training code: AA_20744 / ENG DL 5d / EN

Securing Windows Server 2016

Purpose of the training

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

Benefits of completing the training

After completing this 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.

Expected Listener Preparation

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.
- To increase the comfort of work and training’s effectiveness we suggest using an additional monitor. The lack of additional monitor does not exclude participation in the training, however, it significantly influences the comfort of work during classes.

Training Language

- **Training**: English
- **Materials**: English

Training Includes

- manual in electronic form available on the platform: https://www.altkomakademia.pl/
- access to Altkom Akademia's student portal
- manual in electronic form available on the platform: https://www.altkomakademia.pl/
- access to Altkom Akademia's student portal

Duration

5 days / 35 hours

Training agenda

1. Attacks, breach detection, and Sysinternals tools
   - Understanding attacks
   - Detecting security breaches
   - Examining activity with the Sysinternals tools
2. Protecting credentials and privileged access

- Understanding user rights
- Computer and service accounts
- Protecting credentials
- Privileged Access Workstations and jump servers
- Local administrator password solution

3. Limiting administrator rights with Just Enough Administration
   - Understanding JEA
   - Verifying and deploying JEA
4. Privileged access management and administrative forests
   - ESAE forests
   - Overview of Microsoft Identity Manager
   - Overview of JIT administration and PAM
5. Mitigating malware and threats
   - Configuring and managing Windows Defender
   - Restricting software
   - Configuring and using the Device Guard feature
6. Analyzing activity with advanced auditing and log analytics
   - Overview of auditing
   - Advanced auditing
   - Windows PowerShell auditing and logging
7. Deploying and configuring Advanced Threat Analytics and Microsoft Operations Management Suite
   - Deploying and configuring ATA
   - Deploying and configuring Microsoft Operations Management Suite
   - Deploying and configuring Azure Security Center
8. Secure Virtualization Infrastructure
   - Guarded fabric
   - Shielded and encryption-supported virtual machines
9. Securing application development and server-workload infrastructure
   - Using SCT
   - Understanding containers
10. Planning and protecting data
    - Planning and implementing encryption
    - Planning and implementing BitLocker
    - Protecting data by using Azure Information Protection
11. Optimizing and securing file services
    - File Server Resource Manager
    - Implementing classification and file management tasks
    - Dynamic Access Control

12. Securing network traffic with firewalls and encryption
    - Understanding network-related security threats
    - Understanding Windows Firewall with Advanced Security
    - Configuring IPsec
    - Datacenter Firewall
13. Securing network traffic
14. Configuring advanced DNS settings
15. Examining network traffic with Message Analyzer
16. Securing and analyzing SMB traffic