TECHNICAL UNIVERSITY OF CLUJ-NAPOCA ROMANIA

BIECO

Building Trust in Ecosystems and Ecosystem Components

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

PRO INVENT 2021

21th October 2021

H2020 BIECO

OUTLINE

BIECO
Building Trust in Ecosystems and Ecosystem Components

1. Context
2. BIECO Consortium
3. UTCN Research Team
4. UTCN Involvement
5. Video Presentation
6. Design Phase Architecture
7. Runtime architecture
8. UTCN Results
9. Current and Future Activities

TECHNICAL UNIVERSITY OF CLUJ-NAPOCA ROMANIA

PRO INVENT 2021

BIECO
Building Trust in Ecosystems and Ecosystem Components

Context

Modern ICT ecosystems are complex and heterogeneous, which makes their security a major concern, given the speed with which cyber threats are evolving.

BIECO is a research project, that aims to build and validate methodologies and technologies tailored to foster security and trust within ICT ecosystems, across their entire lifecycle, from design to runtime.

PRO INVENT 2021

TECHNICAL UNIVERSITY OF CLUJ-NAPOCA ROMANIA

BIECO Building Trust in Ecosystems and Ecosystem Components

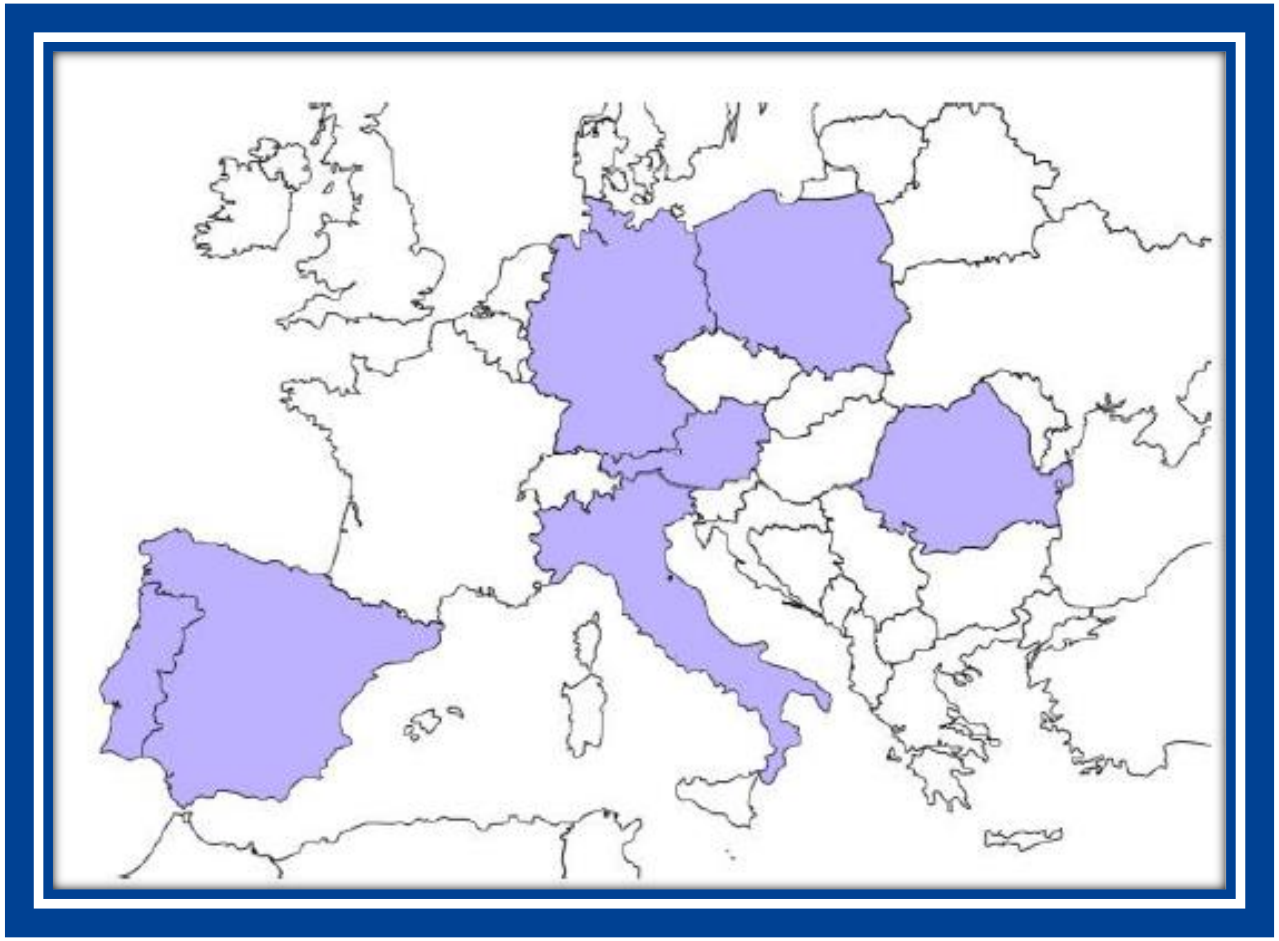
Research consortium

https://www.bieco.org/consortium/

The research consortium is composed of

11 partners, from
7 European countries:

- Portugal
- Italy
- Romania
- Austria
- Spain
- Poland
- Germany



It received founding from the European Union, through the Horizon 2020 Research and Innovation Program

TECHNICAL UNIVERSITY OF CLUJ-NAPOCA ROMANIA

PRO INVENT 2021

BIECO
Building Trust in Ecosystems and Ecosystem Components

https://www.bieco.org/consortium/

BIECO Consortium

The purpose of this Consortium is in respect to the Project the relationship among the Parties, in particular concerning the organisation of the work between the Parties, the management of the Project and the rights and obligations of the Parties concerning inter alia liability, Access Rights and dispute resolution.

TECHNICAL UNIVERSITY OF CLUJ-NAPOCA ROMANIA

BIECO
Building Trust in Ecosystems and Ecosystem Components

UTCN Research team


Ovidiu Cosma


Petrică Pop-Sitar


Cosmin Sabo


Ioana Zelina


Mara Măcelaru

PRO INVENT 2021

https://www.bieco.org/work-packages/

UTCN involvement

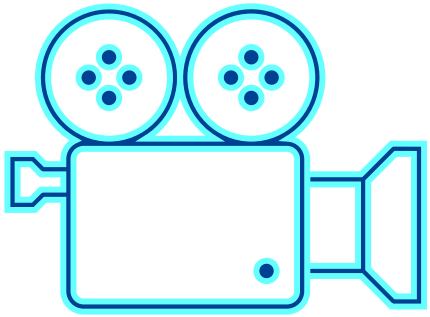
UTCN is
- involved in 6 work packages
- leader of one work package
- leader of 4 work tasks

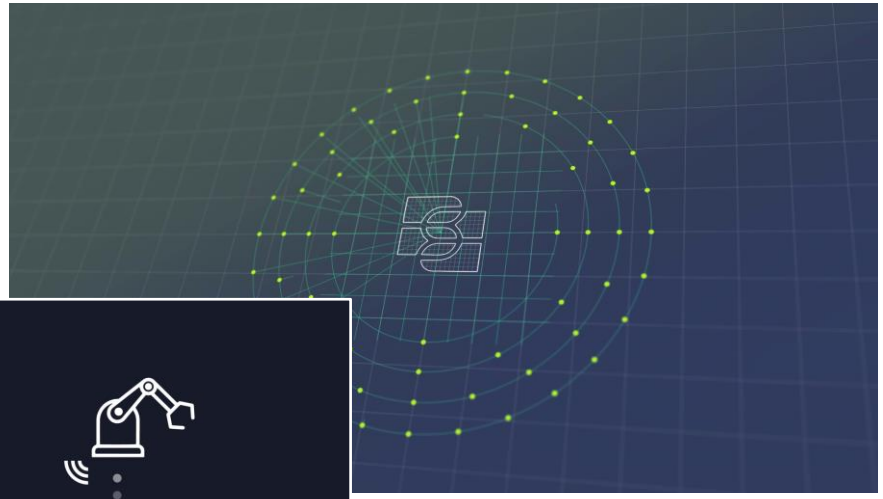
PRO INVENT 2021

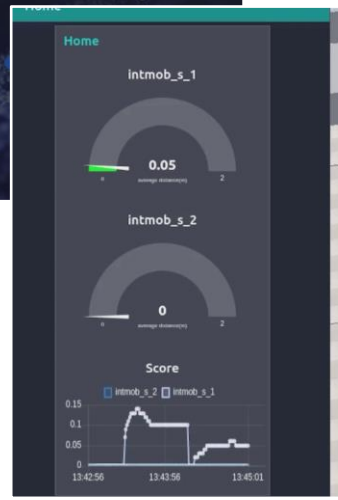
TECHNICAL UNIVERSITY OF CLUJ-NAPOCA ROMANIA

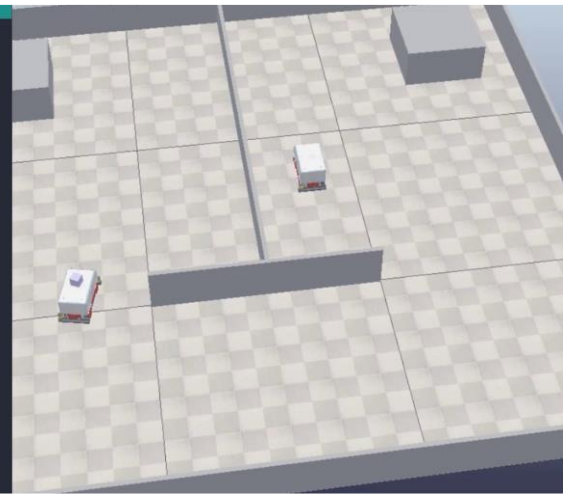
BIECO
Building Trust in Ecosystems and Ecosystem Components

Video presentation





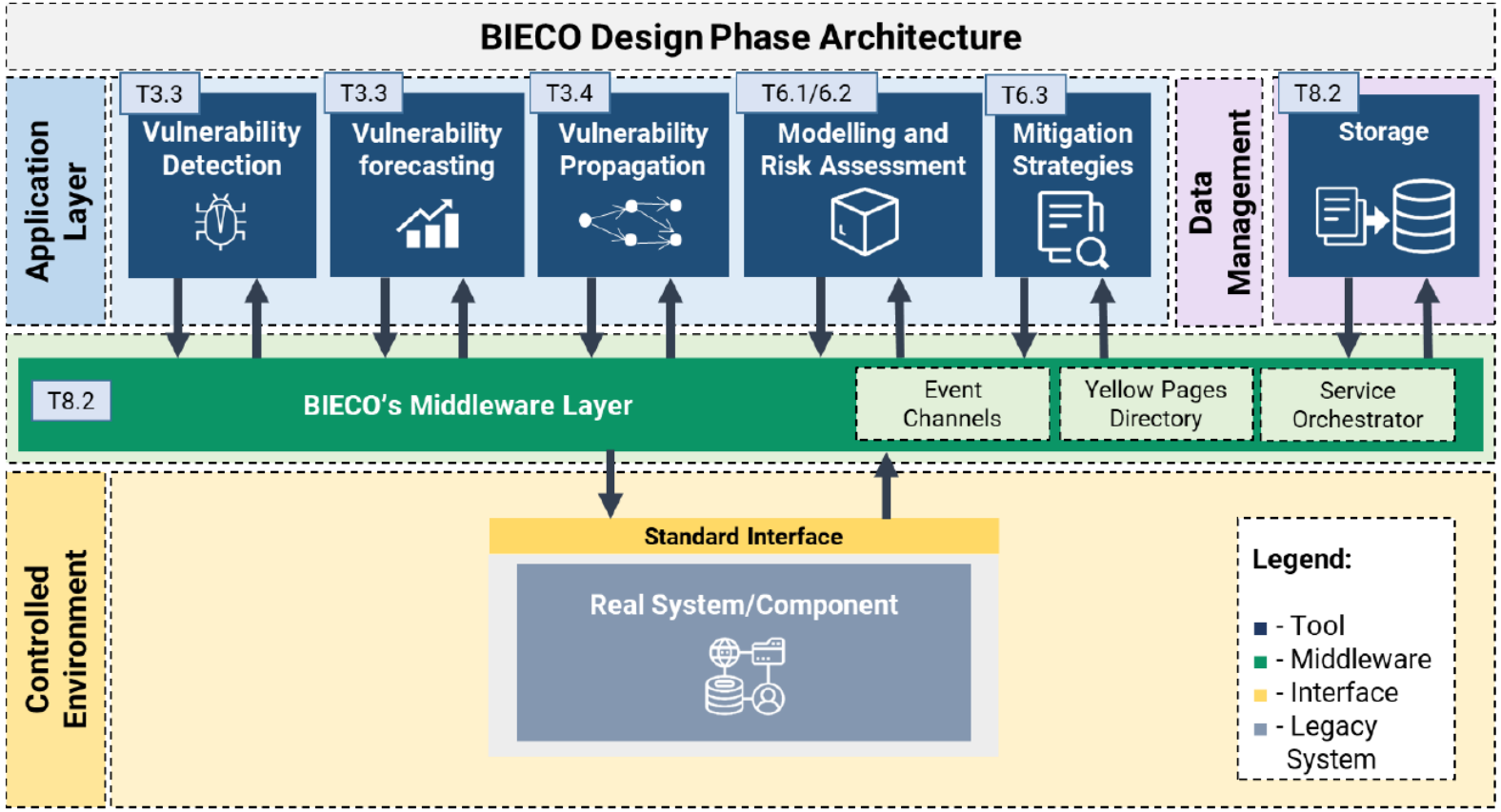




PRO INVENT 2021

TECHNICAL UNIVERSITY OF CLUJ-NAPOCA ROMANIA

BIECO
Building Trust in Ecosystems and Ecosystem Components



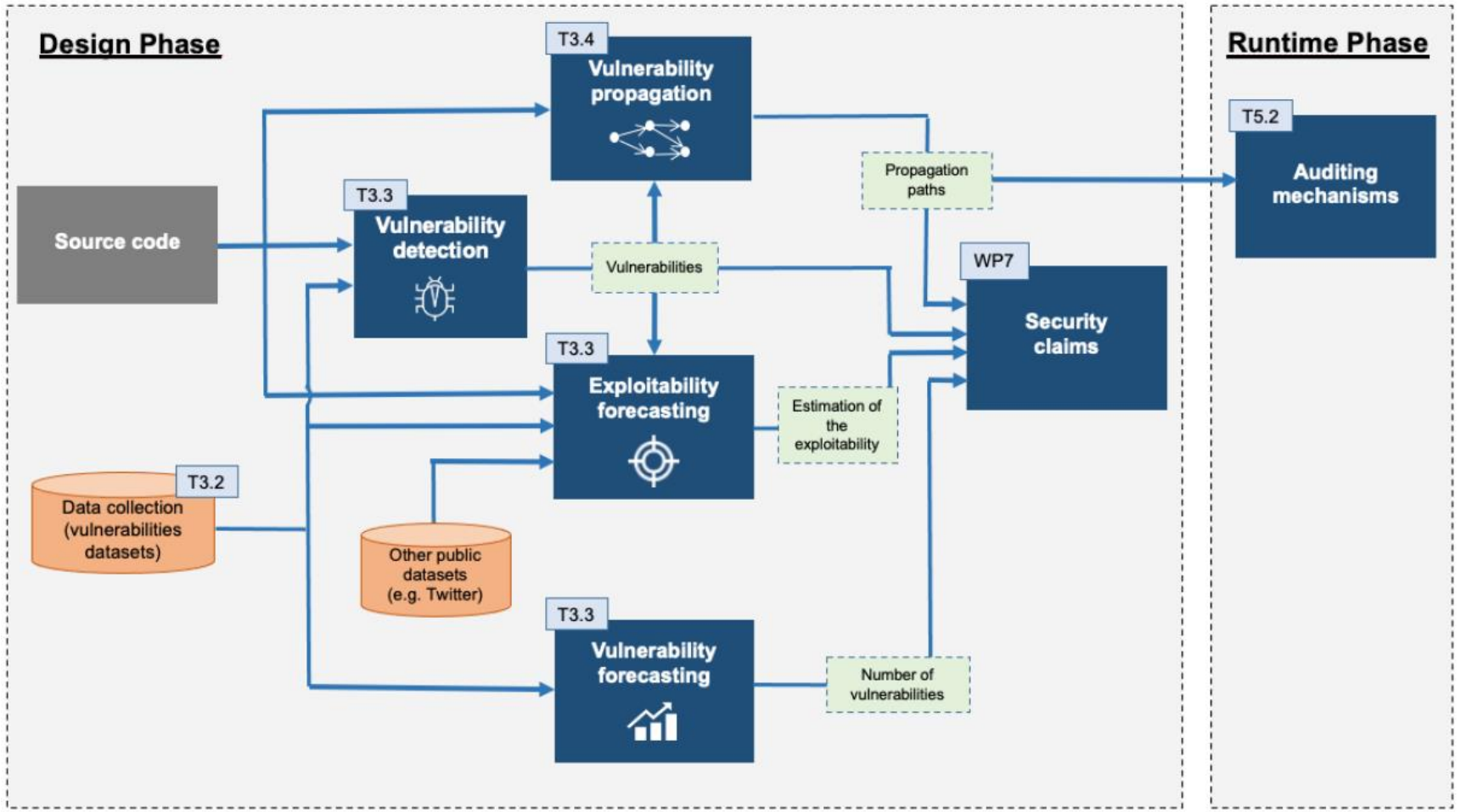
During design time,
a use case ecosystem is modelled with a toolchain that includes features of threat and risk analysis, identification and simulation of mitigations.

A vulnerability assessment process (consisting of vulnerability detection, forecasting and propagation) for software components.

TECHNICAL UNIVERSITY OF CLUJ-NAPOCA ROMANIA

PRO INVENT 2021

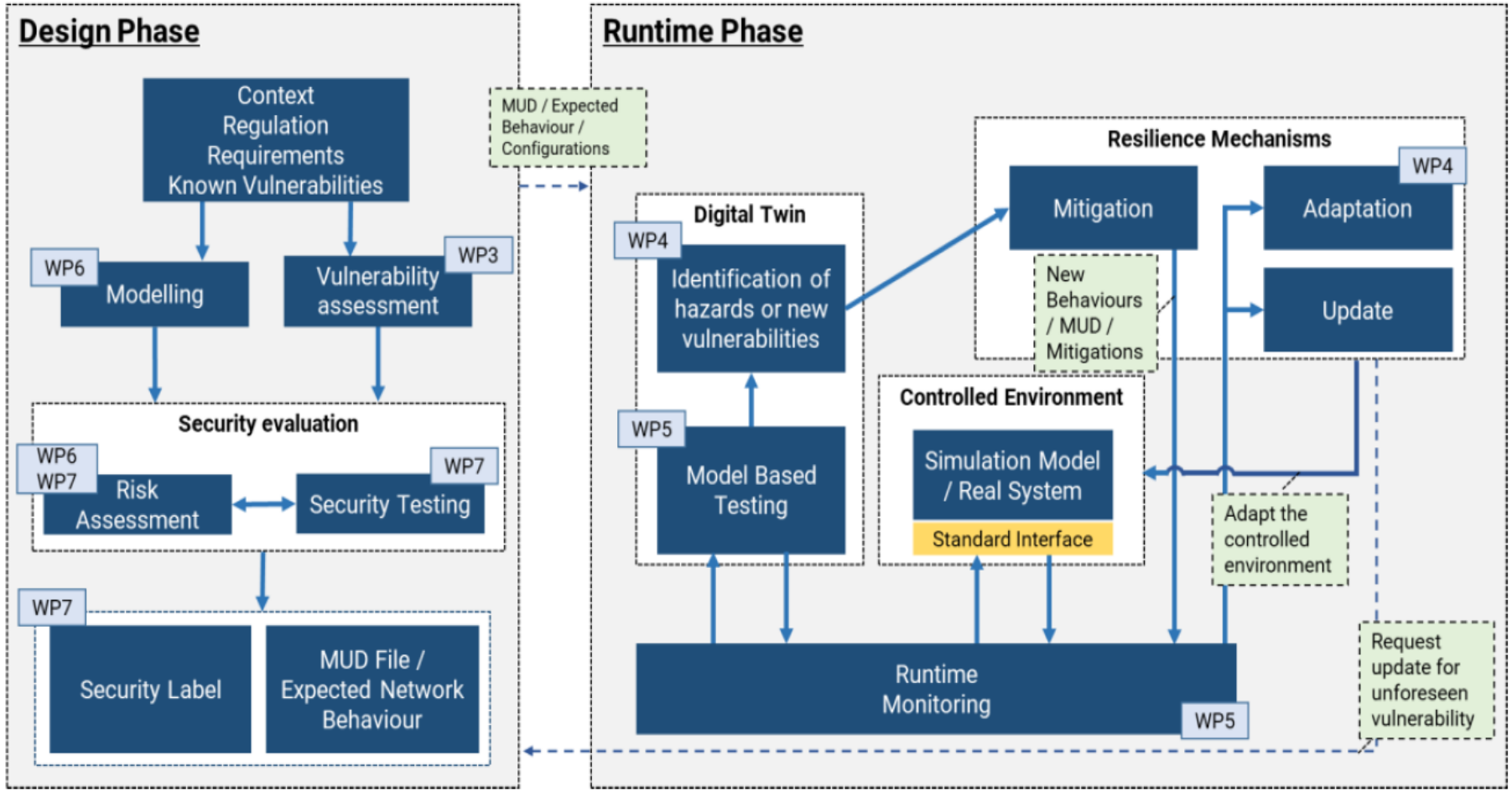
BIECO
Building Trust in Ecosystems and Ecosystem Components



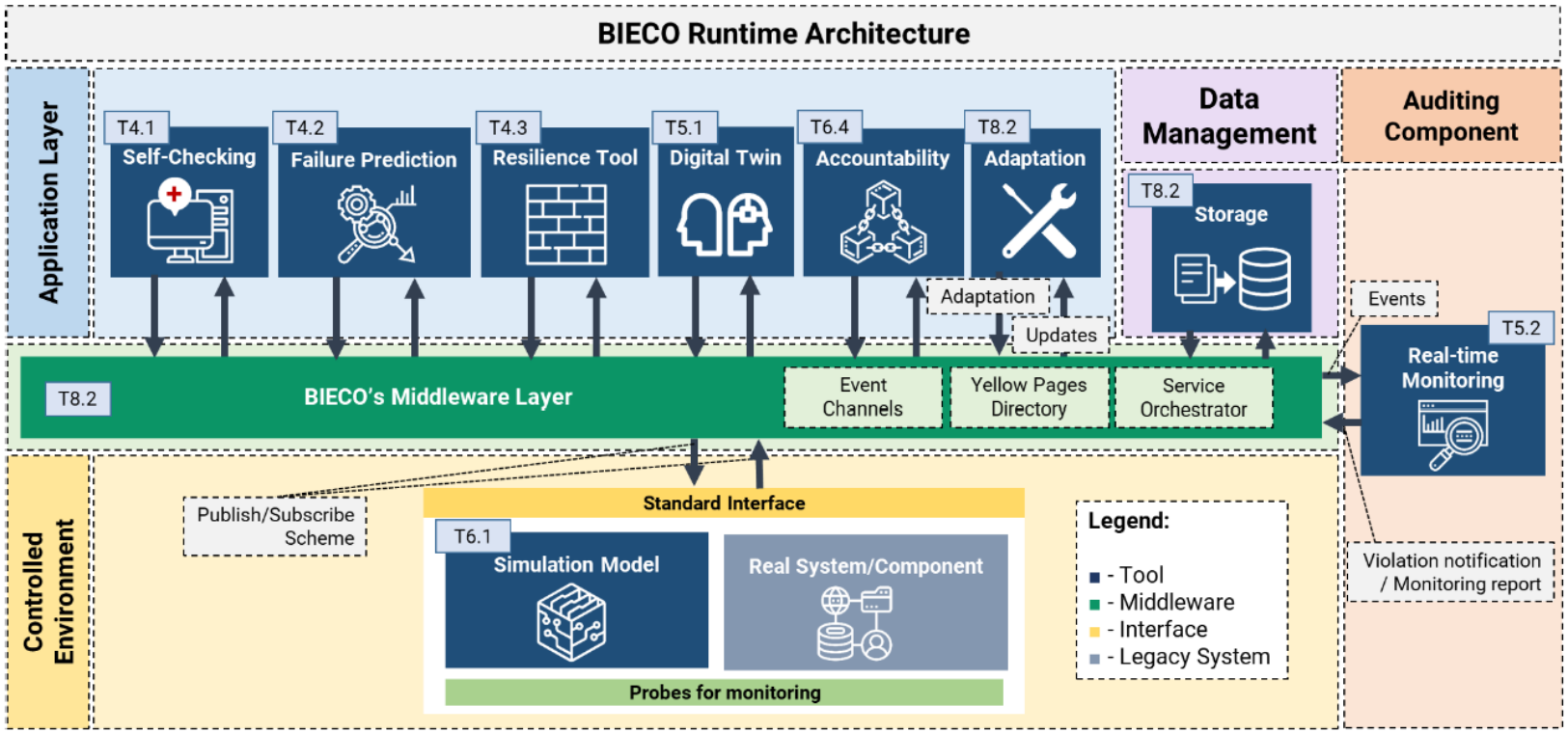
A security evaluation process is executed to determine the security level achieved by the system.

TECHNICAL UNIVERSITY OF CLUJ-NAPOCA ROMANIA

BIECO
Building Trust in Ecosystems and Ecosystem Components



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 a predictive simulation environment, a runtime monitor mechanism and a controlled environment.

The predictive simulation executes in a simulated environment (the digital twins), which are abstractions of software components created according to a Domain Specific Language.

PRO INVENT 2021

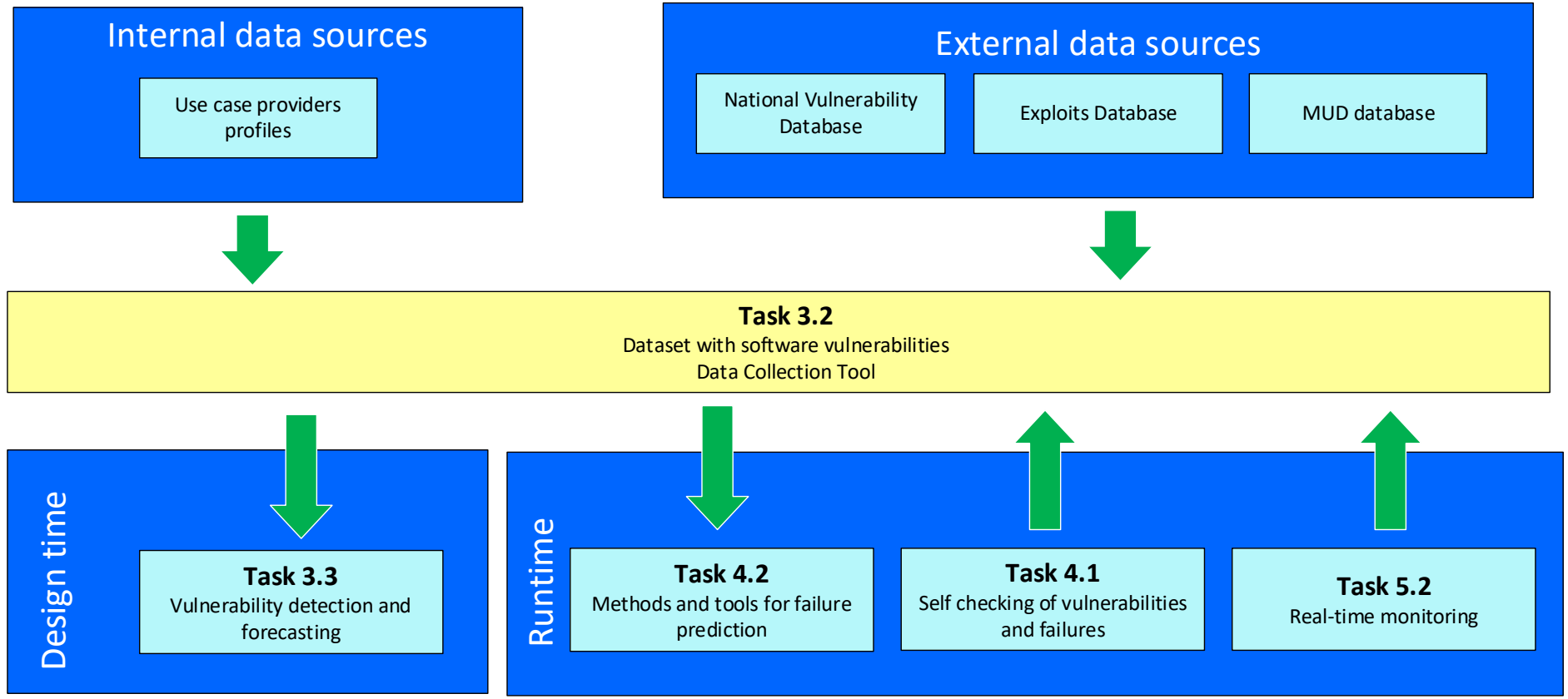
UTCN Results

BIECO
Building Trust in Ecosystems and Ecosystem Components

Data Collection Tool – developed by UTCN in the first year of BIECO

The data collection tool is an information repository that allows an in-depth analysis of the use cases weaknesses.

It works with information sources that are both public and internal.



PRO INVENT 2021

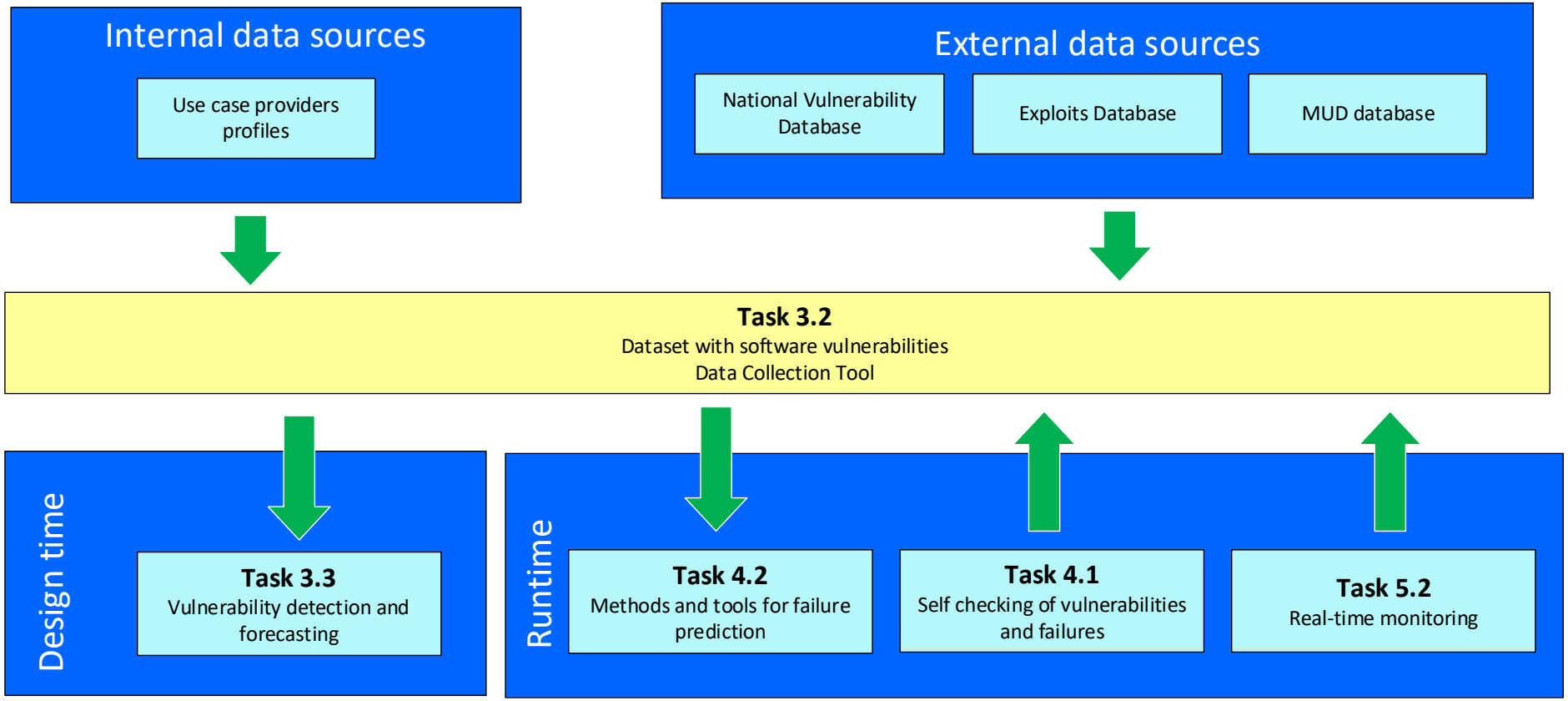
TECHNICAL UNIVERSITY OF CLUJ-NAPOCA ROMANIA

BIECO
Building Trust in Ecosystems and Ecosystem Components

Data Collection Tool

The public information sources are vulnerability databases, exploits databases and MUD files repositories.

The internal information sources are the BIECO use cases. For each use case, profile information and runtime monitoring data are stored.



PRO INVENT 2021

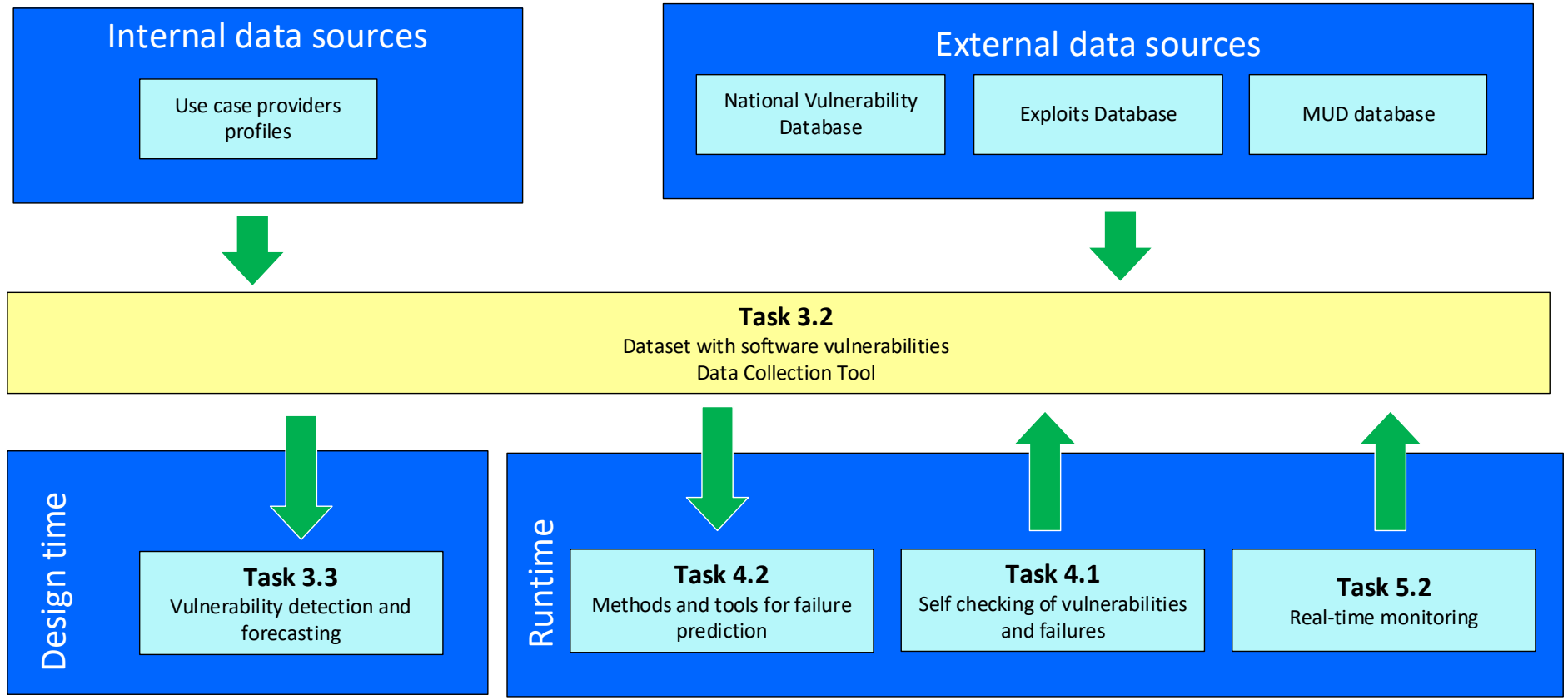
TECHNICAL UNIVERSITY OF CLUJ-NAPOCA ROMANIA

BIECO
Building Trust in Ecosystems and Ecosystem Components

Data Collection Tool

The profiles contain information about the use case components (libraries, frameworks, operating systems, and applications), and also, the bug history.

The runtime monitoring data contains parameters, sensor readings and failure events.



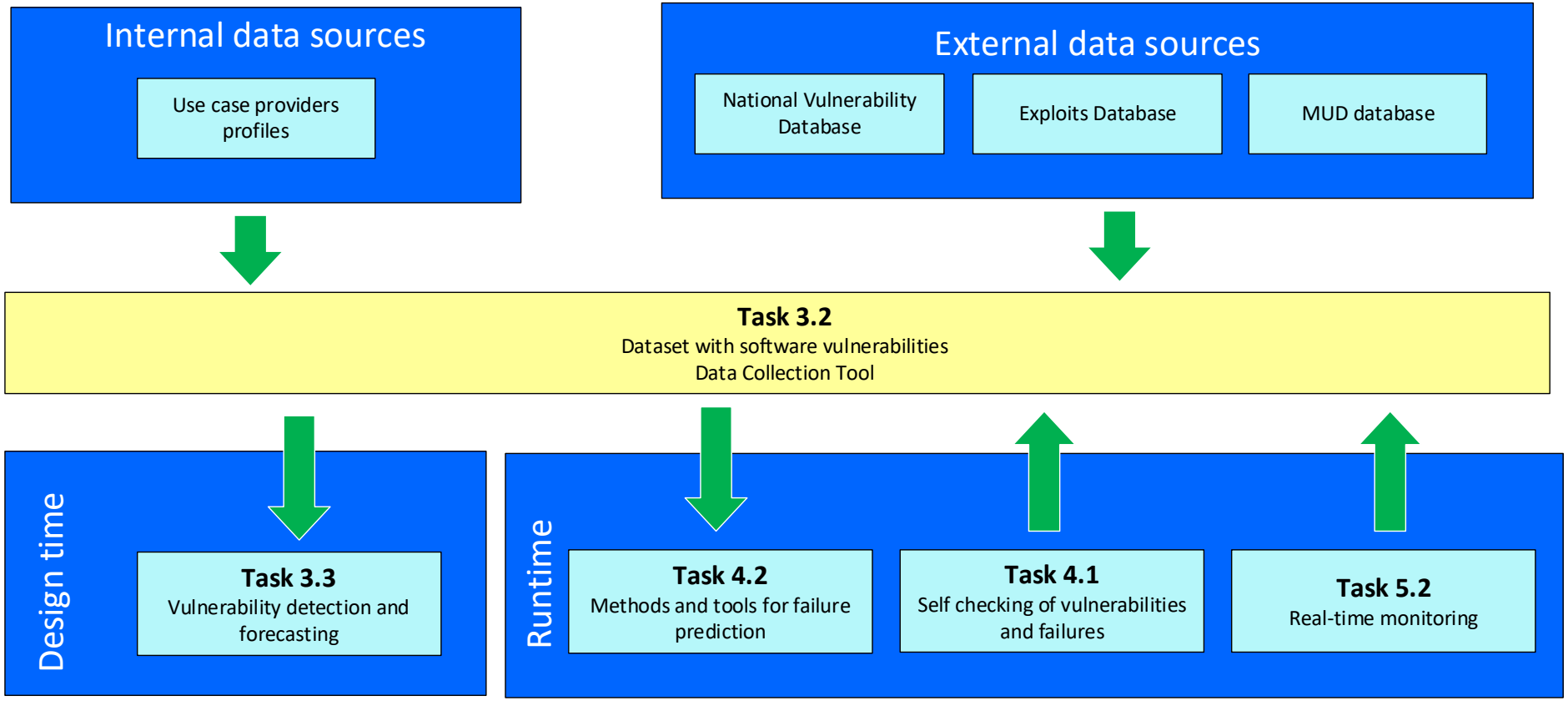
PRO INVENT 2021

TECHNICAL UNIVERSITY OF CLUJ-NAPOCA ROMANIA

BIECO
Building Trust in Ecosystems and Ecosystem Components

Data Collection Tool (DCT)

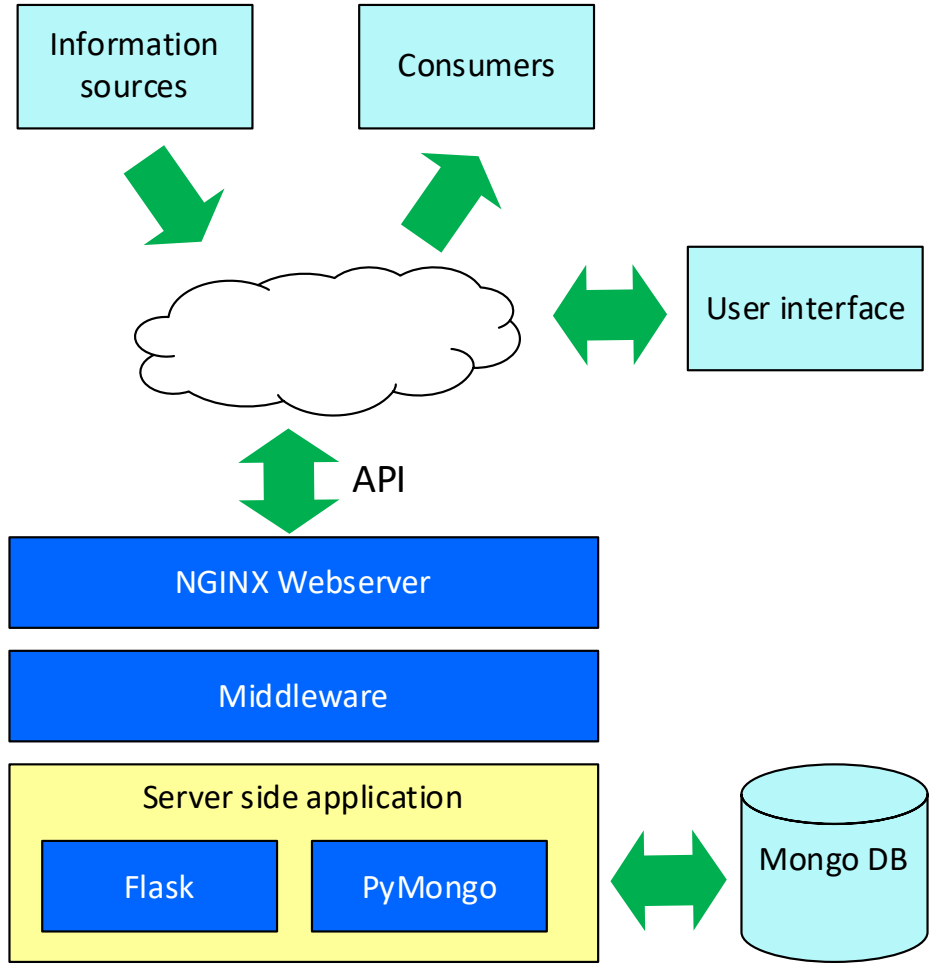
The main consumers of the Data Collection Tool information, are the machine learning algorithms of BIECO, trained to forecast vulnerabilities, exploits and failures.



TECHNICAL UNIVERSITY OF CLUJ-NAPOCA ROMANIA

BIECO
Building Trust in Ecosystems and Ecosystem Components

Data Collection Tool architecture

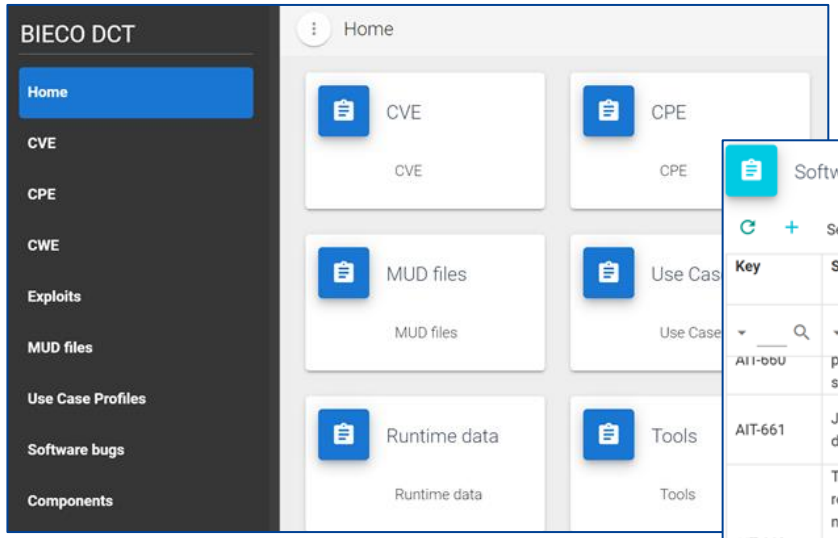


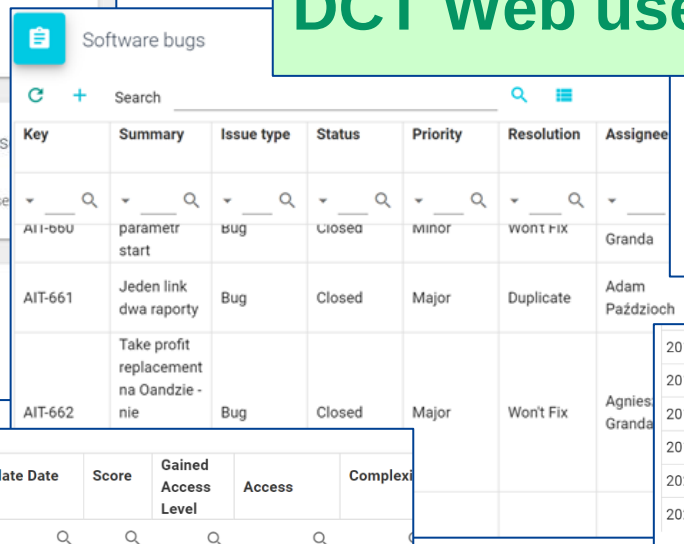
PRO INVENT 2021

TECHNICAL UNIVERSITY OF CLUJ-NAPOCA ROMANIA

BIECO
Building Trust in Ecosystems and Ecosystem Components

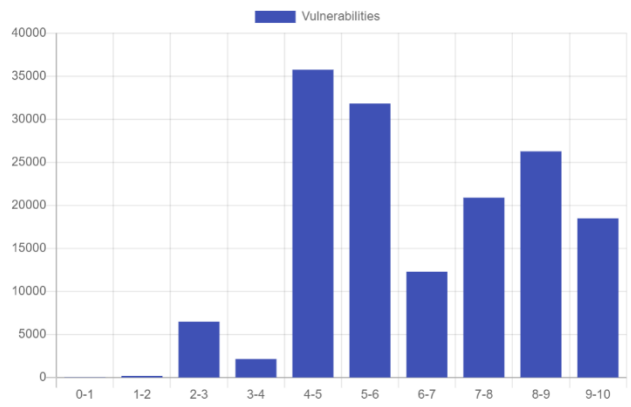
DCT Web user interface





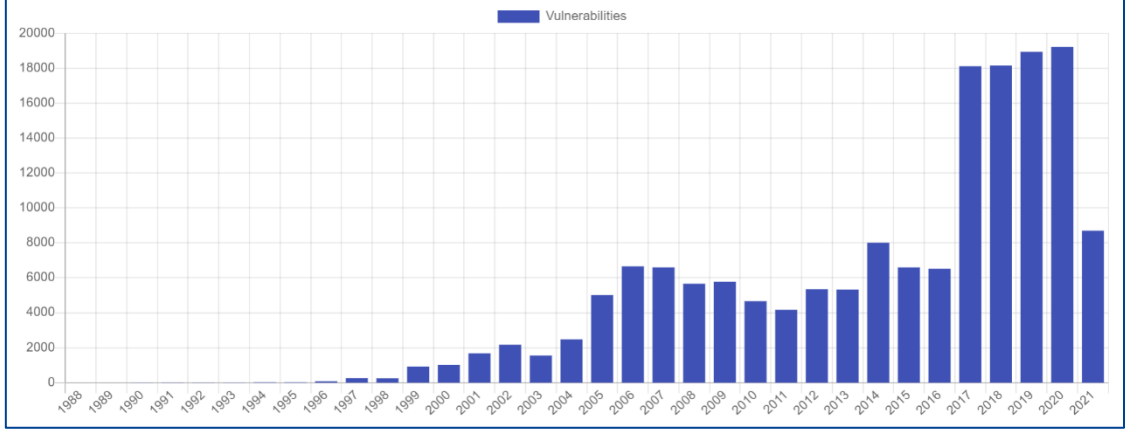
Current CVSS Score Distribution For All Vulnerabilities

CVSS Score	Number Of Vulnerabilities	Percentage
0	23	0.01
1	181	0.12
		4.2
		1.39
		23.17
		20.62
6	12285	7.96
7	20880	13.53
8	26260	17.02
9	10019	6.49
10	8458	5.48



	CVE ID	CWE ID	# of Exploits	Vulnerability Type(s)	Publish Date	Update Date	Score	Gained Access Level	Access	Complexi
	CVE-1999-0038	NVD-CWE-Other			1997-04-26	2018-10-30	7.2	ADMIN	LOCAL	LOW
	CVE-1999-0046	NVD-CWE-Other			1997-02-06	2018-10-30	10	ADMIN	NETWORK	LOW
	CVE-1999-0341	NVD-CWE-Other			1998-01-01	2008-09-09	7.2	ADMIN	LOCAL	LOW
	CVE-1999-0368	NVD-CWE-Other			1999-02-09	2008-09-09	10	ADMIN	NETWORK	LOW
	CVE-1999-0373	NVD-CWE-Other			1999-02-01	2008-09-09	7.2	ADMIN	LOCAL	LOW
	CVE-1999-0374	NVD-CWE-Other			1999-02-16	2008-09-09	2.1	NONE	LOCAL	LOW
	CVE-1999-0381	NVD-CWE-Other			1999-02-26	2008-09-09	7.2	ADMIN	LOCAL	LOW
	CVE-1999-0389	NVD-CWE-Other			1999-01-03	2008-09-09	7.2	ADMIN	LOCAL	LOW
	CVE-1999-0405	NVD-CWE-Other			1999-02-18	2008-09-09	7.2	ADMIN	LOCAL	LOW
	CVE-1999-0457	NVD-CWE-Other			1999-01-17	2008-09-09	7.2	ADMIN	LOCAL	LOW
	CVE-1999-0434	NVD-CWE-Other			1999-03-30	2008-09-09	7.5	OTHER	NETWORK	LOW
	CVE-1999-0730	NVD-CWE-Other			1999-06-12	2008-09-05	10	NONE	NETWORK	LOW

2016	6517	January	February	March	April	May	June	July	August	September	Octomber	November	December	
2017	18113	January	February	March	April	May	June	July	August	September	Octomber	November	December	
2018	18154	January	February	March	April	May	June	July	August	September	Octomber	November	December	
2019	18938	January	February	March	April	May	June	July	August	September	Octomber	November	December	
2020	19222	January	February	March	April	May	June	July	August	September	Octomber	November	December	
2021	8697	January	February	March	April	May	June	July	August					



PRO INVENT 2021

DCT REST API

A1.1. LIST: This code snippet is an example of retrieving CVE records.

cURL

```
curl --location -g --request GET
'api.dct.bieco.org:80/ils/nvd_cve?projection=
{%22cve.CVE_data_meta.ID%22:1, %22cve.CVE_data_meta.ASSIGNER%22:1,
%22publishedDate%22:1,%22lastModifiedDate%22:1,%22action%22:1}&sort=[(%22la
stModifiedDate%22,-1)]&max_results=12&page=10' \
--header 'Authorization: 99998a72-ede0-11eb-9f9b-110eb294d8b7'
```

A1.6. DELETE: This code snippet is an example of deleting a CVE record.

cURL

```
curl --location --
request DELETE 'api.dct.bieco.org:80/ils/nvd_cve/60fe5a62b62618c309eac6f7'
\
--header 'If-Match: 97dc996a1c4109ad009e79f61f721b0dea2317f6' \
--header 'Authorization: 99998a72-ede0-11eb-9f9b-110eb294d8b7'
```

A1.3. SEARCH: This code snippet is an example of retrieving data from the vulnerabilities collection using a set of parameters.

cURL

```
curl --location -g --request GET
'http://api.dct.bieco.org:80/ils/nvd_cve?projection={%22cve.CVE_data_meta.I
D%22:1,%22cve.CVE_data_meta.ASSIGNER%22:1,%22cve.problemtype.problemtype_da
ta.description.value%22:1,%22publishedDate%22:1,%22lastModifiedDate%22:1,%2
2impact.baseMetricV2.cvssV2.baseScore%22:1,%22impact.baseMetricV2.cvssV2.ac
cessVector%22:1,%22impact.baseMetricV2.cvssV2.accessComplexity%22:1,%22impa
ct.baseMetricV2.cvssV2.authentication%22:1,%22impact.baseMetricV2.cvssV2.co
nfidentialityImpact%22:1,%22impact.baseMetricV2.cvssV2.integrityImpact%22:1
,%22impact.baseMetricV2.cvssV2.availabilityImpact%22:1,%22action%22:1}&wher
e={%22publishedDate%22:{%22$regex%22:%22^2021%22,%22$options%22:%22i%22}}&s
ort=[(%22_id%22,-1)]&max_results=24&page=1' \
--header 'Authorization: 99998a72-ede0-11eb-9f9b-110eb294d8b7'
```

A1.7. VULNERABILITY BY MONTH: This code snippet is an example of retrieving the CVE records sorted by year, month and type.

cURL

```
curl --location --
request GET 'http://api.dct.bieco.org:80/
r_and_type' \
--header 'Authorization: 155fd6e2-c759-11eb-8c98-a32659ac8fd7'
```

A1.4. INSERT: This code snippet is an example of inserting vulnerability data into DCT.

cURL

```
curl --location --request POST
 'http://api.dct.bieco.org:80/ils/nvd_cve' \
--header 'Content-Type: application/json' \
--header 'Authorization: 99998a72-ede0-11eb-9f9b-110eb294d8b7' \
--data-raw '{
    "publishedDate": "2021-01-08",
    "lastModifiedDate": "2021-01-19"
}'
```

A2.4. INSERT: This code snippet is an example of inserting one CPE record into DCT.

cURL

```
curl --location --request POST 'http://api.dct.bieco.org:80/ils/nvd_cpe' \
--header 'Content-Type: application/json' \
--header 'Authorization: 99998a72-ede0-11eb-9f9b-110eb294d8b7' \
--data-
raw '{"cpe22Uri":"cpe:2.3:a:_wp2_favorite_posts_project:_wp_favorite_posts:
*:*:*:*:*:*:x","cpe23Uri":"cpe:2.3:a:_wp2_favorite_posts_project:_wp_favorite
_posts:*:*:*:*:*:*:x","versionStartExcluding":"2.1","versionStartIncluding":"
2.6","versionEndExcluding":"2.6","versionEndIncluding":"2.6","company":"60b
a0e132319e6a94acf6580"}'
```

TECHNICAL UNIVERSITY OF CLUJ-NAPOCA ROMANIA

BIECO
Building Trust in Ecosystems and Ecosystem Components

33 public information sources

https://0day.today/
https://github.com/0x4D31/awesome-threat-detection
https://www.cerias.purdue.edu/site/about/history/coast/projects/vdb.php
https://cert.europa.eu/cert/newsletter/en/latest_SecurityBulletins_.html
https://www.cnvd.org.cn/
https://www.cert.org.cn/publish/english/indix.html
http://www.cnnvd.org.cn/
https://www.cvedetails.com/
https://www.stigviewer.com/stigs
https://osf.io/d45bw/
https://www.exploit-db.com/
https://exchange.xforce.ibmcloud.com/
http://ivd.winicssec.com/
https://www.us-cert.gov/ics/advisories
https://www.misp-project.org/features.html
https://www.kyberturvallisuuskeskus.fi/en/homepage
https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/
https://samate.nist.gov/SARD/index.php
https://packetstormsecurity.com/
https://securiteam.com/
https://www.securityfocus.com/vulnerabilities
https://snyk.io/features/vulnerability-database/
https://www.talosintelligence.com/
https://globalplatform.org/iotopia/mud-file-service/
https://www.kb.cert.org/vuls/
https://help.veracode.com/reader/hHHR3gv0wYc2WbCclECf_A/lQYKhC8AvpIbz5_ULOCYMw
https://github.com/AUEB-BALab/VulinOSS
https://vulners.com/
https://www.first.org/global/sigs/vrdx/vdb-catalog
https://vulndb.cyberriskanalytics.com/
https://vuldb.com/
https://wpvulndb.com
https://www.zerodayinitiative.com/advisories/published/

PRO INVENT 2021

TECHNICAL UNIVERSITY OF CLUJ-NAPOCA ROMANIA

BIECO
Building Trust in Ecosystems and Ecosystem Components

Public information sources

Name	Description	Access
0 Day Today	A database of exploits and vulnerabilities written for educational purposes. The information is collected from submittals and various mailing lists.	Both
Awesome Threat Detection and Hunting	A curated list of threat detection and hunting resources.	Public
CERIAS Vulnerability Database	A vulnerability database maintained by Purdue University.	Private
CERT-EU	The platform of the Computer Emergency Response Team for the EU institutions. It maintains a list of security advisories and information on product vulnerabilities, threats and incidents and hacking techniques.	Public
China National Vulnerability Database (CNVD)	NVD similar database maintained by the Chinese national computer emergency response team (CERT). It often presents vulnerabilities unavailable in other sources	Public
Chinese national CERT's ICS branch	The website contains a list of ICS and IoT vulnerabilities. These vulnerabilities are found in either CNVD or CNNVD.	Public
Chinese National Vulnerability Database of Information Security (CNNVD)	Second database from China. It usually follows data found in NVD.	Public
CVE Details	It provides an easy-to-use web interface to CVE vulnerability data. Information about vendors, products, versions and statistics about vendors, products and versions of products are available.	Public
DISA STIG Compliance Requirements List	A STIGs "are the configuration standards for DOD [information assurance, or IA] and IA-enabled devices/systems…The STIGs contain technical guidance to 'lock down' information systems/software that might otherwise be vulnerable to a malicious computer attack."	Public
Draper VDISC Dataset	A dataset that containing the source code of 1.27 million functions mined from open-source software, labelled by static analysis for potential vulnerabilities.	Public
Exploit Database	**A CVE compliant archive of public exploits and corresponding vulnerable software, developed for use by penetration testers and vulnerability researchers. It contains a comprehensive collection of exploits gathered through direct submissions, mailing lists, as well as other public sources. The Exploit Database is a repository for exploits and proof-of-concepts rather than advisories, making it a valuable resource for research.**	Public
IBM X-Force Exchange	Cloud-based threat platform that enables the research on the latest global security threats, consulting, and collaboration with peers. It contains both human and machine-generated information.	Public
ICS Vulnerability Database	From a Chinese ICS security company Winicssec. Contains data from other sources (NVD, CNVD and CNNVD).	Public
ICS-CERT	The Industrial Control Systems Cyber Emergency Response Team platform. It shares vulnerability information and threat analysis through information products and alerts. It provides vulnerability and malware analysis, onsite support for incident response and forensic analysis.	Public
MISP	It is used to store, share, collaborate on cyber security indicators, malware analysis, and to detect and prevent attacks, against ICT infrastructures. It is used to store, share, collaborate on cyber security indicators, malware analysis, and to detect and prevent attacks, against ICT infrastructures.	Public
National Cyber Security Centre	Located in Finland, it develops and monitors the operational reliability and security of communications networks and services. It provides situational awareness of cyber security.	Public
Netsparker	A fully automatic vulnerability assessment tool that crawls and scans web applications. Vulnerabilities are automatically assigned a severity level to highlight the potential damage and the urgency with which they must be fixed.	Private
NIST Software Assurance Reference Dataset Project	It provides a set of known security flaws in order to allow users to evaluate tools and to test their methods. The dataset includes "wild" (production), "synthetic" (written to test or generated), and "academic" (from students) test cases. The dataset intends to encompass a wide variety of possible vulnerabilities, languages, platforms, and compilers.	Public

PRO INVENT 2021

TECHNICAL UNIVERSITY OF CLUJ-NAPOCA ROMANIA

BIECO
Building Trust in Ecosystems and Ecosystem Components

Public information sources

Packet Storm	An information security website offering current and historical computer security tools, exploits, and security advisories.	Public
SecuriTeam	A security portal containing security information from mailing lists, information channels and tools.	Public
Security Focus	Focuses on a few key areas that are of greatest importance to security: a mailing list for discussion and announcements related to computer security and a vulnerability database.	Public
Snyk Intel Vulnerability Database	An open-source vulnerability database, that also includes additional non-CVE vulnerabilities derived from numerous sources. Numerous vulnerabilities are exposed before they are added to public databases.	Both
Talos	A regular intelligence update from Cisco Talos, highlighting the biggest threats each week and other security news.	Public
The Global Platform MUD File Service	It provides a MUD files database, helping device manufacturers to publish, in a unique location, the MUD file library associated with their products. Publication in the MUD File Service simplifies the access and consumption of MUD files from networks hosting these devices.	Private
The Vulnerability Notes Database (VND)	It provides information about software vulnerabilities. Vulnerability notes include summaries, technical details, remediation information, and lists of affected vendors. Most vulnerability notes are the result of private coordination and disclosure efforts. The CERT/CC Vulnerability Notes Database is run by the CERT Division, which is part of the Software Engineering Institute, a federally funded research and development centre operated by Carnegie Mellon University.	Public
Veracode	An agent-based scan software composition analysis for securing web, mobile and third-party enterprise applications. Veracode provides multiple security analysis technologies on a cloud-based platform, including static analysis, dynamic analysis, mobile application behavioural analysis and software composition analysis.	Private

Vulnerabilities in open-source systems	A project representing a dataset of vulnerabilities in open-source projects, as published in Mining Software Repositories 2018 (MSR) conference.	Public
Vulnerability Assessment Platform	A platform aggregating vulnerability and exploit data from over 130 sources.	Both
Vulnerability Database Catalogue	A catalogue initially of vulnerability databases, underlining differences in identifiers, coverage and scope, size, abstraction and other characteristics. Vulnerability databases are loosely defined as sites that provide vulnerability information, such as advisories, with identifiers.	Both
VulnDB	A commercial vulnerability intelligence mechanism developed by Risk-Based Security that provides actionable information about the latest in security vulnerabilities via a SaaS Portal, or a RESTful API. The tool tracks over 2,000 software libraries looking for security issues and it has a direct mapping with CVE and NVD. The client can configure email alerts to receive a notification when a new vulnerability is released and he can ask for guidance on how to mitigate the vulnerability and for product and vendor evaluations.	Private
Vulnerability Database	A database with more than 166000 entries available. The information is updated daily since 1970. Besides technical details, there are additional threat intelligence information like current risk levels and exploit price forecasts provided.	Both
WordPress Vulnerability Database	A database of WordPress vulnerabilities, plugin vulnerabilities and theme vulnerabilities.	Both
Zero Day Initiative	Platform for reporting of 0-day vulnerabilities privately to the affected vendors by the researchers. There is available a list of publicly disclosed vulnerabilities discovered by Zero Day Initiative researchers.	Both

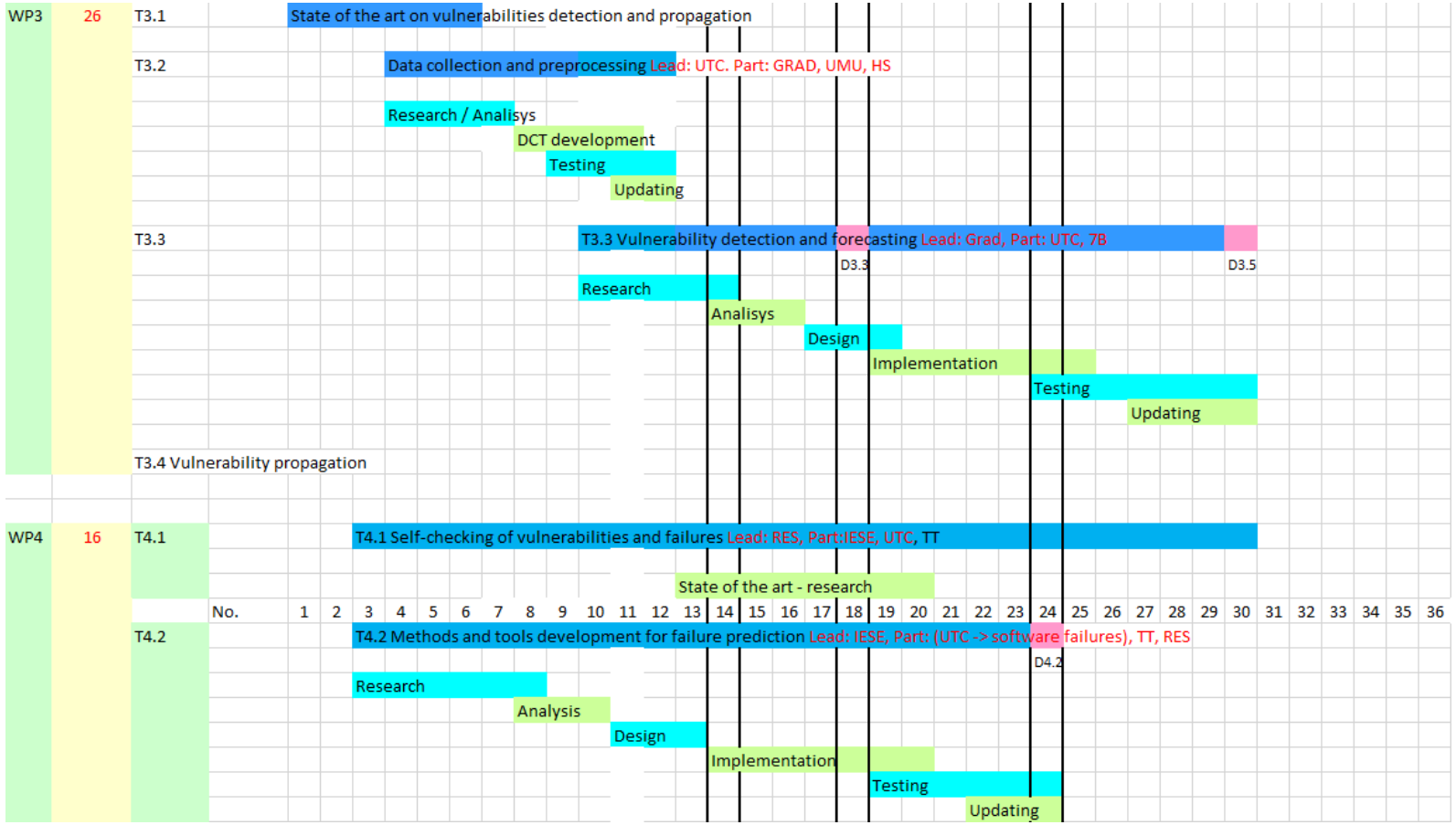
PRO INVENT 2021

UTCN current and future activities

BIECO
Building Trust in Ecosystems and Ecosystem Components

UTCN main research and development activities in the next two years of BIECO

- T3.3 Vulnerabilities forecasting
- T4.2 Failure prediction

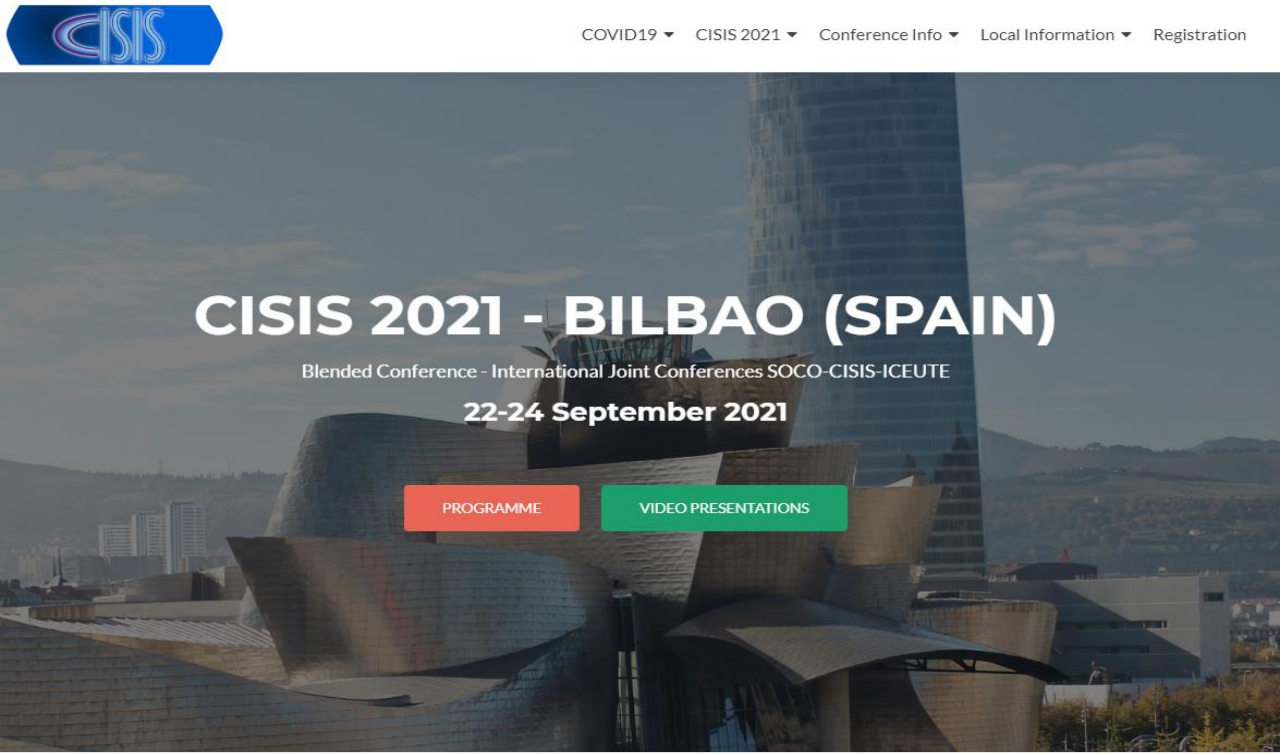


PRO INVENT 2021

TECHNICAL UNIVERSITY OF CLUJ-NAPOCA ROMANIA

BIECO
Building Trust in Ecosystems and Ecosystem Components

State of the art research



CISIS 2021

14th International Conference on Computational Intelligence in Security for Information Systems

A comparative study of the most important methods for forecasting the ICT systems vulnerabilities

O. Cosma[0000-0001-9740-5394], M. Macelaru[0000-0003-3135-1244], P.C. Pop[0000-0002-0626-9284], C. Sabo[0000-0002-5648-7191] and I. Zelina[0000-0002-8855-7350]

Technical University of Cluj-Napoca, North University Center of Baia Mare, Dr. V. Babes 62A, 430083, Romania
{ovidiu.cosma, mara.hajdu, petrica.pop, cosmin.sabo, ioana.zelina}@mi.utcluj.ro

Abstract. Nowadays, companies are facing plenty of IT secure attacks and to guarantee safe, untroubled, and continuous functioning of their business, they should detect and forecast the volume of IT security vulnerabilities and be prepared for future threats. The aim of this paper is to present a comparative study of the most important and promising methods for forecasting the ICT systems vulnerabilities.

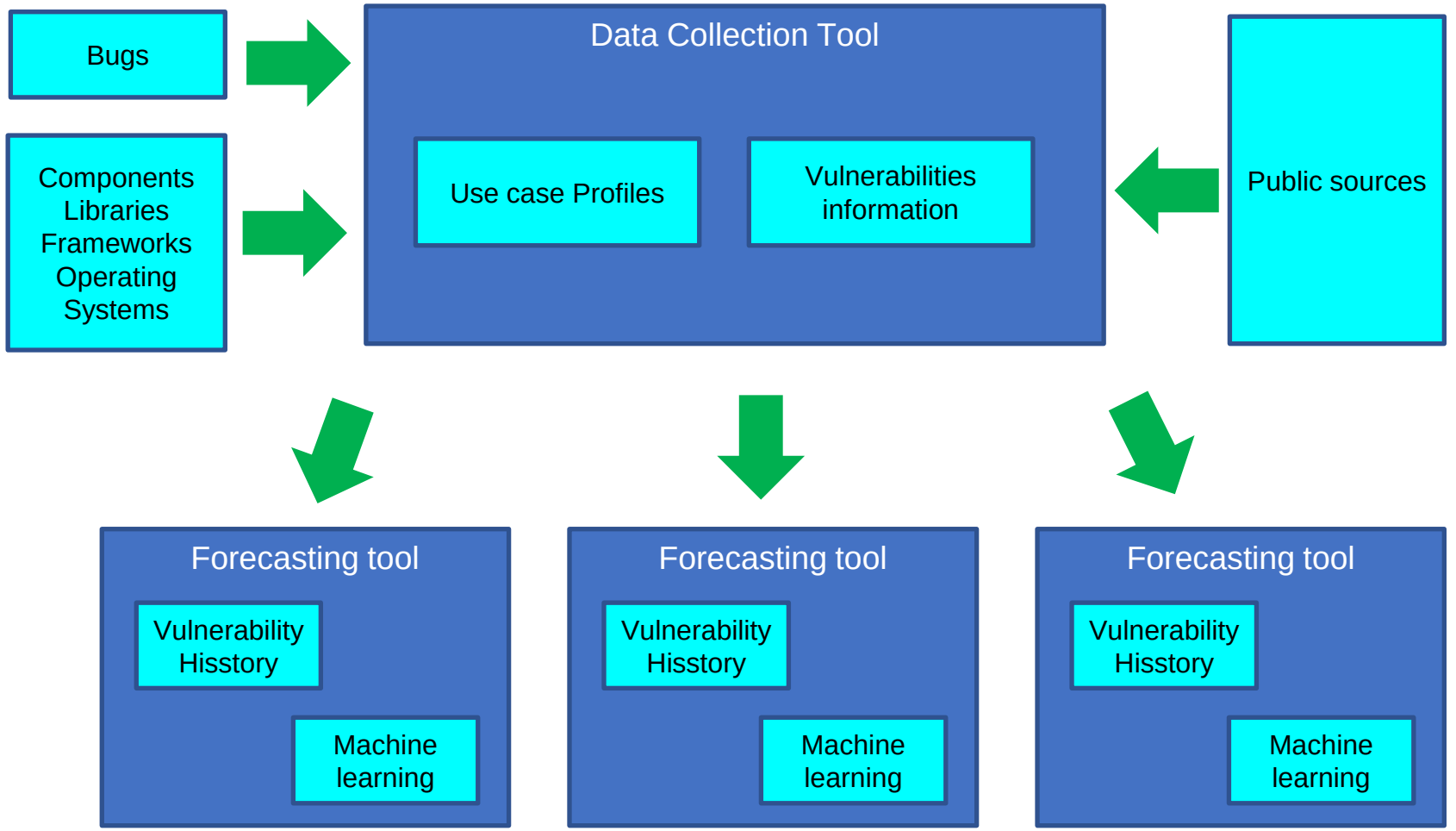
Keywords: Security vulnerabilities, Forecasting, Time series forecasting, Neural networks.

Article: https://www.bieco.org/a-comparative-study-of-the-most-important-methods-for-forecasting-the-ict-systems-vulnerabilities/
Video presentation: https://www.bieco.org/

TECHNICAL UNIVERSITY OF CLUJ-NAPOCA ROMANIA

BIECO
Building Trust in Ecosystems and Ecosystem Components

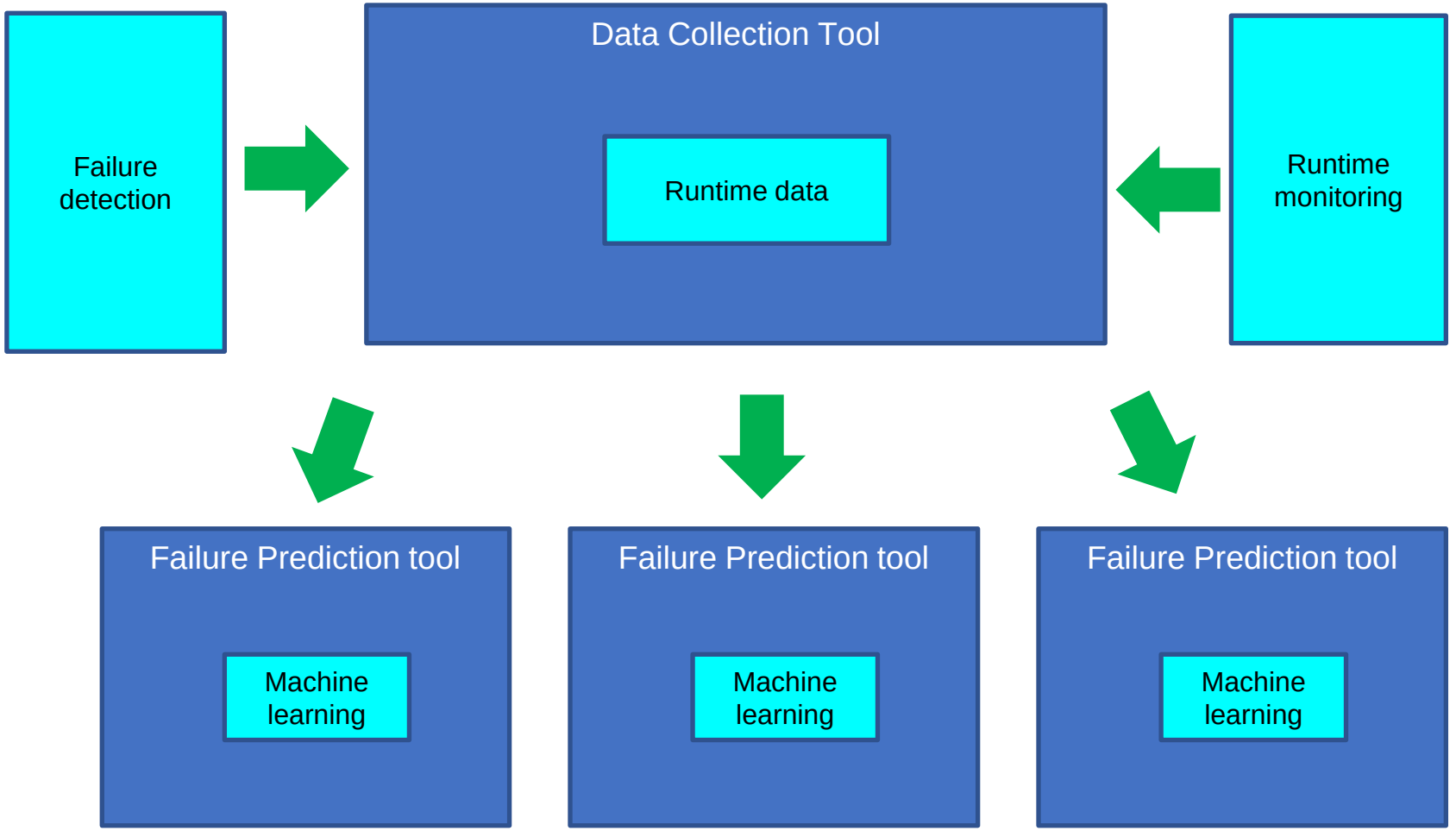
Vulnerabilities forecasting



TECHNICAL UNIVERSITY OF CLUJ-NAPOCA ROMANIA

BIECO
Building Trust in Ecosystems and Ecosystem Components

Failure prediction



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

Contact Us:

www bieco.org

github.com/biecoorg

facebook.com/bieco.org

twitter.com/bieco_org

instagram.com/bieco_org/

BIECO
Building Trust in Ecosystems and Ecosystem Components

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

TECHNICAL UNIVERSITY OF CLUJ-NAPOCA ROMANIA

PRO INVENT 2021

BIECO
Building Trust in Ecosystems and Ecosystem Components

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

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