# Securing Windows Server 2016



**Meet the expert:** Patrick Loner has certifications for MCSA, MCSE, MCITP, A+, Network+, Security+, and more. He has been working as a Microsoft Certified Trainer, network administrator, and network consultant for over ten years. He has over a decade of experience working with and teaching about Windows networks with client and server operating systems. He has guided many students toward Microsoft and CompTIA certifications. Most recently, he has worked as a freelance trainer and network consultant specializing in Windows Server 2008 and Microsoft Exchange 2007 and Exchange 2010 implementations, design, and upgrades. Patrick continues to branch out now working with and training on Windows Server 2012, Windows 8, Exchange 2013, and System Center Configuration Manager 2012.

**Prerequisites:** none

**Runtime:** 13:18:23

**Course description:** This training series focuses on how to secure Windows Server 2016 environments. It covers methods and technologies for hardening server environments and securing virtual machine infrastructures using Shielded and encryption-supported virtual machines and Guarded Fabric. In addition, the series covers the protection of Active Directory and identity infrastructure with the Enhanced Security Administrative Environment (ESAE) Administrative Forest design approach and the management of privileged identities using Just-in-Time (JIT) and Just-Enough-Administration (JEA) approaches, along with Privileged Access Workstations (PAWs) and Local Administrator Password Solution (LAPS). The series also covers threat detection solutions, such as auditing, implementing Advanced Threat Analytics (ATA), the understanding of Operations Management Suite (OMS) solutions, and workload-specific security including the use of Nano Server for particular server workloads.

**Course outline:**

**Understanding Attacks**
- Introduction
- Assume Breach
- Methods of Attack
- Attack Stages
- Prioritizing Resources
- Incident Response Strategy
- Ensuring Compliance
- Summary

**Detecting Security Breaches**
- Introduction
- Locating Evidence
- Event Logs
- Examining Other Configurations
- Summary

**Using Sysinternals Tools**
- Introduction
- Introducing Sysinternals
- Demo: Sysinternals
- Introduction to FSRM
- System Monitor
- AccessChk
- Autoruns
- LogonSessions
- Process Explorer
- Process Monitor
- Sigcheck
- Demo: Locating Systinternals
- Demo: LogonSessions
- Demo: Process Explorer
- Demo: Process Monitor
- Summary

**User Rights and Priveleges**
- Introduction
- Principle of Least Privilege
- Configuring User Rights
- Configuring Account Security Options
- Demo: Control Privileges
- Demo: Account Options
- Demo: Active Directory in PowerShell
- Demo: User Properties
- Account Security Controls
- Complexity Options
- Summary

**Assigning Privileges**
- Introduction
- Password and Lockout Policies
- Demo: Password Policies
- Configuring Fine-Grained Password Policies
- Understanding PSO Application
- Protected Users Security Groups
- Delegating Administrative Control
- Demo: Access Control Lists
- Local Administrator Password Solutions
- LAPS Requirements
- LAPS Process
- Configuring and Managing Passwords
- Demo: LAPS
- Demo: LAPS GPO
- Summary

**Computer and Service Accounts**
- Introduction
- What Is a Computer Account
- Computer Account Functionality
- Working with Secure Channel Passwords
- Service Account Tyoes
- Group MSAs
- Demo: Configure MSA
- Demo: MSA Continued
- Summary

**Protecting User Credentials**
- Introduction
- Introducing Credential Guard
- Credential Guard Requirements
- Configuring Credential Guard
- Verifying Credential Guard Operation
- Credential Guard Weaknesses
- NTLM Blocking
- Searching AD DS for Problem Accounts
- Demo: Locate Problem Accounts
- Summary

**Privileged Access**
- Introduction
- The Need for Privileged Access Workstations
- Privileged Access Workstations
- Jump Servers
- Securing Domain Controllers
- Summary

**Deploy JEA**
- Introduction
- Introduction to JEA
- JEA Components
- Session Configuration Files
- Demo: Session Configuration File
- Role Capability Files
- Demo: Configure JEA
- Demo: DNSops File
- JEA Endpoints
- Demo: JEA Endpoint
- Connecting to JEA Endpoints
- Deploying JEA Endpoints
- Summary

**Enhanced Security**
- Introduction
- ESAE Forests
- Administrative Tiers
- ESAE Best Practices
- The Clean Source Principle
- Implementing the Clean Source Principle
- Summary

**Identity Manager**
- Introduction

*(Continued on page 2)*

# Securing Windows Server 2016



- Overview of MIM
- MIM Requirements
- MIM Service Accounts
- Summary

**IT Admin and PAM**
- Introduction
- Overview of JIT Administration
- Privileged Access Management
- PAM Components
- Creating an Administrative Forest
- Configuring Trust Relationships
- Shadow Principals
- Configuring the MIM Web Portal
- Managing and Configuring PAM Roles
- Summary

**Windows Defender**
- Introduction
- Understanding Malware
- Malware Sources
- Mitigation Methods
- Windows Defender
- Demo: Configure Windows Defender
- Demo: Scan with Windows Defender
- Summary

**Restricting Software**
- Introduction
- Controlling Applications
- Software Restriction Policies
- Security Levels
- AppLocker
- AppLocker
- Support for AppLocker
- Creating Default Rules
- Demo: AppLocker
- Demo: Create Rules
- Summary

**Using Device Guard**
- Introduction
- Ovierview of Device Guard
- Device Guard Features
- Configuring Device Guard
- Device Guard Policies
- Deploying Code Integrity Policies
- Control Flow Guard
- Summary

**Patch Management**
- Introduction
- Overview of WSUS
- Deployment Options
- Server Requirements
- Configuring Clients
- Administering WSUS
- Approving Updates
- Demo: Installl WSUS
- Demo: Navigate WSUS
- Demo: WSUS Options
- Summary

**Auditing**
- Introduction
- Overview of Auditing
- The Purpose of Auditing
- Types of Events
- Auditing Goals
- Auditing File and Object Access
- Demo: Define Audit Policies
- Demo: Event Log Settings
- Summary

**Advanced Auditing**
- Introduction
- Advanced Auditing
- Advanced Auditing Subcategories
- Dynamic Auditing
- Event Log Subscriptions
- Audit Collection Services
- Demo: Event Forwarding
- Demo: Events
- Auditing with Windows PowerShell
- Demo: Auditing with PowerShell
- Demo: Event Logs in PowerShell
- Transaction Logging
- Module Logging
- Script Block Logging
- Demo: Get Logging Modules
- Demo: Logging
- Summary

**Advanced Threat Analytics**
- Introduction
- Overview of ATA
- Usage Scenarios
- Deployment Requirements
- ATA Gateways
- Port Mirroring
- Configuring ATA Center
- Summary

**Operations Management**
- Introduction
- Introduction to Operations Management Suite
- Deployment Overview
- OMS Solutions
- Installing OMS
- OMS Solutions Continued
- Summary

**Virtualization Infrastructure**
- Introduction
- Introduction to Guarded Fabric
- Host Guardian Service
- Preparing HGS Nodes
- Installing and Configuring HGS
- Attestation and Encryption
- Attestation Methods
- Initializing HGS
- Configuring HSG Clients
- Summary

**Security Baselines**
- Introduction
- Security Compliance Manager
- SCM Requirements
- Demo: Install SCM
- Demo: Import GPOs
- Demo: Configuring a Baseline
- Demo: Deploy a Baseline
- Summary

**Deploy Nano Server**
- Introduction
- Planning for Nano Server
- Understanding Nano Server Roles
- Installing Nano Server Roles
- Nano Server Installation
- Installation Steps
- Summary

**File Encryption**
- Introduction
- Introducing Encrypting File System
- EFS Features
- Encryption and Decryption
- Recovering EFS Files
- Demo: EFS
- Demo: Encrypting Folders
- Summary

**BitLocker**
- Introduction
- Overview of BitLocker
- BitLocker and TPMs
- BitLocker Requirements
- Tools for Configuring and Managing BitLocker
- Deploying BitLocker
- Demo: Deploying BitLocker
- Demo: Enable BitLocker on Client
- BitLocker on Hyper-V VMs
- BitLocker and CSVs
- Enabling BitLocker for CSV
- Network Unlock
- Network Unlock Process
- BitLocker Recovery
- Microsoft BitLocker Administration and Monitoring
- Summary

**File Server Resource Manager**
- Introduction
- Capacity Management
- Storage Management
- Introduction to FSRM
- Overview of FSRM
- Installing and Configuring FSRM
- Demo: FSRM
- Quota Management
- Demo: Create Quotas
- Demo: Using Quotas
- Summary

**File Screens and Reports**
- Introduction
- File Screening
- Using File Groups
- Exceptions and Templates
- Demo: File Screens
- Demo: File Screen Properties
- Storage Reports
- Report Tasks
- Demo: Storage Reports
- Demo: Generate Reports
- Automatic File Management
- Summary

**Classification and File Management**
- Introduction
- File Classification
- Classification Rules
- Demo: Classify Confidential Documents
- Demo: Classification Continued
- File Management Tasks
- Summary

**Dynamic Access Control**
- Introduction
- Overview of Dynamic Access Control
- Dynamic Access Control Scenarios
- DAC Technologies
- Understanding Identity
- Understanding Claims
- Types of Claims
- Central Access Policies
- Policy Components
- DAC Prerequisities
- Demo: Prepare for DAC
- Demo: Create Claim Type
- Demo: DAC
- Summary

**Windows Firewall**
- Introduction
- Types of Firewalls
- Well-Known Ports
- Host-Based Firewall
- Network Profiles
- Configuring the Windows Firewall
- Demo: Configure the Firewall via Control Panel
- Demo: Windows Firewall with Advanced Security
- Demo: Configure the Firewall via PowerShell
- Demo: Configure the Firewall be GPME


*(Continued on page 3)*

# Securing Windows Server 2016



• Summary

**Datacenter Firewall**
• Introduction
• Network Controller
• Datacenter Firewall
• Network Security Groups
• Scenarios for Datacenter Firewall
• Summary

**Utilizing IP Security**
• Introduction
• Overview of IP Security
• IPSec Protocols
• IPSec Usage Scenarios
• IPSec Configuration Tools
• Connection Security Rules
• Understanding Rule Types
• Rule Endpoints
• Authentication Settings
• Authentication Methods
• Encryption Settings
• Monitoring Connections
• Demo: Implementing IPSec
• Demo: Protocols
• Summary

**Advanced DNS Settings**
• Introduction
• Managing DNS Services
• Optimizing DNS Name Resolution
• The GlobalNames Zone
• Implementing DNS Security
• DNS Security (DNSSEC)
• Implementing DNSSEC
• Demo: DNSSEC
• Demo: Validating Responses
• Introducing DNS Policies
• Implementing DNS Policies
• RRL Feature
• Demo: Configure DNS Policies
• Demo: RRL
• Summary

**Monitoring Network Traffic**
• Introduction
• Microsoft Message Analyzer
• Demo: MMA
• Summary

**Securing SMB Traffic**
• Introduction
• SMB 3.1.1 Protocol Security
• SMB Encryption Requirements
• Encrypting SMB Shares
• Disabling Support for SMB 1.0
• Summary