Implementing Microsoft Defender for Endpoint

Course Overview

Duration - 12 Hours | Level - Intermediate

Microsoft Defender for Endpoint is an enterprise endpoint security platform designed to help enterprise networks prevent, detect, investigate, and respond to advanced threats. In this workshop you will learn how to enable, configure and implement Microsoft Defender for Endpoint for its industry-leading optics and detection capabilities and its capabilities to manage Windows and non-Windows platform endpoints. The course includes AI-translated audio in following languages. EN - English, CN - Chinese Simplified, CN - Chinese Traditional, DE - Deutsch, ES - Spanish, FR - French, PT - Portuguese, JA - Japanese, KO - Korean, IT - Italian, RU - Russia, TR - Turkey

Course Modules

Day 1

Introduction to Microsoft Defender for Endpoint

Introduction to Zero Trust

Microsoft Defender for Endpoint Core capabilities

Zero Trust and Microsoft Defender for Endpoint

One platform, one agent

Microsoft endpoint security plans

Supported capabilities by platform

Hands on labs

Setting up the Microsoft Defender for Endpoint Environment

Day 2

Planning and Deploying Microsoft Defender for Endpoint

Preparing for your deployment

Assigning roles and permissions

Identifying architecture

Onboarding to Microsoft Defender for Endpoint

Example Deployments

Configuring capabilities

Managing Microsoft Defender for Endpoint after initial setup

Safe Deployment Practice

Hands on labs

Validating Endpoint Onboarding - Conducting a PowerShell Detection Test with Microsoft Defender for Endpoint

Endpoint Security and Attack Detection using Defender for Endpoint

Microsoft Defender for Endpoint Incidents Management and Analysis

Day 3

Onboarding and configuring Devices

Onboarding Windows Clients

Onboarding Windows Servers

Onboarding non-Windows devices

Integration with Microsoft Defender for Cloud

Configuring Microsoft Defender for Endpoint on MacOS

Configuring Microsoft Defender for Endpoint on Linux

Configuring Mobile Threat Defense and Android features

Detecting threats and protecting endpoint

Microsoft Defender for Endpoint integration with Microsoft Sentinel

Hands on Lab

Investigating Microsoft Defender for Endpoint Generated Real-Time Alerts in Microsoft Sentinel