E-mmersion
Defender for Identity

Microsoft Defender for Identity (MDI) E-mmersion

Identity-Driven Defense: Agile, Scalable, and Proactive Security

Organizations face evolving cyber threats that endanger systems, identities, and data integrity. **Microsoft Defender for Identity (MDI)** transforms Active Directory data into intelligence, detecting advanced attacks and insider threats through on-premises signals.

Introducing our E-mmersion: Microsoft Defender for Identity (MDI)

Our **E-mmersion** provides a hands-on, immersive learning experience designed to deepen your understanding of Microsoft Defender for Identity. Through interactive exercises and real-world scenarios, you will explore how MDI **enhances identity security, detects advanced threats**, and **integrates seamlessly with other Microsoft security solutions.** This lab empowers you to proactively safeguard your organization's identity infrastructure against evolving cyber threats.

By participating in this E-mmersion, you will see firsthand...

- **Practical Experience:** Implement and manage Microsoft Defender for Identity sensors in a controlled environment.
- **Threat Detection and Analysis:** Learn to identify anomalous behaviors and investigate real-time alerts using advanced MDI capabilities.
- **Attack Scenario Simulation:** Engage in exercises simulating lateral movement and credential theft to better understand common attack vectors.

Agenda & Activities : Your Defender for Identity E-mmersion Journey

Introduction	Welcome, objectives, and an overview of Microsoft Defender for Identity.
Lab Environment Access	Access validation and a brief tour of the lab interface.
Hands-On Exercises	Participants will explore MDI capabilities in a controlled environment, analyzing security data, user activities, and risk indicators. They will also simulate attack scenarios like lateral movement, credential theft, and reconnaissance.
Scenario Analysis & Discussion	A review of real-time alerts will provide insights into detection logic, response strategies, and best practices for mitigating identity-based threats.
Closing	The session will end with a Q&A, key takeaways, and next steps. Participants can provide feedback and receive guidance on additional resources and future training opportunities.

Identity protection in action: Real-World scenarios enhancing your security

ATTACK, DETECT & INVESTIGATE – LAB 1 - (LIGHT)	
User and IP address reconnaissance (SMB)	SMB enumeration on a domain controller triggers an alert, exposing SYSVOL access patterns that attackers use to track login and move laterally.
Network Mapping Reconnaissance (DNS)	Attackers map networks via DNS reconnaissance; this alert detects unauthorized AXFR transfers and excessive queries.
Investigate a Reconnaissance & Discovery Alert	SMB enumeration on a domain controller triggers an alert, exposing SYSVOL access patterns that attackers use to track login and move laterally.

CREDENTIAL ACCESS ALERTS – LAB 2 - (FULL)	
Security Principal Reconnaissance (LDAP)	Defender for Identity detects LDAP reconnaissance, the initial phase of Kerberoasting attacks where attackers enumerate SPNs to obtain TGS tickets.
Suspected DC Sync attack (replication of directory services)	If attackers have DS-Replication-Get-Changes-All permission, they can replicate Active Directory data, triggering an alert if done from a non-domain controller.
Investigate a Credential Access Alert	MDI helps discover and analyze attacks, ensuring your environment's security. Investigate credential access alerts to understand potential threats.
Suspicious connection over EFS Remote Protocol	MDI detects LDAP reconnaissance, often the first phase of a Kerberoasting attack, used to gather Security Principal Names (SPNs) for obtaining TGS tickets.
Investigate a Lateral Movement Alert	Microsoft Defender for Identity helps discover and analyze attacks, ensuring security. Investigate lateral movement alerts to understand threats.
Data Exfiltration Over SMB	This alert triggers when suspicious data transfers, like copying the ntds.dit file from a domain controller to a workstation, are detected.
Investigate Other Alerts	Microsoft Defender for Identity helps discover and analyze attacks, ensuring security. Investigate other alerts to understand potential threats.

Versions: Your gateway to the Defender for Identity E-mmersion

Light

- **Scenarios:** Focuses on **up to 2 scenarios,** tailored to the needs and objectives of the session.
- **Attendees:** Designed for **up to 6 participants.**
- **Delivery:** Streamlined structure, with sessions designed to deliver an efficient and comprehensive understanding of the topics within **3 to 4 hours,** ensuring execution within a maximum timeframe of **up to 2 weeks.**

Available to selected customers who **qualify for Microsoft programs.**

Differential

- **Scenarios:** Focuses on the remaining scenarios, tailored to the needs and objectives of the session.
- **Attendees:** Designed for **up to 12 participants**.
- **Delivery:** Focused structure, with sessions organized to provide a thorough and efficient understanding of the topics in **4 to 8 hours,** maintaining a maximum execution window of **up to 2 weeks.**

Available for immediate purchase*/**

Full

- **Scenarios:** Focuses on **all scenarios,** tailored to the needs and objectives of the session.
- **Attendees:** Designed for **up to 12 participants**.
- **Delivery:** Focused structure, with sessions organized to provide a thorough and efficient understanding of the topics in **4 to 8 hours,** maintaining a maximum execution window of **up to 2 weeks.**

Available for immediate purchase*/**

*The Light version must already be executed, and either Microsoft or the customer must cover the cost of the additional use cases and activities.

**Either Microsoft or the customer must make the payment directly.

Additional information

This E-mmersion experience is designed for technical decision-makers and IT professionals to enhance their security posture using Microsoft Defender for Identity.

Engage in hands-on activities with real-world scenarios focused on protecting identities and improving organizational security posture.

Gain practical experience in implementing and managing Microsoft Defender for Identity solutions to detect and respond to advanced threats targeting your organization.

Receive technical support and expert guidance throughout the entire E-mmersion experience.

How to get started?

Contact us to learn more about the **Microsoft Defender for Identity (MDI) E-mmersion** experience or our **consulting services**:

LEARN MORE

Why choose Synergy Advisors as your strategic partner?

Consulting Services

13+ years of experience working with hundreds of clients and thousands of users in leading market organizations across various industries, specializing in Security & Compliance, Modern Work, Azure Data & AI, and Azure Infrastructure.

- Designing and implementing Microsoft solutions.
- Focused on usability and protection to drive upselling and adoption in key use cases.
- Integrated approach, creating synergies between Microsoft products.

Managed Services

Experts in cybersecurity, infrastructure, and Modern Work in Microsoft 365, Azure, and Windows 365.

- Proactive and reactive services. Monitoring, optimization, and continuous assessment of new services and features.
- Collaboration with other vendors, providing a single point of contact.
- Support contracts available for escalation with proprietary vendors.

E-Suite

Enhances Microsoft workloads' capabilities and reach to address modern business, governance, and operational needs:

Analytics, workflows, and self-service; empowering end users through:

- Micro-Visor
- E-Visor
- E-Visor Teams App
- E-Inspector
- E-Cryptor
- E-Vigilant
- E-Migrator

Let's talk about your cybersecurity needs:
e-mmersion-mdi@synergyadvisors.biz

SYNERGY ADVISORS