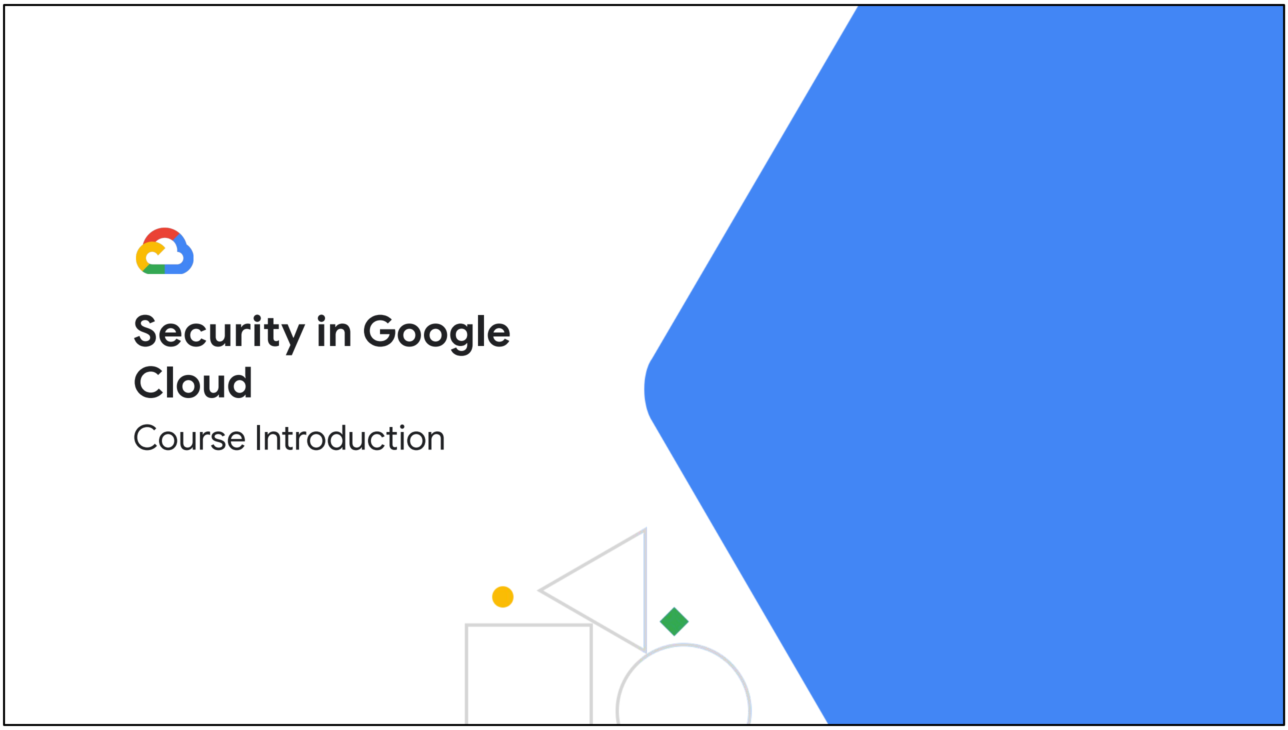
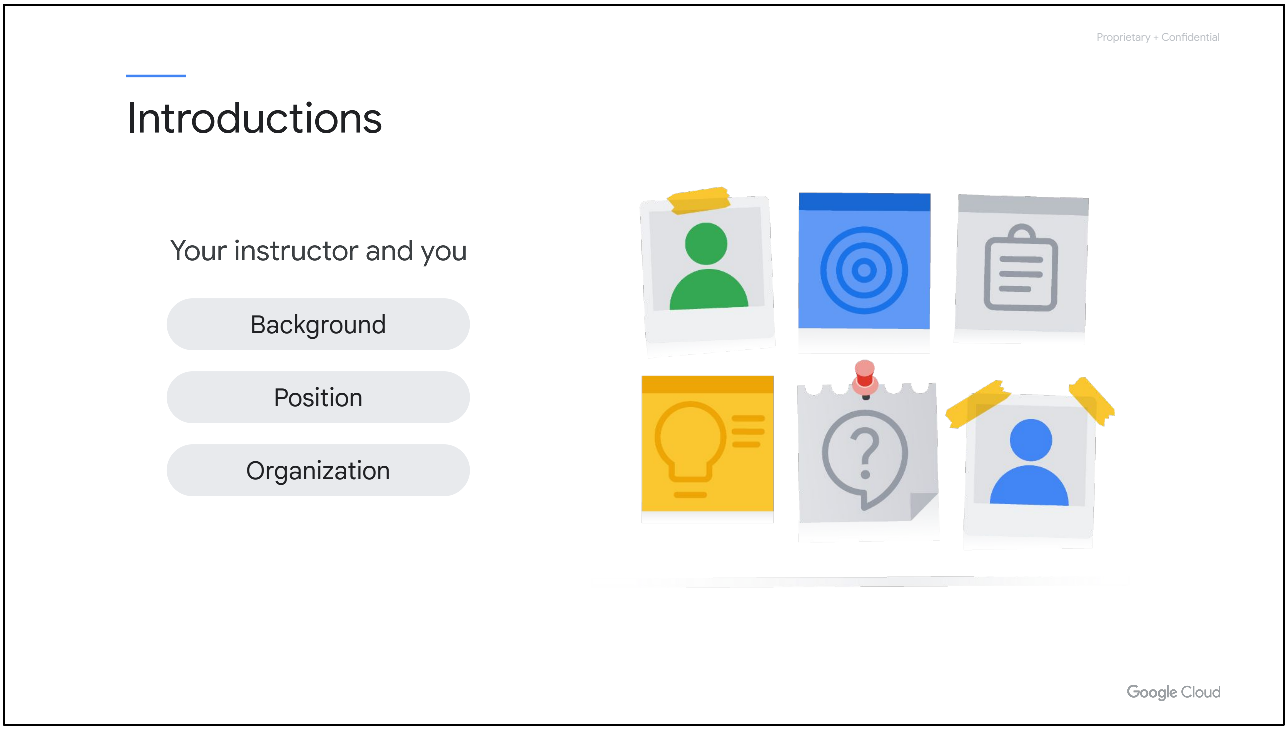


Security in Google Cloud

Course Introduction

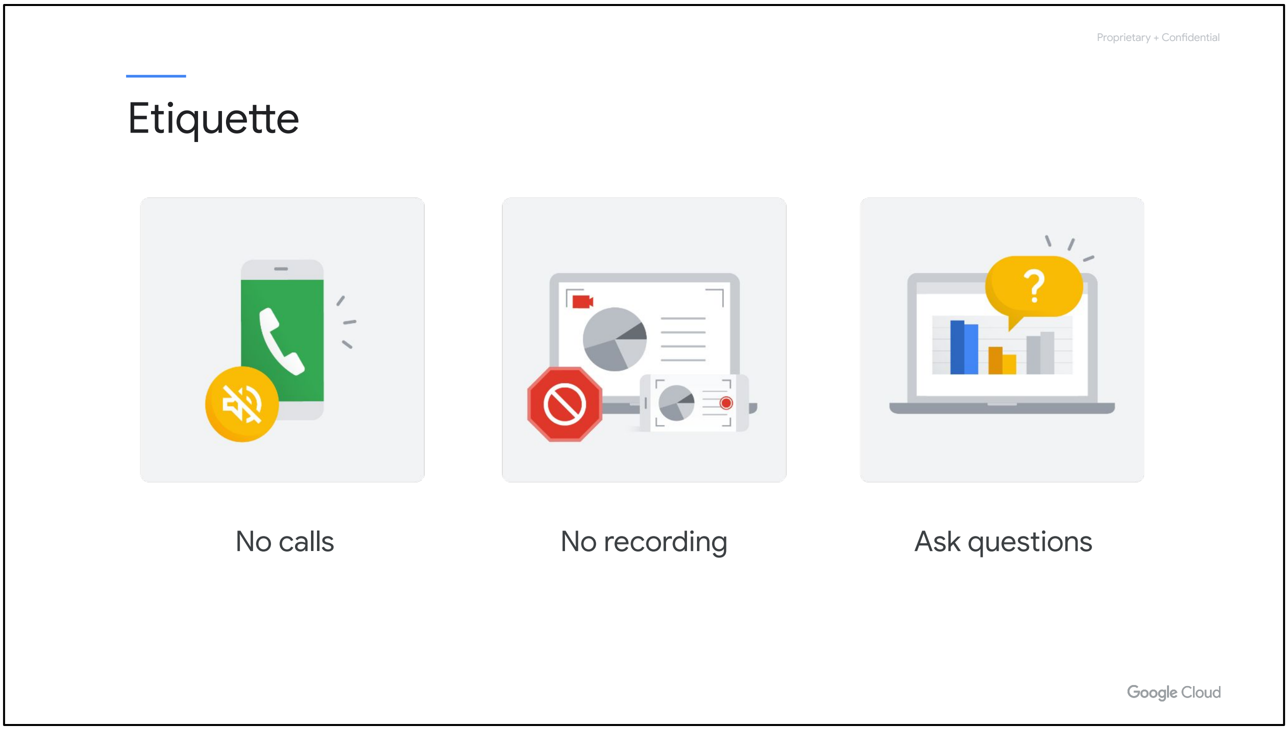
Hello and welcome to Security in Google Cloud.



Introductions

Your instructor and you

- Background
- Position
- Organization



Etiquette

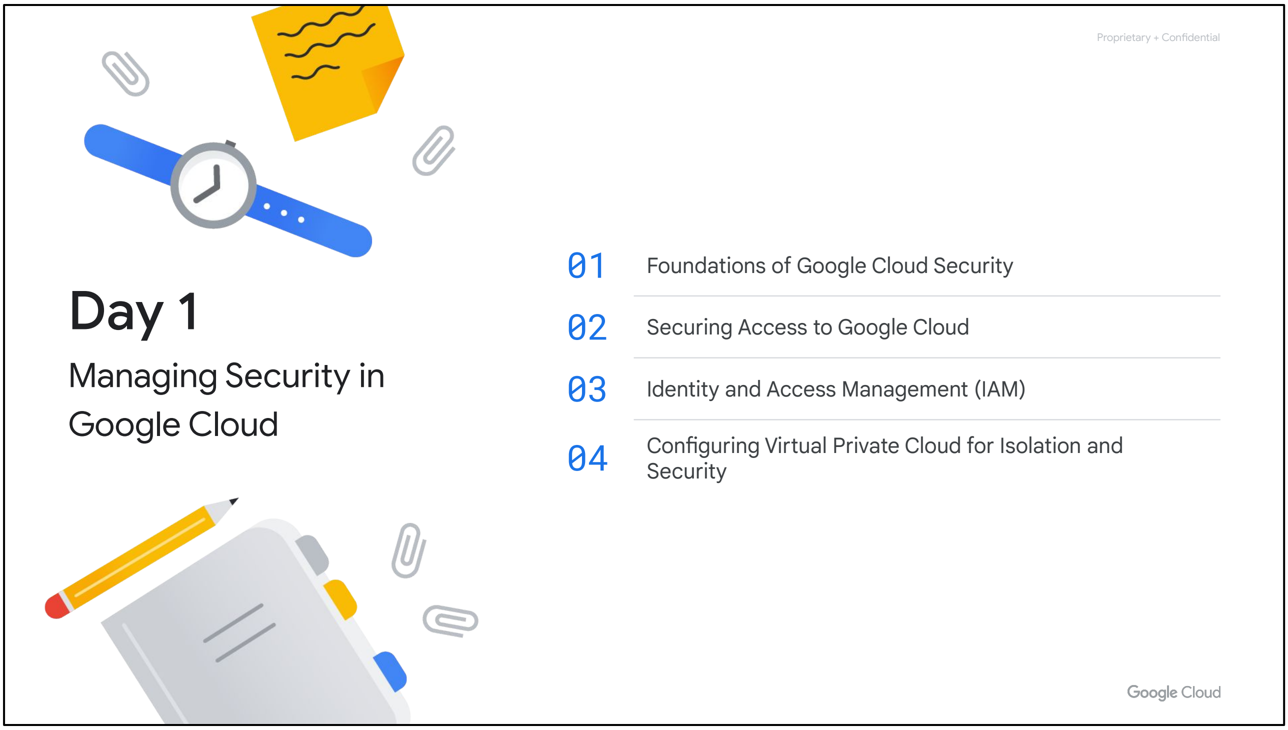
No calls

No recording

Ask questions

Course etiquette:

- Please silence your phone and take calls outside.
- Recording this class is prohibited.
- Ask questions interactively or via chat (online).



Proprietary + Confidential

Day 1

Managing Security in Google Cloud

01 Foundations of Google Cloud Security

02 Securing Access to Google Cloud

03 Identity and Access Management (IAM)

04 Configuring Virtual Private Cloud for Isolation and Security

Google Cloud

Each day of this 3-day course focuses on a different aspect of security in Google Cloud.

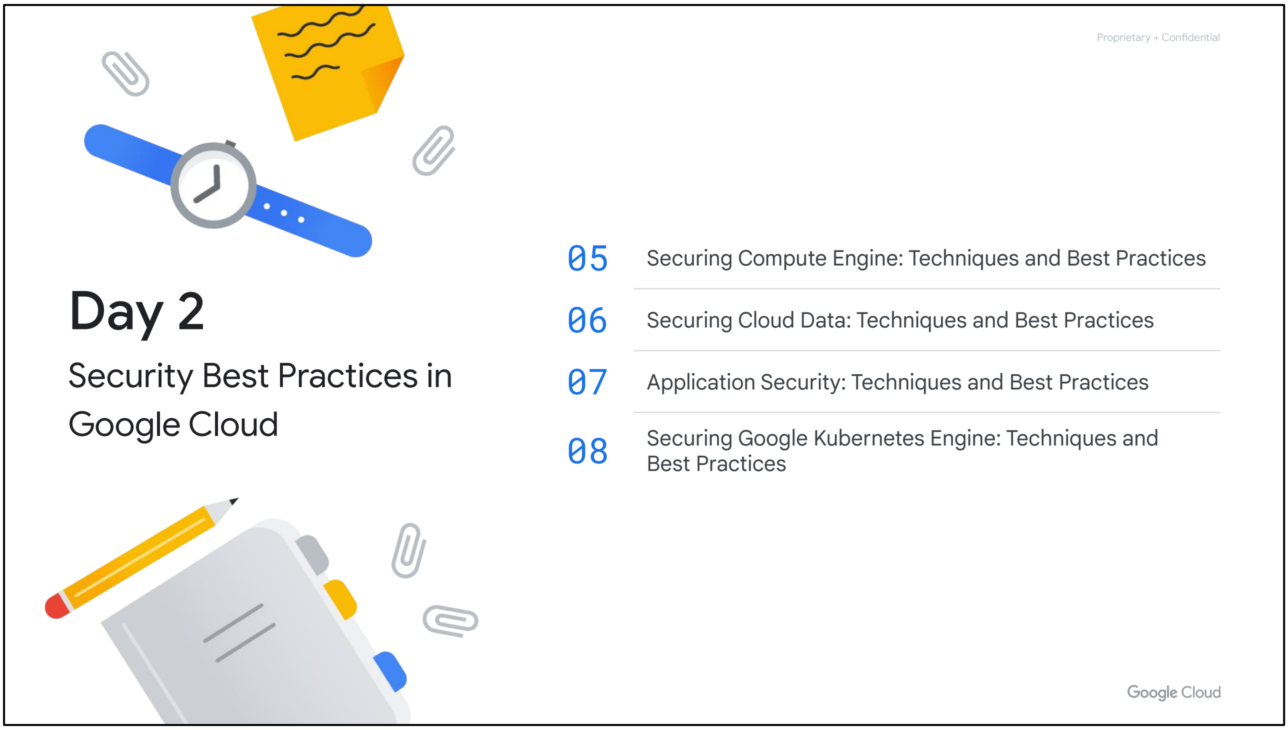
The focus of day 1 is managing security in Google Cloud.

In the **Foundations of Google Cloud Security** module, I will introduce you to Google Cloud's approach to security, the shared security responsibility model, the threats that are mitigated for you when your systems are run on Google's infrastructure in Google Cloud, and access transparency.

In **Securing Access to Google Cloud**, we will discuss how this service makes it easy to manage cloud users, devices, and apps from one console. We will also discuss a few related features to help reduce the operational overhead of managing Google Cloud users, such as the Google Cloud Directory Sync and Single Sign On. We will also highlight some authentication best practices.

We will then explore how Identity and Access Management (or IAM as it is known) lets administrators authorize who can take action on specific resources, giving you full control and visibility to manage your cloud resources centrally.

In the final module of Day 1, we will discuss many VPC related security concepts, including VPC firewalls, load balancing SSL policies, network interconnect and peering options, VPC network best practices and VPC flow logs.



Proprietary + Confidential

Day 2

Security Best Practices in Google Cloud

05	Securing Compute Engine: Techniques and Best Practices
06	Securing Cloud Data: Techniques and Best Practices
07	Application Security: Techniques and Best Practices
08	Securing Google Kubernetes Engine: Techniques and Best Practices

Google Cloud

The focus of day 2 is security best practices in Google Cloud.

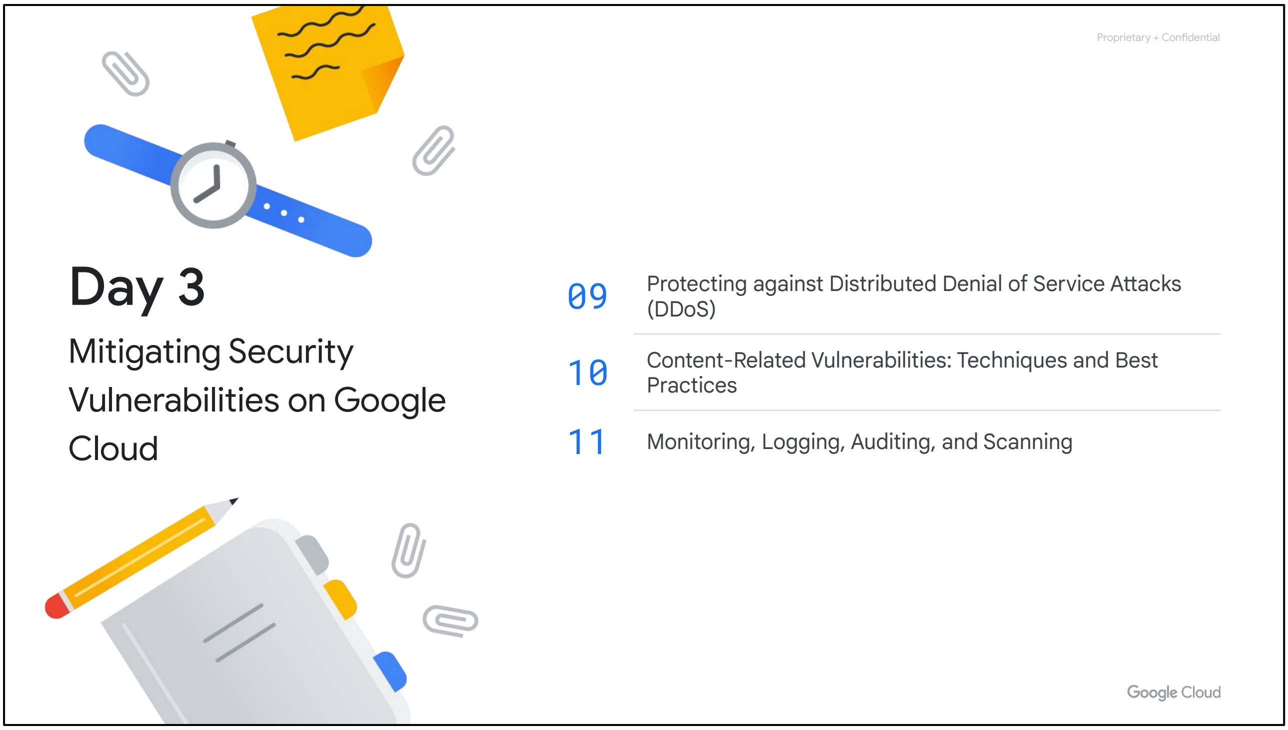
In the first module, we will start with a discussion of service accounts, IAM roles and API scopes as they apply to Compute Engine. We will also discuss managing VM logins and using shielded VMs, and how to use organization policies to set constraints that apply to all resources in your organization's hierarchy. We will also review Compute Engine best practices to give you some tips for securing Compute Engine.

Securing your cloud data is obviously extremely important. In the Securing Cloud Data module, we are going to cover many topics related to securing Google Cloud storage, and there will be several labs so you can get some hands-on experience with the topics we discuss.

In the Application Security module we will discuss application security techniques and best practices. We will start with a discussion of a few common types of application security vulnerabilities and then see how the Google Cloud Security scanner can be used to identify vulnerabilities in your applications. The threat of Identity and Oauth phishing will be reviewed and we will see how the Identity-Aware Proxy or IAP can be used to control access to your cloud applications.

Protecting workloads in Google Kubernetes Engine involves many layers of the stack, including the contents of your container image, the container runtime, the cluster network, and access to the cluster API server. In the Securing Google Kubernetes Engine module, we will discuss how authentication and authorization work in Google

Kubernetes Engine. We will also talk about hardening your clusters, securing your workloads, and how to use logging and monitoring to make sure everything remains in good health.



Day 3

Mitigating Security Vulnerabilities on Google Cloud

09 Protecting against Distributed Denial of Service Attacks (DDoS)

10 Content-Related Vulnerabilities: Techniques and Best Practices

11 Monitoring, Logging, Auditing, and Scanning

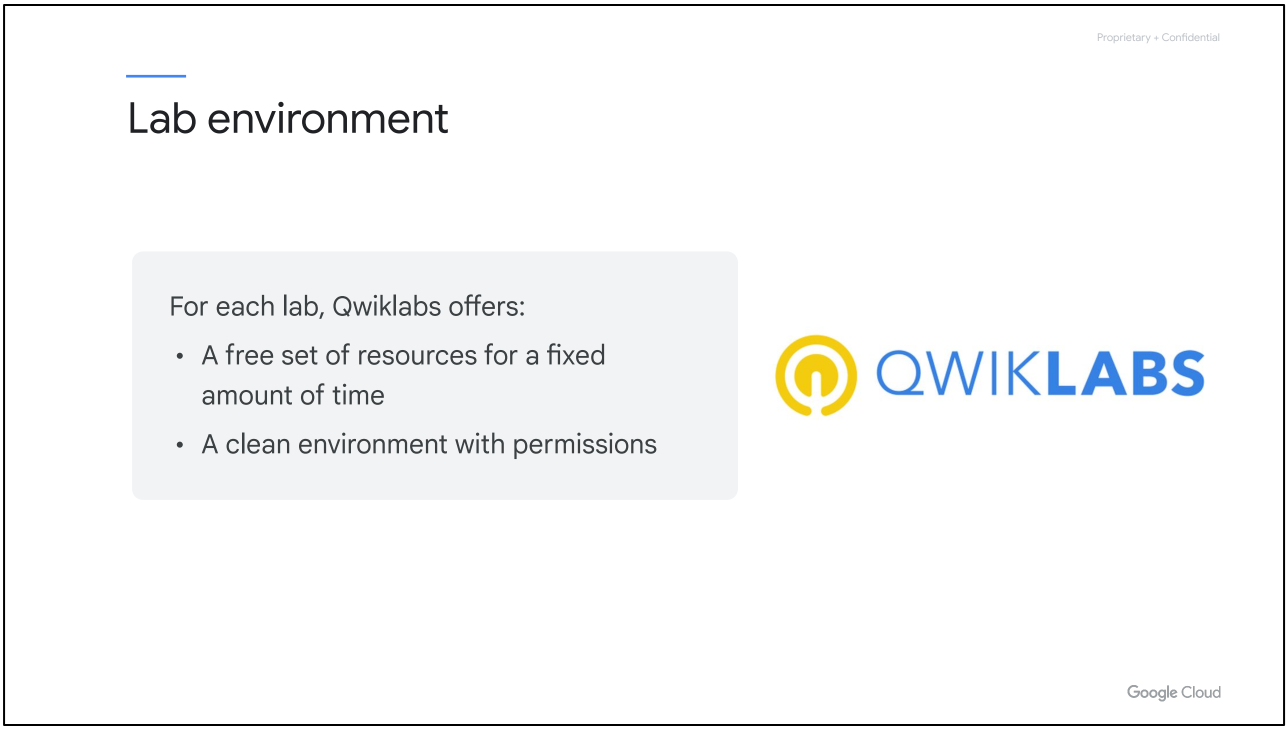
Google Cloud

The focus of day 3 is mitigating security vulnerabilities on Google Cloud.

Distributed Denial of Service Attacks are a major concern today. They can have a huge - and potentially fatal - impact on businesses if the business is not adequately prepared. In the first module, we will discuss how DDoS attacks work and then review some DDoS mitigation techniques that are provided by Google Cloud and complementary partner products.

In the Content-Related Vulnerabilities module we will review the ransomware threat and some of the mitigations you can utilize to help protect your systems from ransomware. We will then look at threats related to data misuse and privacy violations related to sensitive, restricted, or unacceptable content. We will also discuss a few mitigation strategies that can be utilized to protect applications and systems from data misuse and privacy violations.

In the final module, we will investigate the Security Command Center, then move into Cloud monitoring and logging and Cloud Audit logs. Finally, we will look at how to leverage Forseti Security to systematically monitor your Google Cloud resources to ensure that access controls are set as you intended.



Proprietary + Confidential

Lab environment

For each lab, Qwiklabs offers:

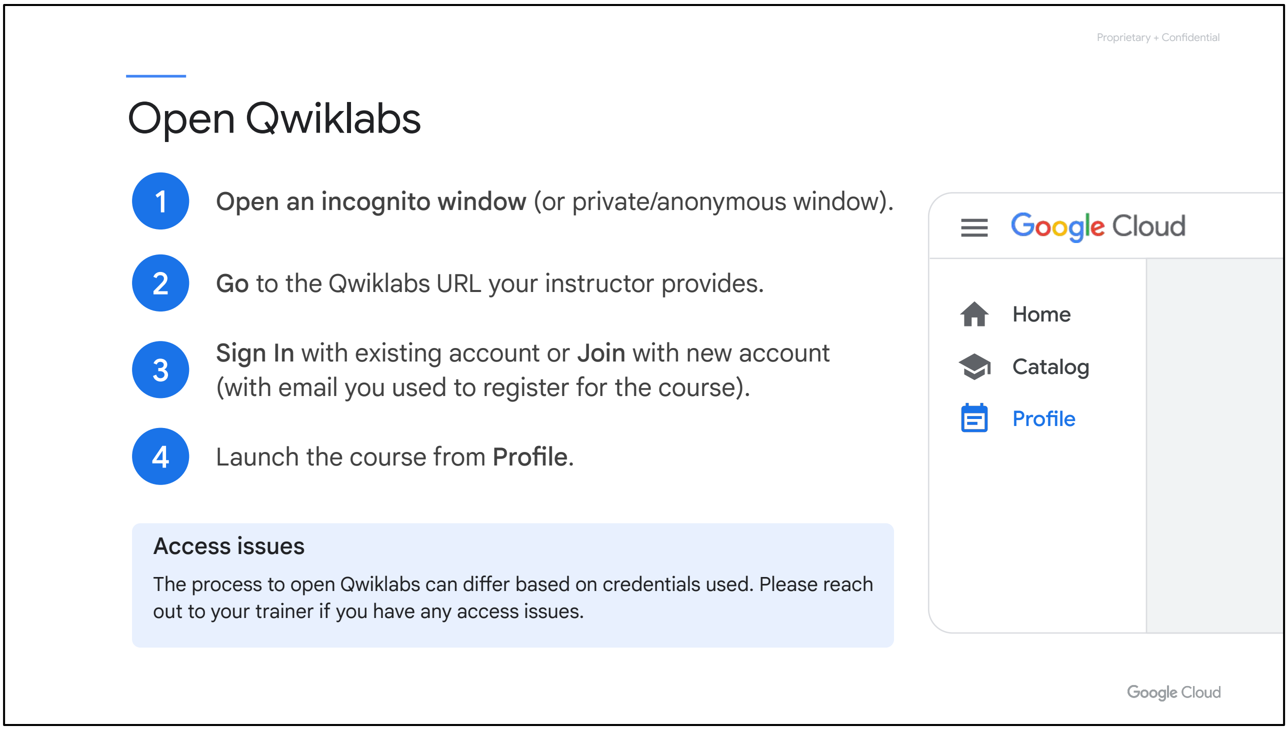
- A free set of resources for a fixed amount of time
- A clean environment with permissions

QWIKLABS

Google Cloud

Qwiklabs provisions you with Google account credentials, so you can access the Google Cloud Console for each lab at no cost. Specifically, for each lab, Qwiklabs offers:

- A free set of resources for a fixed amount of time
- A clean environment with permissions



Open Qwiklabs

1. **Open an incognito window** (or private/anonymous window).
2. **Go** to the Qwiklabs URL your instructor provides.
3. **Sign In** with existing account or **Join** with new account (with email you used to register for the course).
4. Launch the course from **Profile**.

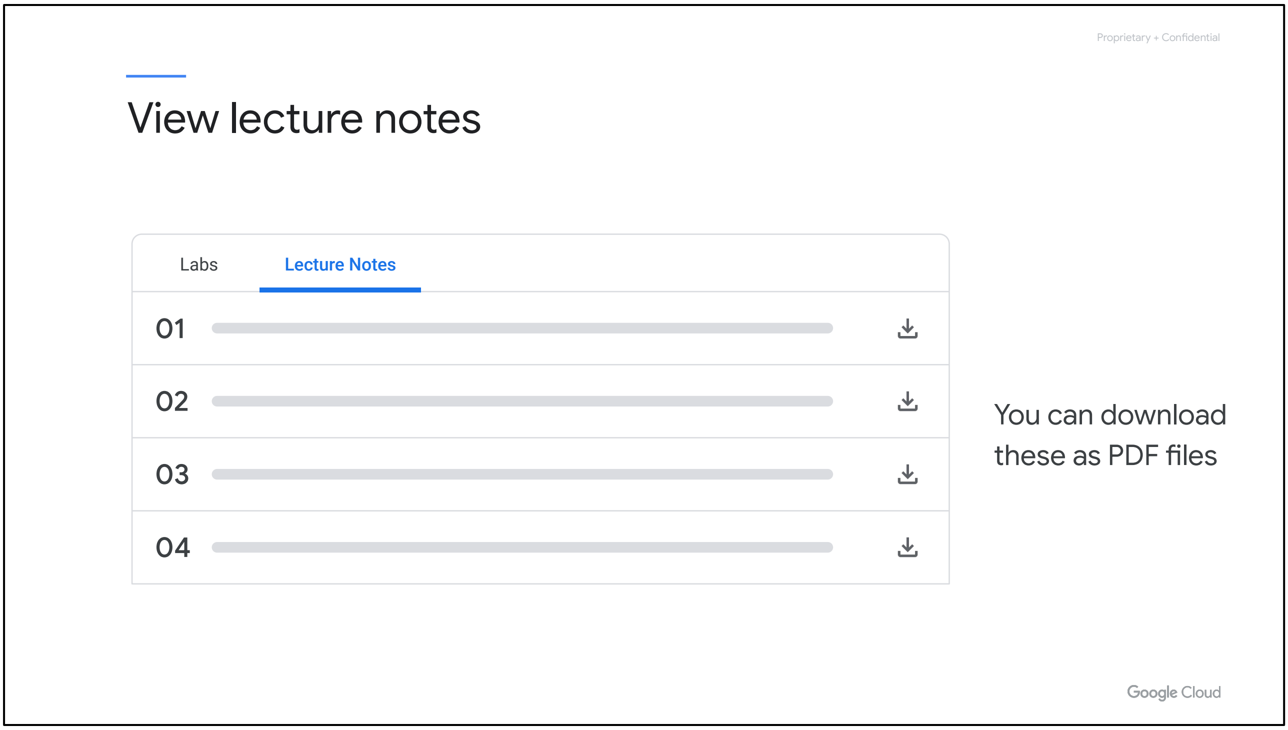
Access issues

The process to open Qwiklabs can differ based on credentials used. Please reach out to your trainer if you have any access issues.

Google Cloud

Go ahead and open Qwiklabs:

1. **Open an incognito window** (or private/anonymous window). Use of an incognito browser window reduces the risk that you will accidentally do the labs using your own Google Cloud account instead of Qwiklabs.
2. **Go** to the Qwiklabs URL your instructor provides.
3. **Sign** in with an existing account or **Join** with a new account (with email you used to register for the course).
4. Launch the course from **Profile**.



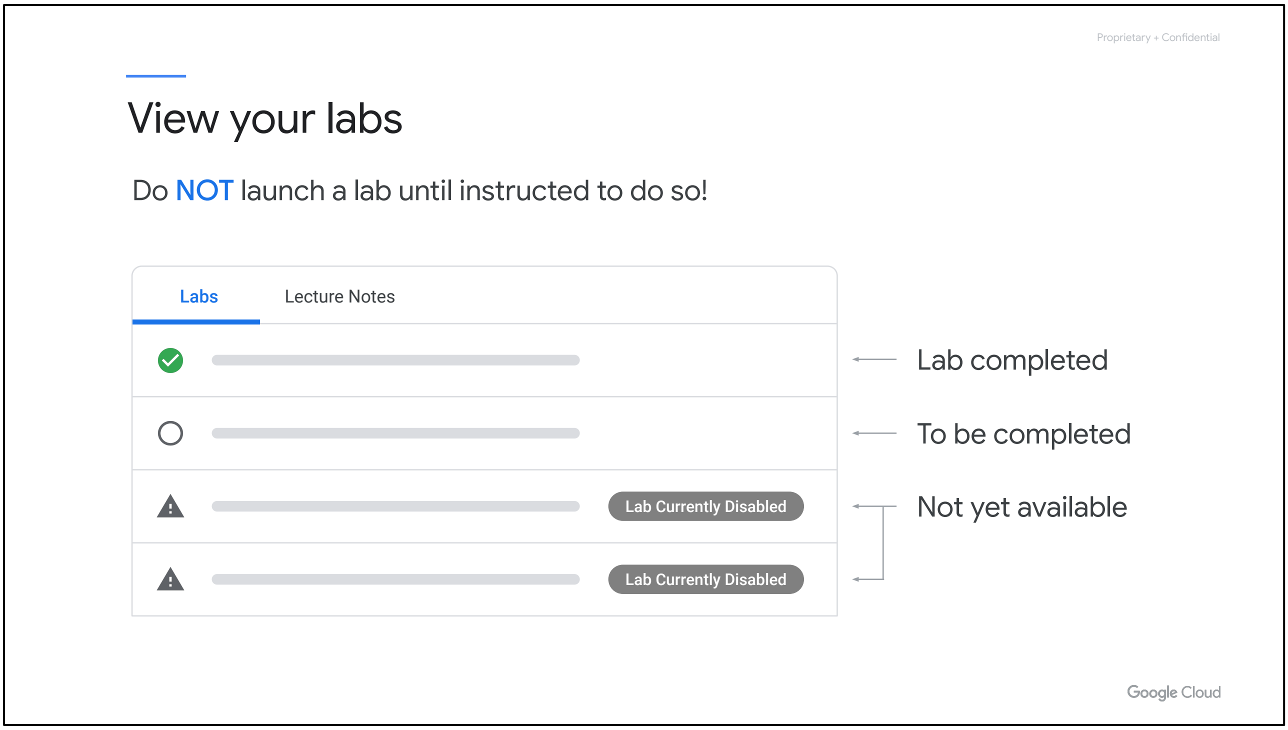
Proprietary + Confidential

View lecture notes

You can download these as PDF files

Google Cloud

Within the course, you can also view the lecture notes. You can download these as PDF files.



View your labs

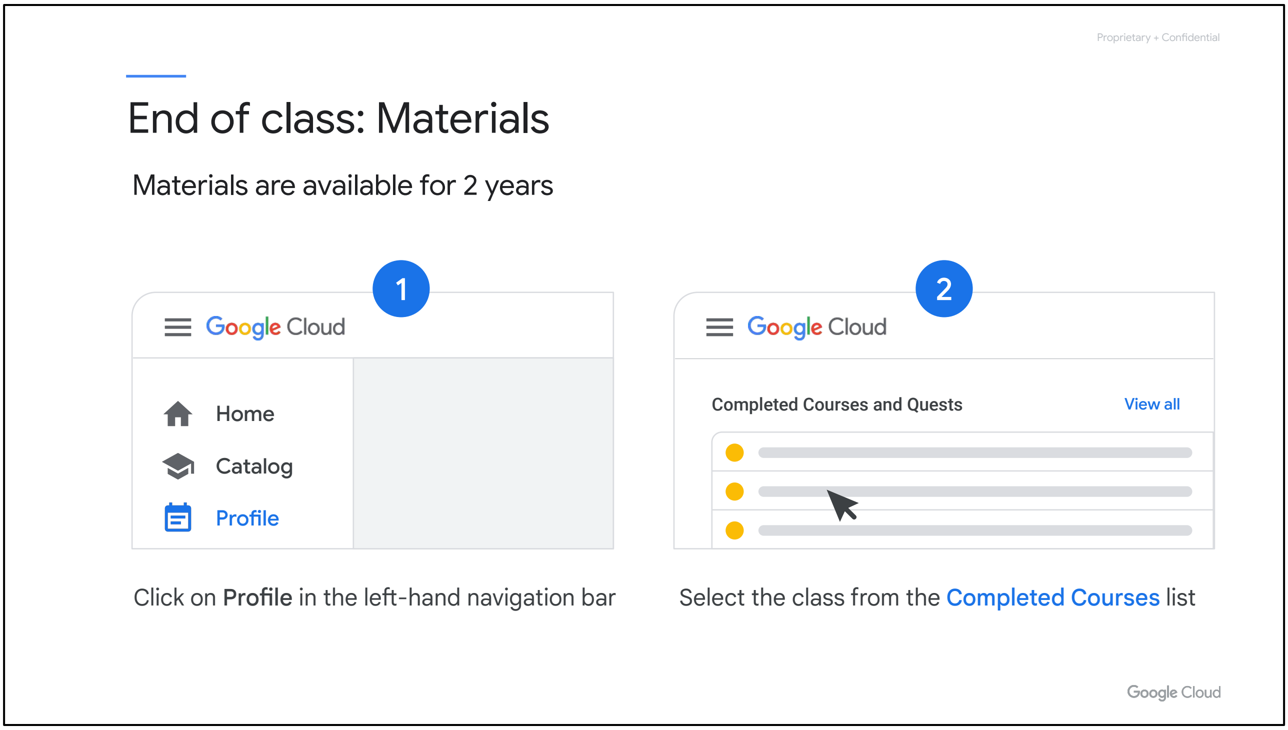
Do **NOT** launch a lab until instructed to do so!

Google Cloud

After you launch the course, you can view your labs. The lab list will indicate whether a lab is:

- Completed (by you)
- Active
- Not yet available

Your instructor will let you know when it’s time to launch a lab. Once you start a lab, you won’t be able to pause and restart it, so you’ll need a continuous block of time to complete the work.



Proprietary + Confidential

End of class: Materials

Materials are available for 2 years

Click on **Profile** in the left-hand navigation bar

Select the class from the Completed Courses list

Google Cloud

You can view the course materials within Qwiklabs as follows:

1. Click on ***Profile*** in the left-hand navigation bar.
2. Scroll down to the ***Completed Courses*** section.
3. Select the class from the ***Completed Courses*** list.

Materials are available for 2 years following the completion of a course.

Google Cloud

Now let’s move onto Module 1: Foundations of Cloud Security.