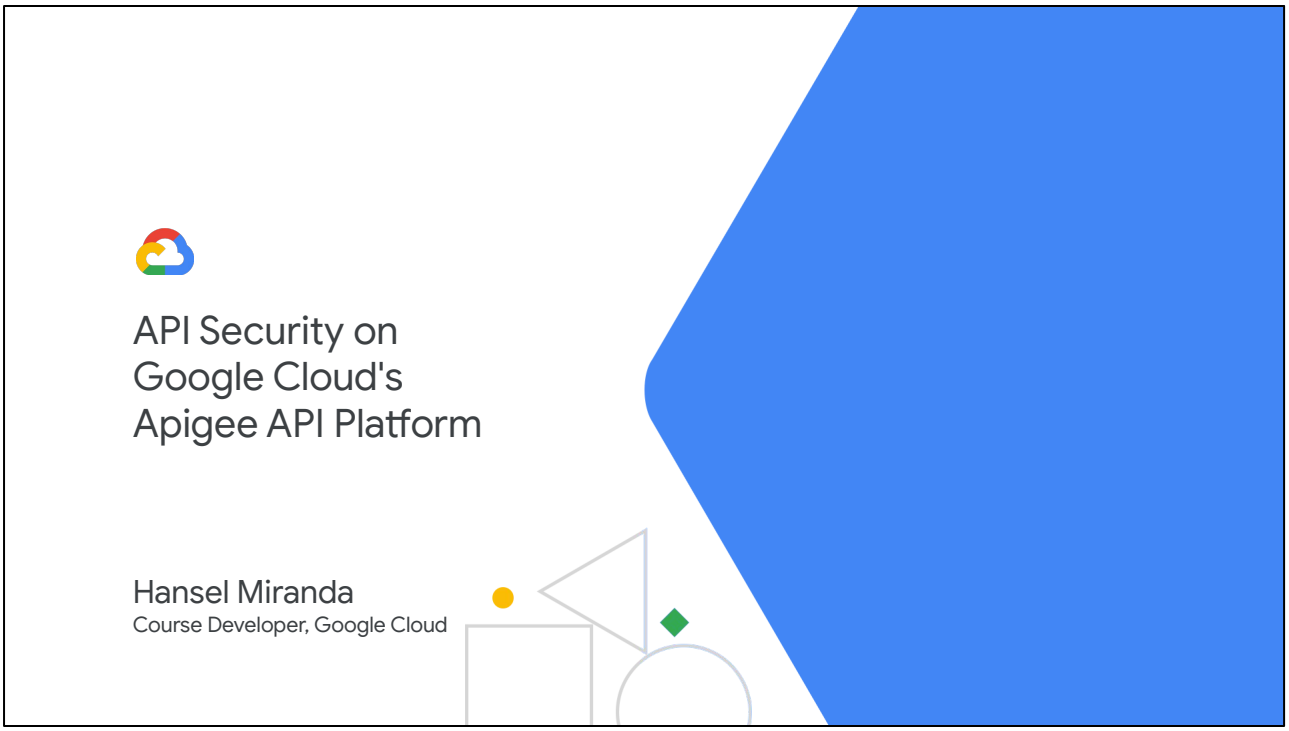
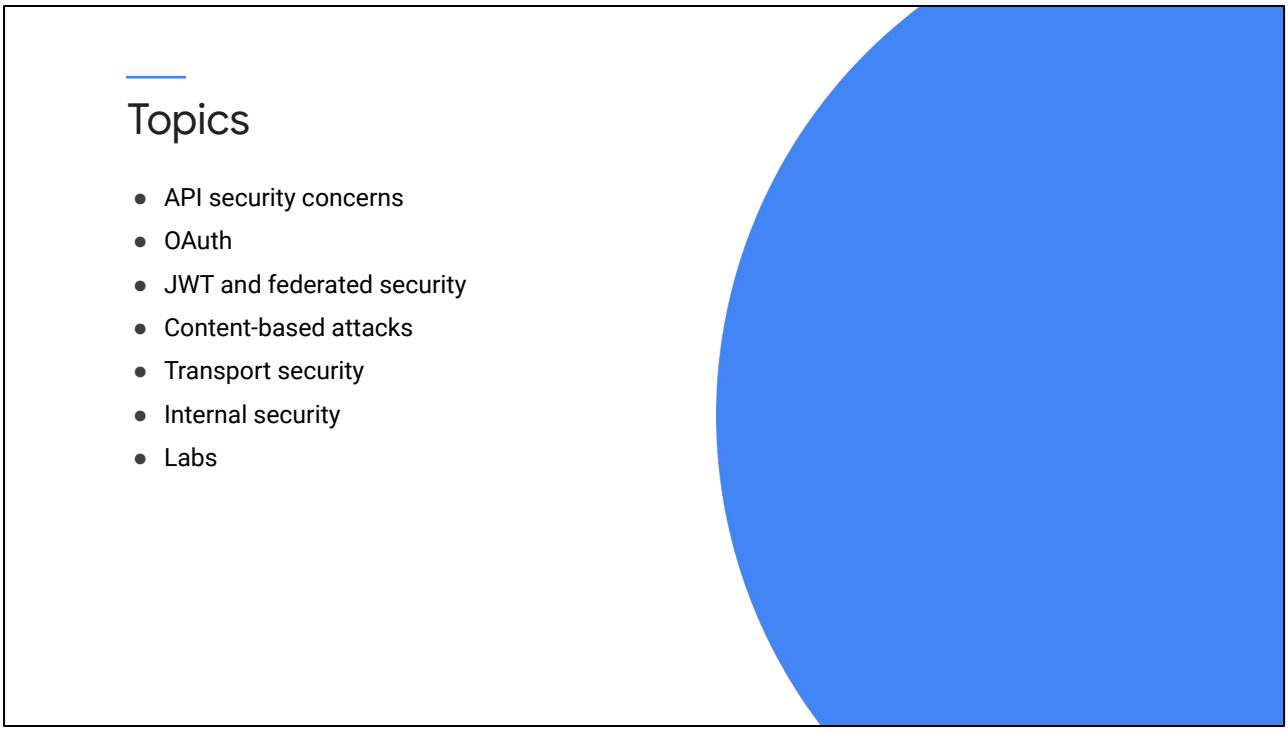


Welcome to API Security, the second course in Developing APIs with Google Cloud's Apigee API platform.



In this course you will learn about different API security concerns, and how you can use Apigee to secure your APIs to address these concerns.

We will learn about OAuth, an authorization framework for APIs. You'll learn how to use OAuth for API authorization, and how to choose between the different OAuth grant types, which represent the different scenarios that can be handled by OAuth.

You will also learn about JWT tokens and federated security for APIs.

We will discuss content-based attacks, and how to protect against them.

You will learn how to secure API requests and responses being sent across the Internet.

We will learn about internal security features in Apigee that allow us to control access for and hide sensitive data from users logged into the Apigee management UI.

Finally, you will use labs to explore these security topics.

You will continue to add functionality to a lab that was started in the API Design and Apigee Fundamentals course. If you have not taken that course, we recommend you take that course before you take this one. But don't worry; we'll provide a starting API proxy for you if you do not have the proxy from the previous course.

You will add OAuth to your retail proxy, and test using OAuth tokens with your proxy.

You will also add JSON threat protection to your API proxy, to protect against malicious JSON payloads, and you will store and use backend credentials in a way that prevents users of Apigee from seeing the credentials.

Other labs will use regular expression threat protection to protect against dangerous patterns in your incoming requests, and you'll learn how to use private variables and data masking to keep users of the Apigee UI from seeing sensitive data while tracing API proxy traffic.