26th InfoCom World Conference

Digital Greece: Time for a Leap!

Tuesday 12 November 2024 – Divani Caravel Hotel

CyberSecDome

CyberSecDome added values from a pilot OTE Group

Fotis Stathopoulos

fstathopoulos@ote.gr

26th InfoCom World Conference

Digital Greece: Time for a Leap!

Tuesday 12 November 2024

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

CyberSecDome

Duration: September 2023 – August 2026

An advanced Virtual Reality based intrusion detection, incident investigation and response approach for enhancing the resilience, security and privacy of complex and heterogeneous digital infrastructures

CyberSecDome Consortium

CyberSecDome Consortium

Industry

University

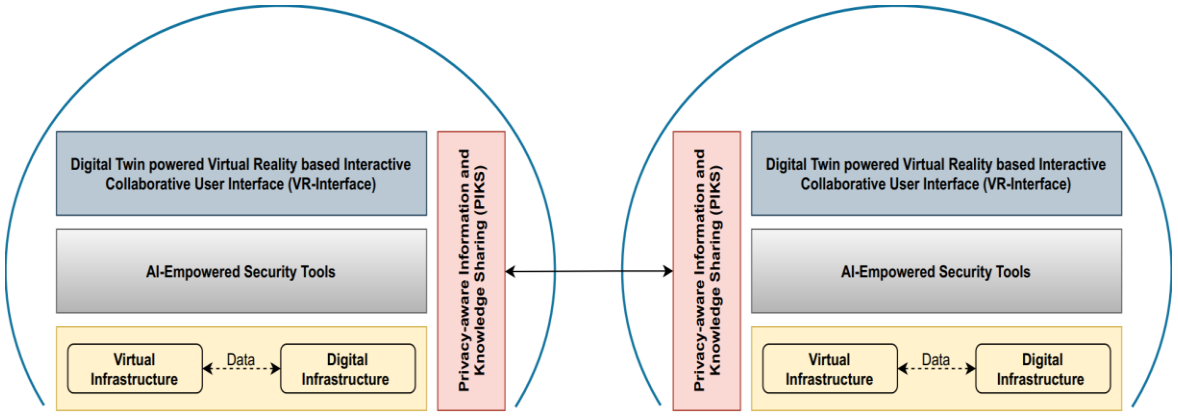
SMEs

Association

Collaborative Training for AI Models and Federated Learning

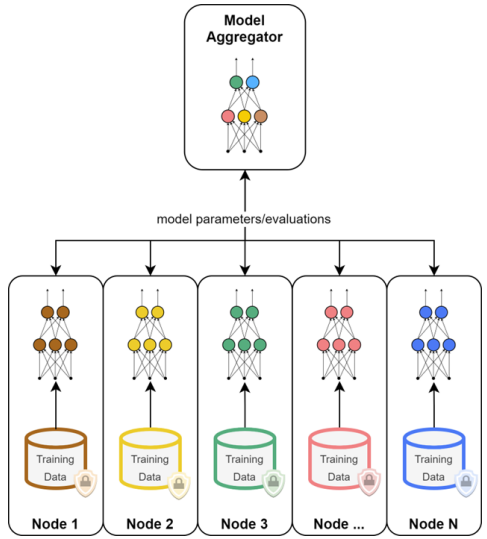
Collaborative Training for AI Models

Goal: Powerful collaborative training of AI models among organizations while keeping organisation data local and protected



Federated Training

- An ML technique where **multiple clients** collaboratively train a model without sharing raw data.
- **Local models** are trained on individual nodes (e.g., organization), and only **model parameters** are shared with a central server, not the actual data.
- The server aggregates these parameters to improve the **global model**.



OTE Pilot: Benefits and Responsibilities

OTE Benefits:

- **Strengthen our security posture against new types of cyber-attacks** by using up-to-date detection and prediction tools
- **Improve our cybersecurity systems in specific directions**:
  - Reduce the amount of time to detect an incident
  - Reduce the downtime during an incident
  - Improve the absolute number of reported incidents

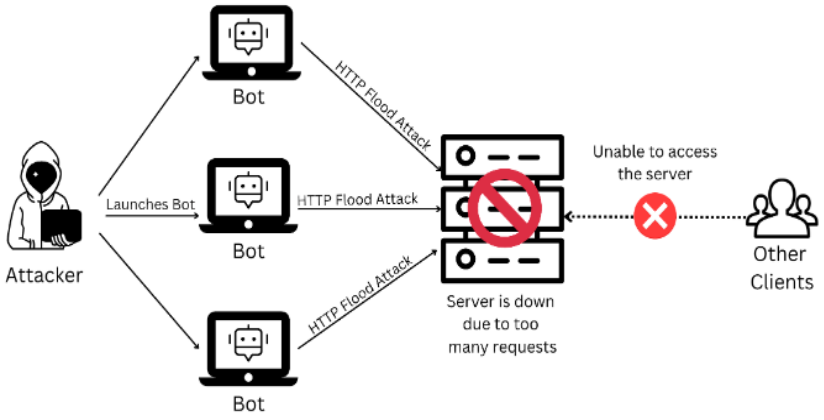
OTE Responsibilities :

- Provide **Infrastructure**
- Provide/execute **use case attack scenarios**
- **Test the security tools** developed by the project consortium
- **Evaluate** the CyberSecDome platform

OTE Pilot: Use Cases

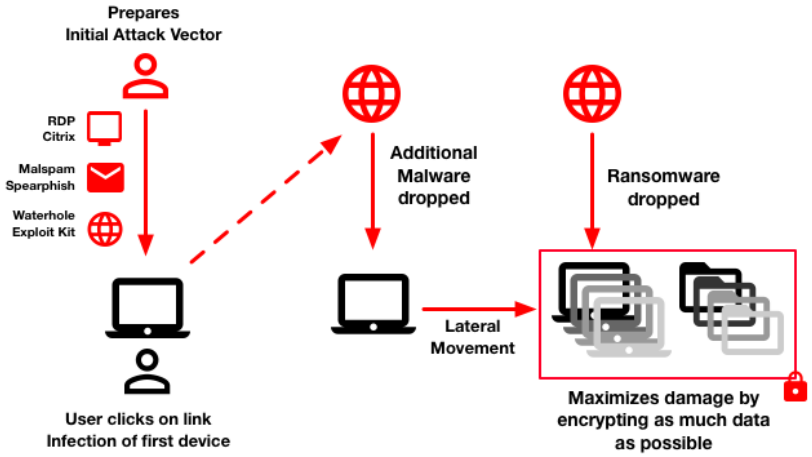
Use Case #01: DDoS attack scenario

Layer 7 DDoS attack (or application attack) that will target a specific service instead of an entire network. This type of DDoS is becoming increasingly more common than broad network attacks.



Use Case #02: Ransomware attack scenario

Crypto ransomwares encrypts all or some files on a computer and demands a ransom from the victim in exchange for a decryption key. Some newer variants also infect shared, networked and cloud drives. Crypto ransomware spreads through various means, including malicious emails, websites and downloads



OTE Pilot: Assets

Scenario	Assets	Security & digital infrastructure	Related processes
Use Case #01: DDoS attack	○ Target Web Server ○ Web Application	○ DDoS Protection Mechanism ○ Web Application Firewall ○ SIEM (Security Information and Event Management)	OTE's Security Incident Management Process
Use Case #02: Ransomware attack	○ Servers ○ Workstations	○ Anti-Malware Mechanisms ○ EDR (End point Detection and Response) ○ SIEM (Security Information and Event Management)	OTE's Security Incident Management Process

Overview of CyberSecDome Open Call

► Objective of the Open Call:

- To foster the development and adoption of cybersecurity solutions that will enhance the security and resilience of European digital infrastructures.
- Engage a diverse range of SMEs and large companies to provide innovative solutions aligned with **CyberSecDome's** strategic goals.

~~**Outcome:**~~ Accelerating readiness of impactful cybersecurity solutions with practical relevance to OTE and other **CyberSecDome** pilots.

► AEGIS's Role:

- Lead Coordinator of the Open Call operations.
- Oversee evaluation, selection, and support of Open Call participants.
- Ensure rigorous assessment and alignment with **CyberSecDome's** objectives, directly contributing to OTE's use case.

Funding Highlights:	Open Call Round 1 Key Dates:
Total funding: €1.2M over two rounds	**Announcement**: December 4, 2024
Up to **€120K** per project	**Submission Deadline**: February 11, 2025
100% funding for SMEs	Project Start Date: April 1, 2025

Benefits for OTE from CyberSecDome Open Call

Direct Testing for Pilot Scenarios:
Opportunity for OTE to leverage tested solutions to strengthen its cybersecurity posture against emerging threats.

Alignment with OTE's Use Cases:
Selected projects will deliver innovations supporting OTE's specific needs, including DDoS attack mitigation and ransomware protection.

Continuous Engagement:

- Ongoing collaboration between Open Call participants and OTE's technical teams.
- AEGIS provides coordination, ensuring selected solutions address real-world requirements for large-scale infrastructure security.

Enhanced Incident Response Capabilities:
Access to new tools to reduce response time, minimize downtime, and increase incident detection accuracy.

Contact

Fotis Stathopoulos
fstathopoulos@ote.gr

Mina Marmpena
mina.marmpena@itml.gr

Spiros Fotis
spyros.fotis@aegisresearch.eu

Dimitris Papanikas
dpapanikas@ote.gr

Vina Rompoti
vina@itml.gr