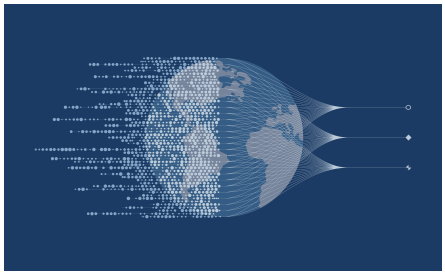

ID: **P4.3-483** Type: **E-poster**

-Driven Detection of Malicious Codes when Integrating Data from Monitoring Technologies

Integrating data from various monitoring technologies has become essential to detect and mitigate the spread of malicious code in modern digital ecosystems. However, the heterogeneity and complexity of data sources present significant challenges to ensure smooth and accurate detection. This paper presents an AI-based framework for detecting malicious code that leverages a deep learning approach to analyse and correlate data from various monitoring technologies, including network traffic analyzers, endpoint detection and application logs. The proposed system uses advanced feature extraction and fusion methods to unify disparate data streams into a coherent data set, enabling the identification of complex attack patterns that are often missed by traditional detection methods. Experimental evaluations demonstrate the framework's ability to improve detection accuracy, reduce false positives and adapt to evolving threats in real time. This work highlights the potential of AI to improve cybersecurity by providing a robust and scalable approach to detecting malicious code on multi-source monitoring platforms.

E-mail

serrhini@mail.ru

In-person or online preference

Primary author: Prof. SERRHINI, Mohamed (University Mohamed Premier Oujda,Morocco)

Presenter: Prof. SERRHINI, Mohamed (University Mohamed Premier Oujda,Morocco)

Session Classification: P4.3 Use of enabling Information Technologies

Track Classification: Theme 4. Sustainment of Networks, Performance Evaluation, and Optimization: T4.3 Use of enabling Information Technologies