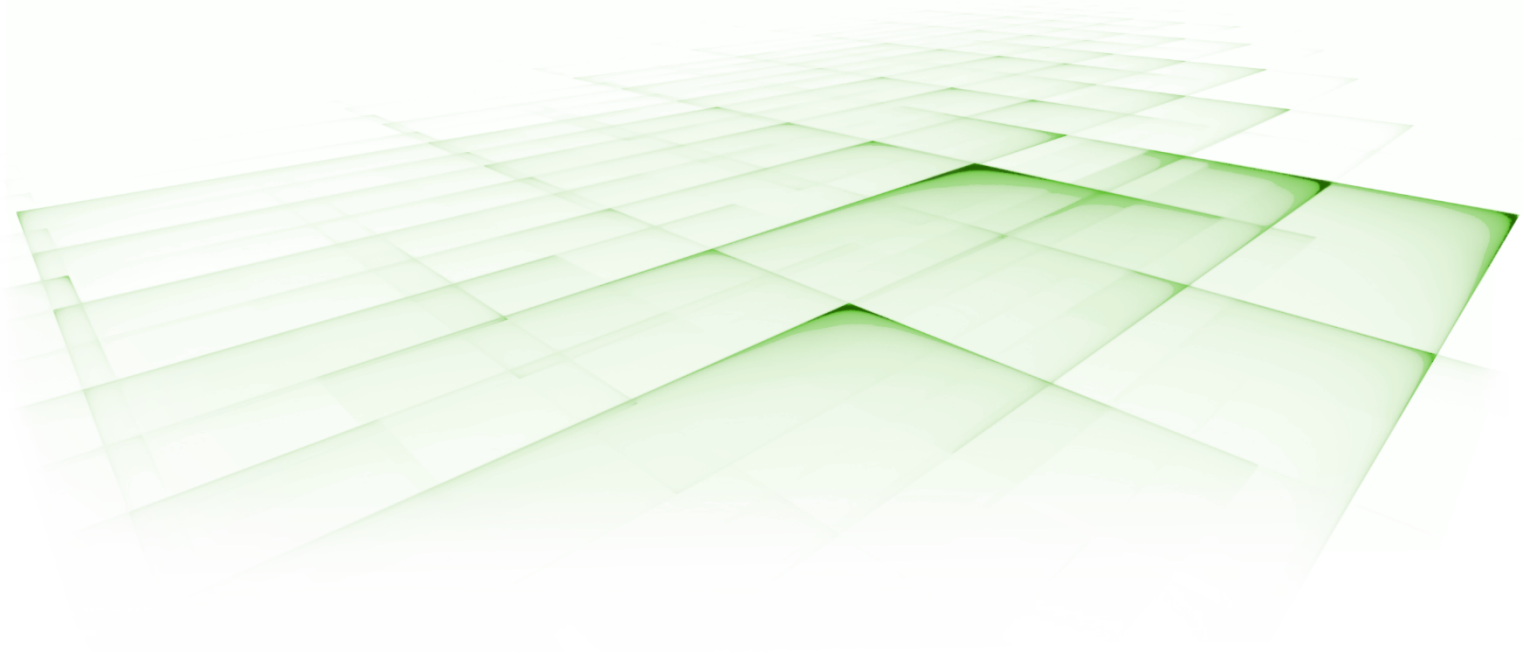
EUCloudEdgeIoT - expression of interest CETIC

Sébastien Dupont

V.1.0 – 16/04/2023



CETIC ASBL – Centre d'Excellence en Technologies de l'Information et de la Communication
Aéropole – Avenue Jean Mermoz 28 – B-6041 Charleroi
e-mail : info@cetic.be - TVA BE 0474 549 932

Motivation

Resilience and security of the Cloud-Edge-IoT continuum are proving to be more important than ever. The convergence of IT and OT brings new security risks, as illustrated by the Industroyer2 attack on Ukraine energy infrastructure in 2022, or the attack on a Florida Water treatment plant in 2021.
Hardening Cloud-Edge-IoT has to be done by design, not as an afterthought. The lifecycle of such systems need to implement security and quality at every step, from the planning phases to the operations activities. Updates should be frequent and easy, for example to patch newly discovered vulnerabilities as soon as possible on lots of heterogeneous edge devices. Remediation should also be automated to provide a level of autonomy in the system's response to an incident in case the edge devices lose connectivity or if a real time response is required.

Current Status

Standards and regulations are constantly evolving and improving, they provide a baseline to design resilient and secure Cloud-Edge-IoT systems. Regulations, such as GDPR or the NIS2 Framework that aims at providing a high common level of cybersecurity across the Union, will be complemented by the Cyber Resilience Act that defines EU cybersecurity rules to ensure safer hardware and software. Those can be coupled for example with ISO/IEC 27001 for security and ISO/IEC 25010 for quality.
Edge devices are currently hard to update, when at all possible, which increases the attack surface of the Cloud-Edge-IoT continuum. On the other hand, those devices can provide increasing compute capabilities that can be leveraged to improve their observability and resilience. For example, lightweight intrusion detection and protection systems can provide a first autonomous line of defense at the edge while more powerful security mechanisms will manage the threat in the cloud.

Research Challenges

In order to improve the security and resiliency of the Cloud-Edge-IoT continuum by design, we have identified and are interested in the following research challenge.

Autonomous response for security and resiliency

In response to a problem, the Cloud-Edge-IoT continuum should be "self-healing". This involves automation at various levels to reduce the time to detect, respond to, and recover from incidents. In order to simulate and train the autonomous security and resiliency response against new and unknown threats, various automated tests can be applied: penetration testing, load testing, chaos engineering, … Tools and methodologies need to be adapted or created to manage this autonomous response across the Cloud-Edge-IoT

continuum. Security Information and Event Management (SIEM) systems, Security Operations Centers (SOC), cyber ranges or cyber labs for example should integrate the concept of digital twin to manage IoT devices. This autonomous response also needs to keep the human in the loop, helping the cybersecurity analysts and software reliability engineers make better and more informed decisions.

This challenge relies on a risk-based approach, where security and resilience are approached “by design”. The validation of the autonomous response relies on assessment tools that collect and analyze information from the various components of the Cloud-Edge-IoT continuum across the system’s life cycle. This can be achieved by relying on the DevSecOps approach that integrates development, operations and security activities to build quality and secure software.