Newsletter #1

SecureCyber Cluster

Welcome to the 1st issue!

The newsletter will be out monthly and will include all the news and updates regarding the projects' progress and the relevant activities performed by their consortia!

Few words about the cluster!

SECURECYBER CLUSTER

The cluster started its activities in May 2022, with the aim to create synergies for joint cybersecurity solutions, and since then many have been achieved! In a nutsell: Monthly meetings, a common policy brief, a joint white paper, two joint workshops with the participation of all projects, a common press release which you can find on the projects' websites, several workshops and webinars organised by individual projects in which the cluster participated!

And so many more that are about to come, so stay tuned!.

Meet the cluster!

ARCADIAN-IoT

ELECTRON

ERATOSTHENES

IDUNN
INDUSTRIAL CYBERSECURITY

IRIS

KRAKEN

SECANT

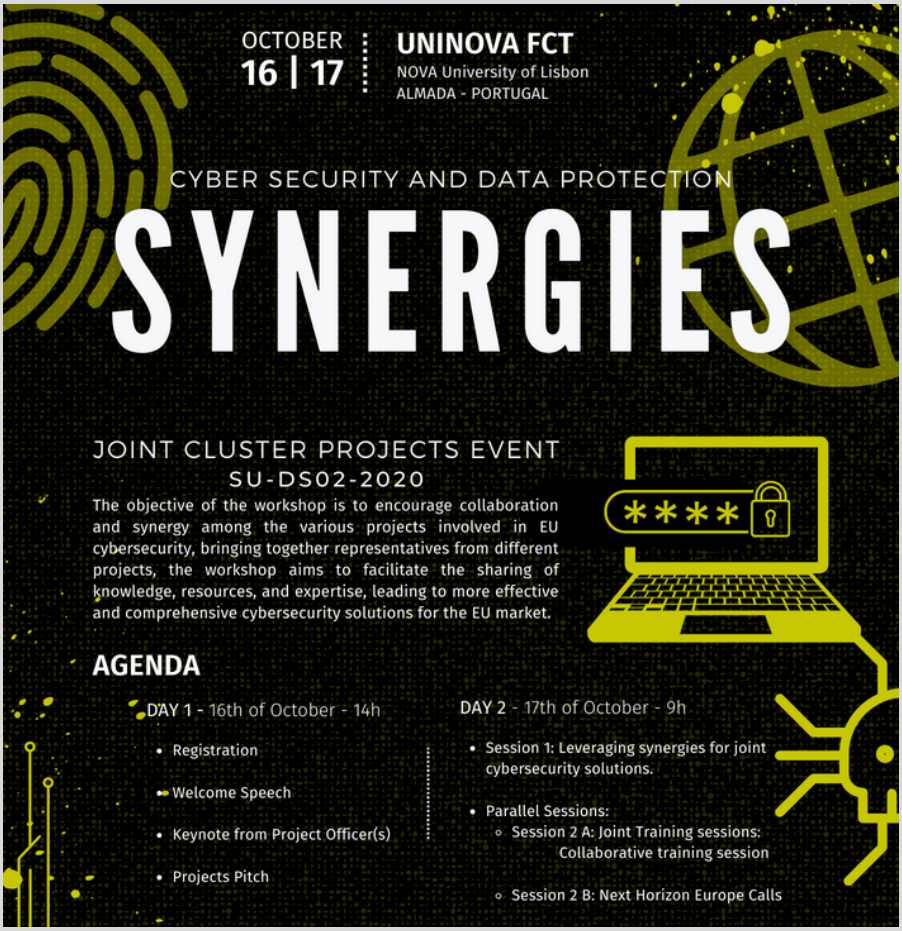
SENTINEL

TRUST aWARE

SPATIAL

Joint Events

“Cyber Security and Data Protection Synergies“ Joint Meeting



The Joint Cluster Meeting was held on 16 and 17 October 2023 in Lisbon, Portugal and online. It was a great chance to create and promote more collaborations in the research community. During the two meeting days, the representatives of IRIS, ARCADIAN, ELECTRON, ERATOSTHENES, IDUNN, IRIS, KRAKEN, SECANT, SENTINEL, SPATIAL and TRUSTAWARE discussed challenges the EU funded projects face, the possible solutions and the future collaborations.

The first day opened with a Keynote presentation from Juuso Stenfors, Project Officer of the European Commission and continued with presentations from all the projects representatives. The second day started with a session focused on the possible synergies for joint cybersecurity solutions, continued with a joint open training session and was completed with a session about next Horizon Europe Calls.

Watch the highlights **here**!

News from the Projects

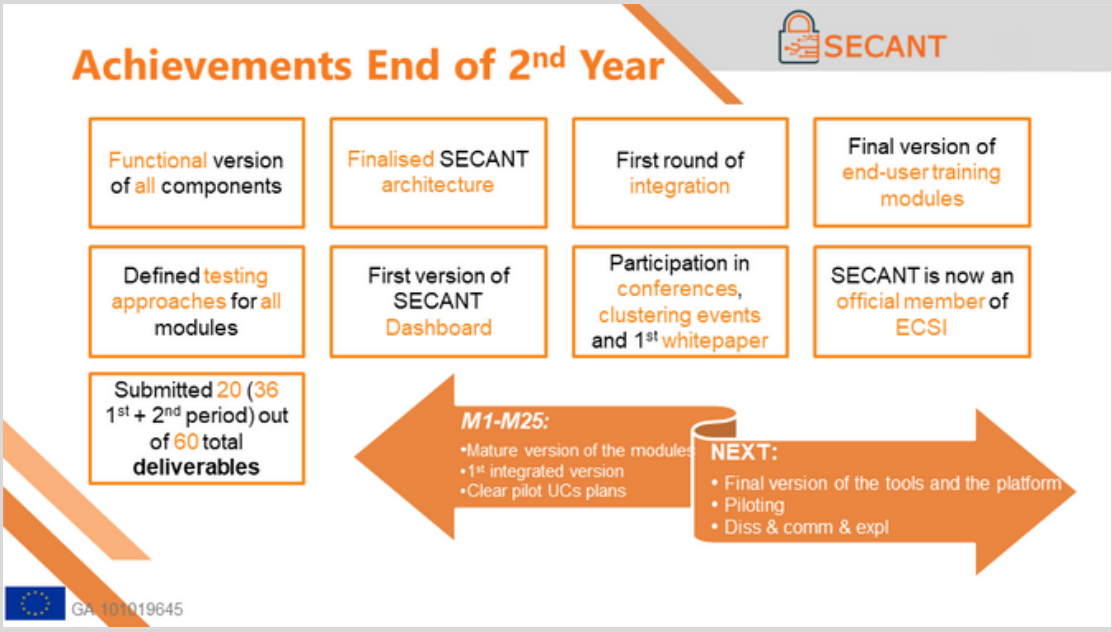
CROSSCON organised the workshop "Security Services for Connected Devices on 12 January 2024, in conjusction with N**ECS-PhD Winter School 2024**. More information you can find on the project's **website.**

The ARCADIAN-IoT training sessions offer comprehensive knowledge on implementing and utilising the ARCADIAN-IoT cybersecurity framework for IoT devices and systems.

The ARCADIAN-IoT training sessions offer comprehensive knowledge on implementing and utilising the ARCADIAN-IoT cybersecurity framework for IoT devices and systems, enhancing understanding of its various components. The trainings are divided into sessions focusing on different aspects:
1. Session 1: Secure identity management for IoT services, covering decentralized identifiers, biometrics, network-based and multi-factor authentication.
2. Session 2: Securing IoT networks in medical services, including network self-protection and blockchain technology.
3. Session 3: Secure IoT support for private IoT infrastructures, discussing remote attestation of devices and reputation system and policy management.

These trainings are designed for ICT users and aim to strengthen their skills in these key areas.

Read more



Final Architecture
The final architecture of SECANT has been completed providing an enhanced and robust platform for monitoring, risk assessment, and training in healthcare organisations.
Through SECANT, considerable progress has been made in addressing the unique cybersecurity challenges encountered by

healthcare organisations, with the goal of safeguarding sensitive data, protecting critical systems, and enhancing the overall security posture of the healthcare industry.
The developed architecture demonstrates a holistic approach, incorporating key components such as monitoring agents, distributed ledger (DLT) storage of IDs and data, and a clearly outlined distinction between the design and execution phases. These developments enhance the efficacy and efficiency of the cybersecurity infrastructure by facilitating proactive monitoring, timely risk assessment, and targeted training initiatives, thereby enhancing the organisation's ability to quickly identify and mitigate potential risks. The DLT on the other hand has enabled the establishment of auditable, tamper-resistant and authorised data exchange and management. The explicit separation of design and runtime phases in the architecture promotes a stringent cybersecurity approach. It enables healthcare organisations to establish security policies, take precautions, and assess risk. This separation also enables efficient and targeted training, which equips healthcare professionals and personnel to identify and respond to security issues.
visit the project's **website**

Get to know the SPATIAL project and its work performed over two years with this article that provides insights into the objectives and accomplishments, elaborates on the implementation of its podcast and work package series, and shares the testimonials collected from stakeholders.
Learn more!

IRIS pilot use cases start soon!

Some facts about them:

Pilot Use Case #1: Securing the smart city's IoT and control systems against confidentiality & integrity breaches.

Focus: Securing the IoT and control system infrastructure deployed in a tramway station against confidentiality and integrity breaches.

Place: Barcelona, Spain
Expected outcomes:

- Safer environment where tramways, pedestrians and bikes may coexist safely
- Less safety issues and accidents stemming from man-made cyber-attacks

End Users: CERTs/CSIRTs, transport operators

Pilot Use Case #2: Securing AI-enabled infrastructure of autonomous transport systems in a smart city.
Focus: Protection of the AI-enabled infrastructure of the autonomous transport system (AV shuttle and the Remote Operation Centre) available in Tallinn against potential orchestrated attacks.

Place: Tallinn, Estonia
Expected outcomes:

- Minimization of the impact of the attack by identifying the threat, self-recovering from it and sharing the corresponding intelligence with other related system operators and platforms
- Assisting system operators to identify if specially crafted data, designed to confuse AI-based decision making, (e.g., spoofed/fuzzed) are received from onboard vehicle sensors, or injected directly to APIs

End Users: CERTs/CSIRTs, CI security operators

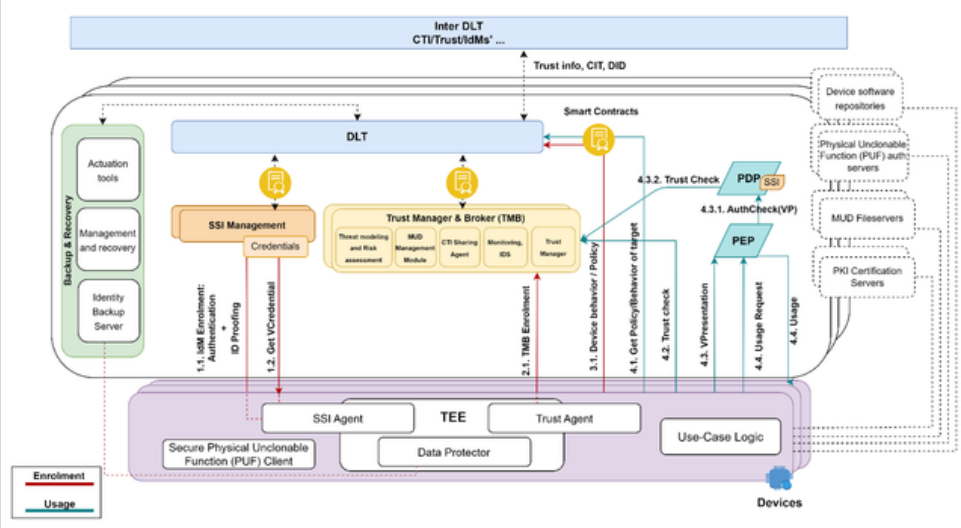
Pilot Use Case #3: Effective incident response and threat intelligence collaboration for critical cross-border smart grid threats.
Focus: Education of CERTs/CSIRTs on effective incident response and threat intelligence collaboration in cross-border cyber-attacks.
Place: Tallinn, Estonia and Helsinki, Finland
Expected outcomes:

- Safer services and more protected components of the smart grid to the building residents
- Better decision-making for the energy operators
- Secure energy infrastructure

End Users: CERTs/CSIRTs, Energy infrastructure stakeholders.
Learn more

The Annual Data Protection Officers Forum reaches its fourth edition

TRUST aWARE played a pivotal role in the success of the European Banking Federation's fourth edition of the Data Protection Officers Forum (DPO Forum) held on November 30, 2023, in Brussels. This event, brought together 45 Data Protection Officers, representatives from Data Protection Authorities, and key European institutions. Notable contributions from TRUST aWARE include a range of novel and integrated tools and services co-created by citizens and stakeholders to identify, audit, analyze, prevent, and mitigate the impact of various S&P threats associated with citizens' digital activities. The forum addressed practical challenges within the banking sector, covering topics like AI integration, the Right of Access, GDPR compliance, and the impact of new digital policy initiatives. The event's success highlights collaborative efforts in navigating the evolving data protection landscape, with TRUST aWARE significantly enhancing DPOs' roles and ensuring robust compliance.
More info **here.**



The **ERATOSTHENES** architecture envisions an environment with multiple independent (but potentially collaborating through information exchange) domains, serving to group operations depending on physical or logical criteria. The components related to the architecture will act within the device, pertain to a specific domain, or operate across multiple ones to enable global functionalities.

ERATOSTHENES establishes identity management based on self-sovereign principles, with SSI Agents in devices managing credentials to enable security and privacy and supporting infrastructural components like SSI Management. Physical Unclonable Function (PUF) based authentication is considered to further enhance the security of identification and cryptographic fingerprinting.

The Trust Management & Broker (TMB), groups key components for achieving a trust framework based on zero-trust principles. Devices will interact with the trust framework through Trust Agents and the TEE will be anchor of trust for devices along with their identity. The TMB's components for IDS, monitoring, threat modelling and risk assessment… will perform the necessary monitoring and evaluation tasks for maintaining an updated trust network for devices. The use of services will require continuous authorization both through identity and trust policies, with the PDP and PEP serving to delegate the process to the domain infrastructure when necessary.

Along with the identity and trust, the architecture also tackles the management of devices' lifecycles through supporting tools like those for backup, recovery, secure data storage, and management (actuation tools, management and recovery, data protector) and the use of MUD files and CTI sharing both for device's security configurations and coordinated responses to cyber-threats.

The whole ecosystem is enabled by DLTs acting as verifiable data registries enriched with smart contracts. Particularly, specific information (such as related to CTI, identity…) **can be carried out across domains through inter-DLT to al**low collaboration that helps achieve a global ecosystem with enhanced security.

Pilots' description and activities:

In ERATOSTHENES project, core technical components will be designed and developed to improve cybersecurity of IoT devices throughout lifecycle phases such as design, implementation, bootstrapping, operation and maintenance. These core components are validated, integrated and deployed using various recipes in the 3 individual pilots.

It will make the ERATOSTHENES components for the real-world deployment. The pilots include use cases from transport, health and industry 4.0. Specifically:

- Pilot 1: Connected Vehicles
- Pilot 2: Smart Health
- Pilot 3: Disposable IDs in Industry 4.0

Pilot 1: Connected Vehicles: In the automotive world the increasing number of IoT devices involved has contributed to the evolution of the environment to a smarter one. In this new era, all the actors are interacting between themselves and making decisions by themselves. Due to this tendency, increasing cybersecurity in this field is a requirement. In pilot 1 there will be two use cases to be validated. Specifically, the first use case is about the interaction with the infrastructure and the second use case wants to cover a key topic in the automotive world, a software update of the vehicle units.

Pilot 2: Smart Health: The Smart Health pilot is a Remote patient monitoring system. It enables remote assistance and follow up on patients who suffer from chronic diseases (e.g., diabetes). Also, it includes other diseases where patients at least partly can stay at home (e.g., COVID-19). In general, the eHealth use case enables patients to stay home during treatment and care and foster self-care. It includes a Personal Health Gateway, which is deployed in every patient's home, that is responsible for collecting data from various medical sensors and sending them to the back-end Cloud services. The services provide data to health personnel allowing for remote patient monitoring, data is recorded in the patient's electronic health journal, and it normalizes data according to standard eHealth ontologies to allow for performing various data analysis.

Pilot 3: Disposable IDs in Industry 4.0: The industry 4.0 revolution has accelerated the rise of usage of IoT devices for controlling, managing, monitoring and optimizing industrial processes. While the revolution has significantly improved the processes, it has increased at the same time the attack surface (e.g., introduction of new attack vectors).

Therefore, the security of the contributing IoT devices is considered of high priority. Pilot 3 details the process of the secure identification of IoT devices, as a step towards the secure execution of authentication and authorization activities.
Visit the **website**