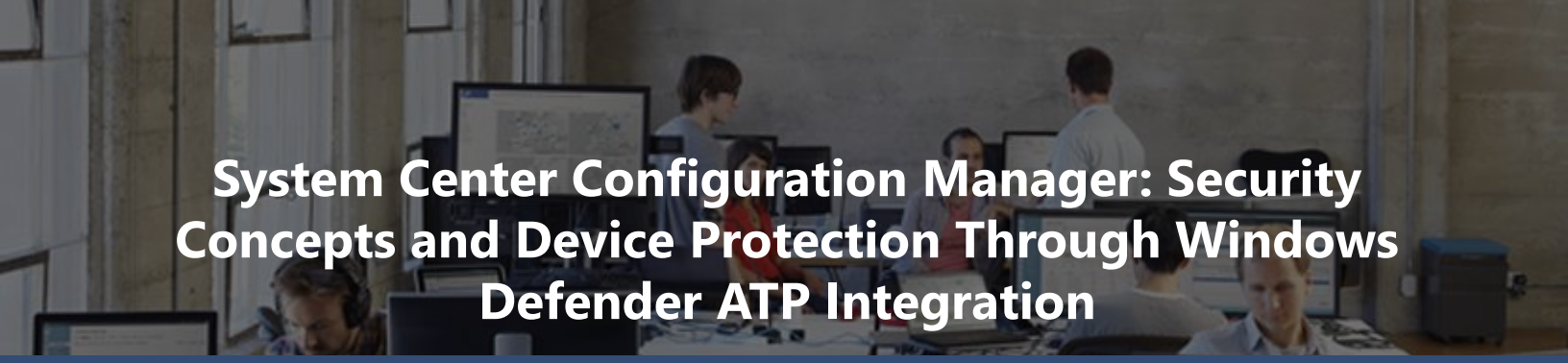


System Center Configuration Manager: Security Concepts and Device Protection Through Windows Defender ATP Integration

WorkshopPLUS

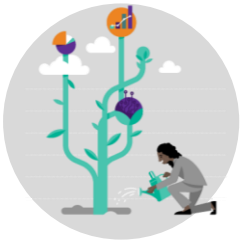
Duration: [4 days] | **Focus Area:** [Security and Compliance] | **Level**: [Advanced]

This 4-day course summarizes the fundamental security components of any System Center Configuration Manager environment, such as role-based administration, securing client endpoints, System Center Configuration Manager accounts and groups, privacy, System Center Endpoint Protection, Security Content Automation Protocol extensions and Windows Defender ATP Integration.

OUTCOMES

Security Concepts

Learn about SCCM security concepts



Compliance

Learn about SCCM Compliance settings

Advanced Protection

Learn how to integrate with Windows Defender ATP

PREREQUISITES

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

Recommended Qualifications

- Basic knowledge of the Microsoft Azure platform
- Advanced knowledge of System Center Configuration Manager

Hardware Requirements

- An Intel Core-i5-based PC
- 4 GB RAM
- 128 GB HDD
- Windows 7 SP1 or later
- Office 2013 Professional Plus
- Internet access with at least 1 Mbps bandwidth per student

Microsoft

AGENDA

Duration: 4 days

Module 1: Overview
Module 2: Role Based Access Control
Module 3: Endpoint Protection Overview
Module 4: Endpoint Protection Policies

Module 5: CAMP, Engine and Definition Updates
Module 6: Endpoint Protection Alerts and Reporting
Module 7: Endpoint Protection Technologies
Module 8: Endpoint Protection Troubleshooting

Module 9: Application Guard
Module 10: Exploit Guard
Module 11: Advanced Thread Protection

Module 12: Introduction to Software Updates
Module 13: Compliance Settings Overview
Module 14: SCAP Extensions

SYLLABUS

Module 1: Overview: This module provides an overview of different Security aspects that SCCM can support.

Module 2: Role Based access Control: In this module, you will be presented with techniques and necessary concepts to implement RBA in SCCM Hierarchy.

Module 3: Endpoint Protection Overview: This module presents the different components for System Center Endpoint Protection.

Module 4: System Center Endpoint Policies: This module outlines Endpoint protection policies, how create and manage it.

Module 5: CAMP, Engine and Definition Updates: In this module you will learn about Common Anti-Mallware Platform.

Module 6: System Center Endpoint Protection Alerts and Reporting: In this module, you will be presented with the most common reporting and alerting for SCEP.

Module 7: System Center Endpoint Protection Concepts Protection Technologies: This module provides an overview of the different SCEP capabilities and how to integrate with SCCM.

Module 8: System Center Endpoint Protection Troubleshooting: This module explains how to troubleshoot SCEP client

Module 9: Application Guard: This module provides an overview and system requirements for Application Guard and how to deploy it.

Module 10: Exploit Guard: In this module you will learn about Exploit Guard components and requirements.

Module 11: Advanced Thread Protection: This module explains what is ATP, its configuration methods and dashboards.

Module 12: Introduction to Software Updates: Software Updates in System Center Configuration Manager are a set of tools and resources that will help you manage the complex task of tracking and applying Software Updates to Computers across your Enterprise..

Module 13: Compliance Settings Overview This module explores SCCM Compliance settings and various ways an organization may use them.

Module 14: SCAP Extensions This module explores what SCAP Extensions are and how SCCM may use them for reporting purposes.

NEXT STEPS: If you are interested in a Compliance and Security Concepts for your organization, contact your Microsoft Account Representative.

Microsoft