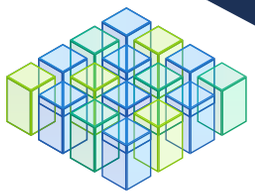
As an End-User, I want to include a new 3rd party component into my system



Design Phase

BIECO helps me find vulnerabilities and exploits, and provides adequate mitigation strategies

Before Deployment

BIECO applies a certification methodology, to provide a security label and a set of claims

At runtime

BIECO helps me ensure a trusted and secure behaviour of my system, verifying design claims

The Consortium

UNINOVA · Fraunhofer IESE · National Research Council of Italy · Technical University of Cluj-Napoca Romania · gradiant · Universidad de Murcia · RESILTECH Technologies for Resilience · HOLISUN · TTTechAuto · 7bulls.com · IFEVS

Project Coordinator 2020-2023
Prof. José Barata (UNINOVA)
jab@uninova.pt

This project has received funding from the European Union´s Horizon 2020 Research and Innovation Program under Grant agreement No. 952702.

bieco.org

BIECO

Building Trust in Ecosystems and Ecosystem Components

Improving security and trust at a supply chain level.

bieco.org

Our Approach

The ongoing events of this decade have once more brought to the limelight the importance of ensuring proper cybersecurity and safety of Europe's critical infrastructure.

As one of the more significant examples, the war in Ukraine has led to one of the largest energy crises in recent history, with experts warning that if sustained cyberattacks are targeted at the European energy sector the consequences could be disastrous.

Interruptions to the already fragile energy markets could further raise fuel prices to hundreds of millions of consumers, contributing to further economic and human losses. **This represents a major cross-sectorial challenge, with many interdisciplinary challenges to be addressed.**

As such, it is crucial European industry leaders and policy makers to bolster the overall resilience of Europe's key infrastructure against cyber attacks and vulnerabilities, with efforts including for instance the promotion of security-by-design and improved risk and vulnerability management across the value chain.

BIECO provides a holistic approach to improve security in complex ecosystems and ecosystem components along their lifecycle, improving trust at a supply chain level.

BIECO includes over 15 different tools covering the software lifecycle from design to runtime.

The large majority of these tools is integrated into a common platform to facilitate their interoperability and orchestration in easily deployed tool chains tailored to address specific business needs.

BIECO leverages a combination of state-of-the-art artificial intelligence, digital twins, simulation and static analysis to address the following key areas:

- ✔ **Vulnerability Assessment and Management**
- ✔ **Risk Assessment and Mitigation**
- ✔ **Resilience Mechanisms**
- ✔ **Security Certification and Testing**
- ✔ **Runtime Auditing of ICT Ecosystems**

A holistic approach for building and validating technologies and methodologies that are specifically oriented towards fostering security and trust within ICT ecosystems.

BIECO's validation takes place across three distinct business cases spanning different activity sectors, namely **Energy, Manufacturing and Electric Mobility, and Finance.**