CYBERSECDOME

November 2023
Press Release

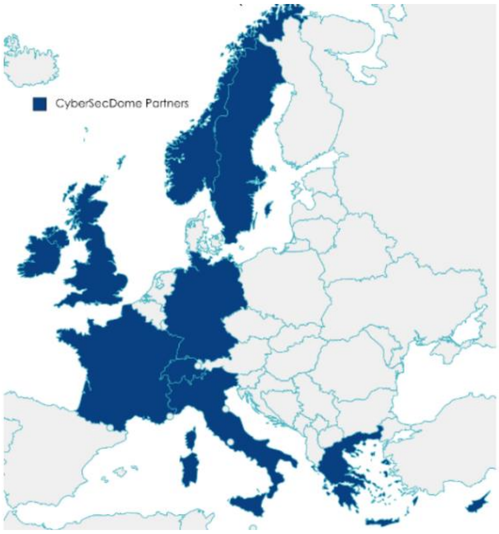
“An advanced Virtual Reality based intrusion detection, incident investigation and response approach, for enhancing the resilience, security and privacy of complex and heterogeneous digital infrastructures.”

The digital infrastructure has become one of the most important pillars that uphold our economy, our democracy, and our daily lives. It consists of servers, data centres, telecom exchanges, radio access networks, satellites, databases, data stores, information technology services, cloud applications, and IoT device endpoints. The ongoing war in Ukraine has shown that disrupting critical infrastructure can be a strategic objective that could be achieved even before ground invasions are conducted. Cyber-attacks (such as Ransomware, DDoS, etc.) against digital infrastructure may cause digital disruption, which can in turn result in huge financial losses, reduced trust in societal services, and even loss of human life. Therefore, the protection of digital infrastructure from ever-evolving cybersecurity threats is becoming increasingly important.

However, it is also challenging for several reasons. First, while exploits and attacks are increasingly automated and able to scale massively, the protection schemes remain largely manual and resource demanding. For example, existing proactive security protection solutions (e.g., firewalls) cannot guarantee the continuity of digital infrastructures, especially when we consider zero-day attacks.

Not forget to mention here, there is a need for collaborative incident response against cross-border cyber incidents and threats that can affect multiple sectors across multiple countries. Finally, there is a lack of sharing threat information mechanisms that are compliant with data protection regulations and can address all concerns regarding mass surveillance and the protection of personal spaces.

CyberSecDome offers a solution that realizes a suite of security tools for addressing all the aforementioned challenges. CyberSecDome provides **a set of AI-Empowered security tools** used to ensure that every digital infrastructure operates even in adverse circumstances and **can recover quickly following cyber-attacks.** The tools will be used to **predict** and **detect incidents**, automate pen-testing, assess ongoing risks, **respond to attacks**, and **recover digital infrastructure services** in a very efficient manner. The project provides its users with an interactive advanced Virtual Reality-based interface that enhances their understanding of the digital infrastructure to protect and enable them with so-called situational awareness about the detected attacks and ongoing risks. Finally, CyberSecDome will facilitate effective collaboration and coordination among the different stakeholders and cybersecurity agencies to **prevent widespread disruption due to the domino effect of cyber-attacks** and to coordinate sophisticated large-scale incident response strategies.



The **CyberSecDome** project is enforced by a **multidisciplinary consortium**, consisting of 15 partners from six EU member states (IT, DE, IE, SE, EL, CY) and two affiliated countries (UK, CH), providing all expertise necessary for the ambitious but achievable objectives of the project. These organizations were chosen for their diverse experience, essential competencies, and their complementarity, for building a strong consortium that guarantees the successful outcome of the project.

CyberSecDome partners:

Industry	GRUPPO Maggioli	AIRBUS CYBERSECURITY	OTE	ATHENS INTERNATIONAL AIRPORT ELEFTHERIOS VENIZELOS	
University	Technical University of Munich TUM	IMT Atlantique Bretagne-Pays de la Loire École Mines-Télécom	LiU LINKÖPING UNIVERSITY	ΠΟΛΥΤΕΧΝΕΙΟ ΚΡΗΤΗΣ TECHNICAL UNIVERSITY OF CRETE	a.r.u. Anglia Ruskin University
SMEs	AEGIS IT RESEARCH		CYBERANALYTICS ANTICIPATE · DISCOVER · DEFEND	itml innovation applied	Sphynx Technology Solutions
Association	eit Digital				

Stay tuned with the CyberSecDome project!
More updates to come.

@cybersecdome_eu

@CyberSecDome – EU project