Updated on 30/09/2025

Sign up

Cybersecurity Introductory Course

10 days (70 hours)

PRESENTATION

Our "Introductory Cybersecurity Course" is designed for technicians and system and network administrators who wish to acquire a global and operational vision of IT security and move into cybersecurity professions.

Over the course of ten days, you will develop a global vision of cybersecurity and its environment, by discovering the economic and societal stakes, the threat actors and the institutional and regulatory ecosystem. You'll learn to understand and use the main cybersecurity reference frameworks, standards and tools (ISO, NIST CSF, CIS Controls, ANSSI, SIEM, EDR, vulnerability scanners), while integrating essential legal obligations (RGPD, NIS2, LPM).

The course will also enable you to gain an understanding of the various cybersecurity-related professions and their career paths, so you can better situate your role and development prospects in this fast-growing field. You will be trained to identify the main risks and threats (malware, ransomware, phishing, APTs, Cloud/IoT misconfigurations) and to implement the appropriate protection measures (defense in depth, Zero Trust, IAM, supervision, incident management).

Finally, you will learn how to integrate good IT security practices into your day-to-day activities, raise user awareness and contribute to building a genuine cybersecurity culture within your organization.

At the end of the course, you'll be able to apply the fundamental principles, standards and tools of cybersecurity in an operational context.

OBJECTIVES

- Gain an overview of cybersecurity and its environment (challenges, ecosystem, etc.).
- Understand the various cybersecurity standards and tools.
- Gain an understanding of cybersecurity-related professions

- Understand the legal obligations associated with cybersecurity
- Understand the main risks and threats, as well as protective measures
- Identify best practices in IT security

TARGET AUDIENCE

- Anyone interested in a career in cybersecurity
- System and network technicians and administrators

Prerequisites

General knowledge of information systems and familiarity with the ANSSI security hygiene guide.

OUR TRAINING PROGRAM: INTRODUCTORY COURSE IN CYBERSECURITY

[Day 1 - Morning]

Introduction and context

- Why cybersecurity is strategic: economic & societal issues
- Recent major incidents and business impacts
- Threat actors: cybercrime, hacktivism, espionage

[Day 1 - Afternoon] Security

fundamentals

- CIA model (Confidentiality, Integrity, Availability)
- Attack surfaces and intrusion vectors
- "Misuse cases and risk-based approach
- Cryptography: encryption, hashing, signatures, certificates
- Practical workshop: Mapping an organization's critical assets.

Legal ecosystem and framework

- ANSSI, CERT-FR, ENISA, CNIL: roles & interactions
- RGPD, NIS2, LPM overview: key obligations
- Legal responsibilities & sanctions
- Practical workshop: Case study. Impacts of an RGPD breach.

[Day 2 - Morning]

International standards

- ISO/IEC 27001 & 27002, ISO 27035 (incidents)
- NIST CSF & CIS Controls: comparison
- ANSSI IT hygiene guide

[Day 2 - Afternoon]

Governance and PSSI

- Drawing up a security policy (PSSI)
- Roles, responsibilities, security committees
- Indicators & dashboards
- Practical workshop: Creating a mini-ISPP for an SME.

Compliance and audit

- Security audit methodology
- Security debt management
- Remediation plan and follow-up
- Practical workshop: Simulation of a basic audit.

[Day 3 - Morning]

Cybersecurity professions

- Overview of roles: CISO, SOC analyst, pentester, auditor, forensic
- Key interactions: in-house teams, service providers, CERT/ANSSI
- Essential skills according to sector (technical, organizational, cross-functional)
- Practical workshop: mapping a career path in cybersecurity.

[Day 3 - Afternoon] Certifications & career paths

- Professional paths: offensive (pentest), defensive (SOC/Blue Team), governance (CISO/consultant)
- Panorama of certifications: Security+, eJPT, CEH (beginners), CISSP, OSCP, ISO Lead (advanced)
- Building a career plan: stages, specialization, continuous monitoring

Everyday tools

- SIEM, EDR, IDS/IPS, IAM
- Vulnerability scanners (SCA/SAST/DAST)
- Alerting, correlation & sorting
- Practical workshop: Handling a simple scanner.

[Day 4 - Morning] Threat

typology

- Malware, ransomware, APT, supply chain
- Social engineering & human risks
- IoT, mobility, cloud: new vectors
- Practical workshop: Phishing simulation & debriefing.

[Day 4 - Afternoon] Technical

vulnerabilities

- System, network, application
- CVE life cycle
- Examples: Heartbleed, Log4Shell

Risk analysis & management

- Quick overview: EBIOS RM, MEHARI, FAIR
- Probabilities, impacts, risk appetite
- Risk mapping & prioritization
- Practical workshop: Mini-EBIOS on a fictitious IS.

[Day 5 - Morning]

Perimeter security

- Firewalls, proxies, web/mail filtering
- VPN & remote access
- Bastion and DMZ
- Practical workshop: Configuring a software firewall.

[Day 5 - Afternoon]

Defense in depth & Zero Trust

- Layering principles
- Micro-segmentation & PoLP
- Dynamic access controls

Supervision & detection

- Log collection & correlation
- SIEM, SOC, UEBA
- Detection use cases
- Practical workshop: Analyzing a system log.

[Day 6 - Morning]

Application security: key principles

- Secure Coding principles
- Understanding the main vulnerabilities (OWASP Top 10)
- Input validation & error handling
- Sessions & strong authentication
- Essential logging & encryption
- Presentation of tools: OWASP ZAP, Burp Suite
- Hands-on workshop: OWASP Juice Shop (a deliberately vulnerable application) and automated scanning with ZAP.

[Day 6 - Afternoon]

Mastering critical vulnerabilities

- A01 Broken Access Control to A10
- Prevention & remediation mechanisms
- Checklists & code reviews
- Practical workshop: OWASP mapping on a test application. Put the OWASP Top 10 into practice on a vulnerable application, linking each vulnerability encountered to its category and associated associated countermeasures.

DevSecOps & Shift Left

- Shift Left" principle: integrate security from the earliest stages
- Secure development cycle (Secure SDLC)
- Introduction to automatic analysis tools (SAST, DAST, SCA)
- Quality & continuous validation (tests, security gates)

[Day 7 - Morning] Cloud

security

- Shared responsibility (IaaS/PaaS/SaaS)
- Common configuration errors
- Hardening & monitoring
- Practical workshop: Audit of a simulated cloud environment.

[Day 7 - Afternoon]

Introduction to Containers & Kubernetes

- Introduction: fast, flexible deployment, but new attack surfaces (images, secrets, network)
- Image hardening: use minimal, updated and scanned images for vulnerabilities
- Secure secret management: protected passwords, keys and certificates
- Network policies: control and limit inter-container communications
- Good deployment practices: least privilege, workload isolation, continuous supervision

IAM & identity

- MFA, SSO, OAuth 2.1, OIDC
- Roles, RBAC/ABAC
- Zero Trust applied to identities
- Practical workshop: Configuring an MFA on a cloud service.

[Day 8 - Morning]

Incident management

- NIST SP 800-61: complete workflow
- Playbooks & CERT/CSIRT organization
- Automation & SOAR (principles)
- Practical workshop: Incident table-top exercise.

[Day 8 - Afternoon]

Forensic & evidence

- Chain of custody & legality
- Logging and timeline
- Tools & procedures

Crisis communication

- Internal vs. external: messages & channels
- Role of management & IT
- Notifications to authorities (CNIL, etc.)
- Practical workshop: Post-incident communication simulation.

[Day 9 -

Morning] Human

factor

- Social engineering mechanisms
- Ongoing awareness programs
- Case studies: phishing, pretexting, tailgating

[Day 9 - Afternoon]

Good user practices

- Passwords & MFA
- Digital hygiene (updates, backups)
- Workstations & mobiles
- Practical workshop: Creating an awareness kit.

Cybersecurity culture

- Integration into corporate culture
- Rituals, challenges, gamification
- Measuring maturity & ROI
- Practical workshop: Designing an annual campaign.

[Day 10 - Morning]

Review & overview

- Key points & transversal synthesis
- Feedback from participants
- Guided Q&A and self-assessment

[Day 10 - Afternoon]

Comprehensive case

study

- Scenario: company victim of ransomware
- Attack vector analysis & containment
- Response plan & remediation
- Practical workshop: end-to-end incident management (technical, organizational, communication)

Perspectives and career paths

- Career opportunities & cybersecurity specializations
- Recommended labs for progress: TryHackMe, HackTheBox, Blue Team Labs, LetsDefend, OWASP Juice Shop
- Recommendation of an individual 90-day action plan (guided progress via labs)

Pentest Web Training

Keycloak Training

Keycloak Advanced 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 IT 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, the learner receives a self-assessment questionnaire enabling us to assess his or her estimated level in different types of technology, as well as his or her expectations and personal objectives for the forthcoming course, 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 training: 60% hands-on, 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 is used to check that skills have been correctly acquired.

Certification

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