

Workshop – Microsoft Defender for Identity

WorkshopPLUS

Duration: 1 Day [Remote / Onsite]

Difficulty Level: 200 - Intermediate

Description

Defender for Identity is fully integrated with Microsoft Defender XDR, and leverages signals from both on-premises Active Directory and cloud identities to help you better identify, detect, and investigate advanced threats directed at your organization.

This offering is designed to provide you with essential knowledge to plan for deployment and operationalization of Microsoft Defender for Identity.

Objectives

- Explore MDI and its core components and how it integrates with Microsoft Defender XDR
- Discover key planning topics such as prerequisites sizing, accounts, and multi-forest considerations
- Walk-through deployment steps and decisions to integrate Microsoft Defender for Identity into your environment
- Familiarization with post-deployment optimization and SOC guidance from Microsoft

Outcomes

Appreciation of key steps towards Microsoft Defender for Identity deployment and optimization.

Methodology

Learn by example

Participate in group discussions and learn from presentations and demonstrations.

Scope

This offering is scoped for MDI knowledge transfer.

Agenda

Day 1

- MDI Overview
- MDI Planning
- Deployment Overview
- Post Deployment Activities overview

Delivery Outline

Requirements

Participants

- AD and Security engineering, as well as support staff and others who share responsibility for securing; domain controllers, ADFS & AD Certificate Services.

Skill Requirements

- Strong identity and security operations knowledge

Time Commitment

- One full-day engagement with relevant roles

Delivery Requirements

- Computer with Windows 10 or later, audio equipment, internet access. Modern browser and at least 1 Mbps bandwidth per participant
- Microsoft Teams for remote deliveries

Readiness

Day 1	MDI Overview	<ul style="list-style-type: none">▪ MDI integration with Microsoft Defender XDR▪ Sensors and alerts▪ Lateral Movement Paths▪ Reporting and hunting
Day 1	MDI Planning	<ul style="list-style-type: none">▪ Prerequisites (networking, Network Name Resolution, service limits)▪ Multi-Forest▪ Action account and permissions▪ Sizing Tool▪ Retention & Export
Day 1	Deployment Overview	<ul style="list-style-type: none">▪ Sensor onboarding▪ VPN, ADFS & AD CS integration▪ Policies and audit settings▪ Testing and verification
Day 1	Post Deployment Activities overview	<ul style="list-style-type: none">▪ Automated response▪ Alert examples and thresholds▪ Tuning and exclusions▪ Notifications▪ Sensitive groups and honeytokens▪ PowerShell module▪ Operations guide

For more information: Please contact your Microsoft Representative for more details.