le cnam Conservatoire national des arts et métiers

USEEV2 - Applications of AI and Cyber-threat Management

Mis à jour le 05-07-2024

CONSERVATOIRE NATIONAL DES ARTS ET MÉTIERS BDO 2024 DOCET OMNES UBIQUE

Code : USEEV2

Unité spécifique de type cours

3 crédits

Responsabilité nationale :

EPN05 - Informatique / Stefano SECCI

Présentation

Prérequis

Data communication, Networking, Basic IT security background.

Objectifs pédagogiques

The main objective of this course consists in delivering a solid background in cybersecurity and AI applied to cybersecurity and cybercrime. The course will deliver an overview of the cyber-risks and related implications at both technical and operational level. The students will also get some use cases related to the use of AI in the cybersecurity sector and the new trends and techniques used by cyber criminals.

Programme

Contenu

The course is divided into two parts, a theoretical part alternated to practical modules. After the first 2 days of theory, the students will apply the concepts in the frame of lab exercises.

Topics:

- Understanding security of IT (Informational Technology) and OT (Operational Technology) systems and its impact on industrial operational aspects.
    - Introduction to IT security and OT security
        - Overview of the concept and the strategic importance of security.
        - Principles of networking and data communication infrastructures.
        - Principles of IT security.
        - IT vs. OT security.
    - Cybersecurity and cybercrime: the problems, their evolution, their trends
        - Presentation of case studies of cybersecurity incidents.
        - Lessons learned form known cyberattacks
    - The impact of cybercrime
        - Impact and implications of cyberattacks to IT infrastructures.
        - Impact and implications of cyberattacks to OT infrastructures.
- Applications in Connected Industries
    - Industry 4.0 and the digital transformation
        - The use of cyber threat intelligence to protect industrial processes.
        - The strategic importance of reliable and secure data communication in modern industries.
    - Supply chain attacks
        - Advanced monitoring to detect and prevent supply chain attacks.
        - Asset monitoring and management for business continuity.
        - Monitoring of cloud based solutions to support the connected industry.
    - AI as the core of events and traffic analysis, for threat detection and prevention
        - AI and ML driven solutions for threat detection.
        - Reinforcement learning and federated learning to improve timely asset and operation protection.
- The growing importance of AI and ML in the cybersecurity landscape.
    - Case Studies and Best Practices
        - Real-world examples of successful implementations of cybersecurity solutions to protect connected industries.
        - Lessons learned and best practices for several application domains.
    - Challenges and Opportunities
        - Identification of challenges in implementing AI based protection.
        - Expected upcoming trends.

Modalités de validation

- Contrôle continu
- Examen final

Description des modalités de validation

Reports on the laboratory/practical exercises

Bibliographie

Titre	Auteur(s)
Hands-On Artificial Intelligence for Cybersecurity: Implement smart AI systems for preventing cyber attacks and detecting threats and network anomalies; Packt Publishing, August 2019	Alessandro Parisi
Data Analytics for Cybersecurity; Cambridge University Press July 2022	Vandana P. Janeja