APPLIED SKILLS

Secure Azure services and workloads with Microsoft Defender for Cloud regulatory compliance controls

Days	SKILL LEVEL	DELIVERY METHOD	Role	TECHNOLOGY
1	Intermediate	VILT/ILT	Administrator	Security

Course Overview

This learning path guides you in securing Azure services and workloads using Microsoft Cloud Security Benchmark controls in Microsoft Defender for Cloud via the Azure portal.

Tasks performed.

- Configure Microsoft Defender for Cloud
- Implement just-in-time (JIT) virtual machine (VM) access
- Implement a Log Analytics workspace
- Mitigate network security risks
- Mitigate data protection risks
- Mitigate endpoint security risks
- Mitigate posture and vulnerability management risks

Prerequisites

Before attending this course, delegates must know:

- Experience using the Azure portal to create resources.
- Basic knowledge of security concepts like identities, permissions, and encryption.
- Basic knowledge of networking concepts like virtual networks and subnetting.
- Basic knowledge of Azure Policy and Azure Kubernetes Service concepts.

Prepare for the assessment.

Module 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.

Learning objectives

By the end of this training module, participants will:

- Understand the purpose and benefits of using Azure NSG to filter network traffic.
- Learn how to create and configure NSGs to enforce access controls for Azure resources.
- Gain insights into how NSGs can be used to allow or deny specific types of traffic based on source, destination, and port.
- Understand how to prioritize NSG rules and leverage Azure NSG flow logs for monitoring and troubleshooting.
- Recognize the role of NSGs in implementing network security best practices in Azure.

Module 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.

Learning objectives

By the end of this training module, participants will:

- Understand the importance of a centralized logging solution like Azure Log Analytics workspace for Microsoft Defender for Cloud.
- Learn how to create and configure a Log Analytics workspace in Azure.
- Gain insights into collecting and analyzing security data from Microsoft Defender for Cloud within the Log Analytics workspace.
- Understand how to create custom queries and alerts to proactively detect security threats and incidents.
- Recognize the benefits of integrating Log Analytics workspace with other Azure services and tools.

Module 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.

Learning objectives

By the end of this training module, participants will:

- Understand the features and benefits of Microsoft Defender for Cloud, Microsoft Security Benchmark, Security Recommendations, and Defender for Cloud Secure Score.
- Learn how to leverage these tools to monitor, protect, and improve the security of cloud environments.
- Explore the MITRE Attack Matrix to identify common attack techniques and prioritize security efforts.
- Understand the concept of Brute Force Attacks and the importance of implementing preventive measures.
- Familiarize yourself with Just in Time Virtual Machine to implement fine-grained access controls for enhanced security.

Module 4: Configure 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.

Learning objectives

By the end of this training module, participants will:

- Understand the importance of a centralized log collection and analysis solution in Microsoft Defender for Cloud.
- Learn how to configure and deploy the Log Analytics agent in Azure.
- Gain insights into creating and configuring a Log Analytics workspace for Defender for Cloud.
- Understand how to integrate the Log Analytics workspace with Defender for Cloud to collect and analyze security logs.
- Recognize the benefits of leveraging centralized log analytics for proactive security monitoring and threat detection.

.

Module 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.

Learning objectives

By the end of this training module, participants will:

- Understand the importance of configuring networking settings for Azure Key Vault in ensuring secure access and communication.
- Learn how to configure network access control for Azure Key Vault using virtual network service endpoints and private endpoints.
- Gain insights into configuring firewall rules and virtual network service endpoints to restrict access to Key Vault.
- Understand the process of configuring private endpoints to securely access Key Vault from virtual networks.
- Recognize the benefits of properly configuring networking settings for Azure Key Vault in enhancing overall security.

Module 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.

Learning objectives

By the end of this training module, participants will:

- Understand the importance of using Azure Private Endpoint to establish secure connections to Azure SQL Server.
- Learn how to configure and create an Azure Private Endpoint for Azure SQL Server in the Azure portal.
- Gain insights into the network architecture and components involved in setting up an Azure Private Endpoint.
- Understand how to validate and test the connection between the Azure Private Endpoint and Azure SQL Server.
- Recognize the benefits of using Azure Private Endpoint for securing database connections and isolating network traffic.

Take the assessment.

This assessment will use an interactive lab to evaluate your performance. It will take a few minutes to load the lab, and you may do other activities while it loads. After you launch the lab, you will need to wait 72 hours to launch it again. Your mouse movements and text entered during the lab will be recorded for quality purposes. Learn more.

Follow on Course

Schedules | Netcampus Group