Secure Azure Services and Workloads w/ Microsoft Defender for Cloud Regulatory Compliance Controls – Intensive Training («SC5X2»)

Learn about securing Azure services and workloads using Microsoft Cloud Security Benchmark controls in Microsoft Defender for Cloud via the Azure portal.

Duration: 1 day
Price: 900.–
Course documents: Official Microsoft Courseware on Microsoft Learn

Content

1 Filter network traffic with a network security group using the Azure portal
In this module, we will focus on filtering network traffic using Network Security Groups (NSGs) in the Azure portal. Learn how to create, configure, and apply NSGs for improved network security.

2 Create a Log Analytics workspace for Microsoft Defender for Cloud
In this module, you'll discover how to create a Log Analytics workspace in the Azure portal for Microsoft Defender for Cloud, improving data collection and security analysis.

3 Set up Microsoft Defender for Cloud
In this module, you'll learn how to implement Microsoft Defender for Cloud using the Azure portal, to strengthen security and threat detection in your Azure environment.

4 Create and integrate a Log Analytics agent and workspace in Defender for Cloud
This module will guide you to configure and integrate a Log Analytics agent with a workspace in Defender for Cloud via the Azure portal, boosting security analysis.

5 Configure Azure Key Vault networking settings
In this module, you'll learn to configure Azure Key Vault networking settings via the Azure portal, ensuring secure and controlled access to your stored secrets.

6 Connect an Azure SQL server using an Azure Private Endpoint using the Azure portal
This module will guide you on securely connecting an Azure SQL server via Azure Private Endpoint in the Azure portal, enhancing data communication security.

Key Learnings

- Creating and configurting NSGs to enforce access controls for Azure resources
- Prioritizing NSG rules and leverage Azure NSG flow logs for monitoring and troubleshooting
- Creating and configuring a Log Analytics workspace in Azure and custom queries and alerts to proactively detect security threats and incidents
- Gaining insights into collecting and analyzing security data from Microsoft Defender for Cloud within the Log Analytics workspace
- Understanding the features and benefits of Microsoft Defender for Cloud, Microsoft Security Benchmark, Security Recommendations, and Defender for Cloud Secure Score
- Monitoring, protecting, and improving the security of cloud environments
- Exploring the MITRE Attack Matrix to identify common attack techniques and prioritize security efforts
- Understanding the concept of Brute Force Attacks and the importance of implementing preventive measures
- Familiarizing with Just in Time Virtual Machine to implement fine-grained access controls for enhanced security
- Configuring and deploying the Log Analytics agent in Azure
- Configuring network access control for Azure Key Vault using virtual network service endpoints and private endpoints.Configure and create an Azure Private Endpoint for Azure SQL Server in the Azure portal
- Gaining insights into the network architecture and components involved in setting up an Azure Private Endpoint
- Understanding how to validate and test the connection between the Azure Private Endpoint and Azure SQL Server
- Recognizing the benefits of using Azure Private Endpoint for securing database connections and isolating network traffic

Target audience

This course is aimed at Azure Administrators and Security Engineers.

Additional information

This workshop is integrated into the course AZ-500: Microsoft Azure Security Technologies.

Any questions?

We are happy to advise you on +41 44 447 21 21 or info@digicomp.ch. You can find detailed information about dates on www.digicomp.ch/courses-digital-transformation-technologies/cloud/microsoft-azure/course-secure-azure-services-and-workloads-w-microsoft-defender-for-cloud-regulatory-compliance-controls-intensive-training