Media contact :

itrust consulting s.à r.l.

Ingo Senft
Public Relations Manager
+352 26 17 62 12
senft@itrust.lu

Improving the resilience of essential service providers against cyber-attacks in Europe.

Niederanven, Luxembourg – 7th of October, 2016[1] – itrust consulting s.à r.l. announces its partnership with an international consortium of essential services operators and providers, industrial actors, universities, research centres and SME's, in order to develop and validate tools to improve the resilience of essential service providers (critical infrastructures) throughout Europe.

The law enforcement agency of the European Union Europol is expecting an increase in cyber-attacks on essential service providers (especially on gas, water and electricity providers) throughout Europe. To face this threat, the EU is co-funding a research project called ATENA: "Advanced Tools to assEss and mitigate the criticality of ICT compoNents and their dependencies over Critical InfrAstructures". During this project, the Luxembourg-based SME itrust consulting, in collaboration with the electricity and natural gas grid operator CREOS, organised a visit of the CREOS dispatching in Heisdorf (Luxembourg) on September 27th to learn about their infrastructure and to define requirements for advanced security tools. In this sense, this assembly was followed by a visit at the Société wallonnie des Eaux (SWDE) in Verviers (Belgium) on September 28th and 29th 2016. These meetings also gave the opportunity to the essential service providers, CREOS and SWDE to define their needs and explain how they will validate the project results.

ATENA supports a unique collaboration between itrust consulting s.à r.l., the University of Luxembourg/SnT, CREOS S.A., and other European partners, within Horizon 2020, the EU framework programme for research and innovation. While providing a test platform that represents an exact duplication of their supervisory control and data acquisition system (SCADA), CREOS will benefit from the project by receiving results of the cyber-resilience of their SCADA system and proposals on

[1] updated 14th of March, 2019

how to improve it. Having such a test infrastructure allows simulating possible cyber-attacks and proposing and evaluating appropriate countermeasures to hamper these attacks.

In order to test the resilience of the SCADA system in the event of cyber-attacks, the project partners will develop and validate on the CREOS test-platform, new monitoring and risk prediction systems finalised during the ATENA project. itrust consulting assists the project by providing the required risk assessment tools, by defining cyber-attack scenarios, by conducting penetration tests on the new tools to assess their reliability, and by collaborating to the implementation of big data analysis tools for observing and gathering information related to new attacks in the darknet and other public sources. Carlo Harpes, managing director of itrust consulting, to predict: "this cooperation will allow us to improve our risk monitoring application TRICK, to integrate it into the ATENA system, to validate it with real data and eventually, being able to offer it as a new service for SCADA incident response management."

In addition to the CREOS test-platform, a SCADA test-lab, implemented by the University of Luxembourg/SnT will be used to develop and evaluate distributed anomaly and intrusion detection system that allows validating risk attacks scenarios, for effective risk detection and attack mitigation on essential service providers. University of Luxembourg/SnT will also be involved in the design of novel reaction and resilience mechanisms based on the new concept of Software Defined Security (SDS). SDS will efficiently orchestrate the different tools provided by the ATENA project by allowing dynamic and flexible programming of security functions. The ultimate purpose is to come up with a smart, context-aware, self-defending system.

"This is a key project for Luxembourg to address the security issues with the ultimate purpose to come up with a smart, context-aware, self-defending system" stresses Prof. Dr. Thomas Engel, University of Luxembourg, "Together with the international partners University of Luxembourg/SnT will deploy an anomaly detection and attack prediction tool that will alert the operator of critical infrastructure to any abnormalities happening in their system and suggest investigative or corrective actions."

About itrust consulting: itrust consulting s.à r.l. is an SME from Luxembourg that specialises in Information Security Systems. itrust consulting helps actors from the public, financial and private sector to protect their information against any divulgence, manipulation or unavailability with consulting, auditing, and training services or with tools or innovative services developed and improved through multiple research projects. In the field of Information Security, itrust consulting, has become a well-recognised and trustworthy partner in Luxembourg and throughout Europe. The company applies innovation, participates in research projects (FP7, H2020, ITEA2, Celtic, ESA), and

develops norms, security tools and information processing techniques, covering topics like information Security Management Systems, risk management, penetration testing, digital signatures, cryptology, Internet security, essential service providers Protection, SCADA, Secure Localisation, data privacy, computer forensics, operates malware.lu CERT. itrust consulting is also well accepted for its SECurity as a Service (SECaas) approach. Further information on: https://www.itrust.lu/

About CREOS: CREOS Luxembourg S.A. owns and manages electricity and natural gas networks in Luxembourg. The company is responsible for the planning, realisation, maintenance and operation of High- Medium- and Low-Voltage electricity grids and natural gas pipelines. Further information on: http://www.creos-net.lu/start.html

About SnT: The Interdisciplinary Centre for Security, Reliability and Trust (SnT) which belongs to the University of Luxembourg conducts internationally competitive research on security and reliability in information and communication technology (ICT), with high relevance creating socio-economic impact. In addition to long-term, high-risk research, SnT engages in demand driven collaborative projects with industry and the public sector. The project ATENA is performed within the SECAN-Lab research group headed by Prof. Dr. Thomas Engel. Further information on: http://wwwen.uni.lu/snt/about_us

About ATENA: The ATENA project (Advanced Tools to assess and mitigate the criticality of ICT compoNents and their dependencies over Critical InfrAstructures) aims at developing a Software Defined Security paradigm combining new anomaly detection algorithms and risk assessment methodologies within a distributed environment and will provide a suite of integrated market-ready ICT networked components and advanced tools embedding innovative algorithms both for correct static critical infrastructure configuration and for fast dynamic reaction in presence of adverse events. The ATENA project is co-funded by the European Commission at the amount of 6.9 million Euros and is set to start at Mai 16th 2016 and end on April 19th 2019. The consortium of the project consists of partners from eight different European countries and Israel. The project assembly consists of end-users (IEC, CREOS and SWDE), industrial actors (Leonardo and Sapienza SL), research centres (ENEA, IBS and CRAT), universities (University of Luxembourg, University of RomaTre and the University of Coïmbra) and private companies (itrust consulting and Multitel) and is led by the Italian company Leonardo S.p.A. specialized in Defence and Security Systems. Further information on: https://www.atena-h2020.eu/information/

Photos

Photo 1: Water treatment plant in Verviers (SWDE)

Photo 2: Testing and training centre in Verviers (SWDE)