Workshop - Microsoft 365 Security Center

WorkshopPLUS

Duration: 2 Days [Remote / Onsite]
Difficulty Level: 300 - Advanced

Description

The Workshop - Microsoft 365 Security Center is designed to provide you with the knowledge, expertise, and hands-on experience you need to configure and implement the various security features in the Microsoft 365 Security Center. This offering will help you adhere to the security mandates of your organization that affect different workloads within Office 365. Also, we examine the security tools commonly used by Microsoft 365 Security Administrators.

Objectives

After completing this workshop, you will:

- Understand the various security features presented and how they provide protection and mitigate the risk from threats like phishing, ransomware, impersonation, and loss of data.
- Understand how the Microsoft 365 Security Center provides unified security controls across Microsoft 365.

Outcomes

- Participants become knowledgeable about the different features of the Security Center and can competently integrate them into organizational security requirements.
- Attendees can now competently plan, create, publish, and manage policies for each feature in the Security Center.
- Participants apply their new skills in their enterprise environment.

Methodology

Learn by example

Each group of modules is organized by scenario and is designed to provide you with in-depth understanding, exposure to tools, and experience configuring and implementing the various security features in Microsoft 365.

Hands-on

- You will participate in hands-on labs and demonstrations to apply the key concepts of this offering.
- You will have access to resources and labs for up to six months after the workshop.

Scope

In scope

Microsoft 365 Commercial, Education, Government, or other cloud tenant

Not in scope

Azure Security Center

Agenda

Day 1

- Permissions in Microsoft 365 Security Center
- Protecting, training, and security for your organization

Day 2

- Seeing the Threat Stream
- Hunting the Threat; Incidents, Alerts, AIR, & Action; Next steps

Microsoft

Delivery Outline

Requirements	
Participants ▪ Microsoft 365 Administration staff who has already migrated to Microsoft 365, IT Change Management practitioner, Office 365 end-user support staff, security team, and incident response team **Skill requirements** ▪ Microsoft 365 administrators, basic knowledge of Microsoft 365 **Time commitment** ▪ Two full-day engagements with relevant roles	**Delivery requirements** • Microsoft/Windows Live ID to connect to the virtual environment **Hardware running:** ▪ Supported version of Windows ▪ Supported version of Office ▪ Modern browser, such as Microsoft Edge (or equivalent) ▪ Internet access

Education		
Day 1	Permissions, protection, and training	▪ Configure role-based access controls with role groups in the Microsoft 365 security portal. ▪ Use Microsoft Defender for Office 365, including Safe Attachments, Safe Links, Defender for O365 SharePoint Online, One Drive for Business and Teams, Anti-Phishing, Preset Policies, Configuration Analyzer, and MCAS/OCAS integration. ▪ Train your staff in Attack Simulation and the Learning Hub. Use Secure Score to help improve your overall security posture.
Day 2	Threat stream, hunting, incidents, action, and next steps	▪ Find and identify threats with Threat Analytics, Campaign Views, and the Security Center reports. ▪ Learn to use Advanced Hunting, Custom Detection Rules, and Threat Explorer and Trackers to give security teams visibility into their environments. ▪ Use the Incidents and Alerts feature to get the "whole picture" of an attack or other activity, including MCAS/OCAS integration. We also examine the Automated Investigation and Response feature and the Action Center. ▪ Adopt a holistic approach to security and your data and learn how to use the Security Center with other Microsoft technologies to secure your whole environment; next steps to implement these features.

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