Microsoft

Security - Securing Windows Server

WorkshopPLUS

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

- *On-Demand hands-on labs and demos*

Overview

The 4-day WorkshopPLUS – Security - Securing Windows Server course provides students with the skills required to ensure that host servers are secure and protected from unwanted access or intrusion. This workshop covers security threats, threat modelling countermeasures, and Windows Server 2016 strategies, tools, and best practices for comprehensively securing servers from the file system, applications, and server communications across a network. The workshop also focuses on the use of the security-rich features of Windows Server 2016 to help detect and defend against security threats that target your most valuable organizational assets.

The workshop contains Level 200+ content that covers people and process as well technical security topics. So, while it covers technical concepts it is a balance between process and technology that results in Defense in Depth. In this workshop, we outline common security risks to each layer of Security in the Defense in Depth Model, and discuss mitigations for those risks.

Please review the target-audience information and contact your Microsoft Services representative to ensure that this workshop is appropriate to the student's experience and technical expertise.

Technical Highlights

After completing this course, 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 2016 tools and techniques

Syllabus

Prerequisites

The students must possess knowledge of the following:

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

Hardware Requirements

- *Students should attend the course with their own laptops in order to consume the Learning-on-Demand labs.*

This Workshop*PLUS* suggested duration four full days. Students should anticipate consistent start and end times for each day. Early departure on any day is not recommended.

Module 1: Security Threat Landscape. This module provides an overview of impact of security, general vulnerabilities, threats and layered security protection, protecting the virtualization fabric. It covers Pass-the-Hash attack mitigation techniques.

Module 2: Introduction to Threat Modelling. This module presents topics covering SDL and threat modelling essentials.

Module 3: Hardening Servers. This module details tools that help you define security baselines, tooling that have Microsoft recommended practices, and enforcing security settings across a large number of systems.

Module 4: Mitigating Credential Theft. This module provides foundations for understanding Credential Theft, and introduces concepts like Tier Modelling and Containment models, as well as using IPSec to secure traffic and identities.

Module 5: Mitigating Credential Theft – modern approach. Here we take the discussion a little bit further, and cover core topics such as Just Enough Administration and Just In Time administration. We complete the with Credential Guard.

Module 6: Securing Systems – modern approach: This module focuses on new concepts in securing Windows servers including Device Guard, Code Integrity Policies and Guarded Fabric.

Module 7: Security Architecture. In IT today, securing only the endpoints won't resolve all challenges. Building and understanding architecture plays a key role. These lessons are covering secure administrative workstations, and secure administrative environments.

Microsoft