Reference: MB/EN/SECL1

Cybersecurity Training Course Level 1

Identifying, Analysing and Countering Threats

Duration: 1 Day | Hours: 7 h

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

DESCRIPTION

Cybersecurity is no longer just about policies and tools. It relies on the ability to understand attackers' techniques in order to better defend against them. This is the mindset shift that makes the difference between a defender who reacts and one who anticipates.

This immersive Cybersecurity Level 1 training course immerses you in the world of cyber threats and teaches you, through hands-on experience, how to detect, analyse and block the most common attacks. Through real-world scenarios (phishing, ransomware, network scanning, privilege escalation), you will develop the essential reflexes of a security professional while consolidating your technical foundations.

LEARNING OBJECTIVES

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

- Understand the lifecycle of a cyberattack (reconnaissance, exploitation, persistence)
- Identify common threats: phishing, malware, exploits, lateral movement
- Use analysis and defence tools (Wireshark, fail2ban, AV, EDR)
- Respond effectively in the event of compromise or suspicion
- Apply technical and behavioural best practices
- Strengthen the security culture within the team or organisation

PREREQUISITES

- Proficiency with Windows or Linux workstations
- Basic knowledge of networks, systems or IT architecture
- No cybersecurity prerequisites required (beginner to intermediate level)

> *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 technicians, system and network administrators, and anyone wishing to take an active stance against cyber threats.

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 – Overview of Current Threats

- Types of attacks: phishing, ransomware, DDoS, APT
- Attackers' motivations and threat actor profiles
- Common entry points into organisations

Module 2 – Offensive Methodology: Understand the Adversary

- Reconnaissance, mapping and network scanning
- Privilege escalation and lateral movement
- Data exfiltration and Red Team thinking

Module 3 – Detection and Investigation

- Network analysis and detection of abnormal activity
- System logs, antivirus and EDR signals
- Post-mortem analysis of a compromised workstation

Module 4 – Responding to an Attack

- Isolation, containment and communication
- Removal of the intruder and evidence collection
- Initial actions and first-hour playbook

Module 5 – Best Practices and Security Culture

- MFA, backups and password policies
- Update management and patching discipline
- User training and security awareness

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