Metrics for community dynamics applied to unsupervised attacks detection

Icube - Laboratoire des sciences de l'ingénieur,de l'informatique et de l'imagerie, UMR 7357 Université de Strasbourg, 67000 Strasbourg, France;

Laboratoire de Recherche de L'EPITA (LRE),
14-16 rue Voltaire, 94270 Le Kremlin-Bicètre, France

julien.michel@epita.fr

Directed by Pierre Parrend

Julien MICHEL
28/06/2023

Context

BIG DATA :

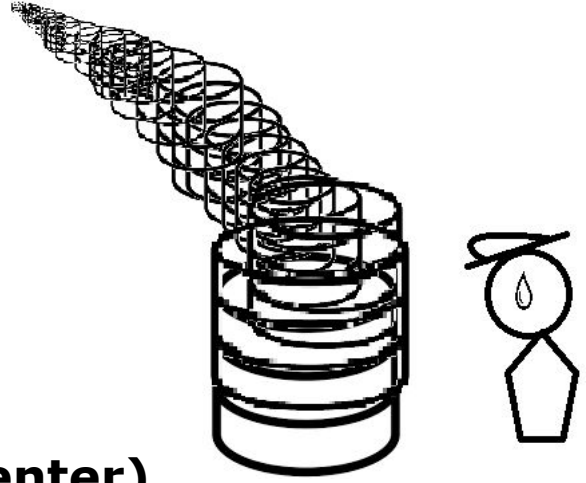
How to manage an ever increasing amount of data ?

A.I. ?

A.I. CHALLENGES :

- Scalability
- Explainability
- Time robustness

Problem definition



Core network Data

Continuous Data Stream

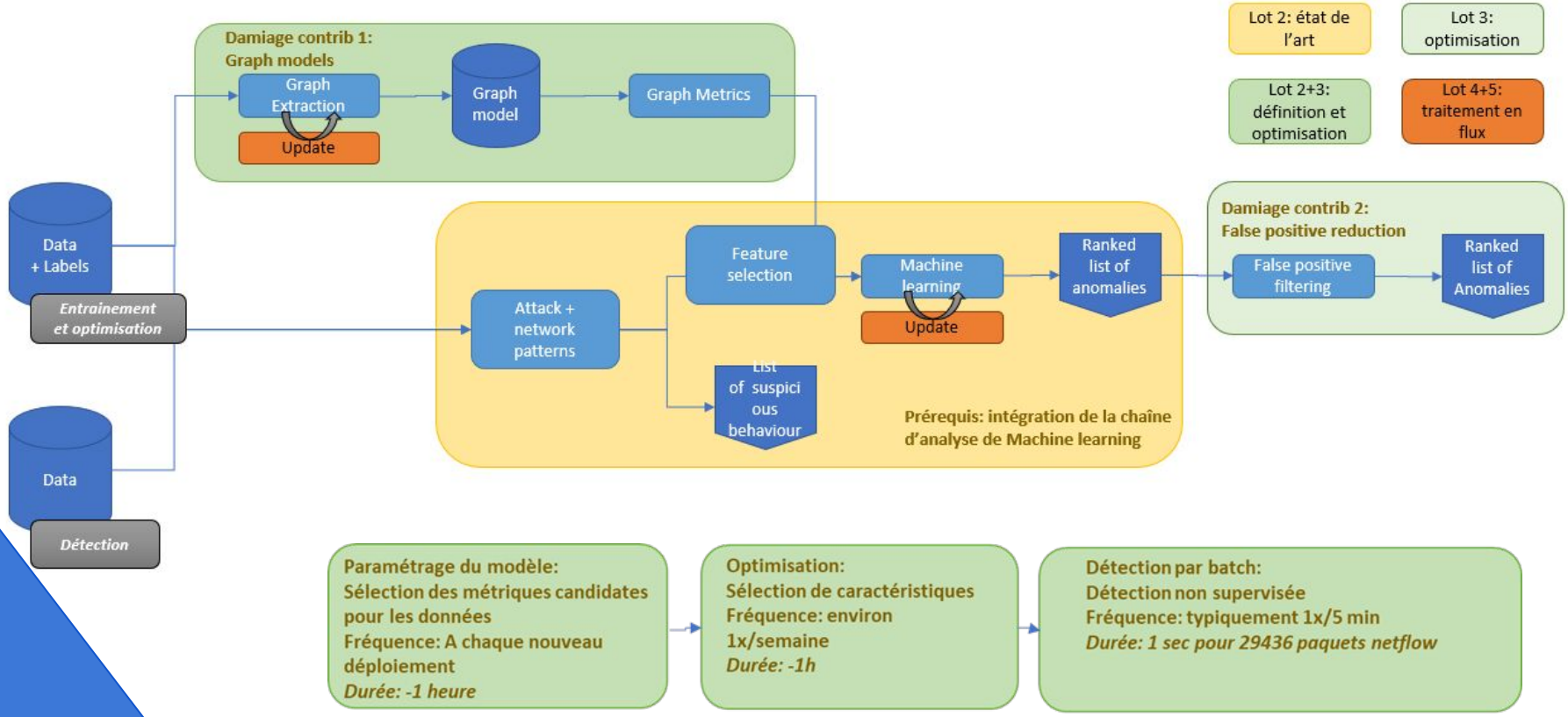
DAMIAGE PROJECT

To help analyst in SOC (security operating center)

Constraints !!!

- New data have to be processed
- Data behaviours change with time
  = **Concept drift**
- Ever increasing amount of data

Data analysis and processing chain



Unsupervised attacks detection

Principals characteristics :

- **Opposed to supervised approaches**
- **Do not make use of target label**

Why ?

At any time we may not have any prior knowledge to attacks we want to detect

A new model is generated for any detection which may prove more secure

But important limits :

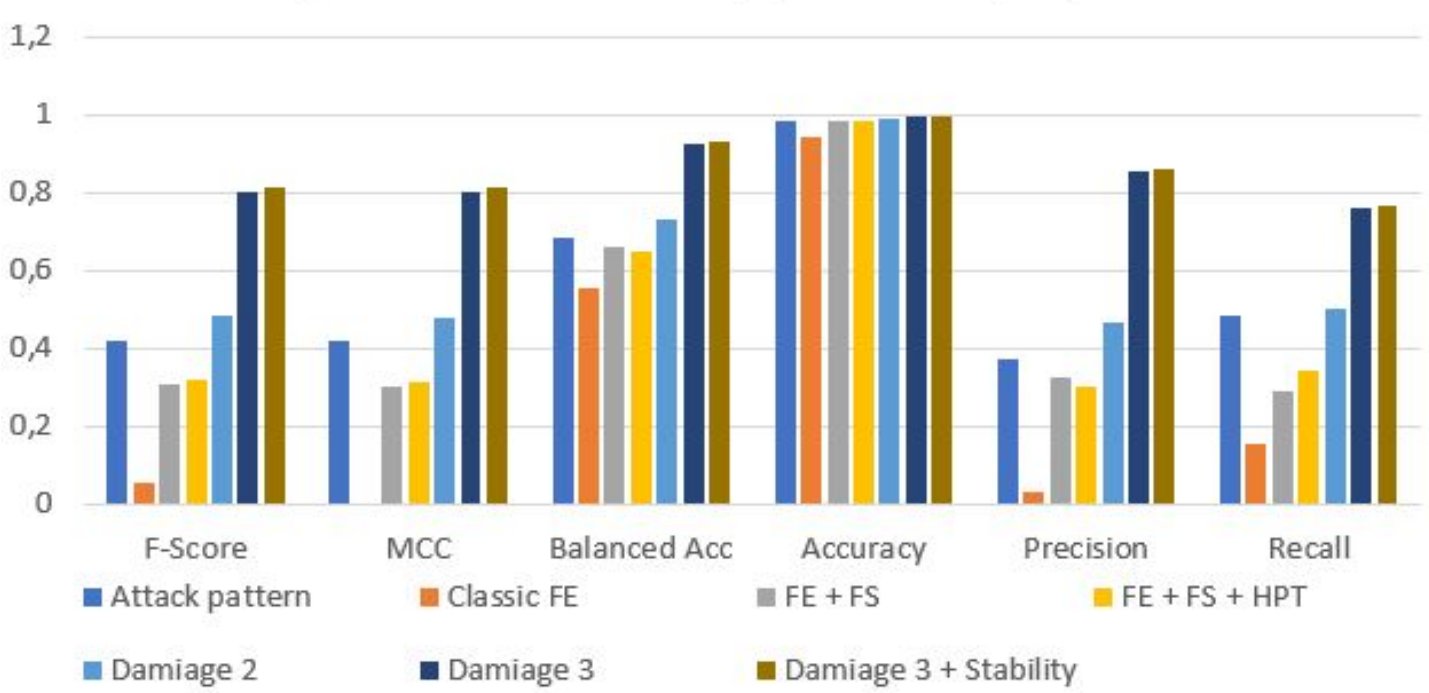
- Very sensitive to statistical anomalies
- Depending on the approach, it may prove hard to detect different types of attacks
- High false positive rate

UGR’16 Dataset

Date time	Duration	Source IP	Destination IP	Source Port	Destination Port	Protocol	Flag	Forwarding status	ToS	Packets	Bytes	Label
2016-07-27 13:43:29	0.0	143.72.8.137	42.219.158.161	53	43192	UDP	.A....	0	0	1	214	background
2016-07-27 13:43:29	0.0	42.219.154.119	143.72.8.137	60185	53	UDP	.A....	0	0	1	72	background
2016-07-27 13:43:30	0.0	42.219.154.107	143.72.8.137	48598	53	UDP	.A....	0	0	1	77	background
2016-07-27 13:43:30	0.0	42.219.154.98	143.72.8.137	51465	53	UDP	.A....	0	0	1	63	background
2016-07-27 13:43:30	0.0	43.164.49.177	42.219.155.26	80	37934	TCP	.A...F	0	0	1	52	background

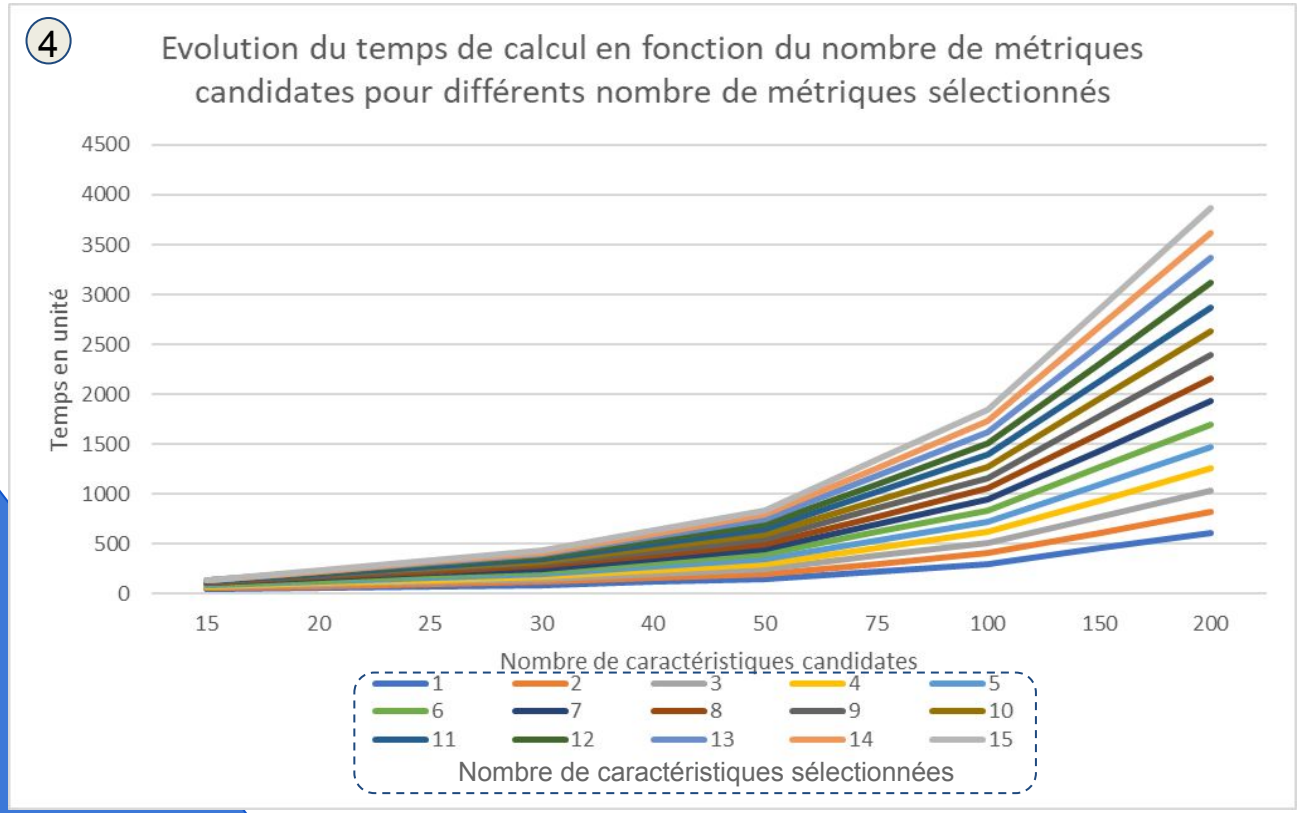
- Background data gathered from march to august 2016
- Simulated attacks from the last week of july and august in the background data. (DoS and Port Scan)
- Re-inserted some attacks detected using anomaly detection . (Spam and Botnet)
- Some unnoticed attacks may still be labelled as background

Results



Detection score depending on the method using isolation forest algorithm on the same sample of data of the UGR'16 dataset

Scalability evaluation



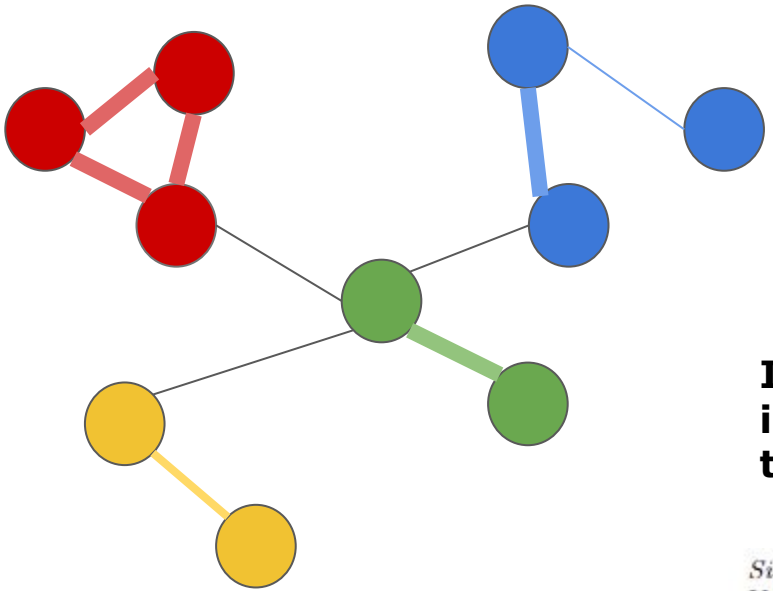
On cherche m caractéristiques sélectionnées parmi n caractéristiques candidates.

Complexité bornée par O(n) et O(n²).

$$\Omega\left((\mathbf{n}\times 2 - 1)\times \mathbf{d}\right)$$

$$O\left(\frac{n\times(n+1)}{2}\times \mathbf{d}\right)$$

Graph community



Groups of nodes more connected to each others than to the other nodes of the graph.

In general a graph partition is obtained by maximizing the modularity.

$Size_i$: Number of nodes in community i
V_{all} : The number of nodes in the graph

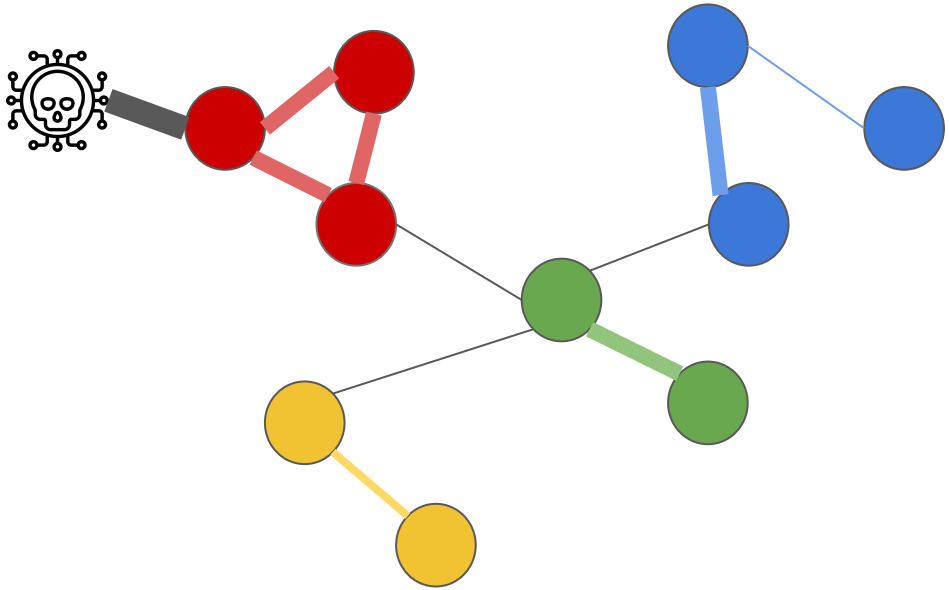
$$Mod = Cov - \frac{\sum \frac{M_{all}}{V_{all}^2} . Size_i^2}{M_{all}}$$

M_{in} : The number of edge with both vertex in same community
M_{all} : The number of edge in the graph

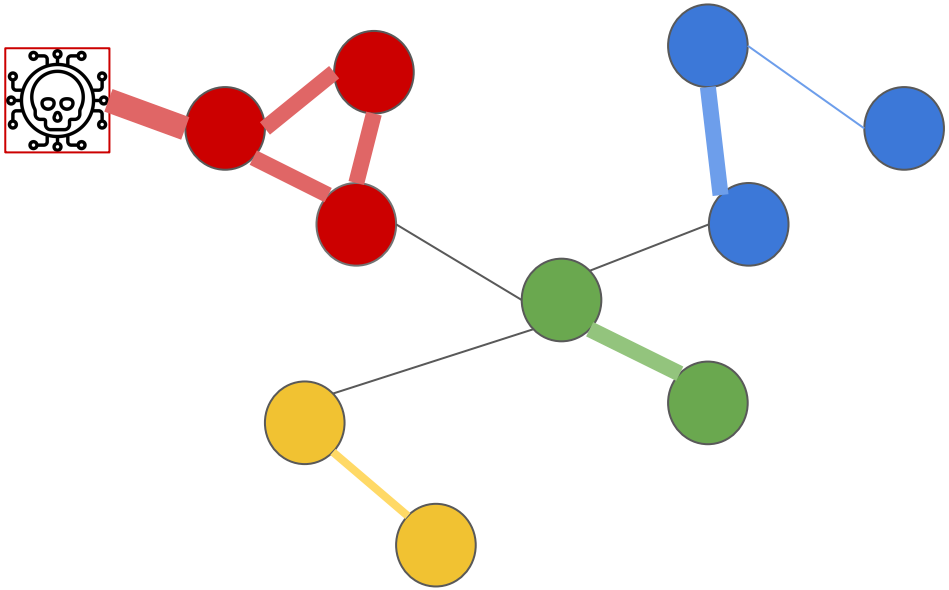
$$Cov = \frac{M_{in}}{M_{all}}$$

[9] H. S. Pattanayak, H. K. Verma, and A. L. Sangal, "Community detection metrics and algorithms in social networks," in 2018 First International Conference on Secure Cyber Computing and Communication (ICSCCC) 2018, pp. 483–489.

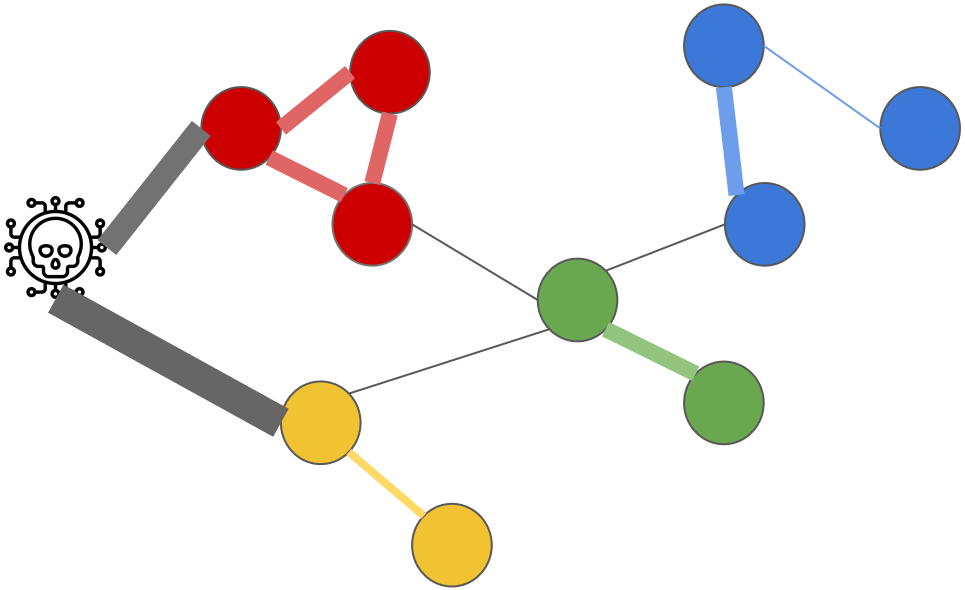
Why Graph community ?



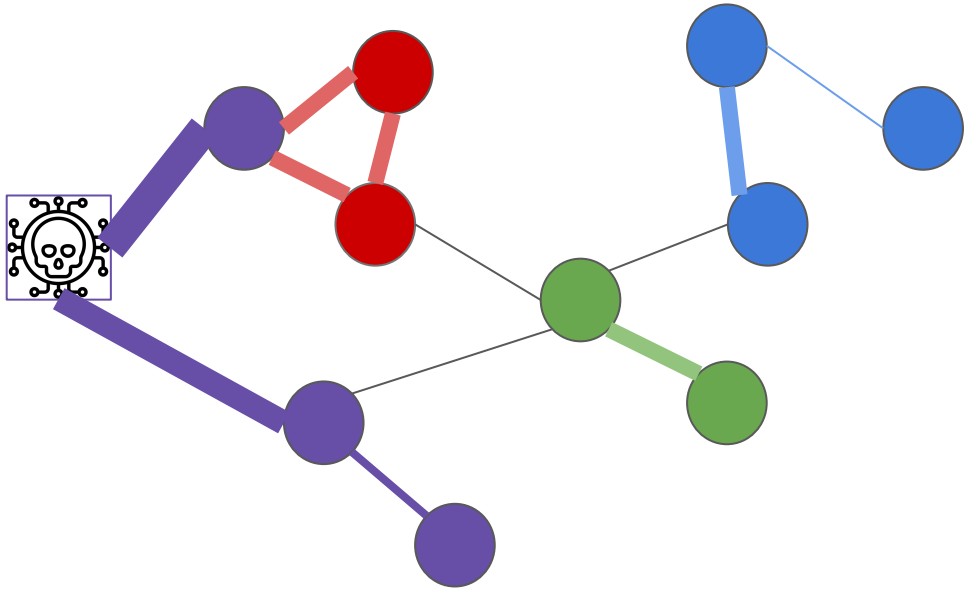
Why Graph community ?



Why Graph community ?

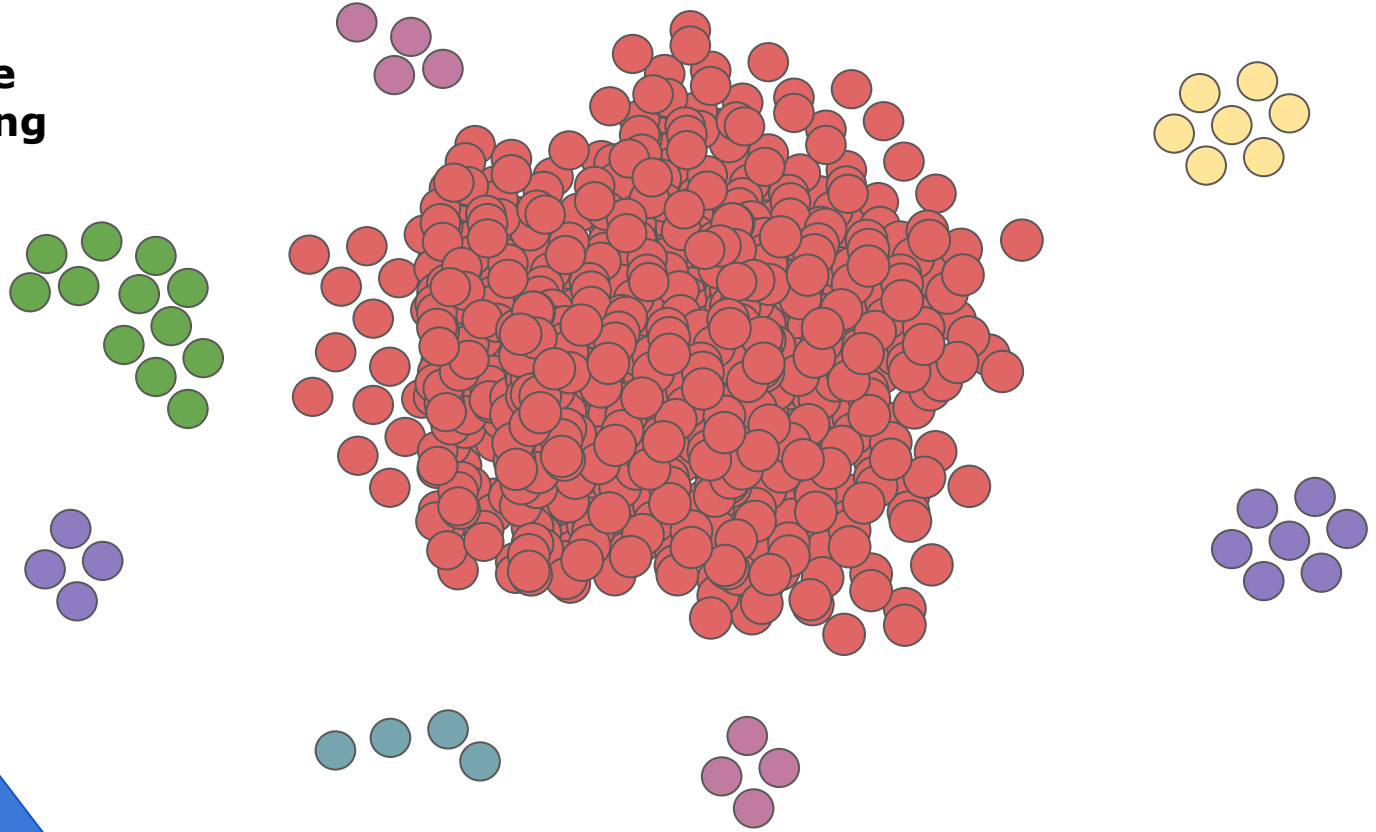


Why Graph community ?



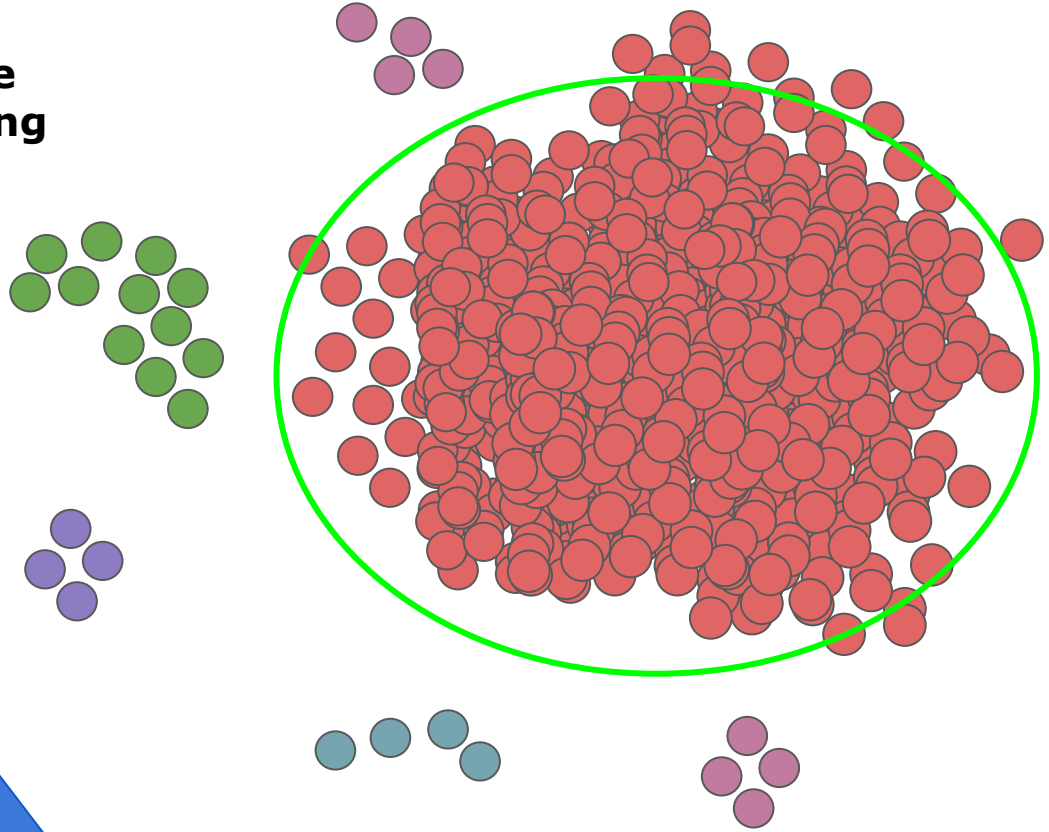
Why Graph community metrics ?

A simple clustering



Why Graph community metrics ?

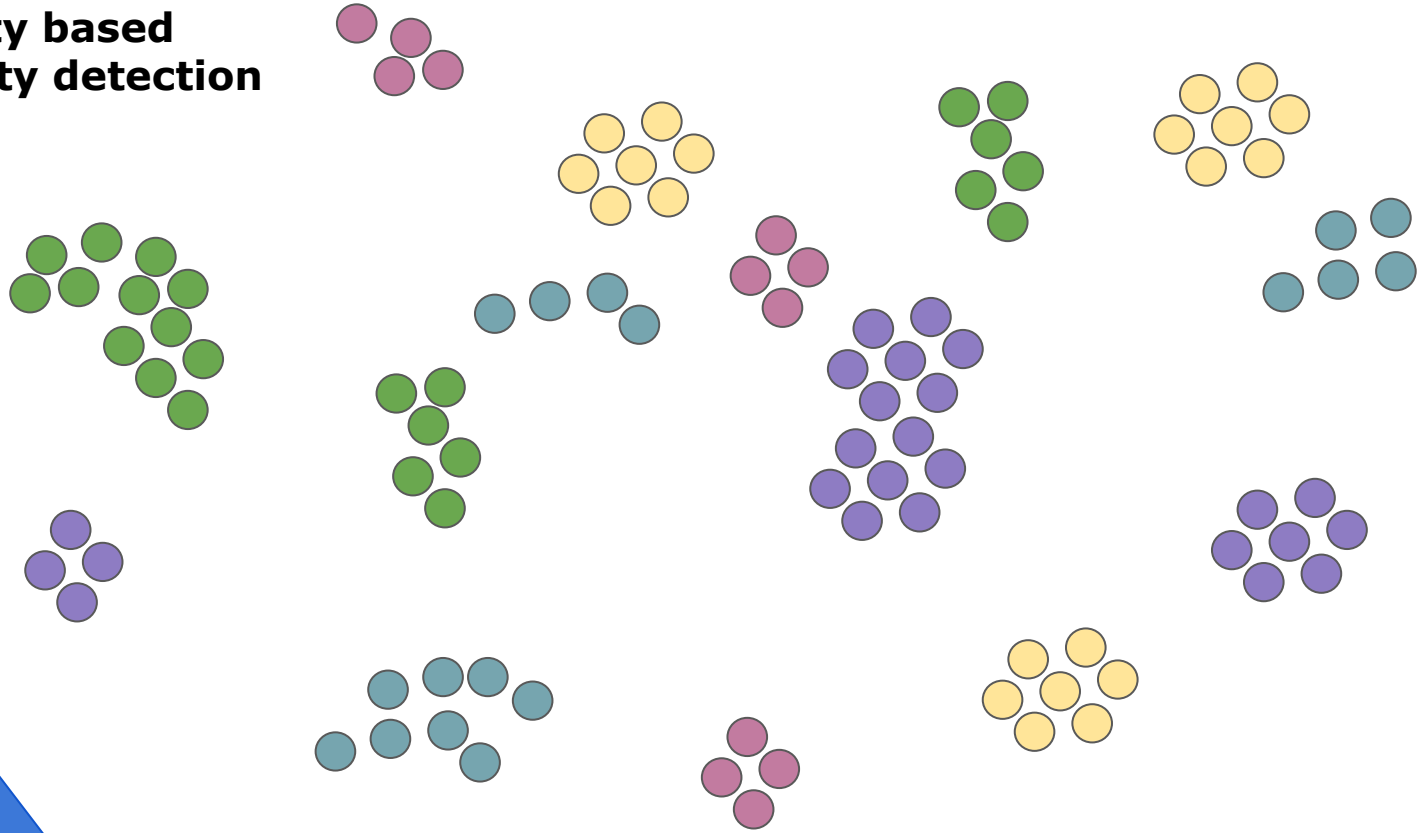
A simple clustering



Most of the attacks are in there !!!

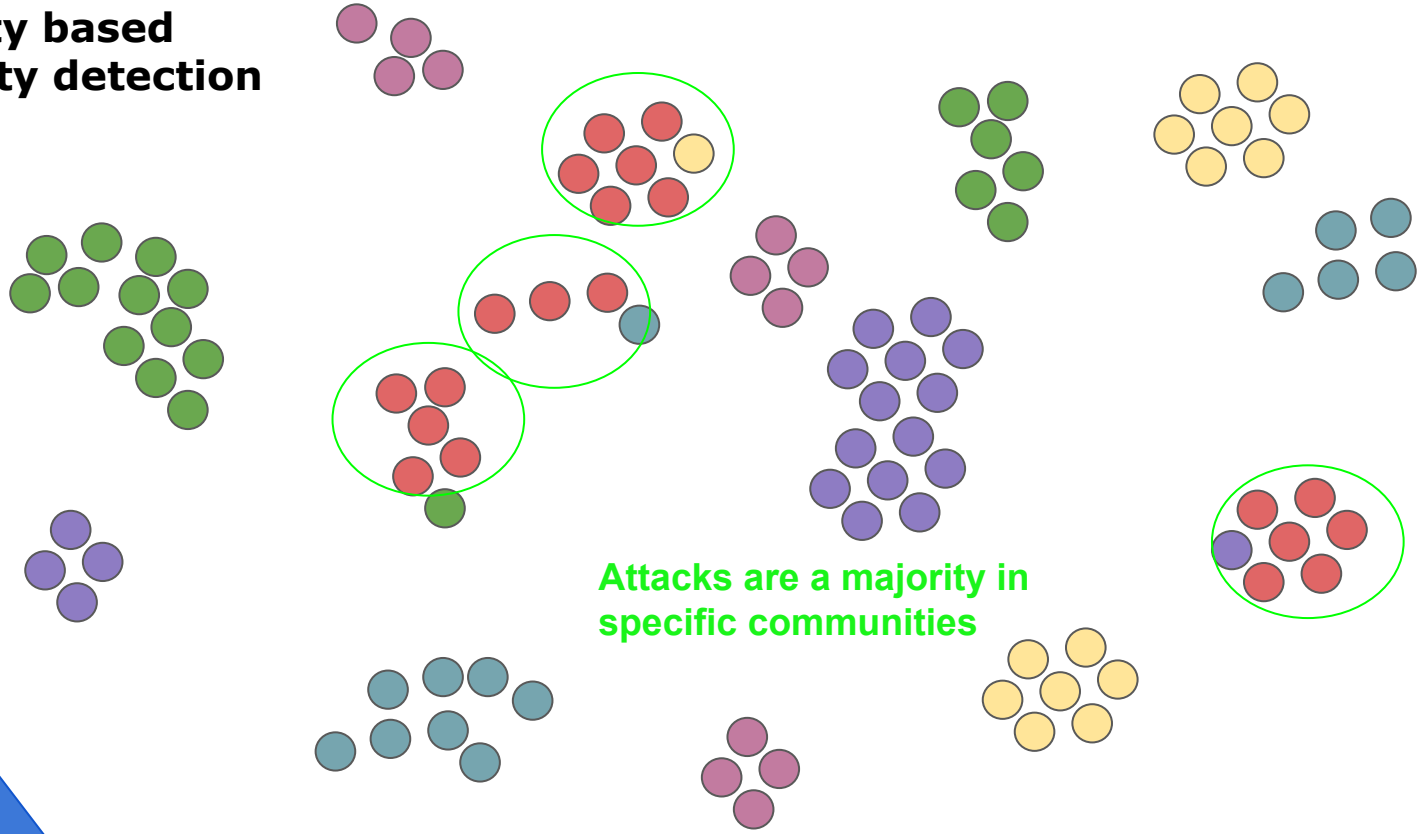
Why Graph community metrics ?

Modularity based community detection



Why Graph community metrics ?

Modularity based community detection



Why Graph community metrics ?

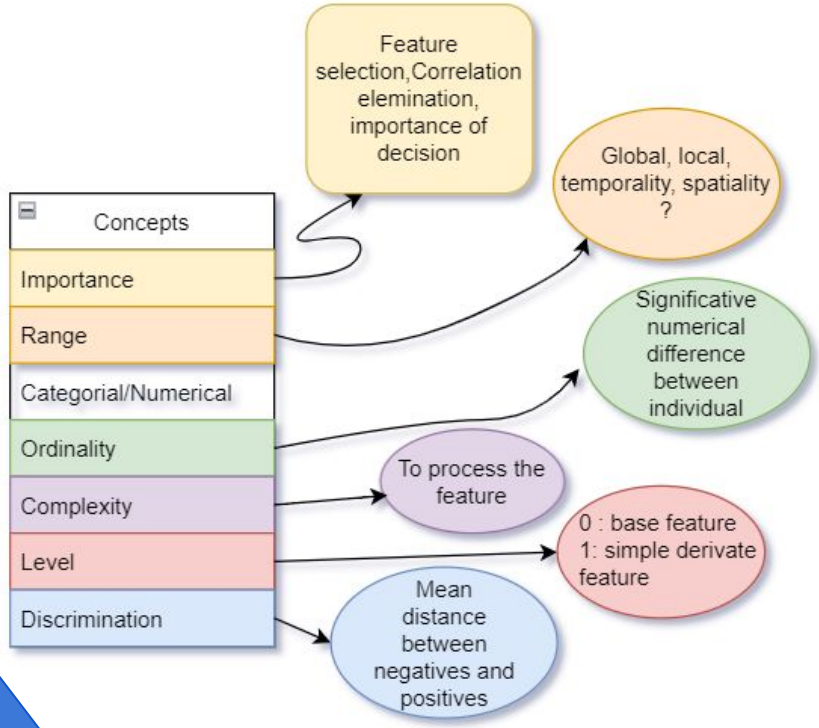
How to find in which community are the attacks ?

We need to find a way to discriminate the communities (example : [10] J.-H. Park and H.-Y. Kwon, “Cyberattack detection model using community detection and text analysis on social media, ”ICT Express, vol. 8, no. 4, pp. 499–506, 2022.)

What we know :

- **We used modularity to make the community partition**
- **Modularity is calculated using topological information of the graph.**
- **Attacks are a majority inside the same community => Topological information linked to each community could be used to discriminate the communities from each other ?**

Why Graph community metrics ?



- Features are an important aspect if not the most important in anomalies detection.
- You need to keep only relevant features
- They need to discriminate positive and negative
- They need to be computable in your study case

Why Graph community metrics ?

Unsupervised detection algorithms need to be fed the right features and only the right features !!!

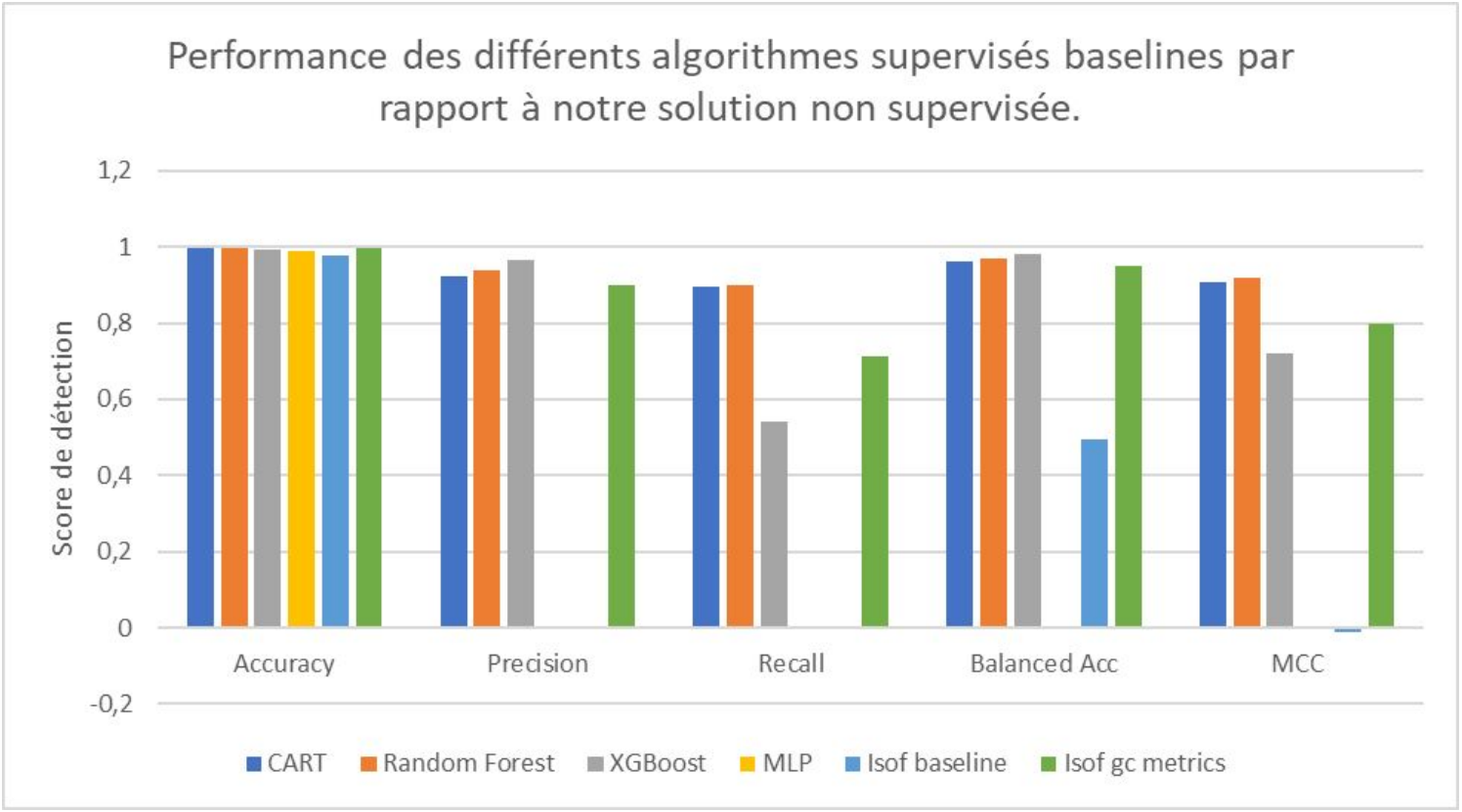
How do you make attacks different from normal data ?

Graph representation is commonly used for network data
→ Topological informations

Attacks will have an impact on part of the topology of the network
→ part of the graph are the community

=> graph community metrics can be used as indicators

Results


Performance des différents algorithmes supervisés baselines par rapport à notre solution non supervisée.
Score de détection
1,2
1
0,8
0,6
0,4
0,2
0
-0,2
Accuracy
Precision
Recall
Balanced Acc
MCC
CART
Random Forest
XGBoost
MLP
Isof baseline
Isof gc metrics

Graph Processing for Machine Learning

Actuellement primairement composé de 2 fonctions :

- *gc_metrics_first_order(G)*
  out : fo_metrics_c, fo_metrics_g
- *gc_metrics_second_order(fo_metrics_c,fo_metrics_g)*
  out: so_metrics_c,so_metrics_g

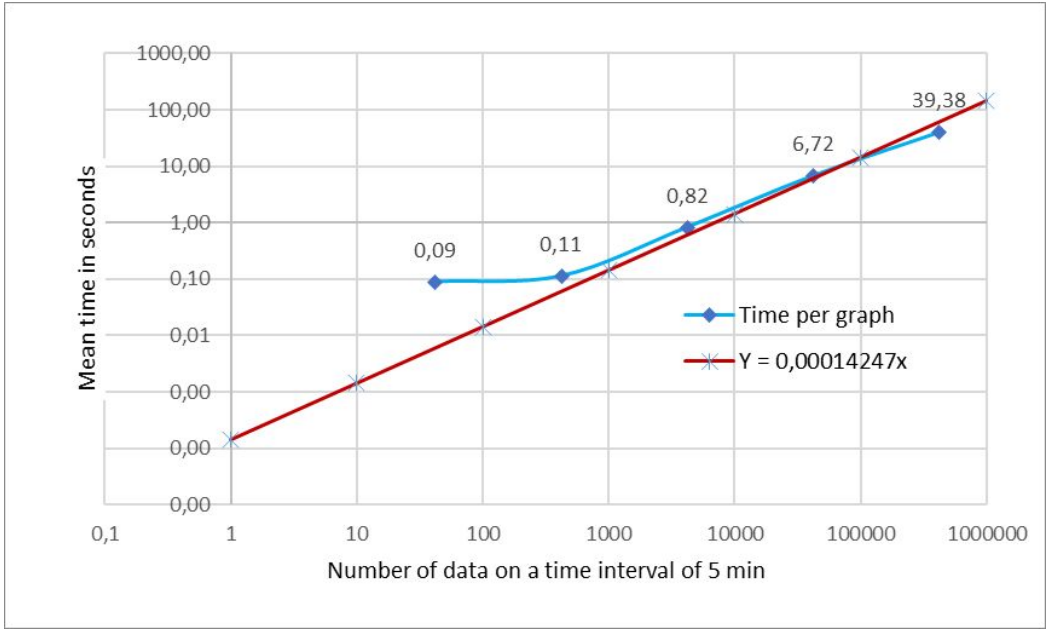
Permet de calculer toutes les métriques statiques référencées dans la librairie en faisant le moins de parcours de graphe possible.

+ 2 fonctions pour le calcul de la stabilité entre les communautés de 2 graphes:

- *compute_stabilities(g1,g2,nb_of_communities,old_stabilities,t)*
- *propagate_community(g1,g2,center,center_t)*

https://github.com/lre-security-systems-team/gpml

Scalability evaluation



3 algorithms have been set up for extraction of graph community metric in time which scale linearly

Attack patterns : TrustSecLearn

- Approach used in real world security operations center
- 1 pattern => 1 type of attack
- 1 type of attack => n patterns
- Pattern deducted from characteristics of attacks in the literature

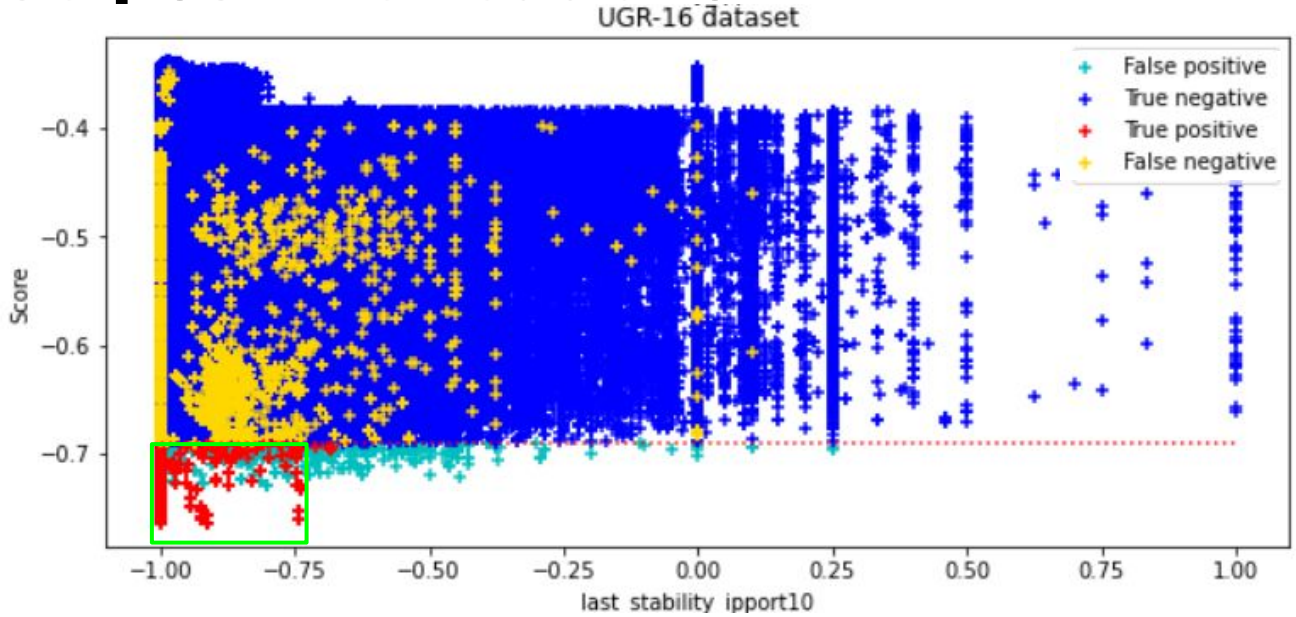
=> Can be used a baseline for our approach

https://gitlab.cri.epita.fr/laboratoires/lse/research-devs/trustseclearn

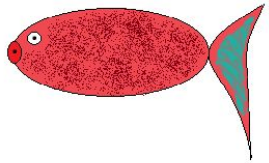
Attack	Type	Criteria	UGR-16
DoS	Service overload	Port number = CONSTANT and number of message between Ip source and destination spaced by less than 3 min over : **[total_number_of_flow*0.0002* sampling]**	True Port = 80
Scan	Port scan	Number of messages between Ip source and destination spaced by less than 3 min over : **[total_number_of_flow*0.0002* sampling]** and number of different ports between the two ip over 50	True

Scan False Positive Rate : 0.00116809518 / DoS FPR : 0.00227426215
Scan True Positive Rate : **0.68578661065** / DoS TPR : **0.2593768905**
Scan False Negative Rate : **0.30333205668** / DoS FNR : **0.7406231095**
Scan True Negative Rate : 0.9988912 / DoS TNR : 0.99772573785

False positive reduction



Precision 87.84 % before false positive reduction and 89.38% after reduction.
=> 12.68% of false positives can be avoided.



Concept drift : what is it ?

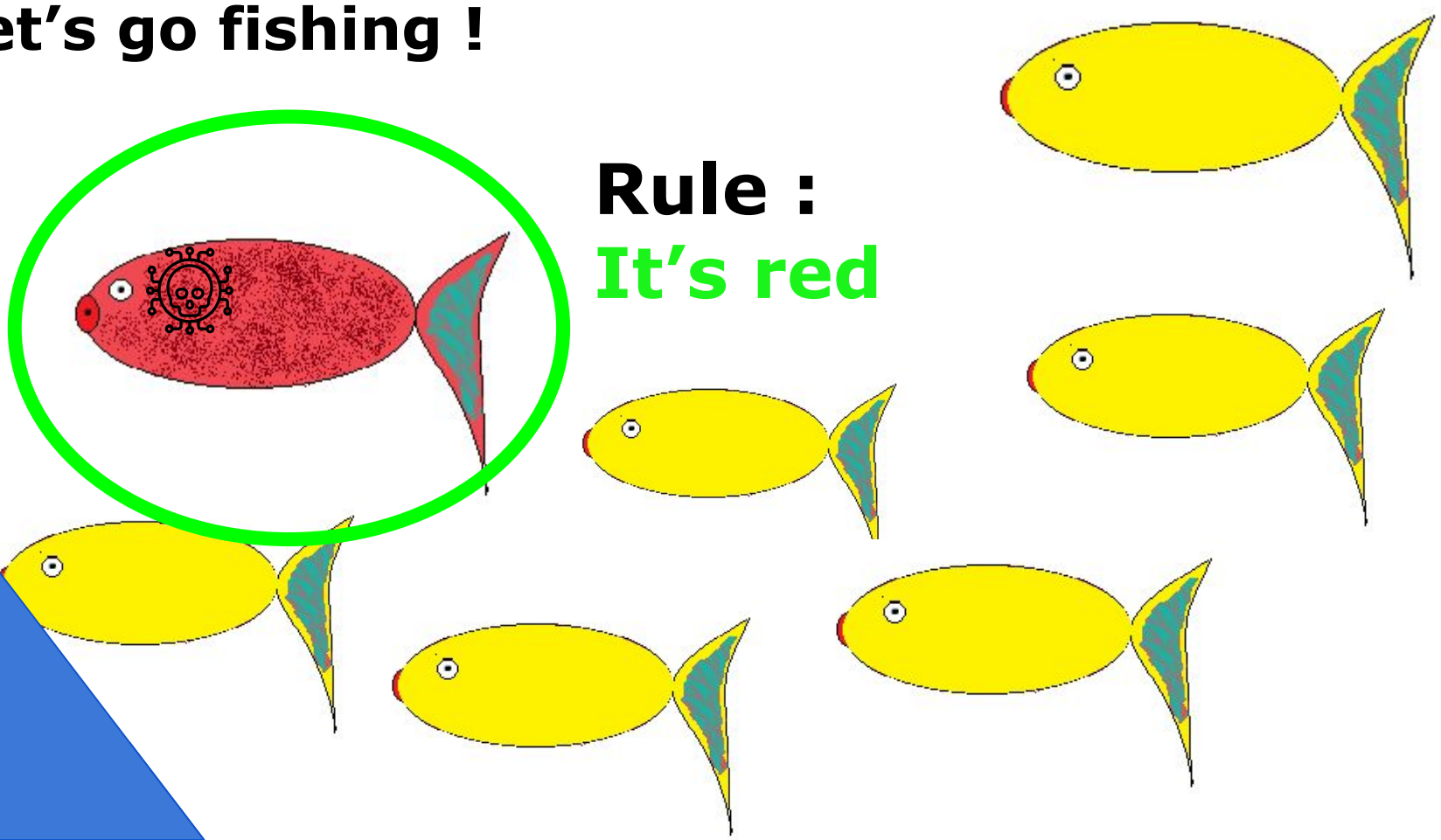
Simple Definition :

The characteristics of the target you are trying to detect are changing with passing time and this target is itself in an environment that is evolving with passing time

Add to the mix :

- **Different targets appearing at any time**
- **Disparition of older target**
- **High diversity in the data**
- **….**

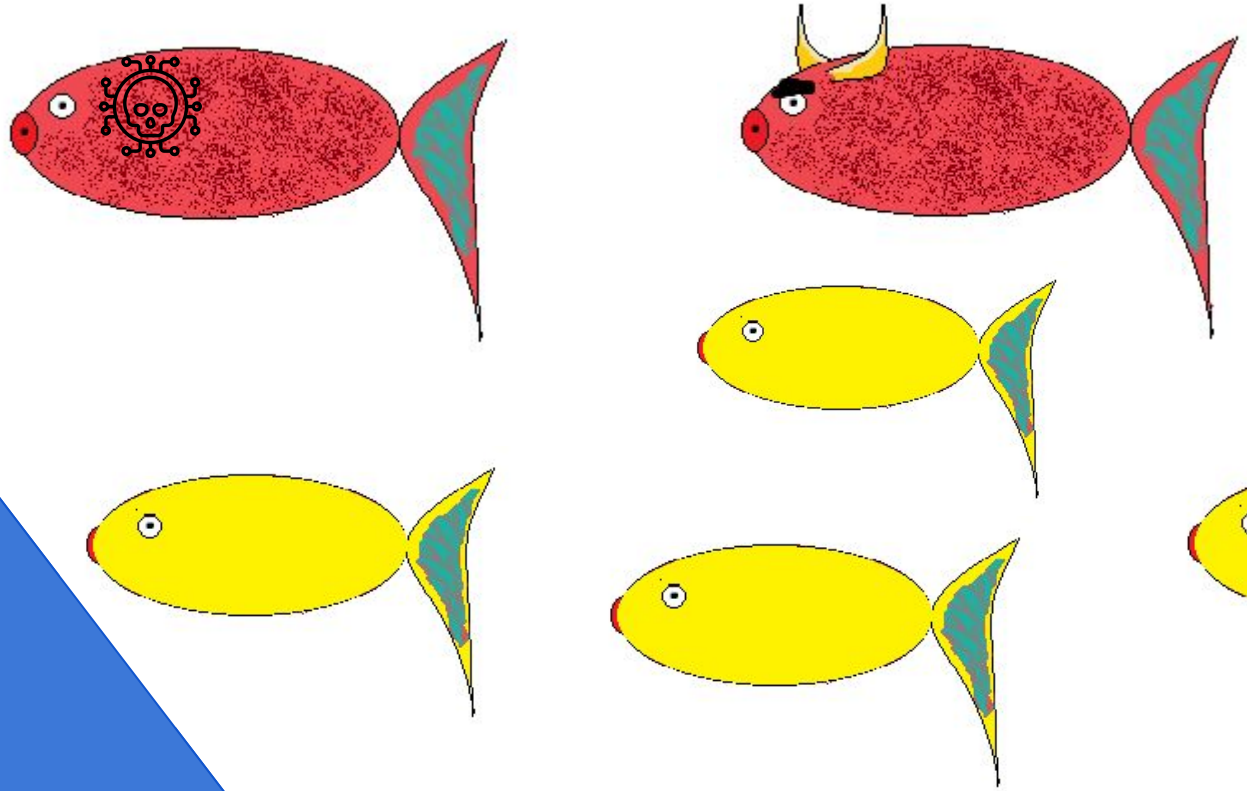
Let’s go fishing !



Rule :

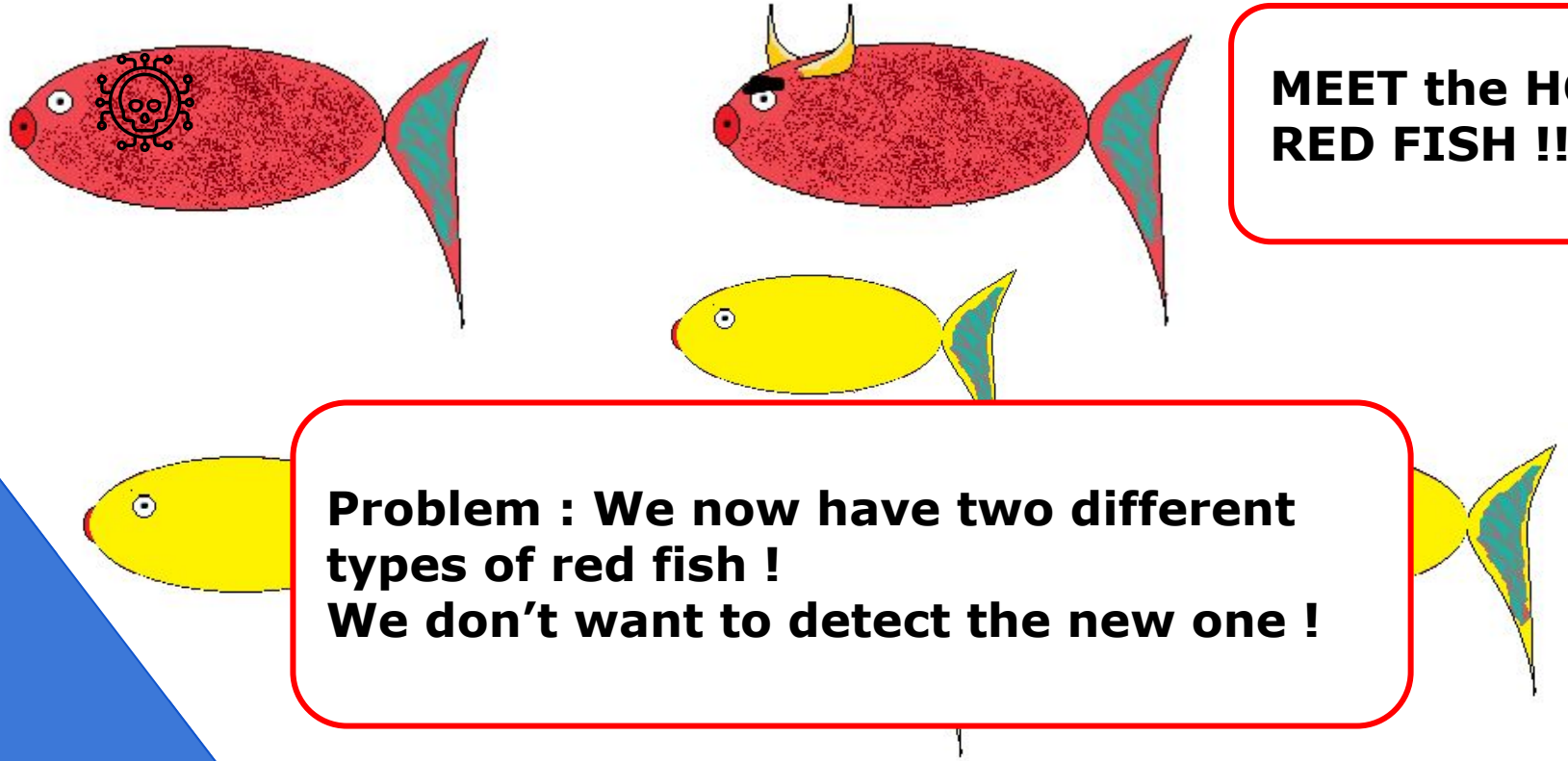
It’s red

Here comes a new challenger !



MEET the HORNY RED FISH !!!

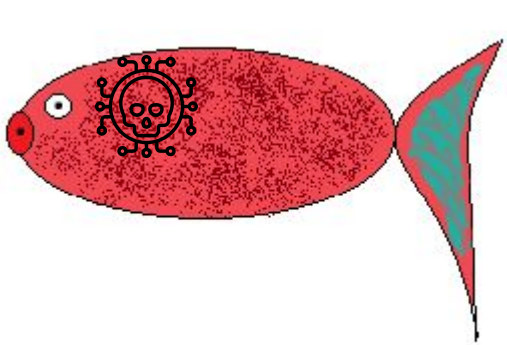
Here comes a new challenger !

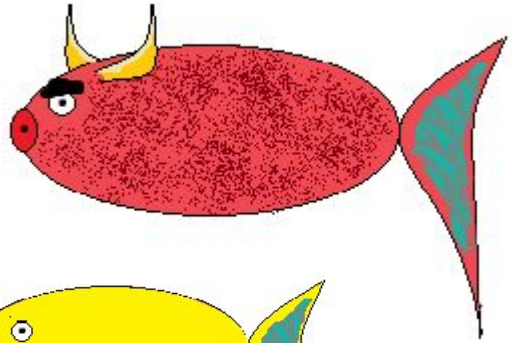


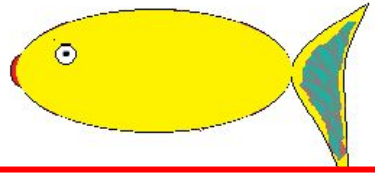
MEET the HORNY RED FISH !!!

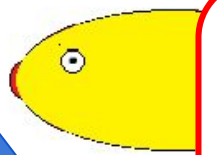
Problem : We now have two different types of red fish !
We don’t want to detect the new one !

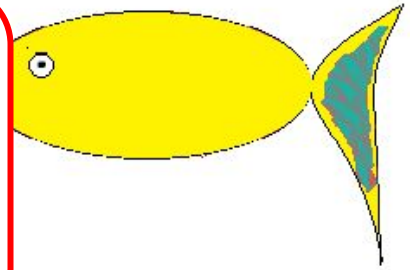
Here comes a new challenger !











NEW RULES :

It’s red
It doesn’t have horn
(not horny)

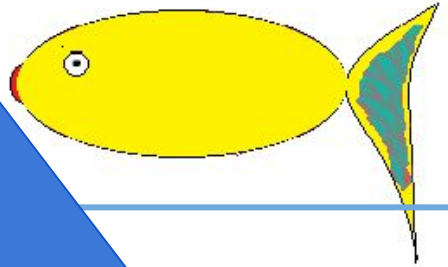
<u>If we don’t change our model :</u>

Increase of false positive rate !

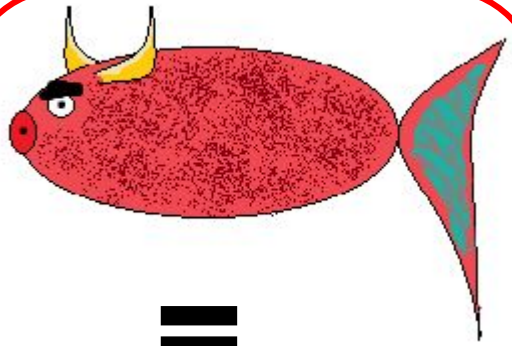
We were looking for this :

= Target

Beside those :



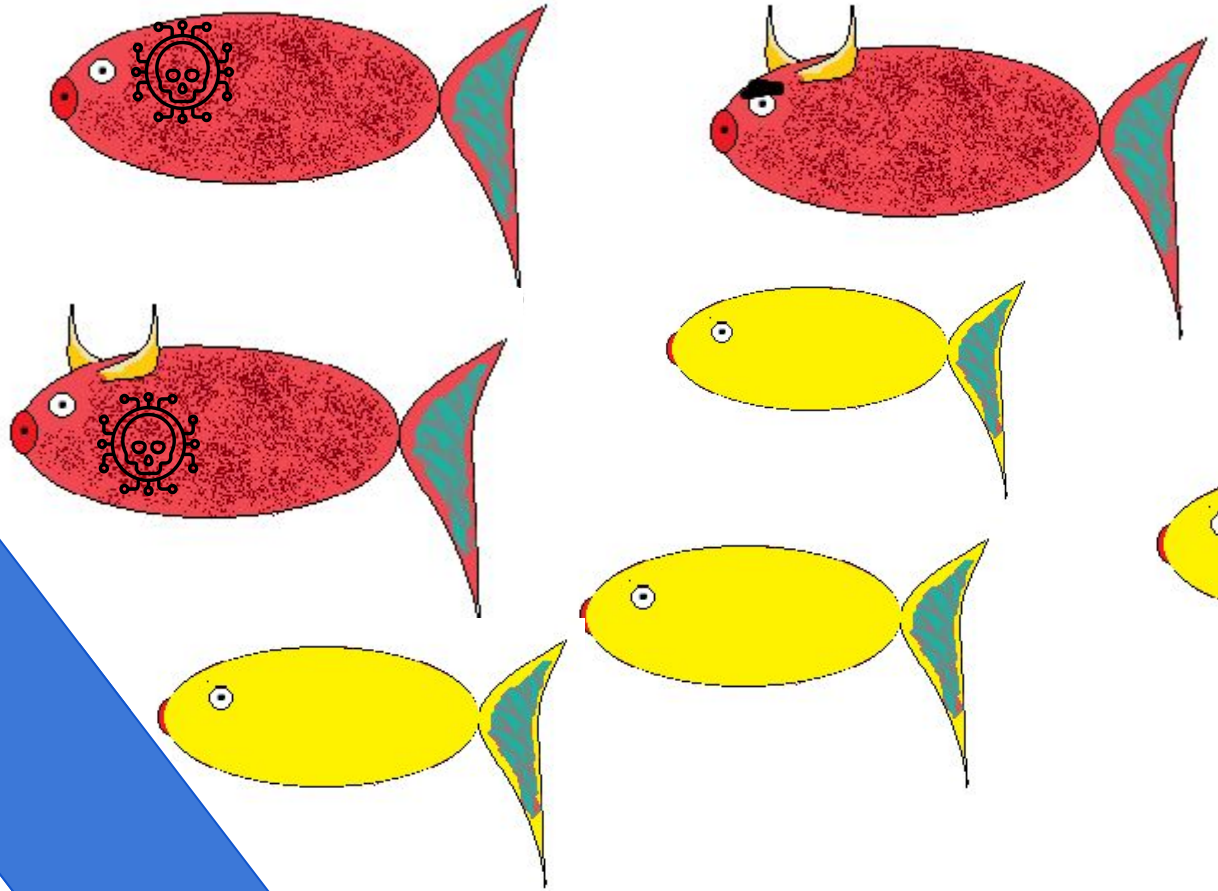
= Environment



=

Change in environment

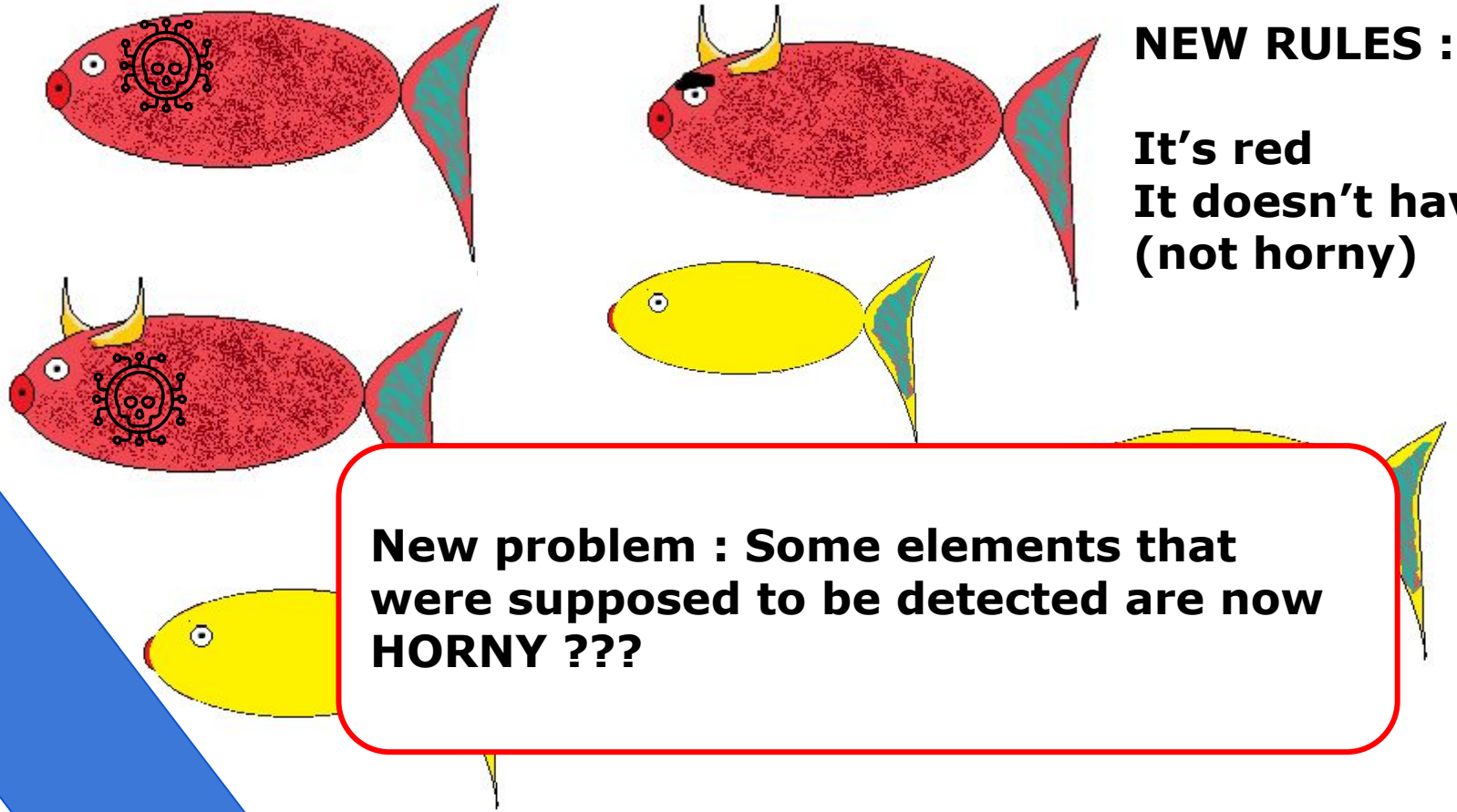
There is something fishy !



NEW RULES :

It’s red
It doesn’t have horn
(not horny)

There is something fishy !

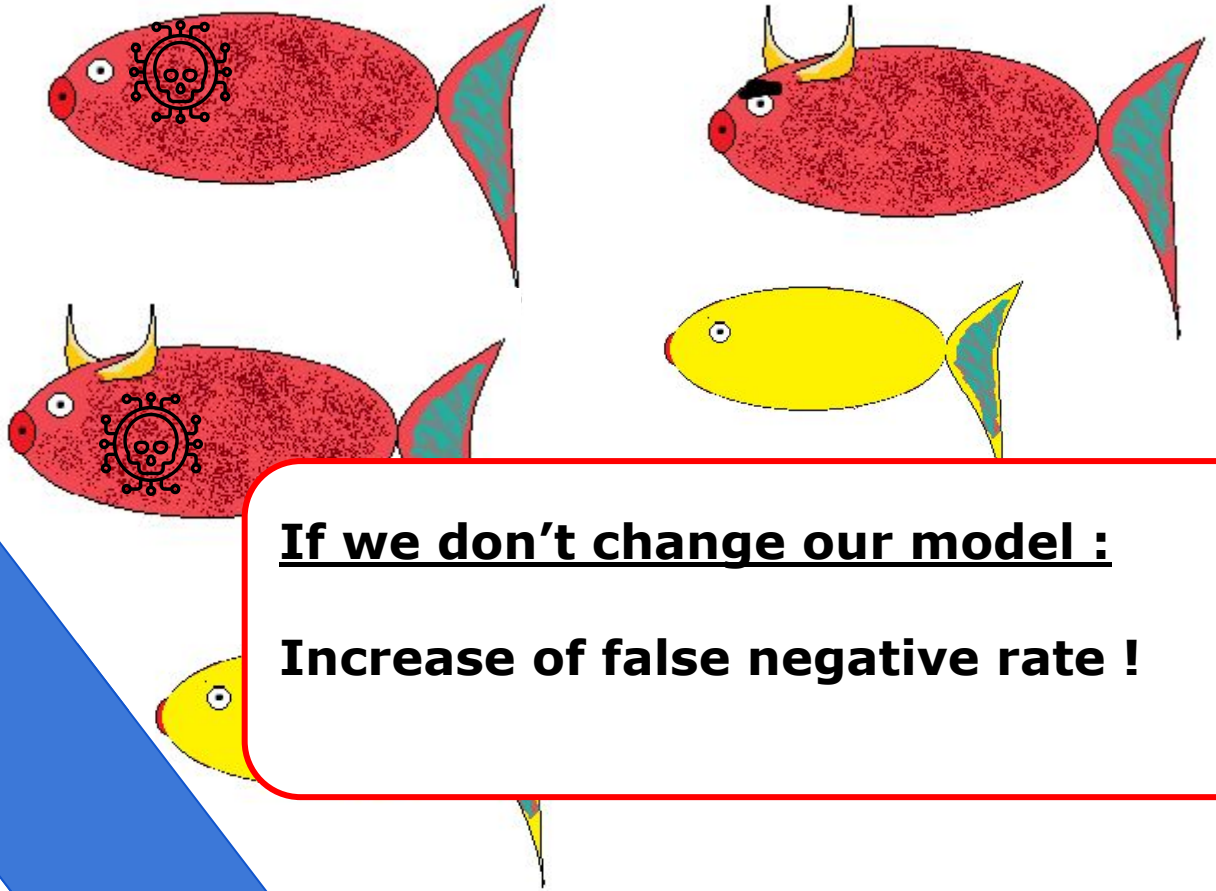


NEW RULES :

It’s red
It doesn’t have horn
(not horny)

New problem : Some elements that were supposed to be detected are now HORNY ???

There is something fishy !



NEW RULES :

It’s red
It doesn’t have eyebrows

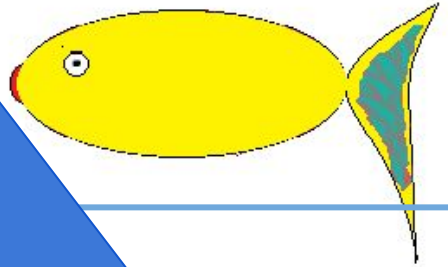
<u>If we don’t change our model :</u>

Increase of false negative rate !

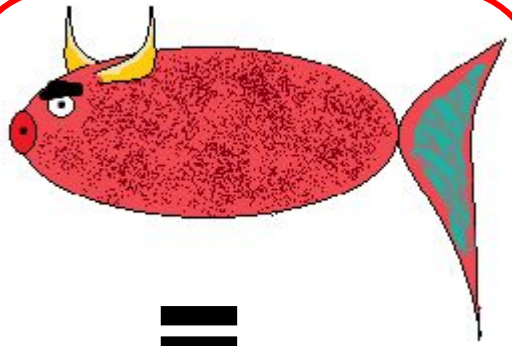
We were looking for this :

= Target

Beside those :

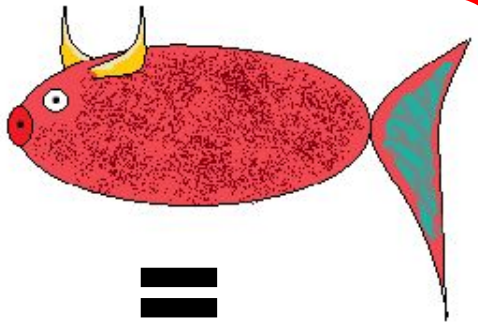


= Environment



=

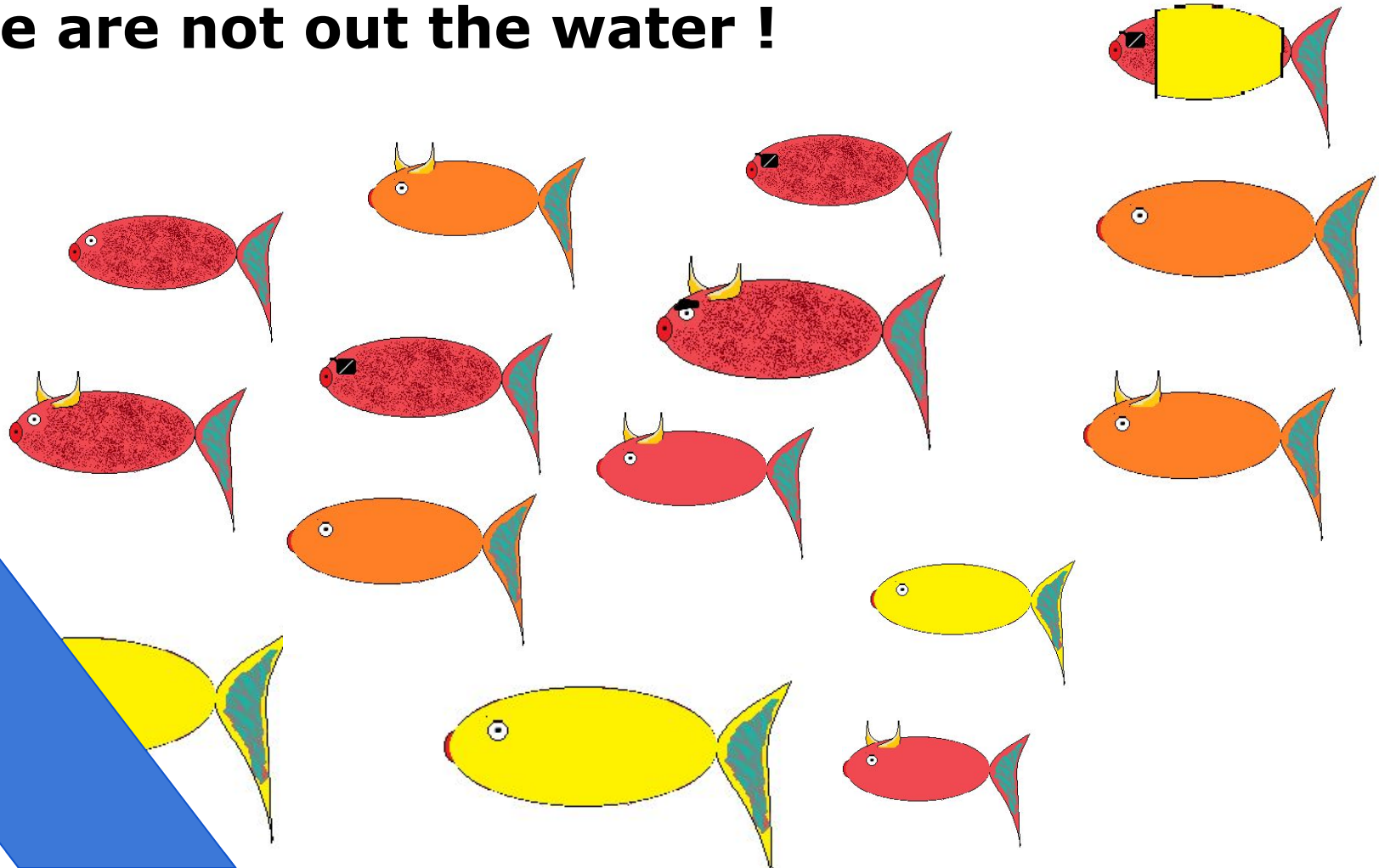
Change in environment



=

Change in Target

We are not out the water !



Scenario for attack detection

The first 2 days of the dataset are considered as labeled.

Those 2 days of data are use to both train a Xg_boost model and to build an isolation forest model using graph community metrics.

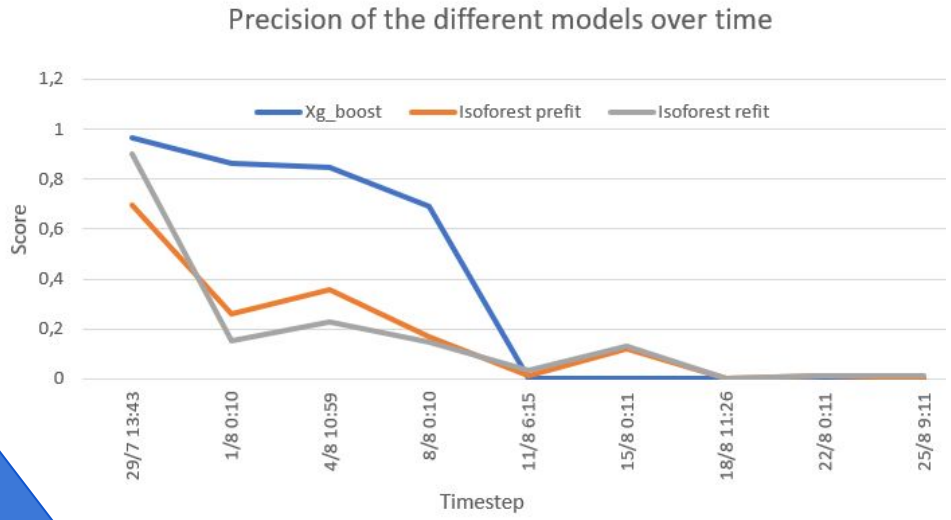
Then all remaining data in the data set are distributed in 9 time interval.

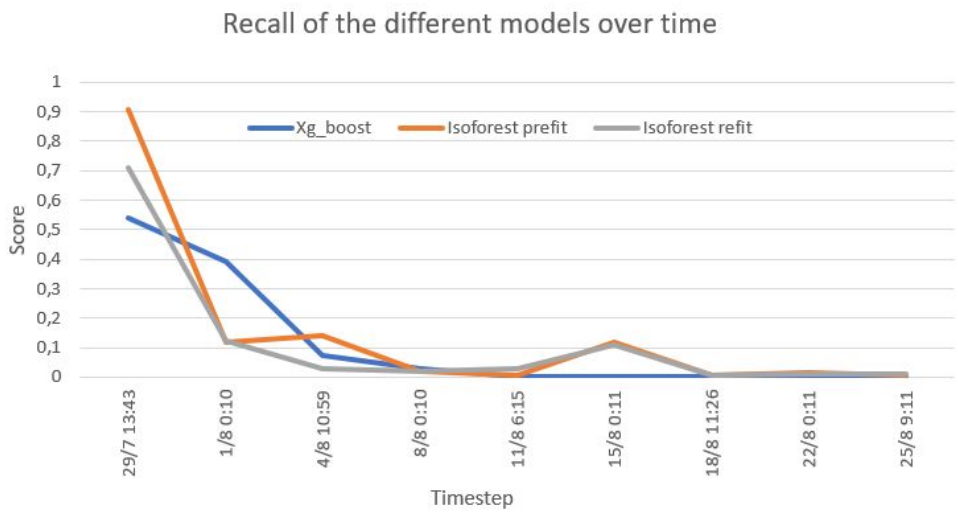
Accuracy, precision and recall for the Xg_boost model are calculated for each of the time interval.

We consider 2 measure for the isolation forest model, fit at the previous time step and fit at the current one.

Accuracy, precision and recall for the isolation forest models are calculated for each of the time interval.

Concept drift : Résults





Conclusions

Feature extraction and selection are very important !

Graph community metrics seems relevant to the detection of cyber attacks.

It is especially true for unsupervised detection !

The approach can fulfill the constraint of scalability !

Time robustness is yet a challenge to tackle.

Icube - Laboratoire des sciences de l'ingénieur,de l'informatique et de l'imagerie, UMR 7357
Université de Strasbourg, 67000 Strasbourg, France;

Laboratoire de Recherche de L'EPITA (LRE),
14-16 rue Voltaire, 94270 Le Kremlin-Bicètre, France

julien.michel2@etu.unistra.fr

Thank you

[1] A. Abou Rida, R. Amhaz, and P. Parrend. Anomaly Detection on Static and Dynamic Graphs using Graph Convolutional Neural Networks, chapter -, page 23. Studies in Computational Intelligence Series. Springer, 2022.
[2] Siddharth Bhatia, Bryan Hooi, Minji Yoon, Kijung Shin, and Christos Faloutsos. Midas : Microclusterbased detector of anomalies in edge streams. In Proceedings of the AAAI Conference on Artificial Intelligence, volume 34, pages 3242–3249, 2020.
[3] Xavier Larriva-Novo, Víctor A. Villagrá, Mario VegaBarbas, Diego Rivera, and Mario Sanz Rodrigo. An iot-focused intrusion detection system approach based on preprocessing characterization for cybersecurity datasets. Sensors, 21(2), 2021.
[4] Gabriel Maciá-Fernández, José Camacho, Roberto Magán-Carrión, Pedro García-Teodoro, and Roberto Therón. Ugr‘16 : A new dataset for the evaluation of cyclostationarity-based network idss. Computers & Security, 73 :411–424, 2018.
[5] J. Navarro, A. Deruyver, and P. Parrend. A systematic survey on multi-step attack detection. Computers and Security, page 102, 2018.
[6] William Robertson, Giovanni Vigna, Christopher Krügel, and Richard Kemmerer. Using generalization and characterization techniques in the anomaly-based detection of web attacks. In NDSS, 01 2006.
[7] Jaewon Yang and Jure Leskovec. Defining and evaluating network communities based on ground-truth. In Proceedings of the ACM SIGKDD Workshop on Mining Data Semantics, MDS ’12, New York, NY, USA, 2012. Association for Computing Machinery.
[8] Tommaso Zoppi, Andrea Ceccarelli, Tommaso Capecchi, and Andrea Bondavalli. Unsupervised anomaly detectors to detect intrusions in the current threat landscape. ACM/IMS Trans. Data Sci., 2(2), apr 2021
[9] H. S. Pattanayak, H. K. Verma, and A. L. Sangal, “Community detection metrics and algorithms in social networks,” in 2018 First International Conference on Secure Cyber Computing and Communication (ICSCCC) 2018, pp. 483–489.
[10] J.-H. Park and H.-Y. Kwon, “Cyberattack detection model using com-munity detection and text analysis on social media, ”ICT Express, vol. 8, no. 4, pp. 499–506, 2022.