Securing Windows Server 2016 (On Demand OD20744)

Securing Windows Server 2016 (On Demand OD20744)

Seminar | Zurzeit keine Termine | Teilnahmebescheinigung

E-Learning | 40 Unterrichtseinheiten

Seminarnummer: 29483 | Herstellernummer: OD20744

Stand: 01.05.2024. Alle aktuellen Informationen finden Sie unter https://akademie.tuv.com/s/29483

This MOC On Demand teaches IT pros how they can enhance the security of the IT infrastructure that they administer. This course begins by emphasizing the importance of assuming that network breaches have occurred already, and then teaches you how to protect administrative credentials and rights to help ensure that administrators can perform only the tasks that they need to, when they need to.

Nutzen

After completing this MOC On Demand online course, students will be able to:

- Secure Windows Server.
- Protect credentials and implement privileged access workstations.
- Limit administrator rights with Just Enough Administration.
- Manage privileged access.
- Mitigate malware and threats.
- Analyze activity with advanced auditing and log analytics.
- Deploy and configure Advanced Threat Analytics and Microsoft Operations Management Suite.
- Configure Guarded Fabric virtual machines (VMs).
- Use the Security Compliance Toolkit (SCT) and containers to improve security.
- Plan and protect data.
- Optimize and secure file services.
- Secure network traffic with firewalls and encryption.
- Secure network traffic by using DNSSEC and Message Analyzer.

® TÜV, TUEV und TUV sind eingetragene Marken. Eine Nutzung und Verwendung bedarf der vorherigen Zustimmung.

Zielgruppe

IT-Administratoren, IT-Consultants, Verantwortliche für IT Security in Windows Infrastrukturen

Voraussetzungen

This course explains how you can use auditing and the Advanced Threat Analysis feature in Windows Server 2016 to identify security issues. You will also learn how to mitigate malware threats, secure your virtualization platform, and use deployment options such as Nano server and containers to enhance security. The course also explains how you can help protect access to files by using encryption and dynamic access control, and how you can enhance your networks security.

Students should have at least two years of experience in the IT field and should have:

- Completed courses 740, 741, and 742, or the equivalent.
- A solid, practical understanding of networking fundamentals, including TCP/IP, User Datagram Protocol (UDP), and Domain Name System (DNS).
- A solid, practical understanding of Active Directory Domain Services (AD DS) principles.
- A solid, practical understanding of Microsoft Hyper-V virtualization fundamentals.
- An understanding of Windows Server security principles.

Inhalte des Seminars

Module 1: Attacks, breach detection, and Sysinternals tools

This module frames the course so that students are thinking about security in environments where the infrastructures basis is predominantly Microsoft products. The module begins with teaching students about the -assume breach-philosophy and getting them to understand the different types of attacks that can occur, including attack timelines and vectors. Additionally, it gets students thinking about key resources, how they respond when they detect an incident, and how an organizations direct needs and legislative requirements dictate its security policy.

Module 2: Protecting credentials and privileged access

This module covers user accounts and rights, computer and service accounts, credentials, Privileged Access Workstations, and the Local Administrator Password Solution. In this module, students will learn about configuring user rights and security options, protecting credentials by using Credential Guard, implementing Privileged Access Workstations, and managing and deploying Local Administrator Password Solution to manage local administrator account passwords.

Module 3: Limiting administrator rights with Just Enough Administration

This module explains how to deploy and configure Just Enough Administration (JEA), which is an

® TÜV, TUEV und TUV sind eingetragene Marken. Eine Nutzung und Verwendung bedarf der vorherigen Zustimmung.

administrative technology that allows students to apply role-based access control (RBAC) principles through Windows PowerShell remote sessions.

Module 4: Privileged access management and administrative forests

This module explains the concepts of Enhanced Security Administrative Environment (ESAE) forests, Microsoft Identity Manager (MIM), and Just In Time (JIT) Administration, or Privileged Access Management (PAM).

Module 5: Mitigating malware and threats

This module explains how to use tools such as Windows Defender, Windows AppLocker, Microsoft Device Guard, Windows Defender Application Guard, and Windows Defender Exploit Guard.

Module 6: Analyzing activity with advanced auditing and log analytics

This module provides an overview of auditing, and then goes into detail about how to configure advanced auditing and Windows PowerShell auditing and logging.

Module 7: Deploying and configuring Advanced Threat Analytics and Microsoft Operations Management Suite

This module explains the Microsoft Advanced Threat Analytics tool and the Microsoft Operations Management suite (OMS). It also explains how you can use them to monitor and analyse the security of a Windows Server deployment. You will also learn about Microsoft Azure Security Center, which allows you to manage and monitor the security configuration of workloads both on-premises and in the cloud.

Module 8: Secure Virtualization Infrastructure

This module explains how to configure Guarded Fabric VMs, including the requirements for shielded and encryption-supported VMs.

Module 9: Securing application This module describes the SCT, which is a free, downloadable set of tools that you can use to create and apply security settings. You will also learn about improving platform security by reducing the size and scope of application and compute resources by containerizing workloads.

Module 10: Planning and protecting data

This module explains how to configure Encrypting File System (EFS) and BitLocker drive encryption to protect data at rest. You will also learn about extending protection into the cloud by using Azure Information Protection.

Module 11: Optimizing and securing file services

This module explains how to optimize file services by configuring File Server Resource Manager (FSRM) and Distributed File System (DFS). Students also will learn how to manage access to shared files by

® TÜV, TUEV und TUV sind eingetragene Marken. Eine Nutzung und Verwendung bedarf der vorherigen Zustimmung.

Terminübersicht und Buchung

Buchen Sie Ihren Wunschtermin jetzt direkt online unter https://akademie.tuv.com/s/29483 und profitieren Sie von diesen Vorteilen:

- Schneller Buchungsvorgang
- Persönliches Kundenkonto
- Gleichzeitige Buchung für mehrere Teilnehmer:innen

Alternativ können Sie das Bestellformular verwenden, um via Fax oder E-Mail zu bestellen.

® TÜV, TUEV und TUV sind eingetragene Marken. Eine Nutzung und Verwendung bedarf der vorherigen Zustimmung.