i2cat R

The Internet Research Centre

Implementing PreventUEBA for risk assessment: Lessons Learned and Challenges

Nil Ortiz - Cybersecurity researcher
Albert Calvo - Artificial Intelligence researcher

11/12/2024

CERCA Centres de Recerca de Catalunya

tecnio catalonia | ACCIÓ Generalitat de Catalunya

Who we are

Albert Calvo

Research engineer | PhD Candidate

Trust-aware systems for cybersecurity and utilities domain

Msc. in Artificial Intelligence

albert.calvo@i2cat.net **LinkedIn**/in/albertcalvo/

Nil Ortiz

Senior R&D Cybersecurity engineer

Incident response and threat intelligence analysis

Msc. in Cybersecurity

nil.ortiz@i2cat.net **LinkedIn**/in/nilortiz/

About i2cat …

- **An interdisciplinary team of 200 members**
- **Different research areas with a focus on digital technologies**
- **We have contributed to 39 European projects and we have coordinated seven projects**

AI4CYBER Projects

Some of our relevant projects on the AI and CYBER ecosystem:

- **SIEVA (SIEM visibility assessment)** visibility to information log and classification into the MITRE ATT&CK Framework.

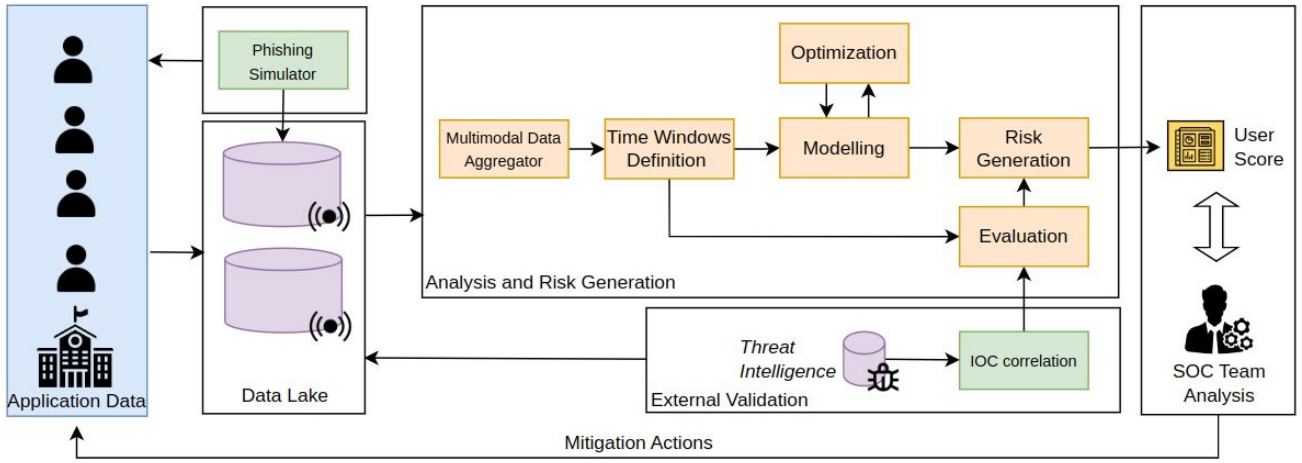
- **preventUEBA**: Calculate the user and entity exposure degree against specific threats through the power of CTI and AI working together.

- **detectUEBA:** Threat Detection capabilities with the power of SOTA Machine Learning methods.

PreventUEBA

The Data-driven Approach

- We have proposed a data-driven methodology that is developed following a CRISP-DM structure and is capable of gathering application logs from sources, training a classification model using labels from bad behaviors, and proposing a risk score to the SOC Team.
  - TestBed I (Real time data from a spanish regional University, 500k samples, 1772 different users).
  - TestBed II (Real time data from UPC University, 2 Million logs per day , 7 different alerts types, 1800 different users).

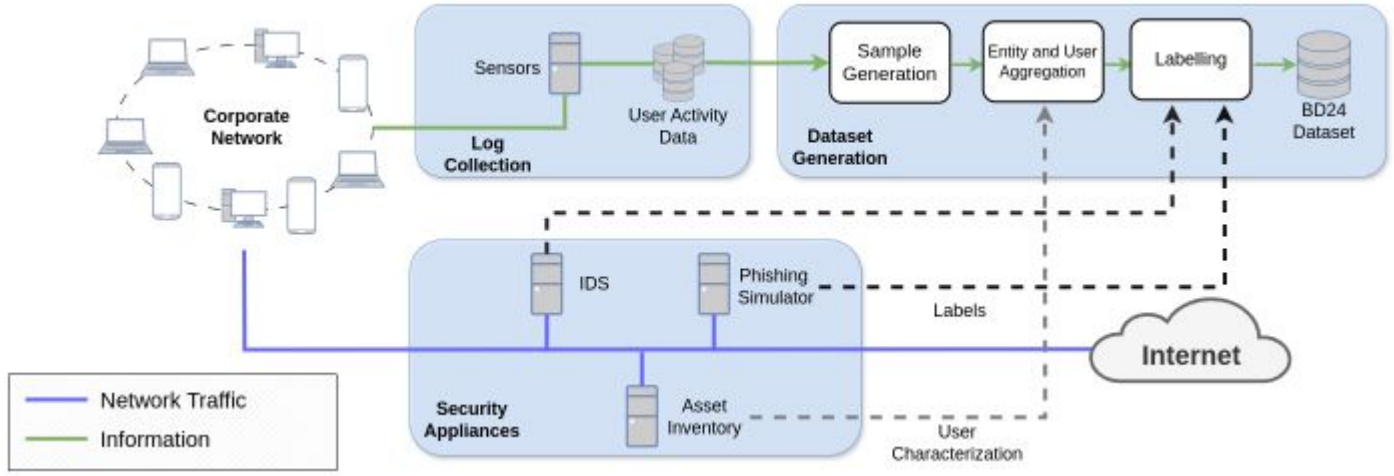


PreventUEBA

The Data Acquisition Architecture

To develop a data-driven approach for calculating the risk of a user being exposed to a specific threat.

- Extraction of different risk activities to model the user behaviour (Crypto, OutFlash, OutTLS, P2P, NonEnc …)
- It is proposed a Data Acquisition Architecture that extract multi-modal application logs from the corporate network for the later analysis



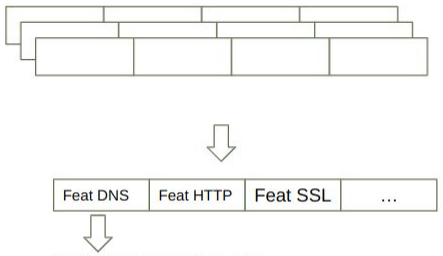
DatasetId	Risk Activity	Device	Benign (0) [#User/#Samples]	Risk (1) [#User/#Samples]
Crypto	Miner Checking	DE	738/161202	11/1343
		SM	613/180021	4/956
OutFlash	Outdated software	DE	738/161202	56/10820
		SM	613/180021	22/6639
OutTLS	Outdated TLS	DE	738/161202	18/2458
		SM	613/180021	11/2930
P2P	P2P Activity	DE	738/161202	177/35892
		SM	613/180021	94/21688
NonEnc	Non-encrypted	DE	738/161202	291/59943
		SM	613/180021	167/41434
Phishing	Phishing email	DE	98/13864	19/3072
		SM	117/34006	26/8968

PreventUEBA

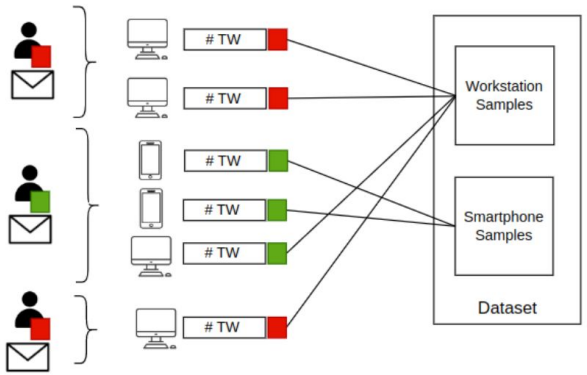
Multimodal Data Aggregation & Time windows definition & Prior Results

The time windows representation is a set of statistical features that summarizes the entity behaviour within a time interval

- The Phishing simulator allows to deliver phishing emails to users. We label the dataset according if they activate the breadcrumb (visit an url or activate a macro) and 15 days of historical data.
- In total, we launch and label users from three different phishing campaigns with the following results



- *ProtocolUsed*: protocol used during the time window, specifying the ratio between applications logs using TCP and UDP connections.
- *PortUsed*: ratio of DNS request privileging the port 5353 and 53. All queries not using the standard port could be addresses as unusual.
- *ReturnCode*: percentage of return codes is a feature that indicates whether a query has been completed successfully (RCODE: 0) or with errors (e.g. RCODE: 3 for "no such domain" or RCODE: 5 for "query refused").



Model Configuration I

	Smartphone			Workstation			Both		
	TW L: 3	TW L: 6	TW L: 12	TW L: 3	TW L: 6	TW L: 12	TW L: 3	TW L: 6	TW L: 12
F-score	0.60	0.67	0.70	0.72	0.73	0.68	0.63	0.49	0.56
Specificty	0.70	0.72	0.84	0.91	0.68	0.69	0.75	0.42	0.65
Accuracy	0.64	0.67	0.75	0.80	0.74	0.72	0.70	0.49	0.57

Model Configuration II

	Smartphone			Workstation			Both		
	TW L: 3	TW L: 6	TW L: 12	TW L: 3	TW L: 6	TW L: 12	TW L: 3	TW L: 6	TW L: 12
F-score	0.67	0.60	0.58	0.63	0.69	0.70	0.46	0.53	0.51
Specificty	0.70	0.50	0.61	0.72	0.73	0.84	0.44	0.61	0.65
Accuracy	0.69	0.60	0.59	0.59	0.70	0.71	0.47	0.54	0.54

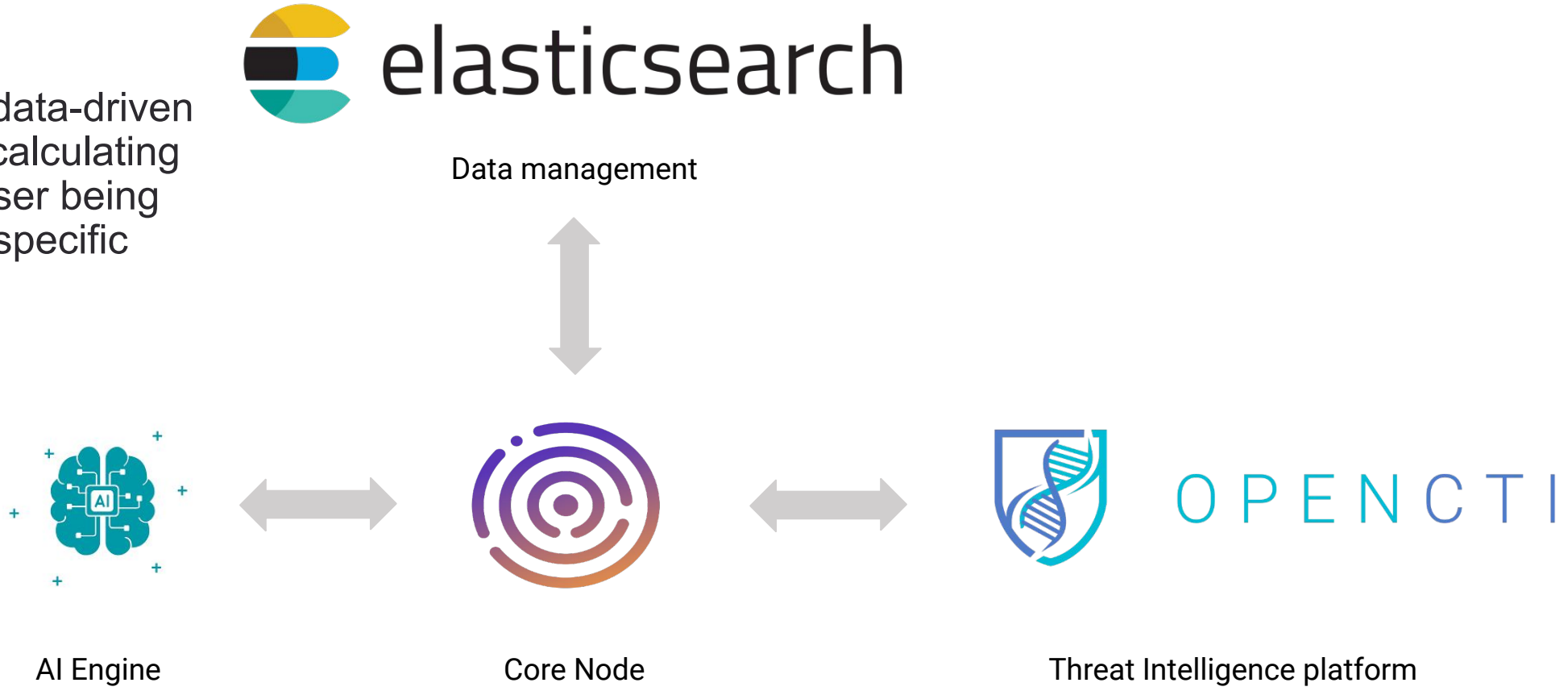
Model Configuration III

	Smartphone			Workstation			Both		
	TW L: 3	TW L: 6	TW L: 12	TW L: 3	TW L: 6	TW L: 12	TW L: 3	TW L: 6	TW L: 12
F-score	0.57	0.70	0.58	0.60	0.79	0.71	0.67	0.47	0.68
Specificty	0.76	0.68	0.81	0.67	0.92	0.80	0.80	0.51	0.80
Accuracy	0.64	0.70	0.68	0.65	0.80	0.72	0.71	0.48	0.71

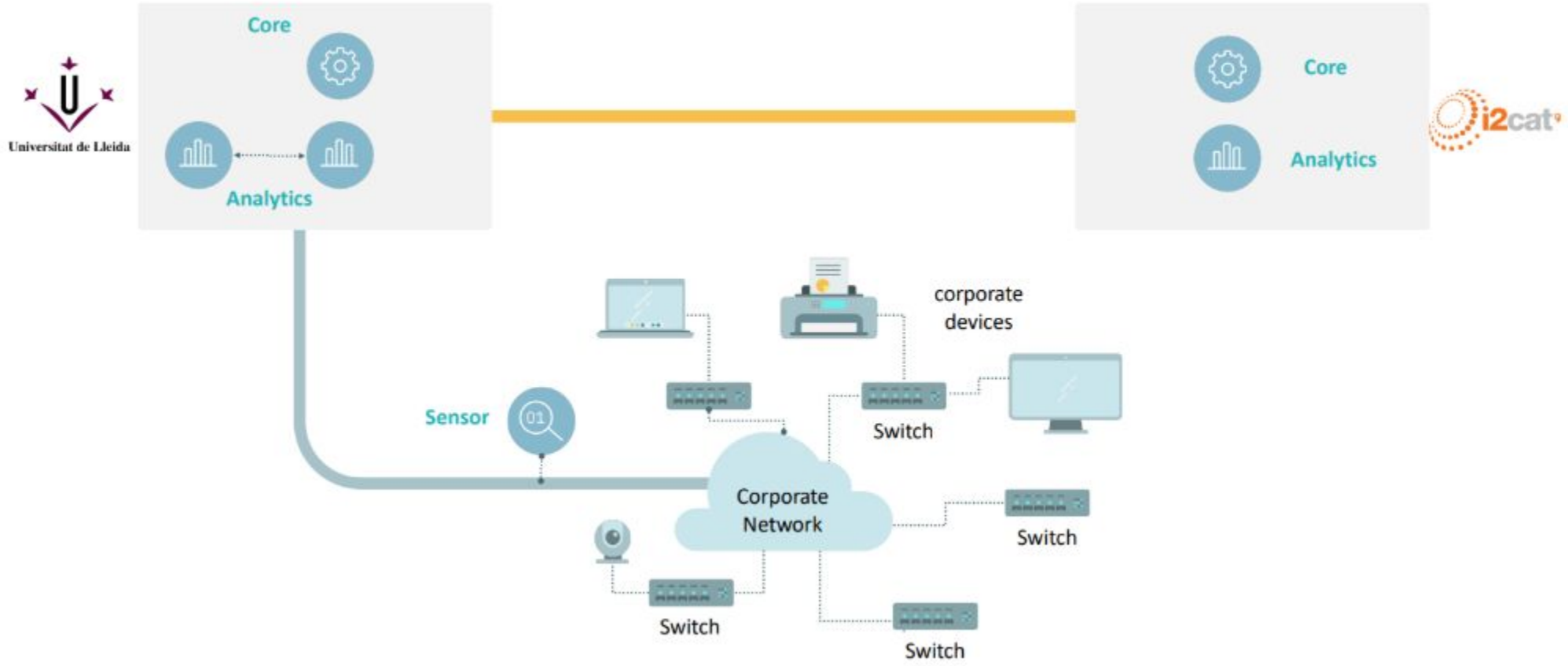
A. Calvo, S. Escuder, J. Escrig, M. Arias, N. Ortiz and J. Guijarro, "A Data-driven Approach for Risk Exposure Analysis in Enterprise Security," *2023 IEEE 10th International Conference on Data Science and Advanced Analytics (DSAA)*, Thessaloniki, Greece, 2023, pp. 1-9, doi: 10.1109/DSAA60987.2023.10302480.

PreventUEBA

To develop a data-driven approach for calculating the risk of a user being exposed to a specific threat.



Deployment scenario



Challenges

Lack of data gathering & monitoring tool stack

Data Readiness for AI

Findings Validation Complexity

Data privacy concerns

Lessons learned

Having a data plan is essential

Start with Validation Metrics in Mind

Stakeholder Communication Matters

Invest in Explainable AI

i2cat

The Internet Research Centre

Thank you!

Gran Capità, 2-4
Nexus I Building, 2nd Floor
08034 Barcelona
Tel. (+34) 935 532 510

X/Twitter | Linkedin | YouTube