# Course : Windows 2016, securing your infrastructure

*Practical course - 3d - 21h00 - Ref. WSI*
*Price : 1800 € E.T.*

This course will provide you with the knowledge you need to secure your Windows Server 2016 environment and implement the security tools that are built into it. You'll see how to secure the OS, Active Directory, create a PKI architecture, and protect your data and network access.

## Teaching objectives

**At the end of the training, the participant will be able to:**

- Key features of a secure infrastructure
- Setting up a certificate server
- Implement Active Directory security
- Implement NAP with mandatory access controls
- Implementing IPSec on Windows

## Intended audience

System administrators and engineers.

## Prerequisites

Good knowledge of TCP/IP, Windows Server 2016 administration and Active Directory.

## Course schedule

### 1 Operating system security

- Minimum installation option and Core mode.
- Dynamic access control for user accounts.
- Windows 2016 Server advanced firewall.
- Windows login and authentication: NTLM authentication.
- Implementation of update management (WSUS).
- Assessing, identifying and managing safety with MSAT, MBSA and MSCM tools.

**Hands-on work**
Basic settings and parameters for securing a Windows 2016 server.

---

**PARTICIPANTS**
System administrators and engineers.

**PREREQUISITES**
Good knowledge of TCP/IP, Windows Server 2016 administration and Active Directory.

**TRAINER QUALIFICATIONS**
The experts leading the training are specialists in the covered subjects. They have been approved by our instructional teams for both their professional knowledge and their teaching ability, for each course they teach. They have at least five to ten years of experience in their field and hold (or have held) decision-making positions in companies.

**ASSESSMENT TERMS**
The trainer evaluates each participant's academic progress throughout the training using multiple choice, scenarios, hands-on work and more.
Participants also complete a placement test before and after the course to measure the skills they've developed.

## 2. Certificates and PKI architecture

- PKI basics.
- Certificate and private key management.
- The certificate server role.
- 2-level PKI architecture.
- Certification authority server: certification authority (AD-CS).

### Hands-on work

Setting up a certificate server. Basic certificate administration. Securing Web access with HTTPS.

## 3. Securing Active Directory

- Basic principle of AD security.
- What's new in Active Directory Certificate Services (AD CS).
- RODC (Read-Only Domain Controller): benefits and implementation.
- ACL (access control list) protection.

### Hands-on work

Active Directory security. Password granularity. RODC installation and configuration.

## 4. Data protection

- Reminder of the fundamentals of NTFS and ReFS security.
- Setting up EFS. EFS limits.
- BitLocker: disk encryption and encryption key storage.

### Hands-on work

Implementation of EFS. Data recovery with an agent.

## 5. NAP network access protection

- Configure NAP (Network Access Protection).
- Control of internal and external PCs.
- Configure NAP implementation for VPN.
- NPS servers. RADIUS Infrastructure components.

### Hands-on work

Set up NAPs with mandatory access controls. Restrict network access for non-DHCP-compliant machines.

## 6. VPN and IPSec

- VPNs: the tunneling principle.
- Secure domain access with IPSec.

### Hands-on work

Implementing IPSec on Windows. Advanced firewall configuration. RADIUS server setup.