UNIVERSITÀ
DEGLI STUDI
DI PADOVA

HORIZON EUROPE
PROJECTS FUNDED AT THE UNIVERSITY OF PADOVA

OPTIMA - Organization sPecific Threat Intelligence Mining and sharing

The OPTIMA project (Organization sPecific Threat Intelligence Mining and sharing) aims to design techniques and tools for the extraction of Threat Intelligence targeted to organizations using ML algorithms, and effectively share attack records using privacypreserving methods. The project will use technologies to protect societies from cyber-attacks and sophisticated threats prioritized in the European Council's New Strategic Agenda. The key beneficiaries of the project are (a) security operation center-to support real time monitoring (b) incident response, threat hunting, fraud detection team-to prioritize risk (c), operational leaders- to prioritize activities of IT staff and (d) Strategic leaders such as Chief Information Security Officers - to make well-informed business decisions. This project will be executed at the University of Padua, under the supervision of Prof. Mauro Conti. The project will investigate solutions for the core questions: RQ1: How effectively can ML algorithms extract organization-specific threat artefacts to be utilized for preparing actionable Threat Intelligence? RQ2: How can organizations share threat intelligence without disclosing their private information to others?

The objectives (SO) of the project are as follows:

1. SO1-To develop techniques for automatic extraction of threat intelligence using OSINT data for diverse IT industries (health care, finance, IoT, education, etc.) using deep learning approaches.
2. SO2-To create a novel automated system to derive Indicator of Compromise (IOC) based on word embedding and syntactic dependencies of words to identify unseen IOCs. Utilizing the extracted IOCs a threat index will be estimated to define the impact of threat and attack trends across individual organizations;
3. SO3-To build a system by integrating cryptographic tools and Federated learning which will enable an organization to anonymously share threat logs with different parties in a privacy-preserving manner.

UNIPD Supervisor: Mauro Conti

MSCA Fellow: Puthuvath Vinod

Department: Department of Mathematics

Coordinator: Università degli Studi di Padova (Italy)

Total EU Contribution: Euro 188.590,08

Call ID: HORIZON-MSCA-2021-PF-01

Project Duration in months: 24

Find out more: https://cordis.europa.eu/projects/en