Caracterização da Unidade Curricular / Characterization of the Curricular Unit

Designação da Unidade Curricular (UC) / Title of Curricular Unit (CU): Aprendizagem Automática Aplicada à Segurança / Machine Learning Applied to Security

Área científica da UC / CU Scientific Area: Ciências Informáticas / Computer Science

Semestre / Semester: 2º

Número de créditos ECTS / Number of ECTS credits: 6

Carga horária por tipologia de horas / Workload by type of hours: TP: 45; OT: 6; O: 9

Carga letiva semanal / Weekly letive charge: 3h

Objetivos de aprendizagem (conhecimentos, aptidões e competências a desenvolver pelos estudantes):

No final desta unidade curricular, o aluno deverá:

- Compreender os princípios e fundamentos dos algoritmos e metodologias de aprendizagem máquina;
- Reconhecer a importância da aprendizagem máquina na área da segurança informática;
- Aplicar técnicas de aprendizagem para detetar anomalias em sistemas computacionais ou redes;
- Justificar a escolha de uma solução de aprendizagem máquina para identificar problemas de segurança;
- Aplicar e adaptar algoritmos de aprendizagem máquina a um novo conjunto de dados na área da segurança;
- Avaliar criticamente os resultados dos processos de aprendizagem máquina.

Intended learning outcomes (knowledge, skills and competences to be developed by the students):

At the end of this course unit the student will have to:

- Understand the principles and fundamentals of machine learning algorithms and methodologies;
- Recognize the importance of machine learning in the area of computer security;
- Apply learning techniques to detect anomalies in computer systems or networks;
- Justify the choice of a machine learning solution to identify security problems;
- Apply and adapt machine-learning algorithms to a new set of data in the area of security;
- Critically evaluate the results of the machine learning processes.

Conteúdos programáticos:

1. Aprendizagem máquina

1.1. Conceitos base

1.2. Técnicas de agrupamento e classificação

1.3. Aprendizagem com e sem supervisão

1.4. Redes neuronais

1.5. Aprendizagem por deep learning

2. Perceção do comportamento de entidades de rede

2.1. Perceção das técnicas para detetar evidências de ataques/intrusões

2.2. Perceção dos comportamentos dos utilizadores, sistemas computacionais e redes

2.3. Perceção dos modelos de assinaturas ou comportamentos

3. Deteção de anomalias usando aprendizagem máquina

3.1. Classificação e deteção de anomalias de tráfego em rede

3.2. Classificação e deteção de eventos anómalos em sistemas computacionais

3.3. Desafios do uso de aprendizagem máquina na deteção de anomalias

3.4. Exemplos de aplicações da aprendizagem de máquina na deteção de anomalias

3.5. Áreas de aplicação emergentes

Syllabus:

1. Machine learning

1.1. Basic concepts

1.2. Grouping and classification techniques

1.3. Learning with and without supervision

1.4. Neural Networks

1.5. Deep learning

2. Perception of the behavior of network entities

2.1. Understanding techniques for detecting evidence of attacks/intrusions

2.2. Perception of user behaviors, computing systems and networks

2.3. Perception of signature models or behaviors

3. Detection of anomalies using machine learning

3.1. Classification and detection of network traffic anomalies

3.2. Classification and detection of anomalous events in computer systems

3.3. Challenges of using machine learning to detect flaws

3.4. Examples of machine learning applications in flaw detection

3.5. Emerging areas of application