+33 (0)1 48 10 09 46
formation@ambient-it.net
140 Avenue Jean Lolive 93500 Pantin - France

Updated on 29/11/2023

Sign up

Resilient Infrastructure Training : Anti-Malware & Ransomware

4 days (28 hours)

PRESENTATION

Organized cybercrime is expected to cost the global economy $5,200 billion a year between 2020 and 2025. All businesses are affected by this threat, which accounts for losses of 6 billion euros in France. The number of malicious software programs, also known as ransomware or malware, is constantly increasing year after year. To counter this threat, technical solutions exist to make your infrastructure resilient. These solutions are based not only on best practices and technical methods for strengthening system security, but also on threat detection, attack analysis, knowing how to stop the attack and drawing up a BCP (Business Continuity Plan) or DRP (Disaster Recovery Plan). Our resilient architecture training course will teach you the concepts that will enable you to develop an IT system that is protected from attack, reinforce the integrity of your backups, learn the various steps to take after an attack, forensic analysis of the attacker and draw up a business continuity plan.

OBJECTIVES

- Be able to develop a resilient infrastructure
- Good knowledge of protection against various cyber attacks
- Implement a resilient database management system with an appropriate backup strategy
- Forensic analysis
- Know the different procedures to follow in the event of cybercriminal attacks
- Estimate costs and draw up a BCP

TARGET AUDIENCE

- IT security project managers
- SSI technicians
- Auditors
- Sliders

- CISO / RSSI
- Ethical hackers
- Highly critical engineers or administrators

Prerequisites

- Basic knowledge of web security

Anti-Malware & Anti-Ransomware Resilient Infrastructure Training Program

Protecting your IS

- Using IAM (Identity and Access Management)
- Setting up your firewall
- Encrypt your communications
- Input validation and whitelisting to protect against cyber attacks
- Best practices to protect against phishing
- Best practices to protect against password theft
- Protect yourself against key logger attacks with Key Scrambler
- Use secure Linux systems
- Use containerized applications to isolate the threat

Backup and data protection strategy

- Create your own data protection process
- Design a robust storage system (LVM, RAID, etc.)
- Database replication
- Choose your backup (item vs image-level backup, selective inclusion or selective exclusion)
- Backup protection (encryption, air gaps, immutability)
- Choose a retrieval type (image, instant...)
- Discover Veam: Modern Data Protection

Redeployment strategy

- Set up your own deployment stack in the event of an incident
- Ansible
- Docker & Kubernetes
- Puppet
- Automated infrastructure replication

Discover the weaknesses in your infrastructure

- Using IDS and IPS to detect a cyberattack
- Protect your site from SQL injection with Burp Suite
- Protect your site from XSS vulnerabilities with Burp Suite
- Testing your SSL/TLS protocol
- Scan your site for malicious scripts

Setting up your Honeypot

- Active defense of its infrastructure
- Lure and neutralize before it's too late
- Monitoring
- Collection
- Analysis

Immediate response to an incident

- Immediate analysis
- Eliminating the threat
- The ISO 27035 standard
- Collecting evidence of the attack
- Legal procedure

Forensic analysis of your system and network

- Discover the attack with Wireshark
- Use forensic collection tools (FastIR, log2timeline...)
- Analyze file systems
- Studying system artifacts
- Log study
- Memory analysis
- Examining the network with Wireshark
- Malware and ransomware review with VirusTotal

Drawing up a recovery plan

- Assess the financial and logistical impact
- Set up a crisis management (CM) system
- Set up a business continuity plan (BCP)
- Monitoring BCP results

Keycloak training

Advanced Keycloak training

Android Security and Pentest training

OWASP Java Training

OWASP training with .NET

Companies concerned

This training course is aimed at both individuals and companies, large or small, wishing to train their teams in a new advanced computer technology, or to acquire specific business knowledge or modern methods.

Positioning on entry to training

Positioning at the start of training complies with Qualiopi quality criteria. As soon as registration is finalized, the learner receives a self-assessment questionnaire which enables us to assess his or her estimated level of proficiency in different types of technology, as well as his or her expectations and personal objectives for the training to come, within the limits imposed by the selected format. This questionnaire also enables us to anticipate any connection or security difficulties within the company (intra-company or virtual classroom) which could be problematic for the follow-up and smooth running of the training session.

Teaching methods

Practical course: 60% Practical, 40% Theory. Training material distributed in digital format to all participants.

Organization

The course alternates theoretical input from the trainer, supported by examples, with brainstorming sessions and group work.

Validation

At the end of the session, a multiple-choice questionnaire verifies the correct acquisition of skills.

Sanction

A certificate will be issued to each trainee who completes the course.