Institut Universitaire des Sciences (IUS)

Faculté des Sciences et de Technologies (FST)

Projet de fin de semestre du cours de Réseaux I

Titre du sujet

« **L'usage de l'intelligence artificielle dans la gestion et la sécurisation des réseaux** »

Préparé par :

Christy Gérys LAMBERT

Donsam Jean Gabard NOEL

Lens Sandro PETIOTE

Niveau : Licence III

Le 4 janvier 2026

L’usage de l’intelligence artificielle dans la gestion et la sécurisation des réseaux

Introduction 1

I. Impact de l’intelligence artificielle dans la gestion des réseaux 2

I.I Intelligence Artificielle 2

I.II Gestion de réseau 2

I.III Importance de l’intégration de l’IA dans la gestion de réseau 4

I.III.I Fonctions de l’IA dans la gestion de réseau 5

I.III.II Avantages de l’IA dans la gestion de réseau 7

II. L’intelligence artificielle dans la sécurisation des réseaux 8

II.I La sécurisation réseau 8

II.I.I Risques de sécurité 9

II.I.II Types de sécurité réseau 11

II.II Importance de l’intégration de l’IA dans la sécurisation des réseaux 13

II.II.I Application de l’IA dans la sécurisation des réseaux 14

II.II.II Avantages de l’IA dans la sécurisation des réseaux 15

III. Défis et Limites de l’IA dans les réseaux 16

III.I Enjeux éthiques et juridiques 16

III.II Limites techniques 17

III.II.I Faux positifs/faux négatifs 17

III.II.II Exemples pratiques de faux positifs et de faux négatifs 18

III.III- Cybermenaces ciblant l’IA 20

IV. Étude de cas et Applications concrètes 21

Conclusion 24

Liste des Abréviations

5G	Cinquième Génération (de réseau mobile)
ML	Machine Learning (Apprentissage Automatique)
DL	Deep Learning (Apprentissage Profond)
DDoS	Distributed Denial of Service (Déni de Service Distribué)
IA	Intelligence Artificielle
DHCP	Dynamic Host Configuration Protocol
RGPD	Règlement Général sur la Protection des Données
LTE	Long Term Evolution
KPI	Keys Performance Indicator (Indicateur de performance clés)
CNIL	Commission Nationale de l'Informatique et des Libertés
IBM	International Business Machines
LLM	Large Language Model
NSIT	National Institute of Standards and Technology
OWASP	Open Web Application Security Project
GSMA	Global System for Mobile Communications Association

Introduction

À l'ère de la transformation numérique, les réseaux informatiques sont confrontés à des défis sans précédent : explosion des cybermenaces, complexité des infrastructures, et besoin croissant d'automatisation, les pratiques traditionnelles de gestion peinent souvent à répondre aux exigences des entreprises modernes. Dans ce contexte, l'intelligence artificielle (IA) émerge comme une solution clé pour moderniser la gestion et la sécurisation des réseaux.

Dans les réseaux informatiques, l'IA et l'apprentissage automatique sont désormais utilisés pour analyser en continu de grandes quantités de données à l'aide d'algorithmes sophistiqués afin de déterminer ce qui se passe exactement sur le réseau, de faire des prévisions et de réagir aux événements au fur et à mesure qu'ils se produisent. Cette capacité à analyser intelligemment les données du réseau et à en tirer des informations détaillées sur les performances du réseau sans intervention humaine est au cœur de son attrait.

L'IA suscite autant d'attention dans le monde informatique, car elle permet une automatisation intelligente de nombreuses tâches, un gain de temps considérable et l'amélioration de l'efficacité opérationnelle. Elle s'applique parfaitement à la gestion du réseau où de nombreuses fonctions impliquées dans le fonctionnement efficace d'un réseau peuvent être automatisées, améliorant considérablement les performances, le dépannage et la sécurité du réseau

L'intégration de l'IA dans les réseaux fait face à une sacrée problématique : « Dans un paysage numérique en constante évolution, comment l'IA peut-elle transformer la gestion et la sécurisation des réseaux, tout en relevant les défis techniques, éthiques et juridiques qu'elle soulève ? ».

Afin de répondre à la problématique posée, il serait intéressant d'étudier les axes suivants : L'intelligence artificielle au service de la gestion et de la sécurisation des réseaux, enjeux, applications et perspectives. L'IA dans la gestion des réseaux, L'IA dans la sécurisation des réseau, Défis et limites de l'IA dans les réseaux, Études de cas et applications concrètes.

I. Impact de l'intelligence artificielle dans la gestion des réseaux

I.I Intelligence Artificielle

L'intelligence artificielle (IA) désigne un ensemble de techniques permettant à des systèmes informatiques d'imiter certaines capacités humaines, comme le raisonnement (l'utilisation de règles pour parvenir à des conclusions approximatives ou définitives), l'apprentissage (l'acquisition d'informations et de règles pour les utiliser), ou l'autocorrection. Elle se divise principalement en deux approches :

1. **L'IA symbolique** : Elle désigne les systèmes capables de comprendre, d'apprendre et d'appliquer des connaissances à une grande variété de tâches, ce qui la rend proche du raisonnement humain. Néanmoins, cette approche montre ses limites face à des tâches complexes impliquant des variations imprévisibles ou nécessitant une adaptation dynamique
2. **Le Machine Learning (ou apprentissage automatique)** : Ce type d'IA ne repose pas sur une logique préétablie. Il utilise des algorithmes capables d'apprendre à partir de vastes ensembles de données, afin d'identifier des tendances et modéliser des comportements. Il est conçu pour accomplir une tâche spécifique comme la reconnaissance faciale, la traduction automatique ou la détection d'anomalies.

Dans la gestion des réseaux, plusieurs types d'IA sont utilisés :

1. **Machine Learning :** principalement utilisé pour l'analyse du trafic réseau, la détection d'anomalies ou d'intrusions, la prévision des pannes ou surcharges.
2. **Deep Learning[2] :** utilisé pour la cybersécurité avancée, la détection de menaces complexes (malwares, attaques zero-day).

I.II Gestion de réseau

La gestion des réseaux se définit comme étant l'ensemble des moyens mises en œuvre tels que les technologies, les techniques, les méthodes, les outils……pour superviser, exploiter, sécuriser et administrer des réseaux informatiques. Une gestion efficace du

réseau garantit que les ressources réseau (le matériel réseau, le stockage, la mémoire, la bande passante, les données, la puissance de traitement …) sont facilement accessible aux utilisateurs de manière efficace et sécurisée.

La gestion réseau est essentielle car elle aide les équipes informatiques à identifier et résoudre de manière proactive les problèmes réseau, à optimiser les performances, à garantir la disponibilité du réseau, et enfin, mais non des moindres, à soutenir la continuité et les résultats de l'entreprise.

En matière de gestion de réseau, quelques exemples de tâches clés sont à prendre en considération :

1. **Mise à jour logicielles :** Cela consiste à appliquer des correctifs, à améliorer, ou à apporter de nouvelles fonctionnalités aux logiciels qui supervisent, configurent et sécurisent les infrastructures réseau. Elle a pour fonction d'améliorer la performance (optimisation de la bande passante, réduction de latence), d'assurer la compatibilité, de corriger des failles de sécurité et surtout la sécurité des systèmes.
2. **Maintenance :** La maintenance du réseau désigne l'ensemble des actions préventives et correctives qui garantissent le bon fonctionnement, la sécurité et la performance d'un réseau informatique. Une maintenance efficace permet d'assurer la continuité du service, de minimiser les interruptions et de renforcer la cybersécurité de l'infrastructure.
3. **Audits réseau :** Les audits réseaux consistent à examiner et à évaluer les performances et la sécurité de l'infrastructure réseau. Les outils d'audit de réseau utilisent l'automatisation pour effectuer des tâches telles que l'identification des appareils, les vérifications de configuration et l'analyse des vulnérabilités.
4. **Surveillance des performances :** La surveillance continue des indicateurs de performance du réseau, tels que l'utilisation de la bande passante, la latence et la perte de paquets, est essentielle pour identifier les problèmes et garantir une expérience utilisateur optimale.
5. **Gestion des menaces et des vulnérabilités :** La gestion des menaces est un processus utilisé par les professionnels de la cybersécurité pour prévenir les

cyberattaques, détecter les cybermenaces et répondre aux incidents de sécurité. Parmi les menaces pesant sur la sécurité des réseaux, citons les attaques par ransomware et celles définies par déni de service distribuée (DDoS). Ces professionnels s'appuient également sur les pratiques de gestion des vulnérabilités et les solutions automatisées pour découvrir les failles ou les faiblesses de la structure d'un réseau. Quant aux vulnérabilités, il peut s'agir d'équipements qui n'ont pas été installés correctement, de mots de passe non sécurisés ou encore de défauts de conception du système d'exploitation.

6. **Gestion de la sécurité :** Elle consiste à protéger le réseau les accès non autorisés, les menaces et les vulnérabilités, parmi les tâches qui garantissent une meilleure protection, citons la création de pare-feu pour bloquer toute activité suspecte au sein du réseau ainsi que la mise en place de l'authentification multi-facteur.
7. **Gestion des adresses IP :** Les administrateurs réseau dressent l'inventaire des adresses IP disponibles et indisponibles pour les appareils résidant sur le réseau. Une adresse IP est attribuée à chaque périphérique jusqu'à ce qu'il soit supprimé du réseau. L'attribution peut se faire à l'aide d'un serveur DHCP, souvent présent dans le réseau des grandes entreprises.
8. **Allocation des ressources :** La gestion efficace des ressources réseau, telles que la bande passante, les canaux de transport (par exemple, câble, haut débit, 5G, LTE, satellite) et la puissance de traitement est essentielle pour optimiser les performances et répondre aux besoins des utilisateurs. La complexité croissante des réseaux, due à la multiplication des appareils, des applications et des services, rend les techniques traditionnelles de gestion de réseau de plus en plus inadaptées.

I.III Importance de l'intégration de l'IA dans la gestion de réseau

En un rien de temps, l'intelligence artificielle s'est imposée comme la principale technologie d'avenir dans de nombreux domaines, notamment celui du secteur informatique, où l'utilisation de modèles d'IA est déjà omniprésente dans la gestion des réseaux. En tirant parti des technologies d'IA, les organisations peuvent améliorer leur

efficacité, automatiser leurs opérations et anticiper les problèmes potentiels. Cette section explore le rôle crucial de l'IA dans la gestion de réseau, en mettant l'accent sur l'amélioration de l'efficacité et des performances, l'automatisation des opérations réseau et le gain de temps, la mise en place d'une identification et d'une résolution proactives des problèmes.

I.III.I Fonctions de l'IA dans la gestion de réseau

Dans les réseaux informatiques, l'IA et le machine learning sont utilisés pour analyser de grandes quantités de données en continu à l'aide d'algorithmes sophistiqués dans le but de repérer ce qui se passe sur le réseau, de faire des prévisions et de réagir aux évènements au fur et à mesure qu'ils se produisent. Elle s'applique parfaitement à la gestion du réseau car de nombreuses fonctions impliquées dans le fonctionnement efficace d'un réseau peuvent être automatisées, ce qui améliore de façon considérable les performances, le dépannage et la sécurité réseau.

Maximiser la performance

Les systèmes basés sur l'IA permettent d'**analyser de vastes quantités de données en temps réel,** ce qui permet aux organisations d'obtenir des informations immédiates sur le réseau, de **surveiller le trafic**, en identifiant les pics et les creux d'utilisation, cette analyse en temps réel permet aux administrateurs réseau d'ajuster l'allocation de bande passante et de prioriser les applications critiques, garantissant ainsi des performances optimales et une expérience utilisateur optimale. Ils fournissent également des **indicateurs de performances**, à l'aide d'une surveillance continue, les outils d'IA peuvent suivre les indicateurs clés de performance tels que la latence, le débit et la perte de paquets. En corrélant ces données avec les configurations réseau et le comportement des utilisateurs, les organisations peuvent identifier les inefficacités et prendre des décisions éclairées pour améliorer les performances.

Optimiser les ressources

L'IA facilite une gestion plus intelligente des ressources en optimisant **l'allocation des ressources** réseau en fonction des demandes en temps réel, les algorithmes d'IA peuvent ajuster automatiquement la répartition des ressources pour répondre aux fluctuations de

la demande, garantissant ainsi aux applications prioritaires la bande passante nécessaire tout en minimisant l'impact sur les services moins critiques. Cette allocation dynamique améliore l'efficacité globale du réseau et réduit les coûts d'exploitation. En analysant les flux de trafic, l'IA peut répartir intelligemment les charges de travail entre les serveurs et les périphériques réseau. Cet **équilibrage de charge** améliore la réactivité et optimise l'utilisation des ressources disponibles.

Automatiser les tâches de routine

L'IA peut automatiser la collecte et l'analyse des données de performance du réseau, ce qui permet de **faire un suivi et de générer des rapports** qui mettent en évidence les indicateurs et les tendances critiques. Cette automatisation élimine la saisie manuelle des données et permet une surveillance continue de l'état du réseau. Les systèmes pilotés par l'IA peuvent **faire une intervention en cas d'incidents** prédéfinis, tels que des pannes de réseau ou des baisses de performance. En exécutant des actions prédéfinies, comme le réacheminement du trafic ou le déploiement de ressources de secours, l'IA peut résoudre rapidement les problèmes, minimisant ainsi les temps d'arrêt et les perturbations.

Mettre en œuvre des actions préventives

La maintenance préventive en IA est l'anticipation des pannes potentielles du réseau pour les résoudre avant qu'elles ne s'aggravent. L'IA peut **prédire des défaillances**, en analysant les données de performance historiques et en identifiant les schémas qui précèdent les pannes de réseau, l'IA peut prévoir quand un appareil tombe en panne. Cette anticipation permet aux organisations de planifier la maintenance de manière proactive, ce qui réduit les temps d'arrêt et minimise les interruptions de service. L'IA peut également analyser l'état et les performances des équipements réseau afin **d'évaluer leur durée de vie**. En prévoyant les besoins de remplacement ou de mise à niveau, les entreprises peuvent optimiser leurs investissements et garantir la robustesse et l'efficacité de leurs réseaux.

I.III.II Avantages de l’IA dans la gestion de réseau

Automatisation et gain de temps

Les systèmes basés sur l’IA allègent la charge de travail des équipes informatiques car ils peuvent traiter et analyser de vastes quantités de données réseau en temps réel. Cette capacité permet aux organisations d'obtenir des informations immédiates sur le réseau. Grâce à des fonctions de sécurité automatisés et à une allocation efficace des ressources, cela permet aux équipes informatiques de se concentrer sur des tâches stratégiques.

Amélioration des performances

Grâce à une surveillance continue, les outils d'IA peuvent suivre les indicateurs clés de performance (KPI) tels que la latence, le débit et la perte de paquets. En corrélant ces données avec les configurations réseau et le comportement des utilisateurs, les organisations peuvent identifier les inefficacités et prendre des décisions éclairées pour améliorer les performances.

Réduction des coûts

L’utilisation de l’IA dans la gestion du réseau agit comme un levier économique puisqu’elle entraîne une réduction significative des coûts d’exploitation, elle diminue les coûts opérationnels, prévient les pertes financières dues aux pannes et optimise l’utilisation des ressources.

Gestion de la sécurité

L’intelligence artificielle renforce la sécurité des réseaux, en contribuant à l’identification en temps réel et l’optimisation de la détection des menaces tout en permettant une réponse rapide aux intrusions potentielles. Les systèmes d'IA peuvent analyser les schémas de trafic réseau et le comportement des utilisateurs afin d'identifier les anomalies susceptibles de révéler des menaces de sécurité. En cas de détection d'une menace, l'IA peut automatiser les mesures de réponse, telles que l'isolement des systèmes affectés, l'alerte des équipes de sécurité ou la mise en œuvre de mesures de sécurité prédéfinies. Cette réactivité minimise l'impact potentiel des incidents de sécurité.

Promotion de l'innovation

L'IA aide les départements de recherche à mettre au point de nouvelles technologies et solutions pour la gestion des réseaux.

II. L'intelligence artificielle dans la sécurisation des réseaux

II.I La sécurisation réseau

La sécurité réseau plus connu sous le nom de « **cybersécurité** » fait référence aux technologies, politiques, personnes et procédures qui défendent toute infrastructure de communication contre les cyberattaques, les accès non autorisés et les pertes de données. En plus du réseau lui-même, ils sécurisent également le trafic et les ressources accessibles au réseau à la fois à la périphérie du réseau et à l'intérieur du périmètre.

La sécurité du réseau est utilisée afin de protéger vos ressources informatiques des attaques, elle garantit la sécurité de vos informations et de vos données en fournissant :

- **Une réduction des cyber-risques** avec des mesures de sécurité solides et robustes permettent de garantir que vos données restent toujours protégées.
- **Une protection renforcée des données** en éliminant des vecteurs de menace garantissant ainsi que les informations sensibles sont protégées contre les accès non autorisés tout en traversant le réseau, protégeant ainsi les données des clients et assurant la conformité.
- **Une amélioration de la continuité des activités** avec des réseaux protégés qui sont plus résilients face aux perturbations potentielles et qui subissent un temps d'arrêt minimal, ce qui permet une productivité optimale.
- **Des meilleures performances réseau** qui empêchent les acteurs malveillants de désactiver le réseau, garantissant ainsi que les ressources critiques sont toujours facilement disponibles.

Le matériel joue un rôle essentiel dans la sécurisation de l'infrastructure. Trois dispositifs, en particulier, sont pertinents pour la sécurité des réseaux :

- **Commutateurs Ethernet** : Ils garantissent une sécurité adéquate à la périphérie du réseau en facilitant le filtrage du trafic et le contrôle d'accès au niveau du port, ce qui permet aux administrateurs d'appliquer des politiques sur des segments de réseau granulaires.
- **Points d'accès Wi-Fi (AP) :** Les points d'accès sans fil mettent en œuvre des protocoles de cryptage et des mécanismes d'authentification, protégeant les données en transit. Ils prennent également en charge les listes de contrôle d'accès (ACL), empêchant les appareils non autorisés de se connecter au réseau.
- **Les passerelles** (5G et LTE) : Elles sont essentielles aux liens redondants et primaires vers les succursales et les campus. Le fait de loger ces appareils sous le même dispositif de sécurité que le reste du réseau garantit une configuration commune, réduisant ainsi la surface d'attaque.

II.I.I Risques de sécurité

Il faut savoir que les réseaux sont confrontés à de nombreux risques de sécurité qui peuvent compromettre leur infrastructure réseau, tels que :

- **Attaques de logiciels malveillants :** les logiciels malveillants sont des logiciels conçus pour infiltrer et endommager les systèmes réseau. Ce risque pour la sécurité comprend les virus, les vers, les chevaux de Troie et les logiciels espions qui peuvent s'autoreproduire et se propager sur les périphériques réseau.
- **Ransomware :** les attaques par ransomware chiffrent les données des organisations et exigent le paiement d'une rançon pour obtenir les clés de déchiffrement. Ce type d'attaque cible à la fois les systèmes de stockage réseau et les terminaux individuels connectés au réseau.
- **Attaques DDoS :** les attaques par déni de service distribué saturent les ressources réseau avec un trafic excessif. Ces attaques ciblent la bande passante du réseau, la capacité de traitement des serveurs et les ressources de la couche applicative.
- **Attaques par hameçonnage** : les attaques par hameçonnage utilisent des communications trompeuses pour voler des identifiants de connexion et des

données sensibles. Ces attaques ciblent les utilisateurs par le biais d'e-mails, de systèmes de messagerie et de faux sites web qui semblent légitimes.

- **Attaques de type "man-in-the-middle" :** les attaques (MiTM) interceptent les communications entre les périphériques réseau. Les pirates se positionnent entre des connexions réseau légitimes afin de capturer ou de modifier les données en transit.
- **Menaces internes** : les menaces internes proviennent d'utilisateurs disposant de droits d'accès légitimes au réseau. Ces menaces impliquent des employés, des sous-traitants ou des partenaires qui abusent de leurs privilèges d'accès pour compromettre la sécurité du réseau.
- **Attaques par injection SQL** : ces attaques visent les applications basées sur des bases de données en insérant du code SQL malveillant dans les champs de saisie. Ces attaques exploitent la mauvaise validation des entrées et la construction incorrecte des requêtes de base de données dans les applications web connectées aux ressources réseau.
- **Cross-Site Scripting (XSS)** : C'est un type d'attaque contre une application web qui amène les utilisateurs à continuer à lire des scripts malveillants introduits par le réseau. Ce type d'attaque consiste à insérer un code côté client via des pages web auxquelles les utilisateurs font confiance pour interagir. Le vol de cookies de session, la capture de frappes clavier et rediriger les utilisateurs vers des sites malveillants ne sont que quelques-uns des types d'attaques XSS. Cela permet aux attaquants de détourner les sessions des utilisateurs, de défigurer le site web et d'effectuer des transactions comme s'ils étaient de vrais utilisateurs s'ils réussissent.
- **Exécution de code à distance** : permet aux pirates d'exécuter des commandes arbitraires sur les systèmes cibles du réseau. Ces attaques exploitent les bogues logiciels, les systèmes non patchés et les applications mal configurées pour exécuter du code malveillant.
- **Cryptojacking** : les attaques de cryptojacking détournent les ressources réseau pour miner des cryptomonnaies. Ces attaques compromettent les systèmes à l'aide de scripts malveillants et d'applications infectées ou exploitent des vulnérabilités pour consommer de la puissance de traitement.

- **Attaques par mot de passe** : les attaques par mot de passe tentent de compromettre les identifiants d'accès au réseau à l'aide de diverses méthodes. Ces attaques comprennent des tentatives par force brute, des attaques par dictionnaire et des attaques par pulvérisation de mots de passe contre les systèmes d'authentification.
- **Vulnérabilités des API** : les vulnérabilités des API exposent les services réseau à des accès et manipulations non autorisés. Ces failles de sécurité se produisent dans les interfaces de programmation d'applications mal sécurisées qui connectent différents services réseau et applications. Les API non sécurisées peuvent divulguer des données sensibles, permettre des opérations non autorisées et fournir des voies d'attaque vers les réseaux internes. Les pirates peuvent exploiter les failles d'authentification, l'exposition excessive des données et l'absence de limites de débit pour compromettre les systèmes connectés.
- **Attaques de protocole réseau** : les attaques de protocole réseau sont celles qui exploitent une ou plusieurs faiblesses des protocoles de communication courants. Elles exploitent les faiblesses des protocoles réseau fondamentaux, tels que TCP/IP, DNS, SMTP et autres, qui sont essentiels pour effectuer de nombreux types de communications réseau actives. Les attaques au niveau du protocole interceptent, manipulent ou modifient le trafic réseau. L'empoisonnement DNS, l'usurpation ARP et les attaques par rétrogradation de protocole sont quelques exemples de ce que les attaquants peuvent faire pour violer les mécanismes de sécurité réseau d'une organisation.

II.I.II Types de sécurité réseau

Les Pare-feu mettent une barrière entre votre réseau interne fiable et les réseaux externes qui ne le sont pas, comme l’Internet.

Sécurité de la messagerie où les passerelles de messagerie constituent le principal vecteur de menaces entraînant des brèches de sécurité.

Logiciels antivirus et anti-logiciels malveillants où les « maliciels » ou « logiciels malveillants » comprennent les virus, les vers informatiques, les chevaux de Troie, les rançongiciels et les logiciels espions.

Segmentation du réseau qui est définie par logiciel répartit le trafic réseau entre différentes catégories et facilite la mise en application des politiques de sécurité.

Contrôle d'accès qui empêche à tous les utilisateurs d'avoir accès à votre réseau.

Sécurité des applications où tous les logiciels que vous utilisez dans votre entreprise doivent être protégés, que votre personnel des TI les ait conçus ou achetés.

Analyse du comportement pour détecter les comportements anormaux de votre réseau, vous devez savoir quels sont des comportements normaux.

Prévention de la perte de données les entreprises doivent veiller à ce que leur personnel n'envoie pas d'information sensible en dehors du réseau.

Systèmes de prévention des intrusions (IPS) fait une analyse du trafic réseau pour bloquer activement les attaques.

Sécurité des appareils mobiles les cybercriminels ciblent de plus en plus les applications et appareils mobiles.

Gestion des renseignements et des événements de sécurité où les produits SIEM rassemblent les renseignements dont votre personnel de sécurité a besoin pour identifier les menaces et y répondre.

VPN qui un réseau privé virtuel chiffre la connexion d'un point d'extrémité avec un réseau, souvent sur l'Internet.

Sécurité Web qui est une solution de sécurisation du web permettant de contrôler l'utilisation du Web chez votre personnel, de bloquer les menaces en ligne et d'empêcher l'accès aux sites Web malveillants.

Sécurité du réseau sans fil qui n'est pas aussi bien protégés que les réseaux filaires. Sans des mesures de sécurité strictes, la mise en place d'un réseau LAN sans fil peut équivaloir à installer des ports Ethernet partout, même dans un stationnement.

II.II Importance de l'intégration de l'IA dans la sécurisation des réseaux

La cybersécurité est l'un des domaines les plus critiques dans lequel l'IA a un impact significatif. Avec la complexité et la fréquence croissantes des cyberattaques, les mesures de sécurité traditionnelles ne suffisent plus à protéger les réseaux contre les menaces en constante évolution. La création et la maintenance de politiques sur plusieurs réseaux nécessitent un temps et des efforts manuels considérables. Les organisations ne déploient souvent pas les bonnes conventions de dénomination pour leurs applications et charges de travail. Cela signifie que les équipes de sécurité peuvent devoir passer plus de temps à déterminer quelles charges de travail appartiennent à des applications spécifiques. L'IA apprend les modèles de trafic réseau des organisations au fil du temps, ce qui lui permet de recommander les bonnes politiques et charges de travail. L'IA dans les réseaux contribue à une meilleure sécurité, elle améliore la sécurité en apprenant continuellement des données de trafic du réseau et en identifiant les activités potentiellement malveillantes. Il peut repérer des modèles inhabituels qui peuvent indiquer une faille de sécurité et réagir presque instantanément pour atténuer les menaces, vous offrant ainsi un environnement en ligne beaucoup plus sûr. Les solutions de cybersécurité basées sur l'IA améliorent :

- **Détection avancée des menaces :** l'IA analyse en permanence de grands ensembles de données afin d'identifier des schémas inhabituels ou des anomalies pouvant indiquer des cybermenaces potentielles. Par exemples, la solution Darktrace qui utilise l'apprentissage auto-supervisé pour apprendre le "rythme de vie" normal d'un réseau. S'il détecte qu'un compte utilisateur accède soudainement à des bases de données sensibles à 3h du matin depuis une IP inhabituelle, il lève une alerte avant même qu'une signature de virus connue ne soit détectée.
- **Réponse automatisée aux incidents :** les systèmes de sécurité basés sur l'IA sont capables de répondre instantanément aux menaces, ce qui réduit considérablement le temps nécessaire pour contenir les cyberattaques. Avec les

plateformes SOAR (Security Orchestration, Automation, and Response) comme IBM Security QRadar, si un logiciel de rançon (ransomware) commence à chiffrer des fichiers, l'IA peut isoler automatiquement la machine infectée du reste du réseau en quelques millisecondes, empêchant la propagation latérale de l'attaque.

- **Détection du phishing :** l'IA analyse les e-mails pour détecter les tentatives de phishing avec une grande précision, réduisant ainsi le risque d'attaques d'ingénierie sociale. Par exemple, Microsoft Defender for Office 365 utilise le traitement du langage naturel (NLP) pour analyser non seulement les liens, mais aussi le ton et l'intention du message. Il peut détecter qu'un e-mail prétendant venir du "Directeur Financier" est suspect car le style d'écriture diffère radicalement de ses habitudes de communication réelles.
- **Analyse des logiciels malveillants :** l'IA est efficace pour détecter et classer les nouvelles formes de logiciels malveillants, ce qui aide les équipes de sécurité à réagir plus efficacement. Des outils comme CrowdStrike Falcon utilisent des modèles de "Machine Learning" pour identifier des malwares dits "zero-day" (inconnus jusqu'alors). Au lieu de chercher une signature spécifique, l'IA analyse le comportement du fichier : s'il tente de modifier le noyau du système de manière suspecte, il est bloqué immédiatement.

En intégrant l'IA à la sécurité des réseaux, les réseaux peuvent se défendre de manière proactive contre les cybermenaces et assurer une meilleure protection des données sensibles.

II.II.I Application de l'IA dans la sécurisation des réseaux

Les applications de l'IA dans la sécurité et l'infrastructure réseau sont très répandues, les entreprises utilisant des solutions basées sur l'IA pour améliorer à la fois l'efficacité et la sécurité. Voici quelques exemples notables :

- **Pares-feux basés sur l'IA :** ces pares-feux analysent le trafic réseau en temps réel, détectant et bloquant les activités malveillantes avant qu'elles ne puissent infiltrer le système.
- **Systèmes de détection d'intrusion (IDS) :** les IDS basés sur l'IA peuvent identifier les comportements suspects sur le réseau et alerter les équipes de sécurité avant qu'une attaque ne se produise.
- **Sécurité cloud améliorée par l'IA :** l'IA surveille en permanence les modèles d'accès afin de garantir la sécurité des environnements cloud et d'empêcher tout accès non autorisé.
- **Détection des anomalies réseau :** les outils d'IA peuvent identifier les irrégularités dans le trafic réseau qui peuvent indiquer une cyberattaque ou une défaillance du système.
- **Surveillance automatisée de la conformité :** l'IA aide les entreprises à respecter les réglementations en matière de sécurité des données en surveillant en permanence les indicateurs de conformité et en alertant les équipes en cas de violations potentielles.

Ces applications de l'IA démontrent comment celle-ci remodèle le paysage de la sécurité et contribue à rendre les infrastructures réseau plus résilientes.

II.II.II Avantages de l'IA dans la sécurisation des réseaux

L'adoption de l'IA dans l'infrastructure réseau et la sécurité offre de nombreux avantages, notamment :

- **Détection améliorée des menaces :** les systèmes de sécurité basés sur l'IA analysent de grandes quantités de données afin d'identifier les activités malveillantes, améliorant ainsi considérablement les capacités de détection des menaces.
- **Réponse plus rapide aux incidents :** l'IA permet aux équipes de sécurité de détecter et de répondre aux cybermenaces en temps réel, minimisant ainsi les dommages potentiels.

- **Réduction des faux positifs :** les systèmes de sécurité traditionnels génèrent souvent un volume élevé de fausses alertes, submergeant les équipes de sécurité. L'IA affine les algorithmes de détection des menaces afin de réduire les faux positifs et d'améliorer la précision.
- **Efficacité et automatisation accrues :** l'IA automatise les tâches répétitives, permettant aux équipes de sécurité de se concentrer sur les problèmes critiques plutôt que sur la surveillance manuelle.
- **Réduction des coûts :** l'IA réduit le besoin d'une surveillance manuelle intensive, ce qui permet de réaliser des économies dans la gestion du réseau et les opérations de cybersécurité.
- **Analyse prédictive pour une sécurité proactive :** la capacité de l'IA à analyser les données historiques et à prédire les menaces potentielles pour la sécurité permet aux entreprises de prendre des mesures préventives avant qu'une attaque ne se produise.

Ces avantages soulignent la manière dont l'IA améliore la sécurité des réseaux, les rendant plus robustes et proactifs face aux défis actuels en matière de cybersécurité.

III. Défis et Limites de l'IA dans les réseaux

III.I Enjeux éthiques et juridiques

Vie privée et surveillance :

Ce sujet est désormais au cœur des priorités pour les chefs de projet IA, Product Owners/Managers, directions tech & produit et équipes data. L'intelligence artificielle bouleverse notre société et soulève de nombreuses questions juridiques complexes. Entre protection des données, responsabilité civile et pénale, et éthique algorithmique, le droit peine à suivre le rythme effréné des avancées technologiques.

Décryptage des enjeux majeurs

L'utilisation massive de données par les systèmes d'**intelligence artificielle** pose de sérieux défis en matière de protection de la vie privée. Le **RGPD** européen encadre

strictement la collecte et le traitement des données personnelles, mais son application aux **algorithmes d'apprentissage automatique** soulève de nombreuses interrogations. Comment garantir un consentement éclairé des utilisateurs quand les finalités du traitement sont floues ? La notion de **minimisation des données** est-elle compatible avec le fonctionnement des réseaux de neurones profonds ?

Les autorités de contrôle comme la **CNIL** en France peinent à auditer efficacement des systèmes d'IA opaques et en constante évolution. De nouvelles approches comme la **privacy by design** ou le **federated learning** émergent pour concilier performance des algorithmes et respect de la vie privée. Mais leur mise en œuvre reste complexe et coûteuse pour les entreprises.

Responsabilité en cas de faille

L'autonomie croissante des systèmes d'**IA** remet en question les régimes classiques de responsabilité civile et pénale. En cas d'accident causé par une **voiture autonome** par exemple, qui est responsable ? Le conducteur, le constructeur automobile, l'éditeur du logiciel d'IA ? La notion de **faute** est difficile à établir face à des systèmes dont le fonctionnement échappe parfois à la compréhension humaine.

Certains juristes plaident pour la création d'une **personnalité juridique** propre aux IA les plus avancées, sur le modèle des personnes morales. D'autres préconisent plutôt des régimes de responsabilité objective ou sans faute. Le **Parlement européen** travaille actuellement sur un projet de règlement sur la responsabilité civile en matière d'IA, mais les débats restent vifs sur ces questions.

III.II Limites techniques

III.II.I Faux positifs/faux négatifs

L'intelligence artificielle (IA) est aujourd'hui au cœur d'une révolution technologique qui transforme profondément nos sociétés, nos économies et nos modes de vie. En 2025, son adoption s'accélère dans de nombreux secteurs, de la santé à la finance, en passant par la sécurité et la gestion des données. Pourtant, malgré ses progrès impressionnants,

l’IA reste confrontée à des limites techniques, éthiques et réglementaires majeures qui freinent son déploiement et soulèvent de nombreuses interrogations.

Malgré plusieurs avancées, l’IA reste un système statistique basé sur l’apprentissage à partir de données massives. Elle ne comprend pas le sens des mots ou des concepts, mais prédit les réponses les plus probables. Cela engendre plusieurs limites.

Découvrons comment les faux positifs et les faux négatifs affectent des domaines tels que la santé, la sécurité et la reconnaissance faciale.

Les décisions fondées sur l’IA promettent efficacité et précision, mais elle n’est pas infaillible. L’un des plus grands défis de ces systèmes est l’émergence de **faux positifs** et **faux négatifs**, des erreurs qui peuvent avoir des conséquences importantes dans divers domaines.

Le concept de faux positifs et de faux négatifs est fondamental dans les statistiques en général. Un **faux positif** se produit lorsqu'un système classe à tort quelque chose comme positif alors que ce n'est pas le cas. D'autre part, un **faux négatif** Cela signifie que le système manque de quelque chose qu’il aurait dû identifier.

Ces erreurs peuvent sembler minimes, mais dans des applications critiques, elles ont de profondes répercussions.

III.II.II Exemples pratiques de faux positifs et de faux négatifs

1. Diagnostic médical

Les systèmes d’IA sont de plus en plus utilisés dans les soins de santé pour détecter les maladies.

Si un modèle d'IA génère un **faux positif** lorsqu’un patient reçoit un diagnostic de cancer, il peut ressentir une anxiété inutile et subir des traitements invasifs inutiles. Si un **faux négatif** l’IA ne parvient pas à détecter la maladie lorsqu’elle est réellement présente, ce qui peut retarder un traitement crucial.

Coût et complexité

L'adoption de l'IA implique des structures de coûts à plusieurs niveaux qui vont bien au-delà de l'achat initial de logiciels ou des frais de licence. Les entreprises doivent tenir compte d'un large éventail d'éléments financiers qui influencent directement les dépenses à court et à long terme. Ces éléments comprennent généralement l'acquisition et la préparation des données, la puissance de calcul, l'infrastructure en nuage, le recrutement de talents spécialisés, ainsi que la formation et la maintenance continues des modèles.

L'un des principaux facteurs de coût est l'utilisation des ressources en nuage. Des fournisseurs comme **Google Cloud**, **Microsoft Azure**, et **Amazon Web Services** offrent des plateformes d'IA évolutives, mais la flexibilité et la puissance sont payantes, en particulier lorsqu'il s'agit de déployer de grands modèles ou de traiter de nombreuses données en temps réel. L'intensité de calcul des flux de travail d'IA, en particulier pour les modèles à grande échelle et les données en temps réel, est très élevée. Des applications telles que celles mises au point par **Open AI,** si elle n'est pas gérée avec soin, elle peut conduire à une croissance explosive des coûts.

Un autre domaine de dépenses important concerne les ressources humaines. Le développement, le maintien et l'amélioration des modèles d'IA exigent l'expertise de data scientists, d'ingénieurs en apprentissage automatique et de spécialistes de la cybersécurité. Les cabinets de conseil tels que **Accenture**, **Deloitte**, et **McKinsey & Company** mettent souvent l'accent sur l'équilibre entre les talents internes et l'externalisation afin d'optimiser les coûts sans sacrifier l'innovation.

La préparation des données est notoirement longue et coûteuse. Le nettoyage, l'étiquetage et la conservation des ensembles de données de formation, que ce soit en interne ou par l'intermédiaire de fournisseurs tiers, peuvent représenter jusqu'à 40% des budgets des projets d'IA. Cette étape comprend également la conformité aux réglementations sur la confidentialité des données, ce qui nécessite des investissements dans des cadres de gouvernance des données, que des entreprises comme **IBM** et **Salesforce** aider à la mise en œuvre.

III.III- Cybermenaces ciblant l'IA

Attaques adversariales

L'**attaque adversariale en intelligence artificielle désigne** la manipulation intentionnelle d'un modèle d'apprentissage automatique par des perturbations quasi invisibles. En modifiant légèrement une image, un texte ou une donnée d'entrée, un cybercriminel peut pousser l'algorithme à **commettre une erreur**, à **révéler des informations sensibles** ou à **produire des réponses malveillantes**.

En 2025, ces menaces ne concernent plus seulement la reconnaissance d'images : elles touchent désormais les **grands modèles de langage (LLM)**, les **systèmes de décision automatisés**, les **IA embarquées** et les **chaînes de production industrielles**.

Le **NIST** (National Institute of Standards and Technology) et l'**OWASP** ont récemment publié des cadres de référence pour encadrer ces risques. Le **NIST AI Risk Management Framework** invite les organisations à cartographier et mesurer leurs vulnérabilités adversariales, tandis que l'**OWASP Top 10 for LLM Applications** répertorie les menaces spécifiques aux modèles génératifs, dont la **prompt injection** ou le **model denial of service**.

Qu'est-ce qu'une attaque adversariale en IA ?

Une attaque adversariale consiste à **manipuler un modèle** via de **légères perturbations d'entrée** (ou des données d'entraînement empoisonnées) pour provoquer une **erreur** ou **extraire de l'information**. Elle couvre l'**évasion**, le **poisoning**, l'**inversion/vol de modèle** et, côté LLM, la **prompt injection** et ses variantes.

Exemple d'attaque adversariale contre un modèle de Machine Learning

Imaginons un système de reconnaissance d'images utilisé pour identifier des panneaux de signalisation.

Un attaquant pourrait :

- **Prendre une image d'un panneau "Stop"**.

- **Ajouter de petites perturbations visuelles** (quasi invisibles à l'œil humain, comme un léger bruit ou des motifs spécifiques).
- Ces modifications sont calculées de manière à **induire en erreur le modèle** : le réseau de neurones pourrait alors classer le panneau "Stop" comme un "Cédez le passage" ou même un "Limitation de vitesse".

Il faut aussi mettre en garde contre l'utilisation de l'IA par les hackers qui l'utilisent pour contourner la défense. Malheureusement, l'IA est devenue un outil attractif pour les hackers. Comme tout système informatique, l'IA conserve des failles, il peut donc être compromis de différentes façons soit par

- **L'empoisonnement des données** : Dans ce cas, il y a une falsification des données d'apprentissage ou une altération du modèle d'IA. Le système ne répond pas certaines entrées comme il devrait le faire. Cela peut permettre à un hacker de faire croire au système qu'une attaque n'en est pas une.
- **L'extraction des données :** Cette attaque donne lieu à une récupération des données confidentielles dans le modèle d'IA après la fin de sa phase d'apprentissage,
- **L'évasion :** Cette manipulation de l'intelligence artificielle conduit à une altération des données d'entrée du système. Cela permet de modifier son fonctionnement. Cette compromission du système représente un vecteur d'attaques non négligeable.

Il est donc indispensable **d'intégrer un contrôle humain de l'IA** par des professionnels de l'IT pour faire face à ces problèmes.

IV. Étude de cas et Applications concrètes

- **Cas d'entreprise**
    1. **Google et son IA pour sécuriser Gmail**

Google utilise l'intelligence artificielle pour protéger les utilisateurs de Gmail contre **les emails de pishings et les spams**. Avec l'aide des modèles de Machine Learning et de Deep Learning, Google analyse en temps réel des milliards d'emails pour détecter

les menaces. Cette approche permet de **réduire les risques de pishings** et **d'améliorer l'expérience utilisateur.**

Technologies utilisées :

- **TensorFlow :** Framework de Machine Learning utilisé pour entraîner des modèles de détection.
- **Analyse comportementale :** Identification des schémas suspects tels que les liens malveillants, les pièces jointes infectées.
- **Classement en temps réel :** Les emails sont analysés et classés (spam, pishing, légitimes) en quelques millisecondes.

Exemple concret :

D'après ai.googleblog.com, Google bloquerait plus de 100 millions d'emails de pishing chaque jour grâce à son système d'IA.

Le taux de faux positifs (emails légitimes marqués comme spam) aurait été réduit à moins de 0,05% contre 1% avec les méthodes traditionnelles.

2. **Microsoft Azure Sentinel**

Microsoft Azure Sentinel est une plateforme de sécurité cloud qui **utilise l'IA pour détecter, investiguer et répondre** aux menaces en temps réel. Elle intègre des fonctionnalités avancées de **corrélations des évènements** et **d'automatisation des réponses.**

Technologies utilisées :

- **Machine Learning :** Pour détecter les anomalies dans les logs et les événements de sécurité.
- **Automatisation des réponses :** Isolation des appareils infectés, blocage des IP malveillantes.
- **Intégration avec d'autres outils** : Azure Sentinel peut se connecter à des sources de données variées (ex. : Office 365, AWS, firewalls).

Exemple concret :

- **Microsoft – Azure Sentinel** : Azure Sentinel réduit le temps moyen de détection (MTTD) des menaces de 50 % et le temps moyen de réponse (MTTR) de 60 %.
- La plateforme utilise des modèles de ML pour corrélation des événements et identification des attaques complexes (ex. : mouvements latéraux dans un réseau).

Azure Sentinel permet aux entreprises de centraliser leurs logs de sécurité et d'utiliser **l'IA pour automatiser la détection et la réponse**. Cette solution est particulièrement utile pour les grandes entreprises avec des infrastructures cloud complexes.

Source : https://azure.microsoft.com/fr-fr/products/microsoft-sentinel/

3. Les réseaux 5G

Les réseaux 5G sont confrontés à de nouvelles vulnérabilités en raison de leur complexité et de leur architecture distribuée. **L'IA est utilisée pour sécuriser ces infrastructures** en **détectant les menaces en temps réel** et en **optimisant les performances.**

Technologies utilisées :

- **Analyse comportementale** : Détection des anomalies dans le trafic 5G (ex. : attaques DDoS, intrusions).
- **Automatisation des réponses :** Isolation des appareils compromis, ajustement dynamique des règles de sécurité.
- **Intégration avec les infrastructures 5G :** L'IA est intégrée **aux cœurs de réseau 5G** et aux antennes pour une protection en temps réel..

Exemple concret :

GSMA – Sécurité 5G : Les opérateurs télécoms comme Ericsson et Nokia utilisent l'IA pour sécuriser leurs réseaux 5G. Par exemple, l'IA peut détecter une attaque par saturation (ex. : tentative de DDoS) et rediriger le trafic vers des serveurs sécurisés. Selon la GSMA, l'IA permet de réduire les temps d'arrêt des réseaux 5G de 40 %.

Les réseaux 5G sont plus vulnérables en raison de leur architecture distribuée et de leur connexion massive d'appareils (IoT). L'IA permet de **détecter les menaces en temps**

réel et **d'automatiser les réponses**, ce qui est crucial pour maintenir la disponibilité du réseau

Conclusion

En conclusion, l'intégration de l'intelligence artificielle dans les infrastructures numériques n'est plus une simple option, mais une nécessité stratégique. Face à la complexité croissante des réseaux, marquée par la multiplication des appareils et des services, les techniques traditionnelles de gestion s'avèrent désormais inadaptées.

L'apport de l'IA est déterminant en fournissant premièrement une gestion optimisée et proactive **:** l'intelligence artificielle transforme radicalement la maintenance des infrastructures en passant d'un modèle réactif à une approche préventive capable d'anticiper les défaillances réseau avant qu'elles ne surviennent. Grâce à l'analyse en temps réel de vastes quantités de données, l'IA assure une allocation dynamique des ressources, telles que la bande passante et la puissance de traitement, en s'ajustant automatiquement aux fluctuations de la demande. Cette gestion intelligente garantit non seulement des performances optimales pour les applications critiques, mais elle agit également comme un levier économique majeur en réduisant les coûts d'exploitation et en optimisant l'utilisation globale des équipements. Deuxièmement une sécurité résiliente et évolutive : face à la multiplication des cybermenaces complexes, l'IA surpasse les mesures de sécurité traditionnelles en apprenant continuellement le « rythme de vie » normal du réseau pour identifier instantanément toute activité suspecte. Elle permet de détecter des menaces inédites, comme les malwares « zero-day », en analysant le comportement des fichiers plutôt que de simples signatures connues. En automatisant la réponse aux incidents, les systèmes pilotés par l'IA peuvent isoler une machine infectée en quelques millisecondes, stoppant ainsi la propagation des attaques et assurant une protection proactive des données les plus sensibles.

Bien que des défis subsistent, notamment concernant les enjeux éthiques liés à la vie privée, les limites techniques des faux positifs ou l'émergence de menaces ciblant l'IA elle-même, l'intelligence artificielle s'impose comme le moteur indispensable de

l'innovation et de la résilience des réseaux modernes. Elle permet aux équipes informatiques de se libérer des tâches répétitives pour se concentrer sur des missions stratégiques, assurant ainsi la continuité et la performance des entreprises dans un environnement numérique en constante mutation.

Appendice

1-Une cyberattaque est le processus qui consiste à tenter de voler des données ou d'obtenir un accès non autorisé aux ordinateurs et aux réseaux à l'aide d'un ou plusieurs ordinateurs.

2- La commutation Ethernet connecte les appareils filaires tels que les ordinateurs, les ordinateurs portables, les routeurs, les serveurs et les imprimantes à un réseau local (LAN).

3- Une passerelle (en anglais, gateway) est le nom générique d'un dispositif permettant de relier deux réseaux informatiques de types différents, par exemple un réseau local et le réseau Internet.

4-Virus : Un virus informatique est une application malveillante ou un logiciel utilisé pour exercer une activité destructrice sur un appareil ou un réseau local.

5-Vers : Un ver informatique est un logiciel malveillant qui se reproduit sur plusieurs ordinateurs en utilisant un réseau informatique comme Internet.

6-Cheval de Troie : Un cheval de Troie, ou Trojan Horse en anglais, est un type de malware qui se déguise en logiciel légitime afin d'accéder à un système informatique.

7-API : Une interface de programmation d'application (API) est un code qui permet à deux logiciels de communiquer.

8- Enpoissement ARP : L'usurpation ARP, également appelée empoisonnement ARP, est la forme la plus répandue de cyberattaque par laquelle un expéditeur malveillant envoie de faux messages ARP à un réseau local.

9-Darktrace est une société britannique de cybersécurité, créée en 2013 et dont le siège est situé à Cambridge, en Angleterre[2]

10- Le SOAR (« Security Orchestration, Automation and Response ») est un type de solution logicielle qui permet aux équipes de sécurité d'intégrer et de coordonner des outils de sécurité distincts, d'automatiser les tâches répétitives et de rationaliser les workflows de réponse aux incidents et aux menaces.

11- IBM QRadar est une plateforme de gestion de sécurité des réseaux offrant une prise en charge de la géolocalisation et de la conformité.

12- *Microsoft Defender pour Office 365* est un logiciel puissant pour sécuriser vos messageries électroniques.

13- CrowdStrike est une entreprise américaine de cybersécurité fondée en 2011 et basée à Austin, au Texas.

Références

https://www.sentinelone.com/fr/cybersecurity-101/cybersecurity/network-security-risks/

https://www.cisco.com/c/fr_ca/products/security/what-is-network-security.html

https://netceed.com/fr/news/how-ai-is-revolutionising-network-infrastructure-security/

https://www.fortinet.com/fr/resources/cyberglossary/artificial-intelligence-in-cybersecurity

https://www.fortinet.com/fr/resources/cyberglossary/what-is-network-security

https://www.darktrace.com/resources/towards-responsible-ai-in-cybersecurity

https://www.ibm.com/products/qradar-soar

https://www.microsoft.com/en-us/security/business/siem-and-xdr/microsoft-defender-office-365

https://www.crowdstrike.com/en-us/resources/white-papers/

https:// doi.org/10.36948/ijfmr.2020.v02i03.37456

https://www.ssi.gouv.fr/

https://www.gartner.com/

https://www.gsma.com/

https://ai.googleblog.com/

https://azure.microsoft.com/fr-fr/products/microsoft-sentinel/