SLISE Project

5G's benefits for the SLISE Project

Technology has undergone a significant change with 5G, which connects several devices into a single grid. This is an advantage that, for instance, enables Redeia to remotely inspect its electrical assets to better optimize facility maintenance and increase security. Additionally, it provides the opportunity for independent communications systems and infrastructure optimization.

The SLISE project has been marketed within this context by Redeia and its technology platform, Elewit. It is a cybersecurity initiative whose goal is to reduce any potential weaknesses that the new 5G architectural technologies might provide to the emerging model of communications as a service.

The project, which will last 37 months, is being developed by a group of 8 Spanish companies, including Redeia and Elewit. In order to handle the risks associated with virtualization technologies, its development will involve technologies that offer research into **new incident analysis, encryption, identification, and automated response algorithms i**n a more flexible context.

In a sequence of usage scenarios that present multiple protection priorities and that include the use of communications in the context of managing critical infrastructure as well as the use of communications in the manufacturing industry, all of this will be studied while defining demanding indicators that extensively cover these objectives.

There are four lines of work in the project:

- **Definition of requirements and use cases:** In this section, **the technical objectives, requirements analysis, definition of technical architecture, definition of virtualized structure, definition of configurable policies and communication interfaces, definition and scope of the generating systems,** and definition and scope of the generating systems are all thoroughly defined. This year is the expected timeline for accomplishing this first phase.

- **Definition of 5G system protection and attack and anomaly detection:** Presentation of the 5G protection system and methods for preventing potential vulnerabilities.

- **Analysis of injection attacks, information extraction, and activity session control:** Study of activity-controlled information extraction methods.

- **Evaluation of the project:** Analysis and appraisal of all past work to determine its viability.

Due to their strategic positioning in relation to their diverse cybersecurity objectives, threats, or study scenarios, the group's companies take part in the project. So that **they may be proven in a set of scenarios that are very relevant for validation, the cybersecurity objectives are in line with the most commonly acknowledged set of vulnerabilities in the communications industry.**

The group has chosen this strategy because it thinks it will make it easier to disseminate and adopt the outcomes they have found and to look for new challenges based on their experience. The group's members will work together, complement each other, and coordinate to provide coverage and solutions for all the project's goals.

The function of Redeia's technical platform, Elewit

In this case, **research on the use of AI in the detection of attacks in shared subnets and the necessary explorations to enable the integration of providers with 5G communication interfaces** into the communication architectures managed or controlled by the company, expanding the capacity for collaboration and business development, are two examples of how Elewit, a technology provider in the energy sector, aims to advance the state of the art in the areas in which it is a reference point.

Project funded by:

GOBIERNO DE ESPAÑA MINISTERIO DE CIENCIA E INNOVACIÓN
CDTI INNOVACIÓN
Plan de Recuperación, Transformación y Resiliencia
Financiado por la Unión Europea NextGenerationEU