WorkshopPLUS - Detect, Respond and Recover Office 365 Security Incident

WorkshopPLUS

Duration: 3 Day [Remote / Onsite]

Difficulty Level: 300 - Advanced

Description

This offering will help you to learn and practice the necessary actions to detect, respond, and recover when a security incident occurs in a Microsoft 365 tenant.

Objectives

- Learn basic concepts about the different solutions available in Microsoft 365 to detect, respond, and recover from a security incident.
- Understand how to use Microsoft 365 tools for threat hunting (Auditing, Threat Explorer, default reports, and Microsoft Defender for O365).
- Learn how to use available tools to take the appropriate actions to secure Microsoft 365.

Outcomes

- Gain a deeper understanding of the security architecture and features available in Office 365.
- Improve your ability to detect security incidents within Office 365 using various tools and techniques.
- Gain practical experience through simulations and exercises that mimic real-world security incidents, so that you can apply what you learned in a controlled environment.

Methodology

Learn by example

Each group of modules is organized by scenario and examples to provide you with an in-depth understanding of the tools and experience necessary to find threats.

Hands-on Labs

- You will participate in hands-on labs and demonstrations to learn the concepts.
- Participants will have access to resources and labs for up to six months after completing the workshop.

Scope

This offering is scoped for Microsoft 365 Environments.

Agenda

Day 1

- User Compromised with malicious URL

Day 2

- User Compromised with malicious File

Day 3

- User compromised with malicious App

This data sheet is for informational purposes only.
MICROSOFT MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS SUMMARY

Microsoft

Delivery Outline

Requirements

Participants

- Office 365 Administrators

Skill Requirements

- Willing to learn how to detect, respond, and recover when security incidents occur in your O365 tenant.

Time Commitment

- Three full-day engagements with relevant roles. It is recommended to attend the entire engagement.

Delivery Requirements

- Computer with a supported version of Windows and audio equipment.
- Internet access with at least 1-Mbps bandwidth per student.
- A Microsoft/Windows Live ID to connect to the virtual environment.
- Microsoft Teams for remote deliveries.
- A modern browser capable of rendering web sites using current web standards.

Education

Day 1	User Compromised with malicious URL	▪ Campaigns ▪ Threat Analytics ▪ Threat Explorer ▪ Microsoft Defender for O365
Day 2	User compromised with malicious File	▪ Phishing and Malware Campaigns ▪ Advanced Auditing ▪ Advanced Hunting for data compromise
Day 3	User compromised with malicious App	▪ Applications in Azure Active Directory ▪ Manage Consent in Azure Active Directory ▪ Detect malicious applications and activities ▪ Investigate App Consent Grant ▪ Respond to illicit grant and applications

For more information: Contact your Microsoft Representative for more details.