# Ransomware: Effective Defense and Recovery

Duration: 1 day
Audience: Professionnel TI

## Who is this training for?

- Security Teams
- IT Directors
- CISOs
- Business Continuity Managers

## Training objectives

- Understand the methods and impacts of ransomware
- Implement prevention and awareness strategies
- Develop recovery and continuity plans
- Learn from real-life cases to build resilience

## Summary

This hands-on training equips participants to prevent, detect and recover from ransomware attacks.

Through concrete cases, learners will develop defence and resilience capacities.

## Course outline

### Module 1: Understanding Ransomware

- History and Evolution
- Attack Vectors and Techniques
- Operational and Financial Impacts

### Module 2: Prevention Strategies

- Endpoint and Network Defense
- Backup Planning and Recovery
- User Training and Awareness

**Module 3: Detection and Response**

- Indicators of Compromise
- Incident Response Playbooks
- Legal and Forensic Considerations

**Module 4: Recovery and Improvement Continuous**

- Continuity Planning and Disaster Recovery
- Case Studies: Major Attacks
- Building Organizational Resilience

## Approach and methodology

Practical case studies, incident simulation, collaborative discussion

## Prerequisites

General knowledge of cybersecurity

## Recommendations

Review: the basics of cybersecurity the types of computer threats (malware, phishing)

Familiarize yourself with: IT environments and their vulnerabilities

Identify your challenges: ransomware protection business continuity disaster recovery