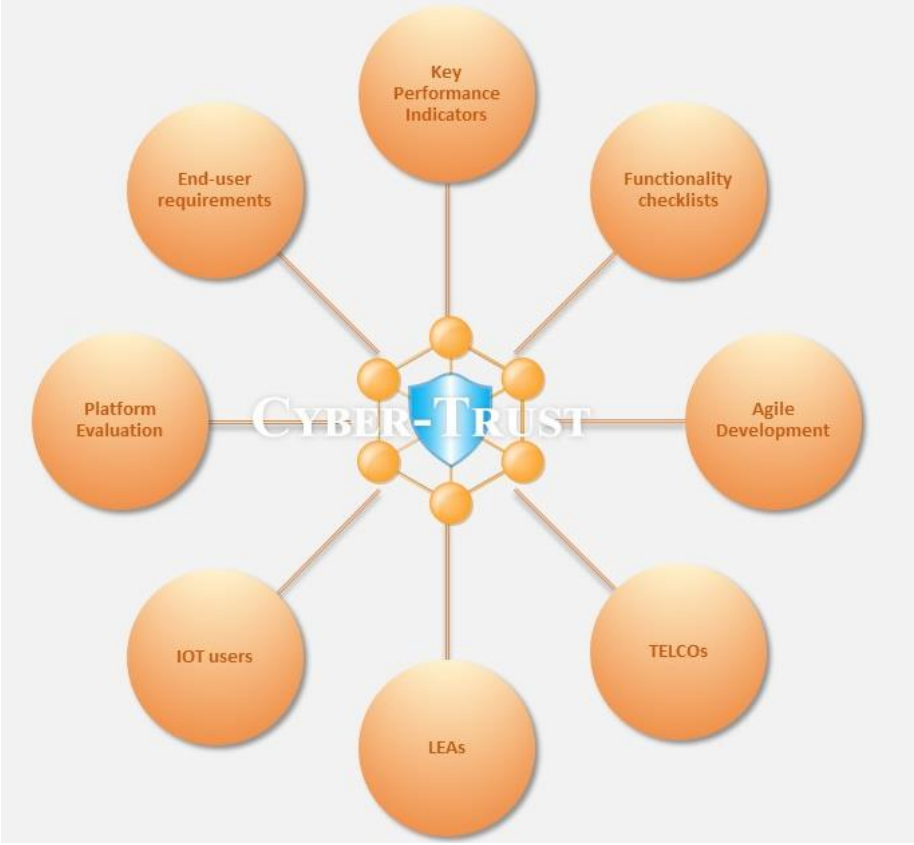
Advanced Cyber-Threat Intelligence, Detection, and Mitigation Platform for a Trusted Internet of Things

Pilot Evaluation strategy and road ahead

To address the major challenges of securing the IoT ecosystem from cyber threats, the Cyber-Trust project has developed a revolutionary framework that will first identify, then analyse, and next mitigate these threats. To achieve this, the Cyber-Trust project conducts research in the following main cyber-security areas: a) develop state of the Art (SOTA) cyber security tools, b) identify cyber-attack and mitigate their consequence, and c) use of distributed ledger technologies. The Cyber-Trust project has developed an innovative platform based on end user specifications that formed the technical and functional requirements of the project.

The validation of the Cyber-Trust platform will be achieved in two (2) pilot phases. In both phases, Cyber-Trust functionality will be verified using several use case scenarios, developed by the potential end users: IoT device owners, Internet Service Providers (ISPs), and Law Enforcement Agencies (LEAs).



Currently, the Cyber-Trust platform is operational and ready to be tested, validated, and evaluated by its potential end-users. The testing procedures and the methodology that will be

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 786698

used to evaluate the platform are adequately documented in the evaluation plan of the platform. The objective of the platform evaluation is to ensure that the requested functionalities are delivered and that the end user requirements sufficiently met.

The evaluation plan includes the measurement of ***Key Performance Indicators (KPI)***, verification of the ***platform functionalities*** while an ***assessment questionnaire*** will measure the *effectiveness*, *efficiency*, *satisfaction*, *maintainability*, and *reliability* of the platform. As a result of this process, the three end-user groups not only will evaluate the developed platform, but also will provide feedback to improve the platform and identify issues that should be addressed by the technical team.

The data processing methodology complies with all appropriate legal measures. The evaluation process will use both qualitative and quantitative methods to process end user inputs. Results from the three end user questionnaires will be reported, along with *recommendations for future platform improvements*. At the end of the platform evaluation a development phase will follow to satisfy additional end *user requirements* and remedy any *issues reported*. The outcome of a successful and direct first pilot phase would not be only the solid basis for the second and final pilot implementation phase, but also for future achievements of the cybersecurity ecosystem.

Further information on Cyber-Trust is available on the project *website*. To stay updated on Cyber-Trust's activities and events, please get in touch with us using this *form*.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 786698