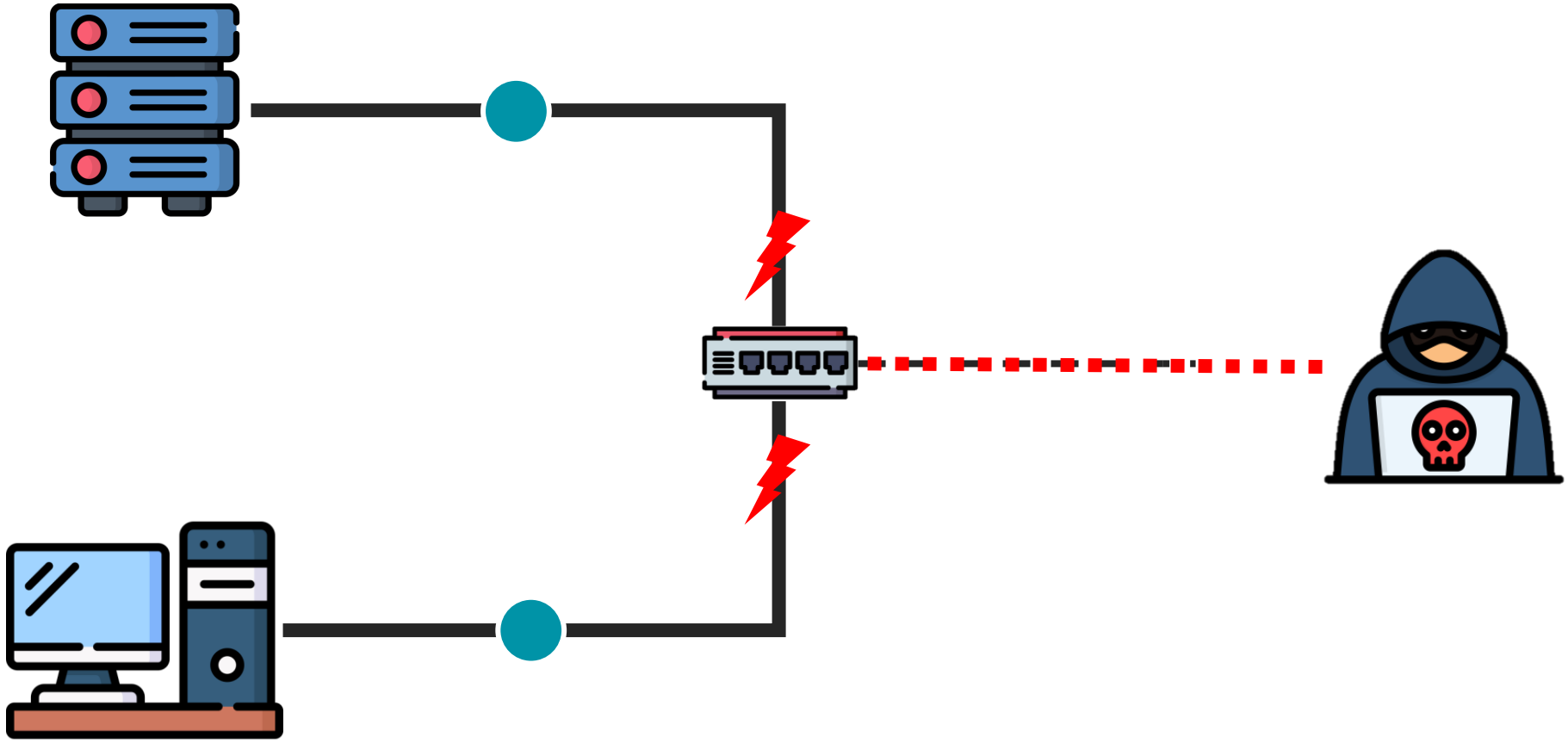
Etude systématique des systèmes de détection d'intrusion basés sur les appels système

Lalie Arnoud, Victor Breux, Pierre-Henri Thevenon, Eric Gaussier

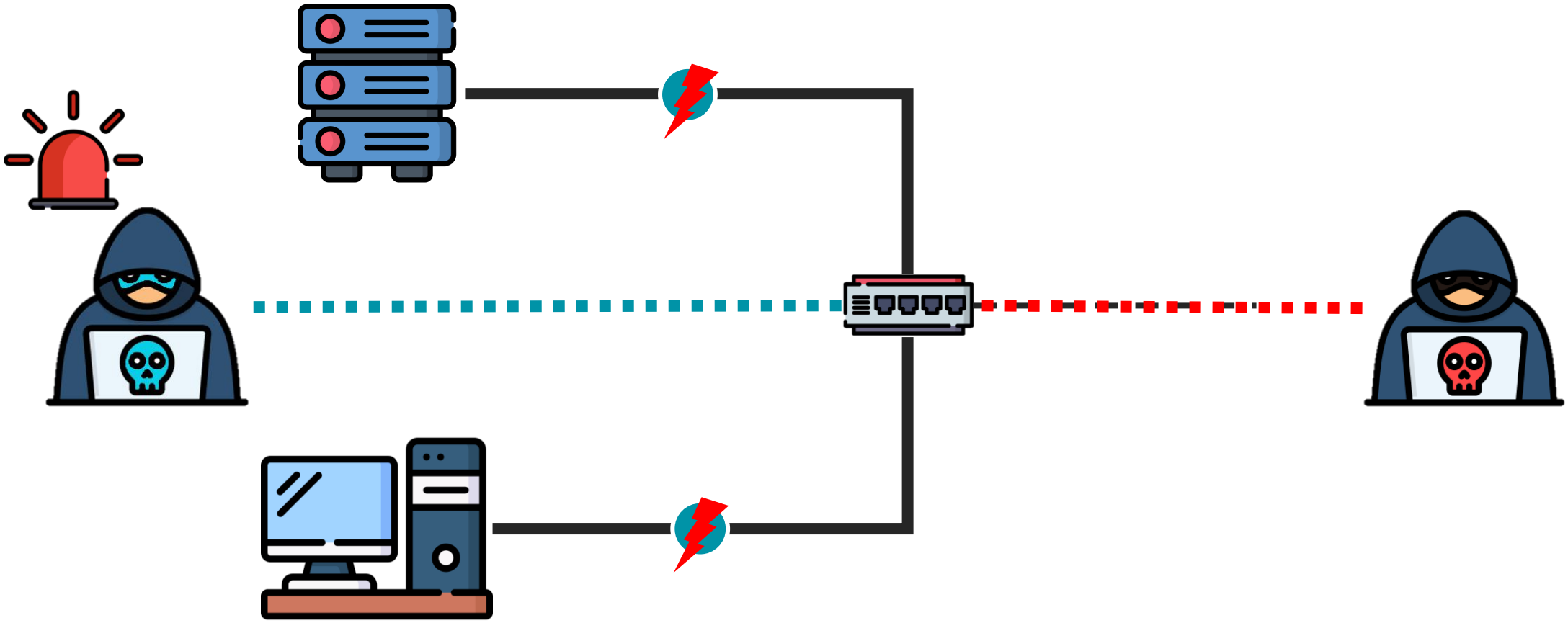
Sommaire

1. Introduction

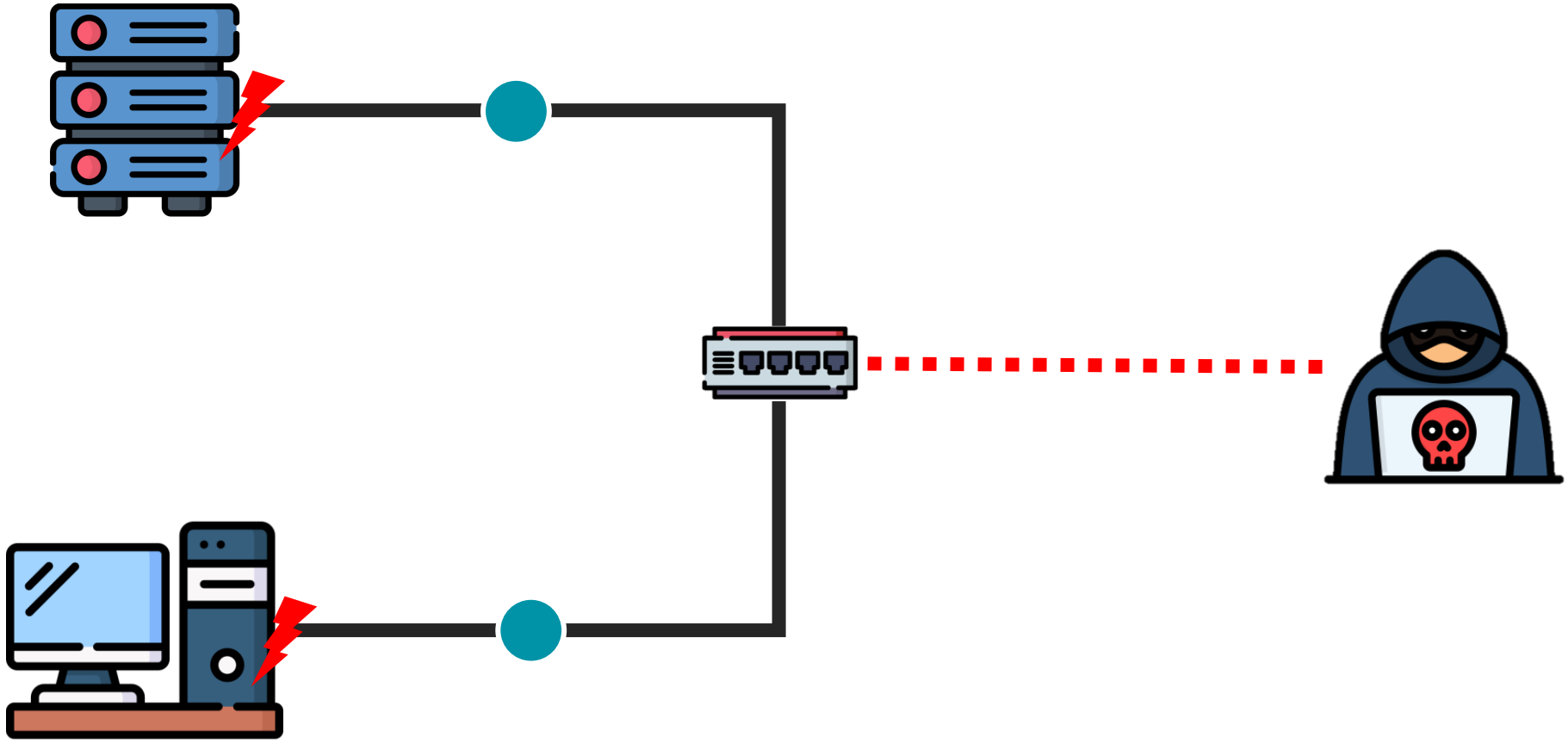
Introduction : la détection d'intrusion réseau



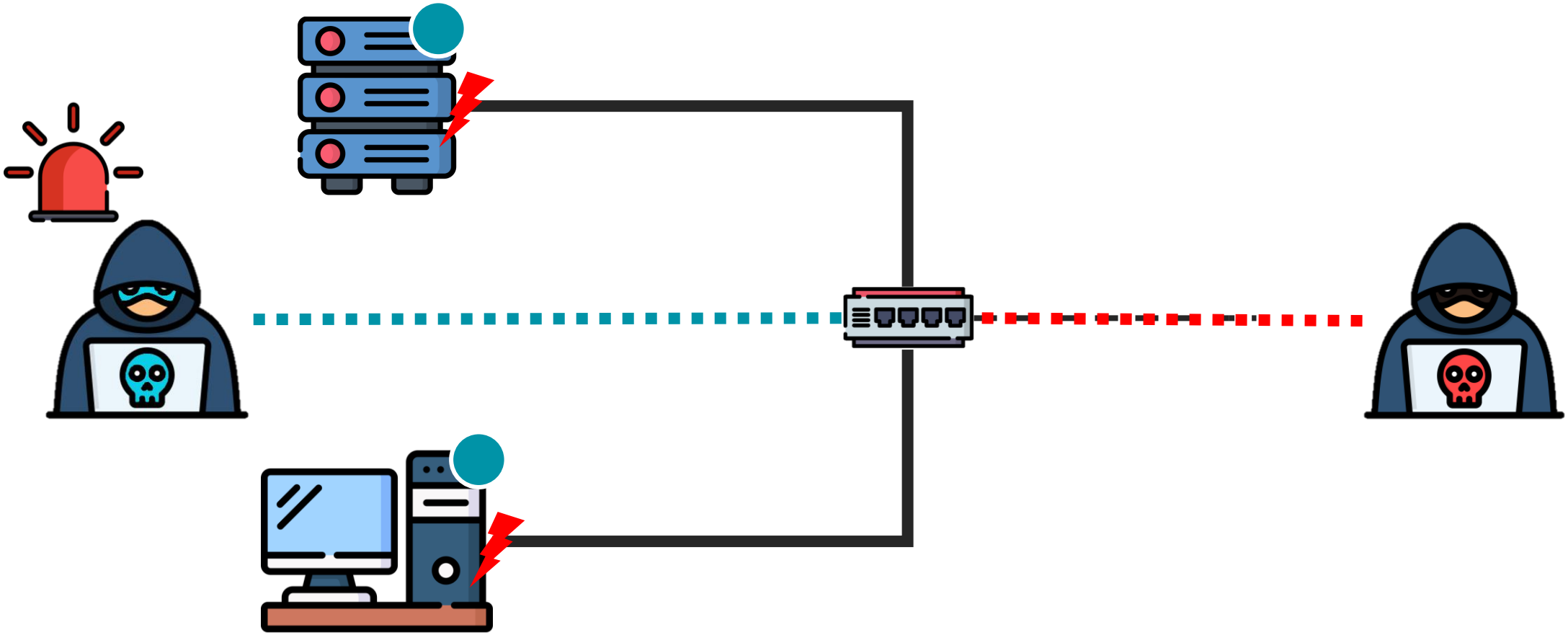
Introduction : la détection d'intrusion réseau



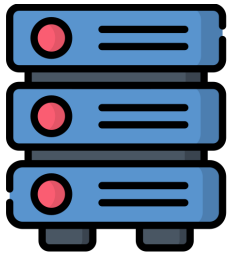
Introduction : la détection d'intrusion réseau

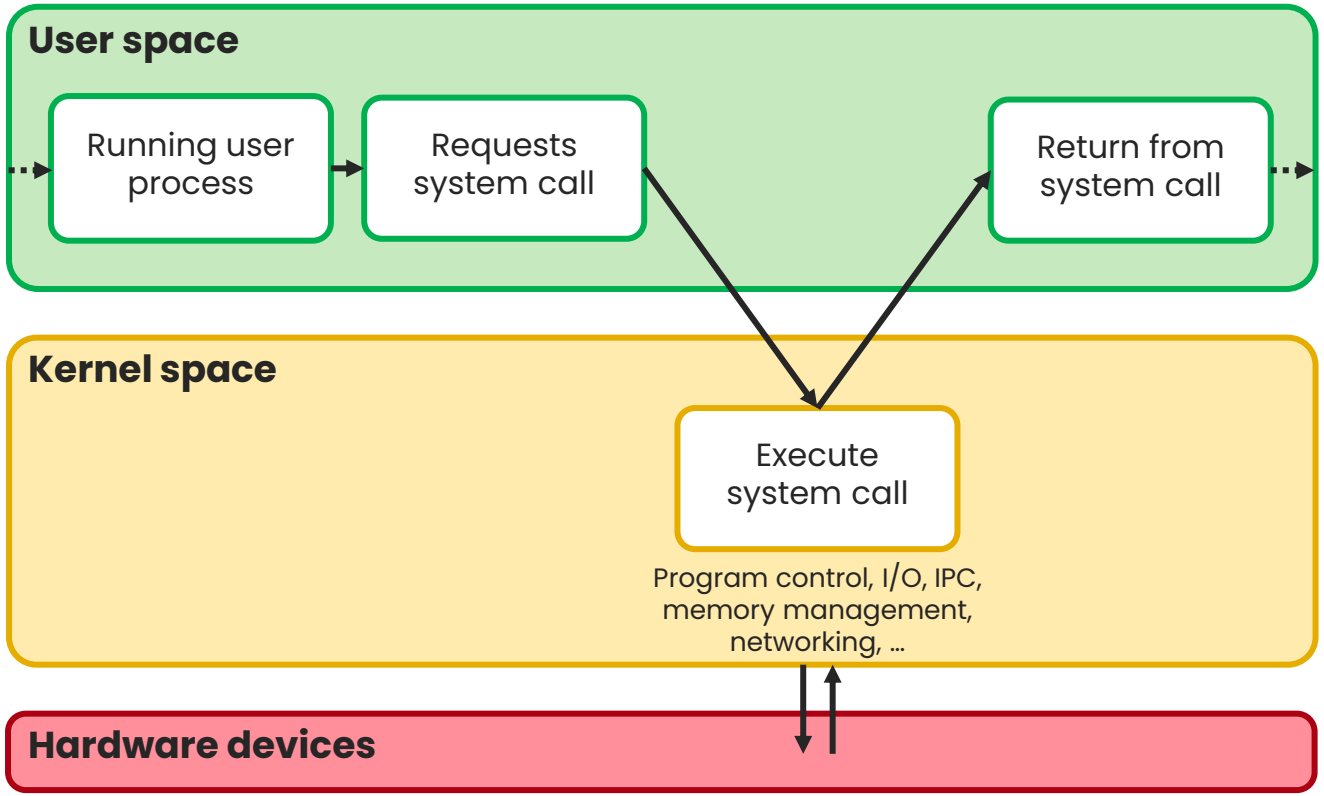


Introduction : la détection d'intrusion hôte

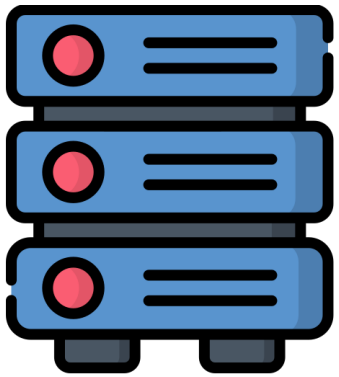


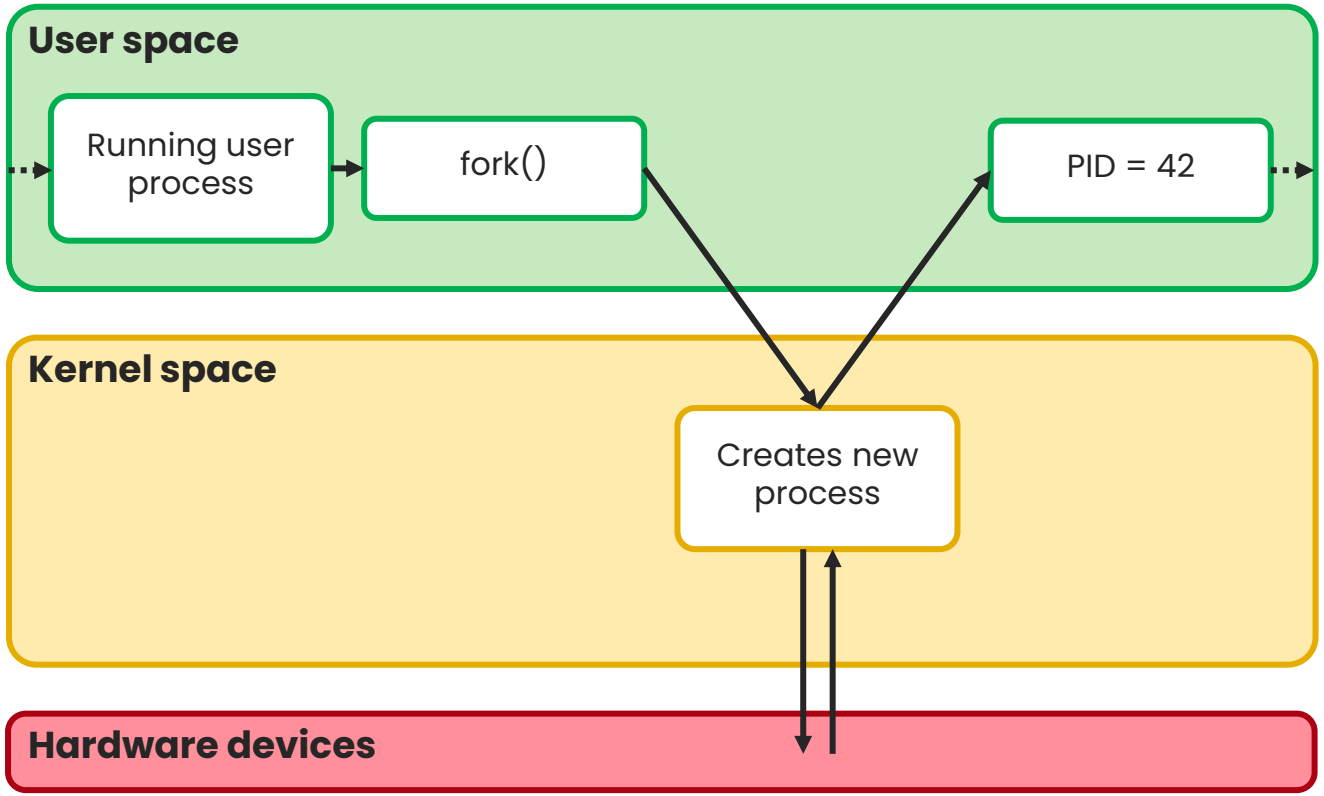
Introduction : les appels système





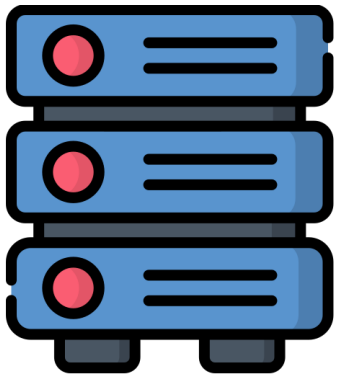
Introduction : les appels système

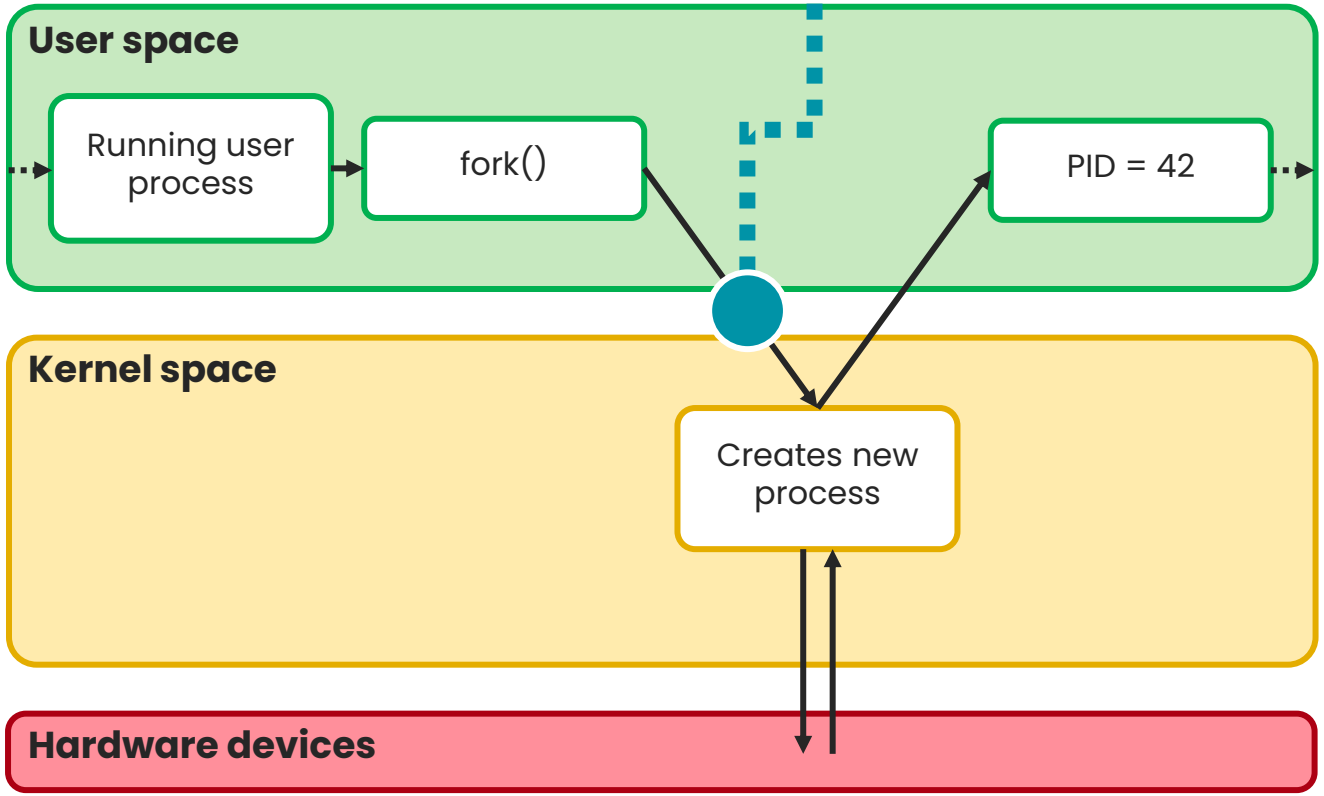




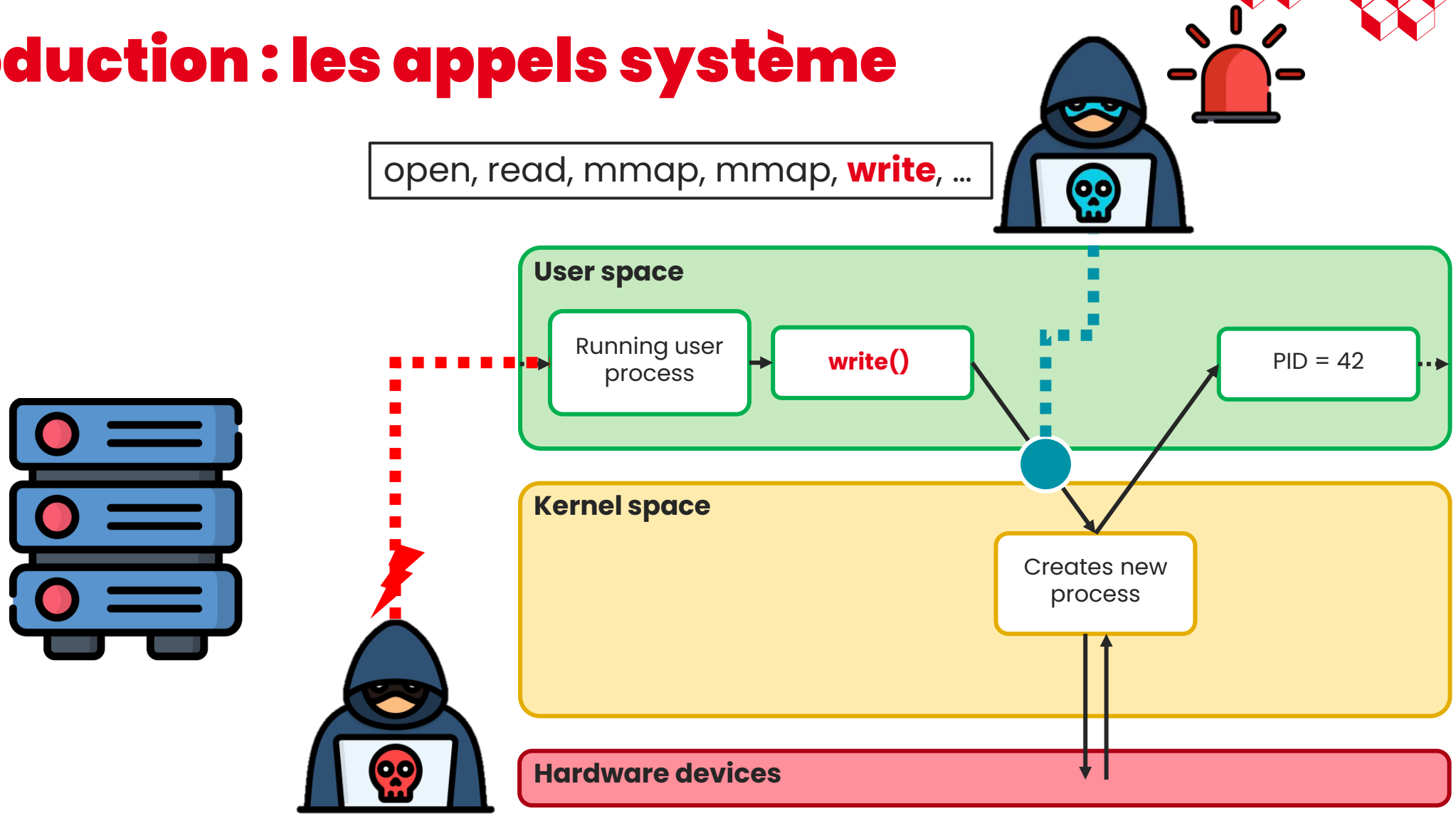
Introduction : les appels système

open, read, mmap, mmap, **fork**, ...

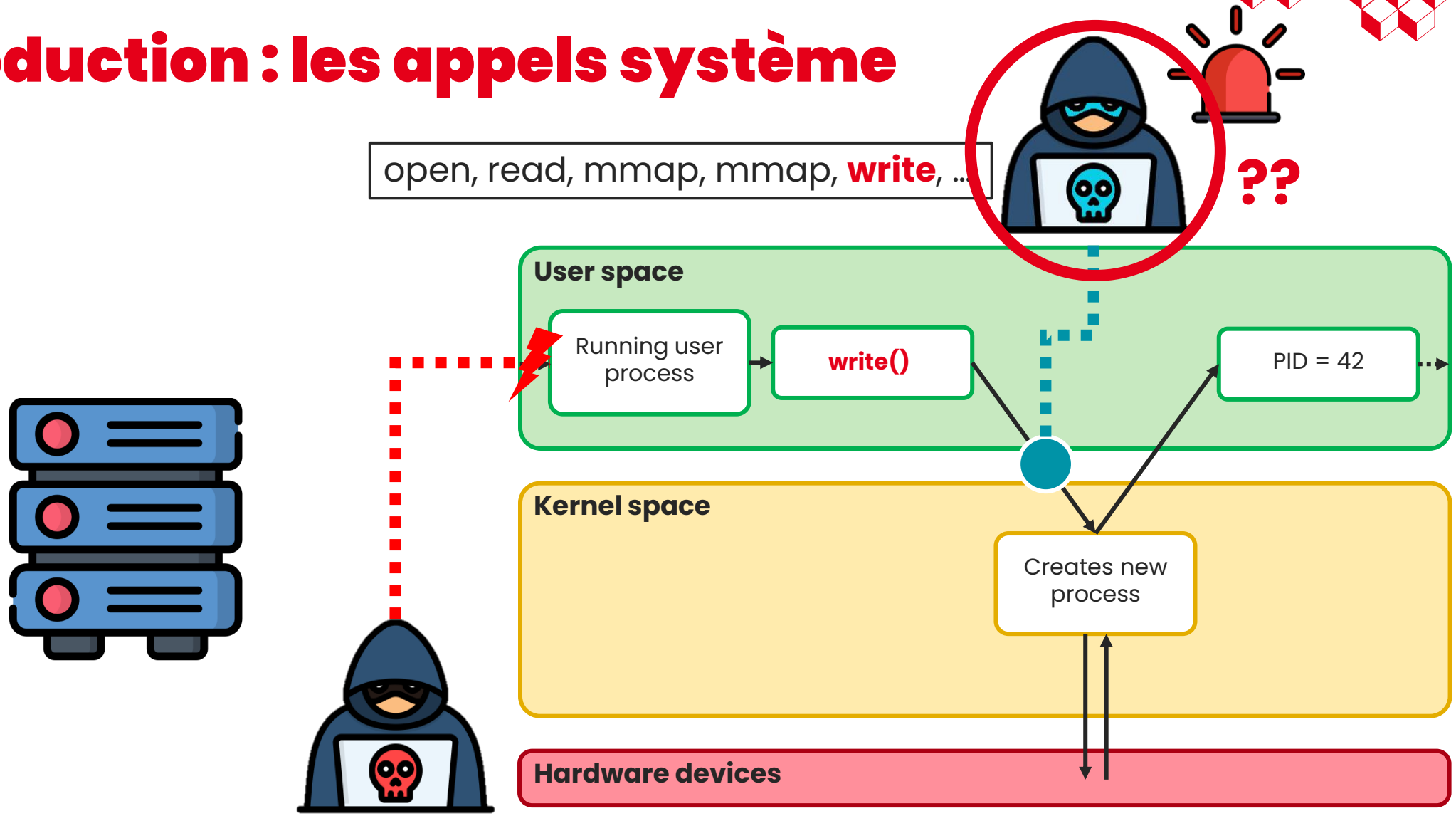




Introduction : les appels système



Introduction : les appels système



Intrusion detection systems based on dynamic analysis of system calls

A Systematic Literature Review (SLR)

with experimental evaluation of SOTA methods

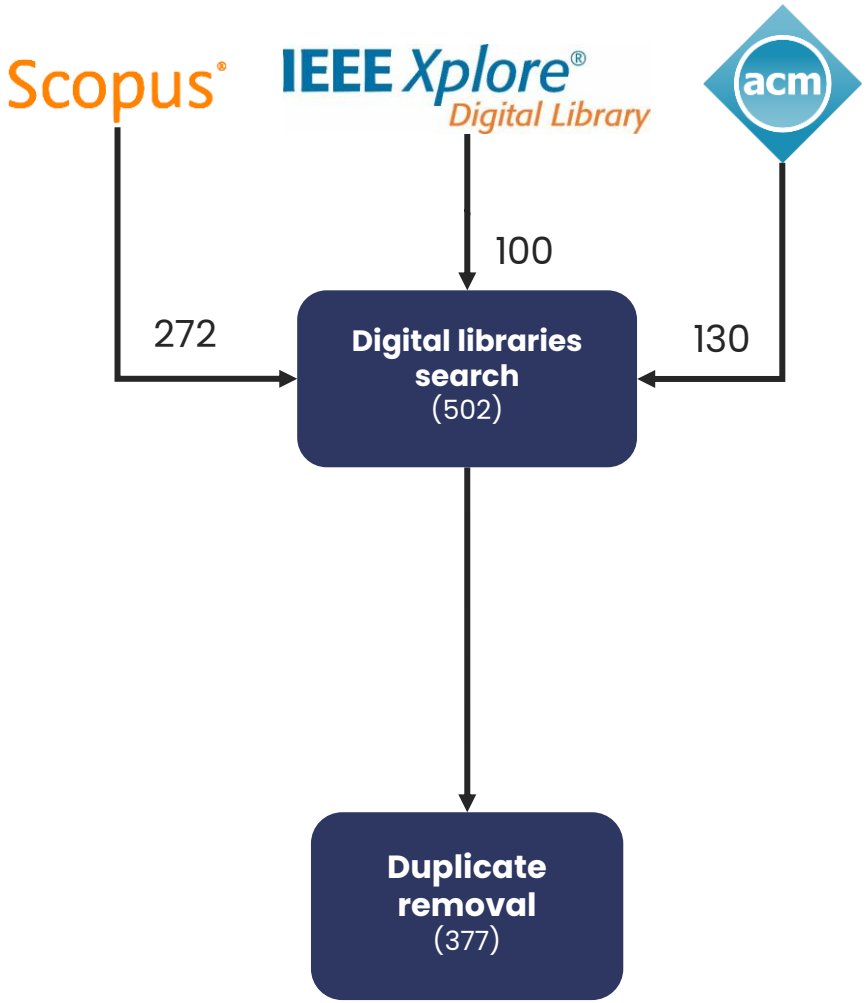
2. Méthodologie

Méthodologie

Basée sur « Guidelines for performing systematic literature reviews in software engineering », Kitchenham et al., 2007

- Quand y-a-t'il besoin d'une SLR ?
- Identifier les questions de recherche
- Construire une stratégie de recherche
- Evaluer la qualité des publications
- Synthétiser ses résultats
- Limiter les biais
- Exemples et retours d'expérience pour chaque étape de la revue

Méthodologie

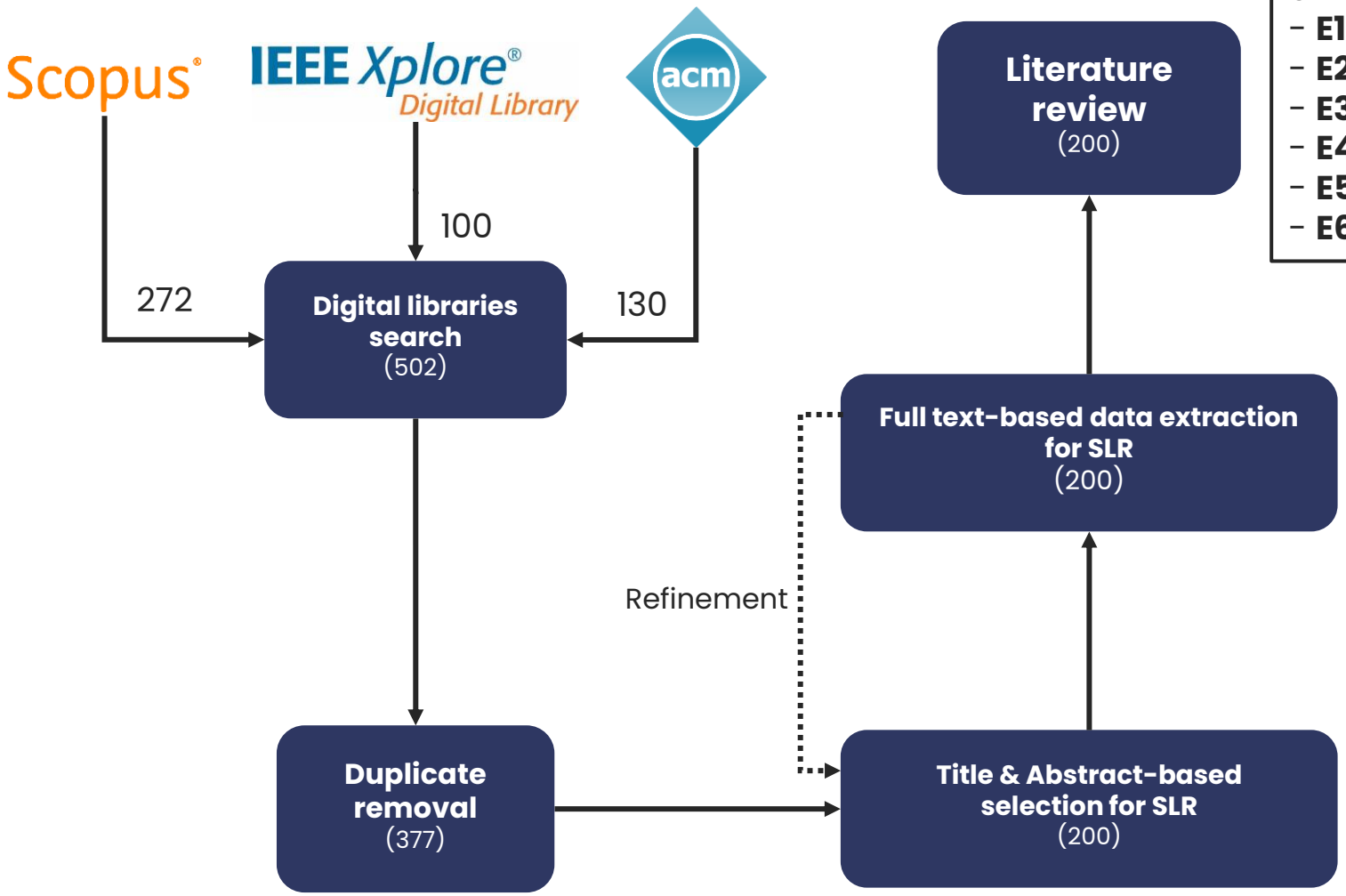


A: hids
B: (host OR "host-based" OR "host based")
C: (intrusion OR anomaly OR misuse OR malware)
D: detection
E: ids
F: ("system call" OR syscall)

➢ **(A OR (B AND ((C AND D) OR E))) AND F**

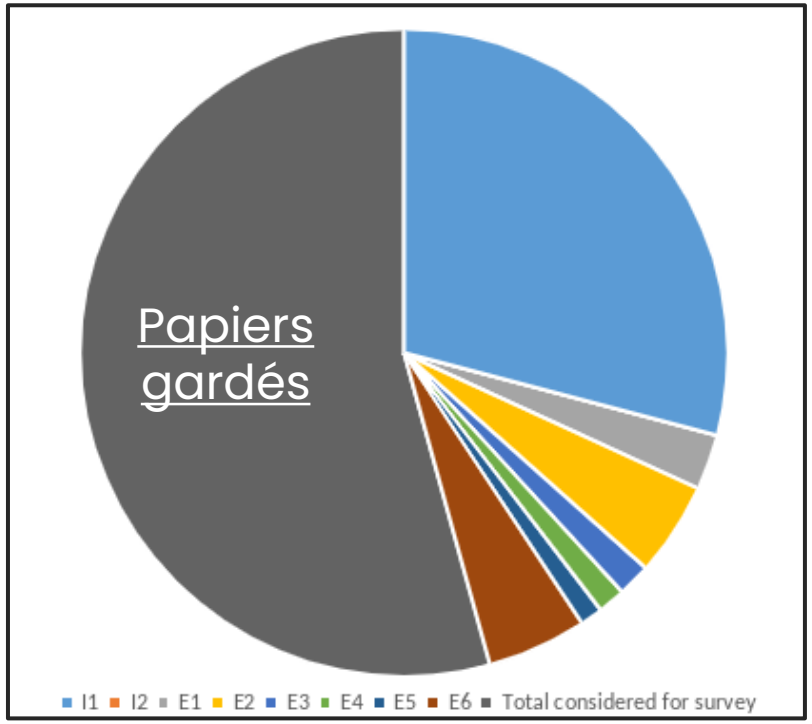
IEEE & ACM ne sont pas redondants avec Scopus car tous les documents ne sont pas indexés

Méthodologie



Inclusion & exclusion criteria for SLR

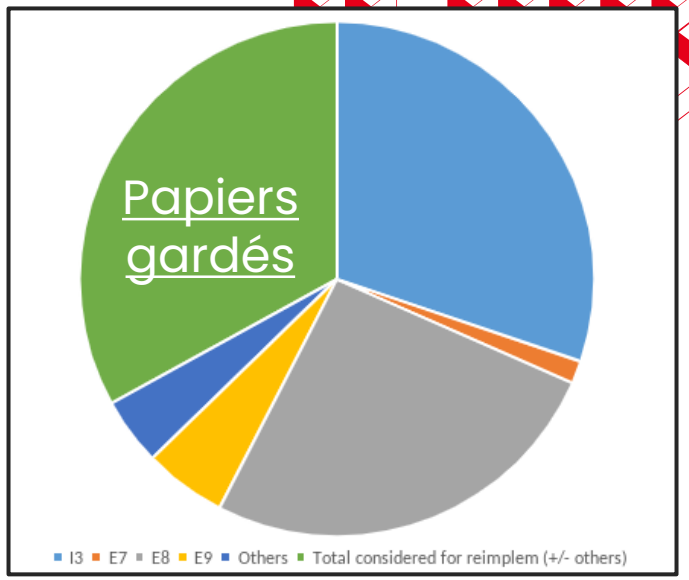
- **I1**: Publications in which the presented IDS is based on dynamic analysis of system calls
- **E1**: Publications that are not written in English
- **E2**: Publications that are not accessible
- **E3**: Conference versions of journal papers
- **E4**: Conference reviews
- **E5**: Surveys
- **E6**: PhD thesis manuscripts



Méthodologie

Inclusion & exclusion criteria for reimplementation

- **I3**: IDS based on syscalls from one host, without further information such as arguments, return code, or other information
- **E7**: Methods that stick too much to their environment
- **E8**: Studies that have been published strictly before 2020 which has less than strictly 30 citations
- **E9**: Studies that have been published between 2020 and 2022 which has less than strictly 10 citations



Scopus

IEEE Xplore Digital Library

acm

272

100

130

Digital libraries search (502)

Duplicate removal (377)

Raffinement

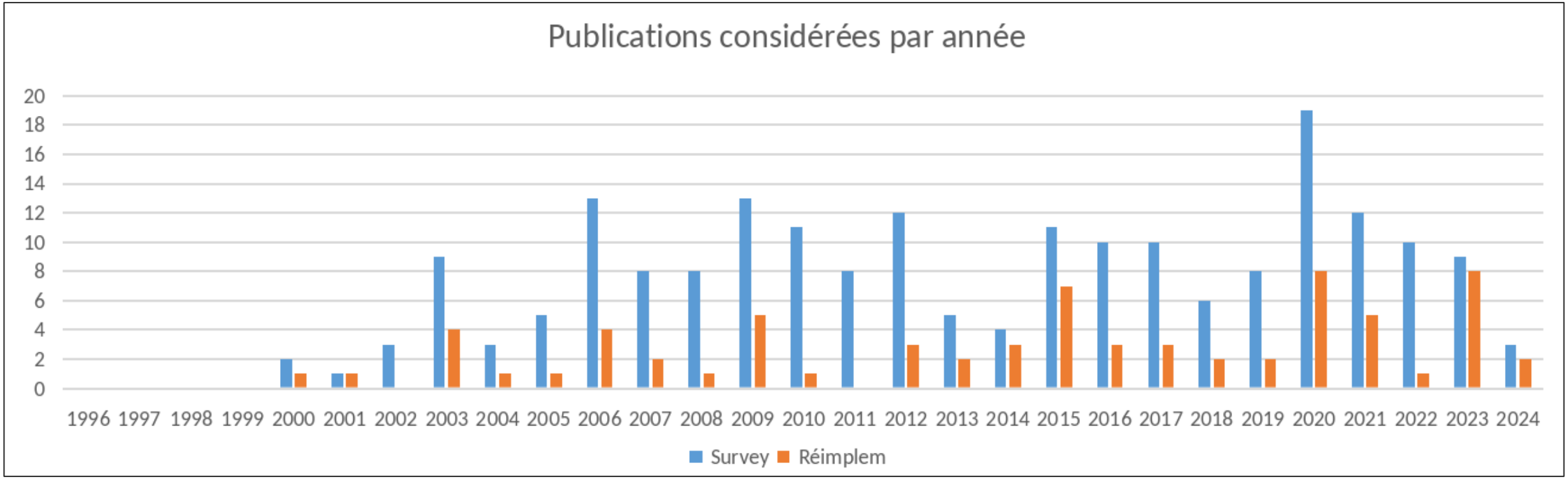
Full text-based data extraction for SLR (200)

Title & Abstract-based selection for SLR (200)

Title & Abstract-based selection for empirical evaluation (70)

Full text-based data extraction and quality assessment for empirical evaluation (18)

Méthodologie



3. Méthodes sélectionnées

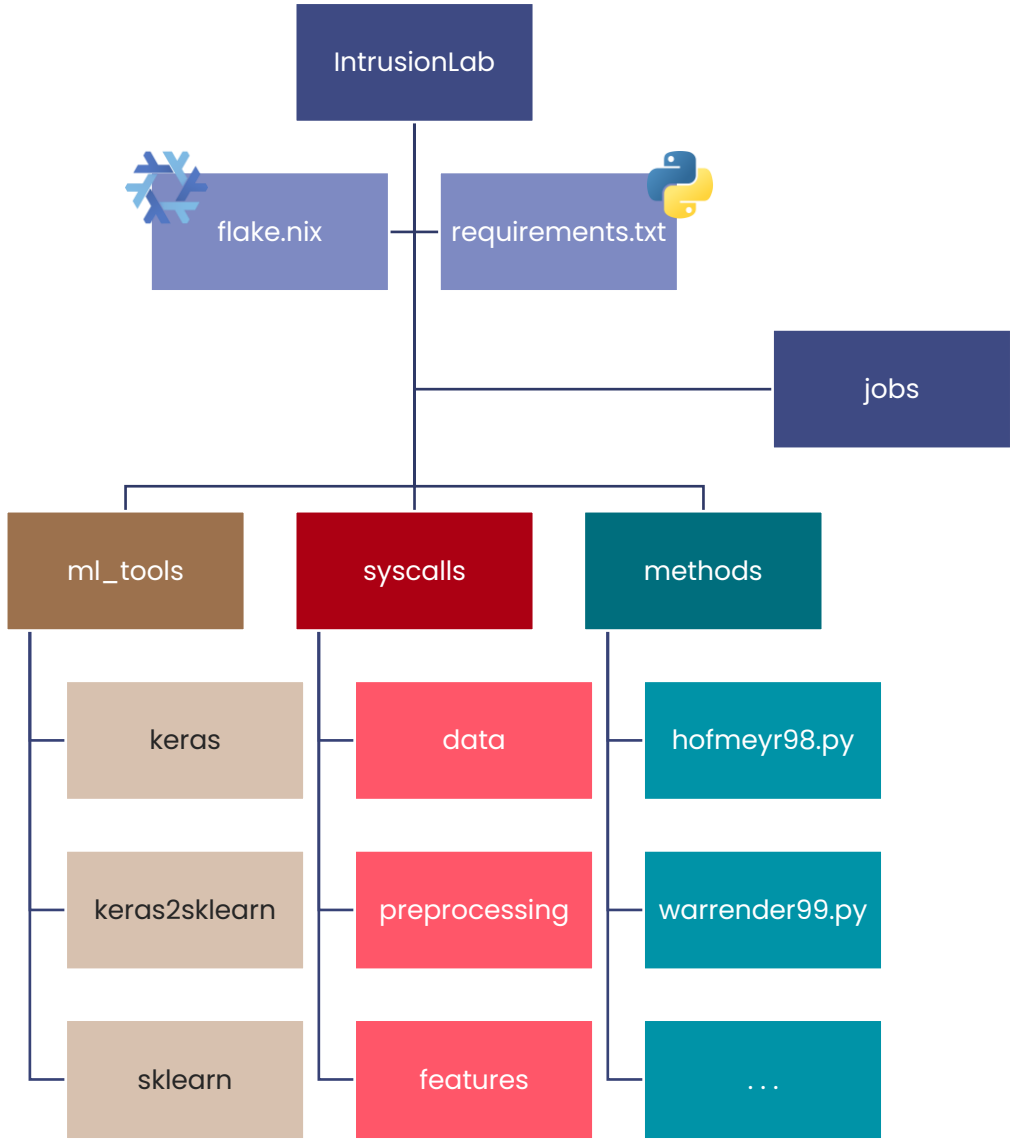
pour une évaluation expérimentale dans les mêmes conditions d'exécution

Méthodes sélectionnées

1	1998, Hofmeyr, « Intrusion Detection using sequences of system calls »	séquences de référence et comptage du nombre de mismatches (TIDE)
2, 3	1999, Warrender, « Detecting Intrusions Using System Calls: Alternative Data Models"	TIDE mais cumul des mismatches dans une période localement proche (STIDE) STIDE avec prise en compte des fréquences d'apparition dans le jeu d'entraînement (t-STIDE)
4	2003, Yeung, "Host-based intrusion detection using dynamic and static behavioral models"	Modèle de Markov caché (HMM)
5	2007, Sharma, "Intrusion detection using text processing techniques with a kernel based similarity measure"	Term Frequency (TF) + similarité sur les proches voisins et seuil
6	2013, Murtaza, "A host-based anomaly detection approach by representing system calls as states of kernel modules"	Abstraction des syscalls en 3 groupes (kernel, memory management, file system) et détection avec des seuils sur la fréquence d'apparition
7	2014, Creech, "A semantic approach to host-based intrusion detection systems using contiguous and discontiguous system call patterns"	N-grams combinés en phrases de 1 à 5 n-grams; TF des phrases de référence comme features d'entrée d'un Extreme Learning Machine.
8	2016, Nauman, "A three-way decision making approach to malware analysis using probabilistic rough sets"	Théorie des ensembles approximatifs
9	2018, Khreich, "Combining heterogeneous anomaly detectors for improved software security"	Combinaison de modèles hétérogènes (STIDE, HMM, OCSVM) dans l'espace ROC
10	2019, Marteau, "Sequence Covering for Efficient Host-Based Intrusion Detection"	Séquences recouvrantes
11	2020, Liu, "A statistical pattern based feature extraction method on system call traces for anomaly detection"	Statistiques descriptives des séquences comme features de modèles (IF, OCSVM, LOF, kNN)
12	2020, Wunderlich, "Comparison of System Call Representations for Intrusion Detection"	OHE + LSTM + Dense
13	2020, Zhang, "Early Detection of Host-based Intrusions in Linux Environment"	Considère les X premiers syscalls d'une trace pour la détection puis TF-IDF et MLP pour la prédiction
14, 15	2021, Ring, "Methods for Host-based Intrusion Detection with Deep Learning"	WaveNet et seuil sur log-likelihood ; Ensembling avec 3 WaveNets
16	2021, Subba, "A tfidfvectorizer and singular value decomposition based host intrusion detection system framework for detecting anomalous system processes"	TF-IDF + Truncated SVD + MLP
17	2021, Zhang, " Syscall-BSEM: Behavioral semantics enhancement method of system call sequence for high accurate and robust host intrusion detection"	DL et embeddings type Word2Vec; considère les séquences, une catégorisation et un encodage différentiel puis CNN pour la prédiction.
18	2023, Shamim, "Efficient Approach for Anomaly Detection in IoT Using System Calls"	Détection de patterns + chaîne de Markov

4. Architecture logicielle & résultats

Architecture logicielle



01 • Initialise l'environnement de développement (micro-mamba, venv) généré par Nix

02 • Initialise le jeu de données (ADFA-LD)

03 • Lance la pipeline de test (toutes les méthodes)

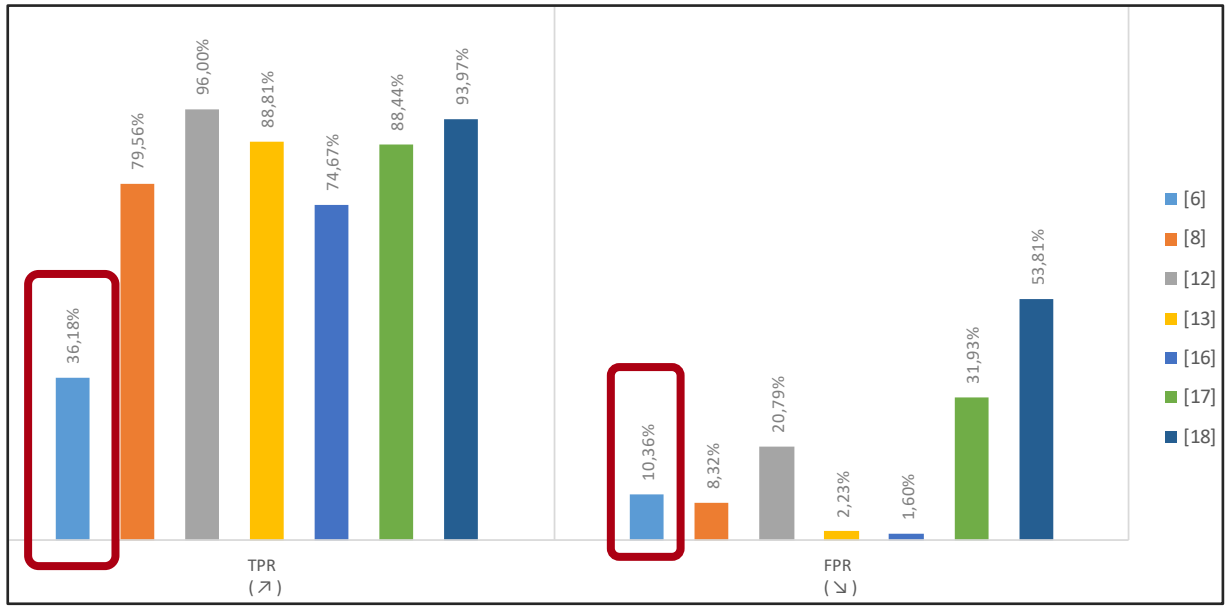
04 • Agrège les résultats de chaque méthode dans un CSV

Pas d'aléas (seeds fixées)

- Division train/validation/test du jeu de données
- Initialisation des poids TF/Keras

Résultats - performances

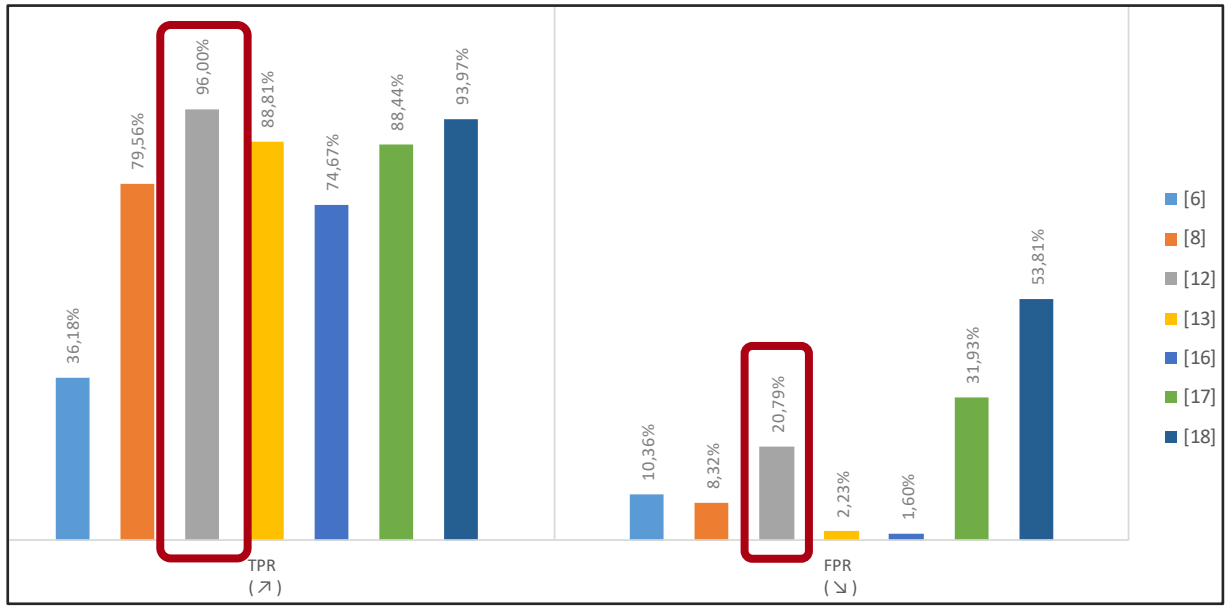
Méthodes à prédiction



6	**2013, Murtaza, "A host-based anomaly detection approach by representing system calls as states of kernel modules"**	**Abstraction des syscalls en 3 groupes (kernel, memory management, file system) et détection avec des seuils sur la fréquence d'apparition**
8	2016, Nauman, "A three-way decision making approach to malware analysis using probabilistic rough sets"	Théorie des ensembles approximatifs
12	2020, Wunderlich, "Comparison of System Call Representations for Intrusion Detection"	OHE + LSTM + Dense
13	2020, Zhang, "Early Detection of Host-based Intrusions in Linux Environment"	Considère les X premiers syscalls d'une trace pour la détection puis TF-IDF et MLP pour la prédiction
16	2021, Subba, "A tfidfvectorizer and singular value decomposition based host intrusion detection system framework for detecting anomalous system processes"	TF-IDF + Truncated SVD + MLP
17	2021, Zhang, " Syscall-BSEM: Behavioral semantics enhancement method of system call sequence for high accurate and robust host intrusion detection"	DL et embeddings type Word2Vec; considère les séquences, une catégorisation et un encodage différentiel puis CNN pour la prédiction.
18	2023, Shamim, "Efficient Approach for Anomaly Detection in IoT Using System Calls"	Détection de patterns + chaîne de Markov

Résultats – performances

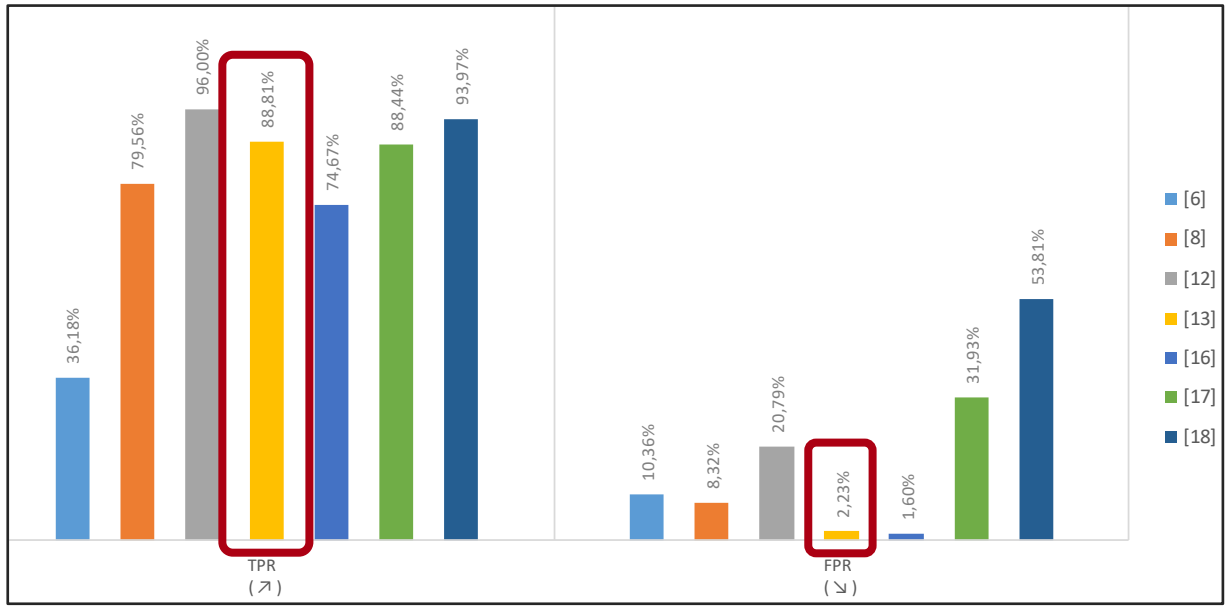
Méthodes à prédiction



6	2013, Murtaza, "A host-based anomaly detection approach by representing system calls as states of kernel modules"	Abstraction des syscalls en 3 groupes (kernel, memory management, file system) et détection avec des seuils sur la fréquence d'apparition
8	2016, Nauman, "A three-way decision making approach to malware analysis using probabilistic rough sets"	Théorie des ensembles approximatifs
12	**2020, Wunderlich, "Comparison of System Call Representations for Intrusion Detection"**	**OHE + LSTM + Dense**
13	2020, Zhang, "Early Detection of Host-based Intrusions in Linux Environment"	Considère les X premiers syscalls d'une trace pour la détection puis TF-IDF et MLP pour la prédiction
16	2021, Subba, "A tfidfvectorizer and singular value decomposition based host intrusion detection system framework for detecting anomalous system processes"	TF-IDF + Truncated SVD + MLP
17	2021, Zhang, " Syscall-BSEM: Behavioral semantics enhancement method of system call sequence for high accurate and robust host intrusion detection"	DL et embeddings type Word2Vec; considère les séquences, une catégorisation et un encodage différentiel puis CNN pour la prédiction.
18	2023, Shamim, "Efficient Approach for Anomaly Detection in IoT Using System Calls"	Détection de patterns + chaîne de Markov

Résultats – performances

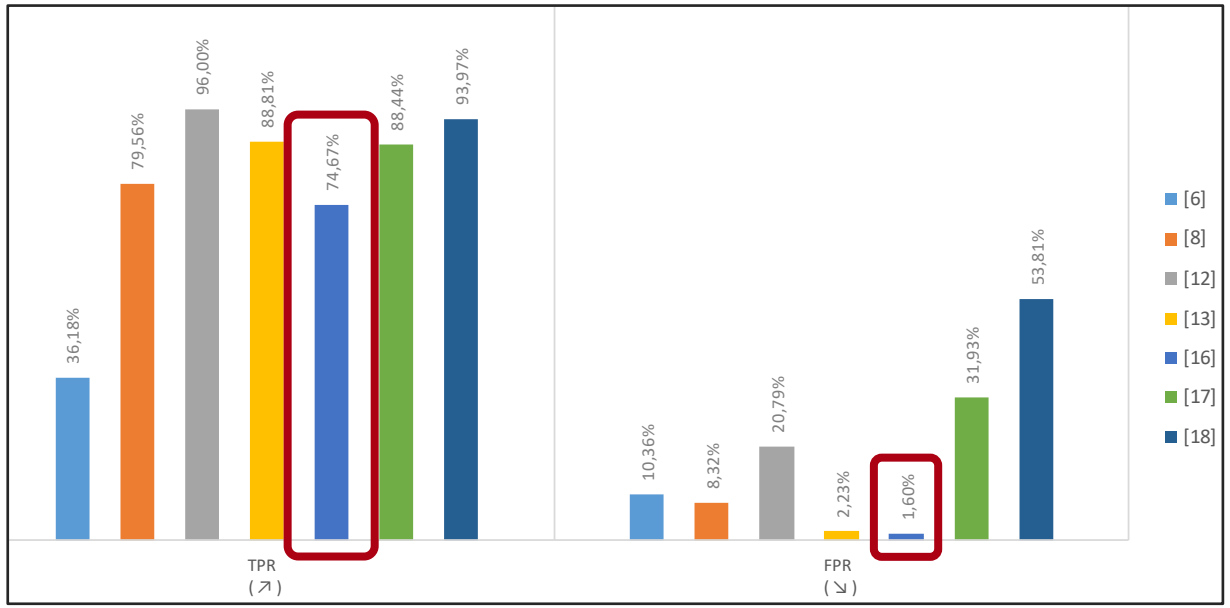
Méthodes à prédiction



6	2013, Murtaza, "A host-based anomaly detection approach by representing system calls as states of kernel modules"	Abstraction des syscalls en 3 groupes (kernel, memory management, file system) et détection avec des seuils sur la fréquence d'apparition
8	2016, Nauman, "A three-way decision making approach to malware analysis using probabilistic rough sets"	Théorie des ensembles approximatifs
12	2020, Wunderlich, "Comparison of System Call Representations for Intrusion Detection"	OHE + LSTM + Dense
13	**2020, Zhang, "Early Detection of Host-based Intrusions in Linux Environment"**	**Considère les X premiers syscalls d'une trace pour la détection puis TF-IDF et MLP pour la prédiction**
16	2021, Subba, "A tfidfvectorizer and singular value decomposition based host intrusion detection system framework for detecting anomalous system processes"	TF-IDF + Truncated SVD + MLP
17	2021, Zhang, " Syscall-BSEM: Behavioral semantics enhancement method of system call sequence for high accurate and robust host intrusion detection"	DL et embeddings type Word2Vec; considère les séquences, une catégorisation et un encodage différentiel puis CNN pour la prédiction.
18	2023, Shamim, "Efficient Approach for Anomaly Detection in IoT Using System Calls"	Détection de patterns + chaîne de Markov

Résultats – performances

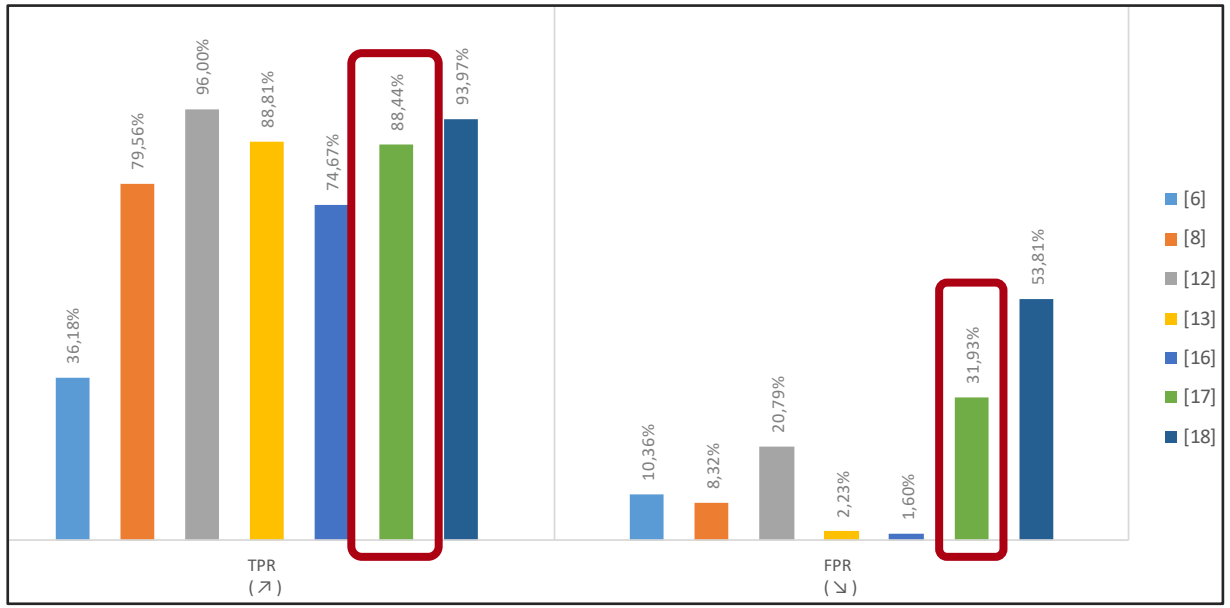
Méthodes à prédiction



6	2013, Murtaza, "A host-based anomaly detection approach by representing system calls as states of kernel modules"	Abstraction des syscalls en 3 groupes (kernel, memory management, file system) et détection avec des seuils sur la fréquence d'apparition
8	2016, Nauman, "A three-way decision making approach to malware analysis using probabilistic rough sets"	Théorie des ensembles approximatifs
12	2020, Wunderlich, "Comparison of System Call Representations for Intrusion Detection"	OHE + LSTM + Dense
13	2020, Zhang, "Early Detection of Host-based Intrusions in Linux Environment"	Considère les X premiers syscalls d'une trace pour la détection puis TF-IDF et MLP pour la prédiction
16	**2021, Subba, "A tfidfvectorizer and singular value decomposition based host intrusion detection system framework for detecting anomalous system processes"**	**TF-IDF + Truncated SVD + MLP**
17	2021, Zhang, " Syscall-BSEM: Behavioral semantics enhancement method of system call sequence for high accurate and robust host intrusion detection"	DL et embeddings type Word2Vec; considère les séquences, une catégorisation et un encodage différentiel puis CNN pour la prédiction.
18	2023, Shamim, "Efficient Approach for Anomaly Detection in IoT Using System Calls"	Détection de patterns + chaîne de Markov

Résultats – performances

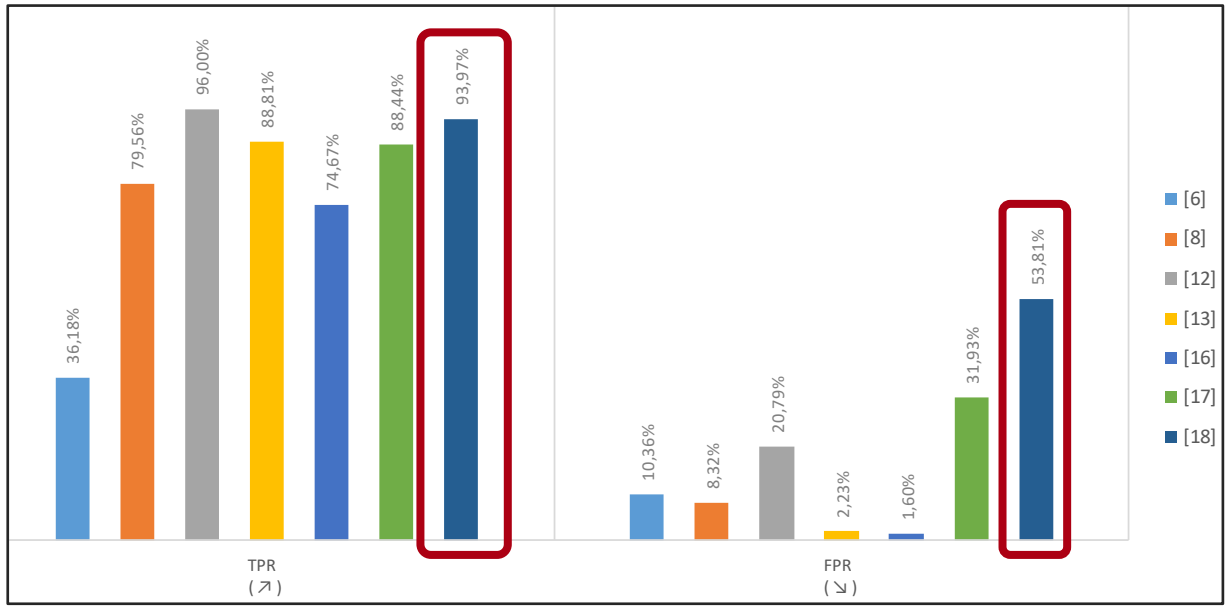
Méthodes à prédiction



6	2013, Murtaza, "A host-based anomaly detection approach by representing system calls as states of kernel modules"	Abstraction des syscalls en 3 groupes (kernel, memory management, file system) et détection avec des seuils sur la fréquence d'apparition
8	2016, Nauman, "A three-way decision making approach to malware analysis using probabilistic rough sets"	Théorie des ensembles approximatifs
12	2020, Wunderlich, "Comparison of System Call Representations for Intrusion Detection"	OHE + LSTM + Dense
13	2020, Zhang, "Early Detection of Host-based Intrusions in Linux Environment"	Considère les X premiers syscalls d'une trace pour la détection puis TF-IDF et MLP pour la prédiction
16	2021, Subba, "A tfidfvectorizer and singular value decomposition based host intrusion detection system framework for detecting anomalous system processes"	TF-IDF + Truncated SVD + MLP
17	**2021, Zhang, " Syscall-BSEM: Behavioral semantics enhancement method of system call sequence for high accurate and robust host intrusion detection"**	**DL et embeddings type Word2Vec; considère les séquences, une catégorisation et un encodage différentiel puis CNN pour la prédiction.**
18	2023, Shamim, "Efficient Approach for Anomaly Detection in IoT Using System Calls"	Détection de patterns + chaîne de Markov

Résultats – performances

Méthodes à prédiction



6	2013, Murtaza, "A host-based anomaly detection approach by representing system calls as states of kernel modules"	Abstraction des syscalls en 3 groupes (kernel, memory management, file system) et détection avec des seuils sur la fréquence d'apparition
8	2016, Nauman, "A three-way decision making approach to malware analysis using probabilistic rough sets"	Théorie des ensembles approximatifs
12	2020, Wunderlich, "Comparison of System Call Representations for Intrusion Detection"	OHE + LSTM + Dense
13	2020, Zhang, "Early Detection of Host-based Intrusions in Linux Environment"	Considère les X premiers syscalls d'une trace pour la détection puis TF-IDF et MLP pour la prédiction
16	2021, Subba, "A tfidfvectorizer and singular value decomposition based host intrusion detection system framework for detecting anomalous system processes"	TF-IDF + Truncated SVD + MLP
17	2021, Zhang, " Syscall-BSEM: Behavioral semantics enhancement method of system call sequence for high accurate and robust host intrusion detection"	DL et embeddings type Word2Vec; considère les séquences, une catégorisation et un encodage différentiel puis CNN pour la prédiction.
18	**2023, Shamim, "Efficient Approach for Anomaly Detection in IoT Using System Calls"**	**Détection de patterns + chaîne de Markov**

Résultats – performances

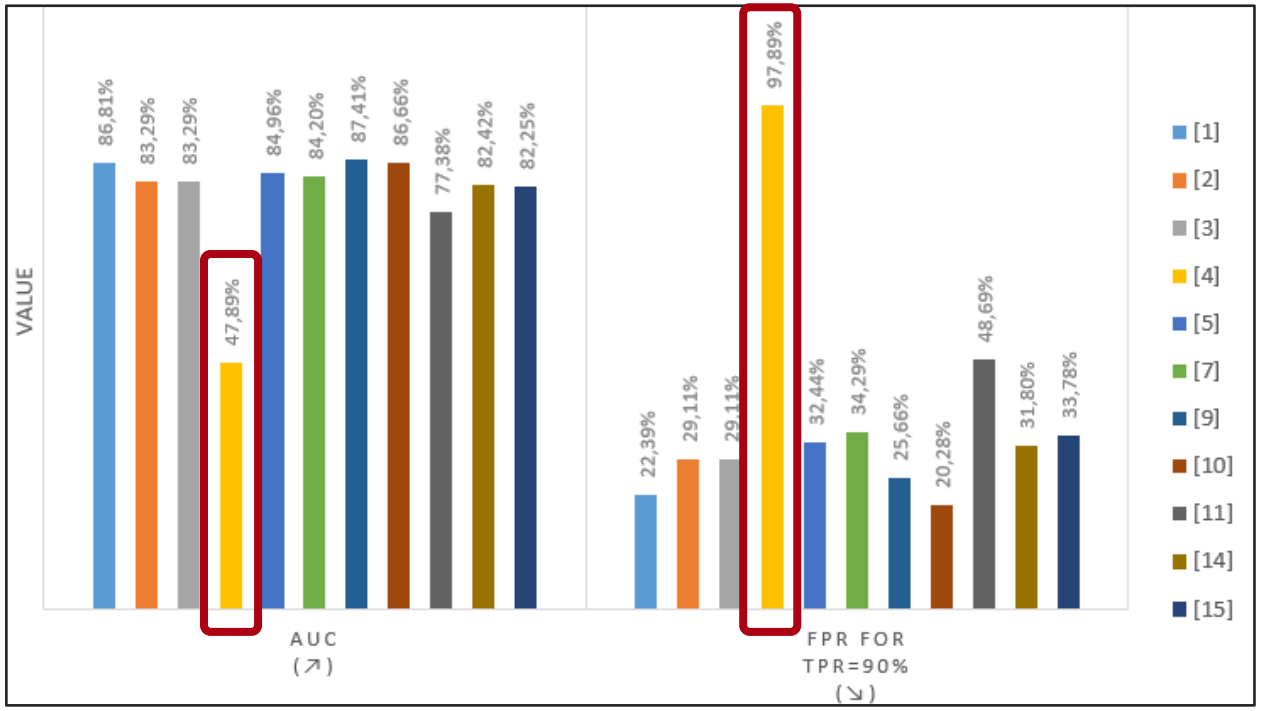
1	**1998, Hofmeyr, « Intrusion Detection using sequences of system calls »**	**séquences de référence et comptage du nombre de mismatches (TIDE)**
2, 3	1999, Warrender, « Detecting Intrusions Using System Calls: Alternative Data Models"	TIDE mais cumul des mismatches dans une période localement proche (STIDE) STIDE avec prise en compte des fréquences d'apparition dans le jeu d'entraînement (t-STIDE)
4	2003, Yeung, "Host-based intrusion detection using dynamic and static behavioral models"	Modèle de Markov caché (HMM)
5	2007, Sharma, "Intrusion detection using text processing techniques with a kernel based similarity measure"	Term Frequency (TF) + similarité sur les proches voisins et seuil
7	2014, Creech, "A semantic approach to host-based intrusion detection systems using contiguous and discontiguous system call patterns"	N-grams combinés en phrases de 1 à 5 n-grams; TF des phrases de référence comme features d'entrée d'un Extreme Learning Machine.
9	2018, Khreich, "Combining heterogeneous anomaly detectors for improved software security"	Combinaison de modèles hétérogènes (STIDE, HMM, OCSVM) dans l'espace ROC
10	2019, Marteau, "Sequence Covering for Efficient Host-Based Intrusion Detection"	Séquences recouvrantes
11	2020, Liu, "A statistical pattern based feature extraction method on system call traces for anomaly detection"	Statistiques descriptives des séquences comme features de modèles (IF, OCSVM, LOF, kNN)
14, 15	2021, Ring, "Methods for Host-based Intrusion Detection with Deep Learning"	WaveNet et seuil sur log-likelihood ; Ensembling avec 3 WaveNets

Méthodes à score

Résultats – performances

1	1998, Hofmeyr, « Intrusion Detection using sequences of system calls »	séquences de référence et comptage du nombre de mismatches (TIDE)
2, 3	1999, Warrender, « Detecting Intrusions Using System Calls: Alternative Data Models"	TIDE mais cumul des mismatches dans une période localement proche (STIDE) STIDE avec prise en compte des fréquences d'apparition dans le jeu d'entraînement (t-STIDE)
4	**2003, Yeung, "Host-based intrusion detection using dynamic and static behavioral models"**	**Modèle de Markov caché (HMM)**
5	2007, Sharma, "Intrusion detection using text processing techniques with a kernel based similarity measure"	Term Frequency (TF) + similarité sur les proches voisins et seuil
7	2014, Creech, "A semantic approach to host-based intrusion detection systems using contiguous and discontiguous system call patterns"	N-grams combinés en phrases de 1 à 5 n-grams; TF des phrases de référence comme features d'entrée d'un Extreme Learning Machine.
9	2018, Khreich, "Combining heterogeneous anomaly detectors for improved software security"	Combinaison de modèles hétérogènes (STIDE, HMM, OCSVM) dans l'espace ROC
10	2019, Marteau, "Sequence Covering for Efficient Host-Based Intrusion Detection"	Séquences recouvrantes
11	2020, Liu, "A statistical pattern based feature extraction method on system call traces for anomaly detection"	Statistiques descriptives des séquences comme features de modèles (IF, OCSVM, LOF, kNN)
14, 15	2021, Ring, "Methods for Host-based Intrusion Detection with Deep Learning"	WaveNet et seuil sur log-likelihood ; Ensembling avec 3 WaveNets

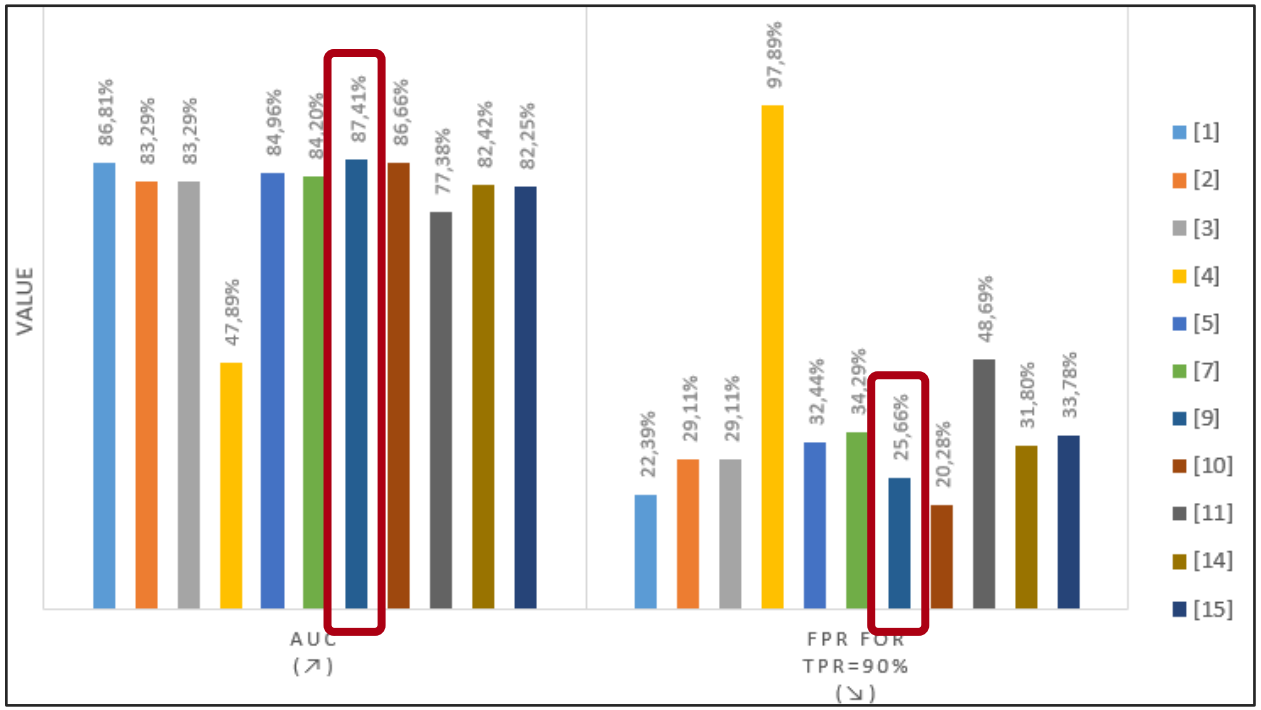
Méthodes à score



Résultats – performances

1	1998, Hofmeyr, « Intrusion Detection using sequences of system calls »	séquences de référence et comptage du nombre de mismatches (TIDE)
2, 3	1999, Warrender, « Detecting Intrusions Using System Calls: Alternative Data Models"	TIDE mais cumul des mismatches dans une période localement proche (STIDE) STIDE avec prise en compte des fréquences d'apparition dans le jeu d'entraînement (t-STIDE)
4	2003, Yeung, "Host-based intrusion detection using dynamic and static behavioral models"	Modèle de Markov caché (HMM)
5	2007, Sharma, "Intrusion detection using text processing techniques with a kernel based similarity measure"	Term Frequency (TF) + similarité sur les proches voisins et seuil
7	2014, Creech, "A semantic approach to host-based intrusion detection systems using contiguous and discontiguous system call patterns"	N-grams combinés en phrases de 1 à 5 n-grams; TF des phrases de référence comme features d'entrée d'un Extreme Learning Machine.
9	**2018, Khreich, "Combining heterogeneous anomaly detectors for improved software security"**	**Combinaison de modèles hétérogènes (STIDE, HMM, OCSVM) dans l'espace ROC**
10	2019, Marteau, "Sequence Covering for Efficient Host-Based Intrusion Detection"	Séquences recouvrantes
11	2020, Liu, "A statistical pattern based feature extraction method on system call traces for anomaly detection"	Statistiques descriptives des séquences comme features de modèles (IF, OCSVM, LOF, kNN)
14, 15	2021, Ring, "Methods for Host-based Intrusion Detection with Deep Learning"	WaveNet et seuil sur log-likelihood ; Ensembling avec 3 WaveNets

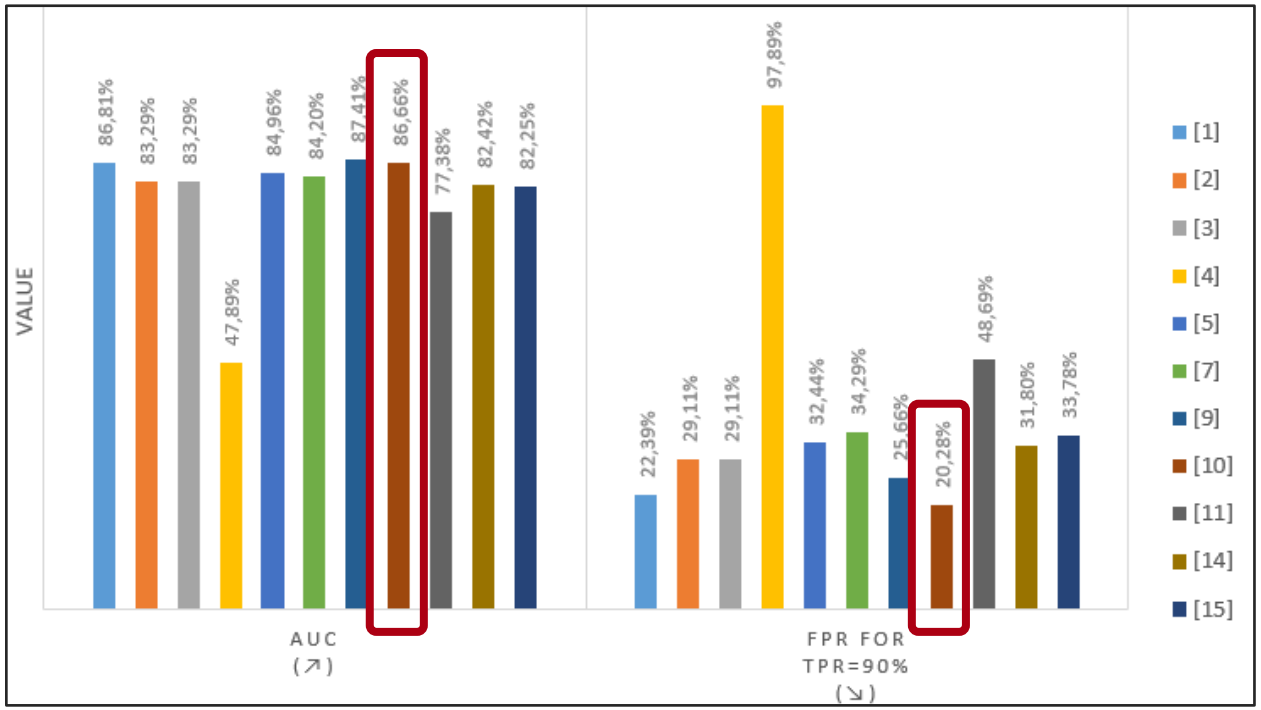
Méthodes à score



Résultats – performances

1	1998, Hofmeyr, « Intrusion Detection using sequences of system calls »	séquences de référence et comptage du nombre de mismatches (TIDE)
2, 3	1999, Warrender, « Detecting Intrusions Using System Calls: Alternative Data Models"	TIDE mais cumul des mismatches dans une période localement proche (STIDE) STIDE avec prise en compte des fréquences d'apparition dans le jeu d'entraînement (t-STIDE)
4	2003, Yeung, "Host-based intrusion detection using dynamic and static behavioral models"	Modèle de Markov caché (HMM)
5	2007, Sharma, "Intrusion detection using text processing techniques with a kernel based similarity measure"	Term Frequency (TF) + similarité sur les proches voisins et seuil
7	2014, Creech, "A semantic approach to host-based intrusion detection systems using contiguous and discontiguous system call patterns"	N-grams combinés en phrases de 1 à 5 n-grams; TF des phrases de référence comme features d'entrée d'un Extreme Learning Machine.
9	2018, Khreich, "Combining heterogeneous anomaly detectors for improved software security"	Combinaison de modèles hétérogènes (STIDE, HMM, OCSVM) dans l'espace ROC
10	**2019, Marteau, "Sequence Covering for Efficient Host-Based Intrusion Detection"**	**Séquences recouvrantes**
11	2020, Liu, "A statistical pattern based feature extraction method on system call traces for anomaly detection"	Statistiques descriptives des séquences comme features de modèles (IF, OCSVM, LOF, kNN)
14, 15	2021, Ring, "Methods for Host-based Intrusion Detection with Deep Learning"	WaveNet et seuil sur log-likelihood ; Ensembling avec 3 WaveNets

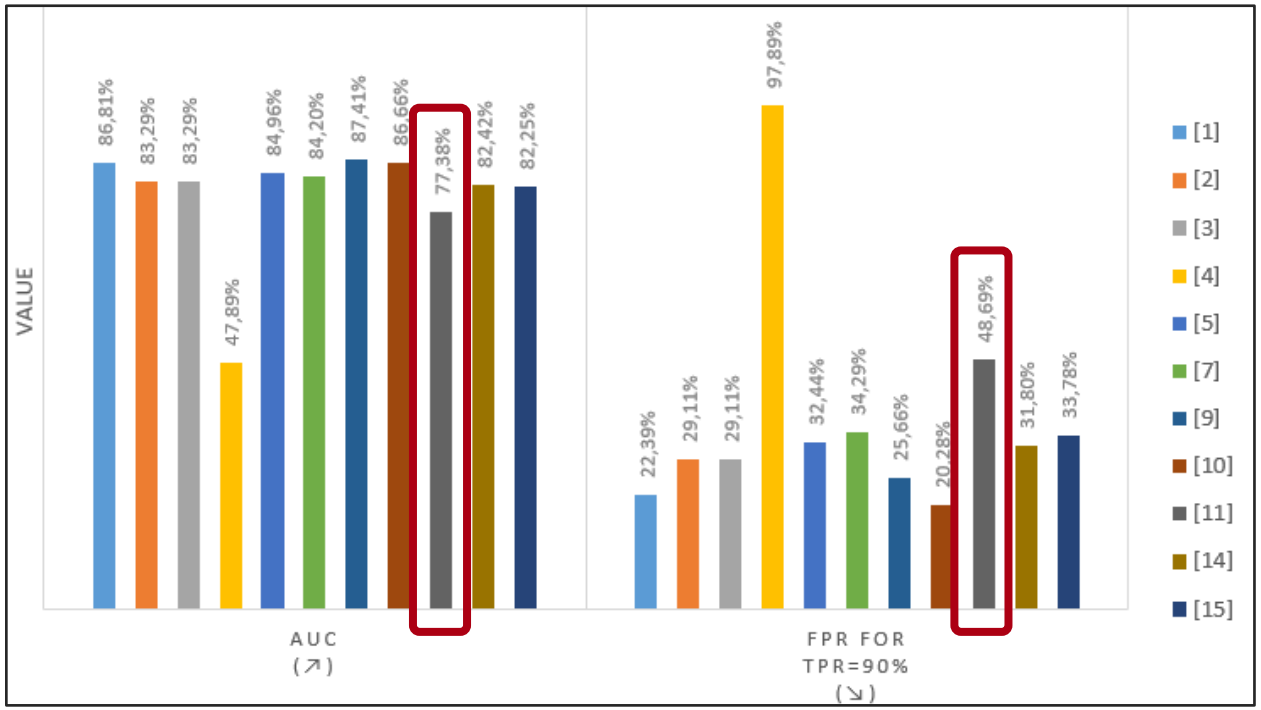
Méthodes à score



Résultats – performances

1	1998, Hofmeyr, « Intrusion Detection using sequences of system calls »	séquences de référence et comptage du nombre de mismatches (TIDE)
2, 3	1999, Warrender, « Detecting Intrusions Using System Calls: Alternative Data Models"	TIDE mais cumul des mismatches dans une période localement proche (STIDE) STIDE avec prise en compte des fréquences d'apparition dans le jeu d'entraînement (t-STIDE)
4	2003, Yeung, "Host-based intrusion detection using dynamic and static behavioral models"	Modèle de Markov caché (HMM)
5	2007, Sharma, "Intrusion detection using text processing techniques with a kernel based similarity measure"	Term Frequency (TF) + similarité sur les proches voisins et seuil
7	2014, Creech, "A semantic approach to host-based intrusion detection systems using contiguous and discontiguous system call patterns"	N-grams combinés en phrases de 1 à 5 n-grams; TF des phrases de référence comme features d'entrée d'un Extreme Learning Machine.
9	2018, Khreich, "Combining heterogeneous anomaly detectors for improved software security"	Combinaison de modèles hétérogènes (STIDE, HMM, OCSVM) dans l'espace ROC
10	2019, Marteau, "Sequence Covering for Efficient Host-Based Intrusion Detection"	Séquences recouvrantes
11	**2020, Liu, "A statistical pattern based feature extraction method on system call traces for anomaly detection"**	**Statistiques descriptives des séquences comme features de modèles (IF, OCSVM, LOF, kNN)**
14, 15	2021, Ring, "Methods for Host-based Intrusion Detection with Deep Learning"	WaveNet et seuil sur log-likelihood ; Ensembling avec 3 WaveNets

Méthodes à score



Résultats – overhead

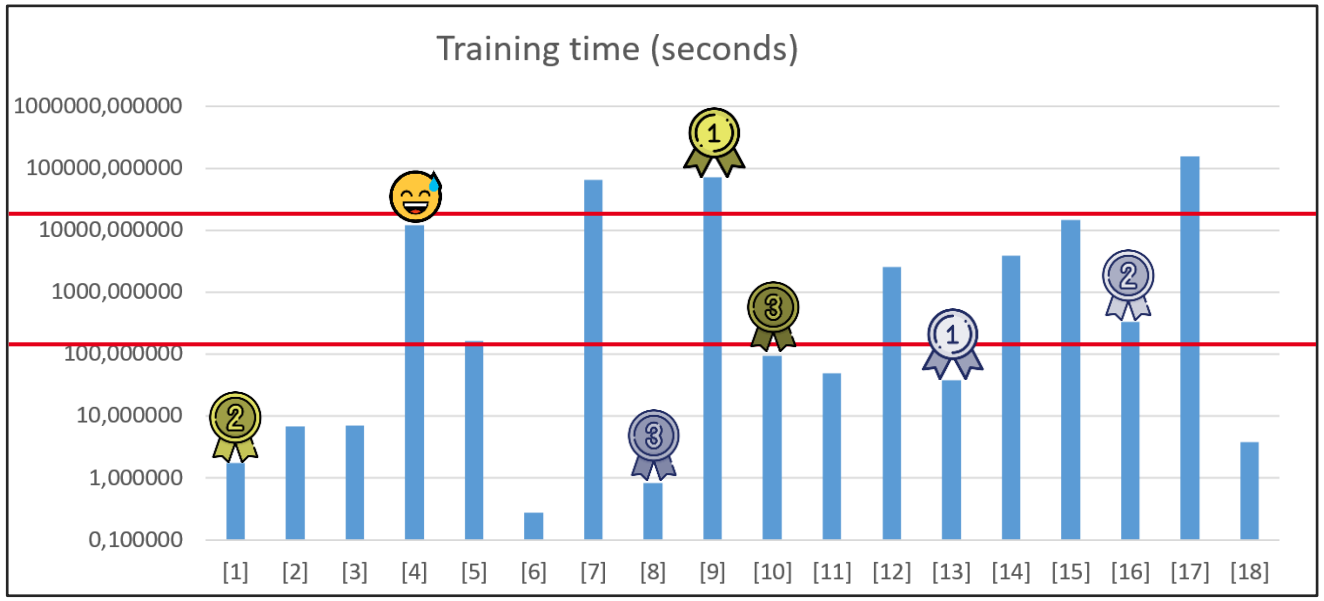
CPU : Intel bi-Xeon Gold 6348, 2x28 cœurs, 2.6GHz (Turbo 3.5GHz)
RAM : 512Go
GPU : Nvidia Tesla A100, 80Go VRAM
OS : SL7

[1]	**Hofmeyr98**
[2]	Warrender99 (STIDE)
[3]	Warrender99 (tSTIDE)
[4]	Yeung03
[5]	Sharma07
[6]	Murtaza13
[7]	Creech14
[8]	Nauman16
[9]	**Kreich18**
[10]	**Marteau19**
[11]	Liu20
[12]	**Wunderlich20**
[13]	**Zhang20**
[14]	Ring21 (simple)
[15]	Ring21 (ensembling)
[16]	**Subba21**
[17]	Zhang21
[18]	Shamim23

Classement selon f1-score pour méthodes à prédiction, et selon AUC pour méthodes à score

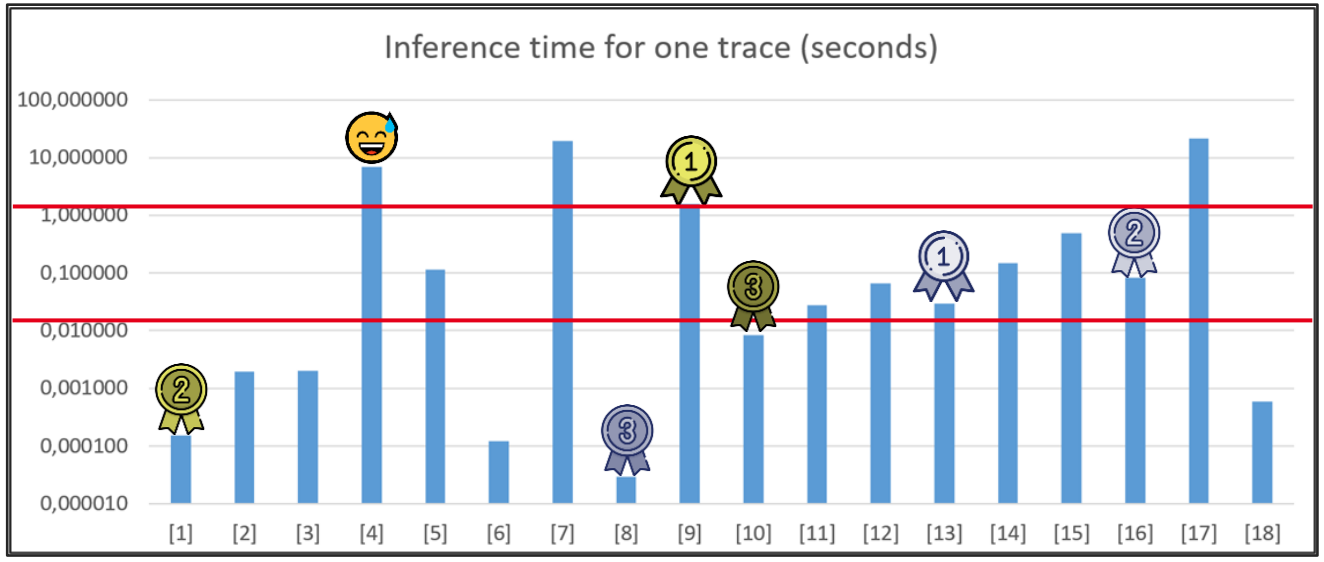
Moyenne = 3,3h

Médiane = 128s



Moyenne = 2,79s

Médiane = 0,04s



5. Conclusion

Conclusion

- Nouveau ne veut pas dire meilleur
- Des modèles complexes n'obtiennent pas forcément de meilleurs résultats

- Mais… attention au dataset !
  - **ADFA-LD, 2013 :** Ubuntu 11.04 (kernel 2.6.38 32 bits, **EOL 2011**), 6 attaques dont 1 CVE

- Peu d'articles traitant de systèmes embarqués (5/200)
  - Pas de dataset public

Biais possibles

- Biais de sélection
  - plusieurs librairies
  - critères d'inclusion et d'exclusion clairs et objectifs
- Biais d'analyse
  - lecture itérative
  - relecture croisée entre auteurs
- Biais dans la réimplémentation des méthodes
  - reproduction des résultats obtenus par les auteurs
  - prise de contact avec les auteurs en cas de résultats différents
  - relecture croisée entre auteurs (publications + code)

Merci !

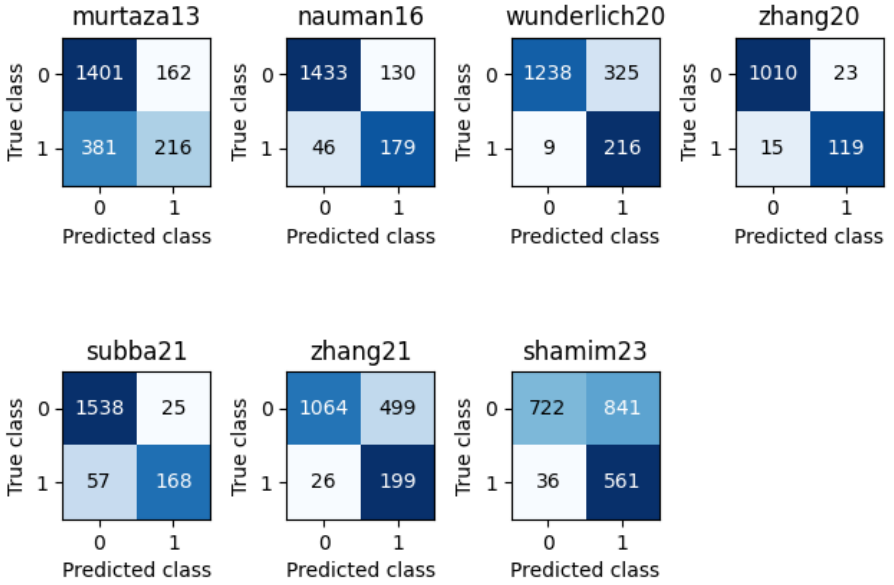
Lalie ARNOUD

lalie.arnoud@cea.fr

Images from www.freepik.com
and www.flaticon.com

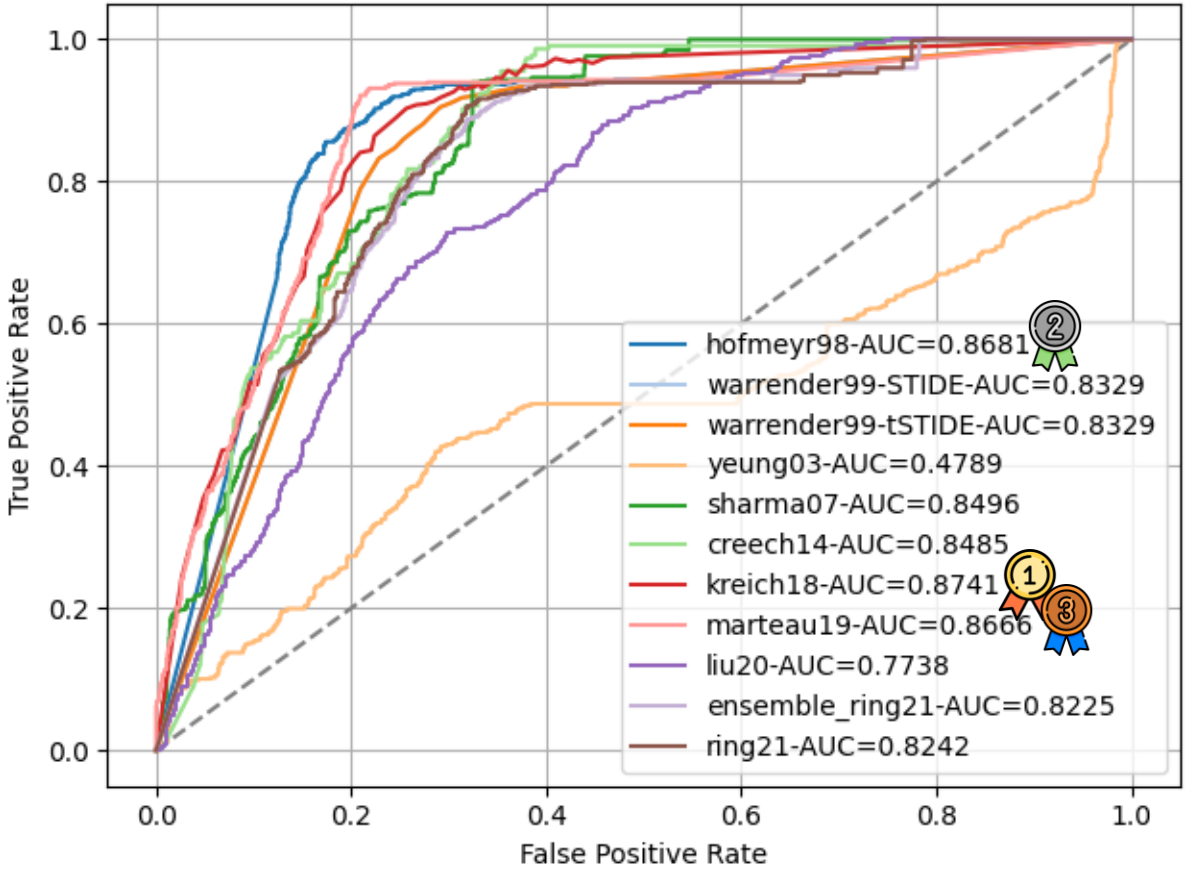
Résultats – performances

Méthodes à classification



Method	Acc	Balanced Acc	TPR	FPR	Precision	F1-score
murtaza13	0.7486	0.6290	0.3618	0.1036	0.5714	0.4430
nauman16	0.9015	0.8561	0.7955	0.0831	0.5792	0.6704
wunderlich20	0.8131	0.8760	**0.9600**	0.2079	0.3992	0.5639
zhang20	**0.9674**	**0.9328**	0.8880	0.0222	0.8380	**0.8623**
subba21	0.9541	0.8653	0.7466	**0.0159**	**0.8704**	0.8038
zhang21	0.7063	0.7825	0.8844	0.3192	0.2851	0.43120
shamim23	0.5939	0.7008	0.9396	0.5380	0.4001	0.56128

Méthodes à score



Méthodes sélectionnées – 16 papiers, 18 méthodes

Est-ce que des déviations du comportement normal peuvent être détectées…

- **… depuis un dictionnaire de séquences de référence ? (méthodes de référence)**
  - TIDE (« Intrusion Detection using sequences of system calls », Hofmeyr et al., 1998)
  - STIDE, t-STIDE (« Detecting Intrusions Using System Calls: Alternative Data Models », Warrender et al., 1999)
- **… par un HMM ?**
  - « Host-based intrusion detection using dynamic and static behavioral models », Yeung et al., 2003
- **… par une analyse des fréquences d'apparition des syscalls ?**
  - « Intrusion detection using text processing techniques with a kernel based similarity measure », Sharma et al., 2007
- **… par une analyse fréquentielle d'apparition de la catégorie fonctionnelle des syscalls (memory management, file system, network, …) ?**
  - « A host-based anomaly detection approach by representing system calls as states of kernel modules », Murtaza et al., 2013
- **… par une analyse fréquentielle d'apparition de combinaisons de n-grams ?**
  - « A semantic approach to host-based intrusion detection systems using contiguous and discontibuous system call patterns », Creech et al., 2014
- **… par une classification utilisant la théorie des ensembles approximatifs ?**
  - « A three-way decision making approach to malware analysis using probabilistic rough sets », Nauman et al., 2016
- **… par une combinaison de modèles hétérogènes (STIDE, HMM, OCSVM) dans l'espace ROC ?**
  - « Combining heterogeneous anomaly detectors for improved software security », Khreich et al., 2018

Méthodes sélectionnées – 16 papiers, 18 méthodes

Est-ce que des déviations du comportement normal peuvent être détectées…

- **… par la recherche de séquences recouvrantes depuis un dictionnaire de séquences de référence**
  - « Sequence Covering for Efficient Host-Based Intrusion Detection », Marteau et al., 2019
- **… par l'analyse de métriques statistiques descriptives de la composition des séquences**
  - « A statistical pattern based feature extraction method on system call traces for anomaly detection», Liu et al., 2020
- **… par une analyse des fréquences d'apparition seulement sur les premiers syscalls de chaque processus ?**
  - « Early Detection of Host-based Intrusions in Linux Environment», Zhang et al., 2020
- **… par un LSTM ?**
  - « Comparison of System Call Representations for Intrusion Detection», Wunderlich et al., 2020
- **… par une analyse fréquentielle d'apparition de certains appels systèmes ?**
  - « A tfidfvectorizer and singular value decomposition based host intrusion detection system framework for detecting anomalous system processes», Subba et al., 2021
- **… par une usine à gaz ? (embeddings Word2Vec + encodage différentiel + catégorisation → CNN)**
  - « Syscall-BSEM: Behavioral semantics enhancement method of system call sequence for high accurate and robust host intrusion detection», Zhang et al., 2021
- **… par un modèle génératif à base de convolutions (WaveNet), et son ensembling ?**
  - « Methods for Host-based Intrusion Detection with Deep Learning», Ring et al., 2021
- **… par une détection de motifs suivi d'une chaîne de Markov ?**
  - « Efficient Approach for Anomaly Detection in IoT Using System Calls », Shamim et al., 2023