FVT Overview

Evangelos Raptis
AEGIS IT RESEARCH GmbH
e.raptis@aegisresearch.eu

This project has received funding from the European Union's Horizon Europe research and innovation programme under Grant Agreement No 101120779

Forensics Visualization Toolkit

- A comprehensive cybersecurity visualization toolkit which combines Host-Based Intrusion Detection Systems (HIDS) with Network Intrusion Systems (NIDS).

- Also acts as a network performance and diagnostic tool to provide a quick overview of an internal network's status and allow operators to monitor network performance and flowing traffic.

Innovations of the FVT

1. Incorporation of both physical and cyber forensics services and algorithms
2. Timeline analysis of a large number of heterogeneous events via advanced visualizations
3. Preconfigured views which provide automatically adapted visualizations based on similar past situations
4. Threat hunting capabilities (empowered by AI-enabled correlation algorithms) for almost real-time mitigation of security incidents

The FVT within the CyberSecDome project

- The advanced AI capabilities of the FVT will be used to carefully examine alerts raised by potential security incidents, uncovering anomalies along the way and performing deep correlation analysis, assisting SOC analysts in the early detection of sophisticated cybersecurity attacks