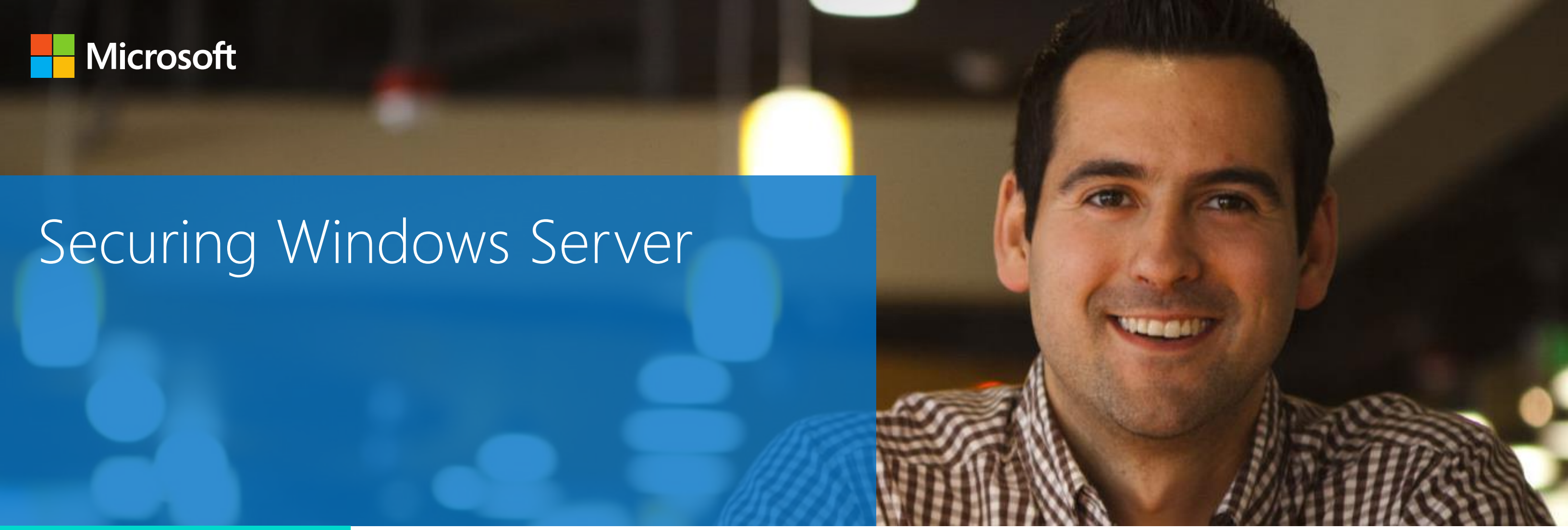

Securing Windows Server

Workshop*PLUS*

Target Audience

This WorkshopPLUS is targeted at the following IT professionals who deploy, design, and implement Windows Server environments::

- *IT Administrators*
- *Windows Infrastructure Engineers*
- *Server Administrators*
- *IT Security staff and Administrators*

Key Features and Benefits

- *Hands-on labs and demos*

Overview

Security threats are increasingly a focal point for many enterprises. Cyber-crime, industrial espionage, and diversity of malware are expanding dramatically. There is no single tool that can protect your assets against all threats. However, by protecting your Windows infrastructure with defenses at different layers of security, you can significantly reduce the potential exposure.

This WorkshopPLUS demonstrates Microsoft's technologies, tools, and methods which can be used to design a secure environment and to securely administer it, by significantly decreasing several risks in Windows environments, and by adapting recommended security processes and strategies.

The four-day Securing Windows Server WorkshopPLUS provides students with the skills required to protect Windows servers against unintended access or intrusion. The Microsoft security strategies that are discussed have been adopted by other security companies, to prevent successful attacks like *Pass-the-Hash* and *Pass-the-Ticket* and other credential theft attacks.

Technical Highlights

After completing this WorkshopPLUS, you will be able to:

- Understand typical security threats and the most effective Windows Server countermeasures against them.
- Protect a server against unauthorized access during and after the login and authentication processes.
- Secure a host against risks from unnecessary software and from non-secure settings.
- Properly secure applications using appropriate Windows Server tools and techniques

Syllabus

This Workshop*PLUS* suggested duration **four** days and contains level 200+ content and nine lab exercises.

Module 1: Introduction This module provides an overview of the current security landscape and explains identity being a security boundary. We also touch upon the *Clean Source* concept, the Microsoft Active Directory *Tiering* model, and the strongly recommended usage of *Privileged Access Workstations*

Module 2: Security IT Operations. This module details approaches to secure IT operations. We discuss the *Privileged Access Workstation* in detail and also take a deep-dive in the *Tiering* model. Furthermore, we discuss the new *Windows Administration Center* which eases configuration of *Just-Enough-Administration* (JeA).

Module 3: Securing the Identity. We will have a look into the built-in *Just-Enough-Administration* feature of Windows, but also the Microsoft *Privileged Access Management* solution, that enables *Just-in-Time* (JiT) privileges to administrators and that adheres to the Microsoft *Tiering* model. Furthermore we will look into the usage of *Authentication Policies and Silos* to restrict where administrators can logon to. We end this module with detailed information on password-less authentication.

Module 4: Protect and Detect – Part 1. We start this module with explaining the *virtualization-based security* feature within Windows, after which we discuss in detail Windows Defender features like *Device Guard, (kernel) Control Flow Guard, (remote) Credential Guard, Exploit Guard* and *Advanced Threat Protection*.

Module 5: Protect and Detect – Part 2. In module 5 we take a closer look to the Windows Defender Firewall and learn how IPsec can assist with securing unsecure systems and/or protocols, in combination with the Defender Firewall.

We learn how *Azure Advanced Threat Protection* can assist with detecting potential malicious activities, and we briefly go through some new security features of AD Domain Services.

We finish this module with information on legacy protocols, why they are considered unsecure, and how you can disable these protocols.

Module 6: How can we help: In the final module of this workshop, we briefly mention additional Microsoft security offerings which you might find valuable.

Prerequisites

The students must possess knowledge of the following:

- *Security threats and vulnerabilities*
- *Group policy management*
- *Windows Firewall*
- *Network security concepts*

Hardware Requirements

Labs are hosted on the *Labs On Demand* internet platform. Students need access to the Internet for the entire length of this workshop. For best user experience, it is recommended to provide two monitors for each user.

© 2020 Microsoft Corporation. All rights reserved.
This data sheet is for informational purposes only.
MICROSOFT MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS SUMMARY