email : techcenter@trainocate.com.my
contact : +603-2281-1111

SC-5002: Secure Azure services and workloads with Microsoft Defender for Cloud regulatory compliance controls

Course Code: SC-5002
Duration: 1 day
Instructor-led Training (ILT) | Virtual Instructor-led Training (VILT)

OVERVIEW

To earn this Microsoft Applied Skills credential, learners demonstrate the ability to implement regulatory compliance controls as recommended by the Microsoft cloud security benchmark.

Candidates for this credential should be familiar with Azure infrastructure as a service (IaaS) and platform as a service (PaaS). They should have experience with security capabilities in Azure, along with a working knowledge of regulatory compliance standards.

SKILLS COVERED

- 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

WHO SHOULD ATTEND?

- Administrator
- Security Engineer

PREREQUISITES

There are no prerequisites required to attend this course.

MODULES

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.

Learning objectives

By the end of this training module, participants will:

- 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.

Prerequisites

None

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.

Learning objectives

By the end of this training module, participants will:

- 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.

Prerequisites

None

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.

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.

Prerequisites

None

Module 4: 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.

Prerequisites

None

Module 5: 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.

Prerequisites

None

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.

Learning objectives

By the end of this training module, participants will:

- 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.

Prerequisites

None

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.

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.

Prerequisites

None

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.

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.

Prerequisites

None

END OF PAGE