Course : Artificial intelligence and operational safety

AI as a field of possibilities for malicious acts

Synthesis course - 1d - 7h00 - Ref. ICY

Price : 990 CHF E.T.

4,1 / 5

This training course will help you understand what artificial intelligence (AI) is, how to define it in the context of cybersecurity, the importance of securing our connected objects, our identities, our personal data, etc., and the importance of operational security.

Teaching objectives

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

- Understanding how artificial intelligence can benefit cybersecurity
- Understanding security issues related to connected objects
- Discover the tools and means for detecting social engineering, biometric and spoofing attacks...

Intended audience

Decision-makers, project managers, engineers, developers, researchers.

Prerequisites

Previous knowledge of a computer language and a programming language.

Course schedule

1 Defining the challenges between AI, robotics and cybersecurity

- Definition and concepts.
- Challenges for governments, armies and all IT-related organizations.
- AI-related cybersecurity opportunities and limits.
- Software threats. Malware detection tools.
- Security issues related to the Internet of Things (IoT).
- Possibilities and limits of the IoT in a cybersecurity context.
- Malicious connected objects versus means of detection.

Demonstration

Demonstrations: polymorphic software, genetic algorithms for polymorphic code generation, electronic and robotic hardware.

PARTICIPANTS

Decision-makers, project managers, engineers, developers, researchers.

PREREQUISITES

Previous knowledge of a computer language and a programming language.

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.

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.

2 Social engineering and artificial intelligence

- What is a social engineering attack? What are the consequences?
- Principles of "deepfakes" (false identities, images, voices and videos).
- Possibilities and limits of a GAN (Generative Adversarial Networks).
- New detection tools

Demonstration
Implementation of a GAN network to produce images with dummy styles.

3 AI as a tool for detection, protection, surveillance, identification...

- Systems of ever-increasing "complexity".
- Statistical indicators "classic" are insufficient to monitor a complex system.
- Machine learning (ML) and deep learning (DP) for anomaly detection and prevention.
- AI as a surveillance tool. Use of ML and DL by biometric systems.
- Possibilities and limits of ML and DL in person identification.
- Misuse: false positives, false negatives, malicious acts...

Demonstration
Detection model. Camera typology (360, HD, 3D-RGBd...). Demonstrations of the limitations, "biases" linked to AI and cases where AI is more effective than the human eye.

4 AI-powered listening

- Eavesdropping context "boosted" with artificial intelligence.
- Tools and resources for eavesdropping on a conversation, detecting a secret code, reconstructing an e-mail...
- Successful projects accessible to all.
- How can we preserve the confidentiality of our exchanges?
- Possibilities and limits between "frappology" and AI. How to protect yourself?

Demonstration
Tools and research useful for reconstructing and predicting indirect signals in a noisy environment.

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.