



Entering the Final Phase

Advancing Cybersecurity Training Across Critical Sectors

From Progress to Completion

As SecAwarenessTruss entered its final six months, the project continues to build momentum through the delivery of training programmes, the coordination of pilot activities and the dissemination of practical cybersecurity resources for critical infrastructure organisations. With the project's objectives steadily being realised, this edition reflects the transition from implementation to delivery of results, while reinforcing SecAwarenessTruss' commitment to strengthening cybersecurity awareness, skills and resilience across the Energy, Telecommunications, Maritime and Healthcare sectors.

6th Plenary Meeting in Heraklion, Crete

On 23–24 June 2026, the SecAwareness Truss consortium gathered in Heraklion, Crete, for its 6th Plenary Meeting, marking an important milestone as the project activities move toward conclusion. Representatives from all consortium partners came together to review the project's progress, strengthen collaboration and coordinate activities to ensure the project's successful completion.

Over the two-day meeting, partners presented the achievements and ongoing work across all active work packages, assessing the progress made against the project's objectives and timeline. Discussions focused on aligning the remaining technical, operational and dissemination activities, ensuring that all deliverables, pilot implementations, training programmes and awareness actions remain on schedule and are fully coordinated.

Special attention was given to the final phase of the project, including completing the cybersecurity awareness training framework, validating the project's cyber range environment, executing pilot activities, and delivering the remaining dissemination and communication actions. The consortium also reviewed the project's key performance indicators and discussed strategies to maximise the visibility, sustainability and long-term exploitation of the project's results beyond its official completion.



Cybersecurity Awareness Lecture at the Hellenic Air Force Academy

On 22 July 2026, SecAwarenessTruss organised a cybersecurity lecture at the Hellenic Air Force Academy, delivered by Dr Michail Smyrlis, Technical Coordinator of the project. The session brought together cadets from all academic years, alongside officers, teaching staff and representatives of organisations participating in the project.

The lecture focused on the current cyber threat landscape and the importance of the human factor in cyber defense. Participants explored social engineering and phishing attacks, essential security practices, operational security and the protection of sensitive data. An interactive demonstration in a controlled cyber range environment gave participants practical insight into realistic threat scenarios, supporting the project's wider goal of strengthening cybersecurity awareness and preparedness.

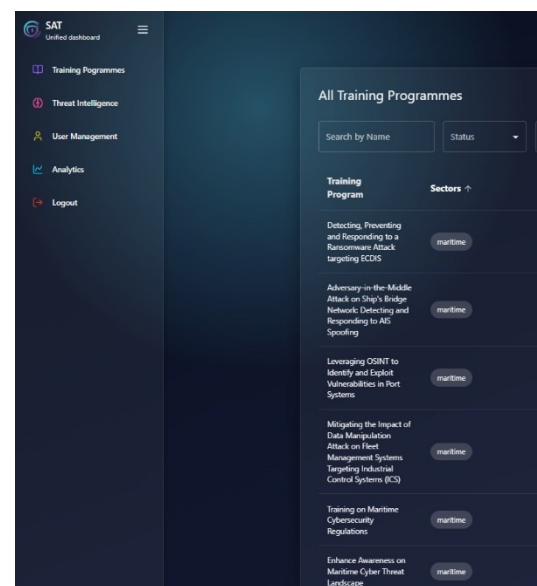


Training Programmes Update

As SecAwarenessTruss enters its final implementation phase, the project's sector-specific training portfolio continues to mature across the Maritime, Energy, Telecommunications and Healthcare pilots. Building upon the core cybersecurity awareness modules already available to all participants—including Cyber Hygiene, GDPR, Phishing Awareness, NIS2 compliance, Fostering organizational awareness and understanding OSINT, the consortium is progressively delivering specialized training programmes tailored to the operational challenges of each critical infrastructure sector.

Maritime Pilot

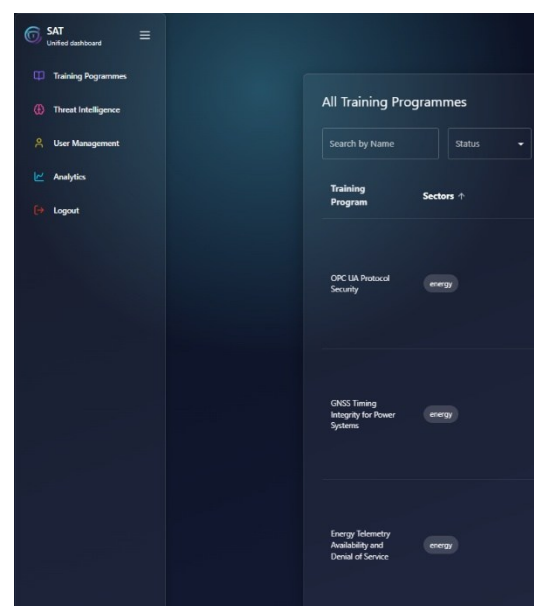
The Maritime pilot, represented by the Cybersecurity and Telecommunications Research Lab (CTRL) of the Open University of Cyprus and the Digital Security Authority (DSA) of Cyprus, has achieved the most advanced level of training delivery, with four specialised cyber range programmes completed. Participants have already engaged in realistic exercises covering ransomware attacks targeting Electronic Chart Display and Information Systems (ECDIS), OSINT techniques for identifying vulnerabilities in port systems, data manipulation attacks against Fleet Management Systems and Industrial Control Systems (ICS), and AIS spoofing attacks targeting ship bridge networks. Together with the maritime cyber threat awareness module, these scenario-based exercises provide participants with holistic practical experience in identifying, analysing and responding to cyber incidents in realistic operational environments. Additional maritime training modules are currently being prepared, further enriching the sector's cybersecurity curriculum.



Energy Pilot

Within the Energy pilot, represented by PPC Group, the training portfolio is expanding to address cyber threats affecting modern energy infrastructures and operational technologies. Alongside the completed awareness programmes on Phishing and NIS2, dedicated modules are being developed on Advanced Metering Infrastructure (AMI) security, GPS spoofing attacks against Wide Area Monitoring Systems (WAMS), physical security in energy facilities, data privacy and confidentiality, as well as cyber range exercises simulating Distributed Denial-of-Service (DDoS) attacks against energy services.

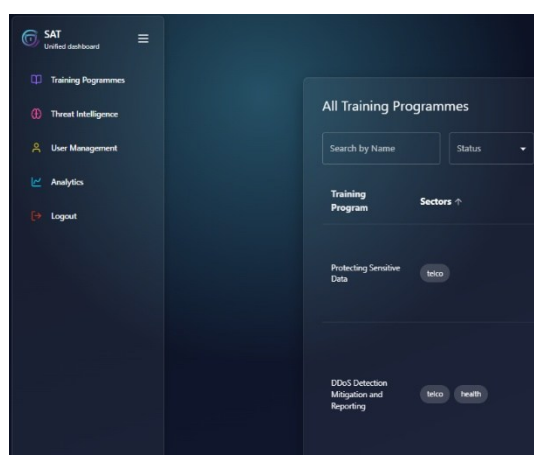
These programmes aim to strengthen both organisational awareness and technical readiness for responding to incidents that may affect the resilience of critical energy infrastructure.



Telecommunications Pilot

The Telecommunications pilot, represented by OTE Group, combines regulatory awareness with technical cyber defence training tailored to telecom environments. Participants already have access to NIS2 compliance, phishing awareness and sensitive data protection modules, while advanced cyber range scenarios addressing Active Directory compromise, privilege escalation, lateral movement and DDoS attacks are being progressively incorporated into the training portfolio.

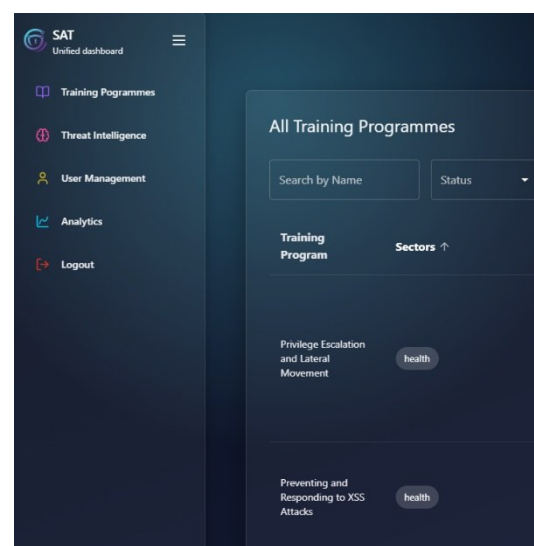
These exercises are designed to strengthen participants' capabilities in detecting, containing and responding to sophisticated attacks targeting telecommunications networks and services.



Health Pilot

The Healthcare pilot, represented by PAGNI Hospital, continues to develop a balanced programme combining cybersecurity awareness with hands-on technical exercises. Healthcare participants already benefit from training on NIS2 compliance, phishing awareness and secure web application practices (XSS), while additional cyber range scenarios covering Active Directory - Privilege Escalation, attacks and DDoS incident management further enhance preparedness against cyber threats affecting healthcare organisations.

By combining awareness, technical knowledge and realistic cyber range simulations, the Healthcare pilot supports the development of practical cyber resilience skills that are directly applicable to healthcare environments.

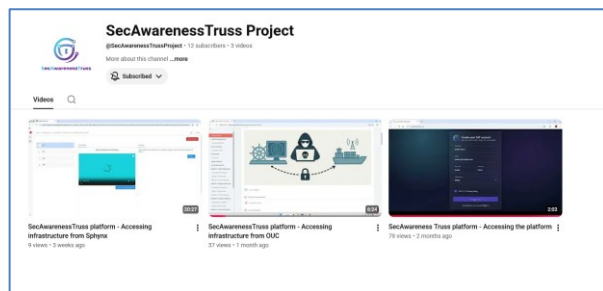


Explore SecAwarenessTruss on YouTube

The SecAwarenessTruss YouTube channel serves as a valuable extension of the project's platform, providing users with practical video tutorials and step-by-step guidance on its features and functionalities.

The videos help learners and trainers navigate the platform, access learning resources, and make the most of the cybersecurity training tools developed within the project. By offering clear and accessible training content, the channel supports the effective adoption of the SecAwarenessTruss platform and contributes to the project's goal of strengthening cybersecurity awareness and digital resilience across Europe.

Visit the channel and explore the available resources at [#SecAwarenessTrussProject](#).



The Road to Project Completion

With the project now entering its final implementation phase, SecAwarenessTruss is focused on completing the delivery of its sector-specific training programmes, finalising pilot activities and validating the project's training framework across the four critical infrastructure sectors.

As the project approaches its conclusion, the consortium remains committed to delivering sustainable results that strengthen cybersecurity awareness, preparedness and operational resilience across the Energy, Telecommunications, Maritime and Healthcare sectors. The final months will consolidate the project's achievements and lay the foundations for the long-term exploitation of its training framework and cyber range capabilities.

[Subscribe to our newsletter to receive exclusive updates and expert content delivered straight to your inbox.](#)

A Dynamic Training Experience for Critical Infrastructures based on Cyber-Ranges

For the latest updates and insights, be sure to follow us on social media.

Connect with us

 [SecAwarenessTruss Project](#)

Visit our website

 <https://secawaresstruss.eu/>

Stay connected, stay informed!



[Co-funded by the European Union](#)

[This project has received funding from the European Union's Digital Europe research and innovation programme under Grant Agreement No 101128049.](#)

[Be part of our growing community!](#)