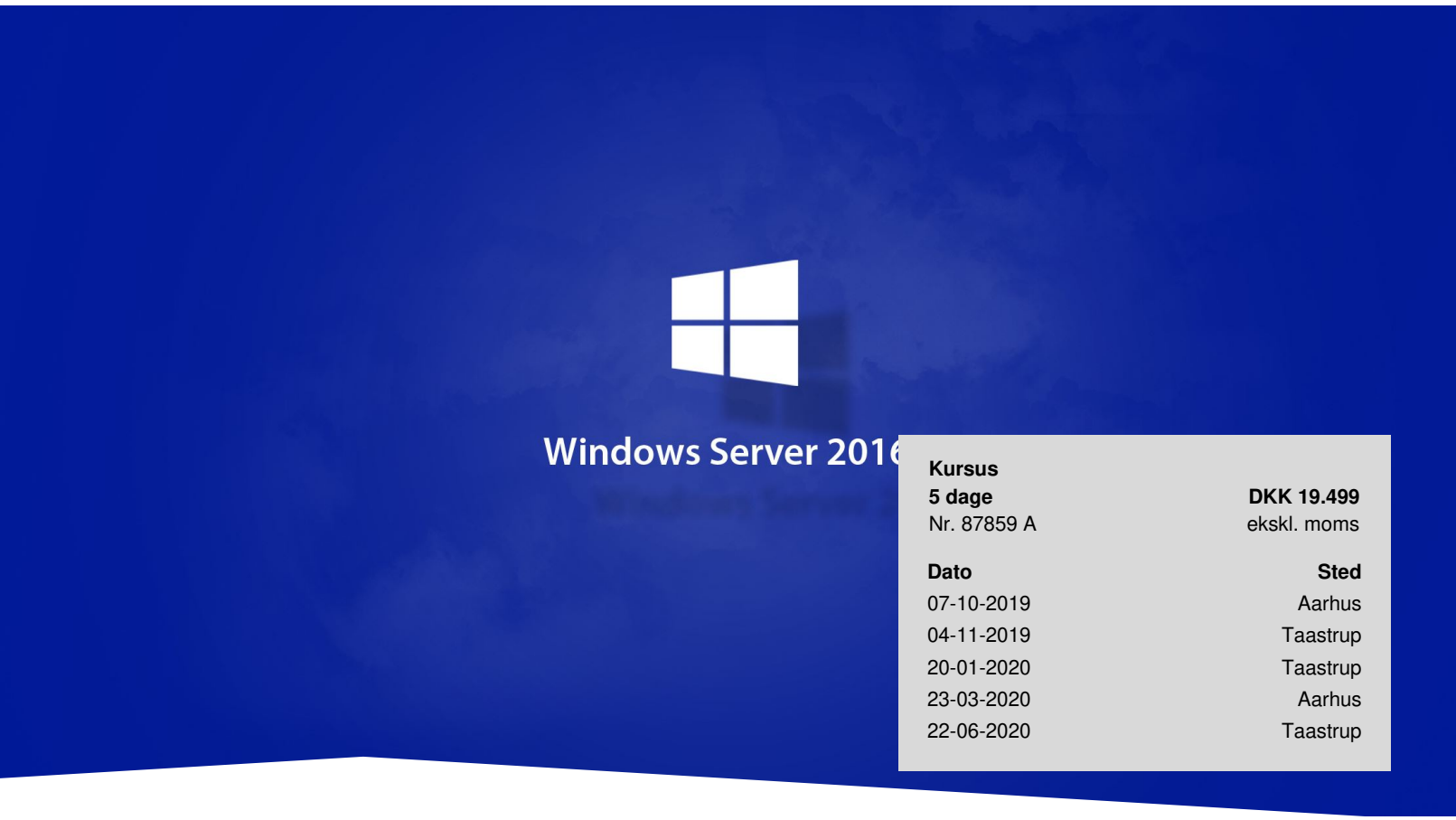
TEKNOLOGISK INSTITUT



Kursus
5 dage **DKK 19.499**
Nr. 87859 A ekskl. moms

Dato	Sted
07-10-2019	Aarhus
04-11-2019	Taastrup
20-01-2020	Taastrup
23-03-2020	Aarhus
22-06-2020	Taastrup

Securing Windows Server 2016 [20744]

Lær, hvordan du øger sikkerheden på jeres IT-infrastruktur. Kurset tager udgangspunkt i, at der er allerede er sket et brud på netværket, og hvordan du forhindrer at det gentager sig. Du lærer også, hvordan du beskytter rettigheder og oplysninger bedst muligt og hvordan det er muligt at begrænse unødvendige handlinger samtidig med at driften opretholdes.

This course also details how you can mitigate malware threats, identify security issues by using auditing and the Advanced Threat Analysis feature in Windows Server 2016, secure your virtualization platform, and use new 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 network's security.

Forudsætninger

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

- Completed courses 20740, 20741, and 20742, 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.

Deltagerprofil

Teknologisk Institut
kurser@teknologisk.dk
+45 72 20 30 00

This course is for IT professionals who need to administer Windows Server 2016 networks securely. These professionals typically work with networks that are configured as Windows Server domain-based environments, with managed access to the Internet and cloud services.

Students who seek certification in the 70-744 Securing Windows server exam also will benefit from this course.

Indhold

Module 1: Breach detection and using the Sysinternals tools

- Overview of breach detection
- Using the Sysinternals tools to detect breaches

Module 2: Protecting credentials and privileged access

- Understanding user rights
- Computer and service accounts
- Protecting credentials
- Understanding privileged-access workstations and jump servers
- Deploying a local administrator-password solution

Module 3: Limiting administrator rights with Just Enough Administration

- Understanding JEA
- Configuring and deploying JEA

Module 4: Privileged Access Management and administrative forests

- Understanding ESAE forests
- Overview of MIM
- Implementing JIT and Privileged Access Management by using MIM

Module 5: Mitigating malware and threats

- Configuring and managing Windows Defender
- Using software restricting policies (SRPs) and AppLocker
- Configuring and using Device Guard
- Using and deploying the Enhanced Mitigation Experience Toolkit

Module 6: Analysing activity by using advanced auditing and log analytics

- Overview of auditing
- Understanding advanced auditing
- Configuring Windows PowerShell auditing and logging

Module 7: Analysing activity with Microsoft Advanced Threat Analytics feature and Operations Management Suite

- Overview of Advanced Threat Analytics
- Understanding OMS

Module 8: Securing your virtualization an infrastructure

- Overview of Guarded Fabric VMs
- Understanding shielded and encryption-supported VMs

Module 9: Securing application development and server-workload infrastructure

- Using Security Compliance Manager
- Introduction to Nano Server
- Understanding containers

Teknologisk Institut
kurser@teknologisk.dk
+45 72 20 30 00

Module 10: Protecting data with encryption

- Planning and implementing encryption
- Planning and implementing BitLocker

Module 11: Limiting access to file and folders

- Introduction to FSRM
- Implementing classification management and file-management tasks
- Understanding Dynamic Access Control (DAC)

Module 12: Using firewalls to control network traffic flow

- Understanding Windows Firewall
- Software-defined distributed firewalls

Module 13: Securing network traffic

- Network-related security threats and connection-security rules
- Configuring advanced DNS settings
- Examining network traffic with Microsoft Message Analyzer
- Securing SMB traffic, and analysing SMB traffic

Module 14: Updating Windows Server

- Overview of WSUS
- Deploying updates by using WSUS

Certificering

Kurset leder hen mod eksamen 70-744 Securing Windows Server 2016. Eksamen bestilles og betales særskilt.

Læs mere om IT-certificering.

Microsoft Software Assurance Vouchere

Kurset kan betales med 5 SA vouchere.

Underviser

Undervisningen varetages af en erfaren underviser fra Teknologisk Instituts netværk bestående af branchens dygtigste undervisere.

Har du faglige spørgsmål så kontakt

Charlotte Heimann
+45 72203147
chhn@teknologisk.dk