Copilot for Microsoft 365 for Administrators (1 Day)

Course Overview

This course begins by examining the Microsoft Copilot for Microsoft 365 design. Its main focus, however, is on the security and compliance features that administrators must configure in their Microsoft 365 tenant to protect their company's organizational data before they implement Copilot for Microsoft 365.

This course is designed for administrators, Microsoft 365 administrators, or persons aspiring to the Microsoft 365 Administrator role who've completed at least one of the Microsoft 365 role-based administrator certification paths.

Course Benefits

- Gain insights into the complex architecture and service designs of Copilot for Microsoft 365.
- Streamline administrative tasks and enhance productivity with guided implementations of Copilot for Microsoft 365.
- Ensure robust data security and compliance with integrated Microsoft 365 tools tailored for Copilot.
- Utilize sophisticated identity and access management tools to secure user interactions within Microsoft 365 environments.
- Optimize role management and access controls to safeguard your organizational resources and data.
- Leverage cutting-edge threat intelligence capabilities of Microsoft Defender XDR to protect against sophisticated cyber threats.
- Implement effective data classification systems to manage and protect sensitive information accurately.
- Control and manage how sensitive information is handled by applying comprehensive sensitivity labels.
- Further secure and govern your enterprise data with advanced sensitivity label management, deployment, and policies.

Course Outline

1. **Examine the Copilot for Microsoft 365 design**
    - Examine the Copilot for Microsoft 365 logical architecture
    - Examine the key components of Copilot for Microsoft 365
    - Explore the Copilot for Microsoft 365 service and tenant architecture
    - Extend Copilot for Microsoft 365 with Microsoft Graph connectors

2. **Implement Copilot for Microsoft 365**
    - Get ready for Copilot for Microsoft 365
    - Prepare your data for searches in Copilot for Microsoft 365
    - Protect your Copilot for Microsoft 365 data with Microsoft 365 security tools
    - Assign your Copilot for Microsoft 365 licenses
    - Drive Copilot for Microsoft 365 adoption with a Copilot Center of Excellence

3. **Examine data security and compliance in Copilot for Microsoft 365**
    - Examine how Copilot for Microsoft 365 uses your proprietary business data
    - Examine how Copilot for Microsoft 365 protects sensitive business data
    - Examine how Copilot for Microsoft 365 uses Microsoft 365 isolation and access controls
    - Examine how Copilot for Microsoft 365 meets regulatory compliance mandates

4. **Manage secure user access in Microsoft 365**
    - Examine the identity and access tools used in Microsoft 365
    - Manage user passwords
    - Implement Conditional Access policies
    - Enable pass-through authentication
    - Implement multifactor authentication
    - Enable passwordless sign-in with Microsoft Authenticator
    - Explore self-service password management
    - Explore Windows Hello for Business
    - Implement Microsoft Entra Smart Lockout
    - Explore Security Defaults in Microsoft Entra ID
    - Investigate authentication issues using sign-in logs

5. **Manage roles and role groups in Microsoft 365**
    - Examine the use of roles in the Microsoft 365 permission model
    - Manage roles across the Microsoft 365 ecosystem
    - Explore administrator roles in Microsoft 365
    - Examine best practices when configuring administrative roles
    - Assign admin roles to users in Microsoft 365
    - Delegate admin roles to partners
    - Implement role groups in Microsoft 365
    - Manage permissions using administrative units in Microsoft Entra ID
    - Elevate privileges using Microsoft Entra Privileged Identity Management

6. **Explore threat intelligence in Microsoft Defender XDR**
    - Explore Microsoft Intelligent Security Graph
    - Explore alert policies in Microsoft 365
    - Run automated investigations and responses
    - Explore threat hunting with Microsoft Threat Protection
    - Explore advanced threat hunting in Microsoft Defender XDR
    - Explore threat analytics in Microsoft 365
    - Identify threat issues using Microsoft Defender reports

7. **Implement data classification of sensitive information**
    - Explore data classification
    - Implement data classification in Microsoft 365
    - Explore trainable classifiers
    - Create and retrain a trainable classifier
    - View sensitive data using Content explorer and Activity explorer
    - Detect sensitive information documents using Document Fingerprinting

8. **Explore sensitivity labels**
    - Manage data protection using sensitivity labels
    - Explore what sensitivity labels can do
    - Determine a sensitivity label's scope
    - Apply sensitivity labels automatically
    - Explore sensitivity label policies

9. **Implement sensitivity labels**
    - Plan your deployment strategy for sensitivity labels
    - Examine the requirements to create a sensitivity label
    - Create sensitivity labels
    - Publish sensitivity labels
    - Remove and delete sensitivity labels