Course Summary

Enhance Endpoint Security with Microsoft Intune and Microsoft Security Copilot (MD-4011)

Lab Summary | 5 Hands-On Labs consolidated into a single All in one module

Course Overview

This course provides a hands-on, end-to-end path for deploying, managing, and securing modern endpoints using Microsoft Intune, Microsoft Entra ID, and Microsoft Defender for Endpoint. Working through a realistic healthcare-organization scenario, learners progress from initial tenant preparation and device enrollment to advanced policy enforcement, data protection, and device hardening. The labs develop practical skills in identity and access governance, configuration and compliance management, mobile data protection, conditional access, and security-baseline deployment. A strong emphasis is placed on zero-trust and least-privilege principles, ensuring configurations reflect real-world security best practices. By the end, learners can build a fully governed, compliant, and threat-resistant endpoint management environment ready for enterprise use.

Detailed Lab Summaries

Lab 1: Configure Tenant for Device Management

- **Objective:** To prepare a Microsoft 365 tenant so it is fully ready to enroll, manage, and secure devices through Microsoft Intune.
- **Key Topics Covered:** Microsoft 365 E5 licensing, Microsoft Entra ID device settings, role-based access control (RBAC) and zero-trust/least-privilege principles, static and dynamic groups, automatic MDM enrollment, and initialization of Microsoft Defender for Endpoint.
- **Hands-On Activity:** Verifying licenses for pilot users, assigning five least-privilege administrative roles to a dedicated admin account, configuring Entra ID device join and registration, creating a static pilot-user group and a dynamic Windows-device group, enabling automatic Intune enrollment, confirming the MDM authority, and provisioning the Defender for Endpoint bidirectional connection.
- **Real-World Application:** IT teams use these foundational steps to stand up a secure, governed management platform before any device is enrolled, ensuring licensing, identity, and access controls are correct from day one.

Lab 2: Enroll and Validate Devices

- **Objective:** To enroll Windows 11 devices into Intune via Entra join and confirm that enrollment succeeded across the management portals.
- **Key Topics Covered:** Microsoft Entra join, automatic MDM enrollment, device inventory and properties, compliance state, dynamic group membership, and manual device synchronization.
- **Hands-On Activity:** Joining two Windows 11 devices to Entra ID under different pilot users, confirming automatic Intune enrollment, locating and reviewing device properties in both the Entra and Intune admin centers, verifying automatic membership in the dynamic Windows-device group, and forcing device sync from both the portal and the device itself.

- **Real-World Application:** Administrators rely on these skills to onboard corporate endpoints at scale and to verify that devices are correctly registered, managed, and reporting before applying policies.

Lab 3: Implement Policy Layering and Compliance

- **Objective:** To enforce device security settings and define the minimum standards a device must meet to be considered compliant.
- **Key Topics Covered:** Settings Catalog configuration profiles, BitLocker and Windows Hello, compliance policies, noncompliance actions and notification templates, and assignment filters based on device ownership.
- **Hands-On Activity:** Creating a Settings Catalog profile to require BitLocker encryption and a minimum PIN length, building a Windows compliance policy covering Secure Boot, firewall, antivirus, and password rules, configuring staged noncompliance actions (notify then retire), creating a corporate-owned device filter, and validating that policies apply only to targeted devices.
- **Real-World Application:** Security teams use policy layering and compliance enforcement to guarantee that every managed device meets organizational and regulatory security standards, with automated remediation for devices that fall out of compliance.

Lab 4: Protect Data with MAM and Conditional Access

- **Objective:** To safeguard corporate data inside applications and to restrict access to corporate resources based on device compliance.
- **Key Topics Covered:** Mobile Application Management (MAM) app protection policies for iOS and Android, data-loss-prevention controls, app-level PIN and encryption requirements, and Conditional Access policies tied to device compliance.
- **Hands-On Activity:** Creating iOS and Android app protection policies for Microsoft 365 apps (blocking copy/paste, screen capture, and printing while requiring encryption and a PIN), building a Conditional Access policy that requires a compliant device for Exchange Online, testing access from compliant and noncompliant devices, and analyzing sign-in logs to confirm policy evaluation.
- **Real-World Application:** Organizations apply these controls to prevent data leakage on personal and mobile devices and to ensure that only trusted, compliant endpoints can reach sensitive corporate email and data.

Lab 5: Harden Devices with Security Baselines

- **Objective:** To strengthen device security posture through baselines, advanced threat protection, and proactive attack-surface controls.
- **Key Topics Covered:** Windows security baselines, Microsoft Defender for Endpoint onboarding and integration, Attack Surface Reduction (ASR) rules, and vulnerability and threat monitoring.
- **Hands-On Activity:** Deploying the Windows security baseline (100+ recommended settings), configuring the Defender for Endpoint connector and onboarding profile, verifying device onboarding in the Defender portal, configuring ASR rules to block credential theft, malicious scripts, Office-macro exploits, and ransomware, and reviewing exposure scores, security recommendations, and alerts.
- **Real-World Application:** Security operations teams use baselines, EDR onboarding, and ASR rules to reduce the attack surface of their endpoint fleet and to continuously monitor and remediate

vulnerabilities and active threats.