Use of AI & VR in Offensive & Defensive Cybersecurity

The OTE Pilot Scenarios

Nikos Kogios

ICT Security Services Senior Manager

Member of Group

European Commission

CyberSecDome

infocom SECURITY

OTE

COSMOTE

CyberSecDome project is funded by the European Union's Horizon 2020 Research and Innovation Programme under grant agreement No. 101120779.

Offensive Security Services

- Web & Mobile Application Penetration Testing
- External & Internal Penetration Testing
- Social Engineering Attacks
- Red & Purple Teaming Exercises
- Wireless Penetration Testing
- Vulnerability Assessments

Defensive Security Services

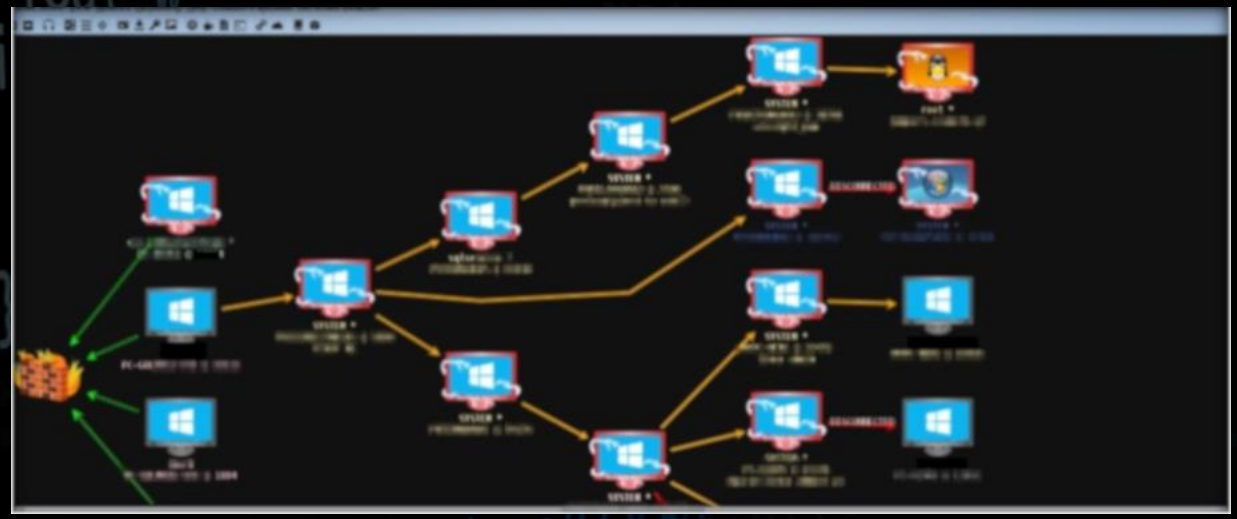
- Managed Security Services / SOC 24x7
- Cloud Security Architecture consulting and hardening
- Security Solutions Integration
- Cloud Web Application Firewall
- Cybersecurity consulting services
- DDoS Protection
- Microsoft Security Services & Solutions

Challenges (1/2)

Common Problems & Attack Paths

- Easily Guessable Passwords
- Lack of MFA (Multi Factor Authentication)
- Lack of effective EDR on endpoints

- New offensive attack methods
- Undetectable Active Directory attacks
- Misconfigurations in management tools or AD



Challenges (2/2)

SIEM

More than 50.000 devices – 150.000 Events Per Second

24x7x365 Monitoring

~ 90 Incidents on a daily basis

Cyber Security Tools

More than 20 different defensive systems

Log Analytics

~ 2T logs per day / 3 attacks per second

Experienced Personnel

Many security challenges in an agile environment – Lots of logs, lots of tools

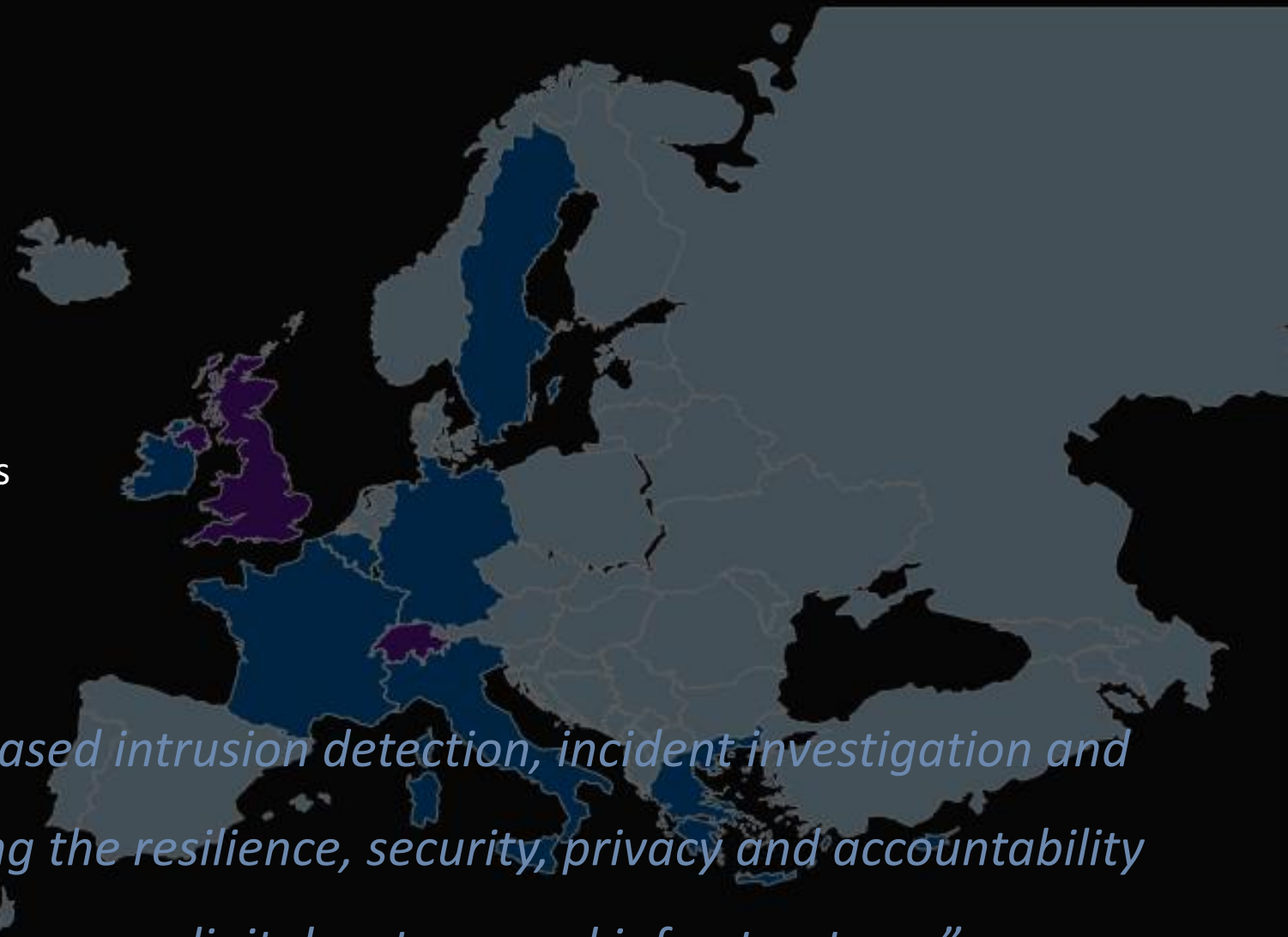
Project ID

Call: HORIZON-CL3-2022-CS-01

Grant Agreement No: 101120779

Type of Action: Innovation Action (IA)

Sep 01.09.2023 - Aug 31.08.2026: 36 months



"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

CyberSecDome

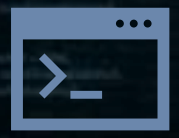
Industry

University

SMEs

Association

Project Objectives



- Increase the disruption preparedness & resilience of digital infrastructure
- Provide dynamic cyber-incident response capability for digital systems and infrastructures
- 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
- Provide better interfaces between humans and cybersecurity algorithms
- Develop solutions to automate penetration testing for proactive security using data-driven AI

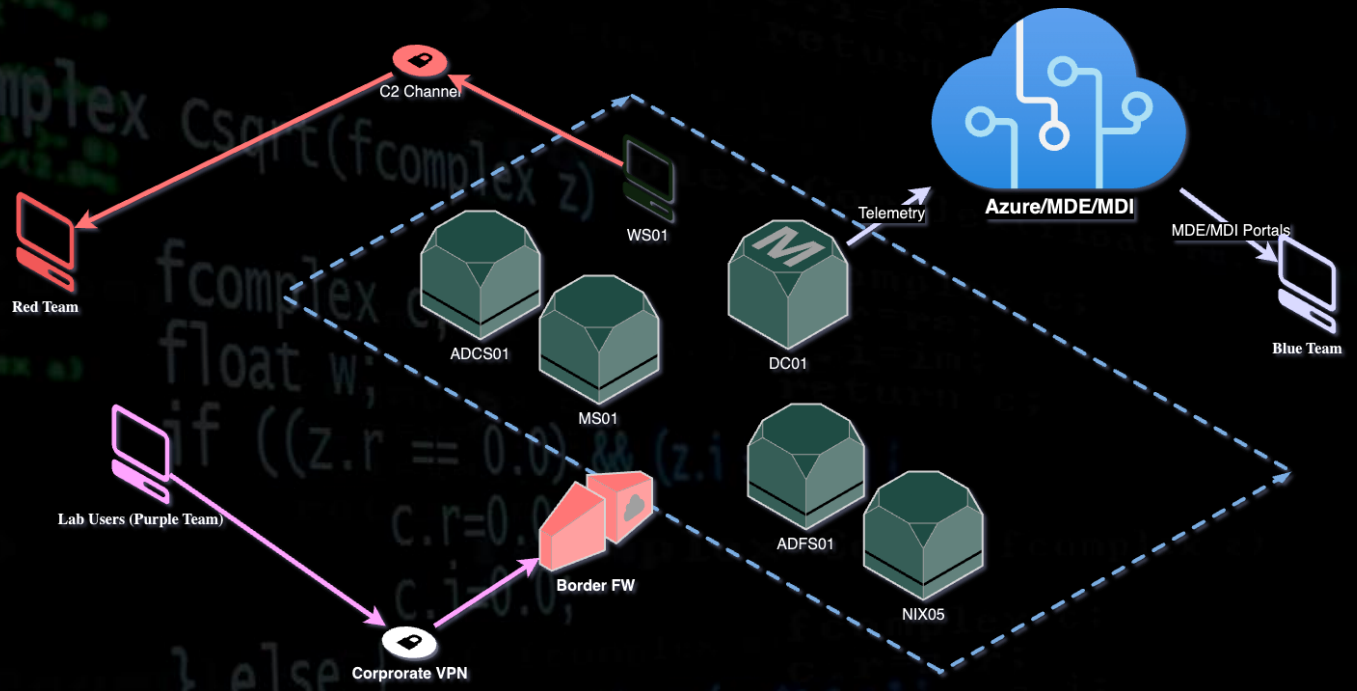
Pilot Use Cases

- 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

Purple Team & Lab

- Combines elements of both Red and Blue Team.
- Simulate and assess security posture.
- Improve detection capabilities
- Enhance incident response
- Fortify overall resilience to cyber threats.




Thank You!