Publication date : 01/16/2024

Course : Cybersecurity and new technologies, advanced training

Practical course - 3d - 21h00 - Ref. NYP
Price : 2470 CHF E.T.

You've already been introduced to data vulnerabilities in both the big data and embedded worlds. We offer you the opportunity to deepen this knowledge, to analyze the security of blockchain, the cloud and certain sensitive systems, and to gain a better understanding of cybersecurity as a whole.

Teaching objectives

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

- ✓ Maîtriser les enjeux de la cybersécurité des nouvelles technologies
- ✓ Knowing the best cybersecurity practices applied to new technologies
- ✓ Understanding the threats to blockchain
- ✓ Understanding the threats to cloud and big data

Intended audience

Security managers and architects. System and network technicians and administrators.

Prerequisites

Knowledge of networks and systems. Completion of the training course "Cybersecurity and new technologies, introduction" or equivalent.

Practical details

Exercise

Each new theoretical concept is followed by a practical application.

Teaching methods

Active teaching, presentations, group discussions, interactive exchanges.

Course schedule

PARTICIPANTS

Security managers and architects. System and network technicians and administrators.

PREREQUISITES

Knowledge of networks and systems. Completion of the training course "Cybersecurity and new technologies, introduction" or equivalent.

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 Reminders of cryptology, the historical blockchain

- Basic cryptology for blockchain.
- Different hashing algorithms.
- The historical blockchain: bitcoin.
- Consensus by mining.
- Bitcoin in figures and pictures.

Storyboarding workshops

Cryptology, blockchain.

2 Attacks and defense in blockchain

- Sécurité blockchain vs cloud.
- Blockchain and IoT (Internet of Things) security.
- Blockchain et vérification d'identité. Blockchain et supply chain.
- Common vulnerabilities.
- Solidity, le langage des smart contracts.
- Hyperledger, la plateforme open source de développement de blockchain.
- Smart contract development security (language, methodology, verification).
- Best practices for securing blockchain.

Hands-on work

Safety analysis.

3 The "blockchain" Hyperledger

- Principles and terminology.
- Different types of nodes.
- Service architecture.
- Operator confidentiality.
- The basics of Go, the language of smart contracts.

Hands-on work

Construction of a blockchain and first Go tests.

4 Threats to cloud computing

- Cloud risk assessment and management using ISO 27005.
- The specifics of risk management in the cloud.
- The main risks identified by ENISA.
- Understanding security analysis.
- Cloud security tools.

Hands-on work

Security analysis on Amazon Web Services EC2.

5 Threats to big data

- Storage solutions: HDFS, NoSQL databases, Hadoop, HBase, MongoDB...
- The architectures used.
- Les différentes vulnérabilités.

Storyboarding workshops

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.

6 System vulnerabilities

- Botnets: how are they created?
- Home automation vulnerabilities: surveillance cameras, alarms, TVs, connected locks...
- Vulnerabilities and attacks on WiFi networks.
- Malware attacks targeting microcomputers, tablets and smartphones: drive-by download...
- Best practices for securing these systems.

Hands-on work

Safety analysis.

Dates and locations

REMOTE CLASS

2026 : 11 Mar., 20 May, 5 Oct., 16 Dec.