Securing Windows Server 2019

Getting Started with Windows Server 2019 Security

- Introduction
- Windows Server 2019 Security Capabilities
- SMB Security Features
- Securing SMB - Auditing and Blocking SMB
- Securing SMB - SMB Signing
- Securing SMB - SMB Encryption
- NTLM Security
- Implementing NTLM Security
- DNS Security
- Implementing DNSSEC
- Secure Management
- Managing Servers Using Windows Admin Center

Securing Credentials

- Introduction
- Protecting Credentials
- Demystifying the Microsoft Tiering Model
- Using the "Protected Users" Group
- Authentication Policy and Silo
- Protecting Privileged Accounts with Authentication Policies and Silos
- Local Admin Password Solution (LAPS)
- Preparing Active Directory for LAPS
- Installing the LAPS Client Side Extension
- Working with LAPS
- Credential Guard
- Verifying Hardware Compatibility for Credential Guard
- Enabling Credential Guard
- User Rights Assignment
- Working with User Rights Assignment
- Privileged Access Workstation (PAW)

Protecting against Malware

- Introduction
- Windows Defender Highlights

- Onboarding Server 2019 into Microsoft Defender for Endpoints
- Configuring Windows Defender Using Group Policy
- Configuring Microsoft Defender Exploit Guard Using GPO
- Configuring WSUS to Update Windows Defender
- Understanding Applocker Design and Components
- AppLocker Rule Conditions
- Implementing Applocker
- Windows Defender Application Control
- Implementing Windows Defender Application Control
- Windows Defender Application Control Compared to Applocker

Hardening Using Baselines

- Introduction
- What Is a Security Baseline?
- Why Use a Security Baseline?
- Where to Find Security Baselines?
- Downloading the Windows Server 2019 Security Baseline and Security Compliance Toolkit
- Working with Policy Analyzer
- Importing Microsoft's Security Baseline