Securing your Web App with SSL Certificates

Cybersecurity

Project Week

© 2023 edX Boot Camps LLC. Confidential and Proprietary. All Rights Reserved.

RECAP

Day 1 Recap

In the first day of your project work, you:

01 Used Microsoft Azure to create a web application.

02 Chose a unique domain from one of two cost options.

03 Deployed a Docker container on your web app.

04 Designed your custom web application.

05 Answered review questions.

Today’s Class

Today’s class will include:

An introduction to Azure Key Vaults

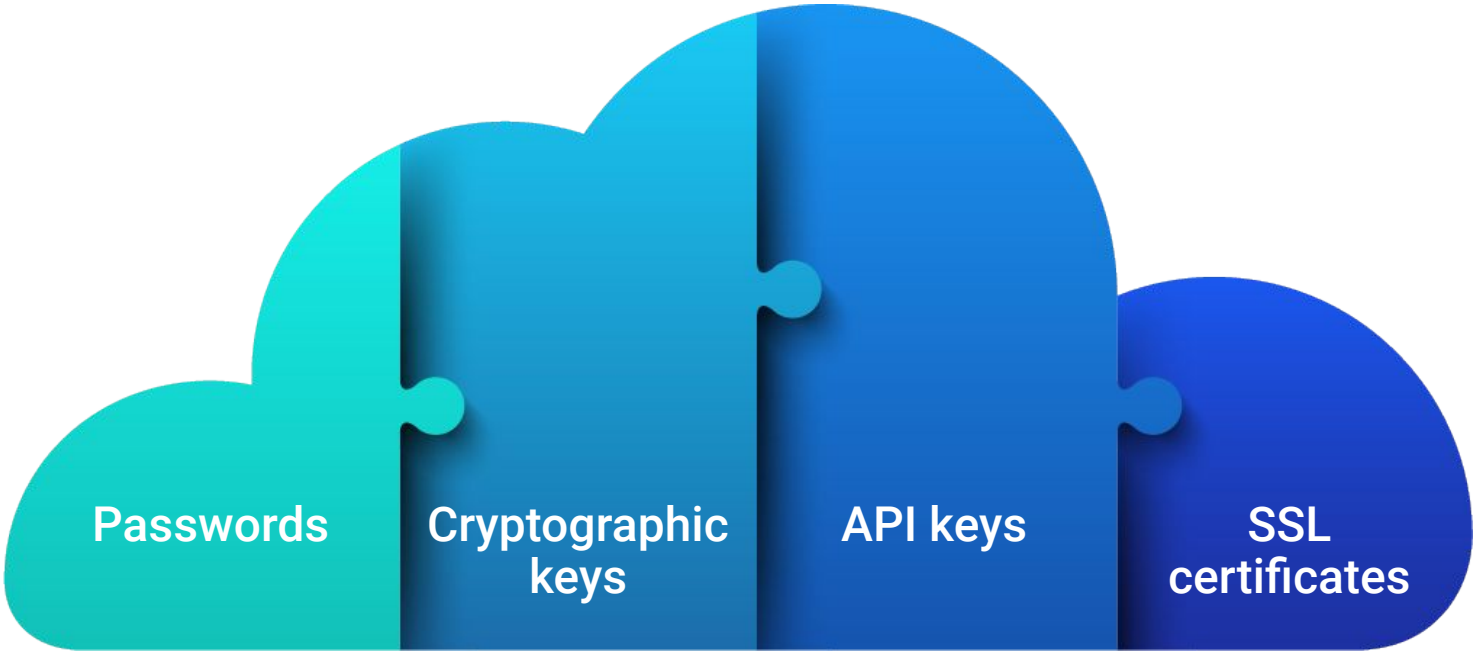
An overview of tasks that you will work on

Project work

Azure Key Vault

Azure Key Vault

When administrators manage cloud services such as web applications, they need to maintain lots of information securely, including:



Azure Key Vault

It is imperative that this information is stored securely, accessible only by specific individuals, and managed in a central location.

Microsoft can accomplish these tasks with **Azure Key Vault**.

Per Microsoft:

“Azure Key Vault is a cloud service for securely storing and accessing secrets.

A secret is anything that you want to tightly control access to, such as API keys, passwords, certificates, or cryptographic keys.”

Azure Key Vault

Benefits of Azure Key Vault include:

Azure Key Vault can store secret information in a single central location.

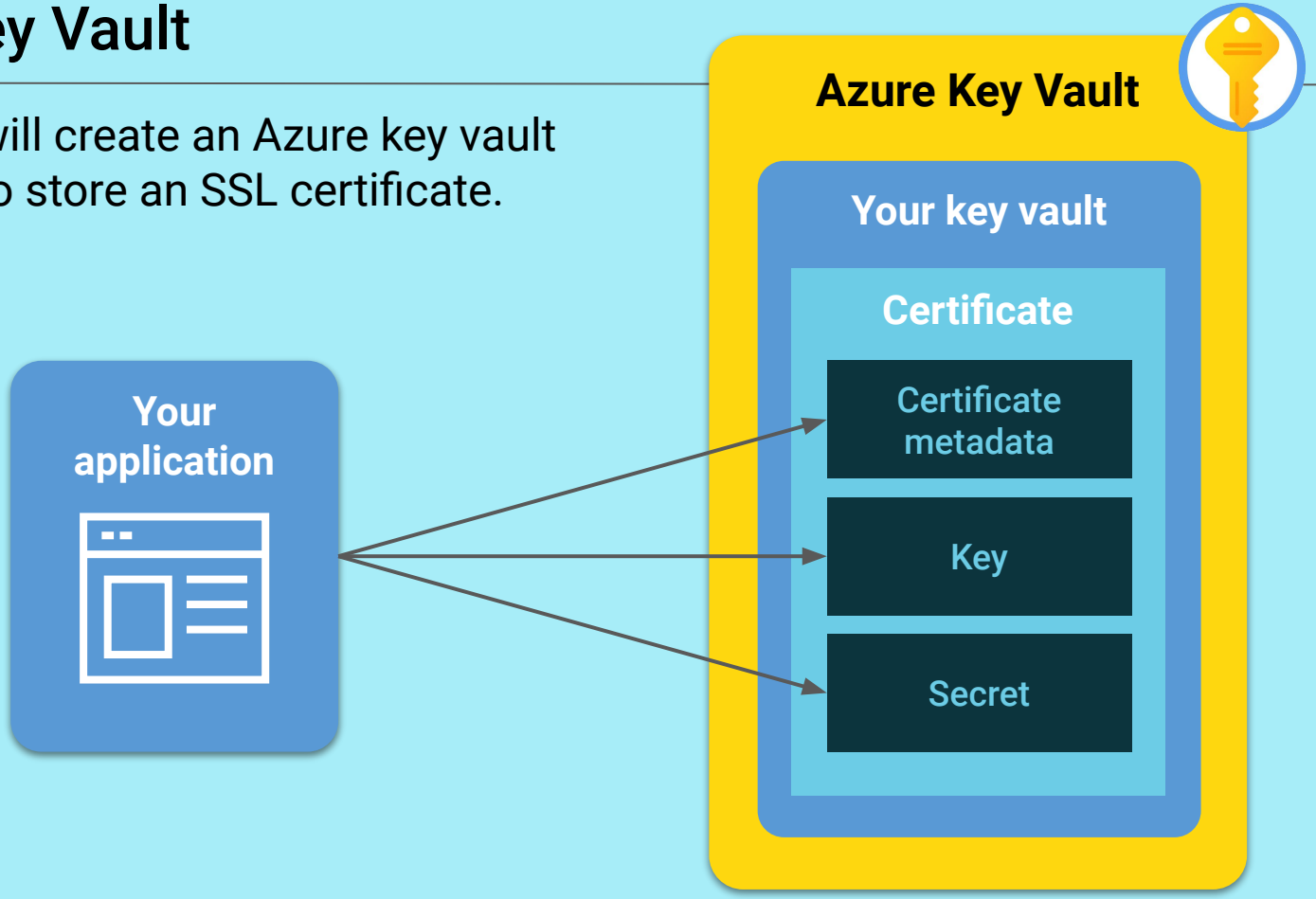
Key Vault secrets can be given access policies either by user or by application.

Secret information from the key vault can be accessed from other cloud resources.

Certificates and keys can be imported or directly generated from within the key vault.

Azure Key Vault

Today, we will create an Azure key vault and use it to store an SSL certificate.



Azure Key Vault

Today, you will create two types of SSL certificates and bind them to your web application. You will explore the advantages and disadvantages of each certificate.

01 Self-signed SSL

02 Azure-managed certificate

Can anyone recall from Cryptography week how SSL certificates are used?

SSL certificates are used to validate the authenticity of a web application and to assist with encrypting the user’s traffic between the client and the server.

Questions?

Day 2
Project Work Overview

Day 2 Project Work

Today, you will complete the following:

01 Create a key vault.

02 Create a self-signed certificate.

03 Import and bind your self-signed certificate to your web application.

04 Create and bind an app service managed certificate.

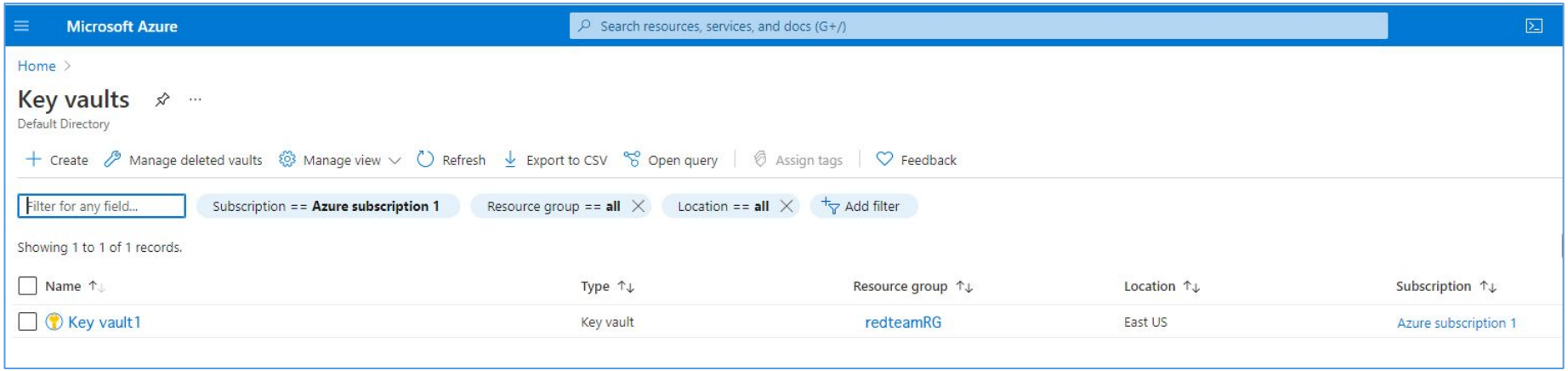
05 Answer review questions.

Step 1 Create a Key Vault

Today's first step is to create an Azure key vault. Steps are included in the activity guide.

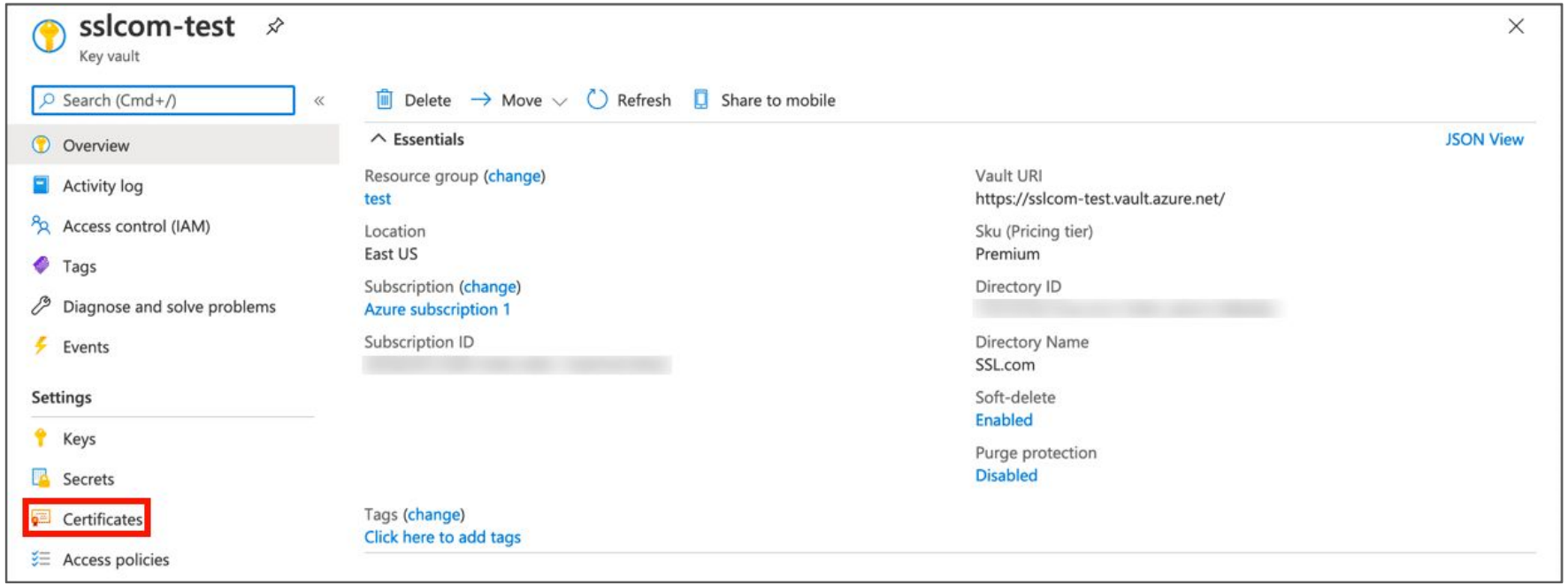
REMEMBER

Use the same subscription and resource group that you did in the previous class.



Step 2 Create a Self-Signed Certificate

In this step, you will return to the command line to use OpenSSL.

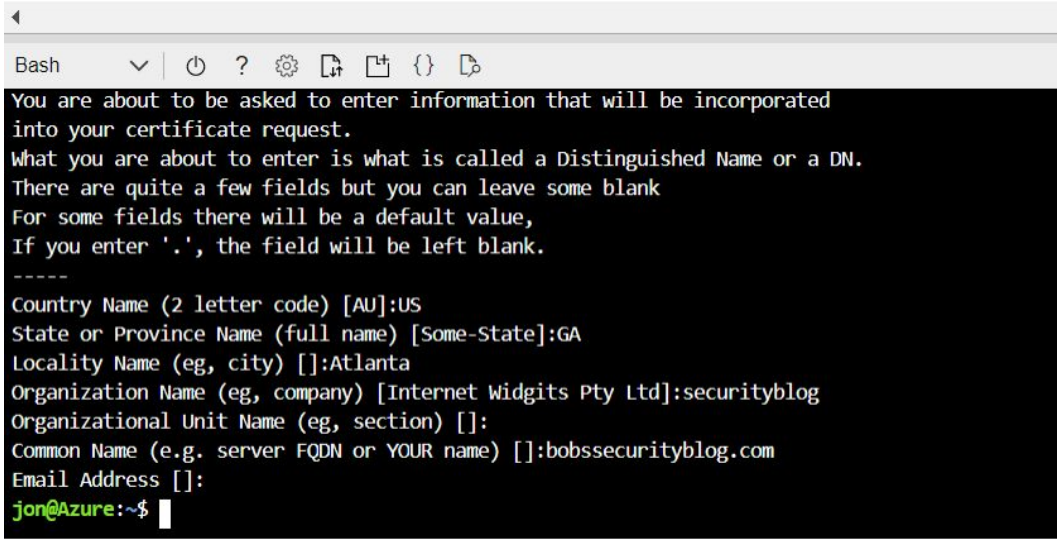


Can anyone recall what we previously used OpenSSL to do?

Step 2 Create a Self-Signed Certificate

During Cryptography week, we used OpenSSL to generate a symmetric key and initialization vector.

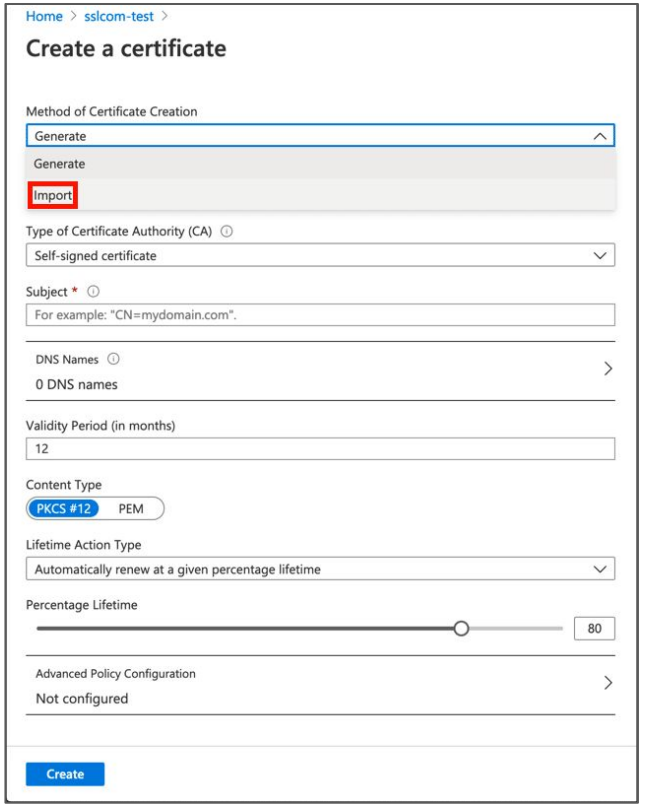
In this project, we will use OpenSSL to generate a certificate called a **self-signed certificate**.



Step 3 Import and Bind the Self-Signed Certificate to the Web App

After you have created your self-signed certificate, you will import your certificate into your Azure key vault.

- You will use the TLS/SSL feature inside your web application to bind your self-signed certificate to your web application.
- Then, you'll view the certificate that you added directly on your browser, and analyze the security risks associated with your new certificate.



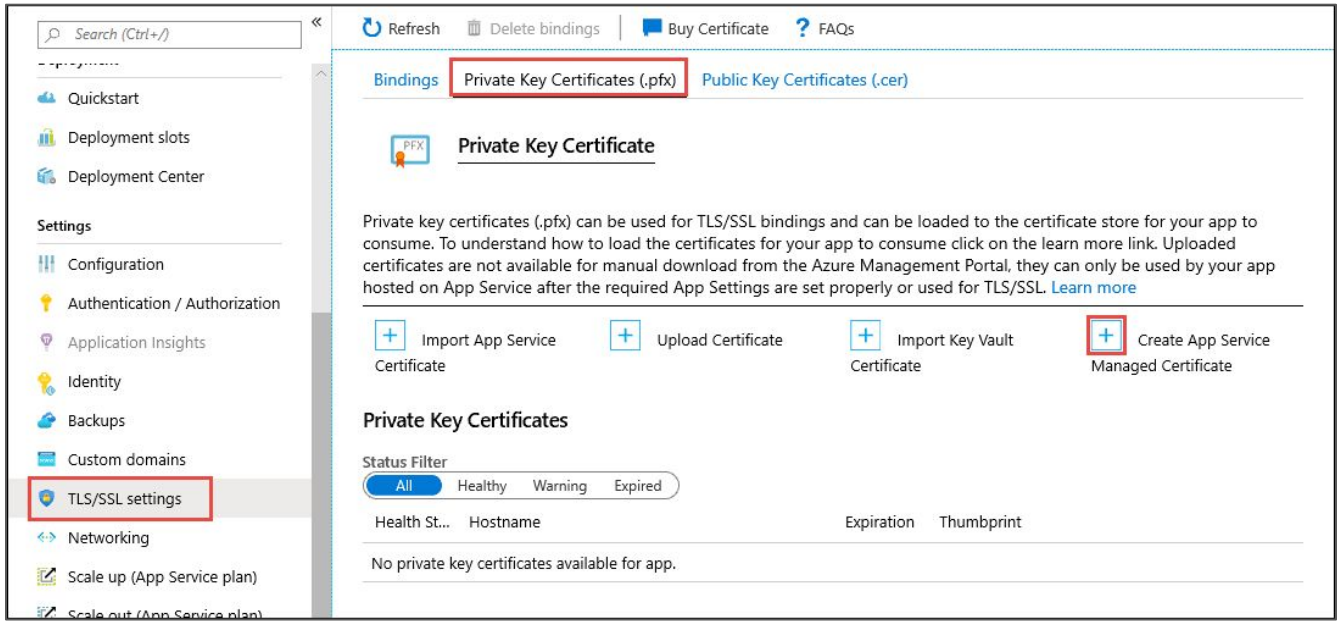
Important:

If you chose a free domain, you will not be able to bind any certificate to your web application, since one has already been provided by Azure.

Your daily guide will provide you with a theoretical exercise.

Step 4 Create and Bind an App Service Managed Certificate

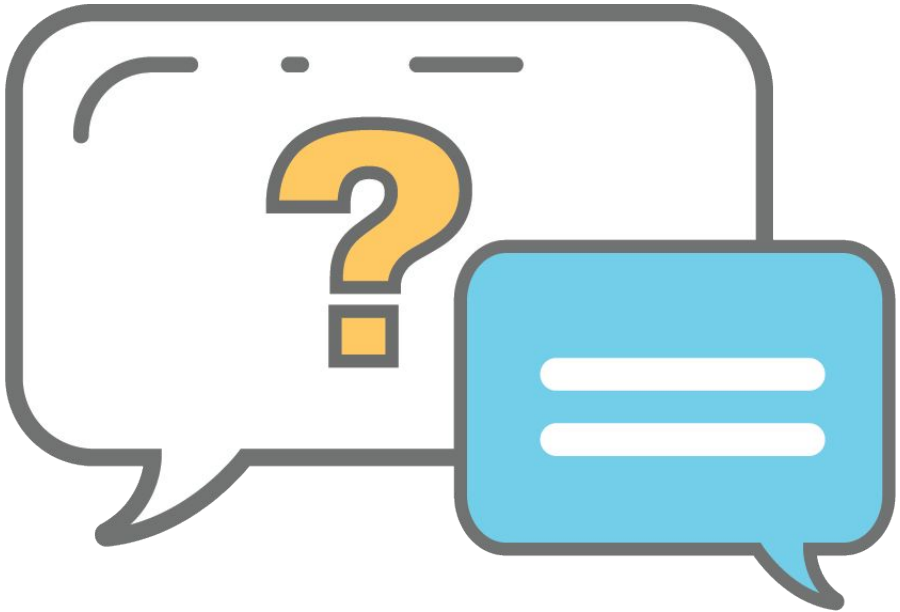
Based on the security risks that you found, you will **replace** your first certificate by using Azure's services to add a more secure certificate—an app service managed certificate—directly to your web application.



Step 5 Answer Review Questions

Once you complete today's activities, you will answer several questions about the project and how it relates to concepts that we've covered in class.

Feel free to use any resources available (class notes, slides, online resources) to answer these questions.



Securing Your Web Application with SSL certificates

For the remainder of today's class, you will work on the daily project tasks.

While each student is responsible for completing their own project, you can use classmates, TAs, or the instructor to assist if you have any questions.

The milestones that you need to complete in order to continue to the next day include adding an SSL certificate to your web application.

Make sure to use the appropriate guide for the domain type that you selected (free or paid).

Securing Your Web Application with SSL certificates

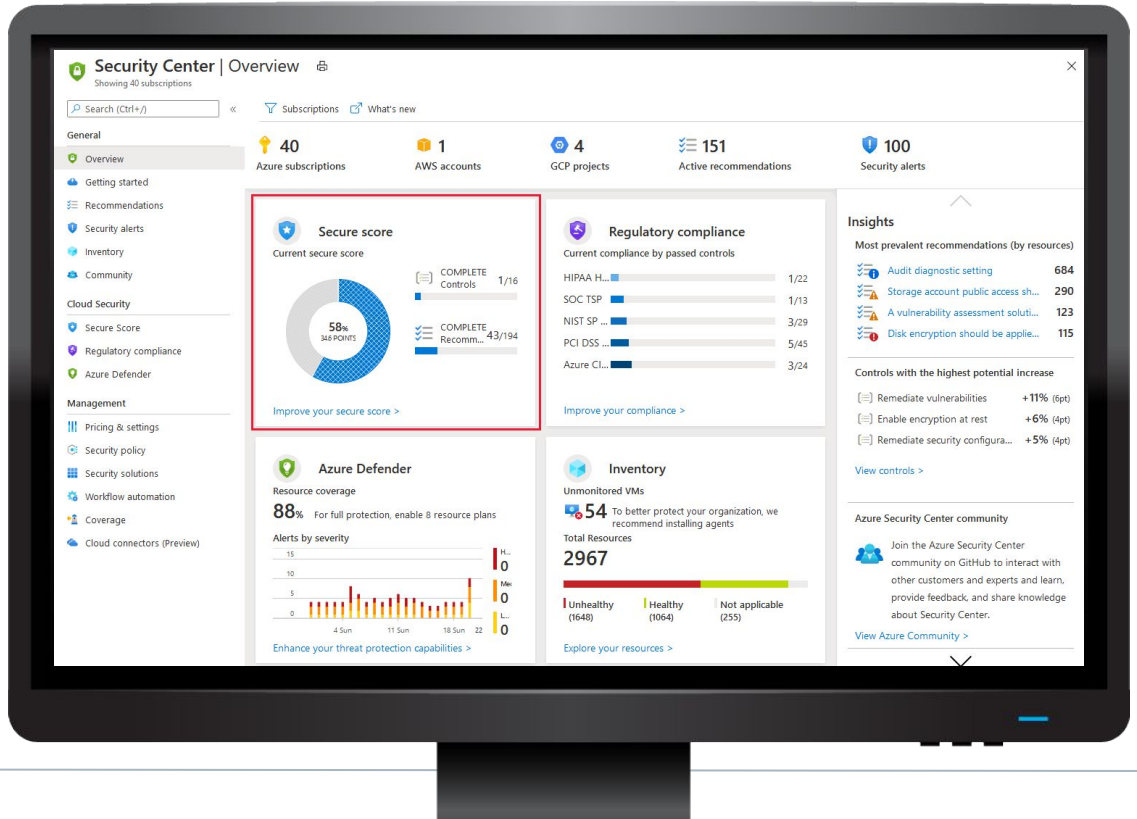
In this activity, you'll work on completing the Day 2 tasks for your project.

Suggested Time:

To end of class

Project Work Time

Tomorrow, you will protect your web application with Azure security features.



Questions?

The End