Technofocus

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

Cloud Introduction to Zero Trust
Cloud Microsoft Defender for Endpoint Core capabilities
Cloud Zero Trust and Microsoft Defender for Endpoint
Cloud One platform, one agent
Cloud Microsoft endpoint security plans
Cloud Supported capabilities by platform

Hands on labs

Cloud Setting up the Microsoft Defender for Endpoint Environment

Day 2

Planning and Deploying Microsoft Defender for Endpoint

Cloud Preparing for your deployment

Cloud Assigning roles and permissions

Cloud Identifying architecture

Cloud Onboarding to Microsoft Defender for Endpoint

Cloud Example Deployments

Cloud Configuring capabilities

Cloud Managing Microsoft Defender for Endpoint after initial setup

Cloud Safe Deployment Practice

Hands on labs

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

Cloud Endpoint Security and Attack Detection using Defender for Endpoint

Cloud Microsoft Defender for Endpoint Incidents Management and Analysis

Day 3

Onboarding and configuring Devices

Cloud Onboarding Windows Clients

Cloud Onboarding Windows Servers

Cloud Onboarding non-Windows devices

Cloud Integration with Microsoft Defender for Cloud

Cloud Configuring Microsoft Defender for Endpoint on MacOS

Cloud Configuring Microsoft Defender for Endpoint on Linux

Cloud Configuring Mobile Threat Defense and Android features

Cloud Detecting threats and protecting endpoint

Cloud Microsoft Defender for Endpoint integration with Microsoft Sentinel

Hands on Lab

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