Publication date : 06/06/2024

Course : Protecting yourself against viruses and malware in the Microsoft environment

Practical course - 2d - 14h00 - Ref. MAL
Price : 1610 CHF E.T.

★★★★★ 5 / 5

This training course details the computer viruses and malware that degrade computer operation and disrupt business activity. At the end of the course, you'll be able to set up an approach, choose the best techniques and use the right tools to detect and eradicate them.

Teaching objectives

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

- ✓ Identify and neutralize malware or viruses
- ✓ Distinguishing infection from dysfunction
- ✓ Use the right tools to detect and eradicate them
- ✓ Draw up an action plan in line with the company's needs

Intended audience

System/network/security technicians, administrators and engineers.

Prerequisites

Good knowledge of networked Windows workstation management.

Practical details

Hands-on work

Workstations running Windows 10 and Windows Server 2016 will be used to put the concepts presented into practice.

Course schedule

PARTICIPANTS

System/network/security technicians, administrators and engineers.

PREREQUISITES

Good knowledge of networked Windows workstation management.

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.

1 Basic concepts

- What are viral infections?
- Defining the virus concept. The right tools.
- The jungle of names (backdoor, worm, Trojan horse, bot/botnet...).
- General principles of threat operation.
- The most common infection vectors.
- Disabling and bypassing safety devices.

Hands-on work

Infection analysis (backdoor, rootkit, etc.). Spyware and phishing.

2 How can I protect myself? Antivirus and Firewall

- Operating principles.
- Types of detection (signature, heuristic, behavioral, etc.).
- Packers (UPX, FSG, Upack, Armadillo, Themida...).
- False alarms.
- Firewall overview. The right tools.
- What can it detect?
- What are its limits?

Hands-on work

Detection test with the different types and bypassing of a firewall.

3 Mechanisms of infection

- How programs work.
- The relationship with DLLs.
- Code injections.
- How to detect a boot infection? The right tools.
- Windows startup reminder.
- The right tools.
- Infections and the registry.

Hands-on work

Example of viral injection. Simulation of malicious code in start-up phase and eradication techniques.

4 Identify for better eradication

- The importance of identifying the threat.
- Use the most appropriate tool: Windows Defender, competing tools.
- Eradicate "the eternal return".
- Remove inactive residues.

Hands-on work

Using scripts to counter infections. How to identify sources of infection? Eradicate without formatting.

TEACHING AIDS AND TECHNICAL RESOURCES

- The main teaching aids and instructional methods used in the training are audiovisual aids, documentation and course material, hands-on application exercises and corrected exercises for practical training courses, case studies and coverage of real cases for training seminars.
- At the end of each course or seminar, ORSYS provides participants with a course evaluation questionnaire that is analysed by our instructional teams.
- A check-in sheet for each half-day of attendance is provided at the end of the training, along with a course completion certificate if the trainee attended the entire session.

TERMS AND DEADLINES

Registration must be completed 24 hours before the start of the training.

ACCESSIBILITY FOR PEOPLE WITH DISABILITIES

Do you need special accessibility accommodations? Contact Mrs. Fosse, Disability Manager, at psh-accueil@orsys.fr to review your request and its feasibility.

5 Prevention rather than cure

- Raising user awareness.
- Procedures to be implemented.
- Choosing your security systems.
- Backups and restore points.
- Choosing the right tools.
- Market solutions and the antivirus appliance.

Hands-on work

Identify the stages in a company action plan.

Dates and locations

REMOTE CLASS

2026 : 26 Mar., 11 June, 22 Oct.