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

December 14, 2023

25th Conference infocom world 2023 | infocom media + ai world

CyberSecDome

OTE

Dimitris Papanikas
IT Security Architect

Project ID

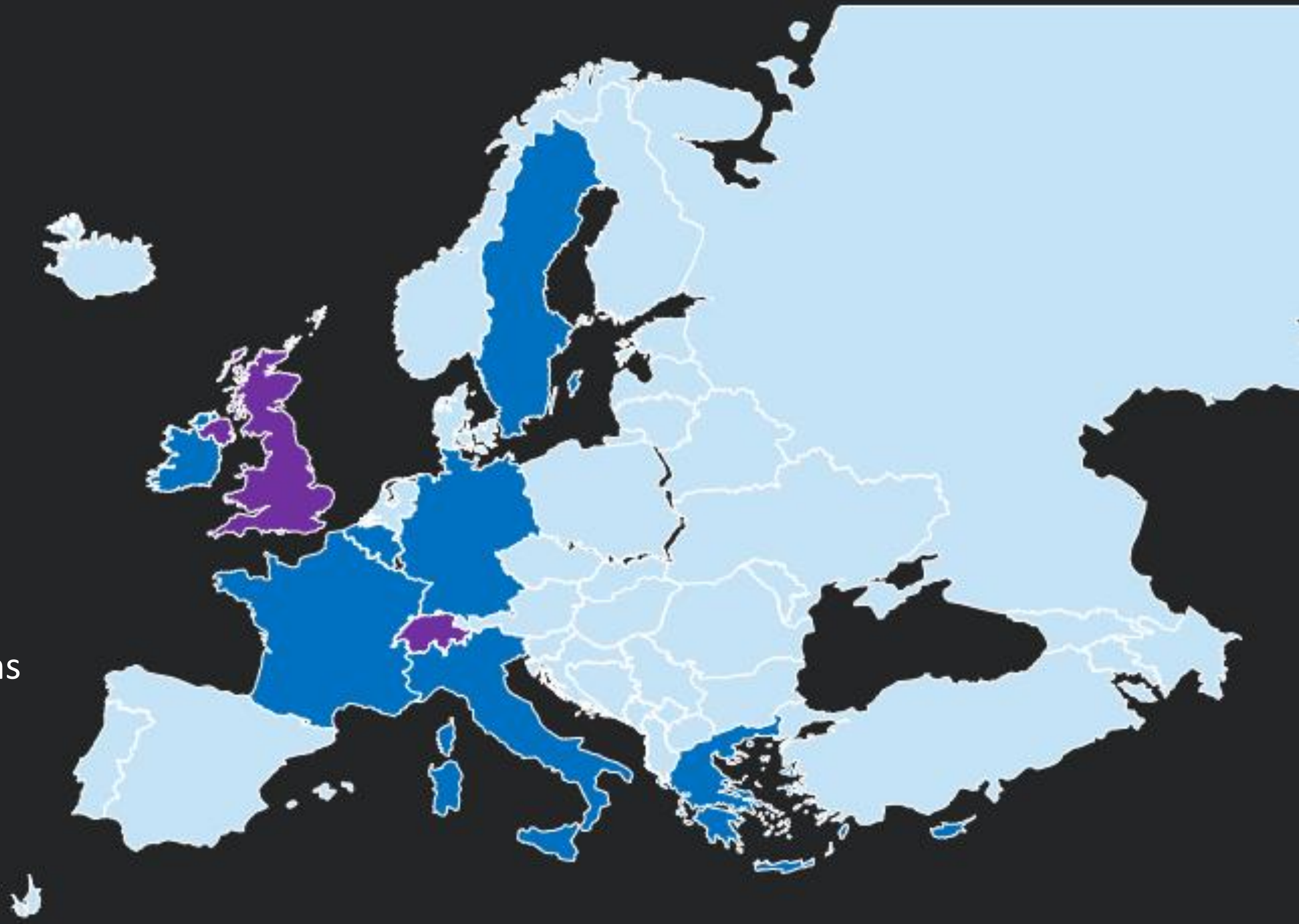
Call: HORIZON-CL3-2022-CS-01

Grant Agreement No: 101120779

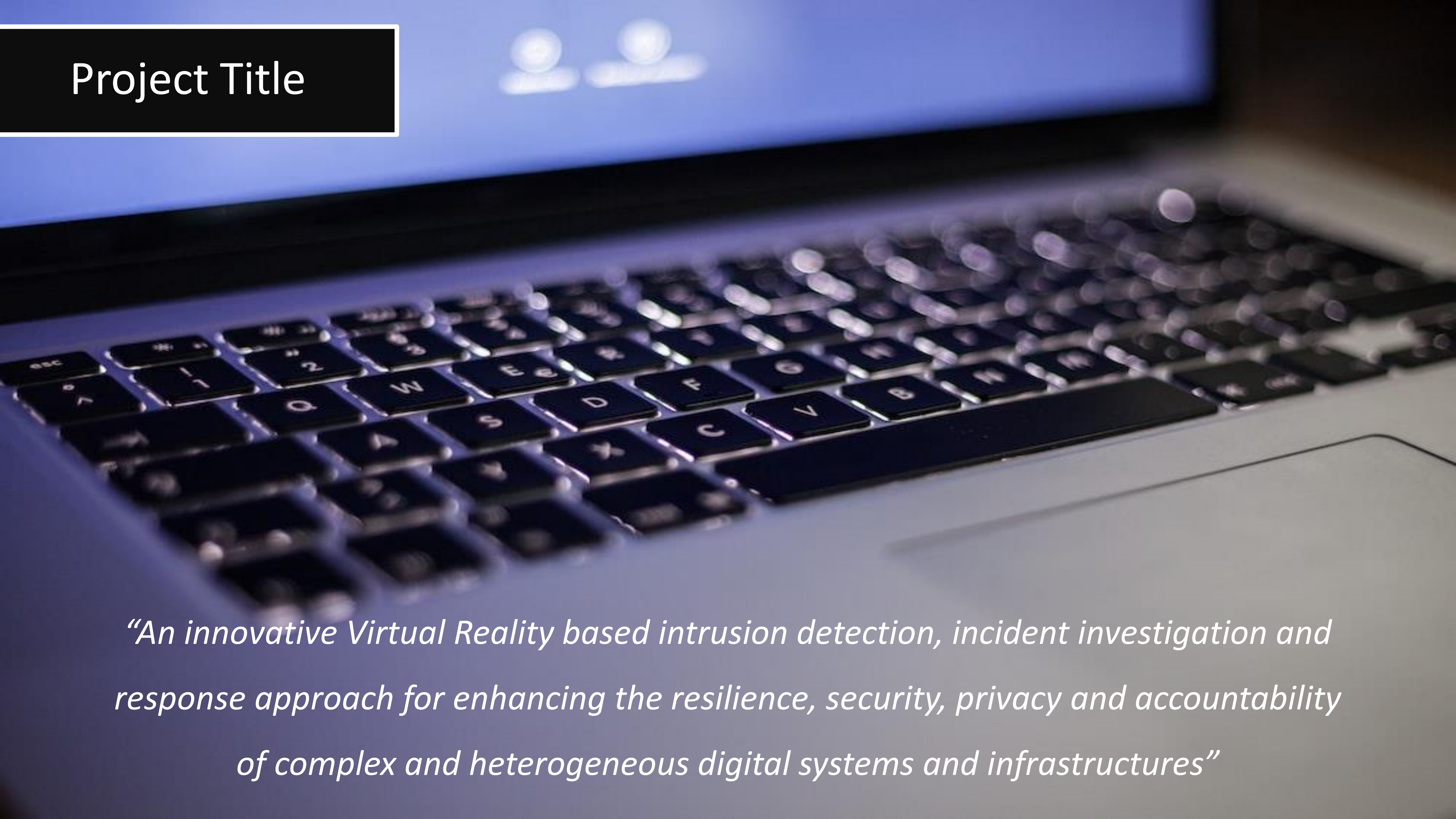
Type of Action: Innovation Action (IA)

EU funding: 5,749,637.50 €

Sep 01.09.2023 - Aug 31.08.2026: 36 months



Project Title



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

Consortium

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

Sphynx Technology Solutions

Association

eit Digital

Project Objectives

- Increase the disruption preparedness & resilience of digital infrastructure

- CyberSecDome will be developed to detect and recover from security attacks as quickly as possible
  - ✓ By leveraging AI, the project will develop security tools for predicting and detecting incidents, assessing ongoing risks, responding to attacks and recovering system services
  - ✓ By utilizing Virtual Reality and digital Twin, the project will develop an Interactive Collaborative User Interface that will provide the CyberSecDome users with better situational awareness of the system under attack

Project Objectives

- Provide dynamic cyber-incident response capability for digital systems and infrastructures

- The project consortium will develop a ***Dynamic and Adaptive Incident Response (DAIR)*** tool that ensures the selection and adoption of responses to cyber incidents dynamically, quickly, and autonomously
    - ➢ By utilizing Virtual Reality and Digital Twin, the tool will take into consideration:

    i. the dynamic behavior of the system and attacks

    ii. the operational mode of the whole system

    iii. the consequence of the selected response

Project Objectives

- Provide high cybersecurity levels via a set of policies and AI-based methods for effective and real-time management in a proactive way of all the security issues

- An Intrusion Detection and Prediction (IDP) tool will be developed with the use of AI-based approaches
  - By leveraging AI, the project consortium will build algorithms for real-time deep analysis of the network traffic and threat related information

Project Objectives

- Provide better interfaces between humans and cybersecurity algorithms

- The project will integrate a unified Digital Twin powered Virtual Reality based Interactive Collaborative User Interface (***VR-Interface***)
  - ➢ The interface will offer intuitive interaction between algorithms and distributed human users, by offering diverse visualizations, and extensive remote collaboration support.

Project Objectives

- Develop solutions to automate penetration testing for proactive security using data-driven AI

- CyberSecDome will develop an Automated Pen-Testing tool to increase the usefulness of penetration testing through ***data-driven AI*** which will enable scalability and more frequent testing.
  - ✓ Penetration testing models will be developed and trained with data collected within the project

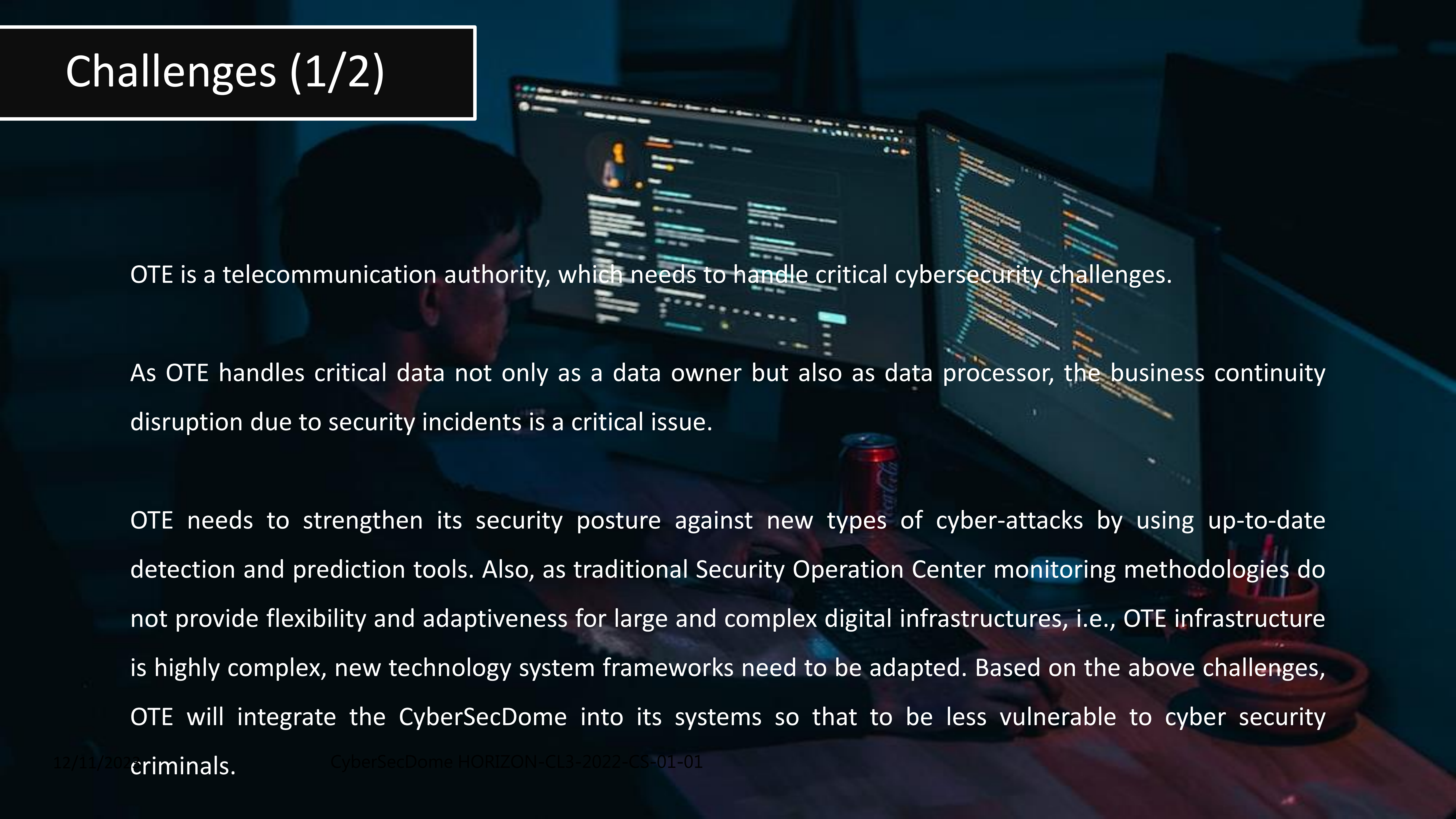
HTO (OTE) Participation

- The Hellenic Telecommunications Organisation S.A. (OTE), a member of the Deutsche Telekom (DT) Group of Companies, is the incumbent telecommunications provider in Greece

- OTE offers its customers a wide range of technologically advanced services, such as high-speed data communications, mobile telephony, Internet access, infrastructure provision, multimedia services, leased lines, maritime and satellite communications, telex and directories

- In the area of ICT, OTE activities include technologies and services, such as Cloud Computing, Big Data Analytics, ML, Blockchain, Security and a large portfolio of innovative services and facilities. Regarding security services, OTE hosts a fully functional Security Operations Center (SOC) that provides 24/7 monitoring not only for its digital infrastructure and services but also for other customers through Managed Security Services (MSS)

- Therefore, OTE is a unique pilot that handles vast amounts of sensitive/personal data gathered and kept on premises, transforming the Group into an attractive and high-value target for organized cyber-criminal teams



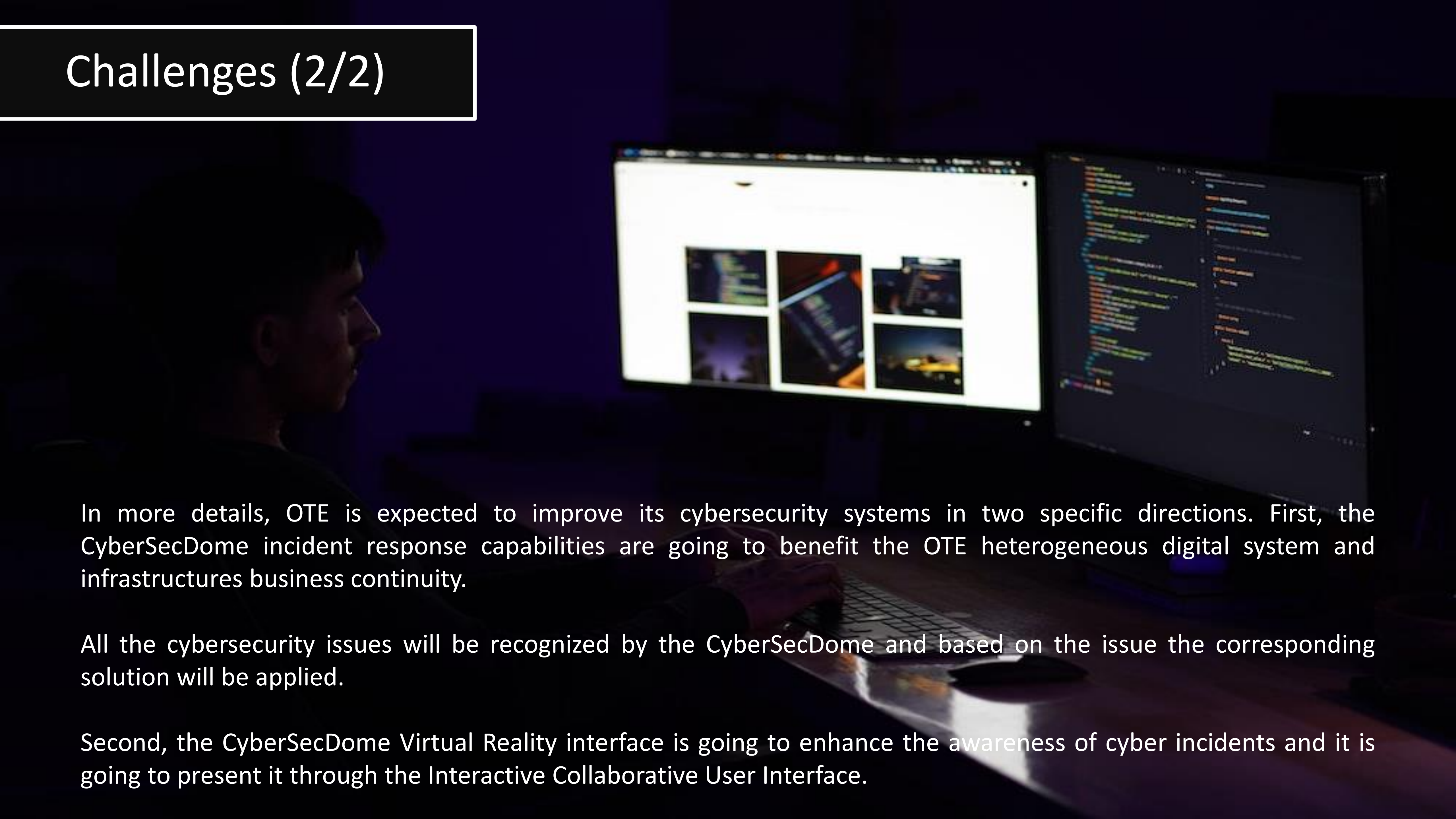
Challenges (1/2)

OTE is a telecommunication authority, which needs to handle critical cybersecurity challenges.

As OTE handles critical data not only as a data owner but also as data processor, the business continuity disruption due to security incidents is a critical issue.

OTE needs to strengthen its security posture against new types of cyber-attacks by using up-to-date detection and prediction tools. Also, as traditional Security Operation Center monitoring methodologies do not provide flexibility and adaptiveness for large and complex digital infrastructures, i.e., OTE infrastructure is highly complex, new technology system frameworks need to be adapted. Based on the above challenges, OTE will integrate the CyberSecDome into its systems so that to be less vulnerable to cyber security criminals.

Challenges (2/2)



In more details, OTE is expected to improve its cybersecurity systems in two specific directions. First, the CyberSecDome incident response capabilities are going to benefit the OTE heterogeneous digital system and infrastructures business continuity.

All the cybersecurity issues will be recognized by the CyberSecDome and based on the issue the corresponding solution will be applied.

Second, the CyberSecDome Virtual Reality interface is going to enhance the awareness of cyber incidents and it is going to present it through the Interactive Collaborative User Interface.

Pilot Use Cases

- DDoS
- Ransomware
- Windows Domain Privilege Escalation

- KPI-1: Reduce the downtime during an incident by 25% compared to the case when CyberSecDome is not used
- KPI-2: Reduce the amount of time to detect an incident by 25% compared to the case when CyberSecDome is not used
- KPI-3: Absolute number of reported incidents compared to the case when CyberSecDome is not used

Thank You!