Securing Windows Server 2016, Part 3 of 5: Auditing and Infrastructure

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: This is part 3 of the course

Runtime: 02:08:00

Course description: This course covers auditing and threat analytics. It will talk about auditing events and using group policy, dynamic auditing, virtualization infrastructure, guarded fabric and shielded virtual machines. It will then cover deploying security baselines, host guardian service, nano server and server roles.

Course outline:

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