Microsoft Security, Identity & Endpoint Administration

Duration: 10 Days

Course Overview

This comprehensive instructor-led bootcamp combines endpoint management, identity and access administration, and security operations into a single end-to-end Microsoft security curriculum. Participants learn Microsoft Intune, Microsoft Entra ID, Microsoft Defender, Microsoft Sentinel, Microsoft Purview, and Microsoft Security Copilot through extensive hands-on labs.

Target Audience

- Microsoft 365 Administrators
- Endpoint Administrators
- Security Administrators
- Identity and Access Administrators
- Security Operations (SOC) Analysts
- Cloud Security Engineers
- Azure Administrators
- IT Professionals responsible for Microsoft security solutions

Prerequisites

- Basic understanding of Microsoft 365 services
- Familiarity with Windows client administration
- Basic networking concepts
- Basic understanding of Microsoft Entra ID (Azure AD)
- Familiarity with Azure fundamentals is recommended
- Experience using the Microsoft 365 admin center is beneficial but not mandatory

Part 1 – Microsoft 365 Endpoint Administration (MD-102)

Module 1: Explore endpoint management

Lessons

- Understand Azure Active Directory (Entra ID)
- Manage Azure Active Directory (Entra ID) identities

Labs

- Managing Identities in Azure AD
- Synchronizing Identities by using Azure AD Connect

Module 2: Execute device Enrollment

Lessons

- Manage device authentication
- Enroll devices using Microsoft Intune

Labs

- Configuring and managing Azure AD Join
- Manage Azure AD device registration
- Manage Device Enrollment into Intune
- Enrolling devices into Microsoft Intune

Module 3: Configure profiles for users and devices

Lessons

- Execute device profiles
- Oversee device profiles
- Maintain user profiles

Labs

- Creating and Deploying Configuration Profiles
- Using a Configuration Profile to configure Kiosk mode
- Using a Configuration Profile to configure iOS and iPad OS Wi-Fi settings
- Using Group Policy Analytics to validate GPO support in Intune
- Monitor device and user activity in Intune

Module 4: Examine application management

Lessons

- Execute mobile application management
- Deploy and update applications
- Administer endpoint applications

Labs

- Deploying cloud apps using Intune
- Configure App Protection Policies for Mobile Devices

Module 5: Manage authentication and compliance

Lessons

- Protect identities in Microsoft Entra

- Enable organizational access
- Implement device compliance
- Generate inventory and compliance reports

Labs

- Configuring Multi-factor Authentication
- Configuring Self-service password reset for user accounts in Microsoft Entra
- Configuring and validating device compliance
- Creating device inventory reports

Module 6: Manage endpoint security

Lessons

- Deploy device data protection
- Manage Microsoft Defender for Endpoint
- Manage Microsoft Defender in Windows client
- Manage Microsoft Defender for Cloud Apps

Labs

- Configure and Deploy Windows Information Protection Policies by using Intune
- Configuring Endpoint security using Intune
- Configuring Disk Encryption Using Intune

Module 7: Deploy using on-premises based tools

Lessons

- Assess deployment readiness
- Deploy using the Microsoft Deployment Toolkit

Labs

- Deploying Windows 11 using Microsoft Deployment Toolkit

Module 8: Deploy using cloud-based tools

Lessons

- Deploy Devices using Windows Autopilot
- Implement dynamic deployment methods
- Plan a transition to modern endpoint management
- Manage Windows 365
- Manage Azure virtual desktop
- Explore Microsoft Intune Suite

Labs

- Deploying Windows 11 with Autopilot
- Refreshing Windows with Autopilot Reset and Self-Deploying mode

Part 2 – Security Operations (SC-200)

Learning Path 1: Mitigate threats using Microsoft Defender XDR

Lessons

- Introduction to threat protection with Microsoft Defender XDR
- Mitigate incidents using Microsoft Defender XDR
- Remediate risks with Defender for Office 365 in Microsoft Defender XDR
- Microsoft Defender for Identity in Microsoft Defender XDR
- Protect your identities with Entra ID Protection
- Defender for Cloud Apps in Microsoft Defender XDR

Labs

- Obtain Your Microsoft 365 Credentials
- Apply Microsoft Defender for Office 365 preset security policies
- Prepare the Microsoft Defender XDR workspace

Learning Path 2: Get started with Microsoft Security Copilot

Lessons

- Fundamentals of Generative AI
- Describe Microsoft Security Copilot
- Describe the embedded experiences of Microsoft Security Copilot
- Security Copilot agents in Microsoft Defender

Labs

- Explore Microsoft Security Copilot

Learning Path 3: Mitigate threats using Microsoft Purview

Lessons

- Microsoft Purview Compliance Solutions
- Investigate and remediate compromised entities identified by Microsoft Purview DLP policies
- Investigate and remediate insider risk threats identified by Microsoft Purview policies
- Investigate threats using Content search in Microsoft Purview
- Investigate threats using Microsoft Purview Audit (Standard)
- Investigate threats using Microsoft Purview Audit (Premium)

Labs

- Explore Microsoft Purview Audit logs

Learning Path 4: Mitigate threats using Microsoft Defender for Endpoint

Lessons

- Examine threat vectors and data breaches
- Protect against threats with Microsoft Defender for Endpoint
- Deploy the Microsoft Defender for Endpoint environment
- Implement Windows security enhancements
- Perform device investigations
- Perform actions on a device
- Perform evidence and entities investigations
- Configure and manage automation
- Configure for alerts and detections
- Utilize Threat and Vulnerability Management

Labs

- Deploy Microsoft Defender for Endpoint
- Mitigate Attacks using Defender for Endpoint

Learning Path 5: Create queries for Microsoft Sentinel using KQL

Lessons

- Construct KQL statements for Microsoft Sentinel
- Analyze query results using KQL
- Build multi-table statements using KQL
- Work with string data in using KQL statements

Labs

- Create queries for Microsoft Sentinel using KQL

Learning Path 6: Configure the Microsoft Sentinel SIEM and Platform

Lessons

- Introduction to Microsoft Sentinel
- Deploy the Microsoft Sentinel SIEM
- Deploy the Microsoft Sentinel Platform
- Query logs in Microsoft Sentinel
- Use watchlists in Microsoft Sentinel
- Utilize threat intelligence in Microsoft Sentinel

Labs

- Configure your Microsoft Sentinel environment

Learning Path 7: Connect data sources to Microsoft Sentinel SIEM

Lessons

- Manage content in Microsoft Sentinel
- Connect data to Microsoft Sentinel using data connectors
- Connect Microsoft services to Microsoft Sentinel
- Connect Microsoft Defender XDR to Microsoft Sentinel
- Connect Windows hosts to Microsoft Sentinel
- Connect Common Event Format logs to Microsoft Sentinel
- Connect syslog data sources to Microsoft Sentinel
- Connect threat indicators to Microsoft Sentinel

Labs

- Connect data to Microsoft Sentinel using data connectors
- Connect the Microsoft Defender for Cloud data connector to Microsoft Sentinel
- Connect the Azure Activity data connector to Microsoft Sentinel
- Connect Windows devices to Microsoft Sentinel using data connectors
- Connect Linux hosts to Microsoft Sentinel using data connectors

Learning Path 8: Create detections and perform investigations using Microsoft Sentinel

Lessons

- Threat detection with Microsoft Sentinel analytics
- Automation in Microsoft Sentinel
- Threat response with Microsoft Sentinel playbooks
- Security incident management in Microsoft Sentinel
- Entity behavioral analytics in Microsoft Sentinel
- Data normalization in Microsoft Sentinel
- Query, visualize, and monitor data in Microsoft Sentinel

Labs

- Create a playbook
- Create a scheduled query
- Explore Entity Behavior Analytics
- Understand detection modeling
- Conduct attacks
- Create detections
- Investigate incidents
- Create ASIM Parsers
- Create Workbooks
- Use Repositories in Microsoft Sentinel

Learning Path 9: Perform threat hunting in Microsoft Sentinel SIEM and Platform

Lessons

- Explain threat hunting concepts in Microsoft Sentinel
- Threat hunting with Microsoft Sentinel
- Use Search jobs in Microsoft Sentinel
- Optional – Hunt for threats using notebooks in Microsoft Sentinel Platform

Labs

- Perform threat hunting in Microsoft Sentinel
- Threat hunting using notebooks with Microsoft Sentinel

Part 3 – Microsoft Identity and Access Administrator (SC-300)

Learning Path 3: Implement an authentication and access management solution

Lessons

- Plan and implement Microsoft Entra multifactor authentication (MFA)
- Manage user authentication
- Plan, implement, and administer Conditional Access
- Manage Microsoft Entra ID Protection
- Implement access management for Azure resources
- Configure and deploy Global Secure Access

Labs

- Enable MFA
- Configure and deploy SSPR
- Microsoft Entra ID Authentication for Windows and Linux VMs
- Assign Azure resources
- Manage Microsoft Entra smart lockout values.
- Implement Conditional Access
- Enable sign-in risk policy
- Configure MFA registration policy
- Key Vault and managed identities

Learning Path 4: Implement access management for apps

Lessons

- What is an app?
- Plan and design the integration of enterprise apps for single sign-on (SSO)
- Implement, and monitor the integration of enterprise apps
- Implement app registrations

Labs

- App discovery
- App access policies
- Register an application
- Implement access management for apps.
- Grant tenant wide access to an app