# ML Project

## Intrusion Detection System

**

*Préparé par :*

*Mohamed Wahchi*

*Malek Hmem*

*Kalthoum Dridi*

*Selim Sahli*

*Nour Hassine*

*Khouloud Zograni*

Introduction

À l'ère de la connectivité numérique, où les réseaux informatiques sont devenus les fondations essentielles de notre monde interconnecté, la sécurité des données et des systèmes revêt une importance capitale. Les progrès technologiques ont créé un paysage dynamique, mais ont également ouvert la porte à une diversité croissante de menaces cybernétiques. Dans ce contexte, la préservation de l'intégrité des réseaux devient une priorité absolue.

Notre projet s'inscrit dans cet environnement complexe et en constante évolution, cherchant à renforcer la sécurité des réseaux à travers des approches innovantes. Alors que les défenses traditionnelles peuvent parfois se révéler insuffisantes face à des attaques sophistiquées et émergentes, notre démarche se concentre sur l'intégration de solutions avancées.

Nous explorons spécifiquement les possibilités offertes par les techniques d'apprentissage automatique pour anticiper, détecter, et contrer les menaces émergentes, tout en minimisant les risques de faux positifs et de faux négatifs.

En adoptant une perspective holistique, notre projet vise à contribuer à l'évolution des défenses numériques, offrant une réponse adaptative aux défis de sécurité contemporains. En mettant l'accent sur l'innovation, nous aspirons à renforcer la résilience des réseaux, assurant ainsi la stabilité et la sécurité des infrastructures informatiques au cœur de notre société interconnectée.

C'est dans ce paysage complexe de la cybersécurité que les Systèmes de Détection d'Intrusion (IDS) émergent comme des acteurs essentiels, dédiés à la protection des réseaux contre des menaces en constante évolution. Ces systèmes, conçus pour anticiper et contrer les activités malveillantes, jouent un rôle crucial dans le maintien de la sécurité des réseaux. Leur importance découle de leur capacité à identifier non seulement les attaques connues, mais aussi à détecter des anomalies et des schémas inédits grâce à des méthodes avancées telles que l'apprentissage automatique.

1. Etude du sujet :
2. **Définition de l’IDS :**

Les Systèmes de Détection d'Intrusion (IDS) sont des piliers essentiels de la cybersécurité contemporaine, jouant un rôle crucial dans la protection des réseaux informatiques contre une diversité de menaces en constante évolution. Ces systèmes sont conçus pour surveiller en temps réel les activités du réseau, identifiant les comportements malveillants et les anomalies qui pourraient indiquer une tentative d'intrusion.

L'importance cruciale des IDS dans la cybersécurité moderne réside dans leur capacité à anticiper, détecter et répondre rapidement aux menaces émergentes.

En offrant une protection proactive, les IDS renforcent la résilience des réseaux, assurant ainsi la confidentialité, l'intégrité et la disponibilité des données dans un paysage numérique en constante évolution.

1. **Types de l’IDS :**

La construction d'un IDS repose sur deux approches fondamentales : les IDS basés sur des signatures et les IDS basés sur des anomalies.

**IDS basés sur des Signatures :**

* Identification des attaques par la comparaison avec des signatures préalablement identifiées.
* Utilisation de bases de données de signatures pour repérer des schémas de données malveillants.
* Efficaces contre des attaques bien connues et documentées.
* Limitations face à des attaques inédites qui ne correspondent pas à des signatures connues.
* Fonctionnent principalement sur la reconnaissance de modèles spécifiques associés à des attaques connues.

**IDS basés sur des Anomalies :**

* Exploitation de techniques d'apprentissage automatique pour analyser le trafic en temps réel.
* Détection de comportements anormaux en comparant le flux de données actuel avec des modèles historiques.
* Adaptatifs aux attaques nouvelles et émergentes.
* Risque de générer des faux positifs en identifiant parfois des activités normales comme anormales.
* Recherche de déviations par rapport aux schémas normaux plutôt que de se baser sur des signatures spécifiques.

Ces deux approches complémentaires sont souvent intégrées dans des systèmes d'IDS hybrides pour tirer parti de leurs forces respectives et atténuer leurs faiblesses respectives :

**IDS Hybrides :**

* Intègrent à la fois des signatures et des techniques d'analyse comportementale pour une détection plus robuste.
* Combinent les avantages des approches basées sur des signatures et des anomalies pour une meilleure couverture de sécurité.

1. **Les formes de l’IDS:**

Les systèmes de détection d'intrusions (IDS) sont des gardiens essentiels de la cybersécurité, adoptant diverses formes pour prévenir et identifier les menaces numériques. Que ce soit à travers des approches basées sur des signatures ou des anomalies, des déploiements réseau, hôtes, sans fil, physiques, virtuels ou même dans le cloud, chaque forme d'IDS offre des avantages spécifiques dans la protection des infrastructures contre les attaques informatiques.

1. **L’IDS Réseau :**

* Surveillent le trafic sur le réseau pour identifier les activités suspectes.
* Peuvent être déployés à différents niveaux du réseau, du périmètre externe aux segments internes.

1. **L’IDS Hôte :**

* Se concentrent sur l'activité au niveau des hôtes individuels, tels que les serveurs ou les postes de travail.
* Détectent les tentatives d'intrusion en surveillant les fichiers système, les journaux d'événements, etc.

1. **IDS Sans Fil :**

* Spécifiquement conçus pour surveiller et détecter les menaces sur les réseaux sans fil.
* Identifient les comportements suspects dans le trafic Wi-Fi et les communications sans fil.

1. **L’IDS Physiques et Virtuels :**

* Les IDS physiques sont des appareils matériels dédiés, tandis que les IDS virtuels sont des logiciels exécutés sur des machines virtuelles.
* Offrent une flexibilité de déploiement en fonction des besoins de l'infrastructure.

1. **Le Cloud-based IDS :**

* S'adaptent aux environnements cloud en surveillant le trafic et les activités au sein des services cloud.
* Fournissent une visibilité dans des environnements cloud dynamiques et évolutifs.

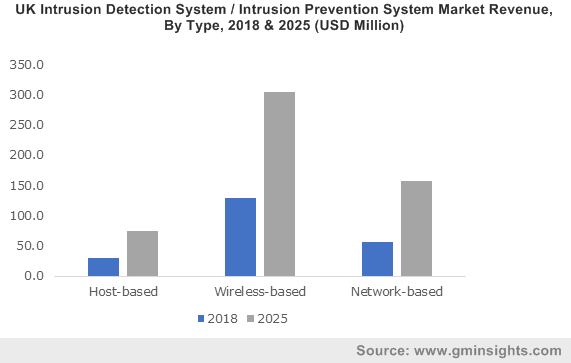
### **Statistiques mondiales sur l’IDS:**

La menace croissante de violations de données et la croissante de la numérisation ont été responsables de la croissance de la part de marché des systèmes de détection d'intrusions au cours des dernières années.

La mise en œuvre de systèmes de détection d'intrusions (IDS) dans le système réseau permet incontestablement aux administrateurs réseau d'évaluer l'emplacement précis des menaces et de les traiter. Ces systèmes contribuent également à prévenir de nouvelles menaces en ces endroits, accélérant ainsi la croissance de l'industrie des IDS.

Le graphique ci-dessus illustre la répartition des revenus du marché britannique des IDS selon trois types : basé sur l'hôte, basé sur le sans fil et basé sur le réseau, en 2018 et les projections pour 2025.

On observe une croissance significative des revenus, mettant en évidence la demande croissante pour ces types spécifiques de systèmes de détection d'intrusions au Royaume-Uni. Ces chiffres reflètent la reconnaissance croissante de l'importance des IDS dans le contexte de la cybersécurité au Royaume-Uni.

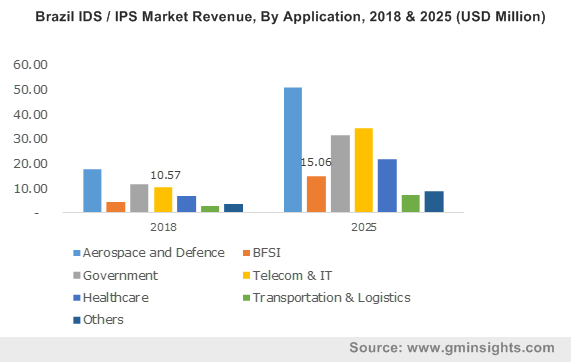


On peut aussi citer que selon des statistiques récentes, la demande d'IDS a connu une croissance significative dans divers secteurs tels que la finance, la santé, les télécommunications et l'énergie.

Une analyse des parts du marché au Brésil, de 2019 à 2025, révèle une tendance marquée vers une adoption accrue de l'IDS.

Le secteur de la défense aérospatiale et le domaine de la santé, confrontés à des défis croissants liés à la confidentialité des dossiers médicaux, ont intensifié leur utilisation d'IDS pour garantir la sécurité des informations médicales.

Cette tendance est corroborée par un graphique illustrant la répartition des parts de marché par revenu, soulignant l'importance croissante de l'IDS dans le paysage de la cybersécurité au Brésil. Cette évolution démontre clairement que les entreprises reconnaissent l'IDS comme une stratégie indispensable pour faire face aux menaces cybernétiques de plus en plus sophistiquées et souligne la nécessité continue d'investir dans des solutions de détection des intrusions pour assurer la résilience des infrastructures numériques.



1. Business Problem :

La problématique métier au cœur de ce projet réside dans la nécessité de renforcer la sécurité du réseau face à une diversité croissante d'attaques cybernétiques.

Les menaces évoluent constamment, rendant le pare-feu traditionnel incapable de protéger efficacement le réseau. Dans ce contexte, l'essor de l'apprentissage automatique offre une opportunité significative pour renforcer les capacités des systèmes de détection d'intrusion.

**Face à la complexité croissante des attaques, comment intégrer de manière efficace les techniques d'apprentissage automatique à un Intrusion Detection System (IDS) pour détecter, comprendre, et contrer les activités malveillantes dans un système ou un réseau?**

Cette question centrale guide notre exploration pour élaborer des solutions innovantes, capitalisant sur les avancées de l'apprentissage automatique pour améliorer la résilience et la réactivité des systèmes de sécurité face aux menaces numériques en constante mutation.

1. Business Understanding :

Dans le paysage en constante évolution de la cybersécurité, la sophistication croissante et la diversité des menaces cybernétiques posent un défi significatif aux mesures de sécurité traditionnelles telles que les pare-feu.

### **Objectifs de l’IDS:**

L'objectif principal du projet de Système de Détection d'Intrusion (IDS) est de remédier à l'insuffisance des défenses conventionnelles et de renforcer le réseau contre les attaques cybernétiques nouvelles et inconnues, ainsi que garantir la :

* **Sécurité du Réseau :** Assurer la sécurité du réseau en identifiant et en réagissant aux activités malveillantes.
* **Préservation de la Confidentialité des Données :** Assurer la protection des données sensibles et confidentielles contre les accès non autorisés ou les fuites.
* **Détection Précoce :** Identifier les attaques le plus tôt possible pour minimiser les dommages.
* **Différenciation entre Activités Normales et Anormales :** Développer des mécanismes pour distinguer entre le trafic réseau normal et les activités suspectes.
* **Réponse Rapide :** Mettre en place des algorithmes de réponse rapides pour neutraliser les menaces détectées.

### **Contraintes de l’IDS:**

Lors de la conception et de la mise en place d'un système de détection d'intrusion (IDS), diverses contraintes doivent être prises en compte afin d'assurer le succès de son déploiement.

* **Contraintes de Budget :** Évaluer les ressources disponibles pour la mise en œuvre et la maintenance du système. ( coûts associés à la conception )
* **Limitations Technologiques :** Considérer les contraintes technologiques qui pourraient influencer la sélection et l'efficacité du système de détection d'intrusion.
* **Contraintes de Scalabilité :** Avec l'évolution des besoins organisationnels, il est essentiel de concevoir un IDS capable de s'adapter à une augmentation du trafic réseau, du nombre d'utilisateurs, et de nouvelles menaces potentielles.
* **Contraintes de Confidentialité et de Conformité :** La nature sensible des données traitées par un IDS soulève des préoccupations quant à la confidentialité et à la conformité. Des contraintes strictes peuvent être imposées par des réglementations ou des politiques internes concernant la manipulation et le stockage des informations liées à la sécurité.

### **Evaluation de l’IDS:**

L'évaluation d'un système de détection d'intrusion (IDS) ne se limite pas seulement à sa conception et à sa mise en œuvre, mais implique également une analyse approfondie de ses performances opérationnelles.

Trois critères essentiels à considérer sont le taux de détection, le taux de faux positifs, et le temps de réponse, qui ensemble définissent l'efficacité globale du système dans la prévention et la gestion des incidents de sécurité.

* **Taux de Détection :** Mesurer l'efficacité du système en termes de détection précise des intrusions.
* **Taux de Faux Positifs :** Minimiser les alertes incorrectes pour éviter les perturbations inutiles
* **Temps de Réponse :** Évaluer la rapidité avec laquelle le système répond aux incidents.

En fin de compte, ce projet vise à faire progresser la compréhension des applications pratiques de l'apprentissage automatique dans la détection d'intrusions et à contribuer aux efforts continus pour renforcer la sécurité des réseaux dans un monde de plus en plus numérisé.

1. Data Understanding :

Le jeu de données NSL-KDD est une version améliorée du jeu de données KDD'99, utilisé pour évaluer les systèmes de détection d'intrusion. Il est composé de plusieurs ensembles, notamment le train set et le test set, disponibles en formats ARFF et TXT.

Les fichiers ARFF contiennent des étiquettes binaires, tandis que les fichiers TXT incluent des étiquettes de type d'attaque et le niveau de difficulté.

Le fichier de jeu de données pour la méthode d’apprentissage supervisé se nomme "KDDTrain+.txt". Il comprend plus de 125972 points de données et 42 attributs.

Ces attributs sont principalement catégoriels, décrivant divers aspects des connexions réseau telles que la durée, le type de protocole, le service réseau, le statut du drapeau, et d'autres caractéristiques pertinentes.

**L'objectif de cette étude est de classer les différents types d'attaques réseau, la variable cible étant 'XAttack'.**

Nous explorerons en détail les variables d'entrée de ce jeu de données pour mieux comprendre les schémas et les caractéristiques associés aux différentes attaques.

Ci-dessous, se trouve l’explication de la dataset et ses attributs.

1. **Attributs de la connexion réseau :**

|  |  |
| --- | --- |
| Nom de la colonne : | Description : |
| Duration | **Durée de la connexion (en secondes) : type int** |
| Protocol\_type | **Type de protocole: udp, tcp, icmp : type string** |
| Service | **Type de réseau: 'private', 'http', 'ftp\_data','telnet','smtp'... : type string** |
| Flag | **Statut du drapeau: 'SF', 'S0', 'REJ', 'RSTR' :type string** |
| Src\_bytes | **Nombre d'octets transférés de la source vers la destination: 146, 0, 232, ... : type int** |
| Dst\_bytes | **Nombre d'octets transférés de la destination vers la source: 0, 8153, 420, ... : type int** |
| Land | **Si la connexion est vers le même hôte land=1, sinon 0 : type int** |

1. **Attributs de la sécurité:**

|  |  |
| --- | --- |
| Nom de la colonne : | Description : |
| Wrong\_fragment | **Nombre de fragments incorrects: 0, 3, 1 : type int** |
| Urgent | **Nombre de paquets urgents: 0, 1, 3, 2, ... : type int** |
| Hot | **Nombre d'indicateurs "hot": 0, 5, 6, 4, ... : type int** |
| Num\_failed\_logins | **Nombre de tentatives de connexion échouées: 0, 2, 1, 3, 4, 5 : type int** |
| Logged\_in | **Si connecté logged\_in=1, sinon 0 : type int** |
| Num\_compromised | **Nombre de conditions compromises : type int** |
| Root\_shell | **Si un shell root est obtenu root\_shell=1, sinon 0 : type int** |
| Su\_attempted | **Si des accès "su root" sont tentés su\_attempted=1, sinon 0 : type int** |
| Num\_root | **Nombre de racines accédées : type int** |
| Num\_file\_creations | **Nombre de créations de fichiers : type int** |
| Num\_shells | **Nombre de prompts de shell : type int** |
| Num\_access\_files | **Nombre d'opérations sur les fichiers d'accès : type int** |
| Is\_host\_login | **Si la connexion est "hot" is\_host\_login=1, sinon 0 : type int** |
| Is\_guest\_login | **Si la connexion est "guest" is\_guest\_login=1, sinon 0 : type int)** |

1. **Statistiques et taux de la connexion :**

|  |  |
| --- | --- |
| Nom de la colonne : | Description : |
| Count | **Nombre de connexions vers le même hôte dans les 2 dernières secondes : type int** |
| Srv\_count | **Nombre de connexions vers le même service dans les 2 dernières secondes : type int** |
| Serror\_rate | **Pourcentage de connexions avec erreur syn : type float** |
| Srv\_serror\_rate | **Pourcentage de connexions avec erreur syn au niveau du service : type float** |
| Rerror\_rate | **Pourcentage de connexions avec erreur rej : type float** |
| Srv\_rerror\_rate | **Pourcentage de connexions avec erreur rej au niveau du service : type float** |
| Same\_srv\_rate | **Pourcentage de connexions du même service : type float** |
| Diff\_srv\_rate | **Pourcentage de connexions de services différents : type float** |
| Srv\_diff\_host\_rate | **Pourcentage de connexions d'hôtes différents au niveau du service : type float** |

1. **Attributs de la destination:**

|  |  |
| --- | --- |
| Nom de la colonne : | Description : |
| Dst\_host\_count | **Nombre de connexions du même hôte de destination : type int** |
| Dst\_host\_srv\_count | **Nombre de connexions du même hôte de destination et du même service : type int** |
| Dst\_host\_same\_srv\_rate | **Pourcentage de connexions ayant le même hôte de destination et le même service : type float** |
| Dst\_host\_diff\_srv\_rate | **Pourcentage de connexions ayant un service différent sur l'hôte actuel : type float** |
| Dst\_host\_same\_src\_port\_rate | **Pourcentage de connexions de l'hôte actuel ayant le même port source : type float** |
| Dst\_host\_srv\_diff\_host\_rate | **Pourcentage de connexions avec erreur rej au niveau du service : type float** |
| Dst\_host\_serror\_rate | **Pourcentage de connexions de l'hôte actuel avec une erreur S0 : type float** |
| Dst\_host\_srv\_serror\_rate | **Pourcentage de connexions de l'hôte actuel d'un service avec une erreur S0 : type float** |
| Dst\_host\_rerror\_rate | **Pourcentage de connexions de l'hôte actuel avec une erreur rst : type float** |
| Dst\_host\_srv\_rerror\_rate | **Pourcentage de connexions de l'hôte actuel d'un service avec une erreur rst : type float** |

1. **Attribut cible:**

|  |  |
| --- | --- |
| Nom de la colonne : | Description : |
| xAttack | **Type d'attaque : type string** |

Le tableau ci-dessous présente une classification des types d'attaques, regroupés en quatre catégories principales : Denial of Service (DoS), User to Root (U2R), Remote to Local (R2L), et Probe.

|  |  |
| --- | --- |
| Classe : | Sous-Classe : |
| DoS | **Neptune, back, land, pod, smurf, teardrop, mailbomb, apache2, processtable, udpstorm, worm** |
| U2R | **buffer\_overflow, loadmodule, perl, rootkit, ps, sqlattack, xterm** |
| R2L | **ftp\_write, guess\_passwd, imap, multihop, phf, spy, warezclient, warezmaster, sendmail, named, snmpgetattack, snmpguess, xlock, xsnoop, httptunnel** |
| Probe | **ipsweep, nmap, portsweep, satan, mscan, saint** |

Conclusion

La progression de notre projet sur le Système de Détection des Intrusions a été caractérisée par une méthodologie rigoureuse, débutant par la définition de notre problématique centrée sur l'efficacité des "Intrusion Detection Systems" (IDS). Notre démarche s'est déployée à travers plusieurs phases, notamment la compréhension approfondie du problème commercial et la nécessité de saisir les enjeux fondamentaux liés à la détection des intrusions dans les systèmes informatiques.

Nous avons également exploré la phase de compréhension des données, où l'examen des données relatives aux incidents d'intrusion a jeté les bases pour notre analyse ultérieure. Ce processus a souligné l'importance d'une préparation minutieuse des données, nécessitant un nettoyage approfondi et une structuration adéquate pour garantir la fiabilité et la pertinence des informations à analyser.

En somme, notre recherche a mis en lumière des questionnements essentiels concernant l'efficacité des Systèmes de Détection des Intrusions dans le domaine de la sécurité informatique. Notre approche méthodique et structurée nous a préparés à aborder la phase cruciale d'analyse, où nous explorerons en profondeur les divers facteurs qui influencent l'efficacité de ces systèmes dans la détection et la prévention des intrusions informatiques.