OWASP

COTONOU CHAPTER

L'IA comme bouclier adaptatif : Innovations en détection et réponse automatisée

Comprendre simplement comment l'IA protège nos données au quotidien

Féliciano N. HOUNMENOU | Senior Software Engineer | +229 0197322632

11 Décembre 2025

Contenu

1. **Introduction : La cybersécurité, une préoccupation pour tous;** Les cyberattaques augmentent et les solutions classiques ne suffisent plus ; l'IA apporte une défense plus dynamique.

2. **La détection et la réponse avant l'IA ;** Détection basée sur des signatures, forte dépendance à l'humain et réponses souvent lentes.

3. **L'IA entre en scène;** Apprentissage continu, analyse de données massives et automatisation des réponses comblent les limites traditionnelles.

4. **L'IA comme bouclier adaptatif : La défense devient dynamique;** L'IA apprend en continu, détecte en temps réel et s'adapte aux nouvelles menaces.

5. **Méthodes simples pour identifier et éviter les menaces courantes du quotidien;** Vérifier les liens, les expéditeurs, utiliser un antivirus et vérifier les informations.

6. **L'écosystème concret : Plateformes et mise en œuvre ;** XDR, SOAR et renseignement sur les menaces forment la base de la cybersécurité moderne.

7. **Les nouveaux défis : Les limites du bouclier intelligent;** IA utilisée par les attaquants, modèles manipulables, attaques adversariales et vigilance nécessaire.

8. **Conclusion : Le meilleur de l'alliance IA et cybersécurité ;** L'IA renforce la cybersécurité ; humains et machines sont complémentaires pour mieux se protéger.

1. Introduction

La cybersécurité, une préoccupation pour tous

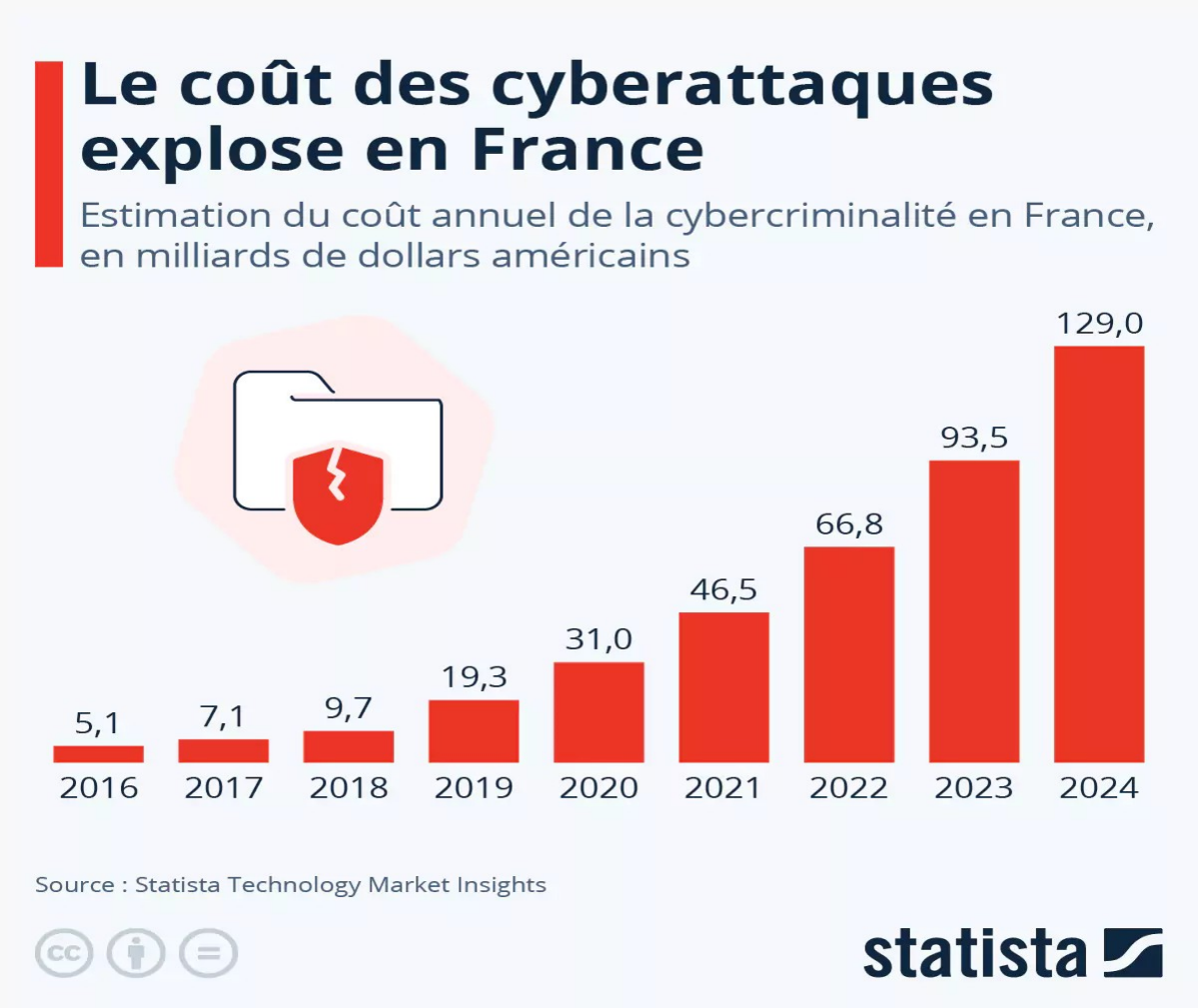
1. Introduction : La cybersécurité, une préoccupation pour tous

La **cybersécurité e**st plus que jamais au cœur des **préoccupations mondiales**, tant pour les **entreprises** que pour les **particuliers**.

Les **cyberattaques ont évolué** avec des menaces plus sophistiquées, notamment les ransomwares avancés et l'exploitation des vulnérabilités.

Les **solutions classiques** (antivirus, firewalls) restent essentielles mais ne sont plus **suffisantes** face à l'**évolution des cybermenaces.**

L'**intelligence artificielle** joue désormais un rôle crucial dans la cybersécurité en 2025, offrant des défenses plus proactives et adaptatives face aux menaces.



2. La détection et la réponse avant l'IA

une vigilance humaine partielle, avec l'homme en première ligne.

2. La détection et la réponse avant l'IA : une vigilance humaine partielle, avec l'homme en première ligne.

Les systèmes classiques de détection : des défenses réactives et limitées

Avant l'IA, la cybersécurité reposait principalement sur des outils statiques.

- **Les antivirus :** Recherche de signatures spécifiques de virus. Reconnaît seulement les virus connus
- **Les firewalls :** Ces pare-feu filtrent le trafic réseau selon des règles préétablies.
- **Les systèmes IDS/IPS :** Ils détectent les intrusions en se basant sur des **modèles préexistants** de comportement.uées.

Si une menace n'est pas encore répertoriée, elle passe souvent inaperçue.

2. La détection et la réponse avant l'IA : une vigilance humaine partielle, avec l'homme en première ligne.

Les limites des systèmes traditionnels : Une surveillance partielle et des réponses lentes

Les systèmes traditionnels de cybersécurité sont souvent centrés sur des règles **rigides** et des **signatures prédéfinies**.

- **Incapacité à détecter les menaces nouvelles**
- **Beaucoup de faux positifs et faux négatifs**
- **Réponse lente car humaine**

Bien que ces outils aient été les premières lignes de défense, ils **manquent d'agilité** et ne sont pas **capables de répondre** à des menaces dynamiques et complexes.

2. La détection et la réponse avant l'IA : une vigilance humaine partielle, avec l'homme en première ligne.

Rôle de l’humain dans les systèmes traditionnels

Volume élevé d'alertes : Les analystes doivent traiter un grand nombre d’alertes, ce qui augmente le risque d'erreur humaine et ralentit la réponse.

Compétence et disponibilité : La détection des menaces avancées, nécessite des compétences spécialisées et de la disponibilité.

Bien que l'humain reste une composante clé dans la détection des menaces, cette approche humaine n’est pas suffisante face à l’évolution rapide et complexe des cyberattaques.

Un analyste peut recevoir jusqu’à 10 000 alertes par jour.

3. L'IA entre en scène

L'Assistant super-intelligent

3. L'IA entre en scène : L'Assistant super-intelligent

Comment l’IA transforme la cybersécurité ?

Avant l’IA : Une défense limitée	Avec l’IA : Un changement de paradigme
Détection basée sur des règles fixes et des signatures connues	Apprentissage continu : l’IA apprend des nouvelles menaces chaque jour
Surplus d’alertes et nombreux faux positifs	Analyse massive : traite en temps réel des millions d’événements pour repérer les signaux faibles
Réponses manuelles souvent trop lentes	Moins de bruit : rÃ©duction des faux positifs, meilleure efficacitÃ© des analystes

L’IA en action : plus rapide, plus intelligente

- **Détection comportementale** : repère des anomalies invisibles aux solutions classiques.
- **Réponse automatisée (SOAR)** : isole un poste infecté, bloque une IP, supprime un e-mail malveillant.
- **Complémentarité humain + machine :** l’IA automatise, l’humain supervise et prend les décisions stratégiques.

4. L'IA comme bouclier adaptatif

La défense devient dynamique

4. L'IA comme bouclier adaptatif : La défense devient dynamique

Un **bouclier adaptatif** est un **système de défense intelligent** et **évolutif** capable de **réagir** immédiatement aux **menaces émergentes**. Il **surveille constamment** l'environnement, **détecte les anomalies** et **ajuste ses mécanismes de protection** en temps réel pour contrer des attaques nouvelles ou inconnues.

4. L'IA comme bouclier adaptatif : La défense devient dynamique

L'intégration de l'intelligence artificielle a transformé la cybersécurité d'un ensemble de mesures statiques et réactives en **un bouclier adaptatif et dynamique**.

- **Adaptation en temps réel et prévention prédictive**
- **Visibilité étendue et corrélation avancée**
- **Automatisation de la réponse à grande échelle**
- **La résilience et la chasse aux menaces proactive**

Détecte → Analyse → Agit → Apprend

4. L'IA comme bouclier adaptatif : La défense devient dynamique

Adaptation en temps réel et prévention prédictive

Capacité à ajuster sa posture de sécurité de manière autonome.

- **Apprentissage continu :** L'IA apprend en permanence des menaces rencontrées ou partagées via des flux de renseignement sur les menaces.
- **Analyse prédictive :** En analysant les tendances et comportements suspects, l'IA prédit les attaques et renforce proactivement les vulnérabilités avant exploitation.

L'IA peut prévoir une attaque avant qu'elle ne démarre.

4. L'IA comme bouclier adaptatif : La défense devient dynamique

Visibilité étendue et corrélation avancée

L'IA offre une compréhension globale de l'environnement informatique que les humains peinent à assembler manuellement.

EDR et XDR : Ces plateformes utilisent l'IA pour corréler les données de différentes sources (endpoints, cloud, réseau, e-mail) et reconstituer des chaînes d'attaque complexes, offrant une vision complète des incidents.

Cartographie comportementale : L'IA modélise les comportements normaux des utilisateurs et systèmes, s'ajustant dynamiquement lorsqu'un comportement anormal est détecté, comme l'accès à des données sensibles à des heures inhabituelles.

4. L'IA comme bouclier adaptatif : La défense devient dynamique

Automatisation de la réponse à grande échelle

La rapidité est l'essence même de la défense dynamique. L'IA permet une action immédiate pour contenir les menaces.

Réponse orchestrée : Via les outils SOAR, l'IA exécute des "playbooks" (**scénarios de réponse**) automatiquement. Cette rapidité d'exécution réduit considérablement la fenêtre d'opportunité pour les attaquants.

Micro-segmentation dynamique : L'IA reconfigure automatiquement les politiques de pare-feu et isole les segments de réseau dès qu'une activité malveillante est détectée, garantissant une défense agile sans intervention humaine.

Menace → Playbook → Action

4. L'IA comme bouclier adaptatif : La défense devient dynamique

La résilience et la chasse aux menaces proactive

Le bouclier adaptatif ne se contente pas de réagir aux alertes ; il cherche activement les menaces cachées.

Threat Hunting assisté par IA : L'IA aide les analystes à "**chasser**" les **menaces** (threat hunting) en mettant en évidence des anomalies faibles et des hypothèses d'investigation, là où un humain seul n'aurait pas su où chercher.

Amélioration continue de la posture : L'analyse continue des incidents et des échecs de détection permet à l'IA d'ajuster les contrôles de sécurité, renforçant ainsi la résilience globale du système face aux attaques futures.

L'IA aide les analystes à trouver les attaques cachées.

5. Méthodes simples pour identifier et éviter les menaces courantes du quotidien.

5. Méthodes simples pour identifier et éviter les menaces courantes du quotidien

Le **phishing** est une méthode d'escroquerie où des cybercriminels se font passer pour des entités légitimes pour voler vos informations personnelles.

Méthodes de prévention :

- Ne cliquez jamais sur des liens dans des e-mails suspects.
- Vérifiez l'authenticité de l'expéditeur et de l'adresse URL.
- Utilisez des outils de détection de phishing intégrés dans les e-mails et navigateurs web.

Outils basés sur l'IA pour détecter et éviter le phishing :

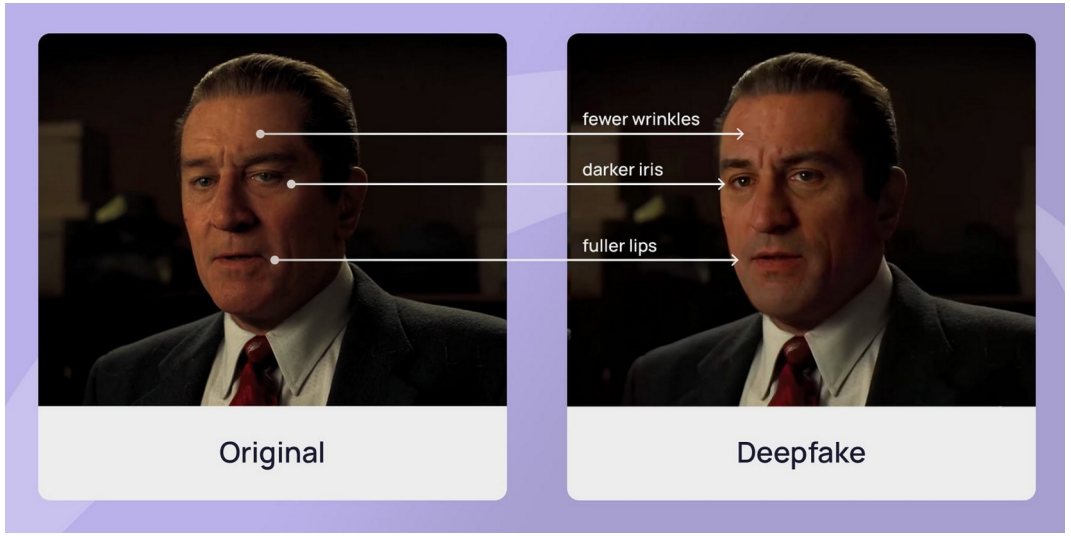
- **Google Safe Browsing :** Analyse les sites en temps réel, détecte les phishing et imitations de pages légitimes via l'IA.
- **PhishBot :** Identifie les modèles de phishing dans les emails et messages avec l'IA.
- **Microsoft Defender SmartScreen :** Bloque les sites de phishing et liens malveillants dans Edge grâce à l'apprentissage machine.

5. Méthodes simples pour identifier et éviter les menaces courantes du quotidien

Les **deepfakes** sont des vidéos, images ou audios manipulés par l'IA pour créer des contenus trompeurs ou faux.

Méthodes de prévention :

- Soyez sceptiques face à des vidéos ou images virales.
- Utilisez des outils pour analyser leur authenticité.



Outils basés sur l'IA pour détecter les deepfakes :

- **Deepware Scanner (par Deepware.ai) :** Deepware Scanner utilise l'IA pour identifier les signes de falsification dans les vidéos et audios.
- **Microsoft Video Authenticator :** Permet d’analyser les vidéos en profondeur pour détecter si elles ont été manipulées à l’aide de deepfakes.
- **Canal Whatsapp de la CNIN : https://whatsapp.com/channel/0029VbBsKGa7DAWuLvZUo039 :** La CNIN (Centre National d'Investigation du Numérique) du Bénin a mis en place un canal WhatsApp permettant de recevoir des notifications concernant les deepfakes.

5. Méthodes simples pour identifier et éviter les menaces courantes du quotidien

Les **virus, malwares** et la **désinformation** représentent des menaces permanentes pour la sécurité des appareils et la fiabilité de l'information.

Méthodes de prévention :

- Installez un antivirus fiable et maintenez-le à jour.
- Soyez prudent avec les sites web, ne téléchargez que des logiciels provenant de sources sûres.
- Utilisez des plateformes de vérification des faits pour contrer la désinformation.

Outils basés sur l'IA pour protéger vos appareils :

- **Norton 360 avec IA :** utilise l'IA pour détecter **malwares**, **ransomwares** et virus en temps réel, améliorant constamment ses capacités à identifier de nouvelles menaces.
- **Bitdefender GravityZone (pour entreprises) :** utilise l'IA pour **protéger les réseaux d'entreprises**, analysant les comportements des fichiers et applications pour détecter les menaces avant qu'elles n'affectent le système.

5. Méthodes simples pour identifier et éviter les menaces courantes du quotidien

Escroqueries par SMS (Smishing)

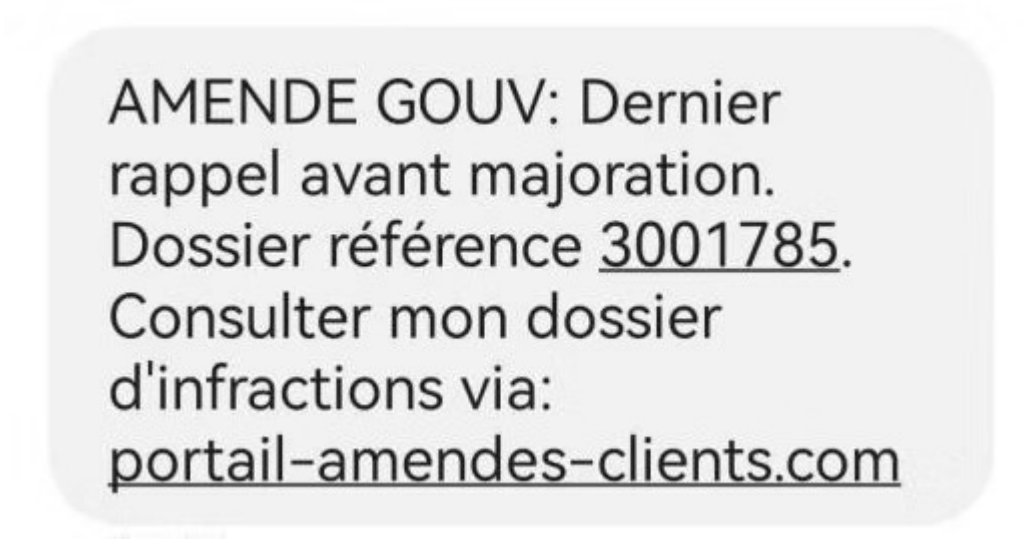
Le **smishing** est une forme de phishing qui utilise des SMS pour tromper les victimes. Les escrocs envoient des messages qui semblent provenir d'organisations légitimes (banques, administrations) pour obtenir des informations sensibles.

Comment s'en protéger :

- Ne répondez jamais à des messages SMS demandant des informations personnelles.
- Vérifiez les informations directement sur les sites web officiels ou en appelant l'entreprise en question.

Outil recommandé :

Truecaller : Cette application utilise l'IA pour identifier et bloquer les appels et SMS frauduleux.



6. L'écosystème concret

Plateformes et mise en œuvre

6. L'écosystème concret : Plateformes et mise en œuvre

L’association des **outils traditionnels** et de **l’intelligence artificielle** a permis de créer un écosystème moderne de cybersécurité, capable de **détecter, analyser et répondre aux menaces** de manière **coordonnée et intelligente**.

Cet écosystème repose sur quatre piliers clés :

- **XDR (Extended Detection & Response) :** plateformes unifiées de détection et de réponse sur tous les environnements.
- **SOAR (Security Orchestration, Automation and Response) :** automatisation et orchestration des actions de sécurité.
- **TIP (Threat Intelligence Platforms) :** collecte et partage du renseignement sur les menaces.
- **SOC (Centre des Opérations de Sécurité) moderne :** équipe centrale qui supervise, analyse et pilote l’ensemble du dispositif.

6. L'écosystème concret : Plateformes et mise en œuvre

Les plateformes de détection et réponse étendues (XDR) : *Le poste de pilotage central de l'IA*

Le **XDR** est l'évolution naturelle des systèmes EDR (**Endpoint Detection and Response)** et **SIEM traditionnels**. C'est le cœur du bouclier adaptatif.

Une plateforme **XDR** collecte et normalise les données provenant de diverses sources : endpoints (ordinateurs, serveurs), réseaux, cloud, e-mails et identités des utilisateurs.

L'utilisation des données de sources variées permettant de reconstituer une attaque complète qui aurait pu passer inaperçue avec des outils isolés.

L'organisation déploie un agent logiciel sur ses appareils et configure des connecteurs pour ses services cloud, tous remontant les données vers la plateforme centrale **XDR**.

6. L'écosystème concret : Plateformes et mise en œuvre

Les Outils d'Orchestration, d'Automatisation et de Réponse (SOAR) : *Le Bouton rouge d'urgence automatique*

Les plateformes SOAR agissent comme le moteur de l'automatisation de la réponse dynamique décrite précédemment.

Scénarios : Les analystes définissent des "playbooks" — des suites d'actions prédéfinies à exécuter en cas d'alerte spécifique. L'IA peut suggérer ou déclencher ces scénarios.

Le SOAR s'interface avec tous les autres outils de sécurité (pare-feu, XDR, gestionnaire d'identité, etc.) pour orchestrer la réponse.

Lorsqu'une alerte critique est validée par l'IA ou un analyste, le SOAR peut automatiquement exécuter des actions comme :

- **Bloquer** une adresse IP malveillante au niveau du pare-feu.
- **Isoler** l'ordinateur infecté du réseau.
- Lancer une **analyse antivirus** complète sur les systèmes affectés.
- **Créer un ticket** d'incident dans l'outil de gestion des services informatiques.

6. L'écosystème concret : Plateformes et mise en œuvre

Les plateformes de renseignement sur les menaces (TIP) : Les renseignements secrets de l'IA

Pour alimenter l'IA en données externes à jour, les TIP (Threat Intelligence Platforms) sont essentielles.

Ces plateformes collectent des flux d'informations sur les nouvelles menaces, les adresses IP compromises, les domaines de phishing et les tactiques d'attaque (TTPs - Tactiques, Techniques et Procédures) provenant de sources publiques et privées.

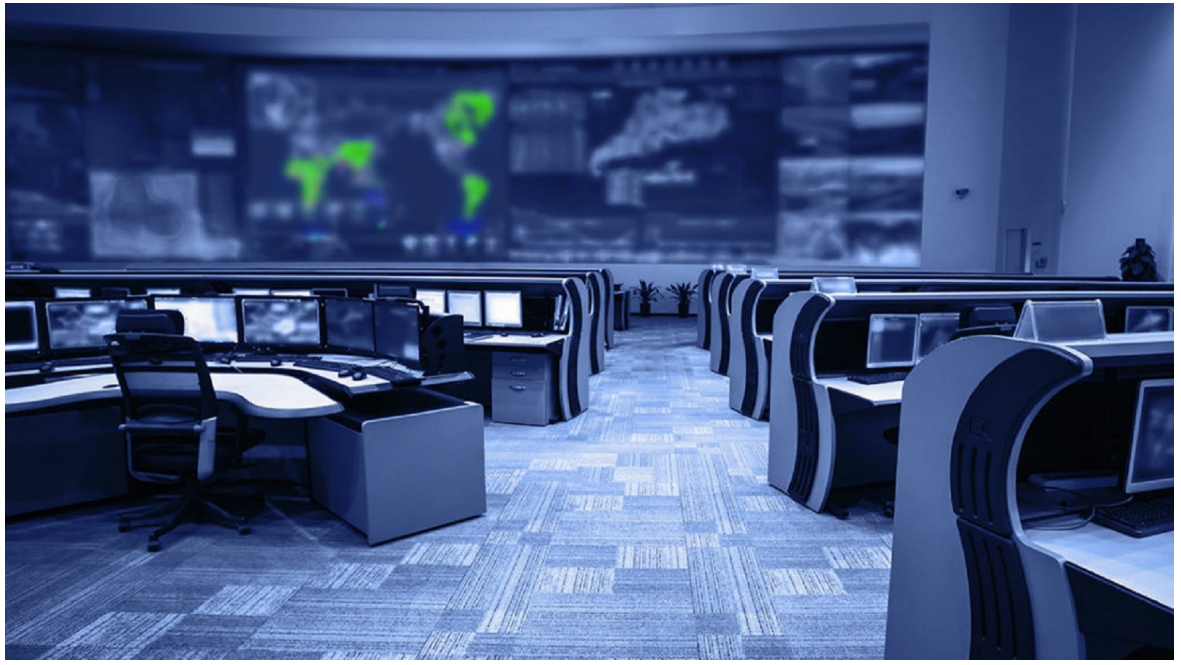
L'IA utilise ces données pour enrichir ses modèles de détection, s'assurant ainsi que le bouclier adaptatif est conscient des menaces les plus récentes au niveau mondial. Des outils comme MISP (Malware Information Sharing Platform) facilitent ce partage d'informations.

6. L'écosystème concret : Plateformes et mise en œuvre

Le rôle central du Centre des Opérations de Sécurité (SOC) Moderne

Même avec l'automatisation, l'humain reste crucial pour la supervision, l'éthique et les décisions stratégiques.

Le SOC agit comme le centre de commandement de la cybersécurité. Ses équipes sont formées pour maîtriser ces nouvelles plateformes et évoluer d’un simple rôle de “répondeur d’alertes” vers une fonction de gestion stratégique de la sécurité.



7. Les nouveaux défis

Les limites du bouclier intelligent

7. Les nouveaux défis : Les limites du bouclier intelligent

Même si l'IA renforce fortement la cybersécurité, elle apporte aussi de nouveaux défis :

1. Les attaquants utilisent eux aussi l'IA

- Création de malwares capables d'échapper à la détection.
- Phishing et deepfakes ultra-réalistes → attaques plus crédibles et ciblées.

2. Fragilité des modèles d'IA

- Attaques adversariales : modifier légèrement une donnée pour tromper l'IA.
- Empoisonnement des données : corrompre les données d'entraînement pour biaiser le système.

3. Manque de transparence

- Les modèles complexes fonctionnent comme des "boîtes noires".
- Difficile d'expliquer ou justifier certaines décisions (problème pour l'audit).

4. Complexité opérationnelle & coût

- Demande des experts rares (data science + sécurité).
- Nécessite des infrastructures puissantes et coûteuses.

8. Conclusion

Le meilleur de l’alliance IA et cybersécurité

8. Conclusion : Le meilleur de l’alliance IA et cybersécurité

L’alliance entre les solutions traditionnelles et les capacités dynamiques de l’IA a permis de créer un **écosystème moderne de cybersécurité**, capable de détecter, analyser et réagir aux menaces de façon coordonnée et intelligente.

Face à la **complexité croissante des cyberattaques**, ni l’humain ni la machine ne peuvent agir seuls.

L’**IA renforce les équipes de sécurité** en traitant des volumes massifs de données et en automatisant les actions rapides, tandis que l’expertise humaine reste indispensable pour la stratégie, le discernement, l’éthique et la gestion de crise.

Ensemble, l’humain et l’IA forment un duo complémentaire : l’IA optimise la réactivité et réduit la charge répétitive, et l’humain apporte l’analyse critique et la prise de décision.