Veille technologique : L'intelligence artificielle dans la cybersécurité

METHODES, OUTILS ET TENDANCES EN 2025

Lycée LouisPergaud Besançon

Sommaire :

1. Introduction :

L'intelligence artificielle (IA) révolutionne la cybersécurité : détection prédictive, réponse automatisée, analyse comportementale. Face à des menaces numériques toujours plus sophistiquées, la veille technologique s'impose comme un outil stratégique pour anticiper les évolutions, renforcer la sécurité des systèmes d'information et adapter les pratiques professionnelles.

Dans un contexte où les cyberattaques se multiplient et gagnent en complexité, les entreprises et les professionnels de l'informatique doivent rester informés des innovations pour maintenir un niveau de protection optimal. L'IA, en particulier, transforme profondément les approches traditionnelles de défense en introduisant des mécanismes capables d'identifier des comportements suspects, d'analyser des volumes massifs de données en temps réel et de réagir automatiquement face aux incidents.

Ce rapport s'inscrit dans une démarche de veille active sur un sujet d'actualité : l'intégration de l'intelligence artificielle dans la cybersécurité. Il vise à démontrer comment une veille structurée et continue peut aider à comprendre les enjeux liés à cette technologie, tout en soutenant l'adaptation permanente des professionnels face aux nouvelles menaces.

Pour atteindre cet objectif, nous présenterons d'abord les principes et les concepts clés de la veille technologique, puis nous expliquerons le choix du sujet et son intérêt stratégique. Ensuite, nous détaillerons les outils utilisés pour la collecte d'informations (Google Alerts, Feedly, Inoreader), leur paramétrage et les méthodes de sélection des sources. Enfin, nous aborderons les modalités de diffusion et de valorisation des informations, avant de conclure sur les apports de cette veille et les perspectives qu'elle ouvre.

2. Présentation de la veille technologique :

2.1. Définition et objectifs :

La veille technologique est bien plus qu'une simple recherche d'informations : c'est un processus structuré, continu et stratégique qui vise à surveiller, analyser et exploiter les évolutions scientifiques, techniques et industrielles dans un domaine donné. Elle repose sur une démarche proactive permettant aux organisations et aux professionnels d'anticiper les changements, de détecter les innovations et de s'adapter aux nouvelles tendances susceptibles d'influencer leur activité.

Concrètement, la veille technologique consiste à collecter des données pertinentes issues de sources fiables (sites spécialisés, blogs, publications scientifiques, flux RSS, réseaux professionnels), à les analyser pour en extraire des informations à forte valeur ajoutée, puis à les diffuser sous une forme exploitable par les décideurs ou les équipes opérationnelles. Cette approche garantit une vision claire et actualisée de l'environnement technologique, favorisant la prise de décision éclairée.

Les objectifs principaux de la veille technologique sont multiples :

- **Anticiper les évolutions : identifier les technologies émergentes avant qu'elles ne deviennent incontournables.**
- **Prévenir les risques : détecter les menaces liées à l'obsolescence des systèmes ou aux nouvelles vulnérabilités.**
- **Optimiser les investissements : orienter les choix stratégiques en matière d'innovation et de sécurité.**
- **Renforcer la compétitivité : rester à la pointe des avancées pour maintenir un avantage concurrentiel.**
- **Améliorer la sécurité : dans le domaine informatique, la veille permet de suivre les solutions innovantes pour contrer les cyberattaques et protéger les données.**

Ainsi, la veille technologique s'inscrit dans une logique d'amélioration continue et de réactivité face à un environnement numérique en perpétuelle mutation. Elle constitue un levier essentiel pour toute organisation souhaitant rester performante et sécurisée.

2.2 Concepts clés :

La veille technologique repose sur plusieurs notions fondamentales qui structurent son fonctionnement et garantissent son efficacité. Ces concepts permettent de comprendre les différentes étapes du processus et les outils mobilisés pour transformer une masse d'informations en données exploitables.

- **Surveillance de l'environnement : Cette étape consiste à identifier les sources fiables et pertinentes pour le domaine étudié. Il peut s'agir de sites spécialisés, de blogs professionnels, de publications scientifiques, de flux RSS, de forums ou encore de réseaux sociaux. L'objectif est de capter les signaux faibles et les tendances émergentes avant qu'elles ne deviennent dominantes.**

- **Collecte automatisée : Pour éviter une recherche manuelle chronophage, des outils comme *Google Alerts*, *Feedly* ou *Inoreader* permettent de recevoir automatiquement les dernières actualités en fonction de mots-clés définis. Cette automatisation garantit une veille continue et réduit le risque de manquer des informations importantes.**

- **Analyse et tri de l'information : Toutes les données collectées ne sont pas pertinentes. Il est donc essentiel de vérifier la fiabilité des sources, de croiser les informations et de sélectionner celles qui apportent une réelle valeur ajoutée. Cette étape implique également une hiérarchisation des contenus selon leur importance stratégique.**

- **Diffusion et partage : Une veille efficace ne se limite pas à la collecte et à l'analyse. Les résultats doivent être diffusés sous une forme adaptée aux besoins des destinataires : rapports synthétiques, tableaux de bord, newsletters internes ou plateformes collaboratives. L'objectif est de rendre l'information exploitable et utile pour la prise de décision.**

- **Capitalisation et mise à jour : La veille technologique est un processus dynamique. Les sources doivent être régulièrement mises à jour, et les informations archivées pour conserver une trace des évolutions. Cette capitalisation permet de construire une base de connaissances solide et évolutive.**

Ces concepts sont interdépendants : la qualité de la veille repose sur la rigueur de la surveillance, la pertinence de la collecte, la fiabilité de l'analyse et l'efficacité de la diffusion. Dans le cadre de ce rapport, ces principes seront appliqués à un sujet stratégique : l'intégration de l'intelligence artificielle dans la cybersécurité, un domaine où les innovations technologiques redéfinissent les méthodes de détection, d'analyse et de réponse face aux menaces numériques.

3. Choix du sujet : L'intelligence artificielle dans la cybersécurité

3.1. Enjeux et intérêt du sujet :

L'intelligence artificielle (IA) s'impose aujourd'hui comme l'un des leviers les plus puissants de l'évolution technologique.
Appliquée à la cybersécurité, elle transforme en profondeur les méthodes de détection, d'analyse et de réponse face aux menaces numériques.

Dans un contexte où les attaques informatiques deviennent plus sophistiquées, rapides et ciblées, les systèmes traditionnels de défense montrent leurs limites. Les experts en sécurité doivent désormais traiter d'immenses volumes de données en temps réel, repérer des anomalies discrètes et anticiper les comportements malveillants.
C'est précisément dans ce domaine que l'intelligence artificielle intervient.

Pourquoi ce sujet est pertinent ? :

- **Parce qu'il combine deux domaines majeurs de l'informatique actuelle : l'IA et la cybersécurité ;**
- **Parce qu'il est au cœur des enjeux de sécurité numérique pour les entreprises, les institutions et les particuliers ;**
- **Parce qu'il illustre parfaitement l'intérêt d'une veille technologique : suivre un secteur en mutation constante pour anticiper les nouvelles méthodes d'attaque et de défense.**

Les apports de l'IA dans la cybersécurité :

L'intelligence artificielle permet de :

- **Automatiser la détection des menaces grâce à l'apprentissage automatique (*machine learning*) ;**
- **Analyser les comportements anormaux sur les réseaux et systèmes en continu ;**
- **Réagir en temps réel aux attaques par des systèmes intelligents de défense adaptative ;**
- **Réduire les faux positifs en affinant la reconnaissance des schémas de menace ;**
- **Renforcer la prévention par la prédiction d'incidents à partir de données historiques.**

Les limites et défis actuels :

Malgré ses avantages, l'IA soulève aussi des enjeux :

- **Dépendance aux données : la qualité des algorithmes repose sur des bases de données vastes et fiables ;**
- **Menaces adversariales : certaines attaques exploitent les failles de l'IA elle-même ;**
- **Questions éthiques et de transparence : comprendre les décisions prises par une IA reste complexe ;**
- **Coûts de mise en œuvre : les technologies d'IA nécessitent des infrastructures puissantes et un savoir-faire spécifique.**

Objectif de la veille :

Cette veille technologique vise à :

- **Surveiller les innovations et solutions émergentes en matière d'IA appliquée à la cybersécurité ;**
- **Identifier les nouveaux outils, protocoles et modèles de détection intelligente ;**
- **Anticiper les évolutions futures pour comprendre comment l'IA façonnera la cybersécurité dans les années à venir.**

4. Outils de veille utilisés

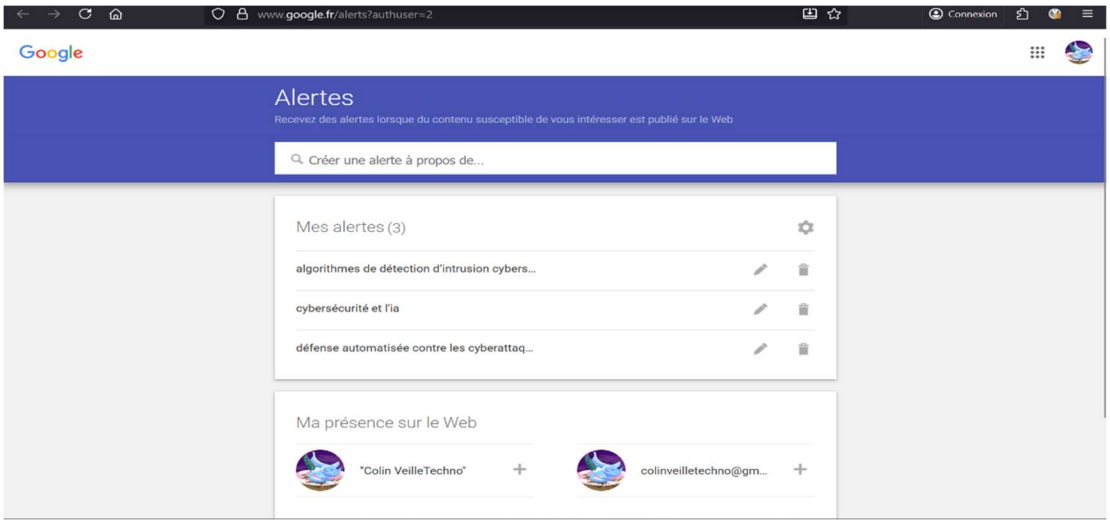
Pour cette veille technologique, trois outils complémentaires ont été mis en place : Google Alerts, Feedly et Inoreader.
Ces outils permettent de collecter, centraliser et suivre automatiquement les informations pertinentes liées au thème de l'intelligence artificielle dans la cybersécurité.

4.1 Google Alerts :

Google Alerts est un service gratuit proposé par Google permettant de recevoir des notifications par e-mail dès qu'un nouveau contenu correspondant à un mot-clé est publié sur le web. C'est un outil simple et rapide à configurer, idéal pour une première veille automatisée.

L'objectif ici est de surveiller l'apparition de nouveaux articles, rapports ou actualités liés à la cybersécurité et à l'IA.
Par exemple, des alertes ont été créées avec des mots-clés comme *« intelligence artificielle cybersécurité », « IA et sécurité informatique », « cyberattaque IA », « machine learning cyberdefense »*.

Les alertes sont configurées pour une fréquence quotidienne, afin de rester informé des publications récentes sans être submergé de courriels.



Interface de Google Alerts – Création d'alertes automatiques sur les mots-clés liés à l'intelligence artificielle et à la cybersécurité.

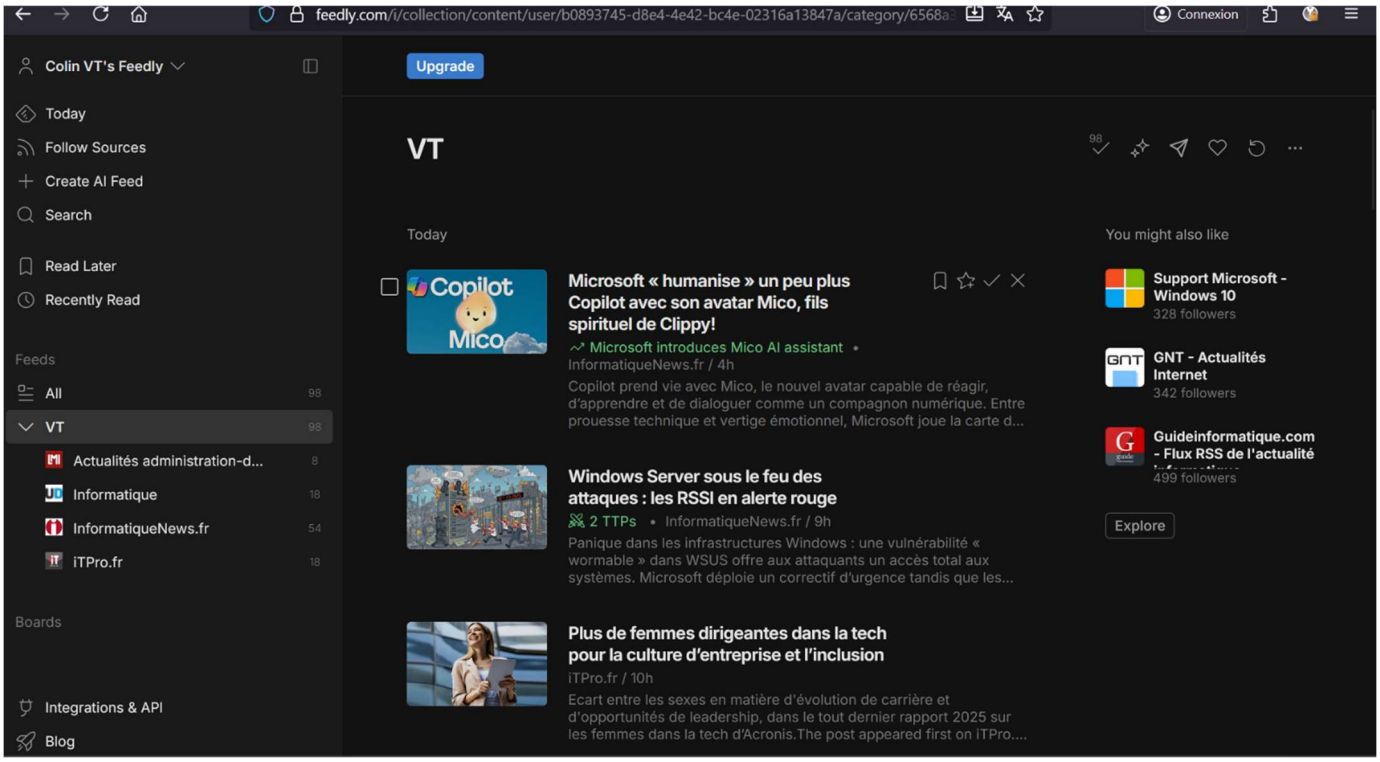
4.2 Feedly :

Feedly est un agrégateur de flux RSS qui permet de regrouper les publications provenant de plusieurs sources dans une interface claire et personnalisée.
Il est particulièrement utile pour suivre les sites spécialisés, blogs et médias technologiques.

Dans le cadre de cette veille, plusieurs flux RSS ont été ajoutés, notamment ceux de :

- ***The Hacker News*** **(actualités de la cybersécurité),**
- ***DarkReading*** **(analyse des menaces et innovations),**
- ***Security Intelligence*** **(veille IBM sur la cybersécurité),**
- ***TechCrunch AI*** **(innovations et IA appliquée à la sécurité).**

Ces sources permettent d'obtenir une veille ciblée et visuelle, en regroupant automatiquement les derniers articles par thème.
Feedly offre également des fonctions de marquage, sauvegarde et partage d'articles pour faciliter l'organisation des informations.



Interface de Feedly – Dossier de veille "VT" regroupant les flux RSS liés à l'intelligence artificielle et à la cybersécurité.

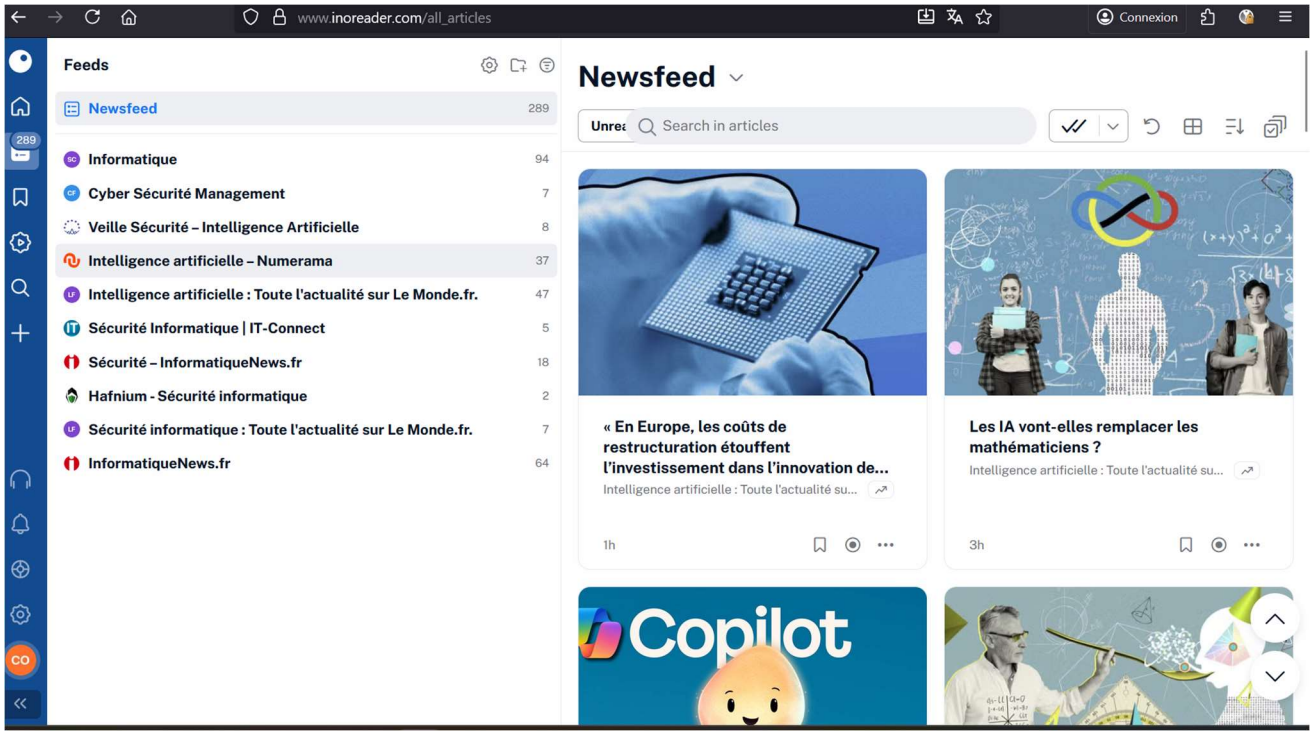
4.3 Inoreader :

Inoreader est un autre agrégateur de flux RSS, plus complet que Feedly sur la partie filtrage et automatisation.
Il permet d'aller plus loin dans la veille grâce à des règles intelligentes, comme le tri automatique des articles selon des mots-clés, ou l'envoi automatique d'un article vers une autre plateforme.

Inoreader a été utilisé pour :

- **Filtrer automatiquement les articles contenant des termes précis comme *"AI security", "machine learning threats", "cyber defense"* ;**
- **Organiser les sources par dossiers thématiques (ex. : *IA appliquée à la cybersécurité*, *analyse comportementale*, *menaces émergentes*) ;**

- **Partager les articles intéressants vers un espace commun ou un autre outil (ex. : Google Drive ou OneNote).**



Interface d'Inoreader – Organisation des flux RSS et filtres automatiques appliqués aux articles sur la cybersécurité et l'intelligence artificielle.

5. Paramétrage des outils

5.1 Mots-clés, flux RSS, filtres

La qualité d'une veille technologique repose en grande partie sur le paramétrage des outils utilisés. Une configuration précise permet de recevoir des informations pertinentes, d'éviter le bruit informationnel et de structurer efficacement la collecte. Dans le cadre de cette veille sur l'IA dans la cybersécurité, trois outils ont été mobilisés : Google Alerts, Feedly et Inoreader. Chacun d'eux a été paramétré selon des critères spécifiques pour garantir une surveillance optimale.

Google Alerts :

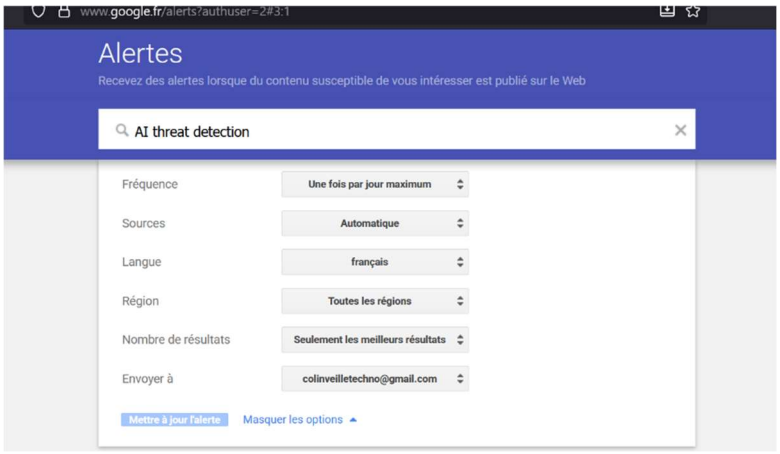
Les alertes ont été configurées autour de mots-clés spécifiques, en français et en anglais, afin de couvrir les actualités à la fois nationales et internationales :

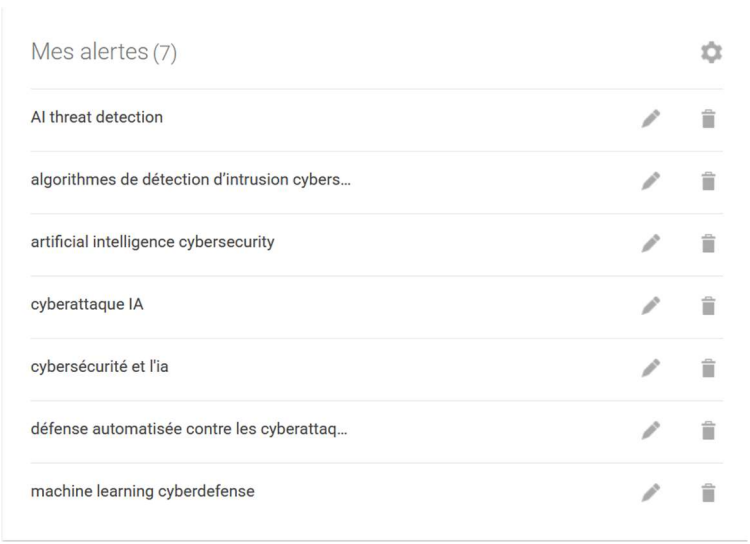
- **“intelligence artificielle cybersécurité”**
- **“IA et sécurité informatique”**
- **“cyberattaque IA”**
- **“machine learning cyberdefense”**
- **“artificial intelligence cybersecurity”**
- **“AI threat detection”**

Les paramètres choisis :

- **Fréquence : une fois par jour**
- **Langue : français et anglais**
- **Sources : actualités, blogs, web**
- **Région : monde entier**

Page Google Alerts montrant les mots-clés configurés et la fréquence d’envoi :





Feedly :

Pour Feedly, les flux RSS ont été ajoutés à un dossier dédié nommé *“VT” (Veille Technologique)* regroupant les sources les plus pertinentes sur le sujet :

Flux RSS ajoutés :

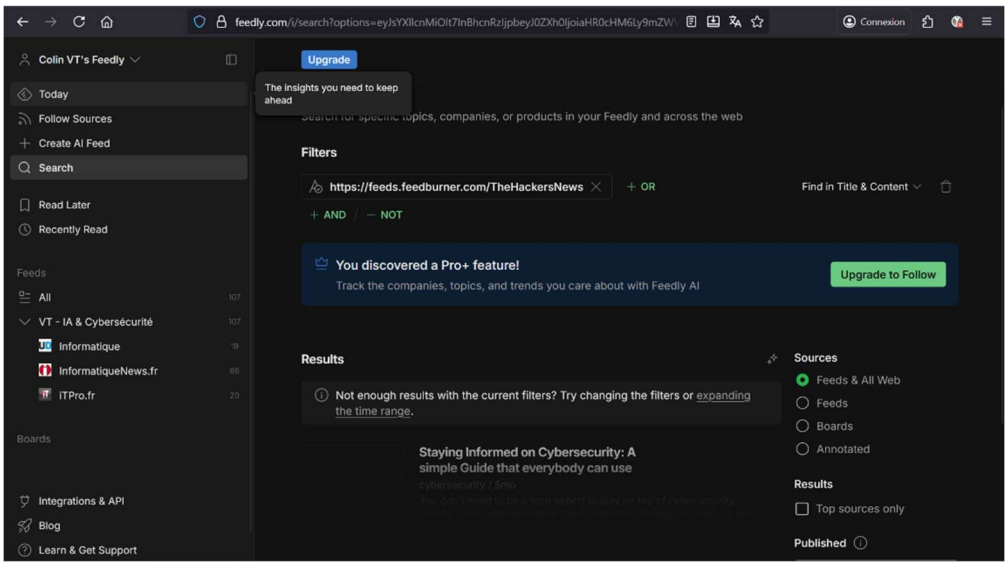
- **https://www.lemondeinformatique.fr/flux-rss/thematique/securite/rss.xml**
- **https://www.zdnet.fr/actualites/cybersecurite/rss.xml**
- **https://www.actuia.com/feed/**

- **https://feeds.feedburner.com/TheHackersNews**
- **https://www.darkreading.com/rss.xml**
- **https://feeds.feedburner.com/Securityweek**

Mots-clés utilisés dans Feedly :

- **“IA”**
- **“cybersécurité”**
- **“AI security”**
- **“machine learning”**
- **“threat detection”**

Les articles contenant ces termes sont automatiquement regroupés dans le dossier VT et peuvent être marqués comme lus, sauvegardés ou partagés.



Interface de Feedly – tentative d’ajout de flux RSS (fonctionnalités limitées dans la version gratuite). Bien que Feedly ait été testé, les limitations de la version gratuite ont restreint la possibilité de suivre certains flux RSS. L’outil Inoreader a donc été privilégié pour la suite de la veille.

Inoreader :

Inoreader a été configuré pour affiner davantage la veille et filtrer automatiquement les résultats. Il a permis de trier les articles en fonction de leur pertinence grâce à des règles intelligentes et à la création de dossiers thématiques.

Filtres configurés :

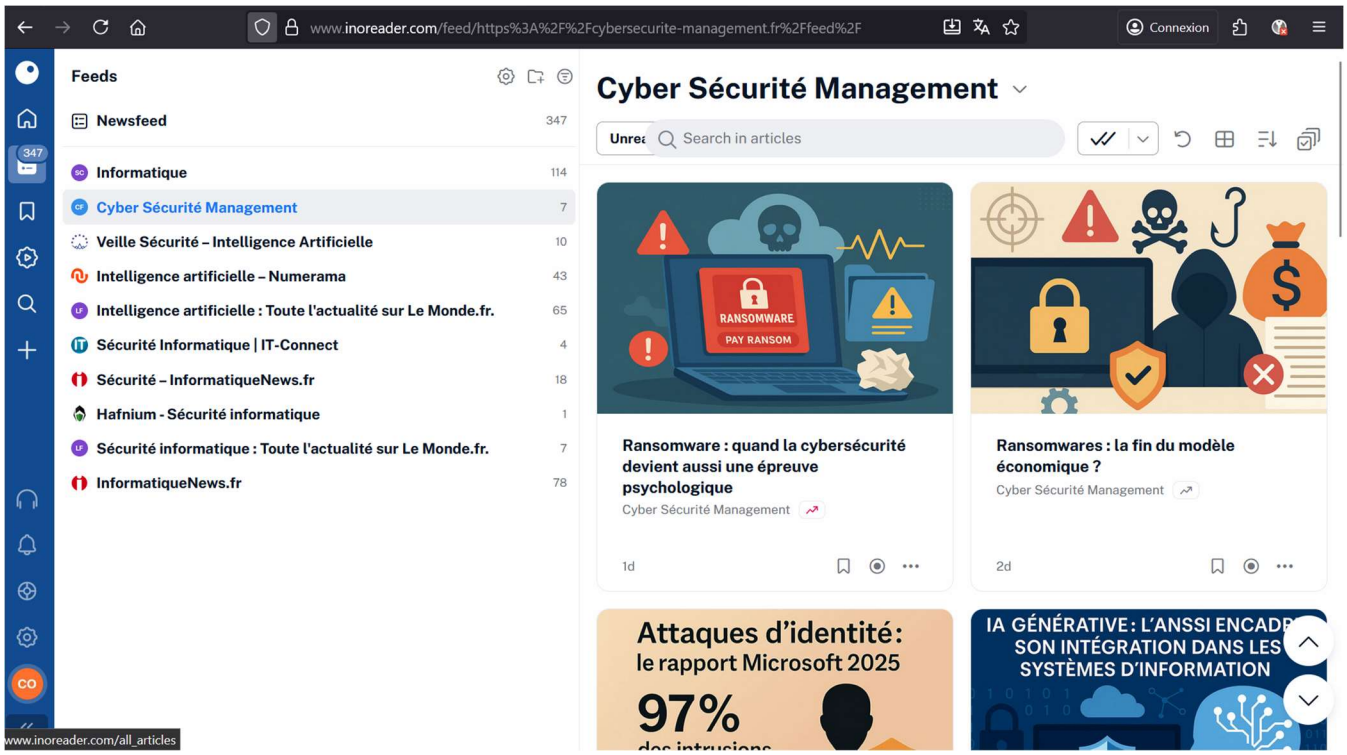
- **“AI security”**
- **“cyber defense”**

- **“machine learning threats”**
- **“deep learning malware detection”**

Dossiers créés :

- ***IA appliquée à la cybersécurité***
- ***Menaces émergentes***
- ***Analyse comportementale***

Les articles contenant les mots-clés prédéfinis sont automatiquement classés dans le dossier correspondant, ce qui simplifie le tri et la sélection des sources utiles.



Interface d’Inoreader montrant les dossiers créés et un filtre actif sur les mots-clés IA / cybersécurité

5.2 Concepts manipulés

Lors de la mise en place de cette veille, plusieurs concepts clés de gestion de l’information ont été utilisés à travers ces trois outils :

- **Flux RSS (Really Simple Syndication) : technologie permettant de recevoir automatiquement les nouvelles publications d’un site web sans devoir le consulter manuellement. Utilisée dans *Feedly* et *Inoreader* pour suivre plusieurs sources en parallèle.**
- **Filtres et règles automatiques : permettent de trier les articles selon des mots-clés, d’éviter les doublons et de repérer les informations les plus pertinentes.**

- **Alertes par mots-clés : principe utilisé dans *Google Alerts* pour détecter l'apparition de nouveaux contenus correspondant à une requête.**
- **Agrégation de contenu : consiste à centraliser les informations issues de plusieurs sources au sein d'une même interface (Feedly / Inoreader).**
- **Veille automatisée : la configuration de ces outils permet une surveillance continue, sans intervention manuelle quotidienne, garantissant une information actualisée et pertinente.**

6. Agrégation et sélection des sources

6.1. Méthodologie de sélection

Une fois les flux RSS et alertes configurés, la première étape consiste à agréger l'ensemble des informations provenant de Google Alerts, Feedly et Inoreader au même endroit. L'objectif est d'obtenir une vue centralisée des publications récentes liées à l'intelligence artificielle et à la cybersécurité.

Les articles collectés sont ensuite triés selon plusieurs critères :

- ***Présence de mots-clés : IA, cybersécurité, machine learning, cyberattaque, sécurité des données ;***
- ***Pertinence du contenu : priorité donnée aux articles détaillant des technologies ou cas concrets d'usage de l'IA dans la sécurité ;***
- ***Source de publication : exclusion des sites non vérifiés ou à caractère commercial abusif ;***
- ***Actualité de l'information : seuls les contenus publiés récemment sont retenus pour garantir la fraîcheur de la veille.***

Ce processus de sélection garantit une veille ciblée et qualitative, axée sur les innovations réelles du domaine.

6.2 Fiabilité et pertinence

La fiabilité des informations est un élément central d'une veille efficace. Chaque article sélectionné est évalué selon trois critères principaux :

- ***La crédibilité de la source : priorité aux sites reconnus dans le milieu technologique (Le Monde Informatique, ZDNet, The Hacker News, DarkReading, ActuIA, etc.).***
- ***La vérifiabilité de l'information : croisement de plusieurs sources avant validation.***

- ***L'objectivité du contenu : exclusion des articles à but purement promotionnel.***

L'analyse des titres et du contenu permet de repérer les publications les plus pertinentes, notamment celles présentant des études de cas, chiffres récents, ou nouvelles applications de l'IA dans la détection de menaces.

7. Partage et valorisation de l'information

7.1. Formats de diffusion

Les informations sélectionnées sont ensuite valorisées à travers plusieurs modes de diffusion. Pour cette veille, le partage s'effectue principalement sous forme de :

- Captures et synthèses intégrées au rapport ;
- Documents partagés (PDF, notes) contenant les liens vers les articles retenus ;
- Résumé personnel reprenant les grandes tendances identifiées.

Dans un contexte professionnel, cette diffusion pourrait se faire via :

- Une newsletter interne destinée à une équipe technique ;
- Un tableau collaboratif (Notion, Trello, Microsoft Teams) ;
- Ou encore un canal de communication sécurisé (ex. : intranet, messagerie d'entreprise).

7.2. Utilisation professionnelle

La veille technologique ne se limite pas à la collecte d'informations : elle constitue un outil d'aide à la décision.

Dans le cas de l'IA appliquée à la cybersécurité, les informations recueillies peuvent être exploitées pour :

- Adapter les politiques de sécurité d'une entreprise aux nouvelles menaces ;
- Anticiper les évolutions technologiques dans le domaine de la défense informatique ;
- Orienter les choix d'investissement vers des solutions utilisant l'IA pour la détection ou la prévention d'incidents.

Cette démarche de veille s'inscrit dans une logique d'amélioration continue, essentielle pour tout professionnel de l'informatique souhaitant rester à jour face à l'évolution rapide du secteur.

Aucune capture obligatoire ici non plus — c'est une partie plus réflexive et analytique.

8. Conclusion

8.1. Apports de la veille

Cette veille technologique sur l'intelligence artificielle dans la cybersécurité a permis de :

- Développer une méthode structurée de recherche et d'analyse d'informations ;
- Comprendre les applications concrètes de l'IA dans la détection et la prévention des cyberattaques ;
- Identifier les tendances actuelles : montée de l'automatisation, analyse comportementale, apprentissage machine, etc. ;
- Renforcer la culture technologique nécessaire à une carrière dans l'informatique et la sécurité des systèmes.

Au-delà de la simple recherche d'informations, cette veille a constitué un véritable travail d'observation et d'interprétation du monde numérique actuel.

8.2. Perspectives

À moyen terme, cette veille pourra être enrichie par :

- L'ajout de nouvelles sources anglophones (rapports d'entreprises spécialisées, blogs de chercheurs) ;
- L'intégration d'outils d'IA générative pour automatiser la synthèse d'articles ;
- La création d'un tableau de bord dynamique pour suivre les tendances en temps réel.

L'objectif futur serait de transformer cette veille en veille collaborative, intégrée à un environnement professionnel, permettant un suivi collectif des innovations en intelligence artificielle et cybersécurité.