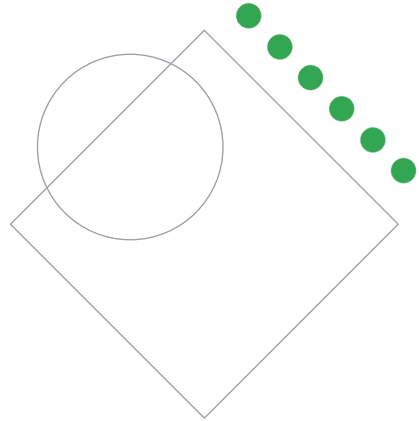Google Cloud

Preparing for Your Professional Cloud Security Engineer Journey

Module 4: Managing Operations Within a Cloud Solution Environment

Welcome to Module 4: Managing Operations Within a Cloud Solution Environment.
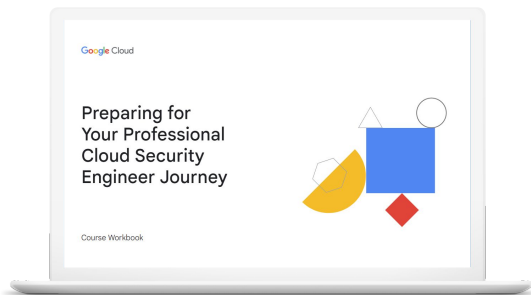
Review and study planning

Now let's review how to use these diagnostic questions to help you identify what to include in your study plan.

Your study plan:

Managing operations within a cloud solution environment

4.1	Building and deploying secure infrastructure and applications
4.2	Configuring logging, monitoring, and detection

Google Cloud

We'll approach this review by looking at the key areas of this exam section and the questions you just answered about each one. We'll talk about where you can find out more about each area in the learning path for this certification and/or where to find the information in Google Cloud documentation. As we go through each one, take notes on the specific courses (and modules!), quests, and documentation pages you'll want to emphasize in your study plan.

4.1 | Building and deploying secure infrastructure and applications

Considerations include:

- Automating security scanning for Common Vulnerabilities and Exposures (CVEs) through a continuous integration and delivery CI/CD pipeline
- Automating virtual machine image creation, hardening, maintenance, and patch management
- Automating container image creation, verification, hardening, maintenance, and patch management
- Automating policy as code and drift detection

Building secure infrastructure and applications is an important part of the Professional Cloud Security Engineer role. You are expected to automate security configuration and deployment for CI/CD pipelines, virtual machine images, and container images.

Question 1 asked you to identify the steps to automate vulnerability scanning in Container Analysis. Question 2 tested your knowledge of Shielded VMs and Integrity Monitoring. Question 3 asked you to automate the creation of secure VM images. Question 4 asked you to automate the creation of secure container images.

Diagnostic Question 01 Discussion

Cymbal Bank has received Docker source files from its third-party developers in an Artifact Registry repository. These Docker fil2es will be part of a CI/CD pipeline to update Cymbal Bank's personal loan offering. The bank wants to prevent the possibility of remote users arbitrarily using the Docker files to run any code. You have been tasked with using Container Analysis' On-Demand scanning to scan the images for a one-time update.

What should you do?

A. Prepare a cloudbuild.yaml file. In this file, add four steps in order—build, scan, severity check, and push—specifying the location of Artifact Registry repository. Specify severity level as **CRITICAL**. Start the build with the command `gcloud builds submit`.

B. Prepare a cloudbuild.yaml file. In this file, add four steps in order—scan, build, severity check, and push—specifying the location of the Artifact Registry repository. Specify severity level as **HIGH**. Start the build with the command `gcloud builds submit`.

C. Prepare a cloudbuild.yaml file. In this file, add four steps in order—scan, severity check, build, and—push specifying the location of the Artifact Registry repository. Specify severity level as **HIGH**. Start the build with the command `gcloud builds submit`.

D. Prepare a cloudbuild.yaml file. In this file, add four steps in order—build, severity check, scan, and push—specifying the location of the Artifact Registry repository. Specify severity level as **CRITICAL**. Start the build with the command `gcloud builds submit`.

Google Cloud

Feedback:
A. Correct! Scanning requires you to build the images, scan them, check for severity, and push to the registry, in that order. Severity level required is CRITICAL to disable remote users from running code using images.

B. Incorrect. The sequence of steps is incorrect because you cannot scan an image or check for severities before building it. The severity level should be CRITICAL, not HIGH, to disable remote users from running code using images.

C. Incorrect. The sequence of steps is incorrect because you cannot scan an image before building it. The severity level should be CRITICAL, not HIGH, to disable remote users from running code using images.

D. Incorrect. The sequence of steps is incorrect because the image should be scanned before you check for severity. Severity level should be CRITICAL, which is correct.

Where to look:
- https://cloud.google.com/container-analysis/docs/ods-cloudbuild
- https://cloud.google.com/container-analysis/docs/container-scanning-overview#severity_levels_for_vulnerabilities

Content mapping:
- ILT course: **Security in Google Cloud**

- ○ M8 Securing Google Kubernetes Engine: Techniques and Best Practices

- ● On-demand course: **Security Best Practices in Google Cloud**
  - ○ M4 Securing Google Kubernetes Engine: Techniques and Best Practices

Summary:
Container Analysis allows you to perform automatic and on-demand scanning in both Artifact Registry and Container Registry. Artifact Registry extends the functionality offered by Container Registry by including support for non-image resources, Customer-Managed Encryption Keys, fine-grained IAM controls, and VPC Service Controls. Container Analysis scans for vulnerabilities in a container's image and non-image resources. Using Cloud Build, you can create yaml templates for CI/CD pipelines that fetch the container from the registry and deploy to the target infrastructure.

| **Diagnostic Question 02 Discussion**

Cymbal Bank's management is concerned about virtual machines being compromised by bad actors. More specifically, they want to receive immediate alerts if there have been changes to the boot sequence of any of their Compute Engine instances.

What should you do?

A. Set an organization-level policy that requires all Compute Engine VMs to be configured as Shielded VMs. Use Secure Boot enabled with Unified Extensible Firmware Interface (UEFI). Validate integrity events in Cloud Monitoring and place alerts on launch attestation events.

B. Set Cloud Logging measurement policies on the VMs. Use Cloud Logging to place alerts whenever actualMeasurements and policyMeasurements don't match.

C. Set an organization-level policy that requires all Compute Engine VMs to be configured as Shielded VMs. Use Measured Boot enabled with Virtual Trusted Platform Module (vTPM). Validate integrity events in Cloud Monitoring and place alerts on late boot validation events.

D. Set project-level policies that require all Compute Engine VMs to be configured as Shielded VMs. Use Measured Boot enabled with Virtual Trusted Platform Module (vTPM). Validate integrity events in Cloud Monitoring and place alerts on late boot validation events.

Feedback:
A. Incorrect. Although Shielded VMs support Integrity Monitoring (a way to determine whether a VM instance's boot sequence has changed), Integrity Monitoring is enabled through Virtual Trusted Platform Module (vTPM) and not Unified Extensible Firmware Interface (UEFI).

B. Incorrect. Use Confidential or Shielded VMs. They can enable Virtual Trusted Platform Module (vTPM), which is required for Integrity Monitoring.

C. Correct! Shielded VMs support Integrity Monitoring, which determines whether a VM instance's boot sequence has changed. The integrity baseline policy is created when you boot a VM for the first time. Every subsequent reboot will now generate and compare Early Boot and Late Boot events against the integrity baseline policy.

D. Incorrect. Using Shielded VMs with Measured Boot and Virtual Trusted Platform Module (vTPM) is correct. However, you need to enable shielded VMs at the organization level, not project level, to capture all instances in Cymbal Bank's infrastructure.

Where to look:
- https://cloud.google.com/compute/shielded-vm/docs/shielded-vm#integrity-monitoring
- https://cloud.google.com/compute/shielded-vm/docs/integrity-monitoring

Content mapping:
- ILT course: **Security in Google Cloud**
  - M5 Securing Compute Engine: Techniques and Best Practices

- On-demand course: **Security Best Practices in Google Cloud**
  - M1 Securing Compute Engine: Techniques and Best Practices

Summary:
Shielded VMs offer Virtual Trusted Platform Module (vTPM) which enables integrity monitoring. A vTPM generates hashes for the boot event and sandwiches all subsequent actions as updates to the hash. The final hash is used to validate against the hashes of every reboot. Any changes, updates, or misconfigurations at boot time can be captured at this stage.

Diagnostic Question 03 Discussion

Cymbal Bank runs a Node.js application on a Compute Engine instance. Cymbal Bank needs to share this base image with a 'development' Google Group. This base image should support secure boot for the Compute Engine instances deployed from this image. How would you automate the image creation?

How would you automate the image creation?

A. Prepare a shell script. Add the command gcloud compute instances stop with the Node.js instance name. Set up certificates for secure boot. Add gcloud compute images create, and specify the Compute Engine instance's persistent disk and zone and the certificate files. Add gcloud compute images add-iam-policy-binding and specify the 'development' group.

B. Start the Compute Engine instance. Set up certificates for secure boot. Prepare a cloudbuild.yaml configuration file. Specify the persistent disk location of the Compute Engine and the 'development' group. Use the command gcloud builds submit --tag, and specify the configuration file path and the certificates.

C. Prepare a shell script. Add the command gcloud compute instances start to the script to start the Node.js Compute Engine instance. Set up Measured Boot for secure boot. Add gcloud compute images create, and specify the persistent disk and zone of the Compute Engine instance.

D. Stop the Compute Engine instance. Set up Measured Boot for secure boot. Prepare a cloudbuild.yaml configuration file. Specify the persistent disk location of the Compute Engine instance and the 'development' group. Use the command gcloud builds submit --tag, and specify the configuration file path.

Google Cloud

Feedback:
A. Correct! You need to stop the Compute Engine instance before creating the image. Use the command gcloud compute images create with the instance's disk and zone. Secure boot requires setting up certificates to establish trust between platform, firmware, and OS.

B. Incorrect. Although Cloud Build could be used, --tag is used to specify existing Docker images. To use Cloud Build to build VM images, use the Packer tool.

C. Incorrect. You need to stop the Compute Engine instance before creating an image. The command create image is correct. Measured Boot is used for Integrity Monitoring, which can check whether any changes were made to the booting sequence, not for secure boot.

D. Incorrect. Although Cloud Build could be used, --tag is used to specify existing Docker images. To use Cloud Build to build VM images, use the Packer tool. Measured Boot is used for Integrity Monitoring, which can check whether any changes were made to the booting sequence, not for secure boot.

Where to look:
- https://cloud.google.com/compute/shielded-vm/docs/creating-shielded-images
- https://cloud.google.com/compute/docs/images/create-delete-deprecate-private-images#guest-os-features
- https://cloud.google.com/compute/docs/images/managing-access-custom-ima

- ges#share-images-within-organization
- https://cloud.google.com/compute/docs/images/image-management-best-practices

Content mapping:
- ILT course: **Security in Google Cloud**
  - M5 Securing Compute Engine: Techniques and Best Practices

- On-demand course: **Security Best Practices in Google Cloud**
  - M1 Securing Compute Engine: Techniques and Best Practices

Summary:
Compute Engine images provide reusability and ease of redeployment. Images can be built from a persistent disk or its snapshot or from an existing image. This existing image could be in a project or Cloud Storage. Shielded VMs leverage the image reusability only if firmware is UEFI-compliant, and you can enable secure boot in images.

Shell scripts and Cloud Build can be used to automate the image creation process if the task is small and does not require a complete CI/CD pipeline. Before creating the image, ensure that the instance is stopped.

Diagnostic Question 04 Discussion

Cymbal Bank uses Docker containers to interact with APIs for its personal banking application. These APIs are under PCI-DSS compliance. The Kubernetes environment running the containers will not have internet access to download required packages.

How would you automate the pipeline that is building these containers?

A. Create a Dockerfile with container definition and cloudbuild.yaml file. Use Cloud Build to build the image from Dockerfile. Upload the built image to a Google Container registry and Dockerfile to a Git repository. In the cloudbuild.yaml template, include attributes to tag the Git repository path with a Google Kubernetes Engine cluster. Create a trigger in Cloud Build to automate the deployment using the Git repository.

B. Create a Dockerfile with a container definition and a Cloud Build configuration file. Use the Cloud Build configuration file to build and deploy the image from Dockerfile to a Google Container registry. In the configuration file, include the Google Container Registry path and the Google Kubernetes Engine cluster. Upload the configuration file to a Git repository. Create a trigger in Cloud Build to automate the deployment using the Git repository.

C. Build a foundation image. Store all artifacts and a Packer definition template in a Git repository. Use Container Registry to build the artifacts and Packer definition. Use Cloud Build to extract the built container and deploy it to a Google Kubernetes Engine (GKE) cluster. Add the required users and groups to the GKE project.

D. Build an immutable image. Store all artifacts and a Packer definition template in a Git repository. Use Container Registry to build the artifacts and Packer definition. Use Cloud Build to extract the built container and deploy it to a Google Kubernetes Engine Cluster (GKE). Add the required users and groups to the GKE project.

Google Cloud

Feedback:
A. Incorrect. In the cloudbuild.yaml file, you should add the image's path and Google Kubernetes Engine cluster name and then upload to a Git repository. The Dockerfile should not be uploaded to Git repository. The usage of Git repository to create a Cloud Build trigger for automation is correct but this process would have automated deployment only. You need to automate build and deployment.

B. Correct! Cloud Build can help build a container image from a Dockerfile and upload it to Google Cloud Registry (GCR). Then you can create a configuration file mapping container image path in GCR to Google Kubernetes Engine (GKE) cluster. Upload this configuration file to a Git repository and use it to create a Cloud Build trigger. Whenever you update the Git repository with a new build and source, Cloud Build will update the GKE cluster.

C. Incorrect. Foundation images require web access to download required packages. You need to build a pipeline, so Cloud Build standalone is not a solution. Use a CI/CD pipeline creator such as Jenkins.

D. Incorrect. Container Registry cannot be used for artifact metadata; instead, use Artifact Registry. You need to build a pipeline, so Cloud Build standalone is not a solution. Use a CI/CD pipeline creator such as Jenkins. However, creating an immutable image for the container is the right choice.

Where to look:

- https://cloud.google.com/build/docs/deploying-builds/deploy-gke#automating_deployments
- https://cloud.google.com/build/docs/build-push-docker-image#build_an_image_using_a_build_config_file
- https://cloud.google.com/architecture/automated-build-images-with-jenkins-kubernetes

Content mapping:
- ILT course: **Security in Google Cloud**
  - M8 Securing Google Kubernetes Engine: Techniques and Best Practices

- On-demand course: **Security Best Practices in Google Cloud**
  - M4 Securing Google Kubernetes Engine: Techniques and Best Practices

- Quest: Google Kubernetes Engine Best Practices: Security

Summary:
With Docker, Kubernetes, Container Registry and Cloud Build, you can design a CI/CD pipeline to read Cloud Build configuration files from a Git repository and perform deployments in your Google Kubernetes Engine (GKE) infrastructure. The pipeline begins at the Git repository that contains the container definitions as a config file and configuration file to build and deploy a container to Container Registry. From the Container Registry, the images are deployed to GKE. Cloud Build supports triggers for automation that wait for the Git repository to signal a change or an update.

4.1 | Building and deploying secure infrastructure and applications

Courses

Security in Google Cloud
- M5 Securing Compute Engine: Techniques and Best Practices
- M8 Securing Google Kubernetes Engine: Techniques and Best Practices

Security Best Practices in Google Cloud
- M1 Securing Compute Engine: Techniques and Best Practices
- M4 Securing Google Kubernetes Engine: Techniques and Best Practices

Skill Badges

Google Cloud

Google Kubernetes Engine Best Practices: Security Quest
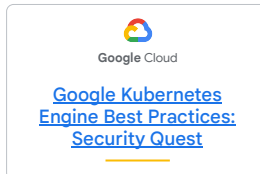
Documentation

Using On-Demand Scanning in your Cloud Build pipeline | Container Analysis documentation | Google Cloud

Container scanning | Container Analysis documentation | Google Cloud

Creating custom shielded images | Shielded VM | Google Cloud

Creating, deleting, and deprecating custom images | Compute Engine Documentation | Google Cloud

Managing access to custom images | Compute Engine Documentation | Google Cloud

Image management best practices | Compute Engine Documentation | Google Cloud

Deploying to GKE | Cloud Build Documentation

Quickstart: Build and push a Docker image with Cloud Build

Automated image builds with Jenkins, Packer, and Kubernetes | Cloud Architecture Center | Google Cloud

---

Let's take a moment to consider resources that can help you build your knowledge and skills in this area.

The concepts in the diagnostic questions we just reviewed are covered in these modules and in this documentation. Reviewing the documentation is highly recommended. You'll find this list in your workbook so you can take a note of what you want to include later when you build your study plan. Based on your experience with the diagnostic questions, you may want to include some or all of these.

- https://cloud.google.com/container-analysis/docs/ods-cloudbuild
- https://cloud.google.com/container-analysis/docs/container-scanning-overview#severity_levels_for_vulnerabilities
- https://cloud.google.com/compute/shielded-vm/docs/creating-shielded-images
- https://cloud.google.com/compute/docs/images/create-delete-deprecate-private-images#guest-os-features
- https://cloud.google.com/compute/docs/images/managing-access-custom-images#share-images-within-organization
- https://cloud.google.com/compute/docs/images/image-management-best-practices
- https://cloud.google.com/build/docs/deploying-builds/deploy-gke#automating_deployments
- https://cloud.google.com/build/docs/build-push-docker-image#build_an_image_using_a_build_config_file
- https://cloud.google.com/architecture/automated-build-images-with-jenkins-ku

- [bernetes](#)

Configuring logging, monitoring, and detection

Considerations include:

- Configuring and analyzing network logs (Firewall rule logs, VPC flow logs, packet mirroring, Cloud Intrusion Detection System [Cloud IDS])
- Designing an effective logging strategy
- Logging, monitoring, responding to, and remediating security incidents
- Exporting logs to external security systems
- Configuring and analyzing Google Cloud audit logs and data access logs
- Configuring log exports (log sinks and aggregated sinks)
- Configuring and monitoring Security Command Center (Security Health Analytics, Event Threat Detection, Container Threat Detection, Web Security Scanner)

Google Cloud

A Professional Cloud Security Engineer should be familiar with the tools and processes available in Google Cloud for logging, monitoring, and detection, and how to design and configure solutions.

Question 5 tested your knowledge of utilizing Cloud Logging to monitor against, detect, and perform forensics for security issues. Question 6 asked you to efficiently configure logging, monitoring, and detection using Event Threat Detection and Security Command Center. Question 7 tested your knowledge of audit logging behavior. Question 8 examined how to configure and use audit logs for a forensic scenario. Question 9 required you to configure log exports for long-term storage and forensics. Question 10 tested your knowledge of using Security Command Center.

| Diagnostic Question 05 Discussion

Cymbal Bank has Docker applications deployed in Google Kubernetes Engine. The bank has no offline containers. This GKE cluster is exposed to the public internet and has recently recovered from an attack. Cymbal Bank suspects that someone in the organization changed the firewall rules and has tasked you to analyze and find all details related to the firewall for the cluster. You want the most cost-effective solution for this task.

What should you do?

A. View the GKE logs in Cloud Logging. Use the log scoping tool to filter the Firewall Rules log. Create a Pub/Sub topic. Export the logs to a Pub/Sub topic using the command gcloud logging sinks create. Use Dataflow to read from Pub/Sub and query the stream.

B. View the GKE logs in the local GKE cluster. Use the kubectl Sysdig Capture tool to filter the Firewall Rules log. Create a Pub/Sub topic. Export these logs to a Pub/Sub topic using the GKE cluster. Use Dataflow to read from Pub/Sub and query the stream.

C. View the GKE logs in the local GKE cluster. Use Docker-explorer to explore the Docker file system. Filter and export the Firewall logs to Cloud Logging. Create a dataset in BigQuery to accept the logs. Use the command gcloud logging sinks create to export the logs to a BigQuery dataset. Query this dataset.

D. View the GKE logs in Cloud Logging. Use the log scoping tool to filter the Firewall Rules log. Create a dataset in BigQuery to accept the logs. Export the logs to BigQuery using the command gcloud logging sinks create. Query this dataset.

Google Cloud

Feedback:
A. Incorrect. This is not the most cost-effective solution. Use BigQuery to analyze the logs that are data-at-rest. A BigQuery dataset can be used as a sink for logs. Use Dataflow when building data transformation pipelines for batch and stream data.

B. Incorrect. Kubectl Sysdig Capture uses Sysdig Inspect, an open source tool to analyze forensic evidence. Kubectl Sysdig is used to correlate activities inside a pod with a Linux system running the pods. Dataflow is more expensive than BigQuery and is used to build batch and stream data transformations.

C. Incorrect. Docker-explorer can only be used with offline containers, which Cymbal Bank does not have in this scenario. Cloud Logging is enabled by default, and exporting to Cloud Logging from Docker-explorer is not required.

D. Correct! Cloud Logging is enabled by default for GKE clusters. The Firewall Rules log captures all changes made to the firewall. BigQuery can be used to capture the data and analyze it using the free quota.

Where to look:
- https://cloud.google.com/architecture/security-controls-and-forensic-analysis-for-GKE-apps#using_analytical_tooling_for_forensic_analysis_of_containers
- https://cloud.google.com/architecture/exporting-stackdriver-logging-for-security-and-access-analytics

Content mapping:
- ILT course: **Security in Google Cloud**
  - M11 Monitoring, Logging, and Scanning

- On-demand course: **Mitigating Security Vulnerabilities in Google Cloud**
  - M3 Monitoring, Logging, and Scanning

Summary:
When you create a GKE cluster, Cloud Logging is enabled by default. Both Google Cloud and the Kubernetes ecosystem provide a range of tools for forensic investigations and audit. Cloud Logging, Docker-explorer, and Kubectl Sysdig Capture plus Sysdig Inspect provide forensic mechanisms. Use Docker-explorer for offline containers, and use Kubectl Sysdig Capture to trigger system events. Cloud Logging stores Firewall rules but not data access rules by default.

| Diagnostic Question 06 Discussion

Cymbal Bank experienced a recent security issue. A rogue employee with admin permissions for Compute Engine assigned existing Compute Engine users some arbitrary permissions. You are tasked with finding all these arbitrary permissions.

What should you do to find these permissions most efficiently?

A. Use Event Threat Detection and configure Continuous Exports to filter and write only Firewall logs to the Security Command Center. In the Security Command Center, select **Event Threat Detection** as the source, filter by **evasion: Iam,** and sort to find the attack time window. Click on **Persistence: IAM Anomalous Grant** to display Finding Details. View the **Source** property of the Finding Details section.

B. Use Event Threat Detection and configure Continuous Exports to filter and write only Firewall logs to the Security Command Center. In the Security Command Center, select **Event Threat Detection** as the source, filter by **category: anomalies**, and sort to find the attack time window. Click on **Evasion: IAM Anomalous Grant** to display Finding Details. View the **Source** property of the Finding Details section.

C. Use Event Threat Detection and trigger the IAM Anomalous grants detector. Publish results to the Security Command Center. In the Security Command Center, select **Event Threat Detection** as the source, filter by **category: iam**, and sort to find the attack time window. Click on **Persistence: IAM Anomalous Grant** to display Finding Details. View the **Source** property of the Finding Details section.

D. Use Event Threat Detection and trigger the IAM Anomalous Grant detector. Publish results to Cloud Logging. In the Security Command Center, select **Cloud Logging** as the source, filter by **category: anomalies**, and sort to find the attack time window. Click on **Persistence: IAM Anomalous Grant** to display Finding Details. View the **Source** property of the Finding Details section.

Google Cloud

Feedback:
A. Incorrect. Use the IAM Anomalous Grant detector and not Continuous Exports. Use Continuous Exports before the incident and not afterward. Use **Persistence: IAM Anomalous Grant** to display Finding Details.

B. Incorrect. Use the IAM Anomalous Grant detector and not Continuous Exports. Use **category: iam** and not anomalies. Use **Persistence: IAM Anomalous Grant** to display Finding Details.

C. Correct! Event Threat Detection has triggers that detect anomalies on specified filters. Event Threat Detection can publish results to the Security Command Center. From the Security Command Center, filter and navigate to find all anomalies for the affected users.

D. Incorrect. Event Threat Detection can directly publish the results to the Security Command Center and does not need Cloud Logging as an intermediate step. Select Event Threat Detection directly as a source. Using Cloud Logging adds additional cost and latency to the process.

Where to look:
https://cloud.google.com/architecture/security-controls-and-forensic-analysis-for-GKE-apps#using_automated_event_detection

Content mapping:

- ILT course: **Security in Google Cloud**
  - M11 Monitoring, Logging, and Scanning

- On-demand course: **Mitigating Security Vulnerabilities in Google Cloud**
  - M3 Monitoring, Logging, and Scanning

Summary:
Event Threat Detection and the Security Command Center together can help find anomalies such as users and service accounts with excessive permissions or compromised Compute Engine instances. Event Threat Detection can trigger event detectors. You can verify that Event Threat Detection is working by intentionally triggering the IAM Anomalous Grant detector and checking for findings.

Diagnostic Question 07 Discussion

Cymbal Bank wants to use Cloud Storage and BigQuery to store safe deposit usage data. Cymbal Bank needs a cost-effective approach to auditing only Cloud Storage and BigQuery data access activities.

How would you use Cloud Audit Logs to enable this analysis?

A. Enable Data Access Logs for ADMIN_READ, DATA_READ, and DATA_WRITE at the service level for BigQuery and Cloud Storage.
B. Enable Data Access Logs for ADMIN_READ, DATA_READ, and DATA_WRITE at the organization level.
C. Enable Data Access Logs for ADMIN_READ, DATA_READ, and DATA_WRITE for Cloud Storage. All Data Access Logs are enabled for BigQuery by default.
D. Enable Data Access Logs for ADMIN_READ, DATA_READ, and DATA_WRITE for BigQuery. All Data Access Logs are enabled for Cloud Storage by default.

Google Cloud

Feedback:
A. Incorrect. Cloud Storage must be configured for Cloud Audit Logging, but BigQuery is enabled by default.

B. Incorrect. ADMIN_READ, DATA_READ, and DATA_WRITE logs are required for Cloud Storage and BigQuery only. Enabling logs at the organization level will incur much higher costs than for specified services.

C. Correct! Cloud Storage must be configured for Cloud Audit Logging, but BigQuery is enabled by default.

D. Incorrect. Cloud Storage must be configured for Cloud Audit Logging, but BigQuery is enabled by default.

Where to look:
- https://cloud.google.com/logging/docs/audit
- https://cloud.google.com/storage/docs/audit-logging
- https://cloud.google.com/logging/docs/audit/configure-data-access

Content mapping:
- ILT course: **Security in Google Cloud**
  - M11 Monitoring, Logging, and Scanning

- On-demand course: **Mitigating Security Vulnerabilities in Google Cloud**

- ○ M3 Monitoring, Logging, and Scanning

Summary:
Cloud Audit Logs has Admin Activity audit logs and Data Access audit logs. Admin Activity audit logs are always written and cannot be disabled. Because data access is very frequent and generates numerous events, Data Access audit logs are disabled by default for all resources except BigQuery. BigQuery stores the Data Access logs for additional security.

| Diagnostic Question 08 Discussion

Cymbal Bank has suffered a remote botnet attack on Compute Engine instances in an isolated project. The affected project now requires investigation by an external agency. An external agency requests that you provide all admin and system events to analyze in their local forensics tool. You want to use the most cost-effective solution to enable the external analysis.

What should you do?

A. Use Event Threat Detection. Trigger the IAM Anomalous Grant detector to detect all admins and users with admin or system permissions. Export these logs to the Security Command Center. Give the external agency access to the Security Command Center.

B. Use Cloud Audit Logs. Filter Admin Activity audit logs for only the affected project. Use a Pub/Sub topic to stream the logs from Cloud Audit Logs to the external agency's forensics tool.

C. Use the Security Command Center. Select Cloud Logging as the source, and filter by category: Admin Activity and category: System Activity. View the Source property of the Finding Details section. Use Pub/Sub topics to export the findings to the external agency's forensics tool.

D. Use Cloud Monitoring and Cloud Logging. Filter Cloud Monitoring to view only system and admin logs. Expand the system and admin logs in Cloud Logging. Use Pub/Sub to export the findings from Cloud Logging to the external agency's forensics tool or storage.

Google Cloud

Feedback:
A. Incorrect. You could use Event Threat Detection, but only with the correct filters and configurations. Instead of directly providing access to your Security Command Center, use Pub/Sub to export the logs to the external agency's forensics tool.

B. Correct! Cloud Audit Logs by default has admin and system activity logged. Filter the logs and use a Pub/Sub topic to send the logs to the external agency's forensics tool.

C. Incorrect. Use Cloud Audit Logs instead of Cloud Logging as the source for forensics. Cloud Logging must be configured for specific logs. However, with the correct filtered data, using Pub/Sub would be correct.

D. Incorrect. Use Cloud Audit Logs, not Cloud Monitoring and Cloud Logging, for forensics. Using Pub/Sub to export the logs is correct.

Where to look:
- https://cloud.google.com/logging/docs/audit
- https://cloud.google.com/storage/docs/audit-logging
- https://cloud.google.com/logging/docs/audit/configure-data-access

Content mapping:
- ILT course: **Security in Google Cloud**
  - M11 Monitoring, Logging, and Scanning

- On-demand course: **Mitigating Security Vulnerabilities in Google Cloud**
  - M3 Monitoring, Logging, and Scanning

Summary:
Cloud Audit Logs provides reliable information during forensics investigations. Cloud Audit Logs returns authentication details, metadata, service name, method name, affected resources, authorization info, and timestamp, along with other details. These findings can be exported to an external agency or auditor for further analysis.

Diagnostic Question 09 Discussion

The loan application from Cymbal Bank's lending department collects credit reports that contain credit payment information from customers. According to bank policy, the PDF reports are stored for six months in Cloud Storage, and access logs for the reports are stored for three years. You need to configure a cost-effective storage solution for the access logs.

What should you do?

A. Set up a logging export dataset in BigQuery to collect data from Cloud Logging and Cloud Monitoring. Create table expiry rules to delete logs after three years.

B. Set up a logging export dataset in BigQuery to collect data from Cloud Logging and the Security Command Center. Create table expiry rules to delete logs after three years.

C. Set up a logging export bucket in Cloud Storage to collect data from the Security Command Center. Configure object lifecycle management rules to delete logs after three years.

D. Set up a logging export bucket in Cloud Storage to collect data from Cloud Audit Logs. Configure object lifecycle management rules to delete logs after three years.

Google Cloud

Feedback:
A. Incorrect. Use Cloud Audit Logs for compliance. Use BigQuery if the logs were also analyzed continuously. Because the requirement is to only store the logs, Cloud Storage is the more cost-effective solution.

B. Incorrect. The Security Command Center lets you view security events and risks; you use Cloud Audit Logs for compliance. The requirement is only to store the logs, not analyze them, so Cloud Storage is the more cost-effective solution. Use BigQuery if the logs must also be analyzed continuously.

C. Incorrect. Cloud Storage is the most cost-effective solution. The Security Command Center lets you view security events and risks; you use Cloud Audit Logs for compliance.

D. Correct! Cloud Audit Logs has provisions for data access logs that are required in this scenario. Cloud Storage provides the most cost-effective storage solution.

Where to look:
https://cloud.google.com/architecture/exporting-stackdriver-logging-for-compliance-requirements

Content mapping:
- ILT course: **Security in Google Cloud**
  - M11 Monitoring, Logging, and Scanning

- On-demand course: **Mitigating Security Vulnerabilities in Google Cloud**
  - M3 Monitoring, Logging, and Scanning

Summary:
Cloud Audit Logs stores incorruptible records that can be used for forensics, auditing, and compliance. Cloud Audit Logs enables Data Access logs, which fit this scenario of recording access to PDF files. Cloud Storage is an ideal sink target due to the cost and object lifecycle rules. Object lifecycle rules enable data deletion after the set time period. Although Cloud Storage is the right solution for this scenario, use BigQuery for storage instead when data needs to be analyzed, not just stored.

| Diagnostic Question 10 Discussion

Cymbal Bank uses Compute Engine instances for its APIs, and recently discovered bitcoin mining activities on some instances. The bank wants to detect all future mining attempts and notify the security team. The security team can view the Security Command Center and Cloud Audit Logs.

How should you configure the detection and notification?

A. Use Event Threat Detection's threat detectors. Export findings from 'Suspicious account activity' and 'Anomalous IAM behavior' detectors and publish them to a Pub/Sub topic. Create a Cloud Function to send notifications of suspect activities. Use Pub/Sub notifications to invoke the Cloud Function.

B. Enable the VM Manager tools suite in the Security Command Center. Perform a scan of Compute Engine instances. Publish results to Cloud Audit Logging. Create an alert in Cloud Monitoring to send notifications of suspect activities.

C. Enable Anomaly Detection in the Security Command Center. Create and configure a Pub/Sub topic and an email service. Create a Cloud Function to send email notifications for suspect activities. Export findings to a Pub/Sub topic, and use them to invoke the Cloud Function.

D. Enable the Web Security Scanner in the Security Command Center. Perform a scan of Compute Engine instances. Publish results to Cloud Audit Logging. Create an alert in Cloud Monitoring to send notifications for suspect activities.

Google Cloud

Feedback:
A. Incorrect. Event Threat Detection could be used, but the detectors are mismatched in this response. The correct detector to use is 'Cryptomining'. With the right detectors, a Pub/Sub topic could be used to invoke a Cloud Function to send a notification.

B. Incorrect. VM Manager is for vulnerability management. You need to provide threat management. Results cannot be written to Cloud Audit Logging.

C. Correct! You should enable Anomaly Detection in the Security Command Center. Use Pub/Sub topics to export the findings. Cloud Functions can then be used to send out any form of notification.

D. Incorrect. The Web Security Scanner supports vulnerability scans for web applications, including App Engine and Compute Engine, and for Google Kubernetes Engine clusters. Usage of Pub/Sub and Cloud Function for notification is correct.

Where to look:
- https://cloud.google.com/security-command-center/docs/concepts-security-sources#anomaly_detection
- https://cloud.google.com/security-command-center/docs/how-to-configure-security-command-center
- https://cloud.google.com/security-command-center/docs/how-to-enable-real-time-notifications

Content mapping:
- ILT course: **Security in Google Cloud**
    - M11 Monitoring, Logging, and Scanning

- On-demand course: **Mitigating Security Vulnerabilities in Google Cloud**
    - M3 Monitoring, Logging, and Scanning

Summary:
The Security Command Center offers built-in, integrated, and third-party services that you can use to scan for vulnerabilities and risks. As a threat reporting service, it measures all critical service, network, and infrastructure metrics and maps them to known security issues. The Security Command Center can probe and collect findings from the entire Google Cloud security suite.

4.2 | Configuring logging, monitoring, and detection

Courses

 Security in Google Cloud

M11 Monitoring, Logging, Auditing, and Scanning

 Mitigating Security Vulnerabilities in Google Cloud

M3 Monitoring, Logging, Auditing, and Scanning

Documentation

Security controls and forensic analysis for GKE apps | Cloud Architecture Center

Scenarios for exporting logging data: Security and access analytics | Cloud Architecture Center | Google Cloud

Security controls and forensic analysis for GKE apps | Cloud Architecture Center

Cloud Audit Logs overview

Cloud Audit Logs with Cloud Storage | Google Cloud

Configure Data Access audit logs

Scenarios for exporting Cloud Logging: Compliance requirements | Cloud Architecture Center | Google Cloud

Security sources for vulnerabilities and threats | Security Command Center | Google Cloud

Configuring Security Command Center

Enabling real-time email and chat notifications

Let's take a moment to consider resources that can help you build your knowledge and skills in this area.

The concepts in the diagnostic questions we just reviewed are covered in these modules and in this documentation. Reviewing the documentation is highly recommended. You'll find this list in your workbook so you can take a note of what you want to include later when you build your study plan. Based on your experience with the diagnostic questions, you may want to include some or all of these.

- https://cloud.google.com/architecture/security-controls-and-forensic-analysis-for-GKE-apps#using_analytical_tooling_for_forensic_analysis_of_containers
- https://cloud.google.com/architecture/exporting-stackdriver-logging-for-security-and-access-analytics
- https://cloud.google.com/architecture/security-controls-and-forensic-analysis-for-GKE-apps#using_automated_event_detection
- https://cloud.google.com/logging/docs/audit
- https://cloud.google.com/storage/docs/audit-logging
- https://cloud.google.com/logging/docs/audit/configure-data-access
- https://cloud.google.com/architecture/exporting-stackdriver-logging-for-compliance-requirements
- https://cloud.google.com/security-command-center/docs/concepts-security-sources#anomaly_detection
- https://cloud.google.com/security-command-center/docs/how-to-configure-security-command-center

- https://cloud.google.com/security-command-center/docs/how-to-enable-real-time-notifications