CYBERSANE

2nd Joint Workshop

Dynamic Countering of Cyber-attacks

Achievements and Standardisation

8th of February 2022 - 09:00 – 16:00 CET

CYBERSANE CARAMEL GUARD SAPPAN SOCCRATES SIMARGL

Supported by: FIWARE FOUNDATION

2nd Joint Workshop - Dynamic Countering of Cyber-attacks | *Achievements and Standardisation*

Following the success of the first edition of the workshop back in 2021, **GUARD** announces the participation in the 2nd Joint Workshop – Dynamic countering of cyber-attacks, which will take place virtually between 9:00 and 16:00CET on the 8th of February 2022.

Organised by the CyberSANE project, and this time supported by the FIWARE Foundation, the workshop aims at gathering the projects from the SU-ICT-01-2018 H2020 call, whose main topic is Dynamic countering of cyber-attacks, to share the main progress of the project, create synergies and set a common ground for standardisation activities.

Moreover, experts representing each project will discuss the different approaches to the common problem of attack detection and situational awareness in different environments.

More information about the agenda and speakers can be found on the registration page: https://bit.ly/348hsxa

The participating projects are: C4IIoT, CARAMEL, GUARD, SAPPAN, SIMARGL, and SOCCRATES.

Know more about these projects:

CYBERSANE	CyberSANE enhances the security and resilience of Critical Information Infrastructures (CIIs) by providing a dynamic collaborative, warning and response system supporting and guiding security officers and operators to recognise, identify, dynamically analyse, forecast, treat and respond to advanced persistent threats (APTs) and handle their daily cyber incidents using structured and unstructured data such as logs, network traffic, or data coming from social networks. CyberSANE introduces a holistic and privacy-aware approach in handling security incidents, addressing the complexity of these nets consisting of cyber assets hosted in cross-border, heterogeneous CIIs from the Energy, Maritime Transportation and Healthcare sectors. CyberSANE System, is an innovative, knowledge-based, collaborative security and response dynamic system, capable of implementing all phases of the Cyber incident handling life cycle for increasing the agility of the security professionals and encourage continuous learning. Follow CyberSANE on Twitter and LinkedIn
C4IIoT	C4IIoT will design, build and demonstrate a novel and unified Cybersecurity 4.0 framework that implements an innovative IoT architecture paradigm to provide an end-to-end holistic and disruptive security-enabling solution for minimizing the attack surfaces in Industrial IoT systems. C4IIoT bridges cyber assurance and protection, machine (deep) learning (ML/DL), edge/cloud computing, blockchain and Big Data technologies to provide a viable scheme for enabling security and accountability, preserving privacy, enabling reliability and assuring trustworthiness within evolving IIoT applications and processes (e.g. automotive). C4IIoT novel cybersecurity mechanisms are carefully orchestrated across all infrastructure elements involved within an IIoT system (e.g., IIoT devices, field gateways, cloud resources) and

	is based upon analysis of various data flows (e.g., IIoT device data, encrypted network flows). Follow C4IIoT on Twitter and LinkedIn
	CARAMEL is a project that aims to introduce an innovative anti-hacking intrusion detection/prevention system for the European automotive industry. Their goal is to proactively address modern vehicle cybersecurity challenges applying advanced Artificial Intelligence (AI) and Machine Learning (ML) techniques and also to continuously seek methods to mitigate associated safety risks. In order to address cybersecurity considerations for the already here autonomous and connected vehicles, well-established methodologies coming from the ICT sector will be adopted, allowing to assess vulnerabilities and potential cyberattack impacts. Although past initiatives and cybersecurity projects related to the automotive industry have reached to security assurance frameworks for networked vehicles, several newly introduced technological dimensions like 5G, autopilots, and smart charging of Electric Vehicles (EVs) introduce cybersecurity gaps, not addressed satisfactorily yet. Considering the entire supply chain of automotive operations, CARAMEL targets to reach commercial anti-hacking IDS/IPS products for the European automotive cybersecurity and to demonstrate their value through extensive attack and penetration scenarios. Follow CARAMEL on Twitter and LinkedIn
GUARD	GUARD is a cybersecurity framework to Guarantee Reliability and trust for Digital service chains. They aim to design a holistic framework for advanced end-to-end assurance and protection of business service chains. GUARD also aims to improve the detection of attacks and identification of new threats as well as develop fine-grained, programmable and low-overhead monitoring, inspection and enforcement systems. Further to improving awareness and reactions to incidents, GUARD aims to elaborate new business models for commercial exploitation after the project lifetime. Follow GUARD on Twitter and LinkedIn
	SAPPAN aims to develop a platform for sharing and automation to enable privacy preserving and efficient response and recovery utilizing advanced data analysis and machine learning. They will provide a cyber threat intelligence system that decreases the effort required by a security analyst to find optimal responses to and ways to recover from an attack. This will be enabled within a single organization as well as across organisations through novel models for privacy-preserving data processing and sharing. SAPPAN will also enable a European level perspective on advanced cyber security threats detection, response, and recovery making four key contributions that go beyond existing approaches: (1) privacy-preserving aggregation and data analytics including advanced client-side abstractions; (2) federated threat detection

	based on sharing of anonymised data and sharing of trained machine learning models; (3) standardisation of knowledge in the context of incident response and recovery to enable reuse and sharing; (4) visual, interactive support for Security Operation Center operators. SAPPAN aims to provide solutions for public international institutions and multinational companies who want to enrich their Situational Awareness by sharing cyber security intelligence as well as solutions for small and midsize companies enabling them to outsource intrusion detection. Follow SAPPAN on Twitter
	SIMARGL is a project co-funded by the European Commission under Horizon 2020 programme, to combat the pressing problem of malware. It aims to tackle the new challenges in the cybersecurity field, including information hiding methods, network anomalies, stegomalware, ransomware and mobile malware. SIMARGL will offer an integrated and validated toolkit improving European cybersecurity. The cutting-edge of the proposed solution stems from the development of a more general approach, one that has the ability to counteract the new, complex malware. SIMARGL will use breakthrough methods and algorithms to analyze the data from networks, such as: concept drift detectors, advanced signal processing and transformations, lifelong learning intelligent systems (LLIS) approach, hybrid classifiers, and deep learning, just to mention some techniques. Follow SIMARGL on Twitter
SOCCRATES	SOCCRATES aims to develop and implement a new security platform for Security Operation Centres (SOCs) and Computer Security Incident Response Teams (CSIRTs) of individual organisations and offered by Managed Security Service Providers (MSSP). They will significantly improve their capability to quickly and effectively detect and respond to new cyber threats and ongoing attacks by using this platform. The platform contains innovative solutions to automated infrastructure modelling, improve attack detection, Cyber Threat Intelligence utilization, AI and machine learning based threat trend prediction, and automation using Attack Defence Graphs (ADG) and business impact modelling to aid human analysis and decision making on the best course of action, enabling the execution of defensive actions at machine-speed. Follow SOCCRATES on Twitter and LinkedIn