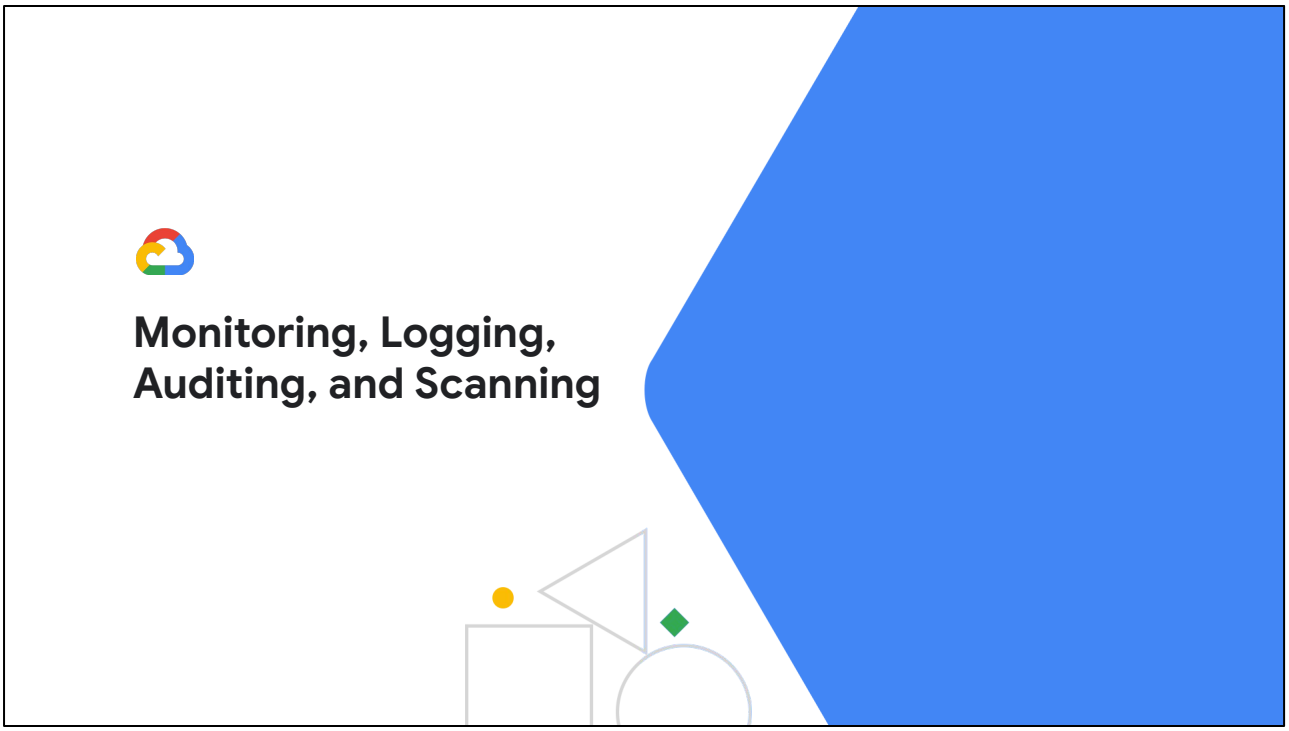


Welcome to the Monitoring, Logging, Auditing, and Scanning module.

Module overview

Security Command Center

Cloud Monitoring and Cloud Logging

Lab: Configuring and Using Cloud Monitoring and Cloud Logging

Cloud Audit Logs

Lab: Configuring and Viewing Cloud Audit Logs

Cloud security automation

Quiz and Module review

Bonus labs

In this module we will investigate the Security Command Center, then move into Cloud Monitoring and Logging, Cloud Audit logs, and then dive in cloud security automation concepts.

We will also give you a chance to practice these concepts.

Monitoring, Logging, Auditing, and Scanning

Security Command Center

Cloud Monitoring and Cloud Logging

Lab: Configuring and Using Cloud Monitoring and Cloud Logging

Cloud Audit Logs

Lab: Configuring and Viewing Cloud Audit Logs

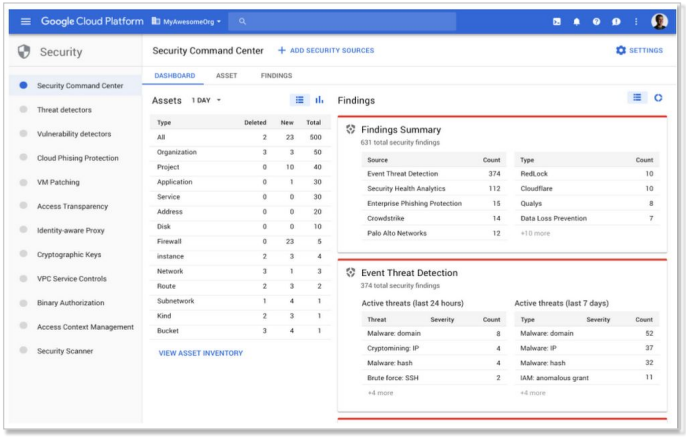
Cloud security automation

Quiz and Module review

Bonus labs

Now, let's learn about the Google Cloud Security Command Center and what it can do to help you discover, mitigate, and prevent attacks on your applications and data.

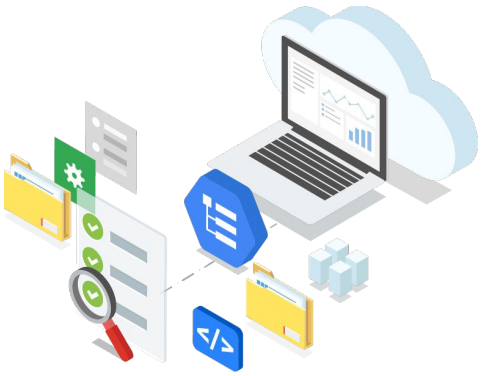
Security Command Center provides a centralized view for cloud resources



Security Command Center provides a single, centralized dashboard so you can view and monitor an inventory of your cloud assets.

Security Command Center helps you prevent, detect, and respond to threats

- Gives centralized visibility into your cloud resources.
- Uncovers machines that are being used for malicious purposes.
- Integrates with both Google and third-party security tools.
- Helps meet compliance requirements.



Security Command Center gives enterprises consolidated visibility into their Google Cloud assets across their organization. Using Security Command Center, you can quickly see:

- The number of projects you have
- What resources are deployed
- Where sensitive data is located
- How firewalls rules are configured

With ongoing discovery scans, enterprises can view asset history to understand exactly what changed in their environment and act on unauthorized modifications.

Anomaly detection from Google, which is integrated with Security Command Center, identifies threats like botnets, cryptocurrency mining, anomalous reboots, and suspicious network traffic. When a threat is detected, Event Threat Detection (also integrated with Security Command Center) surfaces that information so you can quickly take corrective action.

Security Command Center also integrates with Google Cloud security tools like Web Security Scanner and Cloud Data Loss Prevention (Cloud DLP), and even third-party security solutions like:

- Chef
- Cloudflare

- CloudQuest
- McAfee
- Qualys
- Reblaze
- Redlock by Palo Alto Networks
- StackRox
- Tenable.io
- And several others

Google Cloud security accepts feeds from these third-party security solutions so you can include them into your existing systems and workflows.

To help meet compliance requirements, use the Cloud Data Loss Prevention API, integrated with Security Command Center. It scans and reports on which storage buckets contain vulnerable data, such as personally identifiable information (PII). Whenever threats are found, you can get real time alerts triggered by Pub/Sub, which sends pertinent information to Gmail or SMS so quick action can be taken to protect your information.

Security Command Center works by generating “findings” associated with assets

- Security Command Center scans for assets at least once a day.
- Dashboard displays any findings (possible security risks).
- Findings come from Google Cloud, third-party solutions, or other security detectors.

Assets are resources like organization, projects, instances, data, services, and applications. Security Command Center discovers your assets across your organization so you can view them in one place. You can even review historical discovery scans to identify new, modified, or deleted assets.

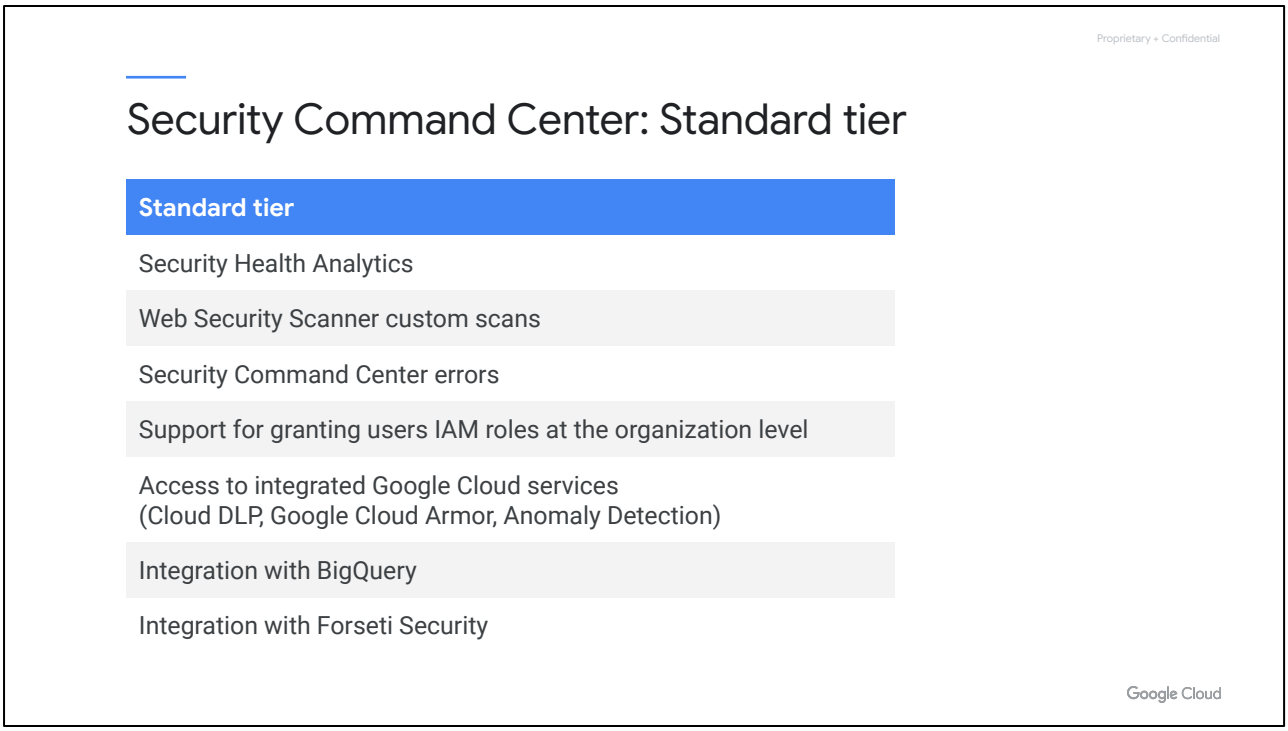
Findings can be viewed by type, by resource, or by findings changed - that is, findings whose status or properties have changed during the selected time period. Finding “freshness” in the Security Command Center dashboard is usually less than one minute after ingestion from the finding source. Assets that haven't been discovered and indexed in an automatic or manual scan will usually appear in the findings inventory within 1 minute after discovery.

Security Command Center can display findings from third-party security sources that have registered as a Google Cloud Marketplace partner. If your third-party security source isn’t on the partner list, you can request that they complete onboarding as a Security Command Center partner. To add a new third-party security source to Security Command Center, you will first need to set up the security source, and then enable it in the Security Command Center dashboard.

Security Command Center requires two IAM administrative permissions to set up

- **Organization Administrator** role - roles/resourcemanager.organizationAdmin
- **Security Center Admin** role - roles/securitycenter.admin

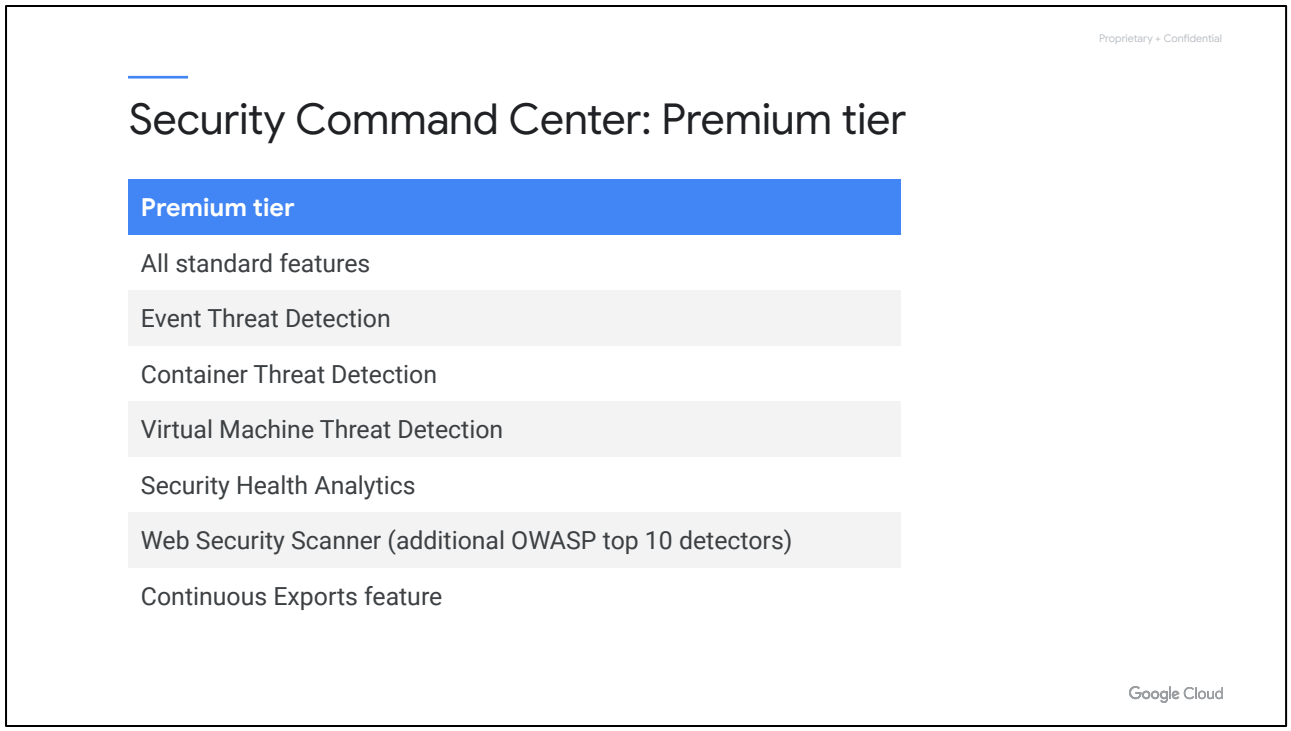
You will also need to enable the Security Command Center dashboard, asset discovery, and the security scanners you're using as security sources.



Security Command Center offers two different tiers: standard and premium.

The standard version offers:

- **Security Health Analytics:** which provides managed vulnerability assessment scanning for Google Cloud that can automatically detect the highest severity vulnerabilities and misconfigurations for your Google Cloud assets
- **Web Security Scanner custom scans:** in the standard tier, Web Security Scanner supports custom scans of deployed applications with public URLs and IP addresses that aren't behind a firewall.
- **Security Command Center errors:** Security Command Center provides detection and remediation guidance for configuration errors that prevent Security Command Center and its services from functioning properly.
- **Support for granting users Identity and Access Management (IAM) roles at the organization level**
- **Access to integrated Google Cloud services**: including Cloud Data Loss Prevention, Google Cloud Armor, and Anomaly Detection.
- **Integration with BigQuery:** which exports findings to BigQuery for analysis.
- **Integration with Forseti Security:** the open source security toolkit for Google Cloud, and third-party security information and event management (SIEM) applications.



The premium tier includes all Standard tier features and adds:

- **Event Threat Detection:** which monitors your organization's Cloud Logging and Google Workspace.
- **Container Threat Detection:** which detects the container runtime attacks.
- **Virtual Machine Threat Detection** which detects cryptocurrency mining applications running inside VM instances.
- **Security Health Analytics:** the premium tier includes managed vulnerability scans for all Security Health Analytics detectors (140+) and provides monitoring for many industry best practices, and compliance monitoring across your Google Cloud assets.
- **Web Security Scanner:** in the Premium tier includes all Standard tier features and additional detectors that support categories in the OWASP Top Ten.
- **Continuous Exports feature:** which automatically manages the export of new findings to Pub/Sub.

For more information on the difference between the two tiers, check out the documentation link in the speaker notes of this module.

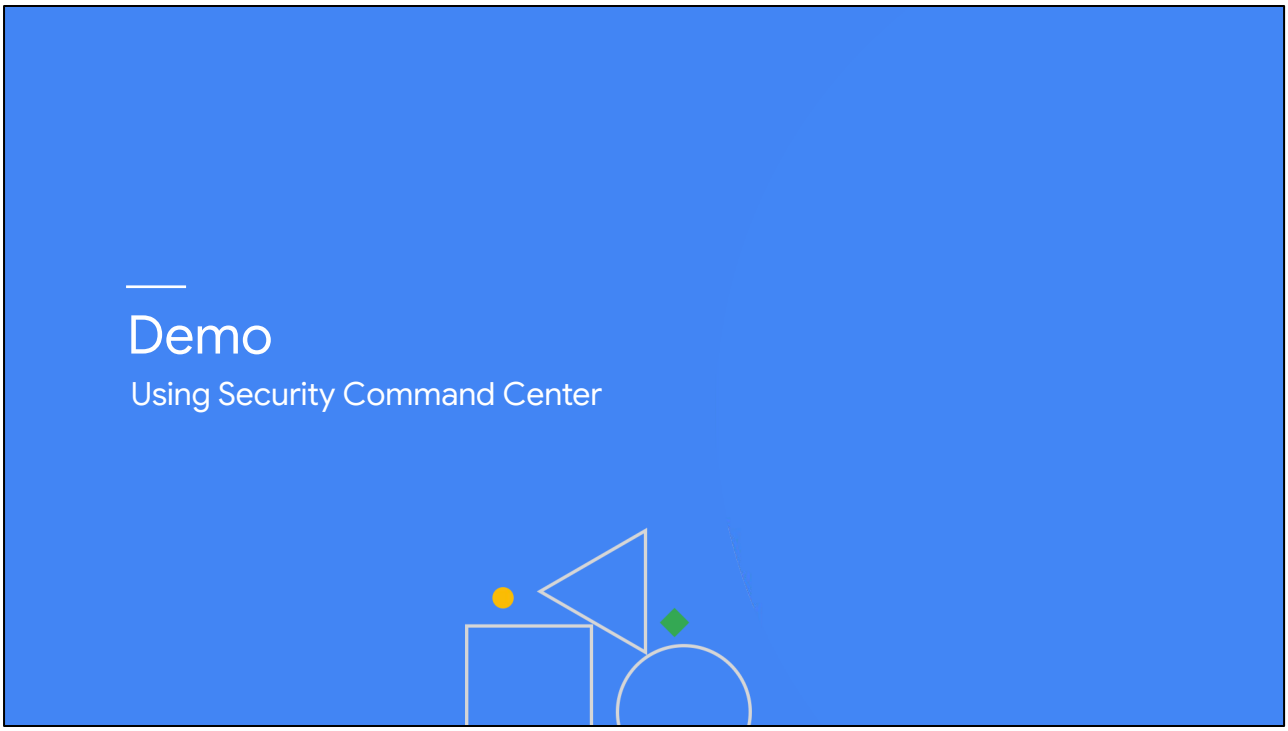
- **Link:** cloud.google.com/security-command-center/pricing

Security Command Center prices vary

- Any costs associated with the Security Command Center tier.
- Any costs associated with additional paid scanners (Cloud DLP, third-party partner).
- Any App Engine costs associated with using Web Security Scanner.

When you use Security Command Center Premium or Standard tier, you might be charged for the following:

- Any costs associated with the Security Command Center tier you select.
- Any costs associated with additional paid scanners like Cloud Data Loss Prevention (Cloud DLP) or a third-party partner scanner to add data to Security Command Center. You will be billed by the scanner provider based on their usage fees.
- Any App Engine costs associated with using Web Security Scanner.



This demo shows how to use the security command center.

https://storage.googleapis.com/cloud-training/gcpsec/v3.x/en/labs/Demo_using_security_command_center.mp4

Monitoring, Logging, Auditing, and Scanning

Security Command Center

Cloud Monitoring and Cloud Logging

Lab: Configuring and Using Cloud Monitoring and Cloud Logging

Cloud Audit Logs

Lab: Configuring and Viewing Cloud Audit Logs

Cloud security automation

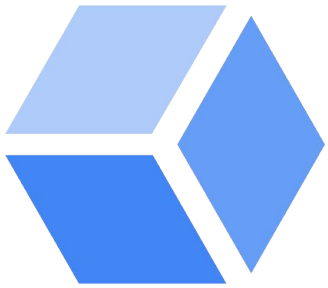
Quiz and Module review

Bonus labs

Now, let's learn about Cloud Monitoring and Cloud Logging - formerly Stackdriver Monitoring and Stackdriver Logging - to see how you can monitor, troubleshoot, and improve application performance on your Google Cloud environment.

Google Cloud's operations suite

- Integrated monitoring, logging, diagnostics.
- Manages across platforms.



Google Cloud's operations suite consists of multi-cloud monitoring and management products that aggregate metrics, logs, and events.

It provides developers, operators, and security professionals a rich set of observable signals that speed root-cause analysis and reduce mean time to resolution.

An effective incident response includes...

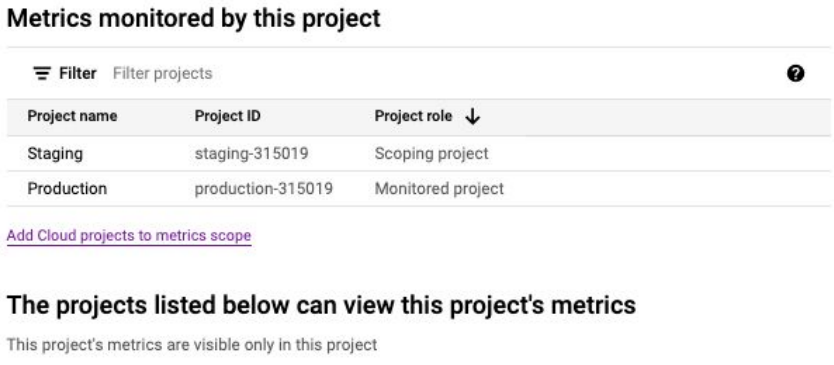
Monitoring dashboard

Alerting regimen

Plans and tools for responding to issues

An effective incident response requires effective tools, such as monitoring dashboards, robust alerting mechanisms, and plans and tools for responding to actual events and issues when they occur.

Metrics scope defines the set projects whose metrics can be accessed



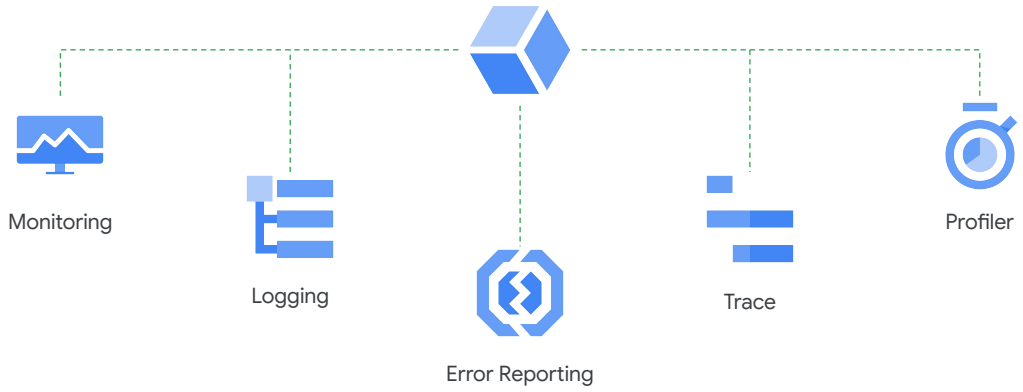
By default, a Google Cloud project has visibility only to the metrics it stores. However, you can expand the set of metrics that a project can access by adding other Google Cloud projects to the project's metrics scope.

The metrics scope defines the set of Google Cloud projects whose metrics the current Google Cloud project can access.

A scoping project hosts a metrics scope. Because every Google Cloud project hosts a metrics scope, every project is also a scoping project.

The scoping project stores information about its metrics scope. It also stores the alerts, uptime checks, dashboards, and monitoring groups that you configure for the metrics scope. You can identify the scoping project for a metrics scope as the project selected by the console project picker.

Multiple integrated products



Google Cloud's operations suite provides performance and diagnostics data, in the form of monitoring, logging, tracing, error reporting, and alerting.

This suite of products comprises Cloud Monitoring, Cloud Debugger, Cloud Logging, Cloud Trace, Cloud Profiler, and Error Reporting. These diagnostics features are well-integrated with each other. This helps you connect and correlate diagnostics data easily.

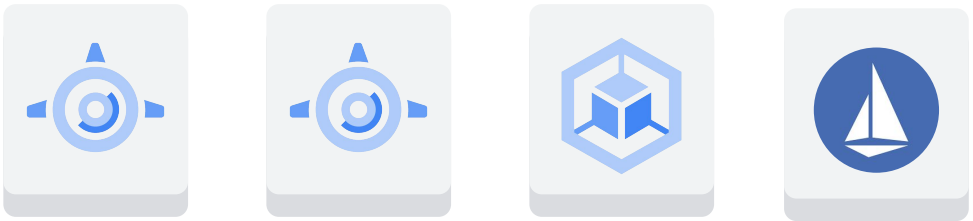
Monitoring

- Platform, system, and app metrics
- Uptime/health checks
- Dashboards
- Alerts

Cloud Monitoring helps increase reliability by giving users the ability to monitor Google Cloud and multi-cloud environments and identify trends to prevent issues. With Cloud Monitoring, you can reduce monitoring overhead and noise to fix problems faster.

Cloud Monitoring enables you to monitor your platform, system, and application metrics. You ingest data into Cloud Logging and you can create different metrics, custom events, monitor for specific metadata changes. You can also monitor and measure uptime and health checks, build custom dashboards and create alerts to perform notifications.

Built-in monitoring



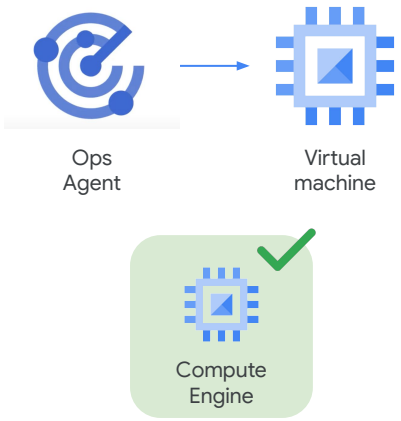
Google Cloud's operations suite includes monitoring for App Engine flexible environment and App Engine standard environment, as well as Google Kubernetes Engine and Istio.

Istio is an open source independent service mesh. It reduces complexity of managing microservice deployments by providing a uniform way to secure, connect, and monitor microservices. It optimizes the communication between microservices within a deployment.

After a Cloud Workspace is created, you can immediately head to the Metrics Explorer and start visualizing those metrics from Istio.

Ops Agent

- Primary agent for collecting telemetry from your Compute Engine instances.
- Monitor your VM instances without the need for any additional configuration after the install.
- Gain visibility into CPU, disk, and network performance.
- Unify gathering of metrics and logs into a single agent.
- Replaces the legacy Logging and Monitoring agents Google Cloud offered.



For other services without Cloud Monitoring built in, such as Compute Engine, there is an agent that can be installed.

The Ops Agent is the primary agent for collecting telemetry from your Compute Engine instances. Combining logging and metrics into a single agent, the Ops Agent allows you to:

- Monitor your VM instances without the need for any additional configuration after the install.
- Gain visibility into CPU, disk, and network performance.
- Unify gathering of metrics and logs into a single agent.

This replaces the legacy Logging and Monitoring agents Google Cloud offered.

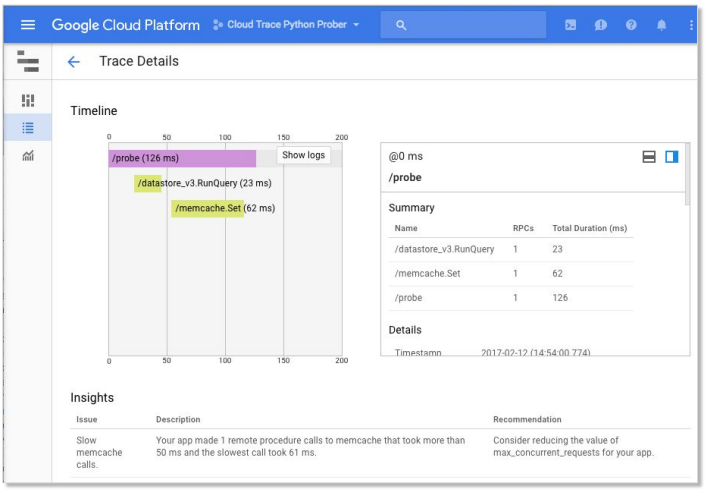
Monitoring third-party applications

- Apache web server
- Cassandra
- CouchDB
- Elasticsearch
- HBase
- JVM Monitoring
- Kafka
- Memcached
- MongoDB
- MySQL
- Nginx
- PostgreSQL
- RabbitMQ
- Redis
- Riak StatsD
- Tomcat
- Varnish
- ZooKeeper

The monitoring agents can be configured to monitor popular third-party applications, which are highlighted on this slide. Monitoring agents on VM instances can transmit data for various metric types for these applications. These metrics can be used in charting or alerting within the workspace.

Trace

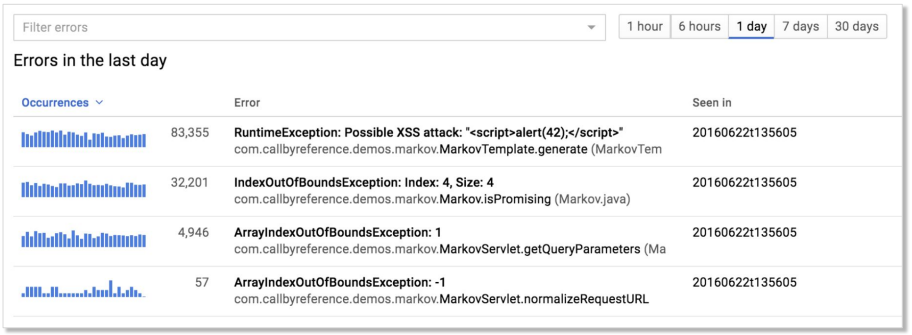
- Latency reporting
- Per-URL latency sampling



Cloud Trace provides latency sampling and reporting for Google App Engine, including per-URL statistics and latency distributions.

Error Reporting

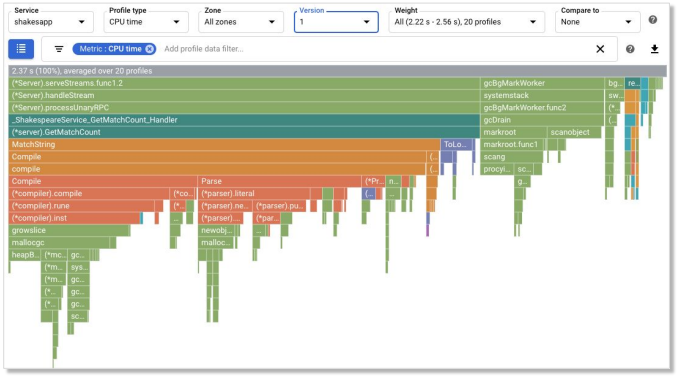
- Error notifications
- Error dashboard



Error Reporting analyzes and aggregates the errors in your cloud applications and notifies you when new errors are detected.

Profiler

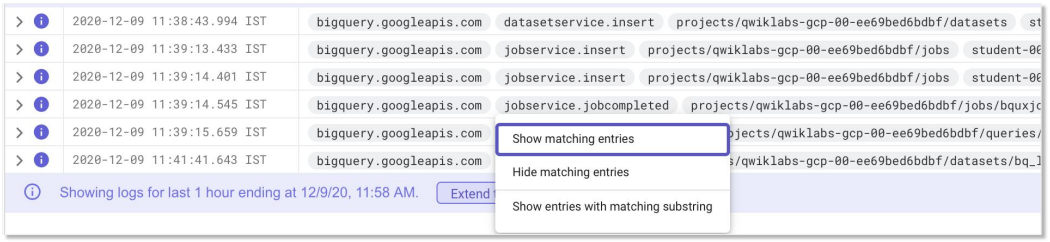
- Continuous CPU and heap profiling
- Broad platform support



Cloud Profiler provides continuous profiling of resource consumption in your production applications, helping you identify and eliminate potential performance issues.

Logging

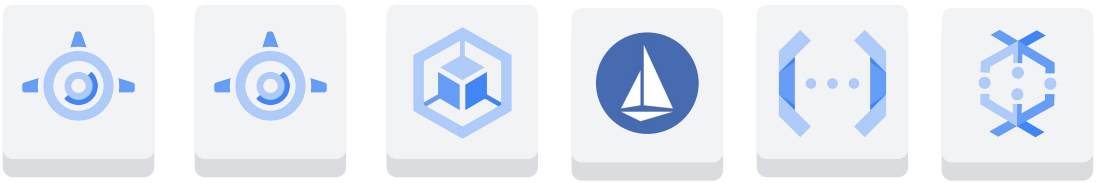
- Platform, system, and app logs
- Log search/view/filter
- Logs-based metrics



Cloud Logging lets you manage and analyze log data from Google Cloud as well as AWS in one place.

You can combine the power of Cloud Logging with Google Cloud's data and analytics products for advanced, real-time log analysis. For example, you can create powerful real-time metrics from the log data and analyze log data in real time in BigQuery.

Cloud Logging is preconfigured in many environments



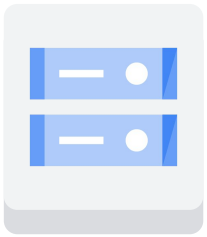
Most Google Cloud services have Cloud Logging built in, such as App Engine Flexible and Standard Environments, Kubernetes, Istio, Cloud Functions, and Dataflow. Using Cloud Logging in a preconfigured environment is very straightforward. For example, to emit a log line from a Cloud Function, write to standard output or standard error. There is no special logging framework or API required.

Log retention

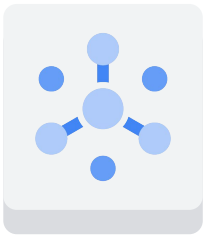
- Cloud Logging stores logs for a limited number of days.
- You can export logs for analysis or longer storage.

Cloud Logging retains the logs for a limited number days. The number of days depends on the type of log. For example, Admin Activity audit logs are kept for 400 days while Data Access audit logs are only kept for 30 days.

Exporting logs



Cloud Storage



Pub/Sub

BigQuery

For longer storage or analysis, logs can be exported to Cloud Storage, Pub/Sub, or BigQuery and then stored indefinitely.

Analyzing logs

- Advanced logs filters
- BigQuery
- Third-party analysis tools

When you export logs to a BigQuery dataset, Cloud Logging creates dated tables to hold the exported log entries. Log entries are placed in tables whose names are based on the entries' log names.

Monitoring, Logging, Auditing, and Scanning

Security Command Center

Cloud Monitoring and Cloud Logging

Lab: Configuring and Using Cloud Monitoring and Cloud Logging

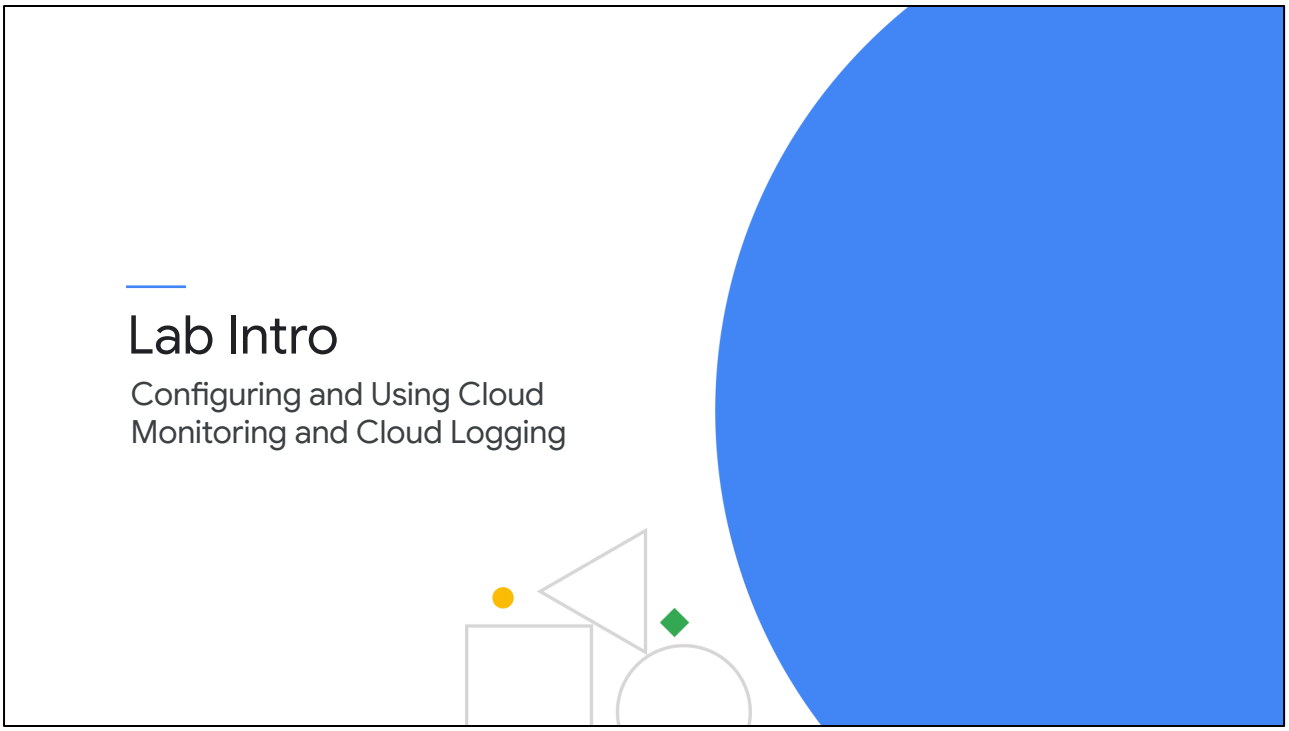
Cloud Audit Logs

Lab: Configuring and Viewing Cloud Audit Logs

Cloud security automation

Quiz and Module review

Bonus labs



In this lab, you learn how to view logs using a variety of filtering mechanisms, exclude log entries and disable log ingestion, and export logs and run reports against exported logs. You also learn to create and report on logging metrics, create an account used to monitor several Google Cloud projects, create a metrics dashboard, and to create and use an alerting policy.

Monitoring, Logging, Auditing, and Scanning

Security Command Center

Cloud Monitoring and Cloud Logging

Lab: Configuring and Using Cloud Monitoring and Cloud Logging

Cloud Audit Logs

Lab: Configuring and Viewing Cloud Audit Logs

Cloud security automation

Quiz and Module review

Bonus labs

Cloud Audit Logs maintains audit logs for each project, folder, and organization. Having an audit trail of all operations performed within your environment is very important. In this section, we will explore how to use Cloud Audit Logs.

Cloud Audit Logs

Who

did what

where and when

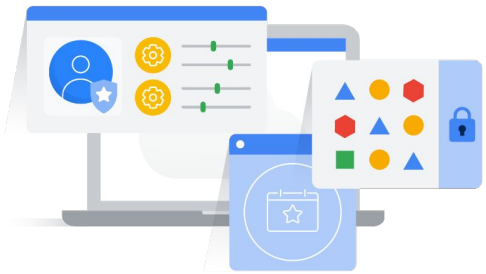
Cloud Audit Logs records Google Cloud account activity, including actions performed with the Google Cloud Console, command line tools, APIs, and AWS services.

Cloud Audit Logs helps you answer the questions of: Who did what, where, and when within your Google Cloud projects.

Cloud Audit Logs

Cloud Audit Logs maintains four audit logs:

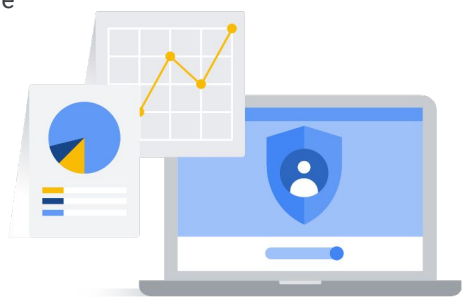
- Admin Activity
- System Events
- Data Access
- Policy Denied



Cloud Audit Logs maintains four audit logs for each project, folder, and organization: Admin Activity logs, System Events, Data Access logs, and Policy Denied logs.

Admin Activity audit logs

- Record administrative actions that modify the configuration or metadata of resources.
- Always enabled.

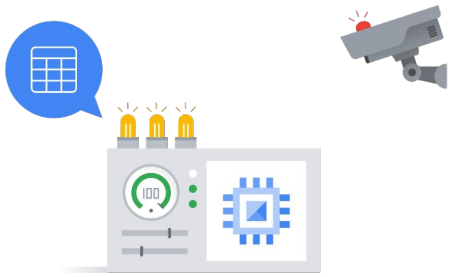


Admin Activity audit logs contain log entries for API calls or other administrative actions that modify the configuration or metadata of resources. For example, the logs record when VM instances and App Engine applications are created and when permissions are changed.

Admin Activity audit logs are always enabled by default and there is no charge for your Admin Activity audit logs.

System Event audit logs

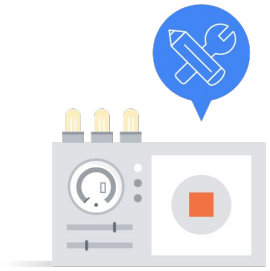
- Record when Compute Engine performs a system event.
- Always enabled.



System Event audit logs contain log entries for when Compute Engine performs a system event. For example, each live migration is recorded as a system event. System Event audit logs are always enabled and there is no charge for your System Event audit logs.

Data Access audit logs

- API calls that create, modify, or read user-provided data.
- Disabled by default.



Data Access audit logs record API calls that create, modify, or read user-provided data. These logs are disabled by default because they can be quite large. Enabling the logs might result in your project being charged for the additional logs usage.

Note that Data Access audit logs do not record data-access operations on resources that are publicly shared.

Policy Denied audit logs

- Recorded when a Google Cloud service denies access to a user or service account because of a security policy violation.
- Generated by default.

Policy Denied audit logs are recorded when a Google Cloud service denies access to a user or service account because of a security policy violation.

Policy Denied audit logs are generated by default and your Cloud project is charged for the logs storage. You can't disable Policy Denied audit logs, but you can use exclusion filters to prevent Policy Denied audit logs from being ingested and stored in Cloud Logging.

BigQuery Data Access audit logs

- Handled differently from other Data Access logs.
- Always enabled.

BigQuery Data Access audit logs are handled differently from other Data Access logs. BigQuery logs are enabled by default and cannot be disabled.

Viewing audit logs

Log can be viewed in:

- Project's Activity page
- Cloud Logging
- Cloud Logging API
- Cloud SDK

You can view audit log entries in your project's Activity page, in the Logs Explorer, in the Cloud Logging API, and in the Cloud SDK. You can also export audit log entries to Cloud Logging, Pub/Sub, or Cloud Storage.

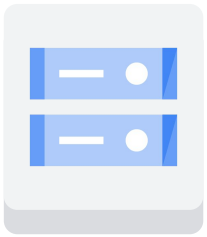
To view the logs, you must have the IAM roles Logging/Logs Viewer for Admin Activity logs and Logging/Private Logs Viewer for Data Access logs. For more information on Cloud Logging roles, see Access Control.

Audit Log retention

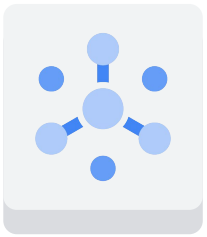
Audit log type	Retention period
Admin Activity	400 days
System Events	400 days
Data Access	30 days

Individual audit log entries are kept for a specified length of time and are then deleted. Admin activity and system events are kept for 400 days, while data access logs are kept for 30 days. For longer retention, you can export audit log entries from Cloud Logging and keep them for as long as you wish.

Exporting Audit Logs



Cloud Storage



Pub/Sub

BigQuery

Just like other logs, you can also export audit log entries to Cloud Storage, Pub/Sub, or BigQuery.

Analyzing Audit Logs

- Advanced logs filters
- BigQuery
- Third-party analysis tools

When exporting logs, log filters can be defined to limit which log events are exported. This can help reduce the amount of data exported and reduce the scope of the data.

When you export to BigQuery datasets, Cloud Logging creates dated tables to hold the exported log entries. The data can then be analyzed using BigQuery.

Log files can also be exported to Pub/Sub and to storage buckets, which facilitates analyzing the data with third-party tools.

Monitoring, Logging, Auditing, and Scanning

Security Command Center

Cloud Monitoring and Cloud Logging

Lab: Configuring and Using Cloud Monitoring and Cloud Logging

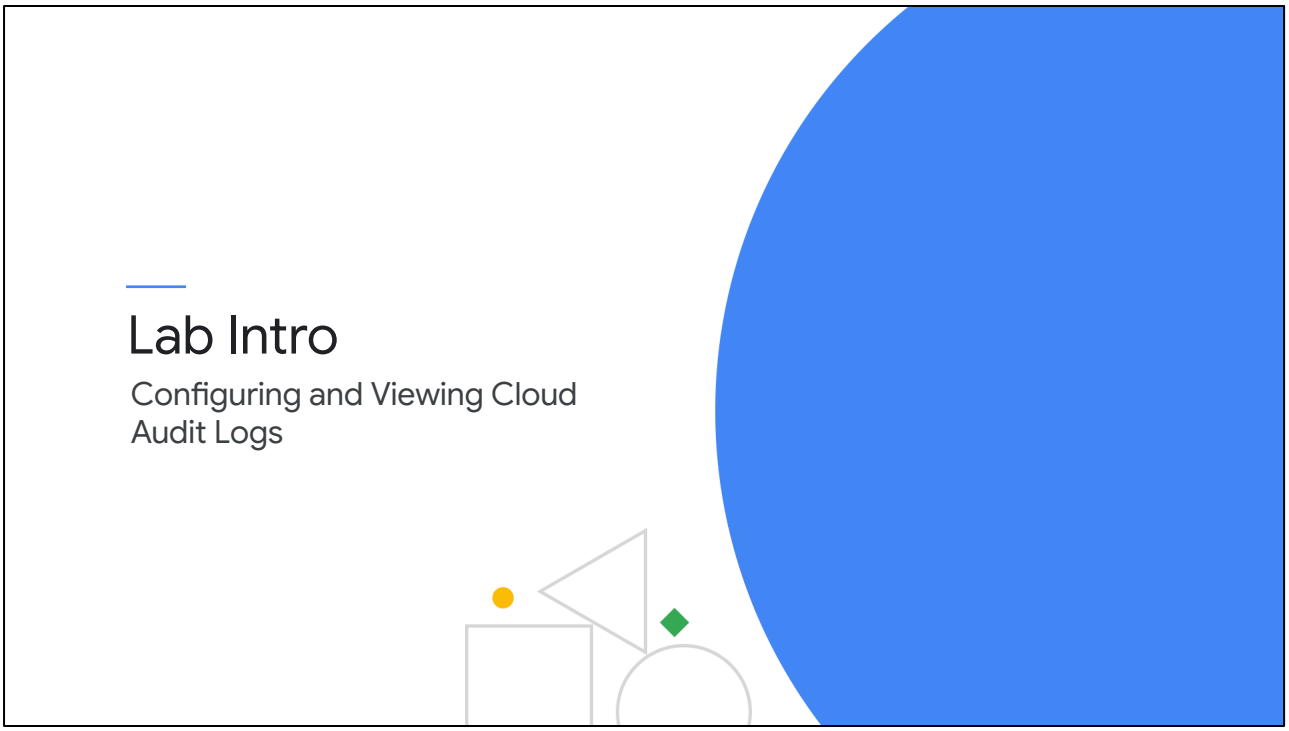
Cloud Audit Logs

Lab: Configuring and Viewing Cloud Audit Logs

Cloud security automation

Quiz and Module review

Bonus labs



In this lab, you learn how to view Cloud Audit Logs in the Activity page, view and filter audit logs, retrieve log entries using the gcloud command, and export Cloud Audit Logs.

Monitoring, Logging, Auditing, and Scanning

Security Command Center

Cloud Monitoring and Cloud Logging

Lab: Configuring and Using Cloud Monitoring and Cloud Logging

Cloud Audit Logs

Lab: Configuring and Viewing Cloud Audit Logs

Cloud security automation

Quiz and Module review

Bonus labs

Now, let's go over some Security automation techniques and best practices.

Security automation benefits

- Improves consistency, quickness, and reliability.
- Once you have encapsulated some task in automation, anyone can execute the task.
- Allows scaling faster than the growth of threats and assets.

Whether you're a security engineer, an analyst, an incident responder, or an architect – creative ways to automate operations (starting with the mundane tasks first) can be a force multiplier that can reduce the burden of operations on your team.

The key benefits of automating security operations revolves around factors of consistency, quickness, and reliability.

Another benefit that is sometimes overlooked is that once you have encapsulated some task in automation, anyone can execute the task. This again gives us a chance to scale faster than the growth of threats and assets.

Security automation risks

- Automated responses can sometimes result in disastrous outcomes, if not planned correctly.
  - Example: production systems at a major technology companies deleted.
- Ensure you have:
  - Peer reviews
  - QA & testing
  - Highly descriptive playbooks
  - Other processes in place when developing automated responses.

There are a few risks in security automation to be aware of.

Automated responses can sometimes result in disastrous outcomes, if not planned correctly. This can happen in both IT operations and Security.

There are many examples where production systems at a major technology companies were deleted by automation. This is a possibility with automation, so it is important to have peer reviews, QA & testing, highly descriptive playbooks, and other processes in place when developing automated responses.

Security automation service examples

Security Command Center: automate the discovery off misconfigurations and vulnerabilities and detect threats targeting your Google Cloud assets.

Web Security Scanner: automates the testing of security vulnerabilities in your web applications by following links and exercising as many user inputs and event handlers as possible.

Artifact Registry: automatically detects risky images from being deployed to Google Kubernetes Engine.

You may not realize it, but you have already been exposed to security automation throughout this course.

Many of the services we have covered have security automation built in. Just a few examples are:

- **Security Command Center**, which automates the discovery of misconfigurations and vulnerabilities and detects threats targeting your Google Cloud assets.
- **Web Security Scanner,** automates the testing of security vulnerabilities in your web applications by following links and exercising as many user inputs and event handlers as possible.
- **Artifact Registry**, which ensures only approved container images can be deployed. Configure this automatic checkpoint to keep risky images from being deployed to Google Kubernetes Engine.

Can you think of other services you've learned about throughout this course that automate many of the tasks a Cloud Security Architect or Engineer are tasked with?

Monitoring, Logging, Auditing, and Scanning

Security Command Center

Cloud Monitoring and Cloud Logging

Lab: Configuring and Using Cloud Monitoring and Cloud Logging

Cloud Audit Logs

Lab: Configuring and Viewing Cloud Audit Logs

Cloud security automation

Quiz and Module review

Bonus labs

Quiz #1

Question

Which TWO of the following statements about Cloud Logging are TRUE?

A. You can analyze Cloud Logging log data in BigQuery.

B. The Cloud Logging Agent can be installed on both Compute Engine and AWS EC2 instances.

C. While Cloud Logging is not built in to most Google Cloud services, you can easily add it for a reasonable fee.

D. Cloud Logging retains logs for an indefinite period of time.

Quiz #1

Answer

Which TWO of the following statements about Cloud Logging are TRUE?

A. You can analyze Cloud Logging log data in BigQuery. 

B. The Cloud Logging Agent can be installed on both Compute Engine and AWS EC2 instances. 

C. While Cloud Logging is not built-in to most Google Cloud services, you can easily add it for a reasonable fee.

D. Cloud Logging retains logs for an indefinite period of time.

A. This feature allows you to create sophisticated log analysis reports.

B. This allows you to stream logs from third-party applications into Cloud Logging.

Quiz #2

Question

Which TWO of the following statements about Cloud Audit Logs are TRUE?

A. Enabling Data Access audit logs might result in your project being charged for the additional logs usage.

B. Unlike Cloud Logging logs, you cannot export Cloud Audit log entries to BigQuery.

C. Data Access audit logs record data-access operations on resources that are publicly shared.

D. Cloud Audit Logs maintains four audit logs for each project, folder, and organization.

Quiz #2

Answer

Which TWO of the following statements about Cloud Audit Logs are TRUE?

A. Enabling Data Access audit logs might result in your project being charged for the additional logs usage. ✓

B. Unlike Cloud Logging logs, you cannot export Cloud Audit log entries to BigQuery.

C. Data Access audit logs record data-access operations on resources that are publicly shared.

D. Cloud Audit Logs maintains four audit logs for each project, folder, and organization. ✓

A. These logs are disabled by default because they can become quite large and incur extra charges.

D. The four audit logs maintained are “Admin Activity audit logs”, “System Event audit logs”, “Data Access audit logs”, and “Policy Denied audit logs.”

Quiz #3

Question

Which ONE of the following statements about security automation is is NOT true?

A. Improves consistency, quickness, and reliability

B. Once you have encapsulated some task in automation, anyone can execute the task.

C. Allows scaling faster than the growth of threats and assets

D. You never have to maintain your automation systems once built

Quiz #3

Answer

Which ONE of the following statements about security automation is is NOT true?

A. Improves consistency, quickness, and reliability

B. Once you have encapsulated some task in automation, anyone can execute the task.

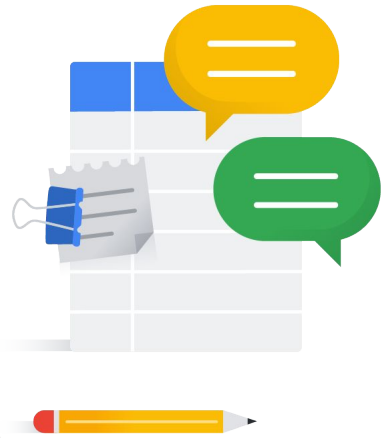
C. Allows scaling faster than the growth of threats and assets

D. You never have to maintain your automation systems once built 

D. You should regularly maintain, test, and audit your systems to ensure that they are reliable and keep your resources secure.

Module review

- **Security Command Center** provides a single, centralized dashboard for cloud resources. By generating 'findings' associated with assets, it helps you prevent, detect, and respond to threats.
- **Google Cloud's operations suite** has many integrated products that will help you monitor, troubleshoot, and improve application performance on your Google Cloud environment. Cloud Monitoring and Cloud Logging specifically, will help you strengthen user's trust.
- **Cloud Audit Logs** maintains audit logs for each project, folder, and organization. Having an audit trail of all operations performed within your environment is very important.



These are the main points covered in this module:

Security Command Center provides a single, centralized dashboard for cloud resources. By generating 'findings' associated with assets, it helps you prevent, detect, and respond to threats.

Google Cloud's operations suite has many integrated products that will help you monitor, troubleshoot, and improve application performance on your Google Cloud environment. Cloud Monitoring and Cloud Logging specifically, will help you strengthen user's trust.

Cloud Audit Logs maintains audit logs for each project, folder, and organization. Having an audit trail of all operations performed within your environment is very important.

Monitoring, Logging, Auditing, and Scanning

Security Command Center

Cloud Monitoring and Cloud Logging

Lab: Configuring and Using Cloud Monitoring and Cloud Logging

Cloud Audit Logs

Lab: Configuring and Viewing Cloud Audit Logs

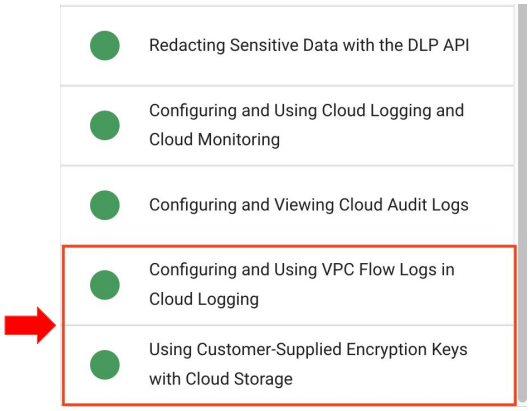
Cloud security automation

Quiz and Module review

Bonus labs

Optional bonus labs

- 2 optional bonus labs can be found in your classroom:
  - *Configuring and Using VPC Flow Logs in Cloud Logging*
  - *Using Customer-Supplied Encryption Keys with Cloud Storage*



If you are looking for more hands-on practice, we've created two bonus labs for you.

These labs dive into more depth in the topics covered in module 4 and module 6 and will teach you how to:

- Configure and Use VPC Flow Logs in Cloud Logging
- Use Customer-Supplied Encryption Keys with Cloud Storage

You can find these at the end of the list of labs in your classroom.


Google Cloud