

Machine Learning Applications in Cyber Security

Lecturer

Lecturer

Danilo Greco
Giovanni Gaggero

Email

danilo.greco@edu.unige.it
giovanni.gaggero@unige.it

Office

Via all'Opera Pia 11

General information

Aim and scope

This course provides an in-depth exploration of how machine learning (ML) techniques can enhance cybersecurity. It is divided into two main parts. The first focuses on Python programming and machine learning fundamentals, while the second applies these concepts to cybersecurity use cases. Prerequisites: Basic knowledge of cybersecurity, probability, statistics, and programming (Python preferred)

Content

Part. 1: Python and Machine Learning Fundamentals. Module 1: Introduction to Python for Machine Learning (5 hours) Module 2: Machine Learning Foundations (5 hours). Part 2: Machine Learning for Cybersecurity. Module 3: Fundamentals of Network Security. Module 4: Machine Learning for Intrusion Detection Systems

Language

English

Assessment Method

Assignments (30%): Hands-on exercises on Python, ML, and cybersecurity datasets.
Project (40%): Implementing an ML-based cybersecurity solution.
Final Presentation (30%): Research-based presentation on an emerging ML security challenge

Bibliography

Hands-on Machine Learning with Scikit-Learn, Keras & TensorFlow. Aurelien Geron
Python Data Science Handbook. Jake VanderPlas

Registration

Email to:

danilo.greco@edu.unige.it
giovanni.gaggero@unige.it

Schedule

Topic	Day	Time
Introduction to Python for Machine Learning	To be defined	9:00-12:00 (in-person/online Teams)
Introduction to Python for Machine Learning	To be defined	9:00-11:00 (in-person/online Teams)
Machine Learning Foundations	To be defined	9:00-12:00 (in-person/online Teams)
Machine Learning Foundations	To be defined	9:00-11:00 (in-person/online Teams)
Fundamentals of Network Security	To be defined	9:00-12:00 (in-person/online Teams)
Fundamentals of Network Security	To be defined	9:00-11:00 (in-person/online Teams)
Machine Learning for Intrusion Detection Systems	To be defined	9:00-12:00 (in-person/online Teams)
Machine Learning for Intrusion Detection Systems	To be defined	9:00-11:00 (in-person/online Teams)

Time schedule may be modified accordingly to students' needs

Exam schedule

Date	Where
To be defined	Giovanni Gaggero Office
To be defined	Giovanni Gaggero Office