FICHE DE VEILLE TECHNOLOGIQUE – BTS SIO

Nom / Prénom : Bayschanov Muslim

Option : SISR

Année : 2024 - 2025

1. THÈME DE LA VEILLE

Sujet : L'apport de l'Intelligence Artificielle dans la cyberdéfense proactive et l'anticipation des menaces.

Problématique :

En quoi l'intégration de l'IA et du Machine Learning permet-elle aux entreprises de passer d'une sécurité réactive à une posture prédictive face aux cybermenaces de nouvelle génération ?

Mots-clés principaux : Cyberdéfense, IA Prédictive, SOC (Security Operations Center), Threat Intelligence, Détection comportementale, Automatisation.

2. MÉTHODOLOGIE ET OUTILS

Pour assurer une surveillance continue et pertinente sur ce sujet évolutif, la méthode suivante est mise en place :

- **Agrégateur de flux RSS (Feedly) :** Abonnement aux flux spécialisés (ANSSI, LeMagIT Sécurité, ZDNet, The Hacker News).
- **Alertes Automatisées :** Google Alerts sur les termes "IA Cybersécurité", "Ransomware IA", "SOC Augmenté".
- **Sources Institutionnelles :** Rapports de l'ANSSI (Agence nationale de la sécurité des systèmes d'information) et du Clusif.
- **Fréquence de la veille :** Hebdomadaire (synthèse des articles le [Jour de ton choix]).

3. SYNTHÈSE DE LA VEILLE (État de l'art 2024-2025)

L'année 2024 marque un tournant où l'IA n'est plus une option mais une nécessité en cybersécurité pour traiter des volumes massifs de données ("Big Data de sécurité").

Axe 1 : De la réaction à l'anticipation (IA Prédictive)

Contrairement aux antivirus classiques basés sur des signatures (connaître le virus pour le bloquer), l'IA de 2024 utilise l'analyse comportementale. Elle établit un "modèle normal" du réseau de l'entreprise. Dès qu'un comportement dévie (ex: un transfert de données inhabituel à 3h du matin), l'IA détecte l'anomalie **avant** que l'attaque ne soit finalisée. Les algorithmes de *Deep Learning* permettent désormais de prédire les vecteurs d'attaques probables en analysant les tendances mondiales.

Axe 2 : L'automatisation des SOC (Centres opérationnels de sécurité)

Les équipes de sécurité font face à une pénurie de talents et une fatigue liée aux alertes. L'IA générative (type Copilot for Security) agit comme un assistant virtuel :

- Elle trie les milliers d'alertes quotidiennes pour éliminer les "faux positifs".
- Elle rédige automatiquement les rapports d'incidents.
- Elle propose des scripts de remédiation immédiate.

Axe 3 : La réponse à la menace "IA contre IA"

Les cybercriminels utilisent désormais l'IA pour créer des malwares polymorphes (qui changent de code tout seuls) et des campagnes de phishing ultra-personnalisées (via Deepfakes). Pour contrer ces attaques "machine-speed" (vitesse machine), seule une IA défensive peut réagir assez vite (en quelques millisecondes) pour isoler une machine infectée sans intervention humaine.

4. SÉLECTION D'ARTICLES ET SOURCES MAJEURES (2024-2025)

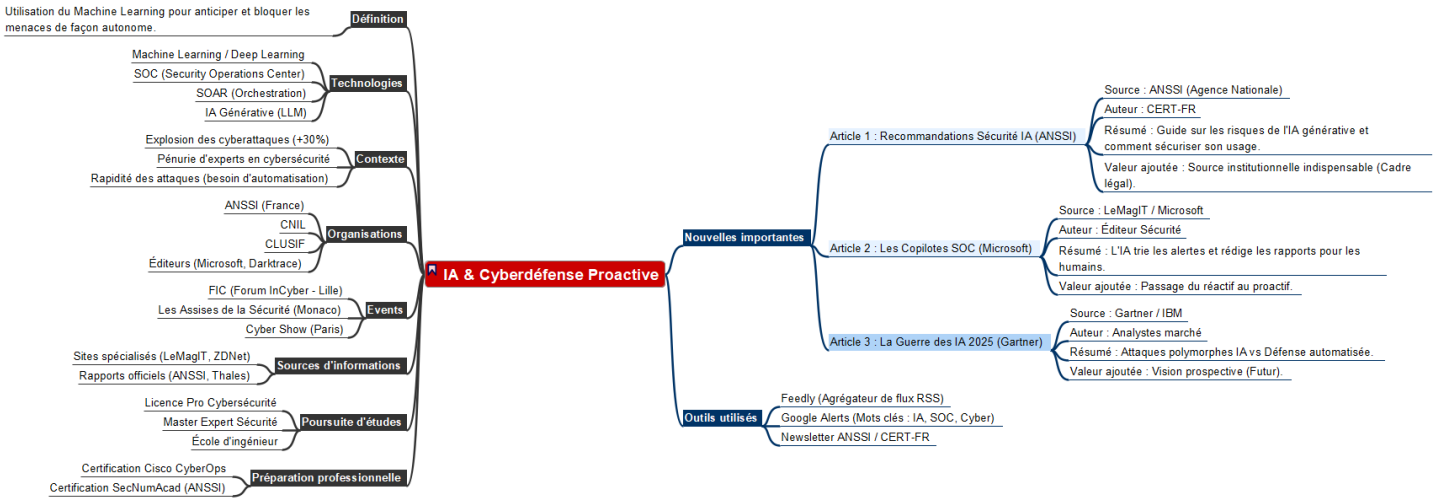
Voici les sources clés analysées pour cette veille :

Date	Source / Éditeur	Titre de l'article / Rapport	Résumé et Intérêt pour la veille
Avril 2024	**ANSSI** (Agence Nationale)	*Recommandations de sécurité pour les systèmes d'IA*	**Contenu :** L'ANSSI publie ses premières règles pour sécuriser l'usage de l'IA en entreprise. **Intérêt :** Cadre légal et technique français indispensable. Souligne que l'IA est un outil de défense mais aussi

Date	Source / Éditeur	Titre de l'article / Rapport	Résumé et Intérêt pour la veille
			une nouvelle surface d'attaque à protéger.
Juin 2024	**LeMagIT / Microsoft**	*L'essor des "Copilotes" de sécurité dans les SOC*	**Contenu :** Analyse de l'arrivée de l'IA Générative (LLM) dans les outils de supervision (SIEM). **Intérêt :** Montre comment l'IA réduit le temps d'investigation de 50% pour les analystes juniors et permet de "discuter" avec ses logs de sécurité.
Janv. 2025	**Rapport Gartner / IBM**	*Top Cybersecurity Trends for 2025*	**Contenu :** Prévisions sur la "guerre des IA". Le rapport indique qu'en 2025, plus de 50% des attaques de phishing utiliseront des Deepfakes générés par IA. **Intérêt :** Justifie pourquoi les entreprises doivent s'équiper d'outils de détection IA pour survivre.

5. CONCLUSION PROVISOIRE

L'intelligence artificielle est devenue le pilier central de la stratégie de cyberdéfense moderne. Elle ne remplace pas l'expert humain, mais elle "augmente" ses capacités en lui permettant de voir l'invisible (signaux faibles) et de réagir à la vitesse de l'attaquant. La veille continuera de se focaliser sur l'évolution des **IA offensives** qui représentent le prochain grand défi technique.


IA & Cyberdéfense Proactive
Définition
Utilisation du Machine Learning pour anticiper et bloquer les menaces de façon autonome.
Technologies
Machine Learning / Deep Learning
SOC (Security Operations Center)
SOAR (Orchestration)
IA Générative (LLM)
Contexte
Explosion des cyberattaques (+30%)
Pénurie d'experts en cybersécurité
Rapidité des attaques (besoin d'automatisation)
Organisations
ANSSI (France)
CNIL
CLUSIF
Éditeurs (Microsoft, Darktrace)
Events
FIC (Forum InCyber - Lille)
Les Assises de la Sécurité (Monaco)
Cyber Show (Paris)
Sources d'informations
Sites spécialisés (LeMagIT, ZDNet)
Rapports officiels (ANSSI, Thales)
Poursuite d'études
Licence Pro Cybersécurité
Master Expert Sécurité
École d'ingénieur
Préparation professionnelle
Certification Cisco CyberOps
Certification SecNumAcad (ANSSI)
Nouvelles importantes
Article 1 : Recommandations Sécurité IA (ANSSI)
Source : ANSSI (Agence Nationale)
Auteur : CERT-FR
Résumé : Guide sur les risques de l'IA générative et comment sécuriser son usage.
Valeur ajoutée : Source institutionnelle indispensable (Cadre légal).
Article 2 : Les Copilotes SOC (Microsoft)
Source : LeMagIT / Microsoft
Auteur : Éditeur Sécurité
Résumé : L'IA trie les alertes et rédige les rapports pour les humains.
Valeur ajoutée : Passage du réactif au proactif.
Article 3 : La Guerre des IA 2025 (Gartner)
Source : Gartner / IBM
Auteur : Analystes marché
Résumé : Attaques polymorphes IA vs Défense automatisée.
Valeur ajoutée : Vision prospective (Futur).
Outils utilisés
Feedly (Agrégateur de flux RSS)
Google Alerts (Mots clés : IA, SOC, Cyber)
Newsletter ANSSI / CERT-FR