Microsoft 365 Security and Compliance: Security Center

WorkshopPLUS

Duration: 2 days

Focus Area: Operations and Monitoring

Difficulty: 300 - Advanced

Overview

The Microsoft 365 Security Center workshop provides attendees with in-depth knowledge and understanding of how to leverage the Microsoft 365 Security Center. The workshop encourages compliance with the organization's security mandates.

Through presentations, white-board discussions, and goal-based labs, this workshop covers the security tools needed for the role of a Microsoft 365 security administrator.

Each group of modules is organized by scenario and designed to provide participants with this expertise and hands-on experience, which helps to configure and implement the various security features in Microsoft 365.

Objectives

After completing this training, students will be able to:

- Understand the various security features presented along with 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.

Key Takeaways

Course Material

Each group of modules is organized by scenario and is designed to provide participants with in-depth expertise, plus tools, and hands-on experience to configure and implement the various security features in Microsoft 365.

Hands-on Labs

- Most of the concepts with the modules covered will be supported by hands-on labs and demos.
- Attendees will have access to lab virtual machines for up to 6 months after workshop completion.

Agenda

Day 1

- Permissions in Microsoft 365 Security Center
- Protecting your Organization
- Training your Organization
- Security your Organization

Day 2

- Seeing the Threat Stream
- Hunting the Threat
- Incidents, Alerts, AIR, & Action
- Putting it all together

Plan for a two full days. Early departure on any day is not recommended due to the amount of content.

Course Details

Module 1: Permissions in M365 Security Center: This module focuses on how role-based access controls are configured using role groups in the Microsoft 365 security portal.

Module 2: Protecting your Organization: This module focuses on Microsoft Defender for Office 365 and includes 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.

Module 3: Training your Organization: This module will focus on Attack Simulation and its many facets and options, as well as the Learning Hub and how you can leverage its knowledge to better educate your team.

Module 4: Securing your Organization: Secure Score is the focus here, with its many improvement actions and reports intended to improve your overall security posture.

Module 5: Seeing the Threat Chain: This module highlights Threat Analytics, Campaign Views, and the Security Center reports; we discuss how this information can better prepare you to hunt for and identify threats in your organization.

Module 6: Hunting the Threat: This module focuses on Advanced Hunting, Custom Detection Rules, and Threat Explorer and Trackers; we'll review how these tools give security teams visibility into their environments which previously never existed.

Module 7: Incidents, Alerts, AIR, and Action: This module focuses on the Incidents and Alerts feature and how they can be used to get the "whole picture" of an attack or other activity; this includes MCAS/OCAS integration. We also examine the Automated Investigation and Response feature, as well as the Action Center.

Module 8: Putting it all together: A holistic approach to security and your data is discussed, emphasizing how the Security Center can be used in conjunction with other Microsoft technologies to secure your whole environment. We also discuss your organizations next steps towards implementation of these features so you're ready to put them to immediate use.

Recommended Qualifications

This is an advanced course for Microsoft 365 Security. It is aimed at Microsoft 365 administrators who have already migrated to Microsoft 365 or will be migrating soon.

Other roles to benefit from this course include the security team and incident response team.
The basic concepts and know-how of the product is covered in this course; however, it is expected that attendees already possess basic knowledge of Microsoft 365.

Hardware requirements

- An Intel Core-i5-based PC
- USB port
- Microsoft Account to connect to the virtual environment
- 4 GB RAM
- 128 GB HDD
- Windows 10
- Office 2016 Professional Plus+ or Office ProPlus
- Internet access with at least 1 Mbps bandwidth per student

For more information

Contact your Microsoft Account Representative for further details.

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

Microsoft