BIECO

Building Trust in Ecosystems and Ecosystem Components

Call: H2020-SU-ICT-2018-2020 (Cybersecurity)

septembire 2020 – august 2023

Ovidiu Cosma
ovidiu.cosma@mi.utcluj.ro

Consortium

UNINOVA

Fraunhofer
IESE

HOLISUN

TTTechAuto

TECHNICAL UNIVERSITY
OF CLUJ-NAPOCA
ROMANIA

gradiant

UNIVERSIDAD DE
MURCIA

RESILTECH
Technologies for Resilience

I-FEVS

7bulls.com

Challenges

BIECO
Building Trust in Ecosystems and Ecosystem Components

Fragmentation of Supply Chain Components

Unverifiable Trust in Third-party Solutions

Increased Risk of Cyberattacks

Impact on Cyber-Physical Systems (CPS)

Need for Mindset Shift to "Untrusted by Default“

Necessity for Verifiable Security Guarantees

BIECO's Concept

BIECO
Building Trust in Ecosystems and Ecosystem Components

BIECO helps build trust in complex ICT systems by:

- Focusing on reliability and security;
- Providing a framework to manage risks and ensure trust across the system's lifecycle.

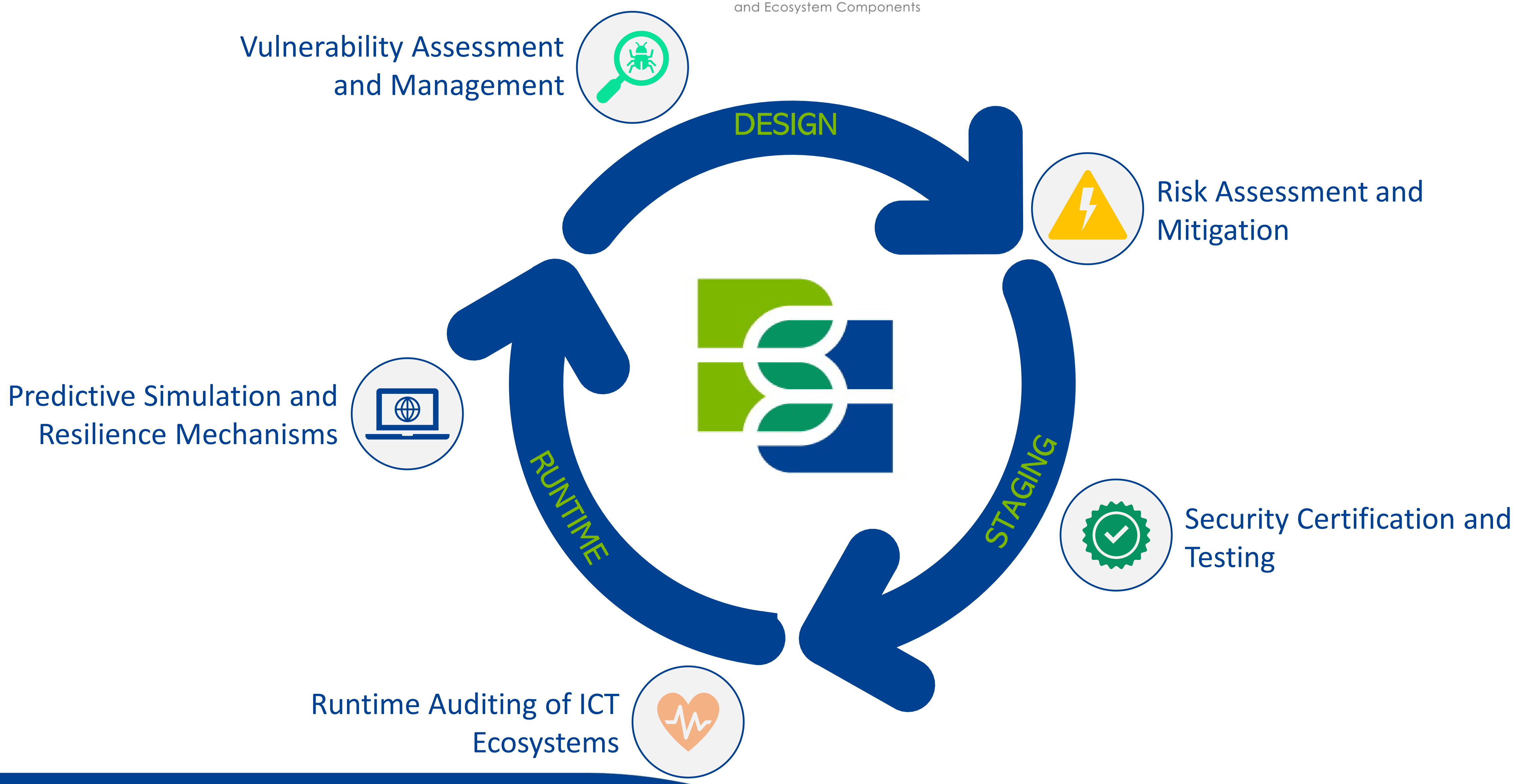
This helps companies to:

- Handle ICT supply chain complexity;
- Reduce cybersecurity risks;
- Keep their systems safe and reliable.

BIECO’s Concept

BIECO

Building Trust in Ecosystems
and Ecosystem Components


Vulnerability Assessment and Management
DESIGN
Risk Assessment and Mitigation
Predictive Simulation and Resilience Mechanisms
STAGING
Security Certification and Testing
RUNTIME
Runtime Auditing of ICT Ecosystems

BIECO’s Lifecycle

Design Methodology

BIECO detects vulnerabilities early and guides effective risk mitigation.

Staging Methodology

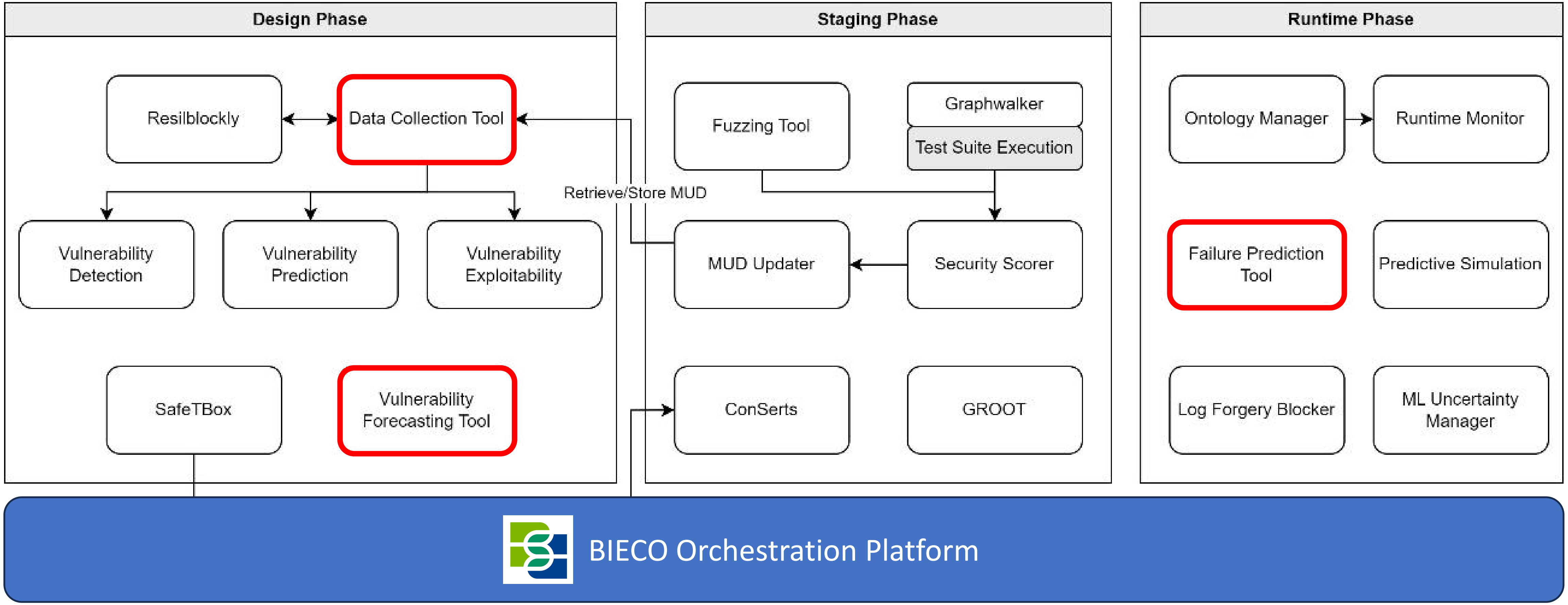
BIECO certifies components with a security label and key assurances.

Runtime Methodology

BIECO ensures a trusted and secure behavior the system, verifying security claims

BIECO Ecosystem

Building Trust in Ecosystems and Ecosystem Components



BIECO’s Use Cases

BIECO
Building Trust in Ecosystems
and Ecosystem Components

BIECO’s validation takes place across three distinct business cases spanning different activity sectors:

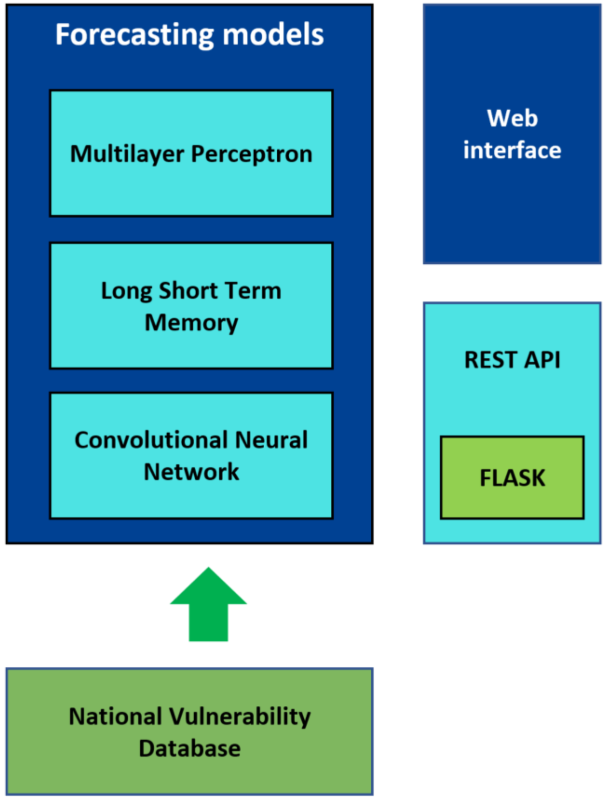
- Manufacturing and Electric Mobility (Smart Microfactory from IFEVS, Turin, Italy)
- Finance (AI Investment Platform from 7Bulls, Warszawa, Poland)
- Energy (ICT Gateway from Resiltech, Pisa, Italy)

T3.3 (M18 - M30)

Vulnerability Forecasting Tool (VFT)

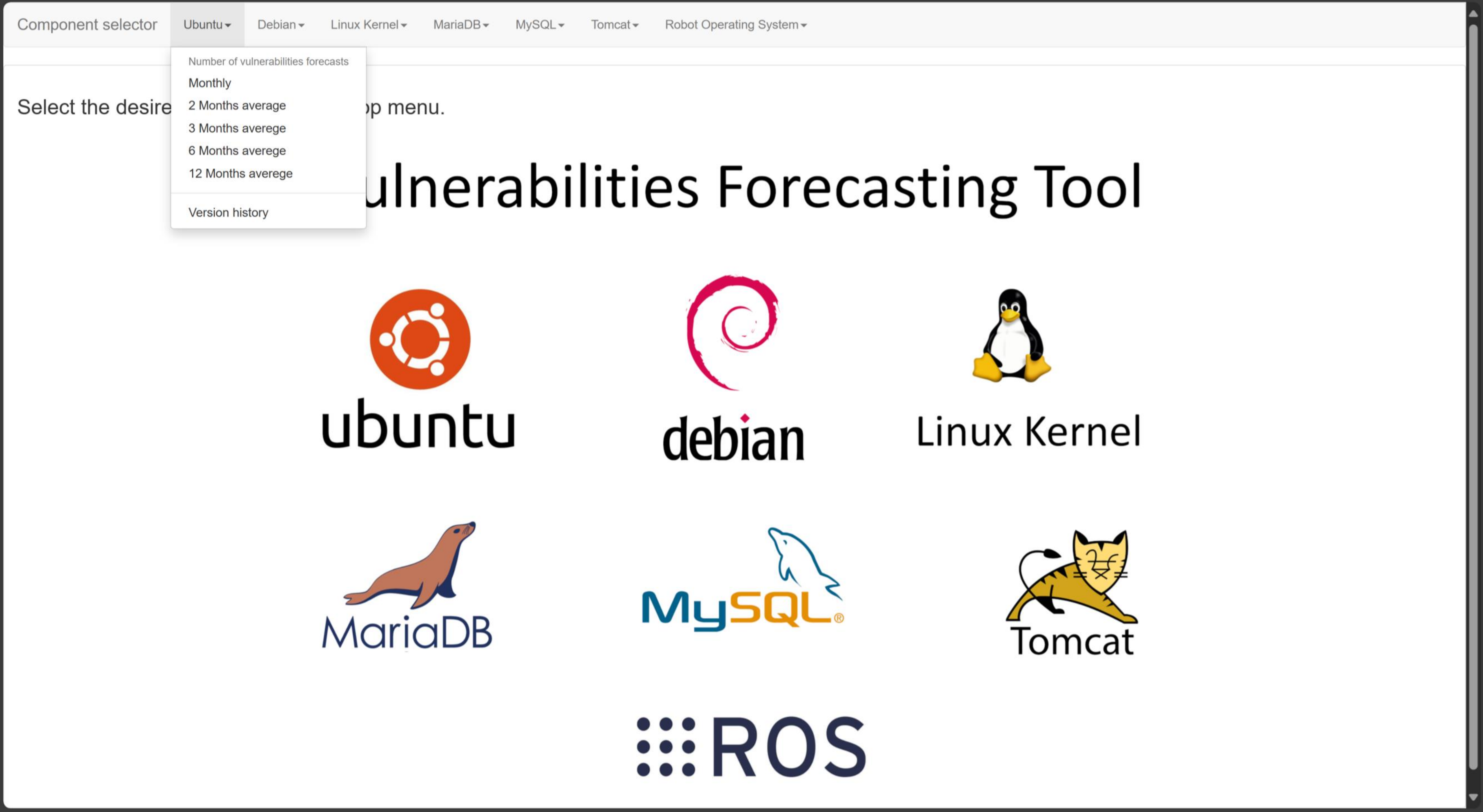
Provides an **estimation** of the number of **vulnerabilities** to be expected for the main **software components** used within complex ICT systems

- **Developing prediction models** for five different software products: Debian, Linux Kernel, Maria DB, MySQL, and Tomcat.
- **Adding prediction models** specifically designed for **one-year forecasts.**
- **Developing the Application Programming Interface**
- **Updating and improving the web interface**
- **Testing the VFT**



http://vf.bieco.org

Ref: D3.5 Update Report of the tools for vulnerability detection and forecasting



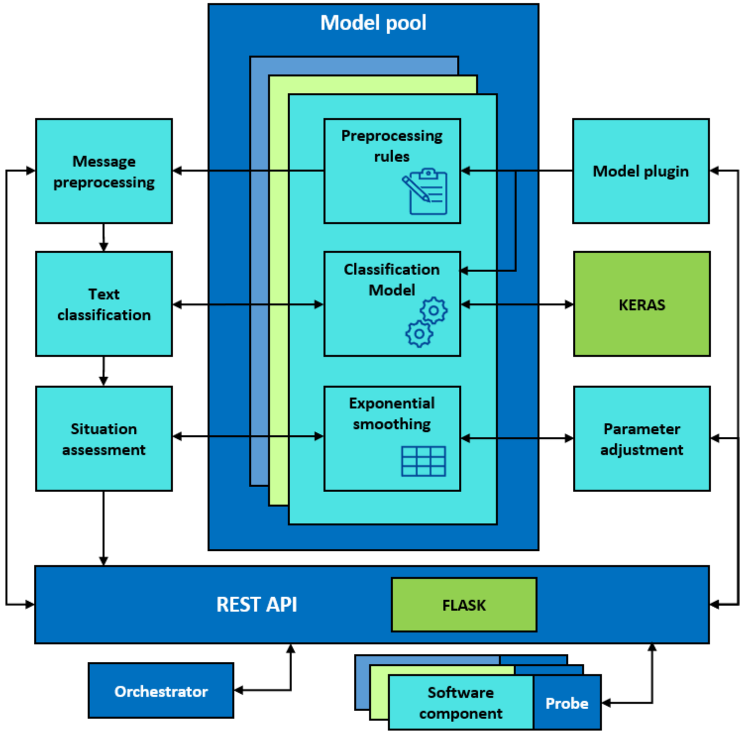
Select the desire op menu.

ulnerabilities Forecasting Tool

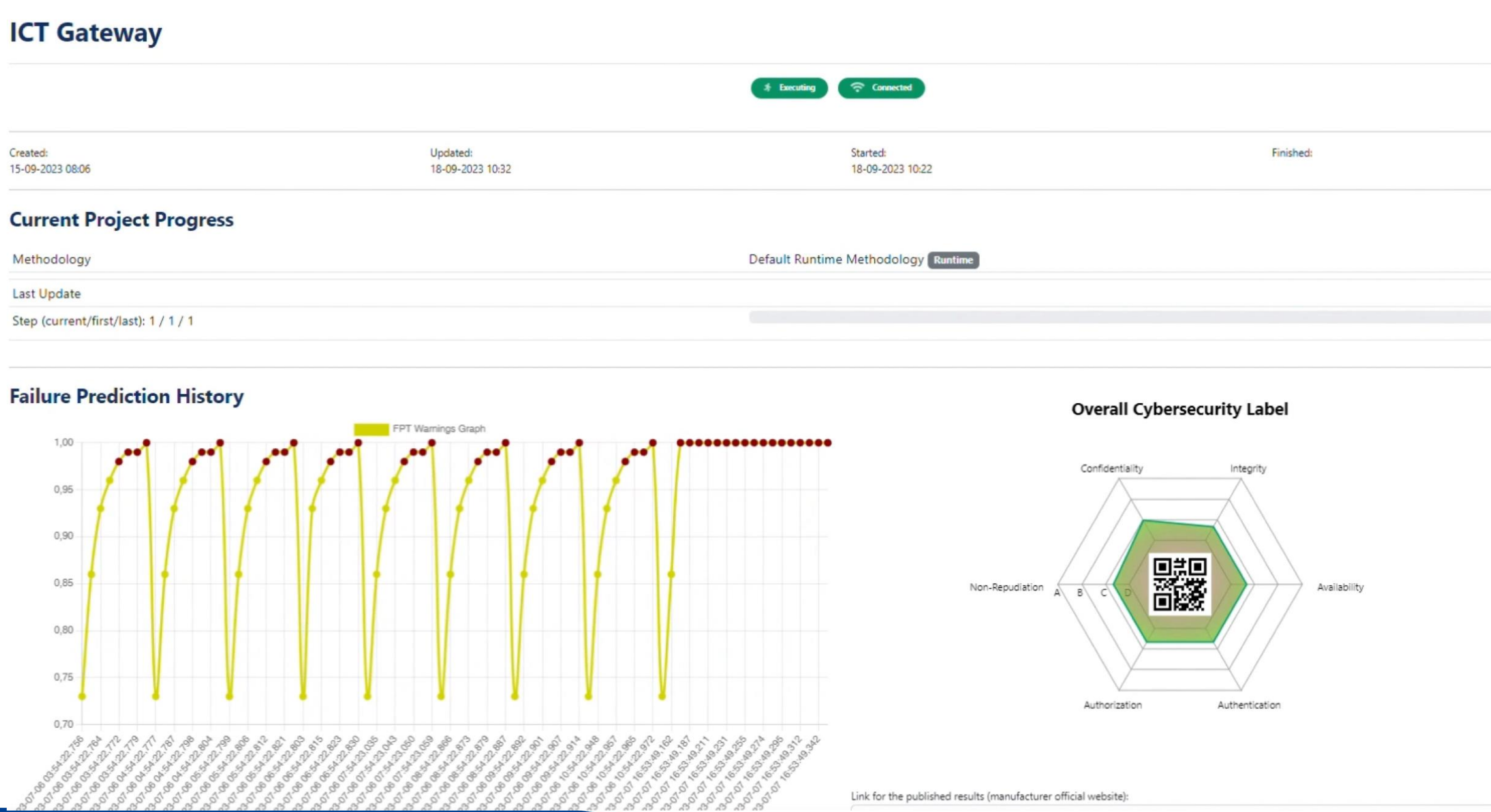
T4.2 Output (1/4)

BIECO
Building Trust in Ecosystems
and Ecosystem Components

- Failure Prediction Tool is a **real-time monitoring solution** designed to anticipate potential system failures.
- Versatile tool, supporting plugin models and parameter modifications, ensuring adaptability to various system requirements.
- FPT enhances system reliability by identifying potential failures in advance, ultimately reducing downtime and improving overall system performance.
- Enables a **constant watch** over system health.
- Incoming log messages are **classified** using a neural network model.
- **Alert** level calculation for each log message.
- Proactive Notifications followed by transmission of a specific **failure predictio**



TECHNICAL UNIVERSITY
OF CLUJ-NAPOCA
ROMANIA



ICT Gateway

Created:
15-09-2023 08:06

Updated:
18-09-2023 10:32

Started:
18-09-2023 10:22

Finished:

Current Project Progress

Methodology: Default Runtime Methodology Runtime

Last Update

Step (current/first/last): 1 / 1 / 1

Failure Prediction History

Overall Cybersecurity Label

Link for the published results (manufacturer official website):

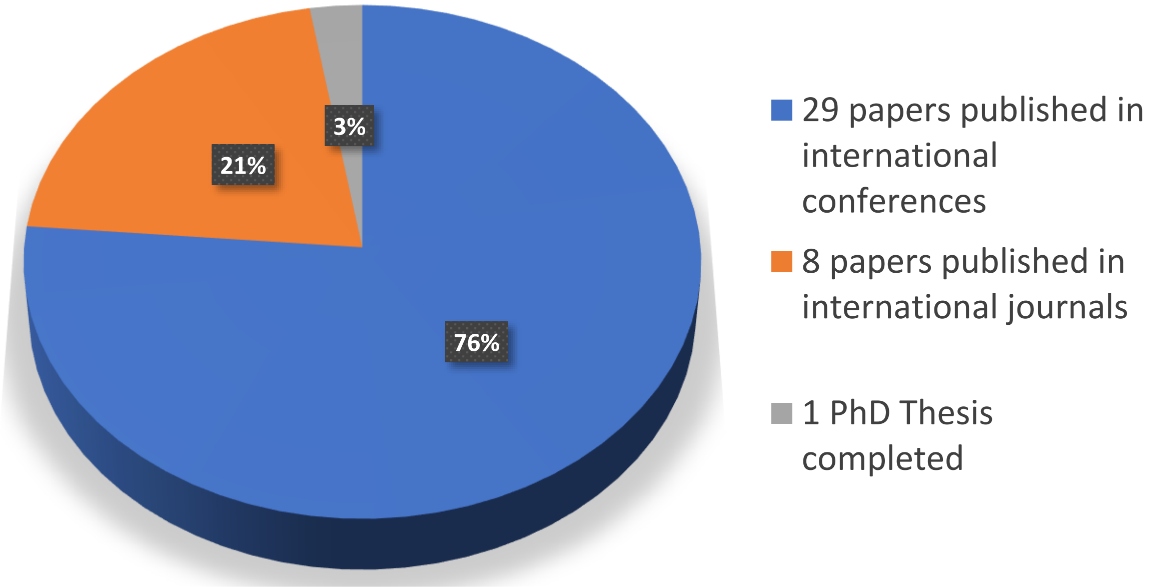
Publications

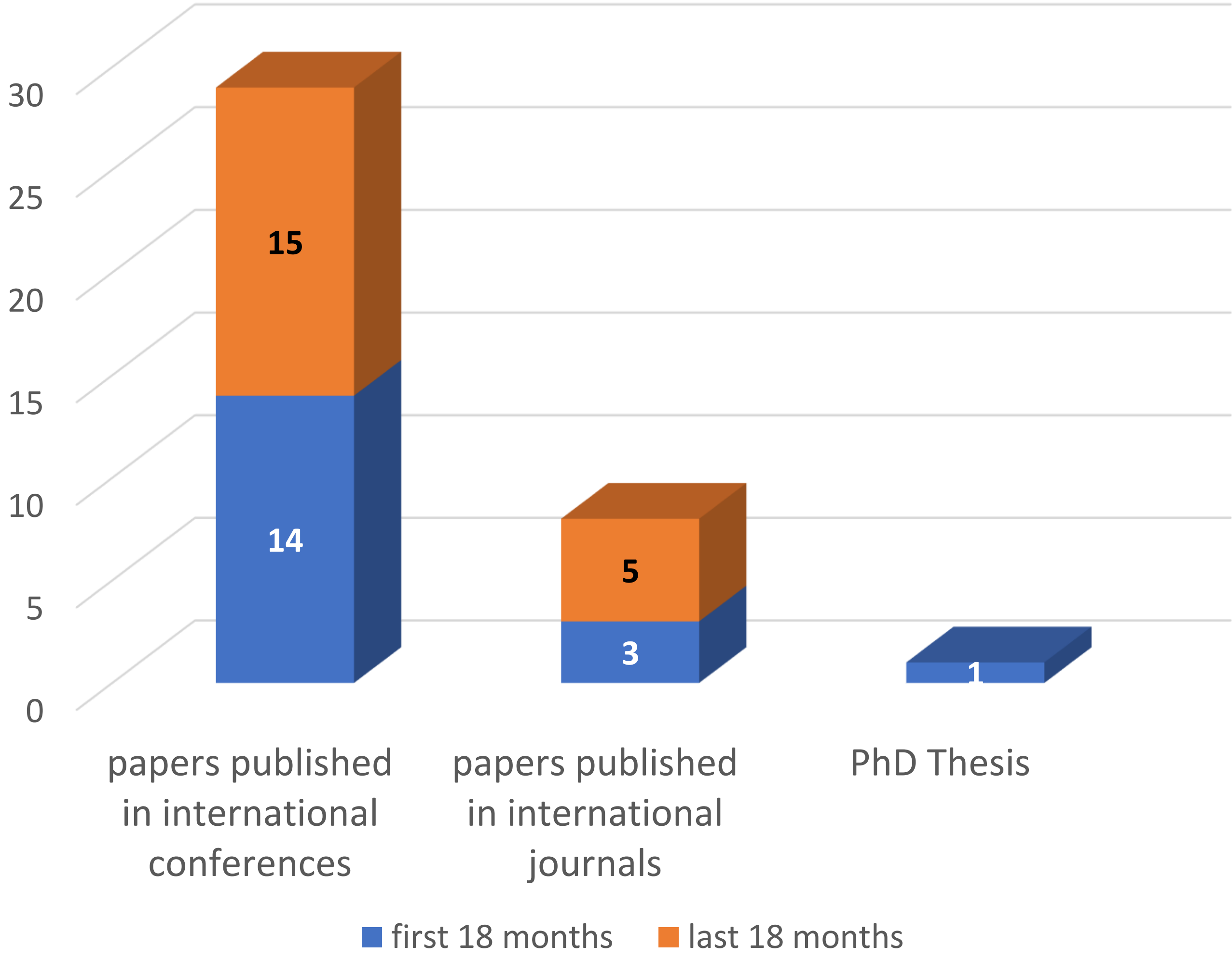
BIECO
Building Trust in Ecosystems
and Ecosystem Components

KPI

- Journal Publications (International, research) **>= 4**
- Publications and Presentations in Conferences (International, research) **>= 4**

38 scientific papers





Impact Factor

BIECO
Building Trust in Ecosystems
and Ecosystem Components

KPI

- Journal Publications (International, research) **>= 4**

Q	Title	Authors	Journal	Year	Impact Factor
Q1	On Autonomous Dynamic Software Ecosystems	Rafael Capilla,Emilia Cioroaica, Barbora Buhnova, and Jan Bosch	IEEE Transactions on Engineering Management, vol. 69, no. 6, pp. 3633-3647	2022	5.8
Q1	Integrating the manufacturer usage description standard in the modelling of cyber-physical systems	Sara Nieves Matheu García, Adrián Sánchez-Cabrera, Enrico Schiavone, Antonio Skarmeta	Computer Standards & Interfaces, Vol. 84, 103777	2023	5
Q2	LPWAN and Embedded Machine Learning as Enablers for the Next Generation of Wearable Devices	Ramon Sanchez-Iborra	Sensors, Vol. 21(15), 5218	2021	3.9
Q2	Defining the Behavior of IoT Devices Through the MUD Standard: Review, Challenges, and Research Directions	José Luis Hernández-Ramos, Sara Nieves Matheu-García, Angelo Feraudo, Gianmarco Baldini, Jorge Bernal-Bernabe, Poonam Yadav, Antonio Skarmeta Paolo Bellavista	IEEE Access, vol. 9, pp. 126265-126285	2021	3.9
Q2	A Formal Validation Approach for XACML 3.0 Access Control Policy.	Carmine Caserio, Francesca Lonetti, Eda Marchetti:	Sensors, Vol. 22(8), 2984	2022	3.9
Q2	Guide in Designing an Asynchronous Performance-Centric Framework for Heterogeneous Microservices in Time-Critical Cybersecurity Applications. The BIECO Use Case	Rudolf Erdei, Emil Marian Pașca,Daniela Delinschi, Iulia Bărăian,Oliviu Matei	Expert Systems (Wiley Open Research)	2023	3.3
Q3	The Challenges of Software Cybersecurity Certification	José Luis Hernández-Ramos, Sara Nieves Matheu-García, Antonio Skarmeta	IEEE Security & Privacy, vol. 19, no. 1, pp. 99-102	2021	1.9
Q3	Federated Cyberattack Detection for Internet of Things-Enabled Smart Cities	Matheu Garcia, Sara Nieves, Mármol, Enrique, Hernández Ramos, José Luis, Skarmeta, Antonio, & Baldini, Gianmarco	IEEE Computer, Vol. 55(12), pp. 65-73	2022	2.2
				TOTAL	**29.9**

https://wos-journal.info/

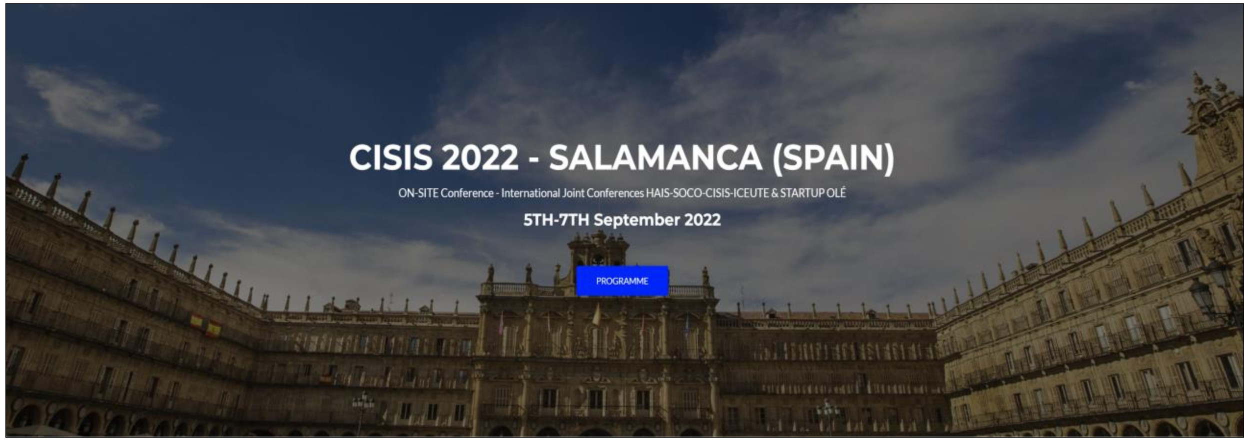
Workshops

KPI

- Workshop at EU level: **1**

We organized

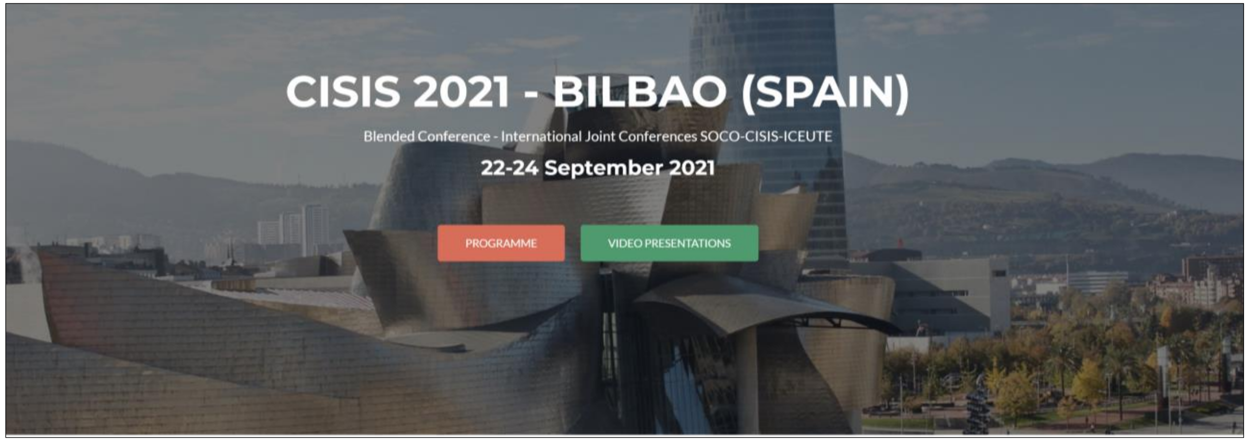
1. The special session ***Building Trust in Ecosystems and Ecosystem Components*** within the 14th International Conference on Computational Intelligence in Security for Information Systems (CISIS) 22 - 24 September 2021.
2. The special session ***Cybersecurity and Trusted Supply Chains of ICT*** within the 15th International Conference on Computational Intelligence in Security for Information Systems (CISIS) 5 – 7 September 2022.



CISIS 2022 - SALAMANCA (SPAIN)

ON-SITE Conference - International Joint Conferences HAIS-SOCO-CISIS-ICEUTE & STARTUP OLÉ

5TH-7TH September 2022



CISIS 2021 - BILBAO (SPAIN)

Blended Conference - International Joint Conferences SOCO-CISIS-ICEUTE

22-24 September 2021

Final Conference

KPI

- Final conference: **1**

The final conference ***Cybersecurity and Future Europe*** was organized on July 20, 2023, in a hybrid format in Lisbon, Portugal, and online. It actively involved 16 projects.

3IECO
Building Trust in Ecosystems
and Ecosystem Components

NetZeROCities

CYRENE

ROMÂNIA
SERVICIUL DE PROTECȚIE ȘI PAZĂ

SGS

CYMAROP

SMART FARM
COLAB
LABORATÓRIO COLABORATIVO
PARA A INOVAÇÃO DIGITAL
NA AGRICULTURA

NebulOuS

HELLENIC REPUBLIC
UNIVERSITY
OF MACEDONIA

SCALE

COSA
Collaborative Framework
for Smart Agriculture

TRIDENT
Guiding the guide

SDK4ED
Software Development ToolKit for Energy Optimization
and Technical Debt Elimination

ICT-AGRI-FOOD ERA-NET
MUSHNOMICS

REPLACER

THE EUROPEAN
DIGITAL INNOVATION HUB
IN TRANSILVANIA

food for
sustainability

Clustering events

BIECO
Building Trust in Ecosystems
and Ecosystem Components

- ➢ Participation in the ***Future Proofing and Certifying Supply Chains Clustering Workshop***, December 13, 2021.
- ➢ Participation in the virtual roundtable ***The need for IoT Security Standardization & Certification***, April 8, 2022.
- ➢ We established **connections with 14 EU projects**.

Clustering Workshop
Co-organized by ASSURED CYRENE
FUTURE PROOFING AND CERTIFYING SUPPLY CHAINS
13 December 2021 | 09:00 - 16:30 CET

European Commission
enisa THE EU CYBERSECURITY AGENCY
ETSI
ECSO
GLOBALPLATFORM
Alliance for Internet of Things Innovation
EY
IOT DAY
VIRTUAL ROUNDTABLE
THE NEED FOR IOT SECURITY STANDARDIZATION & CERTIFICATION
8. APRIL 2022
CONCORDIA
ASSURED
IoT Crawler
CYRENE
FISHY
BIECO
EU-IoT

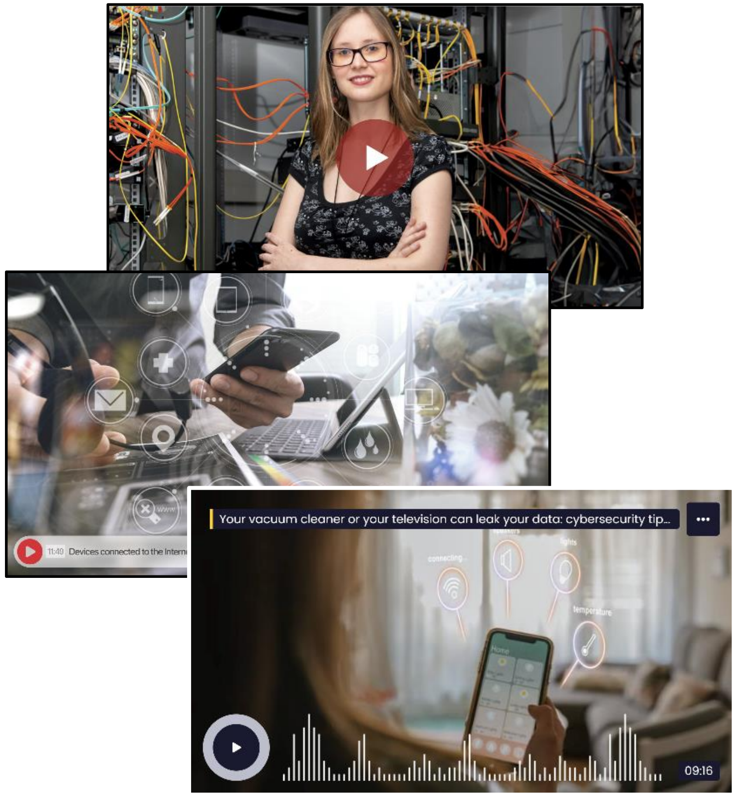
Dissemination outside the research community

BIECO
Building Trust in Ecosystems
and Ecosystem Components

- Participation in the ***Barcelona Cybersecurity Congress***, 31 January - 2 February 2023, within the European Research Innovation for Cybersecurity (ERICYB) cluster, together with the following 6 related projects: ASSURE, FiSHy, CYRENE, IoTAC, Sanctus, and SIFIS-Home.
- 14 ***podcasts and interviews*** focusing on various aspects of IoT cybersecurity, including discussions on cybersecurity evaluation methodologies developed in BIECO
- 2 ***press articles***.

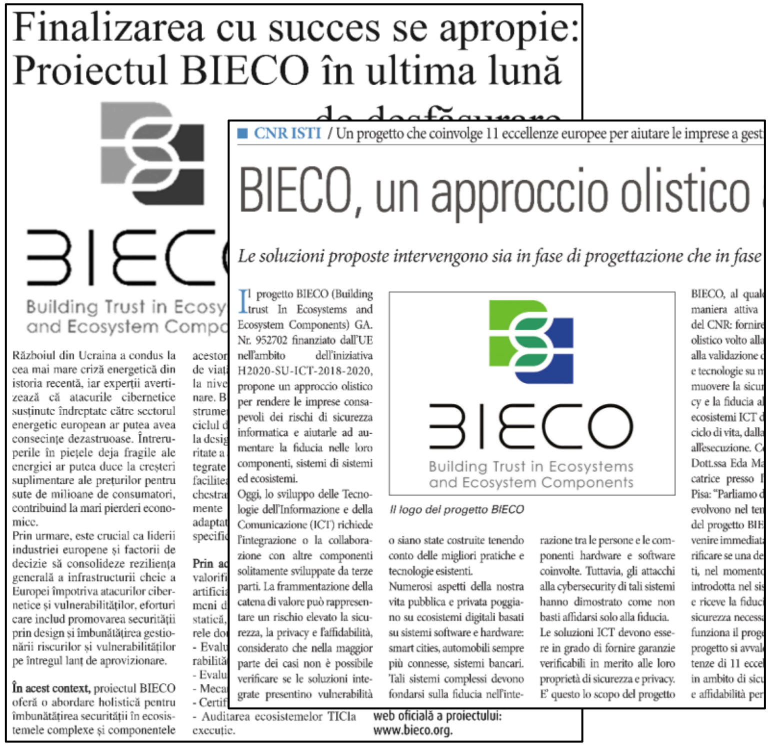
ERICyb
European Research Innovation for Cybersecurity
ASSURE
CYRENE
BIECO
SANCUS
FiSHY
IoT AC
SIFIS-Home
BARCELONA CYBERSECURITY CONGRESS
JAN 31 - FEB 2, 2023
Visit us at stand C350

The projects have received funding from the European Union's Horizon 2020 research and innovation programme under the call SU-ICT-02-2020.


11:49 Devices connected to the Intern

Your vacuum cleaner or your television can leak your data: cybersecurity tip...

09:16



Finalizarea cu succes se apropie: Proiectul BIECO în ultima lună de desfăşurare

Building Trust in Ecosystems
and Ecosystem Components

Războiul din Ucraina a condus la cea mai mare criză energetică din istoria recentă, iar experții avertizează că atacurile cibernetice susținute îndreptate către sectorul energetic european ar putea avea consecințe dezastruoase. Întreruperile în piețele deja fragile ale energiei ar putea duce la creșteri suplimentare ale prețurilor pentru sute de milioane de consumatori, contribuind la mari pierderi economice.

Prin urmare, este crucial ca liderii industriei europene și factorii de decizie să consolideze reziliența generală a infrastructurii cheie a Europei împotriva atacurilor cibernetice și vulnerabilităților, eforturi care includ promovarea securității prin design și îmbunătățirea gestionării riscurilor și vulnerabilităților pe întregul lanț de aprovizionare.

În acest context, proiectul BIECO oferă o abordare holistică pentru îmbunătățirea securității în ecosistemele complexe și componentele

acestor
de viaț
la nive
nare. B
strume
ciclul d
la desig
ritate a
tegrate
facilitea
chestra
mente
adaptat
specific

Prin ac
valorifi
artificia
meni d
statică,
rele do
- Evalu
rabilită
- Evalu
- Meca
- Certif
- Auditarea ecosistemelor TICla execuție.

web oficială a proiectului: www.bieco.org.

CNR ISTI / Un progetto che coinvolge 11 eccellenze europee per aiutare le imprese a gest

BIECO, un approccio olistico

Le soluzioni proposte intervengono sia in fase di progettazione che in fase

Il progetto BIECO (Building trust In Ecosystems and Ecosystem Components) GA. Nr. 952702 finanziato dall'UE nell'ambito dell'iniziativa H2020-SU-ICT-2018-2020, propone un approccio olistico per rendere le imprese consapevoli dei rischi di sicurezza informatica e aiutarle ad aumentare la fiducia nelle loro componenti, sistemi di sistemi ed ecosistemi.

Oggi, lo sviluppo delle Tecnologie dell'Informazione e della Comunicazione (ICT) richiede l'integrazione o la collaborazione con altre componenti solitamente sviluppate da terze parti. La frammentazione della catena di valore può rappresentare un rischio elevato la sicurezza, la privacy e l'affidabilità, considerato che nella maggior parte dei casi non è possibile verificare se le soluzioni integrate presentino vulnerabilità o siano state costruite tenendo conto delle migliori pratiche e tecnologie esistenti.

Numerosi aspetti della nostra vita pubblica e privata poggiano su ecosistemi digitali basati su sistemi software e hardware: smart cities, automobili sempre più connesse, sistemi bancari. Tali sistemi complessi devono fondarsi sulla fiducia nell'interazione tra le persone e le componenti hardware e software coinvolte. Tuttavia, gli attacchi alla cybersecurity di tali sistemi hanno dimostrato come non basti affidarsi solo alla fiducia.

Le soluzioni ICT devono essere in grado di fornire garanzie verificabili in merito alle loro proprietà di sicurezza e privacy. E' questo lo scopo del progetto

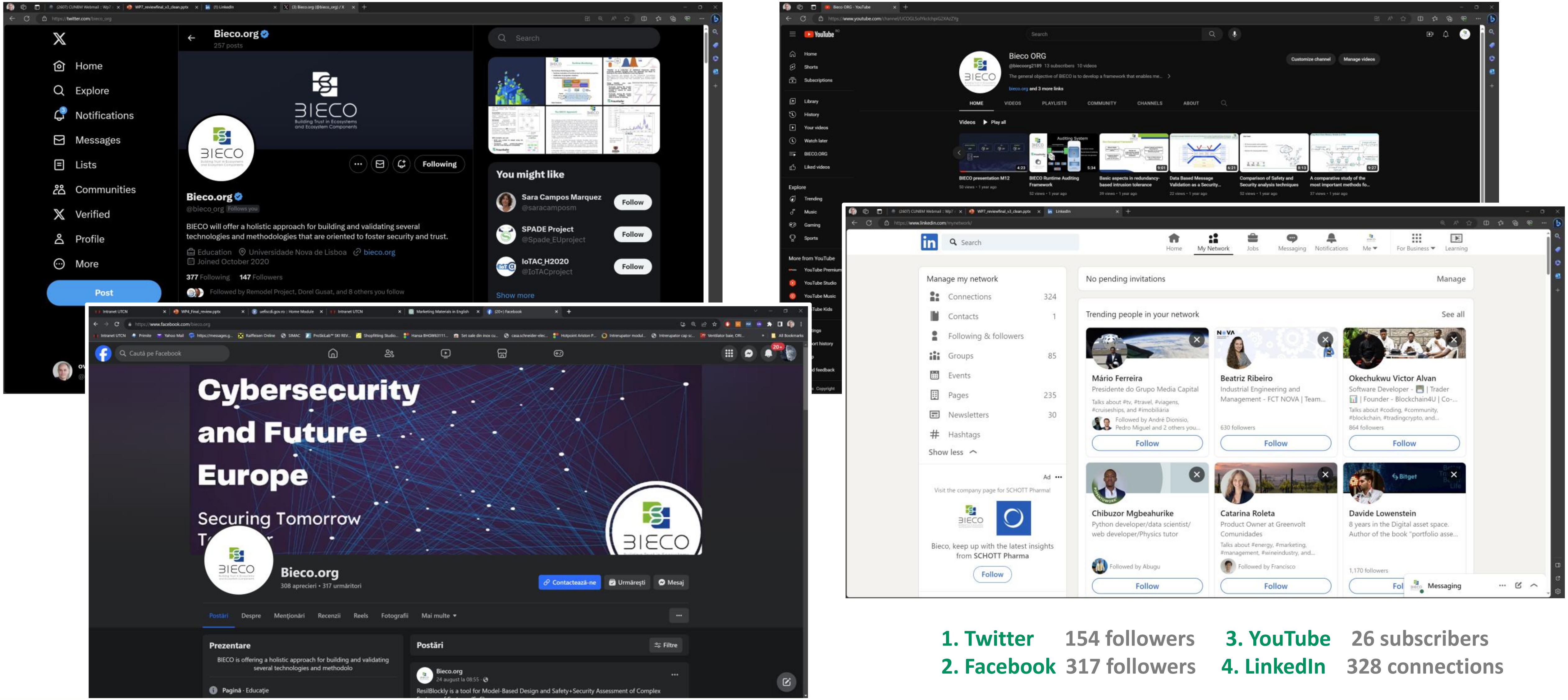
BIECO, al qual
maniera attiva
del CNR: fornir
olistico volto alla
alla validazione d
e tecnologie su m
muovere la sicur
cy e la fiducia al
ecosistemi ICT d
ciclo di vita, dalla
all'esecuzione. C
Dott.ssa Eda Ma
catrice presso I
Pisa: "Parliamo d
evolvono nel ten
del progetto BIE
venire immediata
rificare se una de
ti, nel moment
introdotta nel sis
e riceve la fiduci
sicurezza necess
funziona il prog
progetto si avval
tenze di 11 eccel
in ambito di sicu
e affidabilità per

BIECO
Building Trust in Ecosystems
and Ecosystem Components

Il logo del progetto BIECO

Social Networks

BIECO
Building Trust in Ecosystems
and Ecosystem Components



Home
Explore
Notifications
Messages
Lists
Communities
Verified
Profile
More
Post

Bieco.org
257 posts

Following

Bieco.org
@bieco_org Follows you

BIECO will offer a holistic approach for building and validating several technologies and methodologies that are oriented to foster security and trust.

Education · Universidade Nova de Lisboa · bieco.org
Joined October 2020

377 Following 147 Followers

Followed by Remodel Project, Dorel Gusat, and 8 others you follow

Search

You might like

Sara Campos Marquez @saracamposm Follow
SPADE Project @Spade_EUproject Follow
IoTAC_H2020 @IoTACproject Follow

Show more

Caută pe Facebook

Cybersecurity and Future Europe

Securing Tomorrow

Bieco.org
308 aprecieri • 317 urmăritori

Contactează-ne · Urmărești · Mesaj

Postări · Despre · Menționări · Recenzii · Reels · Fotografii · Mai multe

Prezentare
BIECO is offering a holistic approach for building and validating several technologies and methodolo

Pagină · Educație

Postări · Filtre

Bieco.org
24 august la 08:55
ResilBlockly is a tool for Model-Based Design and Safety+Security Assessment of Complex

Home · Shorts · Subscriptions · Library · History · Your videos · Watch later · BIECO.ORG · Liked videos
Explore · Trending · Music · Gaming · Sports
More from YouTube · YouTube Premium · YouTube Studio · YouTube Music

Bieco ORG
@biecoorg2189 13 subscribers 10 videos
The general objective of BIECO is to develop a framework that enables me...
bieco.org and 3 more links

Customize channel · Manage videos

HOME · VIDEOS · PLAYLISTS · COMMUNITY · CHANNELS · ABOUT

Videos ▶ Play all

BIECO presentation M12 · 50 views • 1 year ago
BIECO Runtime Auditing Framework · 52 views • 1 year ago
Basic aspects in redundancy-based intrusion tolerance · 39 views • 1 year ago
Data Based Message Validation as a Security... · 22 views • 1 year ago
Comparison of Safety and Security analysis techniques · 52 views • 1 year ago
A comparative study of the most important methods fo... · 37 views • 1 year ago

Search
Home · My Network · Jobs · Messaging · Notifications · Me · For Business · Learning

Manage my network

Connections	324
Contacts	1
Following & followers	
Groups	85
Events	
Pages	235
Newsletters	30
Hashtags	

Show less

No pending invitations · Manage

Trending people in your network · See all

Mário Ferreira
Presidente do Grupo Media Capital
Follow

Beatriz Ribeiro
Industrial Engineering and Management - FCT NOVA | Team...
630 followers
Follow

Okechukwu Victor Alvan
Software Developer - | Trader | Founder - Blockchain4U | Co-...
864 followers
Follow

Chibuzor Mgbeahurike
Python developer/data scientist/ web developer/Physics tutor
Followed by Abugu
Follow

Catarina Roleta
Product Owner at Greenvolt Comunidades
Followed by Francisco
Follow

Davide Lowenstein
8 years in the Digital asset space. Author of the book "portfolio asse...
1,170 followers

Ad
Visit the company page for SCHOTT Pharma
Bieco, keep up with the latest insights from SCHOTT Pharma
Follow

Messaging

1. Twitter	154 followers	3. YouTube	26 subscribers
2. Facebook	317 followers	4. LinkedIn	328 connections

Newsletters

BIECO
Building Trust in Ecosystems and Ecosystem Components

- **3** newsletters produced
- **9** newsletters generated from the web site
- **1** final newsletter will be released after the review meeting

This project has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No. 952702

BIECO
Building Trust in Ecosystems and Ecosystem Components

No. 1
October 2021

Newsletter 1 – October 2021

of the BIECO project.
CO project in September 2020 with the aim to les measurable, risk-based trust while developing, lex interconnected ICT systems. We aim to achieve and trust aspects of ecosystem participants (ICT ents and actors) within the supply chain. The et of tools and methodologies, will address the ility management, resilience, auditing of complex strategies and security certification harmonization. achieved through the application of the tools and ses (energy, finance, and industry), which include

Since the beginning of our project, we have worked on detailed descriptions of relevant scenarios and the cybersecurity risks and threats encountered in a software supply chain, along with a list of expected improvements, detailed definition and specification of the use cases, and the design of the overall system architecture based on smart production components that is able to support the identification of risks and threats in the software supply chain according to functional requirements.

I hope you enjoy reading our newsletter and invite you to check our website regularly, follow us on social media or contact us directly for more information.

Sincerely yours,
Prof. dr. Jose Barata

Newsletter 1 – October 2021

oject description

s concept is to deliver a st and security within ICT mplex ecosystems neous technologies, -users, software or anizations) and rate or exchange data information

BIECO will offer a holistic approach for building and validating several technologies and methodologies that are specifically oriented to foster security and trust within ICT ecosystems. To better illustrate how BIECO intends to address these challenges along the entire lifecycle of the ICT supply chain, the above figure shows broadly the interaction flow between the different phases of the lifecycle, as well as the core functionalities involved.

work iteratively in order to d improvement of ICT supply which the cybersecurity s emerging every day. tecture will thus contain a set ologies capable of ultimately of systems and system l ecosystems.
From design to runtime, vulnerabilities and failures are detected, evaluated and mitigated together with prompt reactions that ensure the ultimate trustworthy execution of systems and system components. In order to open the path towards future development and for enabling the possibility to keep up to agile technological progress supported by runtime updates of systems (including safety-critical systems), we further on design the BIECO architecture with expandability in mind.
One possibility in this direction will be that based on detected deviations, runtime updates of systems can be accommodated through a natural extension of the BIECO framework, including the feedback of information to the design time for continuous improvement..

This project has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No. 952702

BIECO
Building Trust in Ecosystems and Ecosystem Components

No. 2
September 2022

Newsletter 2 – September 2022

r second newsletter dedicated to the

CO project made great progresses in s, milestones, and key outcomes, framework that enables measurable, risk-based trust while developing, deploying, and operating complex interconnected ICT systems.

In this newsletter, we present the project status, highlight our important achievements within all our work packages, and the list of publications.

I hope you will enjoy reading our newsletter and invite you to check our website regularly, follow us on social media or contact us directly for more information.

Sincerely yours,
Prof. dr. Jose Barata

Newsletter 2 – September 2022

ns

AS A SECURITY SOFTWARE

on Computational Intelligence in tional Conference on European Advances in Intelligent Systems

schi, Laura Andreica

ST IMPORTANT T SYSTEMS

n Computational Intelligence in Security for Information Systems and 12th International Conference on European Transnational Educational,CISIS - ICEUTE 2021, Advances in Intelligent Systems and Computing, vol 1400, pp 224-233, 2021
Authors: Ovidiu Cosma, Mara Hajdu-Macelaru, Petrica Pop-Sitar, Cosmin Sabo, Ioana Zelina

COMPARISON OF SAFETY AND SECURITY ANALYSIS TECHNIQUES

Publication info : 14th International Conference on Computational Intelligence in Security for Information Systems and 12th International Conference on European Transnational Educational, CISIS - ICEUTE 2021 , Advances in Intelligent Systems and Computing, vol 1400, pp 234–242, 2021
Authors: Emilia Cioroaica, Smruti Ranjan Kar, and Ioannis Sorokos

ON AUTONOMOUS DYNAMIC SOFTWARE ECOSYSTEMS

Publication info : IEEE Transactions on Engineering Management, pp 1-15, 2021
Authors: Rafael Capilla ,Emilia Cioroaica, Barbora Buhnova, Jan Bosch, Göteborg Sweden

This project has received funding from the European Union's Horizon 2020 research and innovation program under Grant Agreement No. 952702

BIECO
Building Trust in Ecosystems and Ecosystem Components

No. 3
July 2023

Newsletter 3 – July 2023

BIECO project, exclusively dedicated owerful tools.

n of over 15 distinct tools that comprehensively span the software lifecycle, ranging from initial design to real-time operation. Notably, the majority of these tools have been integrated into a unified platform, that facilitates their interoperability and orchestration in easy deployable toolchains tailored to meet specific business needs.

We trust that the content presented in this newsletter will captivate your interest and offer valuable insights. For more comprehensive information, we encourage you to visit our project website, stay connected with us through social media channels, or contact us directly.

Thank you for your continued support and enthusiasm.

Warm regards,
Prof. dr. Jose Barata

Newsletter 3 – July 2023

CO detects vulnerabilities within ML techniques.

ers to corrupt a system is the t is vital to execute a suitable y. The tool allows companies to ble security breaches within the tomatic way.

g Tool

The Vulnerability Exploitability Forecasting Tool provides the probability of a known published vulnerability to be exploited in a time window.

Once a known vulnerability is detected within the source code, it is necessary to focus the efforts to mitigate its possible attacks. From BIECO, we are conscious that experts needs to prioritize possible attacks for a more effective results. Thus, the exploitability forecasting tool offers an assessment of a given vulnerability, by indicating if it can be exploited in the next 3, 6 or 12 months from the date of publication.

Vulnerability Propagation Tool

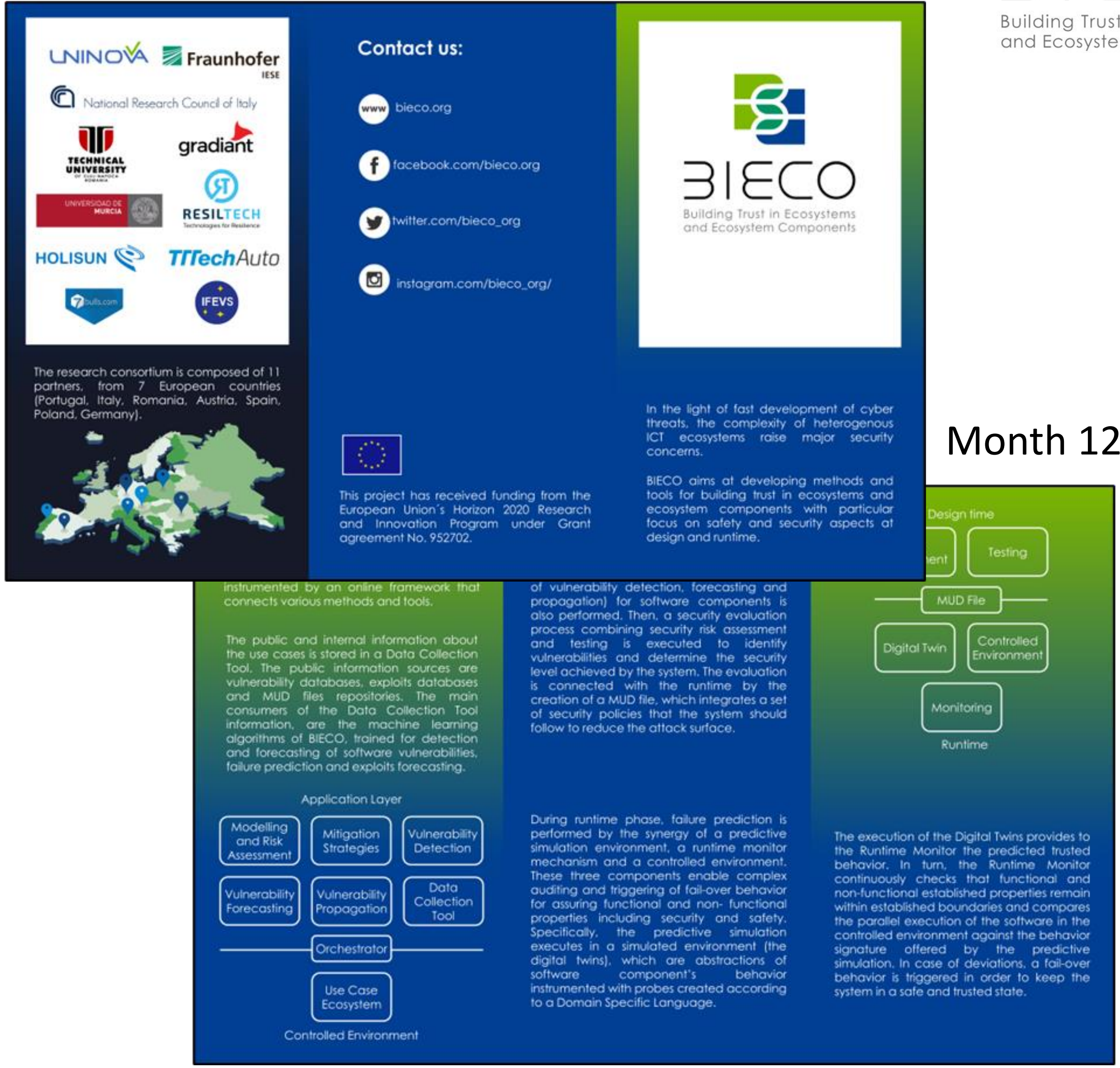
The main goal of the Vulnerability Propagation Tool is to find and indicate the components or elements a single vulnerability can affect and, therefore, its path within the source code.

Sometimes, the most obvious way to reach a vulnerability is by knowing its location. But vulnerabilities can propagate through the source code, offering open doors to cyber attackers to exploit them. Calculating the path affected by a vulnerability helps the cyber security expert to prioritize its mitigation not only directly, but their possible alternative access in the source code.

Leaflets

BIECO

Building Trust in Ecosystems and Ecosystem Components



Month 12

Contact us:

bieco.org

facebook.com/bieco.org

twitter.com/bieco_org

instagram.com/bieco_org/

The research consortium is composed of 11 partners, from 7 European countries (Portugal, Italy, Romania, Austria, Spain, Poland, Germany).

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

BIECO

Building Trust in Ecosystems and Ecosystem Components

In the light of fast development of cyber threats, the complexity of heterogenous ICT ecosystems raise major security concerns.

BIECO aims at developing methods and tools for building trust in ecosystems and ecosystem components with particular focus on safety and security aspects at design and runtime.

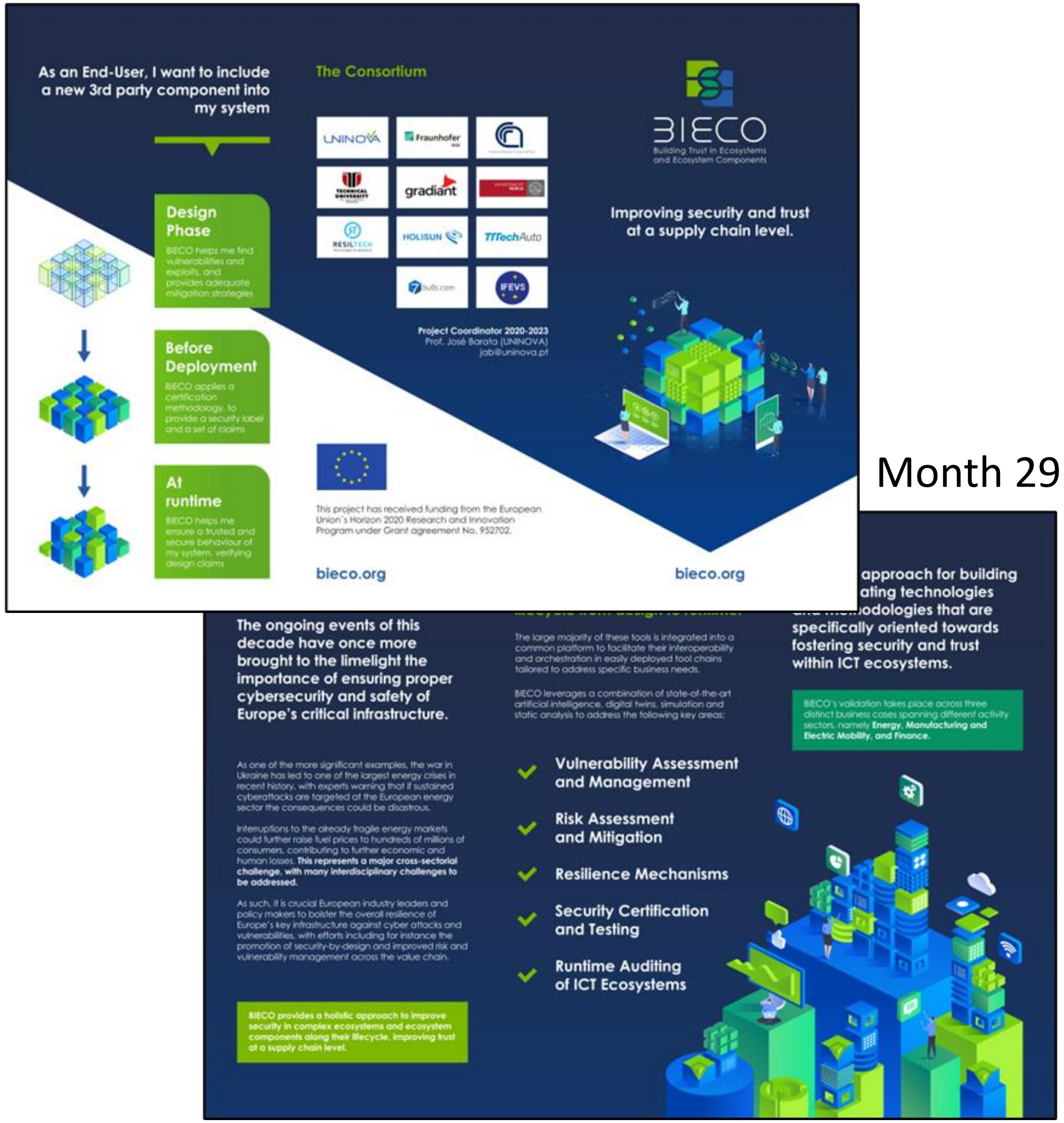
instrumented by an online framework that connects various methods and tools.

The public and internal information about the use cases is stored in a Data Collection Tool. The public information sources are vulnerability databases, exploits databases and MUD files repositories. The main consumers of the Data Collection Tool information, are the machine learning algorithms of BIECO, trained for detection and forecasting of software vulnerabilities, failure prediction and exploits forecasting.

of vulnerability detection, forecasting and propagation) for software components is also performed. Then, a security evaluation process combining security risk assessment and testing is executed to identify vulnerabilities and determine the security level achieved by the system. The evaluation is connected with the runtime by the creation of a MUD file, which integrates a set of security policies that the system should follow to reduce the attack surface.

During runtime phase, failure prediction is performed by the synergy of a predictive simulation environment, a runtime monitor mechanism and a controlled environment. These three components enable complex auditing and triggering of fail-over behavior for assuring functional and non- functional properties including security and safety. Specifically, the predictive simulation executes in a simulated environment (the digital twins), which are abstractions of software component's behavior instrumented with probes created according to a Domain Specific Language.

The execution of the Digital Twins provides to the Runtime Monitor the predicted trusted behavior. In turn, the Runtime Monitor continuously checks that functional and non-functional established properties remain within established boundaries and compares the parallel execution of the software in the controlled environment against the behavior signature offered by the predictive simulation. In case of deviations, a fail-over behavior is triggered in order to keep the system in a safe and trusted state.



Month 29

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

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

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.

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

approach for building ating technologies odologies 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.**

Brochure and Best Practice Handbook

BIECO
Building Trust in Ecosystems
and Ecosystem Components

22 pages inside

BIECO
Building Trust in Ecosystems
and Ecosystem Components

Improving security and trust at a supply chain level.

bieco.org

BIECO
Building Trust in Ecosystems
and Ecosystem Components

have once more brought to
nsuring proper cybersecurity
tructure. As one of the more
raine has led to one of the
ry, with experts warning that
ted at the European energy
e disastrous. Interruptions to
could further raise fuel prices
ners, contributing to further
vertheless, this represents a
with many interdisciplinary

ndustry leaders and policy
resilience of Europe's key
cks and vulnerabilities, with
e promotion of security-by-
erability management across

olistic approach to improve
nd ecosystem components
at a supply chain level.

Before deployment, CO applies a certification ethodology to provide me h a BIECO security label and a set of claims

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

cosystems
mponents

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

14 pages inside

BIECO
Building Trust in Ecosystems
and Ecosystem Components

Best Practice Handbook

bieco.org

BIECO
Building Trust in Ecosystems
and Ecosystem Components

essential security best
rate. These practices are

verification of claimed

y and completeness of
is prevents unauthorized

o honoring contractual
ransaction parties from
ansaction.

nauthorized individuals,
accessing or disclosing
acy, the two terms have
y safeguards data from

mputing systems used to
on, the security controls
ommunication channels
ning correctly.

at there are security
ess levels or user/client
privileges related to system resources, including files, services, computer programs, data, and application features.

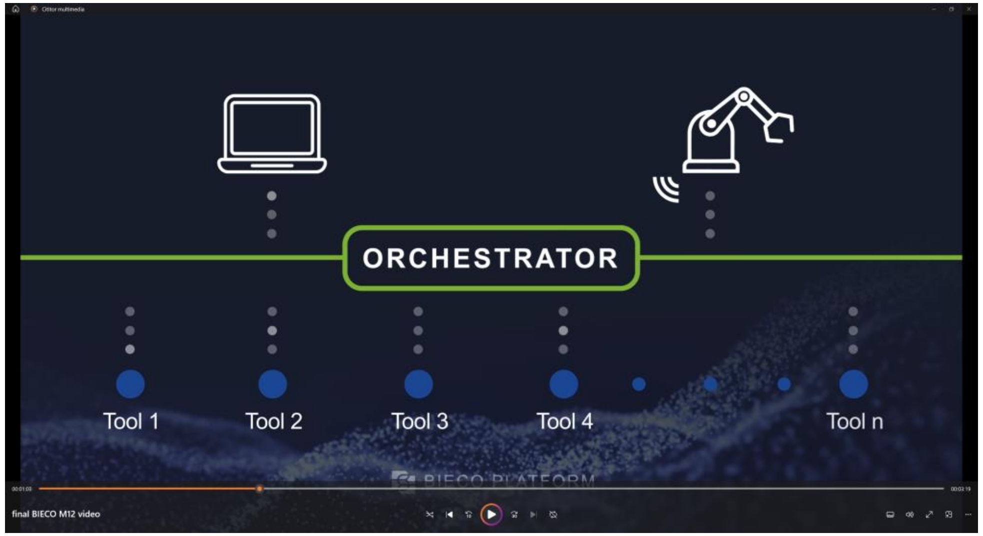
Ecosystems
Components

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

Presentation Videos

BIECO
Building Trust in Ecosystems
and Ecosystem Components

M 12

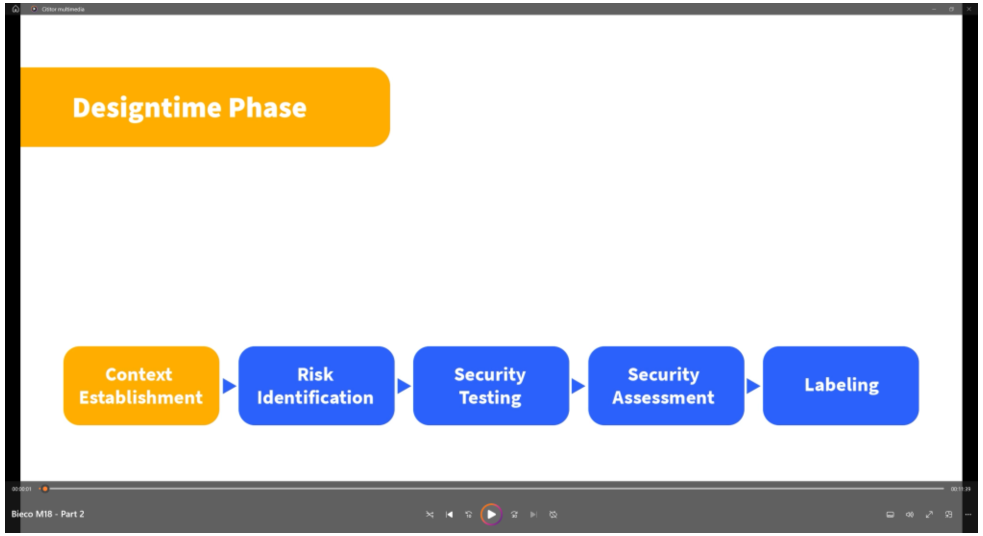


final BIECO M12 video

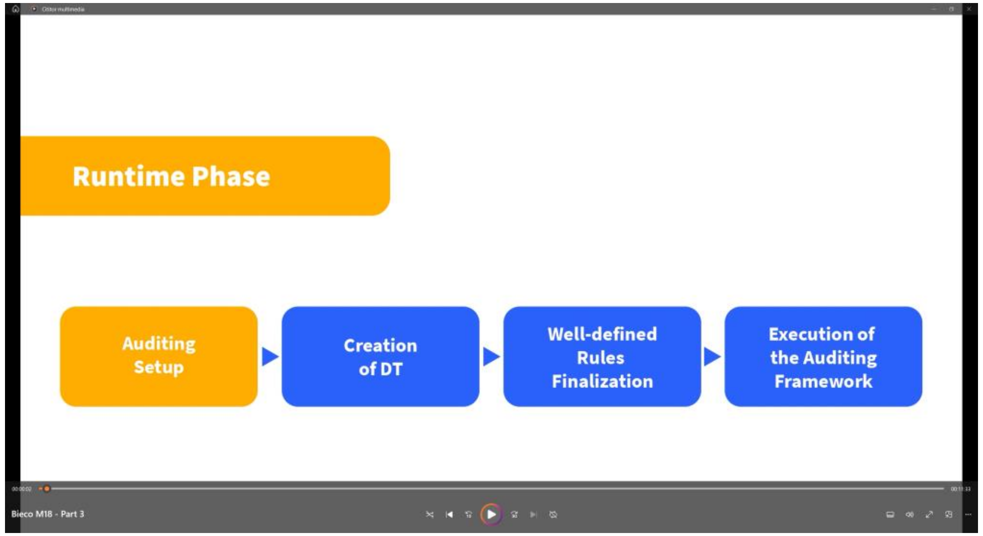
Bieco M18 - Part 1

M 18

M 18



Bieco M18 - Part 2


Runtime Phase
Auditing Setup
Creation of DT
Well-defined Rules Finalization
Execution of the Auditing Framework

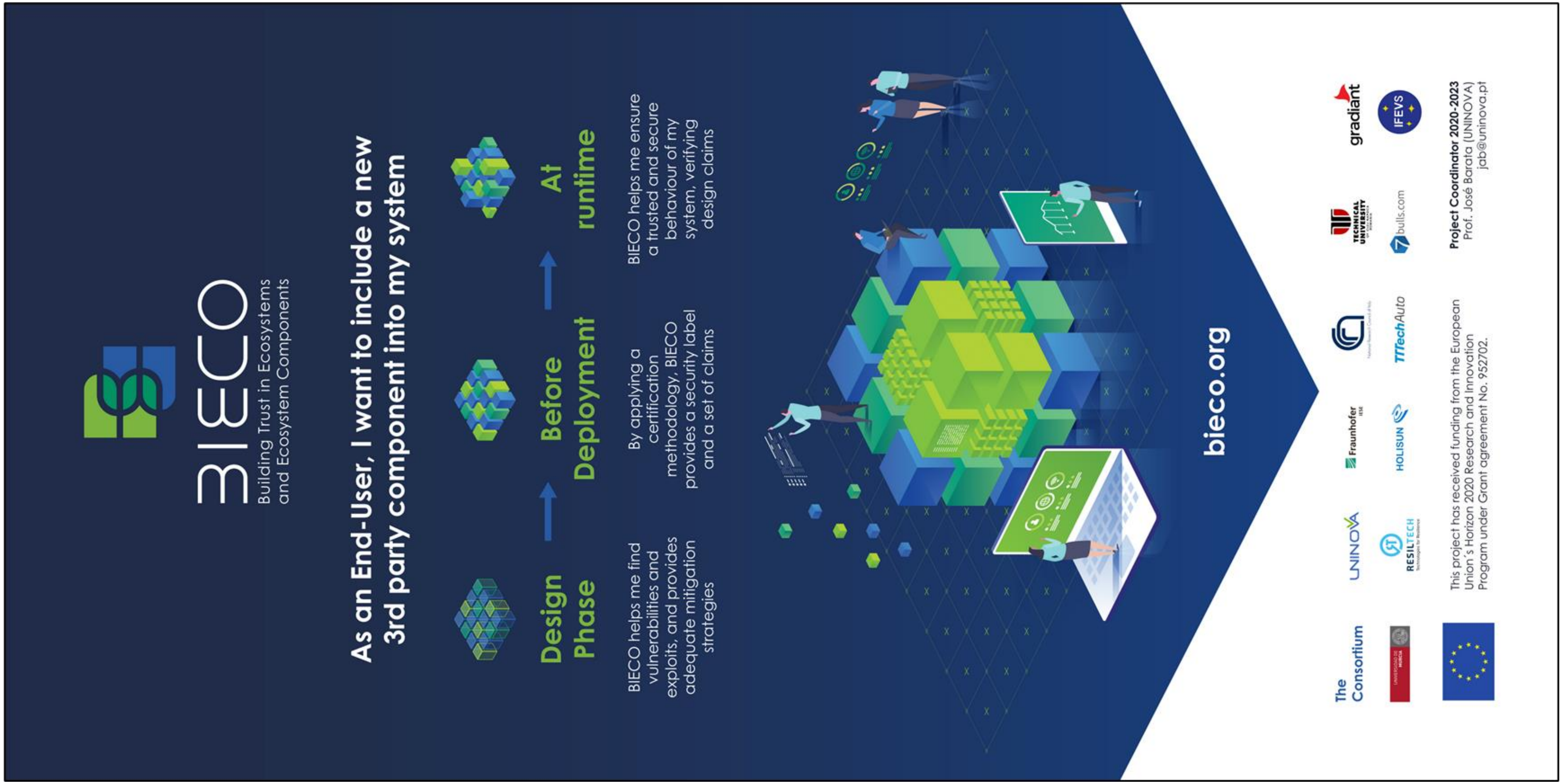
Bieco M18 - Part 3

M 18

Pen and Poster

BIECO
Building Trust in Ecosystems
and Ecosystem Components

Barcelona Cybersecurity Congress



BIECO
Building Trust in Ecosystems
and Ecosystem Components

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

Design Phase → Before Deployment → At runtime

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

By applying a certification methodology, BIECO provides a security label and a set of claims

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

bieco.org

The Consortium

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

Building Trust in Ecosystems
and Ecosystem Components

Thank You For Your Attention!

UNINOVA

Fraunhofer IESE

TECHNICAL UNIVERSITY OF CLUJ-NAPOCA ROMANIA

gradiant

UNIVERSIDAD DE MURCIA

RESILTECH Technologies for Resilience

HOLISUN

TTTechAuto

7bulls.com

I-FEVS