OpenUEBA - An open source framework for User and Entity Behaviour Analytics

TNC 22 Trieste,Italy *14th June 2022*

Albert Calvo (albert.calvo@i2cat.net - /in/albertcalvo/)
Nil Ortiz - (nil.ortiz@i2cat.net - /in/nilortiz/)

THE INTERNET RESEARCH CENTER

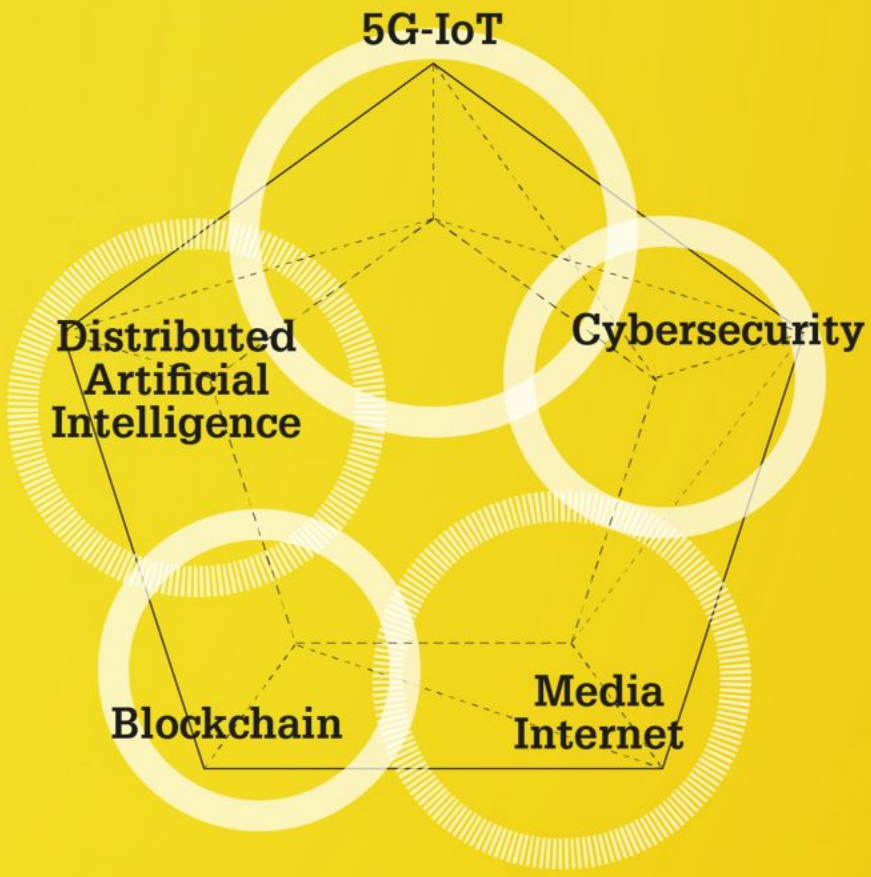
Never stop designing the digital future

i2CAT.net

Intro

The i2CAT Foundation is a non-profit research and innovation center that promotes mission-driven R&D activities in advanced digital technologies.

The center has more than 15 years of experience pursuing international and local R&D projects in the fields of 5G, IoT, VR and Immersive Technologies, Cybersecurity, Blockchain, AI and Digital Social Innovation.



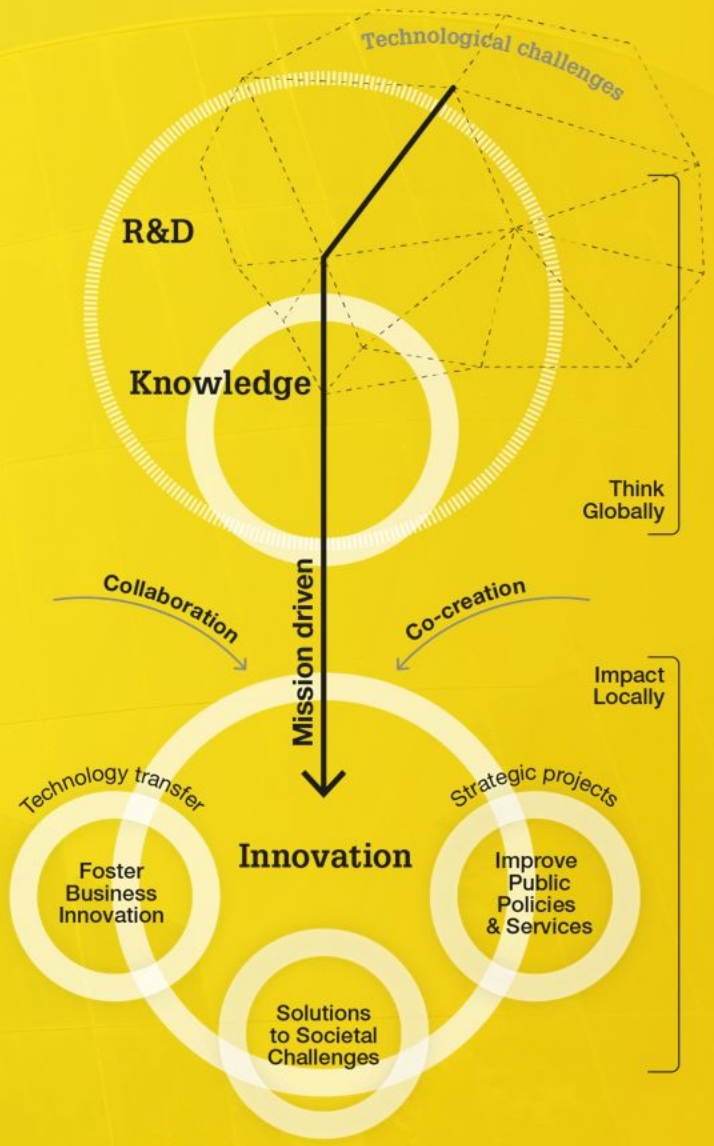
Activities

Research & Innovation, playing a key role in the EU Framework Program for Research and Innovation, as well as in Catalan and Spanish calls.

Collaboration with Public Administrations, playing a fundamental role in the definition and deployment of digital public policies throughout the country.

Cooperation with private companies, working to translate the outcomes and knowledge generated as a result of research activities into productive sectors of the local and international economy.

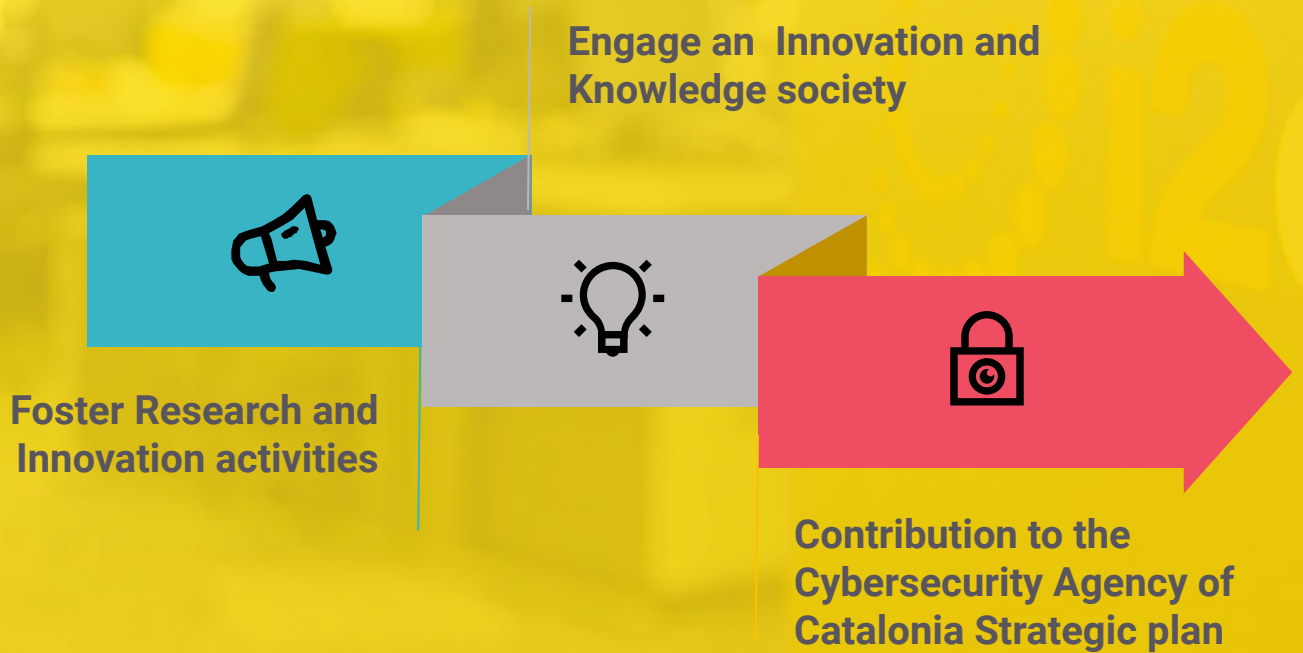
Technology Transfer, boosting collaborations with the innovation ecosystem players through strategic alliances to create innovative market-oriented technologies and solutions.



Challenges in Advanced Digital Technologies - TDA

Generalitat de Catalunya

- Mission-driven project founded by the Generalitat of Catalonia
- Capital Seed to Deep Tech Projects



AGÈNCIA DE CIBERSEGURETAT DE CATALUNYA

i2cat

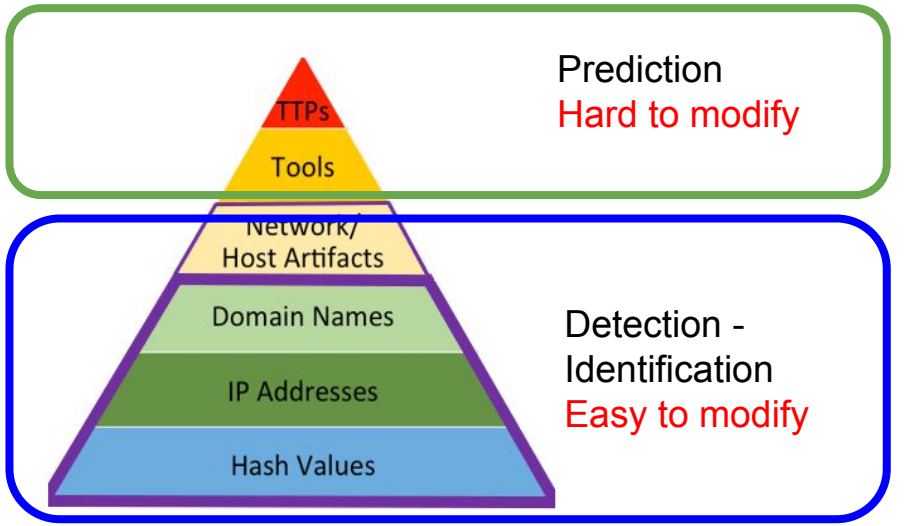
OpenUEBA

Calculate the user and entity exposure analysis against specific threats through the power of CTI and AI working together

Our vision

Learning the behaviour of users is more resilient to changes than analysing atomic indicators or observables

- Determining which users are more susceptible of being cyber threats victims
- Adopting users protection actions
- Reduce attack surface and anticipation capabilities



Our Novelty

Multimodal Data

The proposed framework exploits several heterogeneous data sources allowing to build rich entity profiles.

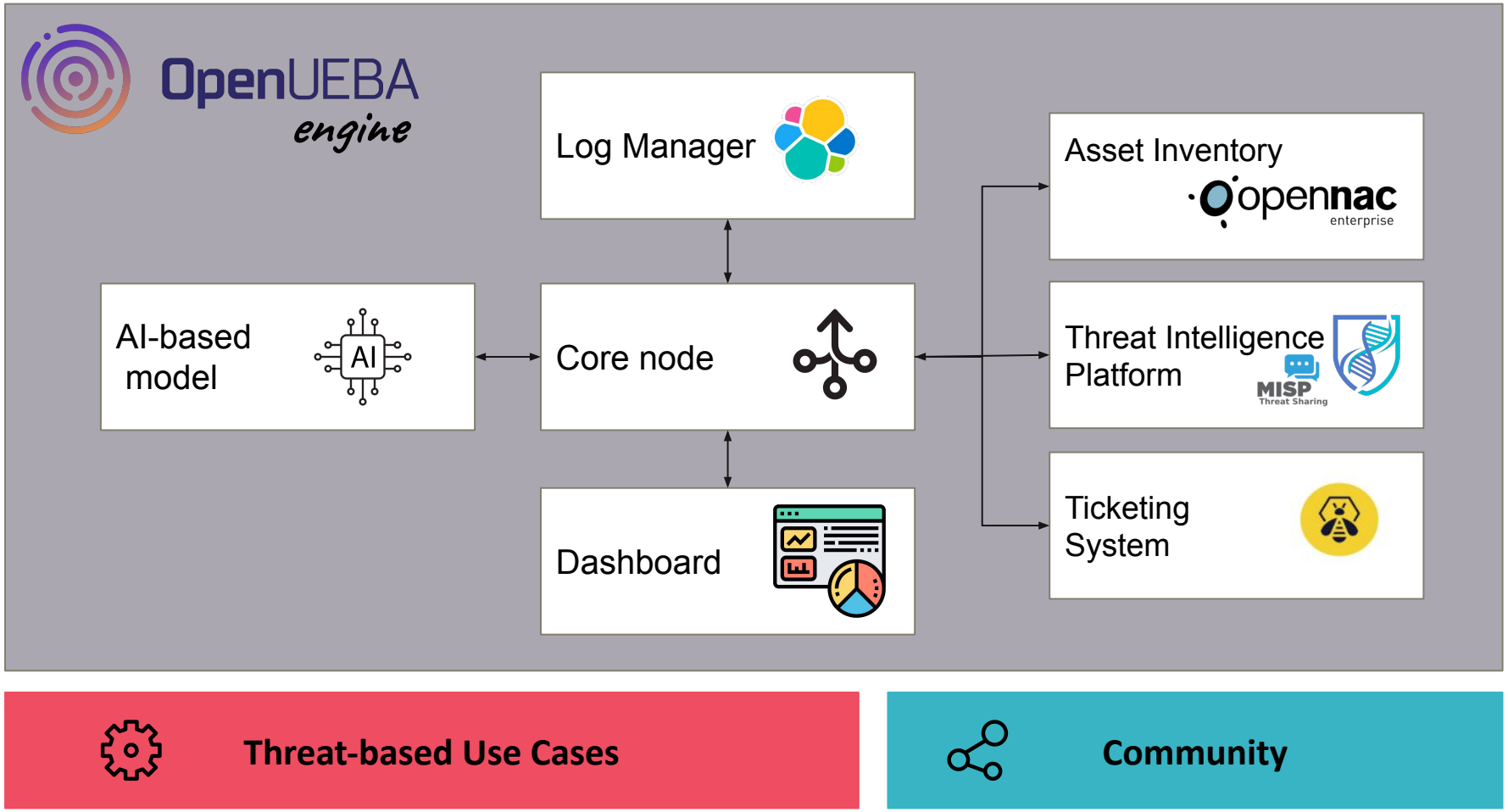
OSINT alignment

Open-source intelligence sources (OSINT) to enhance the profiles and allow the risk calculation of incoming threats.

Real-world validation

The framework is designed under a data-driven project and validated under two real-life test-bed.

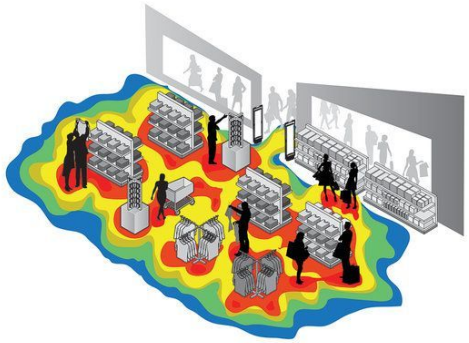
Open UEBA Framework

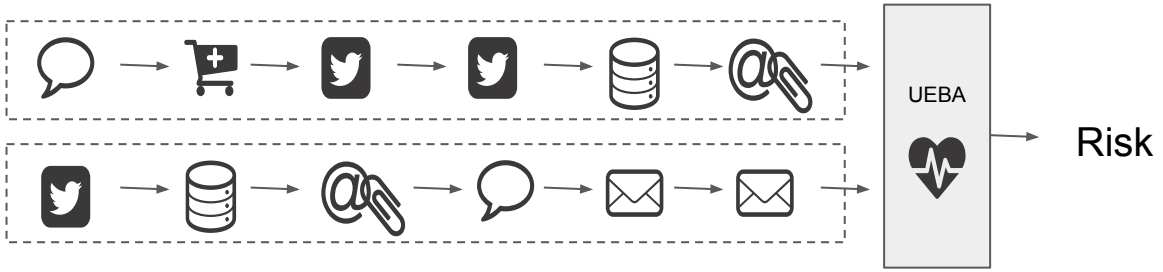


The AI behind openUEBA

Intro to UEBA

The foundations of **Behaviour analytics** rely on psychology, marketing and biology studies where it is modelled the behaviour to understand interactions to achieve objectives.



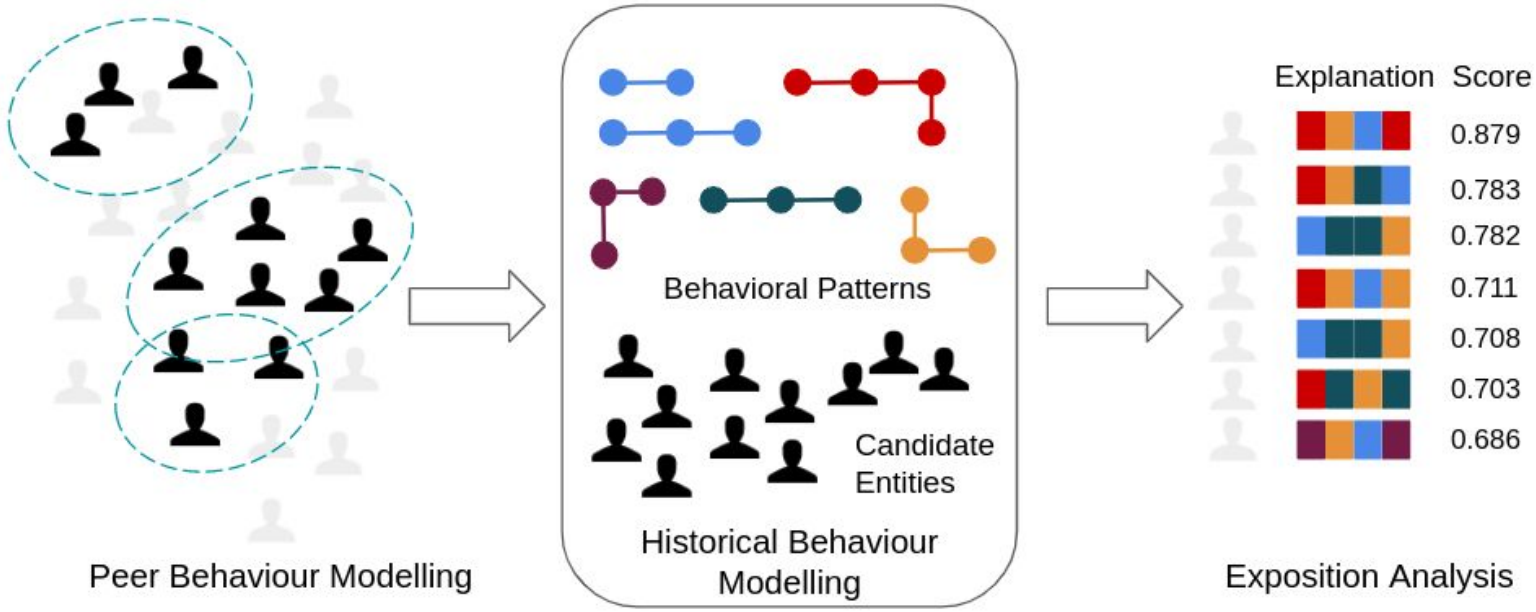


How machine learning could be used to detect potential threats analysing their behaviour?

UEBA techniques

Intro to UEBA

*OpenUEB*A learns the behaviour of entities and map to threats, allowing to predict the exposure and risk degree of a user towards a specific threat.



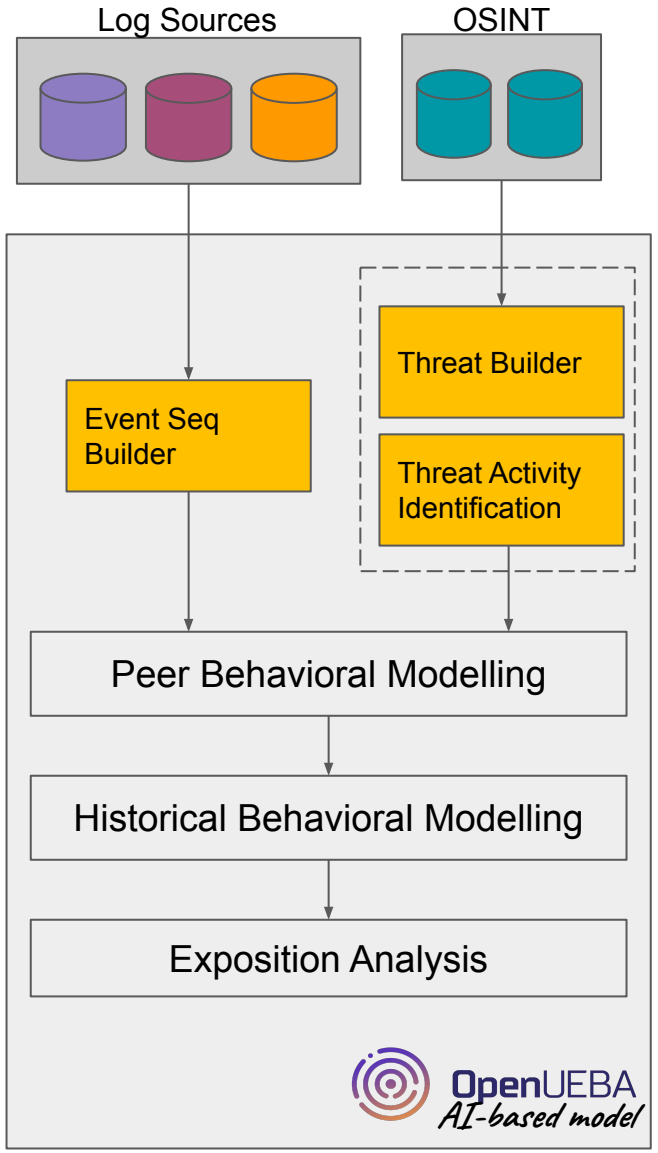
AI-based model

The following sources are considered:

- Network data: information captured with an on-premises hardware sensor in form of bro logs
- Endpoint data: endpoint information captured with an agent (similar to osquery)
- Application data: application logs or forwarded from a SIEM as a proxy
- Threat Intelligence (enrich sources) MISP queries

Event sequences representing entity behaviour at a current timestamp are built :

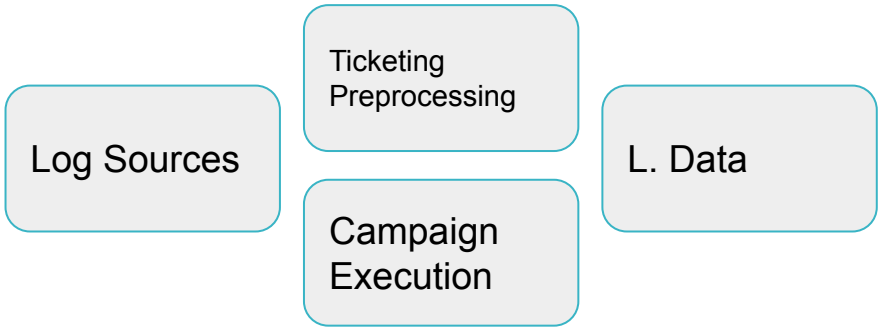
[@timestamp, entity-ID ,
protocols used, dns activity, tiny _url activy, …]

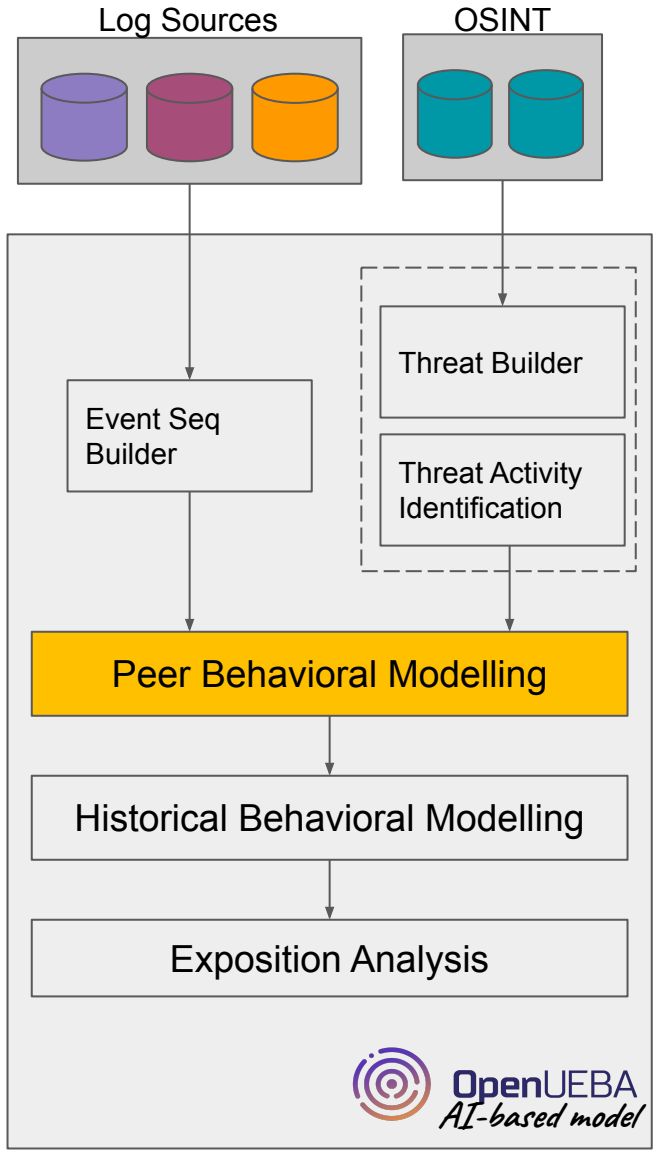


AI-based model

Peer Behavioral Modelling

We extract from all the entities, historical incidents and simulated attacks to tag entities and correlate them to specific threat information





AI-based model

Historical Behavioral Modelling

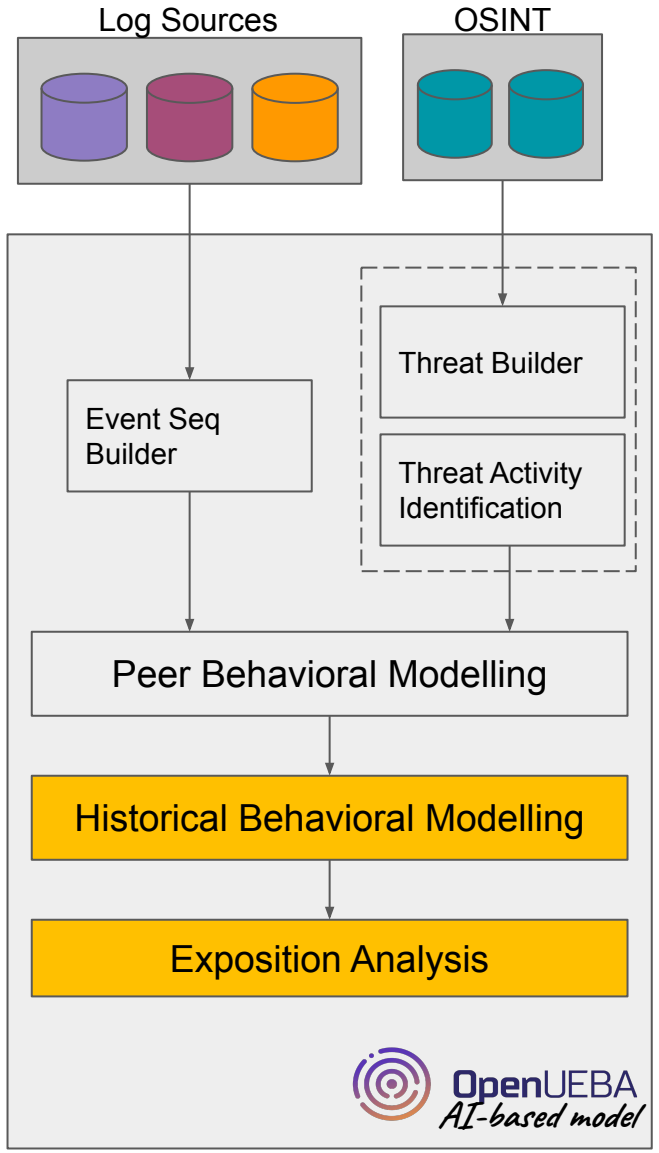
It is train a classification model allowing to find behavioral patterns characterising specific threats.

L. Data | Algorithm | Model $f(x)$

Exposition Analysis

The Machine Learning model allows to predict the risk exposition to other entities

Model $f(x)$ | Prediction | Risk Exposure



Threat Intelligence Platform

CTI Flow Schema

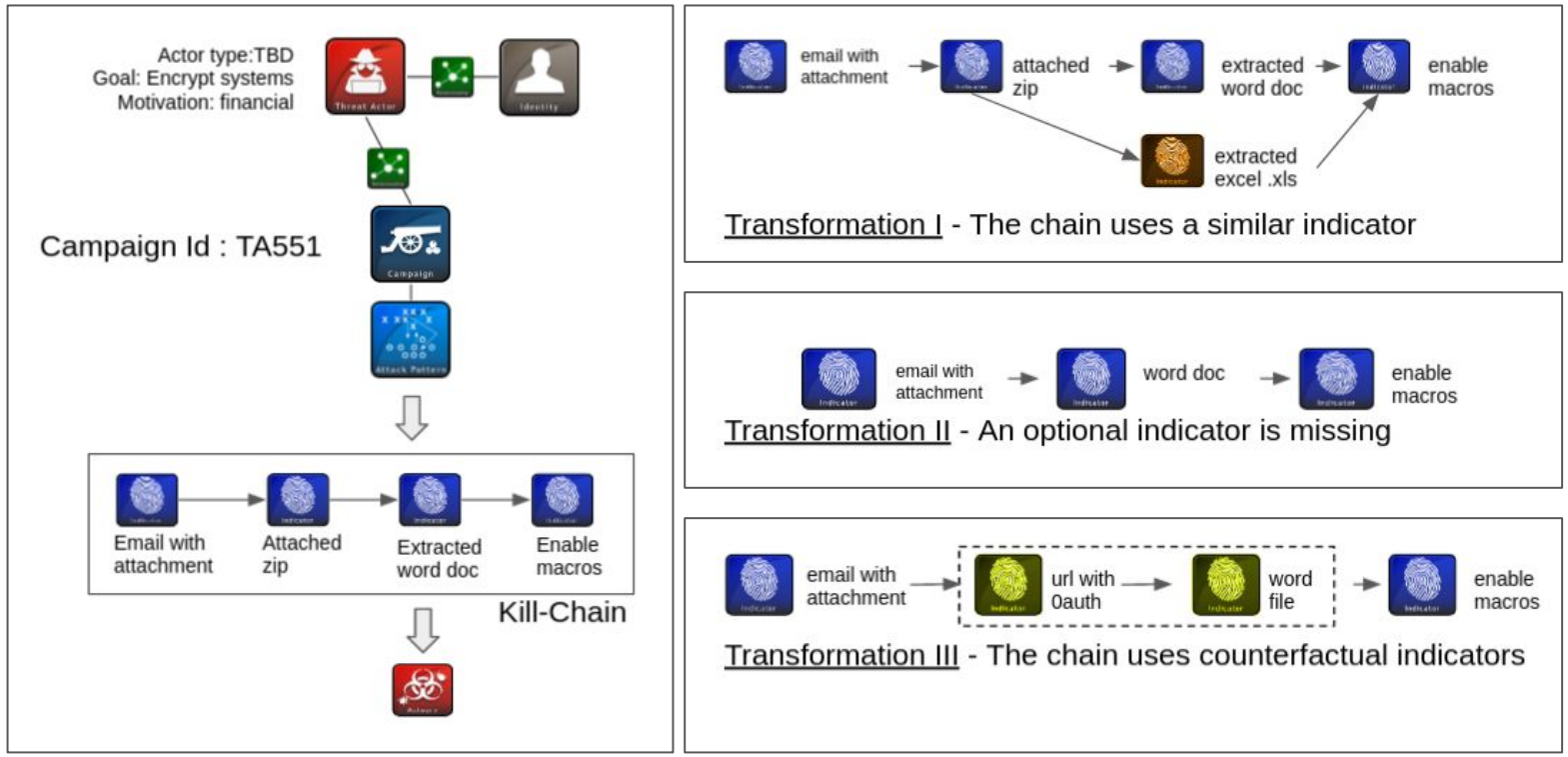
Enrich

Add mutations

Consume CTI

Threat Profiling

Threat Profiling process of extracting knowledge from Threat Intelligence sources and structure it as an indicators sequence.

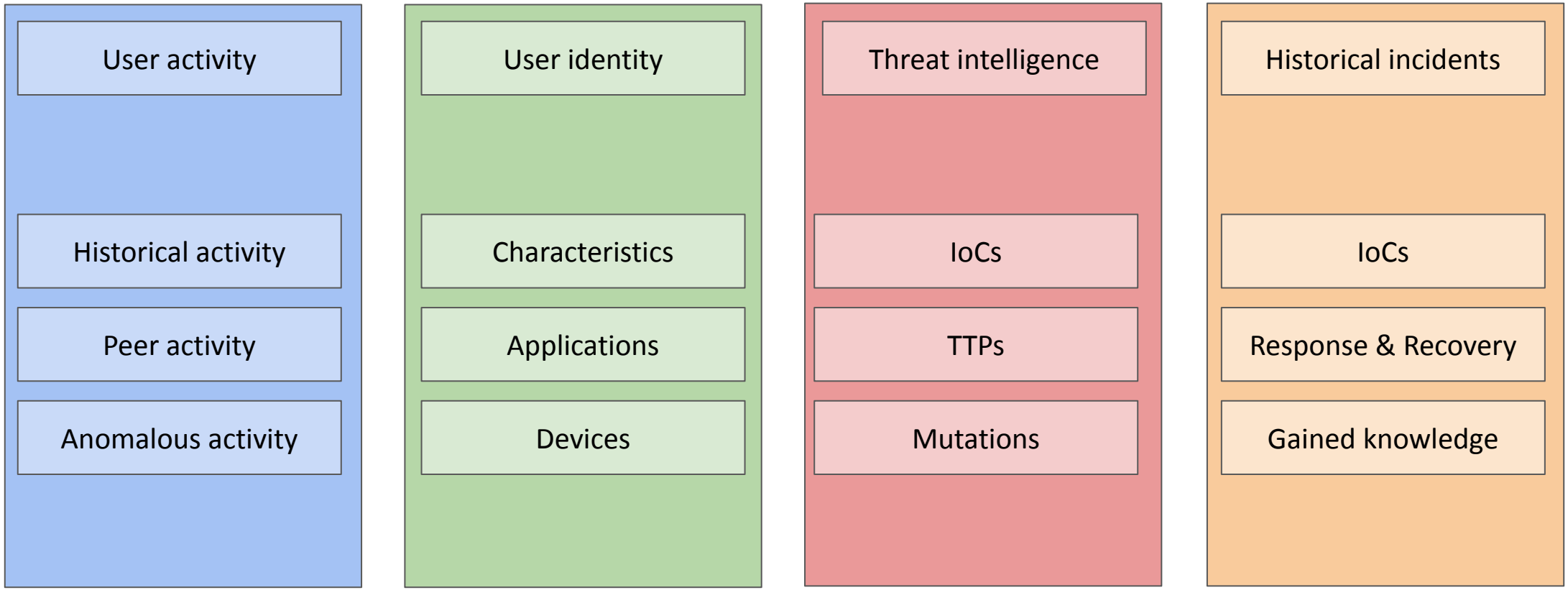


Use cases

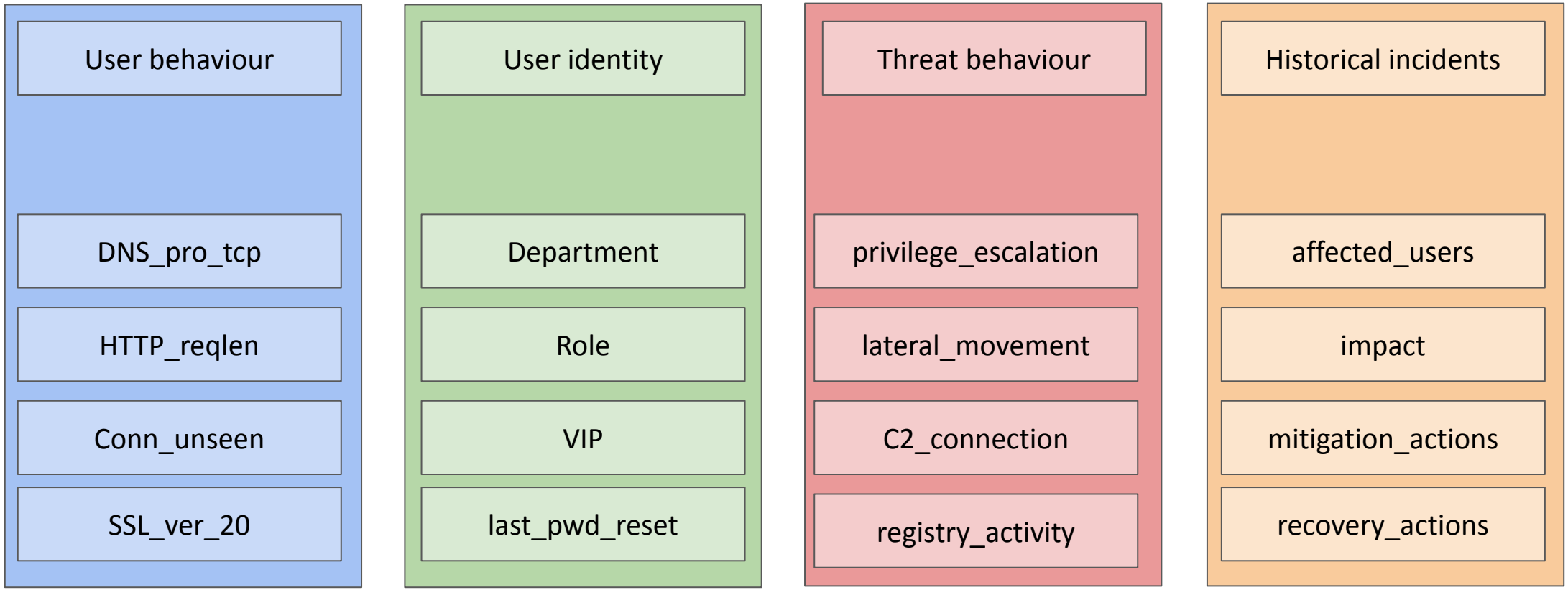
Use cases


1
Malware
2
www
Web-based attacks
3
Phishing
4
Web application attacks
5
Spam
TOP 15 CYBER THREATS
enisa
EUROPEAN UNION AGENCY FOR CYBERSECURITY
6
DDoS
7
Identity theft
8
Data breach
9
Insider threat
10
Botnets
11
Physical manipulation, damage, theft and loss
12
Information leakage
13
Ransomware
14
Cyberespionage
15
Cryptojacking

UC Phishing: Campaign model



UC Phishing: Campaign indicators

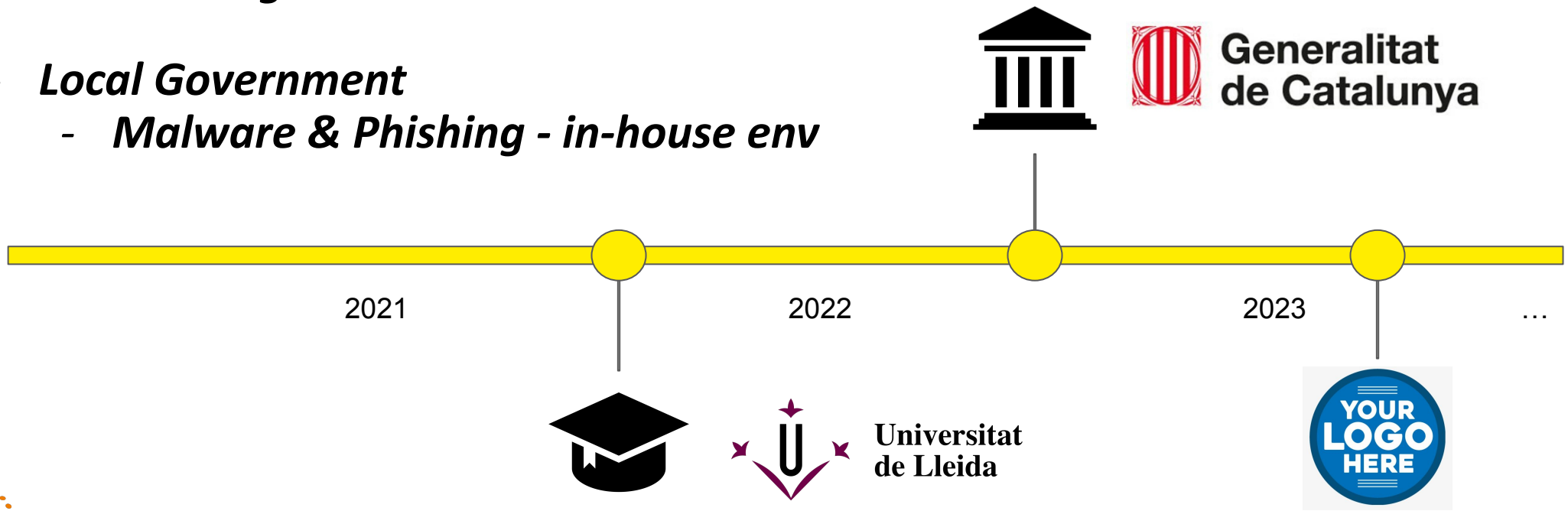


Demonstrators

Demonstrators

Current testbeds

- ***Universitat de Lleida***
  - ***Phishing Use Case - i2CAT env***
- ***Local Government***
  - ***Malware & Phishing - in-house env***



Validation

Phishing simulation

EU-CERTs Threat intelligence

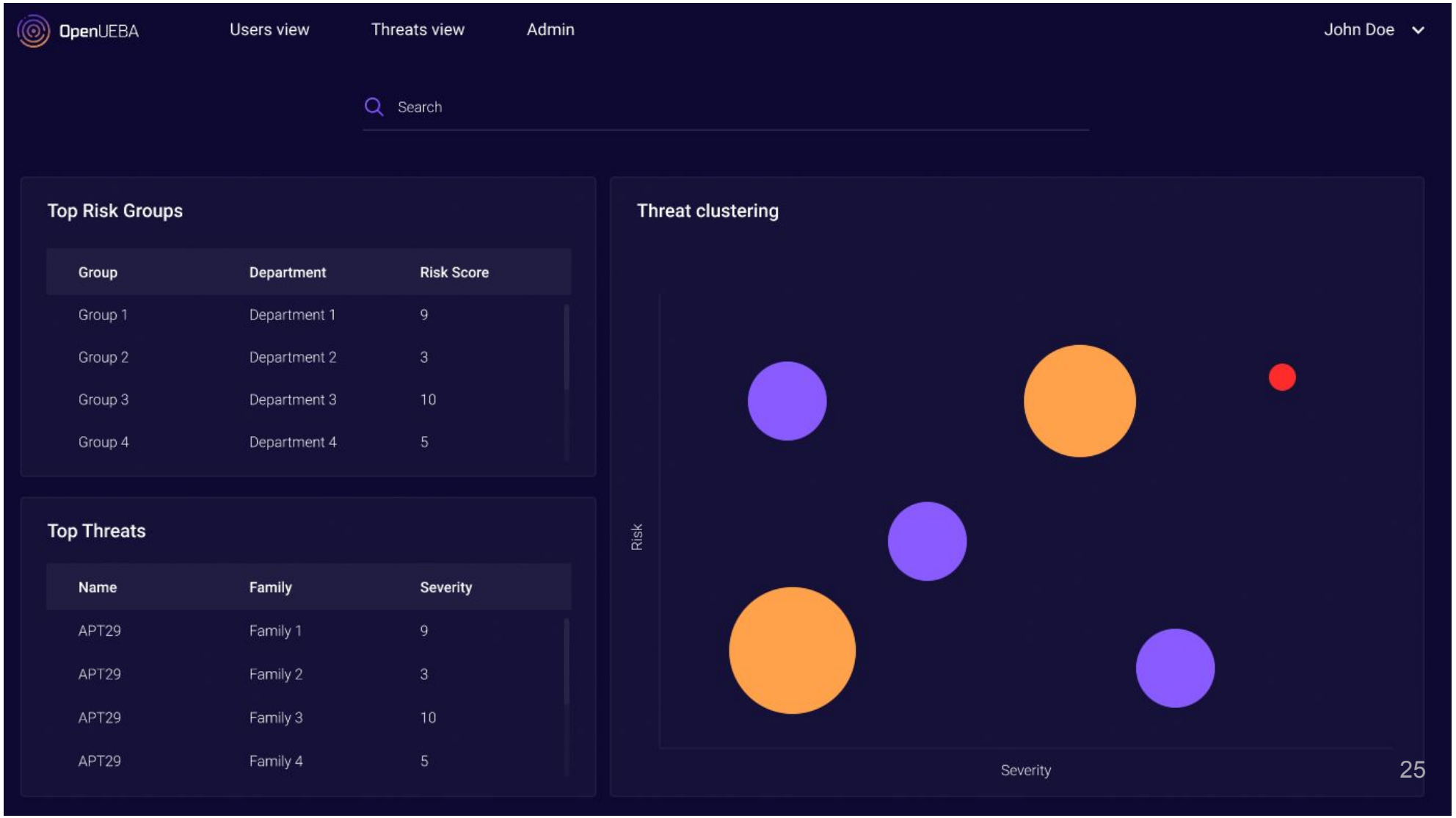
Expected KPIs

Reduced number of incidents

Reduced attack surface

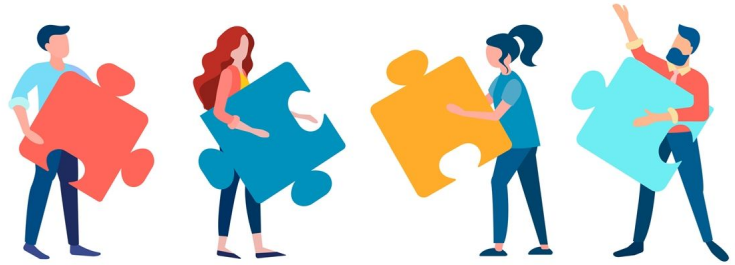
Reduced incident response time

Early UI


OpenUEBA
Users view
Threats view
Admin
John Doe
Search
Top Risk Groups
Group
Department
Risk Score
Group 1
Department 1
9
Group 2
Department 2
3
Group 3
Department 3
10
Group 4
Department 4
5
Top Threats
Name
Family
Severity
APT29
Family 1
9
APT29
Family 2
3
APT29
Family 3
10
APT29
Family 4
5
Threat clustering
Risk
Severity

Conclusions and getting involved

Conclusions



- OpenUEBA aims to disrupt current SOC capabilities with predictive capabilities.

- Getting involved into openUEBA community!
  - Let’s connect to growth the project
  - Collaboration (PoC with us)

SIEVA (INNOVATION PROGRAM)

or simply share …

Stay tuned !

openueba.org

contact@openueba.org

Linkedin group

Acknowledgements:

Generalitat de Catalunya
Departament de la Vicepresidència i de Polítiques Digitals i Territori

AGÈNCIA DE CIBERSEGURETAT DE CATALUNYA