COURSE OUTLINE

MS-SC5002: SECURE AZURE SERVICES AND WORKLOADS WITH MICROSOFT DEFENDER FOR CLOUD REGULATORY COMPLIANCE CONTROLS

DURATION	LEVEL	TECHNOLOGY	DELIVERY METHOD	TRAINING CREDITS
1 Day	Intermediate	Security	Instructor Led	NA

INTRODUCTION

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.

AUDIENCE PROFILE

This course is designed for professionals who are responsible for securing cloud environments and ensuring compliance within Microsoft Azure. The target audience includes:

- Azure Security Engineers – who implement security controls and threat protection.
- Compliance Officers – responsible for regulatory standards and governance.
- Azure Administrators – managing Azure services and configurations.
- Cloud Security Architects – designing secure cloud infrastructure.
- Cybersecurity Consultants – advising organizations on cloud security best practices.
- IT Auditors – assessing and validating security and compliance measures.

PREREQUISITES

Before attending this course, delegates must have:

- Familiarity with Azure IaaS and PaaS offerings.
- A working knowledge of security capabilities in Azure.
- Understanding of regulatory compliance standards

COURSE OBJECTIVES

After completing this course, delegates will be able to:

- Understand regulatory compliance standards supported by Microsoft Defender for Cloud.
- Assess and monitor compliance within Azure using built-in tools and benchmarks.
- Enable Microsoft Defender for Cloud on Azure subscriptions for enhanced threat protection.
- Filter network traffic using Network Security Groups (NSGs) to enforce security boundaries.
- Create and configure Log Analytics workspaces for data collection and analysis.
- Integrate Log Analytics agents with Defender for Cloud to monitor workloads.
- Implement Just-in-Time (JIT) VM access to reduce exposure to threats.
- Configure Azure Key Vault networking settings for secure secret management.
- Connect Azure SQL servers securely using Private Endpoints to restrict access to trusted networks

COURSE CONTENT

Module 1: Examine Defender for Cloud regulatory compliance standards

In this module, we will focus on using Microsoft Defender for Cloud to streamline regulatory compliance by identifying and addressing issues that hinder meeting compliance standards and certifications.

Lessons

- Introduction
- Regulatory compliance standards in Defender for Cloud
- Microsoft cloud security benchmark in Defender for Cloud
- Improve your regulatory compliance in Defender for Cloud
- Module assessment
- Summary

By the end of this module, you'll be able to:

- Understand how to use Microsoft Defender for Cloud's compliance management dashboard.
- Identify and interpret key regulatory compliance standards applicable to your industry.
- Implement and manage compliance controls within Microsoft Defender for Cloud.
- Conduct regular compliance assessments and generate comprehensive compliance reports.

Module 2: Enable Defender for Cloud on your Azure subscription

In this module, we will focus on enabling Microsoft Defender for Cloud on your Azure subscription to enhance security monitoring,

compliance management, and threat protection for your cloud-based applications.
Lessons
- Introduction
- Connect your Azure subscriptions
- Exercise - Configuring Microsoft Defender for Cloud for Enhanced Protection
- Module assessment
- Summary

By the end of this module, you'll be able to:
- Learn how to connect your Azure subscriptions to Microsoft Defender for Cloud.
- Understand the benefits of integrating Azure subscriptions for enhanced security monitoring.
- Explore methods to manage and ensure compliance across connected Azure subscriptions.
- Gain skills to implement best practices for threat protection within your Azure environment.

Module 3: 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.
Lessons
- Introduction
- Azure resource group
- Azure Virtual Network
- How network security groups filter network traffic
- Application security groups
- Exercise - Create a virtual network infrastructure
- Module assessment
- Summary

By the end of this module, you'll be able to:
- 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 4: Create a Log Analytics workspace
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.
Lessons
- Introduction
- Log Analytics workspace
- Exercise - Create a Log Analytics workspace
- Module assessment
- Summary

By the end of this module, you'll be able to:
- 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 5: Collect guest operating system monitoring data from Azure and hybrid virtual machines using Azure Monitor Agent
This module will guide you on how to deploy and manage Azure Monitor Agent, configure Data Collection Rules, and integrate it with Microsoft Defender for Cloud for enhanced security.
Lessons
- Introduction
- Deploy the Azure Monitor Agent
- Collect data with Azure Monitor Agent
- Exercise - Create a data collection rule and install the Azure Monitor Agent
- Module assessment
- Summary

By the end of this module, you'll be able to:
- 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 6: Explore just-in-time virtual machine access
In this module, we'll focus on the risk of open management ports on virtual machines and how JIT VM access in Microsoft Defender for Cloud mitigates this threat.
Lessons
- Introduction
- Understand just-in-time virtual machine access
- Enable just-in-time access on virtual machines
- Exercise - Enable just-in-time access on virtual machines
- Module assessment
- Summary

By the end of this module, you'll be able to:
- Understand the risks associated with open management ports on virtual machines.
- Learn how to implement JIT VM access using Microsoft Defender for Cloud.
- Explore how JIT VM access reduces attack surfaces in Azure and AWS environments.
- Gain skills to configure and manage temporary, controlled access to VMs for authorized users.

Module 7: 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.
Lessons
- Introduction
- Azure Key Vault basic concepts
- Best practices for Azure Key Vault
- Azure Key Vault network security
- Configure Azure Key Vault firewalls and virtual networks
- Exercise - Configure Key Vault networking settings
- Azure Key Vault soft delete overview
- Virtual network service endpoints for Azure Key Vault
- Exercise - Enable soft delete in Azure Key Vault
- Module assessment
- Summary

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 8: 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.

Lessons

- Introduction.
- Azure Private Endpoint.
- Azure Private Link.
- Exercise - Connect to an Azure SQL server using an Azure Private Endpoint using the Azure portal.
- Module assessment
- Summary.

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.

ASSOCIATED CERTIFICATIONS & EXAM

There is no Associated Certification or Exam for this course; however, there is an assessment to achieve your Applied Skills credential. (Assessment Link)