Device protection with Microsoft Endpoint Manager and Microsoft Defender for Endpoint

WorkshopPLUS

Duration: 3 days

Focus Area: Security and Compliance

Difficulty: Intermediate

Overview

This 3-day course summarizing the fundamental security components and features of any Microsoft Endpoint Configuration Manager environment, such as RBAC or role-based administration, Endpoint Protection, Exploit Guard, Application Guard, Microsoft Defender for Endpoint, BitLocker Drive Encryption and Compliance Settings. In addition to classic, on-prem management we also will explore the Intune management possibilities for some features like Compliance Policies, BitLocker for Co-managed windows 10 devices.

Objectives

After completing this course, you will understand how to set up, configure and manage:

- Microsoft Endpoint Configuration Manager Role Based Access
- Endpoint Protection for Microsoft Endpoint Manager
- Application Guard and Exploit Guard integration
- Microsoft Defender for Endpoint
- BitLocker Drive Encryption
- Compliance settings

Key Takeaways

Course Material

Each module contains scenarios that provide students with in-depth expertise, tools, and hands-on experience to help implement and troubleshoot Security Related concepts as they pertain to Microsoft Endpoint Configuration Manager.

Hands-on Labs

- Most of the concepts covered above will be supported by hands-on labs and demos.
- Lab environment is based on Microsoft Endpoint Configuration Manager CB 2010.
- Attendees have access to resources and labs for up to 6 months after workshop completion.

Agenda

Day 1

- Module 1: Introduction to Endpoint Security
- Module 2: Role Based Access Control (RBA)
- Module 3: Endpoint Protection Overview
- Module 4: Endpoint Protection Policies

Day 2

- Module 5: CAMP and Security Intelligence Updates
- Module 6: Endpoint Protection Alerts and Reporting
- Module 7: Endpoint Protection Troubleshooting
- Module 8: Exploit Guard and Application Guard

Day 3

- Module 9: Microsoft Defender for Endpoint
- Module 10: Device Encryption
- Module 11: Compliance Settings

Microsoft

Course Details

Module 1: Introduction to Endpoint Security

Overall introduction to security settings and recommendations that can be managed through Microsoft Endpoint Configuration Manager and Intune

Module 2: Role Based Access Control

Overview of Role Based Administration concept in Microsoft Endpoint Configuration Manager, including Reporting feature

Module 3: Endpoint Protection Technologies Overview

Deeper dive into the technologies that make up Endpoint Protection

Module 4: Antimalware Policies

Learn basic concepts and terminology for Endpoint Protection Antimalware Policies

Module 5: CAMP and Security Intelligence Updates

Manage Endpoint Protection Definition updates through Configuration Manager

Module 6: Endpoint Protection Alerts and Reporting

How to configure and use alerts and reports notifications within Configuration Manager

Module 7: Endpoint Protection Troubleshooting

Learn troubleshooting techniques for securing endpoints

Module 8: Exploit Guard and Application Guard

Learn about attack surface reduction, controlled folder access, exploit and network protection. Also learn how you can mitigate security threats with Application Guard

Module 9: Microsoft Defender for Endpoint

Learn how to onboard endpoints to Microsoft Defender for Endpoint using Microsoft Endpoint Configuration Manager and explore basic operational possibilities within Microsoft Defender for Endpoint

Module 10: Device Encryption

Learn what is BitLocker and explore modern management possibilities to control device encryption (MEMCM and Intune)

Module 10: Compliance settings

Deeper dive into the compliance settings topic, including management possibilities using Microsoft Endpoint Manager (Intune)

Recommended Qualifications

This course is targeted at IT staff who have already started designing and implementing Microsoft Endpoint Configuration Manager integration with Microsoft Security products and concepts.

To ensure that Students are successful at the end of this WorkshopPLUS, it is highly recommended they meet the following criteria:

- Existing knowledge of Microsoft Endpoint Configuration Manager
- Moderate knowledge of Windows Platform and Microsoft Security products
- Basic knowledge of Microsoft Endpoint Manager (Intune)

Hardware Requirements

Participants will require a computer with the following minimum configuration:

- **Operating system:** Windows 10 1809 or later
- **Processor:** Intel Core-i5
- **Memory:** 4 GB
- **Disk:** 128 GB
- **Peripherals:** USB port
- **Network:** 10 MBPS or faster network adapter
- **Application Software:** Office 365/2016 Professional Plus and a PDF reader
- **Microsoft Account:** Participants also need a Microsoft account to connect to the virtual environment.
- **Internet Connection:** The classroom must be networked with access to the Internet with at least Internet bandwidth of 10 MBPS. TCP port 443 must be open. We highly recommend a wired network in the classroom

For more information

Contact your Microsoft Account Representative for further details.

Microsoft