliminates the need to review and reset individual user passwords.*
- ***Centralized management:*** *Configuring the password policy at the organization level provides a centralized mechanism for managing password requirements. This simplifies administration and ensures that all users are subject to the same rules.*

Why other options are less suitable:

- ***Review each user's password configuration and reset existing passwords:*** *This is a time-consuming and inefficient approach, especially for large organizations with many users.*
- ***Review each user's password configuration and select Enforce strong password:*** *While this approach might work for individual users, it doesn't guarantee that the password policy will be enforced consistently across the entire organization.*
- ***Review the organization password management setting and select Enforce password policy at the next sign-in:*** *This option might delay the enforcement of the password policy, as it requires users to sign in again before the new policy takes effect.*

In conclusion, reviewing the organization password management setting and selecting "Enforce strong password" is the most efficient and effective way to ensure that all users within your organization are subject to the mandated password policy.

Hide Solution Discussion 1
Correct Answer: D

Community vote distribution
D (100%)

Question #278

Your organization is preparing to build business services in Google Cloud for the first time. You must determine where to apply appropriate controls or policies. You must also identify what aspects of your cloud deployment are managed by Google. What should you do?

A. Model your deployment on the Google Enterprise foundations blueprint. Follow the blueprint exactly and rely on the blueprint to maintain the posture necessary for your business.
B. Use the Risk Manager tool in the Risk Protection Program to generate a report on your cloud security posture. Obtain cyber insurance coverage.
C. Subscribe to the Google Cloud release notes to keep up on product updates and when new services are available. Evaluate new services for appropriate use before enabling their API.

D. Study the shared responsibilities model. Depending on your business scenario, you might need to consider your responsibilities based on the location of your business offices, your customers, and your data.

Reason:

- ***Shared responsibilities model:*** *Understanding the shared responsibilities model between your organization and Google Cloud is crucial for determining where to apply controls and policies. This model outlines the responsibilities of each party in terms of security, compliance, and operations.*
- ***Business-specific considerations:*** *The location of your business offices, customers, and data can impact your responsibilities. For example, if your data is subject to specific data privacy regulations in a particular jurisdiction, you may have additional responsibilities to ensure compliance.*
- ***Tailored approach:*** *By studying the shared responsibilities model and considering your business scenario, you can develop a tailored approach to controls and policies that addresses your specific needs and ensures compliance with relevant regulations.*

Why other options are less suitable:

- ***Model your deployment on the Google Enterprise foundations blueprint:*** *While the Google Enterprise foundations blueprint can provide valuable guidance, it's important to understand that it's a general blueprint and may not address all of your specific needs or regulatory requirements.*
- ***Use the Risk Manager tool in the Risk Protection Program to generate a report on your cloud security posture:*** *The Risk Manager tool can be helpful for assessing your cloud security posture, but it doesn't address the fundamental question of where to apply controls and policies.*
- ***Subscribe to the Google Cloud release notes to keep up on product updates and when new services are available:*** *Staying informed about Google Cloud product updates is important, but it doesn't address the issue of where to apply controls and policies.*

In conclusion, studying the shared responsibilities model and considering your business scenario is the best way to determine where to apply appropriate controls and policies in your Google Cloud deployment. This will help you ensure that your deployment is secure, compliant, and aligned with your organization's goals.

Hide Solution Discussion 1
Correct Answer: D

Community vote distribution
D (100%)

Question #279

Your organization operates a hybrid cloud environment and has recently deployed a private Artifact Registry repository in Google Cloud. On-premises developers cannot resolve the Artifact Registry hostname and therefore cannot push or pull artifacts. You've verified the following:

- **Connectivity to Google Cloud is established by Cloud VPN or Cloud Interconnect.**
- **No custom DNS configurations exist on-premises.**
- **There is no route to the internet from the on-premises network.**

You need to identify the cause and enable the developers to push and pull artifacts. What is likely causing the issue and what should you do to fix the issue?

A. On-premises DNS servers lack the necessary records to resolve private Google API domains. Create DNS records for restricted.googleapis.com or private.googleapis.com pointing to Google's published IP ranges.
B. Developers must be granted the artifactregistry.writer IAM role. Grant the relevant developer group this role.
C. Private Google Access is not enabled for the subnet hosting the Artifact Registry. Enable Private Google Access for the appropriate subnet.
D. Artifact Registry requires external HTTP/HTTPS access. Create a new firewall rule allowing ingress traffic on ports 80 and 443 from the developer's IP ranges.

Hide Solution Discussion 4
Correct Answer: A

Community vote distribution
A (100%)

Question #280

Your organization has an application hosted in Cloud Run. You must control access to the application by using Cloud Identity-Aware Proxy (IAP) with these requirements:
• Only users from the AppDev group may have access.
• Access must be restricted to internal network IP addresses.
What should you do?

A. Deploy a VPN gateway and instruct the AppDev group to connect to the company network before accessing the application.
B. Create an access level that includes conditions for internal IP address ranges and AppDev groups. Apply this access level to the application's IAP policy.
C. Configure firewall rules to limit access to IAP based on the AppDev group and source IP addresses.
D. Configure IAP to enforce multi-factor authentication (MFA) for all users and use network intrusion detection systems (NIDS) to block unauthorized access attempts.

Hide Solution Discussion 1
Correct Answer: B

Community vote distribution
B (100%)

Question #281

You just implemented a Secure Web Proxy instance on Google Cloud for your organization. You were able to reach the internet when you tested this configuration on your test instance. However, developers cannot access the allowed URLs on the Secure Web Proxy instance from their Linux instance on Google Cloud. You want to solve this problem with developers. What should you do?

A. Configure a Cloud NAT gateway to enable internet access from the developer instance subnet.
B. Ensure that the developers have restarted their instance and HTTP service is enabled.
C. Ensure that the developers have explicitly configured the proxy address on their instance.

D. Configure a firewall rule to allow HTTP/S from the developer instance.

Hide Solution Discussion 1
Correct Answer: C

Community vote distribution
C (100%)

Question #282

You have just created a new log bucket to replace the _Default log bucket. You want to route all log entries that are currently routed to the _Default log bucket to this new log bucket, in the most efficient manner. What should you do?

A. Create exclusion filters for the _Default sink to prevent it from receiving new logs. Create a user-defined sink, and select the new log bucket as the sink destination.
B. Disable the _Default sink. Create a user-defined sink and select the new log bucket as the sink destination.
C. Create a user-defined sink with inclusion filters copied from the _Default sink. Select the new log bucket as the sink destination.
D. Edit the _Default sink, and select the new log bucket as the sink destination.

Hide Solution Discussion 2
Correct Answer: D

Question #283

Your organization's use of the Google Cloud has grown substantially and there are many different groups using different cloud resources independently. You must identify common misconfigurations and compliance violations across the organization and track findings for remedial action in a dashboard. What should you do?

A. Create a filter set in Cloud Asset Inventory to identify service accounts with high privileges and IAM principals with Gmail domains.
B. Scan and alert vulnerabilities and misconfigurations by using Secure Health Analytics detectors in Security Command Center Premium.
C. Set up filters on Cloud Audit Logs to flag log entries for specific, risky API calls, and display the calls in a Cloud Log Analytics dashboard.
D. Alert and track emerging attacks detected in your environment by using Event Threat Detection detectors.

Hide Solution Discussion 1
Correct Answer: B

Question #284

You are responsible for a set of Cloud Functions running on your organization's Google Cloud environment. During the last annual security review, secrets were identified in environment variables

of some of these Cloud Functions. You must ensure that secrets are identified in a timely manner. What should you do?

A. Implement regular peer reviews to assess the environment variables and identify secrets in your Cloud Functions. Raise a security incident if secrets are discovered.
B. Implement a Cloud Function that scans the environment variables multiple times a day, and creates a finding in Security Command Center if secrets are discovered.
C. Use Sensitive Data Protection to scan the environment variables multiple times per day, and create a finding in Security Command Center if secrets are discovered.
D. Integrate dynamic application security testing into the CI/CD pipeline that scans the application code for the Cloud Functions. Fail the build process if secrets are discovered.

Hide Solution Discussion 2
Correct Answer: C

Reason:

- ***Sensitive Data Protection*** *(part of the* ***Cloud Data Loss Prevention API****) is specifically designed to detect and identify sensitive data such as secrets, API keys, and other personally identifiable information (PII) within Google Cloud resources, including* ***environment variables****. By using Sensitive Data Protection, you can regularly scan the environment variables of your Cloud Functions, ensuring any sensitive data or secrets are detected in a timely manner.*
- *Integration with* ***Security Command Center*** *allows you to create findings and track them centrally, ensuring that any discovery of secrets is visible to security teams and handled as part of your security incident management process.*

Why the other options are less ideal:

- ***A. Peer reviews****: While peer reviews are useful for code and security audits, they are not a scalable or timely solution for continuously identifying secrets in Cloud Function environment variables. This approach could lead to delays in identifying sensitive data.*
- ***B. Custom Cloud Function for scanning****: While feasible, building a custom solution to scan environment variables is more complex and less reliable than using Google Cloud's* ***built-in Sensitive Data Protection****. Also, relying on a Cloud Function for scanning may not provide the same depth of detection.*
- ***D. Dynamic application security testing (DAST)****: DAST is more suited for testing application vulnerabilities during runtime, not for scanning environment variables. Moreover, it wouldn't directly target secrets within environment variables and is not as efficient for ongoing, real-time secret detection.*

Therefore, using ***Sensitive Data Protection*** *to scan environment variables and integrate findings into the* ***Security Command Center*** *ensures timely detection of secrets and provides a robust solution for security compliance.*

Question #285

Your organization 1s developing a new SaaS application on Google Cloud. Stringent compliance standards require visibility into privileged account activity, and potentially unauthorized changes and misconfigurations to the application's infrastructure. You need to monitor administrative actions, log

changes to IAM roles and permissions, and be able to trace potentially unauthorized configuration changes. What should you do?

A. Create log sinks to Cloud Storage for long-term retention. Set up log-based alerts in Cloud Logging based on relevant log types. Enable VPC Flow Logs for network visibility.

B. Deploy Cloud IDS and activate Firewall Rules Logging. Create a custom dashboard in Security Command Center to visualize potential intrusion attempts.

C. Detect sensitive administrative actions by using Cloud Logging with custom filters. Enable VPC Flow Logs with BigQuery exports for rapid analysis of network traffic patterns.

D. Enable Event Threat Detection and Security Health Analytics in Security Command Center. Set up detailed logging for IAM-related activity and relevant project resources by deploying Cloud Audit Logs.

Reason:

- ***Comprehensive Monitoring:*** *Security Command Center with Event Threat Detection and Security Health Analytics provides a holistic view of your security posture. It detects threats in real-time, identifies misconfigurations and vulnerabilities, and provides actionable insights to improve your security.*

- ***Granular Visibility:*** *Cloud Audit Logs capture a wide range of administrative actions, including changes to IAM roles and permissions, network configurations, and access to sensitive data. This gives you a detailed audit trail to track potentially unauthorized changes.*

- ***Tracing Configuration Changes:*** *By combining Security Command Center's threat detection capabilities with the detailed audit logs, you can effectively trace the origin and impact of configuration changes, helping you identify the root cause of any security issues.*

- ***Compliance:*** *This approach helps you meet compliance requirements by providing evidence of your security monitoring and auditing practices.*

Why other options are less comprehensive:

- ***Option 1:*** *While log sinks and alerts are useful, they don't provide the same level of threat detection and analysis as Security Command Center. VPC Flow Logs are helpful for network visibility but don't capture all administrative actions.*
- ***Option 2:*** *Cloud IDS and Firewall Rules Logging are important for network security, but they don't provide complete visibility into IAM changes and misconfigurations.*
- ***Option 3:*** *While Cloud Logging with custom filters can detect sensitive actions, it lacks the advanced threat detection and analysis capabilities of Security Command Center. VPC Flow Logs with BigQuery exports are useful for analyzing network traffic but don't cover all aspects of configuration changes.*

By enabling Security Command Center's threat detection and Security Health Analytics and deploying Cloud Audit Logs, you can achieve comprehensive monitoring, granular visibility, and effective tracing of configuration changes, ensuring the security and compliance of your SaaS application.

Hide Solution Discussion 1
Correct Answer: D

Question #286

Your application development team is releasing a new critical feature. To complete their final testing, they requested 10 thousand real transaction records. The new feature includes format checking on the primary account number (PAN) of a credit card. You must support the request and minimize the risk of unintended personally identifiable information (PII) exposure. What should you do?

A. Run the new application by using Confidential Computing to ensure PII and card PAN is encrypted in use.

B. Scan and redact PII from the records by using the Cloud Data Loss Prevention API. Perform format-preserving encryption on the card PAN.

C. Encrypt the records by using Cloud Key Management Service to protect the PII and card PAN.

D. Build a tool to replace the card PAN and PII fields with randomly generated values.

Hide Solution Discussion 3
Correct Answer: B

Reason:

- ***Cloud Data Loss Prevention (DLP) API*** *is specifically designed to identify and protect sensitive data, such as* ***personally identifiable information (PII)*** *and* ***credit card numbers (PANs)****. By using the DLP API, you can scan the transaction records, detect sensitive data, and* ***redact or mask*** *the PII to minimize the risk of exposure.*
- ***Format-preserving encryption (FPE)*** *allows you to encrypt the PAN while maintaining its original format, enabling your team to perform format checks without exposing real credit card data. This approach ensures that sensitive information is protected while still allowing the application development team to test the feature.*

Why the other options are less ideal:

- ***A. Confidential Computing****: While Confidential Computing ensures data is encrypted during use (in memory), it doesn't address the need for* ***redaction*** *or* ***masking*** *of PII before sharing the records with the development team. Confidential Computing is more useful in production environments.*
- ***C. Encrypt the records using Cloud Key Management Service (KMS)****: Encrypting the entire record with KMS protects the data but doesn't allow the development team to perform format checking on the PAN. It also doesn't provide the fine-grained control over PII that redaction or masking would.*
- ***D. Build a tool to replace the PAN and PII with random values****: This custom solution could work, but it's a more manual, complex, and error-prone approach compared to using the* ***DLP API****, which is specifically built for detecting and protecting sensitive data.*

Thus, ***using the DLP API to scan and redact PII, combined with format-preserving encryption for the PAN****, is the most secure and practical way to support the testing request while minimizing the risk of exposing sensitive information.*

Question #287

You work for a banking organization. You are migrating sensitive customer data to Google Cloud that is currently encrypted at rest while on-premises. There are strict regulatory requirements when moving sensitive data to the cloud. Independent of the cloud service provider, you must be able to audit key usage and be able to deny certain types of decrypt requests. You must choose an encryption strategy that will ensure robust security and compliance with the regulations. What should you do?

A. Utilize Google default encryption and Cloud IAM to keep the keys within your organization's control.

B. Implement Cloud External Key Manager (Cloud EKM) with Access Approval, to integrate with your existing on-premises key management solution.

C. Implement Cloud External Key Manager (Cloud EKM) with Key Access Justifications to integrate with your existing one premises key management solution.

D. Utilize customer-managed encryption keys (CMEK) created in a dedicated Google Compute Engine instance with Confidential Compute encryption, under your organization's control.

Hide Solution Discussion 1
Correct Answer: C

Community vote distribution
B (100%)

Reference:

Here's a breakdown of why this is the best choice:

Cloud EKM with Key Access Justifications:

- ***Integration with existing on-premises key management:*** *This option allows you to maintain control over your encryption keys by keeping them within your organization's on-premises key management system.*
- ***Key Access Justifications:*** *This feature provides a robust audit trail, allowing you to track who accessed the keys, when, and for what purpose. This helps ensure compliance with regulations and provides visibility into key usage.*
- ***Denial of decrypt requests:*** *You can configure Key Access Justifications to deny certain types of decrypt requests based on specific criteria, such as user identity, time of day, or location. This helps protect sensitive data from unauthorized access.*

Why other options are less suitable:

- ***Utilize Google default encryption and Cloud IAM:*** *While this option provides some level of control, it doesn't offer the same level of flexibility and auditability as Cloud EKM with Key Access Justifications.*
- ***Implement Cloud External Key Manager (Cloud EKM) with Access Approval:*** *Access Approval is a feature that allows you to require additional approvals for certain actions, but it doesn't provide the same level of control over key usage and auditability as Key Access Justifications.*
- ***Utilize customer-managed encryption keys (CMEK) created in a dedicated Google Compute Engine instance with Confidential Compute encryption:*** *This option provides a high level of security, but it requires managing the encryption keys within a Google Cloud environment, which might not be compliant with your organization's security policies.*

In conclusion, Cloud EKM with Key Access Justifications offers the best combination of security, control, and compliance for migrating sensitive data to Google Cloud while meeting strict regulatory requirements.

Question #288

Your organization is developing an application that will have both corporate and public end-users. You want to centrally manage those customers' identities and authorizations. Corporate end users must access the application by using their corporate user and domain name. What should you do?

A. Add the corporate and public end-user domains to domain restricted sharing on the organization.

B. Federate the customers' identity provider (IdP) with Workforce Identity Federation in your application's project.

C. Do nothing. Google Workspace identities will allow you to filter personal accounts and disable their access.

D. Use a customer identity and access management tool (CIAM) like Identity Platform.

Reason:

- ***Purpose-built for customer identity management:*** *CIAM solutions like Identity Platform are specifically designed to handle the complexities of managing customer identities, including authentication, authorization, and user lifecycle management.*
- ***Scalability and performance:*** *Identity Platform can handle a large number of users and provide a seamless experience for both corporate and public end-users.*
- ***Customization and branding:*** *You can customize the user interface and workflows to match your application's branding and provide a consistent experience for all users.*
- ***Security and compliance:*** *Identity Platform offers robust security features, including multi-factor authentication and compliance with industry standards, to protect customer data.*
- ***Integration with Google Cloud:*** *Identity Platform integrates seamlessly with other Google Cloud services, making it easy to build and deploy your application.*

Why other options are not as suitable:

- ***Option 1:*** *Domain restricted sharing is primarily used for controlling access to Google Workspace resources, not for managing application access.*
- ***Option 2:*** *Workforce Identity Federation is designed for managing access for employees and partners, not for external customers.*
- ***Option 3:*** *Google Workspace identities are not suitable for managing a large number of external customer identities.*

By using a CIAM solution like Identity Platform, you can effectively manage both corporate and public end-users for your application, providing a secure, scalable, and user-friendly experience.

Hide Solution Discussion 2
Correct Answer: D

Question #289

You work for an organization that handles sensitive customer data. You must secure a series of Google Cloud Storage buckets housing this data and meet these requirements:
• Multiple teams need varying access levels (some read-only, some read-write).
• Data must be protected in storage and at rest.
• It's critical to track file changes and audit access for compliance purposes.
• For compliance purposes, the organization must have control over the encryption keys.

What should you do?

A. Create IAM groups for each team and manage permissions at the group level. Employ server-side encryption and Object Versioning by Google Cloud Storage. Configure cloud monitoring tools to alert on anomalous data access patterns.
B. Set individual permissions for each team and apply access control lists (ACLs) to each bucket and file. Enforce TLS encryption for file transfers. Enable Object Versioning and Cloud Audit Logs for the storage buckets.
C. Use predefined IAM roles tailored to each team's access needs, such as Storage Object Viewer and Storage Object User. Utilize customer-supplied encryption keys (CSEK) and enforce TLS encryption. Turn on both Object Versioning and Cloud Audit Logs for the storage buckets.
D. Assign IAM permissions for all teams at the object level. Implement third-party software to encrypt data at rest. Track data access by using network logs.

Hide Solution Discussion 1
Correct Answer: C

Question #290

You are implementing communications restrictions for specific services in your Google Cloud organization. Your data analytics team works in a dedicated folder. You need to ensure that access to BigQuery is controlled for that folder and its projects. The data analytics team must be able to control the restrictions only at the folder level. What should you do?

A. Create an organization-level access policy with a service perimeter to restrict BigQuery access. Assign the data analytics team the Access Context Manager Editor role on the access policy to allow the team to configure the access policy.
B. Create a scoped policy on the folder with a service perimeter to restrict BigQuery access. Assign the data analytics team the Access Context Manager Editor role on the scoped policy to allow the team to configure the scoped policy.
C. Define a hierarchical firewall policy on the folder to deny BigQuery access. Assign the data analytics team the Compute Organization Firewall Policy Admin role to allow the team to configure rules for the firewall policy.
D. Enforce the Restrict Resource Service Usage organization policy constraint on the folder to restrict BigQuery access. Assign the data analytics team the Organization Policy Administrator role to allow the team to manage exclusions within the folder.

Hide Solution Discussion 1
Correct Answer: B

Question #291

Your organization ɯs using a third-party identity and authentication provider to centrally manage users. You want to use this identity provider to grant access to the Google Cloud console without syncing identities to Google Cloud. Users should receive permissions based on attributes. What should you do?

A. Configure the central identity provider as a workforce identity pool provider in Workforce Identity Federation. Create an attribute mapping by using the Common Expression Language (CEL).

B. Configure a periodic synchronization of relevant users and groups with attributes to Cloud Identity. Activate single sign-on by using the Security Assertion Markup Language (SAML).
C. Set up the Google Cloud Identity Platform. Configure an external authentication provider by using OpenID Connect and link user accounts based on attributes.
D. Activate external identities on the Identity-Aware Proxy. Use the Security Assertion Markup Language (SAML) to configure authentication based on attributes to the central authentication provider.

Reason:

- ***Leverages existing identity provider:*** *This option allows you to utilize your organization's central identity provider without needing to duplicate user information in Google Cloud. This simplifies user management and ensures consistency across systems.*

- ***Attribute-based access control:*** *Workforce Identity Federation supports attribute mapping using CEL. This enables you to define fine-grained access control policies based on user attributes from your central identity provider (e.g., job title, department, etc.).*

- ***No identity synchronization:*** *This method avoids the overhead and potential complexities of synchronizing identities between your central identity provider and Google Cloud.*

- ***Seamless user experience:*** *Users can access the Google Cloud console using their existing credentials from the central identity provider, providing a single sign-on experience.*

Why other options are not as suitable:

- ***Option 2:*** *Synchronizing identities with Cloud Identity creates redundancy and introduces potential inconsistencies between your central identity provider and Google Cloud.*
- ***Option 3:*** *Google Cloud Identity Platform is primarily used for customer-facing applications, not for managing internal access to the Google Cloud console.*
- ***Option 4:*** *Identity-Aware Proxy is useful for securing applications, but it's not the most efficient way to manage access to the Google Cloud console for users from a central identity provider.*

By configuring your central identity provider as a workforce identity pool provider and using CEL for attribute mapping, you can achieve secure and efficient access control to the Google Cloud console without the need for identity synchronization.

Hide Solution Discussion 1
Correct Answer: A

Reference: Google Cloud Workforce Identity Federation & Demo

Question #292

You are implementing a new web application on Google Cloud that will be accessed from your on-premises network. To provide protection from threats like malware, you must implement transport layer security (TLS) interception for incoming traffic to your application. What should you do?

A. Configure Secure Web Proxy. Offload the TLS traffic in the load balancer, inspect the traffic, and forward the traffic to the web application.

B. Configure an internal proxy load balancer. Offload the TLS traffic in the load balancer inspect, the traffic and forward the traffic to the web application.
C. Configure a hierarchical firewall policy. Enable TLS interception by using Cloud Next Generation Firewall (NGFW) Enterprise.
D. Configure a VPC firewall rule. Enable TLS interception by using Cloud Next Generation Firewall (NGFW) Enterprise.

Reason:

- ***Purpose-built for secure web traffic:*** *Secure Web Proxy is a Google Cloud service specifically designed for this scenario. It provides a managed solution for TLS interception and inspection of web traffic, allowing you to protect your applications from threats while simplifying management.*

- ***Integrated with Load Balancing:*** *Secure Web Proxy works seamlessly with Google Cloud load balancers. This allows you to offload TLS termination and inspection to the proxy, freeing up resources on your web application servers.*

- ***Advanced security features:*** *Secure Web Proxy offers features like malware detection, intrusion prevention, and data loss prevention (DLP) to enhance your security posture.*

- ***Scalability and availability:*** *As a managed service, Secure Web Proxy scales automatically to handle your traffic needs and provides high availability.*

Why other options are not as suitable:

- ***Option 2:*** *While an internal proxy load balancer can offload TLS traffic, it doesn't provide the same level of security features and ease of management as Secure Web Proxy.*
- ***Option 3 & 4:*** *Cloud Next Generation Firewall (NGFW) Enterprise is a powerful firewall solution, but it's primarily focused on network-level security. While it can perform TLS interception, it's not the most efficient or convenient way to achieve this for web application traffic. Using Secure Web Proxy provides a more specialized and optimized solution for this use case.*

By using Secure Web Proxy, you can effectively implement TLS interception for your web application, ensuring protection from threats while maintaining performance and simplifying management.

Reference: Introducing Cloud Secure Web Proxy

Hide Solution Discussion 4
Correct Answer: A

Question #293

Your organization has hired a small, temporary partner team for 18 months. The temporary team will work alongside your DevOps team to develop your organization's application that is hosted on Google Cloud. You must give the temporary partner team access to your application's resources on Google Cloud and ensure that partner employees lose access. If they are removed from their employer's organization. What should you do?

A. Create a temporary username and password for the temporary partner team members. Auto-clean the usernames and passwords after the work engagement has ended.

B. Create a workforce identity pool and federate the identity pool with the identity provider (IdP) of the temporary partner team.

C. Implement just-in-time privileged access to Google Cloud for the temporary partner team.

D. Add the identities of the temporary partner team members to your identity provider (IdP).

Reason:

Security and Access Control: *Workforce identity pools are specifically designed for scenarios where external users need access to your cloud resources. By federating the identity pool with the partner team's IdP, you leverage their existing identity management system. This ensures that only authenticated users from the partner team can access your resources.*

- ***Automated Access Revocation:*** *When a partner employee is removed from their employer's IdP, their access to your Google Cloud resources is automatically revoked. This eliminates the need for manual de-provisioning and reduces the risk of unauthorized access after the engagement ends.*

- ***Simplified Management:*** *This approach streamlines the onboarding and offboarding process for temporary team members. You don't need to create individual accounts or manage credentials within your own IdP.*

- ***Compliance:*** *Using a workforce identity pool helps you meet compliance requirements by ensuring that access is granted based on verified identities and that access is revoked when no longer needed.*

Why other options are less suitable:

- ***Option 1:*** *Creating temporary usernames and passwords is not secure and can lead to credential leakage. It also requires manual effort to clean up credentials.*
- ***Option 3:*** *Just-in-time privileged access is useful for granting temporary elevated permissions, but it doesn't address the core need for managing access for the entire duration of the partner team's engagement.*
- ***Option 4:*** *Adding partner team members to your own IdP is not ideal for temporary engagements. It creates unnecessary overhead and potential security risks.*

By using a workforce identity pool and federating with the partner's IdP, you can effectively manage access for the temporary team, ensuring security and compliance while minimizing administrative effort.

Hide Solution Discussion 1
Correct Answer: B

Question #294

Your organization has an internet-facing application behind a load balancer. Your regulators require end-to-end encryption of user login credentials. You must implement this requirement. What should you do?

A. Generate a symmetric key with Cloud KMS. Encrypt client-side user credentials by using the symmetric key.

B. Concatenate the credential with a timestamp. Submit the timestamp and hashed value of credentials to the network.

C. Deploy the TLS certificate at Google Cloud Global HTTPs Load Balancer, and submit the user credentials through HTTPs.

D. Generate an asymmetric key with Cloud KMS. Encrypt client-side user credentials using the public key.

Hide Solution Discussion 1
Correct Answer: C

Question #295

Your organization heavily utilizes serverless applications while prioritizing security best practices. You are responsible for enforcing image provenance and compliance with security standards before deployment. You leverage Cloud Build as your continuous integration and continuous deployment (CI/CD) tool for building container images. You must configure Binary Authorization to ensure that only images built by your Cloud Build pipeline are deployed and that the images pass security standard compliance checks. What should you do?

A. Create a Binary Authorization attestor that uses a scanner to assess source code management repositories. Deploy images only if the attestor validates results against a security policy.
B. Create a Binary Authorization attestor that utilizes a scanner to evaluate container image build processes. Define a policy that requires deployment of images only if this attestation is present.
C. Create a Binary Authorization attestor that retrieves the Cloud Build build ID of the container image. Configure a policy to allow deployment only if there's a matching build ID attestation.
D. Utilize a custom Security Health Analytics module to create a policy. Enforce the policy through Binary Authorization to prevent deployment of images that do not meet predefined security standards.

Reason:

- ***Directly links image to trusted build process:*** *This approach focuses on verifying the origin of the image. By associating the image with a specific Cloud Build ID, you can ensure that only images built within your controlled and secured CI/CD pipeline are deployed. This effectively prevents deployment of images from unknown or untrusted sources.*

- ***Strong security control:*** *Cloud Build build IDs are unique and tamper-proof, making them a reliable indicator of image provenance. Binary Authorization can enforce this check at deploy time, providing a strong security control against unauthorized images.*

- ***Easy to implement and manage:*** *This solution leverages existing Cloud Build functionality and integrates seamlessly with Binary Authorization. It doesn't require complex setup or external tools.*

Why other options are not as effective:

- ***Option 1 & 2:*** *While scanning source code and build processes are valuable security practices, they don't directly guarantee that the deployed image originated from your trusted Cloud Build pipeline. Someone could potentially pass the scans with a malicious image built outside your CI/CD.*

- ***Option 4:*** *Security Health Analytics is a useful tool for identifying vulnerabilities and misconfigurations, but it doesn't inherently enforce image provenance. It might flag an issue but not necessarily prevent deployment.*

By focusing on the Cloud Build build ID as the key attestation, you establish a robust and straightforward mechanism to ensure that only authorized images built through your secure CI/CD process are deployed in your serverless environment.

Hide Solution Discussion
Correct Answer: B

Question #296

Your organization operates in a highly regulated industry and uses multiple Google Cloud services. You need to identify potential risks to regulatory compliance. Which situation introduces the greatest risk?

A. The security team mandates the use of customer-managed encryption keys (CMEK) for all data classified as sensitive.
B. Sensitive data is stored in a Cloud Storage bucket with the uniform bucket-level access setting enabled.
C. The audit team needs access to Cloud Audit Logs related to managed services like BigQuery.
D. Principals have broad IAM roles allowing the creation and management of Compute Engine VMs without a pre-defined hardening process.

Hide Solution Discussion
Correct Answer: D

Question #297

Your multinational organization is undergoing rapid expansion within Google Cloud. New teams and projects are added frequently. You are concerned about the potential for inconsistent security policy application and permission sprawl across the organization. You must enforce consistent standards while maintaining the autonomy of regional teams. You need to design a strategy to effectively manage IAM and organization policies at scale, ensuring security and administrative efficiency. What should you do?

A. Create detailed organization-wide policies for common scenarios. Instruct teams to apply the policies carefully at the project and resource level as needed.
B. Delegate the creation of organization policies to regional teams. Centrally review these policies for compliance before deployment.
C. Define a small set of essential organization policies. Supplement these policies with a library of optional policy templates for teams to leverage as needed.
D. Use a hierarchical structure of folders. Implement template-based organization policies that cascade down, allowing limited customization by regional teams.

Reason:

- ***Centralized Control with Flexibility:*** *This approach provides a balance between centralized security standards and regional autonomy. Organization policies applied at the folder level inherit down to the projects within that folder. This ensures consistency across the organization while allowing regional teams to customize policies within defined boundaries.*

- ***Scalability:*** *A hierarchical structure using folders is highly scalable. As your organization grows and adds more teams and projects, you can easily create new folders and apply the appropriate organization policies.*

- ***Reduced Administrative Overhead:*** *Template-based organization policies streamline policy creation and management. Instead of creating policies from scratch, teams can use pre-defined templates and modify them as needed, saving time and effort.*

- ***Improved Security:*** *By setting baseline security policies at the folder level, you can prevent inconsistent application of security policies and permission sprawl. This helps to ensure that all projects adhere to the organization's security standards.*

Why other options are not as effective:

- ***Option 1:*** *While detailed organization-wide policies are useful, relying solely on manual application by individual teams can lead to inconsistencies and errors.*
- ***Option 2:*** *Delegating policy creation entirely to regional teams can result in significant variations in security posture and compliance issues.*
- ***Option 3:*** *While a library of optional templates is helpful, it doesn't provide the same level of control and consistency as a hierarchical structure with cascading policies.*

By implementing a hierarchical structure with template-based organization policies, you can effectively manage IAM and ensure consistent security practices across your rapidly expanding organization on Google Cloud.

Hide Solution Discussion
Correct Answer: D

Question #298

A security audit uncovered several inconsistencies in your project's Identity and Access Management (IAM) configuration. Some service accounts have overly permissive roles, and a few external collaborators have more access than necessary. You need to gain detailed visibility into changes to IAM policies, user activity, service account behavior, and access to sensitive projects. What should you do?

A. Configure Google Cloud Functions to be triggered by changes to IAM policies. Analyze changes by using the policy simulator, send alerts upon risky modifications, and store event details.
B. Enable the metrics explorer in Cloud Monitoring to follow the service account authentication events and build alerts linked on it.
C. Use Cloud Audit Logs. Create log export sinks to send these logs to a security information and event management (SIEM) solution for correlation with other event sources.
D. Deploy the OS Config Management agent to your VMs. Use OS Config Management to create patch management jobs and monitor system modifications.

Hide Solution Discussion
Correct Answer: C

Reason:

- ***Cloud Audit Logs*** *provide detailed visibility into administrative activities, including* ***changes to IAM policies****,* ***user activity****, and* ***service account behavior****. These logs can capture who modified permissions, what changes were made, and when the changes occurred.*
- *By creating* ***log export sinks****, you can forward these logs to a* ***SIEM solution*** *for further analysis and correlation with other security-related events from various sources. This ensures comprehensive monitoring and security incident detection, enabling you to spot excessive permissions, detect anomalies, and respond to security threats more effectively.*

Why the other options are less ideal:

- ***A. Cloud Functions with policy simulator****: While this approach could trigger alerts on IAM policy changes, it is more complex to implement, requires custom code, and doesn't provide comprehensive visibility into user activity, service account behavior, or sensitive project access.*
- ***B. Metrics explorer in Cloud Monitoring****: This would allow you to track some service account authentication events, but it doesn't provide comprehensive details on IAM policy changes or user activities.*
- ***D. OS Config Management agent****: This tool is used for managing operating system configurations and patching on VMs, but it doesn't address IAM policy changes or provide insights into IAM-related security issues.*

Therefore, using ***Cloud Audit Logs*** *and forwarding them to a* ***SIEM*** *for deeper analysis and correlation is the most effective approach for gaining visibility into IAM changes and improving security monitoring across your projects.*

Question #299

You manage multiple internal-only applications that are hosted within different Google Cloud projects. You are deploying a new application that requires external internet access. To maintain security, you want to clearly separate this new application from internal systems. Your solution must have effective security isolation for the new externally-facing application. What should you do?

A. Deploy the application within the same project as an internal application. Use a Shared VPC model to manage network configurations.

B. Place the application in the same project as an existing internal application, and adjust firewall rules to allow external traffic.

C. Create a VPC Service Controls perimeter, and place the new application's project within that perimeter.

D. Create a new project for the application, and use VPC Network Peering to access necessary resources in the internal projects.

Hide Solution Discussion
Correct Answer: D

Reason:

- *Creating a* ***new project*** *for the externally-facing application ensures that you maintain* ***clear separation*** *between internal systems and external-facing resources. This provides strong* ***security isolation****, preventing potential threats from affecting the internal applications and systems.*

- ***VPC Network Peering*** *allows the new application to access necessary internal resources while keeping the network environments separated. This means that traffic flows between projects in a secure, private network without exposing internal systems to the public internet.*

Why the other options are less ideal:

- ***A. Deploy the application within the same project as an internal application (Shared VPC)****: This doesn't provide sufficient security isolation. Even with Shared VPC, hosting external and internal applications in the same project increases the risk of lateral movement between systems if the external application is compromised.*
- ***B. Adjusting firewall rules****: Putting the new application in the same project and just adjusting firewall rules is risky. Firewall rules are prone to misconfigurations, and this approach does not provide the strong isolation that placing the application in a separate project would.*
- ***C. VPC Service Controls perimeter****: While VPC Service Controls are useful for securing APIs and services, it is more suitable for protecting sensitive data and internal APIs from unauthorized access, not for isolating external-facing applications from internal ones.*

Thus, ***creating a separate project*** *and using* ***VPC Network Peering*** *strikes the right balance between isolation, security, and access to internal resources, making it the best approach for your scenario.*

Question #300

You work for an ecommerce company that stores sensitive customer data across multiple Google Cloud regions. The development team has built a new 3-tier application to process orders and must integrate the application into the production environment.

You must design the network architecture to ensure strong security boundaries and isolation for the new application, facilitate secure remote maintenance by authorized third-party vendors, and follow the principle of least privilege. What should you do?

A. Create separate VPC networks for each tier. Use VPC peering between application tiers and other required VPCs. Provide vendors with SSH keys and root access only to the instances within the VPC for maintenance purposes.

B. Create a single VPC network and create different subnets for each tier. Create a new Google project specifically for the third-party vendors and grant the network admin role to the vendors. Deploy a VPN appliance and rely on the vendors' configurations to secure third-party access.

C. Create separate VPC networks for each tier. Use VPC peering between application tiers and other required VPCs. Enable Identity-Aware Proxy (IAP) for remote access to management resources, limiting access to authorized vendors.

D. Create a single VPC network and create different subnets for each tier. Create a new Google project specifically for the third-party vendors. Grant the vendors ownership of that project and the ability to modify the Shared VPC configuration.

Hide Solution Discussion
Correct Answer: C

Question #301

Your organization is implementing separation of duties in a Google Cloud project. A group of developers must deploy new code, but cannot have permission to change network firewall rules. What should you do?

A. Assign the network administrator IAM role to all developers. Tell developers not to change firewall settings.
B. Use Access Context Manager to create conditions that allow only authorized administrators to change firewall rules based on attributes such as IP address or device security posture.
C. Create and assign two custom IAM roles. Assign the deployer role to control Compute Engine and deployment-related permissions. Assign the network administrator role to manage firewall permissions.
D. Grant the editor IAM role to the developer group. Explicitly negate any firewall modification permissions by using IAM deny policies.

Hide Solution Discussion
Correct Answer: C

Question #302

You manage a Google Cloud organization with many projects located in various regions around the world. The projects are protected by the same Access Context Manager access policy. You created a new folder that will host two projects that process protected health information (PHI) for US-based customers. The two projects will be separately managed and require stricter protections. You are setting up the VPC Service Controls configuration for the new folder. You must ensure that only US-based personnel can access these projects and restrict Google Cloud API access to only BigQuery and Cloud Storage within these projects. What should you do?

A. • Create a scoped access policy, add the new folder under "Select resources to include in the policy," and assign an administrator under "Manage principals."
• For the service perimeter, specify the two new projects as "Resources to protect" in the service perimeter configuration.
• Set "Restricted services" to "all services," set "VPC accessible services" to "Selected services," and specify only BigQuery and Cloud Storage under "Selected services."
B. • Enable Identity Aware Proxy in the new projects.
• Create an Access Context Manager access level with an "IP Subnetworks" attribute condition set to the US-based corporate IP range.
• Enable the "Restrict Resource Service Usage" organization policy at the new folder level with an "Allow" policy type and set both "storage.googleapis.com" and "bigquery.googleapis.com" under "Custom values."
C. • Edit the organization-level access policy and add the new folder under "Select resources to include in the policy."
• Specify the two new projects as "Resources to protect" in the service perimeter configuration.
• Set "Restricted services" to "all services," set "VPC accessible services" to "Selected services," and specify only BigQuery and Cloud Storage.
• Edit the existing access level to add a "Geographic locations" condition set to "US."
D. • Configure a Cloud Interconnect connection or a Virtual Private Network (VPN) between the on-premises environment and the Google Cloud organization.
• Configure the VPC firewall policies within the new projects to only allow connections from the on-premises IP address range.
• Enable the Restrict Resource Service Usage organization policy on the new folder with an "Allow"

policy type, and set both “storage.googleapis.com” and “bigquery.googleapis.com” under “Custom values.”

Hide Solution Discussion
Correct Answer: A

Question #303

There is a threat actor that is targeting organizations like yours. Attacks are always initiated from a known IP address range. You want to deny-list those IPs for your website, which is exposed to the internet through an Application Load Balancer. What should you do?

A. Create a Cloud Armor policy with a deny-rule for the known IP address range. Attach the policy to the backend of the Application Load Balancer.
B. Activate Identity-Aware Proxy for the backend of the Application Load Balancer. Create a firewall rule that only allows traffic from the proxy to the application.
C. Create a log sink with a filter containing the known IP address range. Trigger an alert that detects when the Application Load Balancer is accessed from those IPs.
D. Create a Cloud Firewall policy with a deny-rule for the known IP address range. Associate the firewall policy to the Virtual Private Cloud with the application backend.

Hide Solution Discussion
Correct Answer: A

Question #304

You are managing a Google Cloud environment that is organized into folders that represent different teams. These teams need the flexibility to modify organization policies relevant to their work. You want to grant the teams the necessary permissions while upholding Google-recommended security practices and minimizing administrative complexity. What should you do?

A. Create a custom IAM role with the organization policy administrator permission and grant the permission to each team’s folder. Limit policy modifications based on folder names within the custom role’s definition.
B. Assign the organization policy administrator role to a central service account and provide teams with the credentials to use the service account when needed.
C. Create an organization-level tag. Attach the tag to relevant folders. Use an IAM condition to restrict the organization policy administrator role to resources with that tag.
D. Grant each team the organization policy administrator role at the organization level.

Hide Solution Discussion
Correct Answer: C

Question #305

Your organization is using Vertex AI Workbench Instances. You must ensure that newly deployed Instances are automatically kept up-to-date and that users cannot accidentally alter settings in the operating system. What should you do?

A. Enforce the disableRootAccesa and requireAutoUpgradeSchedule organization policies for newly deployed Instances.
B. Enable the VM Manager and ensure the corresponding Google Compute Engine instances are added.
C. Implement a firewall rule that prevents Secure Shell access to the corresponding Google Compute Engine instances by using tags.
D. Assign the AI Notebooks Runner and AI Notebooks Viewer roles to the users of the AI Workbench Instances.

Hide Solution Discussion
Correct Answer: A

Reason:

- ***disableRootAccess*** *policy ensures that users cannot make changes to the operating system, such as altering settings or installing unauthorized software. Disabling root access is a key measure for preventing users from accidentally or maliciously modifying system configurations.*
- ***requireAutoUpgradeSchedule*** *policy ensures that instances are automatically kept up-to-date by enforcing automatic upgrades to the latest security patches and software updates. This policy helps maintain a secure and consistent environment across all instances.*

Why the other options are less ideal:

- ***B. Enable VM Manager****: While VM Manager helps with operational tasks like patching, configuration management, and inventory, it does not inherently prevent users from altering OS settings or guarantee automatic updates without specific configuration.*
- ***C. Implement a firewall rule****: Blocking Secure Shell (SSH) access via a firewall prevents users from accessing instances remotely, but it does not directly address the requirement of enforcing automatic updates or preventing changes to the operating system.*
- ***D. Assigning AI Notebooks Runner and Viewer roles****: These roles control access to notebooks and their execution, but they do not prevent users from altering the operating system or ensure instances are kept up-to-date.*

Therefore, enforcing the ***disableRootAccess*** *and* ***requireAutoUpgradeSchedule*** *policies is the best approach to meet both the requirements of restricting user control over the OS and ensuring automatic updates for the instances.*

Question #306

You must ensure that the keys used for at-rest encryption of your data are compliant with your organization's security controls. One security control mandates that keys get rotated every 90 days. You must implement an effective detection strategy to validate if keys are rotated as required. What should you do?

A. Analyze the crypto key versions of the keys by using data from Cloud Asset Inventory. If an active key is older than 90 days, send an alert message through your incident notification channel.
B. Assess the keys in the Cloud Key Management Service by implementing code in Cloud Run. If a key is not rotated after 90 days, raise a finding in Security Command Center.

C. Define a metric that checks for timely key updates by using Cloud Logging. If a key is not rotated after 90 days, send an alert message through your incident notification channel.

D. Identify keys that have not been rotated by using Security Health Analytics. If a key is not rotated after 90 days, a finding in Security Command Center is raised.

Hide Solution Discussion
Correct Answer: A

Question #307

Your organization is developing a sophisticated machine learning (ML) model to predict customer behavior for targeted marketing campaigns. The BigQuery dataset used for training includes sensitive personal information. You must design the security controls around the AI/ML pipeline. Data privacy must be maintained throughout the model's lifecycle and you must ensure that personal data is not used in the training process. Additionally, you must restrict access to the dataset to an authorized subset of people only. What should you do?

A. De-identify sensitive data before model training by using Cloud Data Loss Prevention (DLP)APIs. and implement strict Identity and Access Management (IAM) policies to control access to BigQuery.

B. Implement Identity-Aware Proxy to enforce context-aware access to BigQuery and models based on user identity and device.

C. Implement at-rest encryption by using customer-managed encryption keys (CMEK) for the pipeline. Implement strict Identity and Access Management (IAM) policies to control access to BigQuery.

D. Deploy the model on Confidential VMs for enhanced protection of data and code while in use. Implement strict Identity and Access Management (IAM) policies to control access to BigQuery.

Hide Solution Discussion
Correct Answer: A

Question #308

Your organization wants to publish yearly reports of your website usage analytics. You must ensure that no data with personally identifiable information (PII) is published by using the Cloud Data Loss Prevention (Cloud DLP) API. Data integrity must be preserved. What should you do?

A. Detect all PII in storage by using the Cloud DLP API. Create a cloud function to delete the PII.

B. Discover and quarantine your PII data in your storage by using the Cloud DLP API.

C. Discover and transform PII data in your reports by using the Cloud DLP API.

D. Encrypt the PII from the report by using the Cloud DLP API.

Hide Solution Discussion
Correct Answer: C

Question #309

Your development team is launching a new application. The new application has a microservices architecture on Compute Engine instances and serverless components, including Cloud Functions. This application will process financial transactions that require temporary, highly sensitive data in

memory. You need to secure data in use during computations with a focus on minimizing the risk of unauthorized access to memory for this financial application. What should you do?

A. Enable Confidential VM instances for Compute Engine, and ensure that relevant Cloud Functions can leverage hardware-based memory isolation.
B. Use data masking and tokenization techniques on sensitive financial data fields throughout the application and the application's data processing workflows.
C. Use the Cloud Data Loss Prevention (Cloud DLP) API to scan and mask sensitive data before feeding the data into any compute environment.
D. Store all sensitive data during processing in Cloud Storage by using customer-managed encryption keys (CMEK), and set strict bucket-level permissions.

Hide Solution Discussion
Correct Answer: A

Reason:

- ***Confidential VMs*** *provide hardware-based memory encryption, which ensures that data in use (i.e., data being processed in memory) is encrypted and isolated, minimizing the risk of unauthorized access. This feature is specifically designed for high-security use cases like processing sensitive financial transactions.*
- *Option A directly addresses the need for protecting data "in use" (during computation) with a* ***focus on minimizing the risk of unauthorized access to memory****.*

Why the other options are not ideal:

- ***B. Data masking and tokenization****: These techniques protect data at rest or in transit but do not directly address the requirement of securing data in memory (in use during computation).*
- ***C. Cloud DLP****: The DLP API helps in identifying and masking sensitive data, but it does not protect the data during computation (in memory).*
- ***D. Cloud Storage with CMEK****: This would secure data at rest (storage), not in use during active computations.*

Thus, option A is the best solution for securing data while it's being processed in memory.

Question #310

You work for a financial organization in a highly regulated industry that is subject to active regulatory compliance. To meet compliance requirements, you need to continuously maintain a specific set of configurations, data residency, organizational policies, and personnel data access controls. What should you do?

A. Apply an organizational policy constraint at the organization level to limit the location of new resource creation.
B. Create an Assured Workloads folder for your required compliance program to apply defined controls and requirements.
C. Go to the Compliance page in Security Command Center. View the report for your status against the required compliance standard. Triage violations to maintain compliance on a regular basis.

D. Create a posture.yaml file with the required security compliance posture. Apply the posture with the gcloud scc postures create POSTURE_NAME --posture-from-file=posture.yaml command in Security Command Center Premium.

Reason:

- ***Assured Workloads:*** *Assured Workloads are specifically designed for organizations in highly regulated industries. They provide a framework for creating controlled environments within Google Cloud that meet specific compliance requirements.*
- ***Compliance Program:*** *By selecting the appropriate compliance program (e.g., HIPAA, FedRAMP, PCI DSS) when creating the Assured Workloads folder, you automatically enforce the necessary controls and configurations for that specific regulation. This includes data residency, personnel access controls, and other compliance requirements.*
- ***Continuous Compliance:*** *Assured Workloads provide ongoing monitoring and enforcement of compliance requirements. This helps ensure that your environment remains compliant over time, even as you make changes or add new resources.*
- ***Simplified Compliance Management:*** *Assured Workloads streamline compliance management by providing a structured approach and automating many of the necessary controls. This reduces the burden on your security and compliance teams.*

Why other options are less comprehensive:

- ***A. Organizational policy constraint:*** *While organizational policies are useful for enforcing constraints, they might not cover all the specific requirements of your compliance program, especially regarding data residency and personnel access controls.*
- ***C. Security Command Center Compliance Reports:*** *SCC compliance reports are valuable for monitoring your compliance posture, but they don't actively enforce the necessary controls or configurations. You still need to manually remediate any violations.*
- ***D. Security Command Center Premium posture.yaml:*** *While SCC Premium postures can define and enforce security configurations, they might not address all the specific requirements of your compliance program, particularly those related to data residency and personnel access controls.*

In summary: *Creating an Assured Workloads folder tailored to your specific compliance program provides the most comprehensive and automated solution for meeting your regulatory requirements. It simplifies compliance management, enforces necessary controls, and helps ensure continuous compliance in your Google Cloud environment.*

Reveal Solution Discussion

Question #311

Your organization is worried about recent news headlines regarding application vulnerabilities in production applications that have led to security breaches. You want to automatically scan your deployment pipeline for vulnerabilities and ensure only scanned and verified containers can run in the environment. What should you do?

A. Use Kubernetes role-based access control (RBAC) as the source of truth for cluster access by granting “container.clusters.get” to limited users. Restrict deployment access by allowing these users to generate a kubeconfig file containing the configuration access to the GKE cluster.

B. Use gcloud artifacts docker images describe. LOCATION-docker.pkg.dev/PROJECT_ID/REPOSITORY/IMAGE_ID@sha256:HASH --show-package-vulnerability in your CI/CD pipeline, and trigger a pipeline failure for critical vulnerabilities.

C. Enforce the use of Cloud Code for development so users receive real-time security feedback on vulnerable libraries and dependencies before they check in their code.

D. Enable Binary Authorization and create attestations of scans.

Reason:

- *Binary Authorization: Binary Authorization acts as a gatekeeper for deployments, ensuring that only images that meet your security policies are allowed to run. This prevents vulnerable containers from reaching production, even if they make it through the CI/CD pipeline.*

- *Attestations of Scans: You can integrate vulnerability scanning tools into your CI/CD pipeline and create attestations that verify the scan results. Binary Authorization can then be configured to require these attestations before allowing an image to be deployed. This ensures that only scanned and approved images are allowed to run.*

- *Automated Security Enforcement: This approach automates security checks and enforcement, reducing the risk of human error and ensuring consistent application of security policies.*

- *Defense in Depth: Binary Authorization provides an additional layer of security on top of vulnerability scanning, adding defense-in-depth to your deployment pipeline.*

Why other options are less suitable:

- *A. Kubernetes RBAC: While RBAC is important for controlling access to your cluster, it doesn't directly address the issue of preventing vulnerable containers from running.*
- *B. gcloud command in CI/CD: Using the gcloud command to check for vulnerabilities is a good practice, but it doesn't prevent the deployment of vulnerable images. It only provides information about vulnerabilities.*
- *C. Cloud Code: Cloud Code can help developers identify vulnerabilities during development, but it doesn't guarantee that all vulnerabilities will be fixed before deployment.*

In summary: Enabling Binary Authorization and requiring attestations of vulnerability scans provides the most robust and automated way to ensure that only scanned and verified containers are deployed to your production environment. This approach strengthens your security posture and reduces the risk of vulnerabilities being exploited in your applications.

Reveal Solution Discussion

Question #312

A team at your organization collects logs in an on-premises security information and event management system (SIEM). You must provide a subset of Google Cloud logs for the SIEM, and minimize the risk of data exposure in your cloud environment. What should you do?

A. Create a new BigQuery dataset. Stream all logs to this dataset. Provide the on-premises SIEM system access to the data in BigQuery by using workload identity federation and let the SIEM team filter for the relevant log data.

B. Define a log view for the relevant logs. Provide access to the log view to a principal from your on-premises identity provider by using workforce identity federation.

C. Create a log sink for the relevant logs. Send the logs to Pub/Sub. Retrieve the logs from Pub/Sub and push the logs to the SIEM by using Dataflow.

D. Filter for the relevant logs. Store the logs in a Cloud Storage bucket. Grant the service account access to the bucket. Provide the service account key to the SIEM team.

Reason:

- ***Log Views for Granular Access:*** *Log views allow you to create filtered subsets of your logs, exposing only the specific data that your on-premises SIEM needs. This minimizes the amount of sensitive information that leaves your cloud environment.*

- ***Workforce Identity Federation:*** *By using workforce identity federation, you can grant access to the log view to a principal (user or group) from your on-premises identity provider (IdP). This allows the SIEM team to authenticate with their existing credentials and avoids the need to create and manage separate Google Cloud identities.*

- ***Security:*** *This approach minimizes the risk of data exposure by:*
  - ***Limiting data access:*** *Only the necessary logs are shared.*
  - ***Secure authentication:*** *Leveraging your existing on-premises IdP for authentication.*
  - ***No sensitive credentials:*** *You don't need to share any service account keys.*
- ***Efficiency:*** *Log views are efficient because they filter data within Cloud Logging itself, reducing the amount of data that needs to be transferred and processed.*

Why other options are less suitable:

- ***A. BigQuery and Workload Identity Federation:*** *While this allows access to logs, it exposes the entire dataset in BigQuery, potentially including sensitive information not intended for the SIEM.*
- ***C. Log sink, Pub/Sub, and Dataflow:*** *This approach is more complex and requires setting up and managing additional components like Pub/Sub and Dataflow. It also increases the attack surface by transferring logs through multiple services.*
- ***D. Cloud Storage and service account key:*** *Sharing service account keys is generally discouraged due to security risks. If the key is compromised, it could grant unauthorized access to your Cloud Storage bucket.*

In summary: *Using log views with workforce identity federation provides a secure, efficient, and granular way to share a subset of your Google Cloud logs with your on-premises SIEM, minimizing the risk of data exposure and simplifying access management.*

Reveal Solution Discussion

Question #313

Your Google Cloud organization is subdivided into three folders: production, development, and networking, Networking resources for the organization are centrally managed in the networking folder. You discovered that projects in the production folder are attaching to Shared VPCs that are outside of

the networking folder which could become a data exfiltration risk. You must resolve the production folder issue without impacting the development folder. You need to use the most efficient and least disruptive approach. What should you do?

A. Enable the Restrict Shared VPC Host Projects organization policy on the production folder. Create a custom rule and configure the policy type to Allow. In the Custom value section, enter under:folders/networking.
B. Enable the Restrict Shared VPC Host Projects organization policy on the networking folder only. Create a new custom rule and configure the policy type to Allow. In the Custom value section, enter under:organizations/123456739123.
C. Enable the Restrict Shared VPC Host Projects organization policy at the project level for each of the production projects. Create a custom rule and configure the policy type to Allow. In the Custom value section, enter under:folders/networking.
D. Enable the Restrict Shared VPC Host Projects organization policy at the organization level. Create a custom rule and configure the policy type to Allow. In the Custom value section, enter under:folders/networking.

Reason:

- ***Targeted Restriction:*** *By applying the Restrict Shared VPC Host Projects organization policy specifically to the production folder, you limit the impact of the change to only the production environment. The development folder remains unaffected.*

- ***Centralized Networking Control:*** *This policy allows you to enforce that projects within the production folder can only attach to Shared VPCs hosted in the designated networking folder. This ensures that all networking resources are centrally managed and controlled, reducing the risk of data exfiltration.*

- ***Granular Control:*** *The "Allow" rule with the under:folders/networking value provides precise control over which projects can act as Shared VPC hosts for the production environment.*

- ***Minimal Disruption:*** *This approach avoids making changes at the organization level or individual project level, minimizing disruption to existing workflows and configurations.*

Why other options are less suitable:

- ***B. Networking folder only:*** *Enabling the policy on the networking folder doesn't prevent production projects from attaching to Shared VPCs outside of that folder.*
- ***C. Project level:*** *Applying the policy at the project level is less efficient and more time-consuming, especially if you have many production projects.*
- ***D. Organization level:*** *Enabling the policy at the organization level would affect all folders, including development, which is not desired.*

In summary: *By enabling the Restrict Shared VPC Host Projects organization policy on the production folder and configuring an "Allow" rule with the appropriate value, you can effectively address the data exfiltration risk without impacting the development environment and with minimal disruption to your existing setup.*

Reveal Solution Discussion

Question #314

Your organization operates in a highly regulated environment and has a stringent set of compliance requirements for protecting customer data. You must encrypt data while in use to meet regulations. What should you do?

A. Enable the use of customer-supplied encryption keys (CSEK) keys in the Google Compute Engine VMs to give your organization maximum control over their VM disk encryption.
B. Establish a trusted execution environment with a Confidential VM.
C. Use a Shielded VM to ensure a secure boot with integrity monitoring for the application environment.
D. Use customer-managed encryption keys (CMEK) and Cloud KSM to enable your organization to control their keys for data encryption in Cloud SQL.

Reveal Solution Discussion

Question #315

Your organization is building a real-time recommendation engine using ML models that process live user activity data stored in BigQuery and Cloud Storage. Each new model developed is saved to Artifact Registry. This new system deploys models to Google Kubernetes Engine, and uses Pub/Sub for message queues. Recent industry news have been reporting attacks exploiting ML model supply chains. You need to enhance the security in this serverless architecture, specifically against risks to the development and deployment pipeline. What should you do?

A. Enable container image vulnerability scanning during development and pre-deployment. Enforce Binary Authorization on images deployed from Artifact Registry to your continuous integration and continuous deployment (CVCD) pipeline.
B. Thoroughly sanitize all training data prior to model development to reduce risk of poisoning attacks. Use IAM for authorization, and apply role-based restrictions to code repositories and cloud services.
C. Limit external libraries and dependencies that are used for the ML models as much as possible. Continuously rotate encryption keys that are used to access the user data from BigQuery and Cloud Storage.
D. Develop strict firewall rules to limit external traffic to Cloud Run instances. Integrate intrusion detection systems (IDS) for real-time anomaly detection on Pub/Sub message flows.

Reveal Solution Discussion

Question #316

You want to set up a secure, internal network within Google Cloud for database servers. The servers must not have any direct communication with the public internet. What should you do?

A. Assign a private IP address to each database server. Use a NAT gateway to provide internet connectivity to the database servers.
B. Assign a static public IP address to each database server. Use firewall rules to restrict external access.
C. Create a VPC with a private subnet. Assign a private IP address to each database server.
D. Assign both a private IP address and a public IP address to each database server.

Reveal Solution Discussion

Question #317

You work for a large organization that recently implemented a 100GB Cloud Interconnect connection between your Google Cloud and your on-premises edge router. While routinely checking the connectivity, you noticed that the connection is operational but there is an error message that indicates MACsec is operationally down. You need to resolve this error. What should you do?

A. Ensure that the Cloud Interconnect connection supports MACsec.
B. Ensure that the on-premises router is not down.
C. Ensure that the active pre-shared key created for MACsec is not expired on both the on-premises and Google edge routers.
D. Ensure that the active pre-shared key matches on both the on-premises and Google edge routers.

Reveal Solution Discussion

Question #318

Your organization must store highly sensitive data within Google Cloud. You need to design a solution that provides the strongest level of security and control. What should you do?

A. Use Cloud Storage with customer-supplied encryption keys (CSEK), VPC Service Controls for network isolation, and Cloud DLP for data inspection.
B. Use Cloud Storage with customer-managed encryption keys (CMEK), Cloud DLP for data classification, and Secret Manager for storing API access tokens.
C. Use Cloud Storage with client-side encryption, Cloud KMS for key management, and Cloud HSM for cryptographic operations.
D. Use Cloud Storage with server-side encryption, BigQuery with column-level encryption, and IAM roles for access control.

Reveal Solution Discussion

Question #319

The InfoSec team has mandated that all new Cloud Run jobs and services in production must have Binary Authorization enabled. You need to enforce this requirement. What should you do?

A. Configure an organization policy to require Binary Authorization enforcement on images deployed to Cloud Run.
B. Configure a Security Health Analytics (SHA) custom rule that prevents the execution of Cloud Run jobs and services without Binary Authorization.
C. Ensure the Cloud Run admin role is not assigned to developers.
D. Configure a Binary Authorization custom policy that is not editable by developers and auto-attaches to all Cloud Run jobs and services.

Reveal Solution Discussion

Question #320

You are developing an application that runs on a Compute Engine VM. The application needs to access data stored in Cloud Storage buckets in other Google Cloud projects. The required access to the buckets is variable. You need to provide access to these resources while following Google-recommended practices. What should you do?

A. Limit the VMs access to the Cloud Storage buckets by setting the relevant access scope of the VM.
B. Create IAM bindings for the VM's service account and the required buckets that allow appropriate access to the data stored in the buckets.
C. Grant the VM's service account access to the required buckets by using domain-wide delegation.
D. Create a group and assign IAM bindings to the group for each bucket that the application needs to access. Assign the VM's service account to the group.

Reveal Solution Discussion

Question #321

Your organization strives to be a market leader in software innovation. You provided a large number of Google Cloud environments so developers can test the integration of Gemini in Vertex AI into their existing applications or create new projects. Your organization has 200 developers and a five-person security team. You must prevent and detect proper security policies across the Google Cloud environments. What should you do? (Choose two.)

A. Apply organization policy constraints. Detect and monitor drifts by using Security Health Analytics.
B. Publish internal policies and clear guidelines to securely develop applications.
C. Use Cloud Logging to create log filters to detect misconfigurations. Trigger Cloud Run functions to remediate misconfigurations.
D. Apply a predefined AI-recommended security posture template for Gemini in Vertex AI in Security Command Center Enterprise or Premium tiers.
E. Implement the least privileged access Identity and Access Management roles to prevent misconfigurations.

Reason:

- ***A. Apply organization policy constraints. Detect and monitor drifts by using Security Health Analytics.*** *Organization policies let you set guardrails that prevent developers from making insecure configurations. This proactive approach is essential with a large developer team. Security Health Analytics then continuously monitors your environments for violations of these policies, alerting your small security team to any drift. This combination provides both prevention and detection.*

- ***D. Apply a predefined AI-recommended security posture template for Gemini in Vertex AI in Security Command Center Enterprise or Premium tiers.*** *Security Command Center Premium offers predefined security posture templates tailored to specific services like Gemini. These templates incorporate Google's best practices and AI recommendations for securing your Vertex AI deployments. This saves your security team significant time and effort in defining and managing security policies from scratch.*

Why the other options are less ideal:

- ***B. Publish internal policies and clear guidelines to securely develop applications.*** *While essential for security awareness, this relies on developers following guidelines perfectly, which is difficult to enforce consistently with a large team.*
- ***C. Use Cloud Logging to create log filters to detect misconfigurations. Trigger Cloud Run functions to remediate misconfigurations.*** *This is a reactive approach that requires building and maintaining custom logging and remediation logic. It can be complex and might not cover all potential misconfigurations.*
- ***E. Implement the least privileged access Identity and Access Management roles to prevent misconfigurations.*** *Least privilege is crucial, but it doesn't prevent all misconfigurations. Developers with limited permissions can still make mistakes that expose data or create vulnerabilities.*

In summary: *Combining organization policy constraints with Security Health Analytics and leveraging AI-recommended security posture templates provides a proactive, scalable, and efficient way to manage security across a large number of developer environments. This approach allows your small security team to effectively prevent and detect misconfigurations while empowering developers to innovate.*