Reference: AM/EN/SW11

Windows 11 Workstation Security Training Course

Best Practices, Hardening and Threat Prevention

Duration: 3 Days | Hours: 21 h

Remote · Sessions guaranteed from 1 registrant · 60% hands-on practice

DESCRIPTION

Windows workstations are a prime target for cyberattacks — ransomware, credential theft, lateral movement and shadow IT all start with a compromised endpoint. Without clear security policies and well-configured tools, the risks of data leaks or intrusions increase significantly.

This training course provides you with the keys to effectively securing Windows 10 and 11 workstations, from the fundamentals to advanced hardening techniques. It covers Microsoft's modern security stack — Defender, BitLocker, SmartScreen, Application Control, LAPS — combined with hardening baselines and user awareness, for a defence-in-depth approach that holds up in real production environments.

LEARNING OBJECTIVES

By the end of this training course, participants will be able to:

- Identify common vulnerabilities on Windows workstations
- Implement Microsoft security recommendations
- Configure BitLocker, Defender, SmartScreen, firewalls and updates
- Apply GPOs or usage restriction scripts
- Train users to adopt safe behaviours
- Strengthen local security without compromising productivity

PREREQUISITES

- Basic knowledge of the Windows environment (10 or 11)
- Understanding of user accounts, UAC and local security
- Experience in system administration or IT support desirable

> *Because each participant is unique, a personalised interview is systematically organised in advance with our expert to design a training programme perfectly aligned with their objectives, level and professional challenges.*

TARGET AUDIENCE

IT administrators, security managers, workstation technicians and digital workplace advisors.

DETAILED PROGRAMME

> The training alternates between theoretical input and hands-on practice (approximately 60% of the time). Modules are built around practical exercises based on real-world business use cases.

Module 1 – Risks and Vulnerabilities on Windows Workstations

- Types of threats: malware, phishing, USB keys, shadow IT
- Business impact and real-life incident cases
- Threat landscape specific to Windows endpoints

Module 2 – Authentication and Identity Security

- Local accounts vs Microsoft Entra ID
- Passwords, MFA and biometric security (Windows Hello)
- Session lockout and inactivity policies

Module 3 – Data and System Protection

- Encryption with BitLocker
- USB copy protection and sensitive file management
- Recovery keys and TPM management

Module 4 – Microsoft Protection Tools

- Microsoft Defender Antivirus and SmartScreen
- Windows Firewall, Core Isolation and Virtualisation-Based Security (VBS)
- Windows Defender Application Guard

Module 5 – Workstation Hardening

- PowerShell scripts and execution restrictions
- Port deactivation and security-specific GPOs
- Software restriction policies and AppLocker / WDAC

Module 6 – Awareness and Good User Practices

- Phishing and social engineering recognition
- Risky behaviour and alert messages
- Update management and ongoing user training

TEACHING METHODS

Format and Delivery

The training is delivered remotely via an interactive virtual classroom. It can also be delivered on-site, with content customised to match the needs of your professional project. The theory/practice split is approximately 40%/60%.

MFE-IT Ultra-Personalised Format

Each session accommodates between 1 and 3 participants, ensuring highly individualised support. A preliminary interview allows us to tailor the content to each participant's profile. Inter-company sessions are guaranteed from just 1 registrant (except in cases of force majeure).

Skills Assessment

Throughout the training, the trainer assesses participant progress through multiple-choice questions, role-playing exercises and hands-on work. At the end, a certificate of achievement is issued to each participant.

Post-Training Support

For one month following the training, each participant can contact MFE-IT trainers with questions about implementing acquired knowledge. A response is provided by email or telephone within 48 working hours.

Accessibility

MFE-IT is committed to welcoming people with disabilities. Contact: contact@mfe-it.com.

PRACTICAL INFORMATION

Trainer Resources

- Structured demonstrations aligned with the detailed programme
- Exercise briefs and solutions throughout the training
- A ready-to-use technical environment for practical workshops
- Trainer validation of acquired knowledge at the end of each workshop
- Digital reference documents

Certification and Validation

At the end of the training, a certificate is sent by email specifying the objectives, nature, duration and assessment results. A completion certificate can also be provided on request.

Benefits for Participants

- Train from your workplace or home, with no travel required
- Benefit from an expert trainer-consultant on the subject
- Enjoy an ultra-personalised format (1 to 3 participants)
- Continue training even in the event of unforeseen circumstances

Benefits for the Organisation

- Optimise the training budget by reducing travel and accommodation costs
- Offer quality training to all employees, regardless of location
- Reduce absence time linked to travel
- Support team upskilling in all contexts