Sec Awareness Truss

A Dynamic Training programme based on Cyber-Ranges Leveraging IT Security, Privacy and Data Protection Culture and Awareness of Critical Information Infrastructures

Project Walkthrough

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under Grant Agreement No 101128049.

Overview

- SecAwarenessTruss is a DIGITAL programme (call: DIGITAL-ECCC-2022-CYBER-03) started on January 2024.

- SecAwarenessTruss will deliver a **customized federated cybersecurity range platform** with **systematic** and **innovative** training programs.

Sec Awareness Truss

Co-funded by the European Union

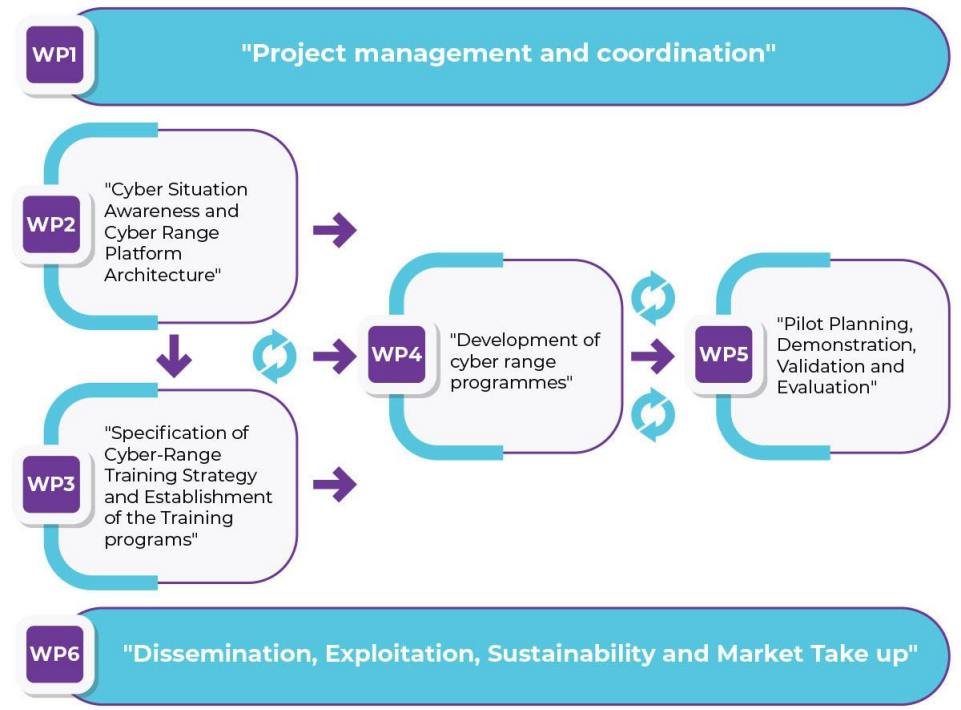
This project has received funding from the European Union's Horizon Europe research and innovation programme under Grant Agreement No 101128049.

Overview

The platform targets **Critical Infrastructure organizations** to develop a skilled workforce for cyber defense and collaborative response.

The project will include:

- Cross-sector complex scenarios
- Gamification-based exercises
- Knowledge-sharing capabilities
- Hands-on and interactive learning facilities



Sec Awareness Truss

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under Grant Agreement No 101128049.

Consortium

SecAwarenessTruss is a collaboration of 10 organizations from Greece and Cyprus, including:

- 4 industrial partners
- 4 critical infrastructure organizations from telecom, energy, health, and maritime sectors
- 2 SMEs

Sec Awareness Truss

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under Grant Agreement No 101128049.

Objectives

Deliver a state-of-the-art platform	Extend capabilities of existing cybersecurity ranges
	Structure training frameworks for effective cyber defence
Develop and deliver training curricul	Innovative and hands-on approach
	Sustainable programs for critical infrastructure
Develop realistic scenario	Large-scale, cross-sector
	Incorporate gaming exercises
Share threat intelligence	Knowledge sharing among cybersecurity ranges
	Coordinated cyber-incident response
	Create common data repository
Evaluate and strengthen ranges	Develop best practices
	Guidelines for wider adoption across Europe

Sec Awareness Truss

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under Grant Agreement No 101128049.

Pilots

- The **four** pilot application scenarios will actively **engage stakeholders** coming from **four critical infrastructure** sectors and featuring different **characteristics**, **services**, **infrastructures** and **training** needs.

Telecom

Energy

HealthCare

Maritime

Sec Awareness Truss

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under Grant Agreement No 101128049.

Pilot Case 1 - Telecom

The Hellenic Telecommunications Organisation S.A. (OTE) manages a large digital infrastructure for ICT services, featuring a 3-tier architecture with presentation, application, and data layers. The scalable virtual infrastructure supports services such as mediation and customer relationship management.

Attack scenarios involve:

- Planning mitigation actions
- Re-training models for infrastructure changes

Training scenarios cover:

- Train response teams
- Enhance situational awareness
- Identify vulnerable systems
- Simulate attack and response scenarios, including ransomware and DDoS attacks

Sec Awareness Truss

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under Grant Agreement No 101128049.

Pilot Case 2 - Energy

Public Power Corporation (PPC) operates a significant energy infrastructure, including the PPC Innovation Hub, offering services like laboratory tests, NDT inspections, and R&D activities. The pilot infrastructure exchanges data for diagnostics and maintenance, focusing on network traffic, electrical measurements, and incident reports.

Attack scenarios involve:

- Planning mitigation actions
- Re-training models for infrastructure changes
- Addressing zero-day threats and Advanced Persistent Threats (APTs)

Training scenarios cover:

- Detection, prevention, simulation, and analysis
- Policies and automation
- Knowledge enhancement

Sec Awareness Truss

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under Grant Agreement No 101128049.

Pilot Case 3 - Healthcare

PAGNI, the largest hospital in Crete, operates an integrated information system connecting medical care, pharmacy, and patient records.

Attack scenarios involve:

- Ransomware
- Phishing
- Insider threats
- Data breaches
- Malicious software
- Denial-of-service attacks

Training scenarios cover:

- Critical system simulation
- Cyber attack detection and prevention
- Real-time network operations management
- Phishing simulation
- Malware detection exercises
- Training healthcare personnel on securing medical devices

Sec Awareness Truss

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under Grant Agreement No 101128049.

Pilot Case 4 - Maritime

DSA will organize a pilot scenario focused on the maritime sector, covering both ashore and ship domains. This scenario will:

- Examine the onboard infrastructure of a specific ship type and its interconnected ashore infrastructure.
- Provide live reaction and planning of cyber defense.
- Improve monitoring and analysis of attacks.
- Optimize information analysis to validate business continuity plans.

Attack scenarios include:

- Ransomware
- Denial of service
- Spoofing attacks
- Sophisticated attacks altering ship behavior

Training scenarios cover:

- Complex cyber threats relevant to maritime ICT infrastructure
- AIS message manipulation
- Navigation system spoofing
- Ransomware attacks on critical systems
- Scenarios tailored to different user profiles

Sec Awareness Truss

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under Grant Agreement No 101128049.

Thank you

ΠΟΛΥΤΕΧΝΕΙΟ ΚΡΗΤΗΣ / TECHNICAL UNIVERSITY OF CRETE

OPEN UNIVERSITY OF CYPRUS

DIGITAL SECURITY AUTHORITY

Zelus

HELLENIC REPUBLIC
Ministry of Digital Governance

ΥΠΟΥΡΓΕΙΟ ΕΘΝΙΚΗΣ ΑΜΥΝΑΣ

Sphynx Technology Solutions

ΟΤΕ

ΔΕΗ

www.pagni.gr
Πανεπιστημιακό Γενικό Νοσοκομείο Ηρακλείου
Πα.Γ.Ν.Η.

Sec Awareness Truss

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under Grant Agreement No 101128049.

www.secawarenesstruss.eu