Ementa

Código	DCC030/049/831
Disciplina	Cybersecurity data science
Turma	3a e 5a - 17:00/18:40
Professor	Michele Nogueira Lima

Ementa. This course aims at preparing the students to handle the massive shifts in technology and operations, driven by data science, that cybersecurity is undergoing. It will overview how to extract security incident patterns (or insights) from cybersecurity data and build corresponding data-driven models, two key aspects to make security systems automated and intelligent. This course starts briefly overviewing the motivation and concepts of cybersecurity data science, next it presents the relevant methods/technologies to understand the applicability of cybersecurity data science towards data-driven intelligent decision making in cybersecurity, the main approaches for security data gathering and preparing, a discussion on different machine learning and statistical learning tasks in cybersecurity, multi-layered frameworks for smart cybersecurity services, cybersecurity testbeds and datasets. This course is enriched with real case studies and the students will be able to prepare their main hands-on projects to put in practice their knowledge.

Programa

Aula	Data	Conteúdo previsto	Modalidade	Interação
1		Introduction	Síncrona (ao vivo – com gravação para acesso posterior)	Remota síncrona
2		Concepts of cybersecurity data science; terminology; introduction to the main data analytics tools	Síncrona (ao vivo – com gravação para acesso posterior)	Remota síncrona
3		Main cyberattacks and cyber risks; basic exercise to illustrate a type of attack	Síncrona (ao vivo – com gravação para acesso posterior)	Remota síncrona
4		Cybersecurity defense strategies; first contact to defense tools.	Síncrona (ao vivo – com gravação para acesso posterior)	Remota síncrona
5		Data science overview and exercise	Síncrona (ao vivo – com gravação para acesso posterior)	Remota síncrona
6		Cybersecurity data science: main stages	Síncrona (ao vivo – com gravação para acesso posterior)	Remota síncrona
7		Machine learning tasks in cybersecurity: supervised learning	Síncrona (ao vivo – com gravação para acesso posterior)	Remota síncrona
8		Machine learning tasks in cybersecurity: unsupervised learning	Síncrona (ao vivo – com gravação para acesso posterior)	Remota síncrona
9		Machine learning tasks in cybersecurity: neural networks and deep learning	Síncrona (ao vivo – com gravação para acesso posterior)	Remota síncrona

10		Machine learning tasks in cybersecurity: other learning techniques	Síncrona (ao vivo – com gravação para acesso posterior)	Remota síncrona
11		Project proposal	Síncrona (ao vivo – com gravação para acesso posterior)	
12		Exam 1		Moodle
13		Statistical learning for cybersecurity	Síncrona (ao vivo – com gravação para acesso posterior)	Remota síncrona
14		Security data gathering and preparing approaches; cybersecurity datasets	Síncrona (ao vivo – com gravação para acesso posterior)	Remota síncrona
15		Behavioral analysis and the design of models	Síncrona (ao vivo – com gravação para acesso posterior)	Remota síncrona
16		Multi-layered frameworks for smart cybersecurity services	Síncrona (ao vivo – com gravação para acesso posterior)	Remota síncrona
17		Main testbeds for cybersecurity	Síncrona (ao vivo – com gravação para acesso posterior)	Remota síncrona
18		Project update	Síncrona (ao vivo – com gravação para acesso posterior)	Remota síncrona
19		Exam 2		Moodle
20		Security-policy rule generation	Síncrona (ao vivo – com gravação para acesso posterior)	Remota síncrona
21		Protecting the valuable security information	Síncrona (ao vivo – com gravação para acesso posterior)	Remota síncrona
22		Context-awareness in cybersecurity	Síncrona (ao vivo – com gravação para acesso posterior)	Remota síncrona
23		Feature engineering in cybersecurity	Síncrona (ao vivo – com gravação para acesso posterior)	Remota síncrona
24		Alert generation and prioritizing	Síncrona (ao vivo – com gravação para acesso posterior)	Remota síncrona
25		Adversarial machine learning	Síncrona (ao vivo – com gravação para acesso posterior)	Remota síncrona
26		Seminar	Síncrona (ao vivo – com gravação para acesso posterior)	Remota síncrona
27		Seminar	Síncrona (ao vivo – com gravação para acesso posterior)	Remota síncrona
28		Project presentation	Síncrona (ao vivo – com gravação para acesso posterior)	Remota síncrona

29		Project presentation	Síncrona (ao vivo – com gravação para acesso posterior)	Remota síncrona
30		Project presentation	Síncrona (ao vivo – com gravação para acesso posterior)	Remota síncrona

Bibliography

Data Science in Cybersecurity and Cyberthreat Intelligence. Leslie F. Sikos and Kim-Kwang Raymond Choo (editors), Intelligent Systems Reference Library, Springer, 2020.

Data Science for Cyber-Security. Nick Heard, Nial Adams, Patrick Rubin-Delanchy, Melissa Turcotte. 2019 World Scientific Publishing Europe Ltd.

Cybersecurity Essentials. Charles J. Brooks, Christopher Grow, Philip Craig, Donald Short. 2018, John Wiley & Sons, Inc.

Cyber Warfare - Truth, Tactics, and Strategies: Strategic concepts and truths to help you and your organization survive on the battleground of cyber warfare. Chase Cunningham and Gregory J. Touhill. 2020, Packt Publishing.

M. Pelloso, A. Vergutz, A. Santos and M. Nogueira, "A Self-Adaptable System for DDoS Attack Prediction Based on the Metastability Theory," 2018 IEEE Global Communications Conference (GLOBECOM), Abu Dhabi, United Arab Emirates, 2018, pp. 1-6.

M. Nogueira, A. Santos and J. M. F. Moura, "Early Signals from Volumetric DDoS Attacks: An Empirical Study", eprint 1609.09560, arXiv. 2016.

Support
Course website (handouts, slides and others)
Moodle (handouts, slides and others)
Vídeos

Evaluation

1	Exam 1 - Remota	20 pontos	TBD
2	Exam 2 - Remota	20 pontos	TBD
3	Project - Remota	30 pontos	TBD
4	Homeworks	30 pontos	TBD

Modo de interação:
Toda comunicação escrita com os alunos será realizada via Moodle, inclusive a divulgação deste plano e a subsequente especificação de quais ferramentas serão utilizadas para as aulas remotas. As aulas remotas serão transmitidas via Microsoft Teams e gravadas. Os exames serão realizados e enviados pelo Moodle de forma assíncrona. A avaliação dos projetos ocorre com base no relatório e apresentação oral.