TECHNICAL SHEET OF THE SUBJECT

Data of the subject

Subject name	Artificial Intelligence Applied to Cybersecurity
Subject code	DOI-MCS-522
Involved programs	Máster en Ciberseguridad [Primer Curso]
Level	Master
Quarter	Semestral
Credits	4,5 ECTS
Type	Optativa
Department	Department of Industrial Organization
Coordinator	Rafael Palacios
Course overview	The objective of the course is to know how from the application of Artificial Intelligence (AI) techniques on cybersecurity use cases, a qualitative and quantitative leap is achieved in the level of detection and protection of a company's information assets thanks to the predictive quality that they provide. Although AI can help defend these information assets, it can also be used as an attack mechanism on them, being a tool increasingly used by cyber attackers. In this way, both defense and attack mechanisms through AI close to the state of the art will be presented, reviewing the main cybersecurity scenarios such as malware detection, fraud analysis and behavior analysis, in addition to others every time with more future such as fake news or fake faces.

Teacher Information

Teacher

Name	Hugo Gascón Polanco
Department	Department of Industrial Organization
EMail	hgascon@icai.comillas.edu

Teacher

Name	Juan Pablo Fuentes Brea
Department	Department of Industrial Organization
EMail	jpfuentes@icai.comillas.edu

SPECIFIC DATA OF THE SUBJECT

Contextualization of the subject

Prerequisites

Basic knowledge of machine learning, cybersecurity and the Python language.

Competencies - Objectives

THEMATIC BLOCKS AND CONTENTS

Contents - Thematic Blocks

Contents

Presentation of the subject

- Objectives
- Temary
- Practices
- Evaluation
- Frameworks
- Contact
- Bibliography

Introduction to AI applied to Cybersecurity

- The current context of cybersecurity and its challenges
- Artificial intelligence applied to cybersecurity
- Use cases for AI / ML in cybersecurity
- Future Trends and Opportunities

Algorithms, Tools and Systems

- Problems and algorithms
- Tools and libraries
- ML systems in production

Analysis and Detection of Threats

- Detection of Phishing and Spear-Phishing
- Malware Analysis and Detection

Threat Intelligence

- Threat Intelligence
- Platforms for IT
- AI use case

Fraud detection

- Presentation of fraud scenarios
- Fraud detection by static scoring
- Fraud detection by dynamic scoring
- Introduction to Deep Learning

UEBA (User and Entity Behavior Analytics)

- Presentation of UEBA scenarios

- Temporal analysis of activities
- Models based on autoencoders
- Recurrent models
- Introduction to Pytorch

Adversarial ML

- Presentation of ML Adversarial scenarios
- Attack methods
- Defense methods
- Security in the AI life cycle

Deepfakes

- Presentation of Deepfakes scenarios
- GANs
- Fake faces
- Fake news
- Fake speech

Optimization of attacks

- Presentation of optimization scenarios
- Black-Box type cyberattacks
- Reinforcement Learning
- Evolutionary computing

Future lines of work in Cybersecurity & AI

- Future scenarios of AI applied to Cybersecurity
- New profiles required: IA4sec
- Final conclusions

TEACHING METHODOLOGY

General methodological aspects of the subject

EVALUATION AND CRITERIA

Ratings

The course grading mechanism will be made up of a theory part and a practical part, the sum of which must be at least 5.0 to pass the course. The percentages of both parties will be as follows:

final qualification = 0.8 * (theory part) + 0.2 * (practical part)

BIBLIOGRAPHY AND RESOURCES

Basic Bibliography

Freeman and Chio. Machine Learning and Security. O'Reilly Media 2018

Duda, Hart and Stork. Pattern Classification. Wiley & Sons 2001

Shawe-Taylor & Cristianini. Kernel Methods for Pattern Analysis. Cambridge 2004

Gollmann. Computer Security. Wiley & Sons, 2011

Szor. The Art of Computer Virus Research and Defense. Addison-Wesley, 2005

Rieck. Machine Learning for Application-Layer Intrusion Detection, Lulu 2009