Pierre Parrend

2021-2022

Security & Artificial Intelligence Project

Planning

- Project start
  - Thursday 10/3 – 15h-17h30
- Work sessions
  - Thursday 24/3 – 15h-17h30
  - Thursday 31/3 – 15h-17h30
- Deliver deliverables
  - Sunday 8/5
- Project defense
  - Tuesday 17/5

premier rendu intermédiaire.

Présentation finale.

Organisation

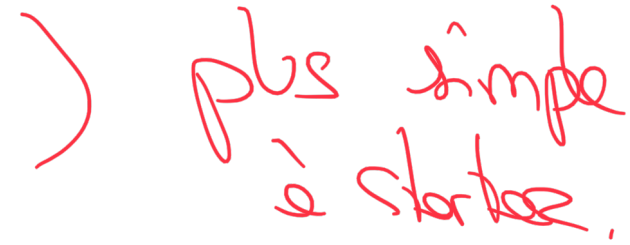
- Work in groups of 3

- Share the work
  - and don't forget to mention task allocation in your presentations !

↳ On doit se partager les tâches.
↳ On doit garder des traces de ce qui a été fait.

Objective

- Chose your objective
  - Objective 1
    - Anomaly detection for tracking attacks
  - Objective 2
    - Adversarial attacks against classification



Datasets

On doit choisir entre ces deux datasets.

- 1) The UGR'16 Dataset
  - Data: https://nesg.ugr.es/nesg-ugr16/index.php
  - Scientific paper:
    - https://nesg.ugr.es/nesg-ugr16/dataset_AuthorVersionFinal.pdf

- 2) The Mawi dataset. Use exports from 3/3/2022 and 4/3/2022
  - https://mawi.wide.ad.jp/mawi/samplepoint-F/2022/202203031400.html
  - https://mawi.wide.ad.jp/mawi/samplepoint-F/2022/202203041400.html
  - Scientific paper
    - http://conferences.sigcomm.org/co-next/2010/CoNEXT_papers/08-Fontugne.pdf

Les Données aggrégées.

Deliverables

- Analysis notebook
  - shared on Google Collab
    GitHub!
- Analysis report
  - 20 pages
- Final oral group presentation (10 min) + demonstration (5 min)

) faire en jupyter Notebook.

) Noter les différentes étapes
↳ Ce que chacun à fait.

↳ faire des test static en plus pour éviter les problèmes.
↳ 5 minutes de démo en live.

Project report

- Detailed specification and implementation details on
  - The complete deployment of the data handling chain (including classification + anomaly detection)
  - Characterization of the dataset under study
  - Benchmark of 3 complementary analysis algorithms
  - Conclusions about cybersecurity events in the dataset

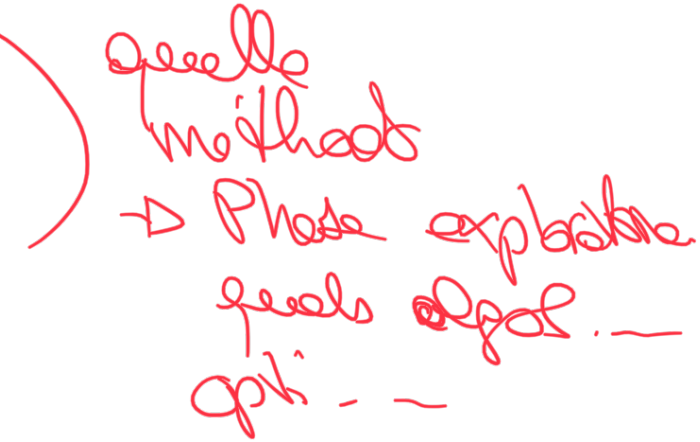
Avoir 3 algos au moins!

C prendre du recul, quelles sont les infos qu'on en sort.

ON NE Prend pas de responsabilités mais on a vu ça, ça ça...

Project defense

- Security analysis review based on the report
  - What are the attacks?
  - Which security-related conclusions can you draw?
- Demonstration



TODO

- 10/3
  - Groups + dataset + objective
  - On: SCIA_Secu&IA_Project_groups.xlsx
- 8/5
  - Deliver deliverables
- 17/5
  - Project defense

commencer cet après-midi.

mettre en nom de groupe.

2 objectifs :
→ On choisi en des 2.


EPITA
ÉCOLE D'INGENIEURS EN INFORMATIQUE