Qu’est ce que la veille technologique et à quoi ça sert ?

La veille technologique est un processus continu et structuré de collecte, d'analyse et de diffusion d'informations sur les innovations, les brevets et les tendances R&D. Elle est cruciale pour l'entreprise puisqu’elle constitue un outil d'intelligence économique indispensable.

En effet, elle permet de maintenir un avantage concurrentiel en anticipant les ruptures et en identifiant de nouvelles opportunités d'innovation, d’éclairer les décisions stratégiques (investissements, partenariats), mais également de contribuer à l'optimisation des performances opérationnelles tout en garantissant la conformité réglementaire.
En définitive, elle est un impératif pour assurer la pérennité et l'adaptabilité de l'organisation face aux évolutions rapides de son environnement technologique.

Les principaux axes de veille

La veille doit être ciblée sur les domaines technologiques clés pour l'activité de l'organisation.
Voici deux exemples d'axes de veille pertinents dans le secteur de l’informatique :

Axe de Veille	Sources Pertinentes	Description
Cyberattaque & Cybersécurité	ANSSI https://cyber.gouv.fr/publications	Publications de l'Agence Nationale de la Sécurité des Systèmes d'Information (France).
	ENISA https://www.enisa.europa.eu/publications	Rapports de l'Agence de l'Union Européenne pour la Cybersécurité.
	CISA https://www.cisa.com/fr/cisa-blog.html	Alertes et publications de la Cybersecurity and Infrastructure Security Agency (USA).
	The hacker new https://thehackernews.com/	Actualités et analyses sur les menaces et vulnérabilités.

Axe de Veille	Sources Pertinentes	Description
	GitHub (outils de sécurité, PoC d'attaques) https://github.blog/	Suivi des dépôts et outils de sécurité open source.
	Baptiste Robert https://www.linkedin.com/in/baptisterobert/	Expertise et analyse sur les failles et techniques d'attaque.
	Parlons Cyber https://www.youtube.com/@ParlonsCyber	Contenu vidéo pédagogique et informatif sur la cybersécurité.
	Bleeping Computer https://www.bleepingcomputer.com/	Actualités sur les ransomwares, malwares et failles de sécurité.
	NVD https://nvd.nist.gov/	Base de données nationale des vulnérabilités (National Vulnerability Database).

Choix du sujet de veille

La veille informationnelle sur le thème de la cybersécurité est cruciale pour plusieurs raisons essentielles :

1. **Anticipation et Prévention des Menaces :** Le paysage des menaces évolue constamment (nouveaux malwares, techniques de phishing, vulnérabilités "zero-day", etc.). Une veille active permet d'identifier rapidement ces nouvelles menaces et de prendre des mesures préventives avant qu'elles ne soient exploitées.
2. **Mise à Jour de la Défense :** La veille permet de rester informé des nouvelles failles de sécurité découvertes dans les logiciels et systèmes utilisés, et des correctifs (patchs) publiés par les éditeurs. C'est la base d'une gestion proactive des vulnérabilités.
3. **Conformité Réglementaire :** De nombreuses réglementations (comme le RGPD en Europe) imposent des exigences strictes en matière de protection des données. La veille aide à s'assurer que les pratiques de sécurité restent en conformité avec les lois et les normes en vigueur.
4. **Amélioration de la Posture de Sécurité :** En analysant les incidents de sécurité chez d'autres organisations, on peut tirer des leçons, adapter ses propres stratégies de défense et renforcer sa posture de sécurité globale.
5. **Sensibilisation et Formation :** Les informations recueillies par la veille sont indispensables pour former et sensibiliser les employés aux dernières techniques d'attaque (ingénierie sociale, par exemple), car l'erreur humaine reste souvent le maillon faible.

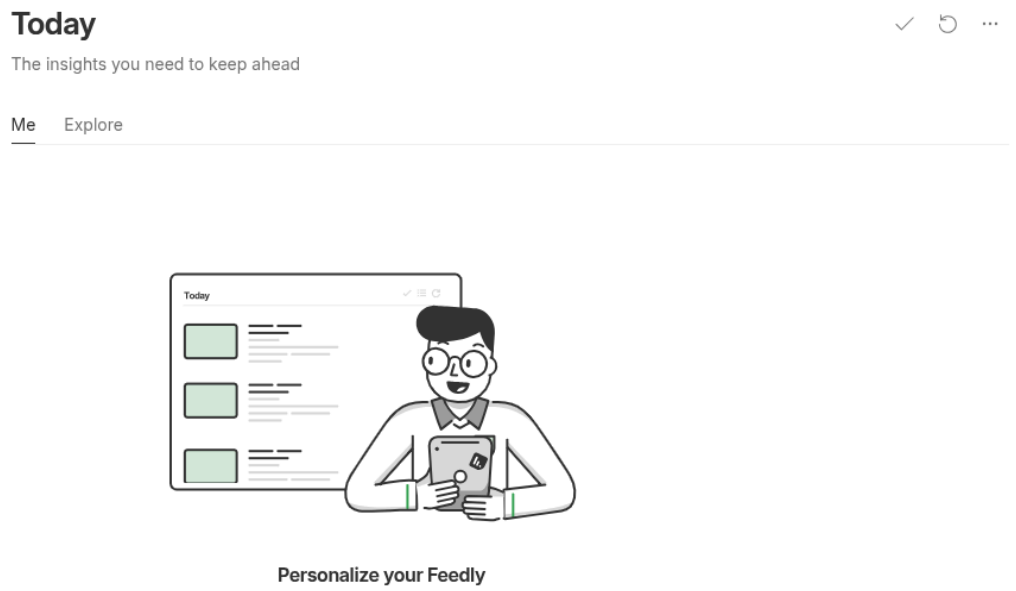
En résumé, dans un environnement numérique où le risque est omniprésent et dynamique, la veille informationnelle n'est pas un luxe, mais une nécessité stratégique pour assurer la résilience et la continuité des activités de toute organisation.
La cybersécurité actuelle est une course aux algorithmes où la maîtrise de l'IA est centrale.

Choix de la solution du dispositif de surveillance

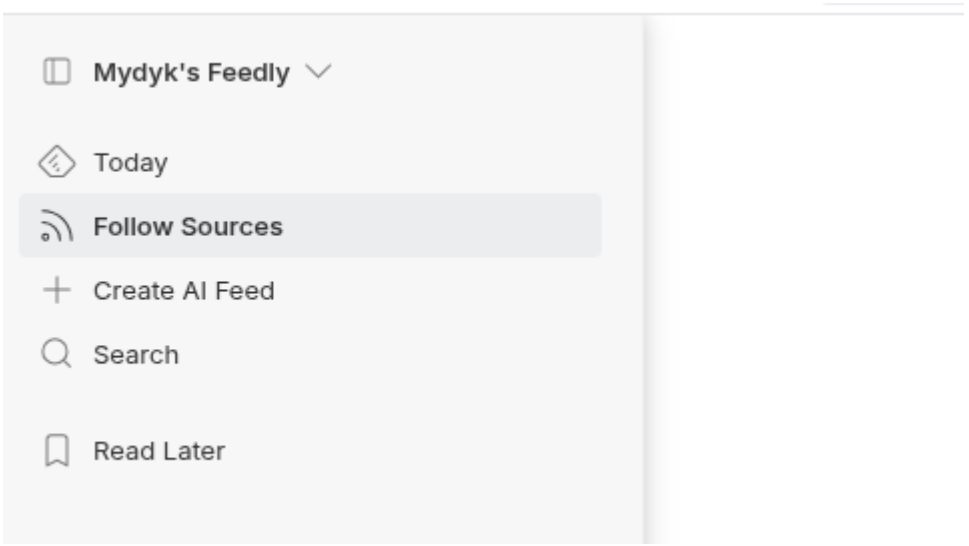
J'ai choisi Feedly comme solution de surveillance principale car il est privilégié pour sa capacité à gérer la veille technologique structurée sur un sujet complexe comme l'IA et la Cybersécurité. Il permet la centralisation et l'organisation des sources dans des tableaux de bord thématiques.
Ses fonctionnalités IA, notamment l'assistant "Leo", sont essentielles pour filtrer le bruit, prioriser les articles pertinents et identifier les signaux faibles et les tendances. De plus, son interface ergonomique et ses outils de partage facilitent la collaboration et permettent un gain de temps considérable, ce qui est indispensable face à la volumétrie d'information sur ce sujet dynamique.

Procédure de mise en place du dispositif de veille technologique

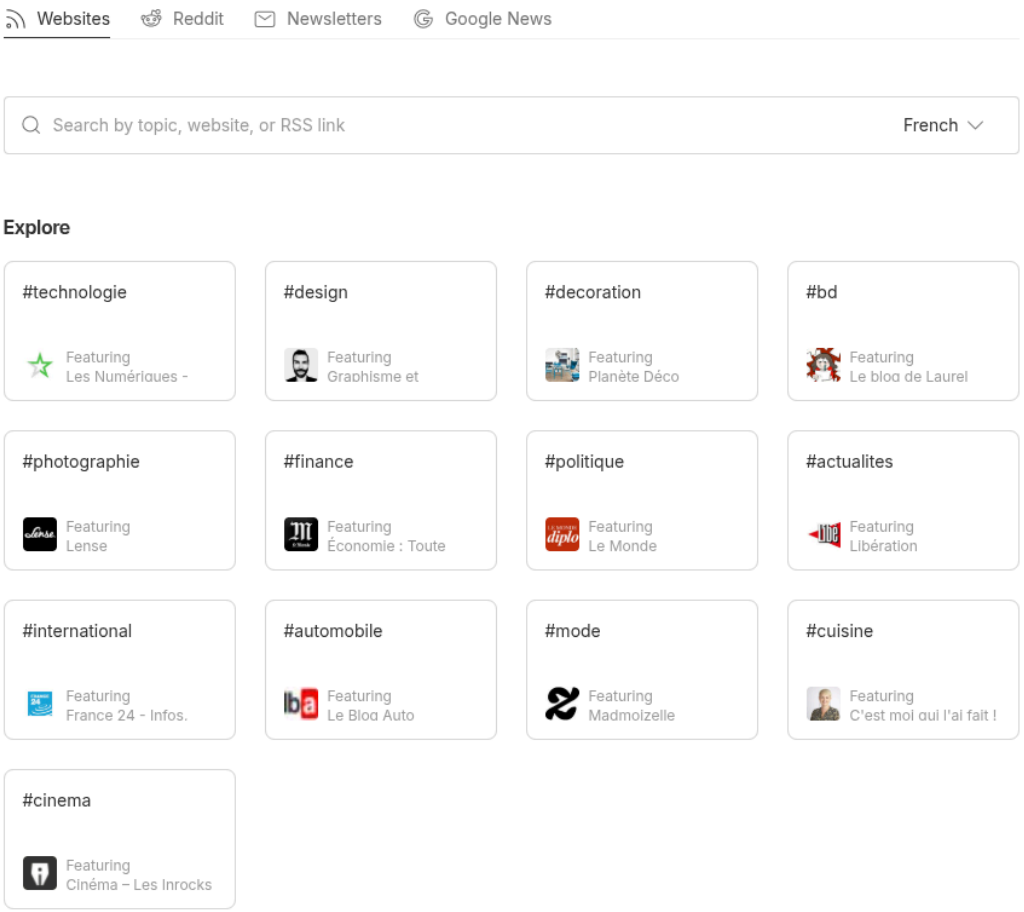
Une fois arrivé sur le site officiel de feedly via https://feedly.com/, le site va alors nous demander avant la création de notre dispositif, de créer un compte pour ensuite arriver sur cette fenêtre :



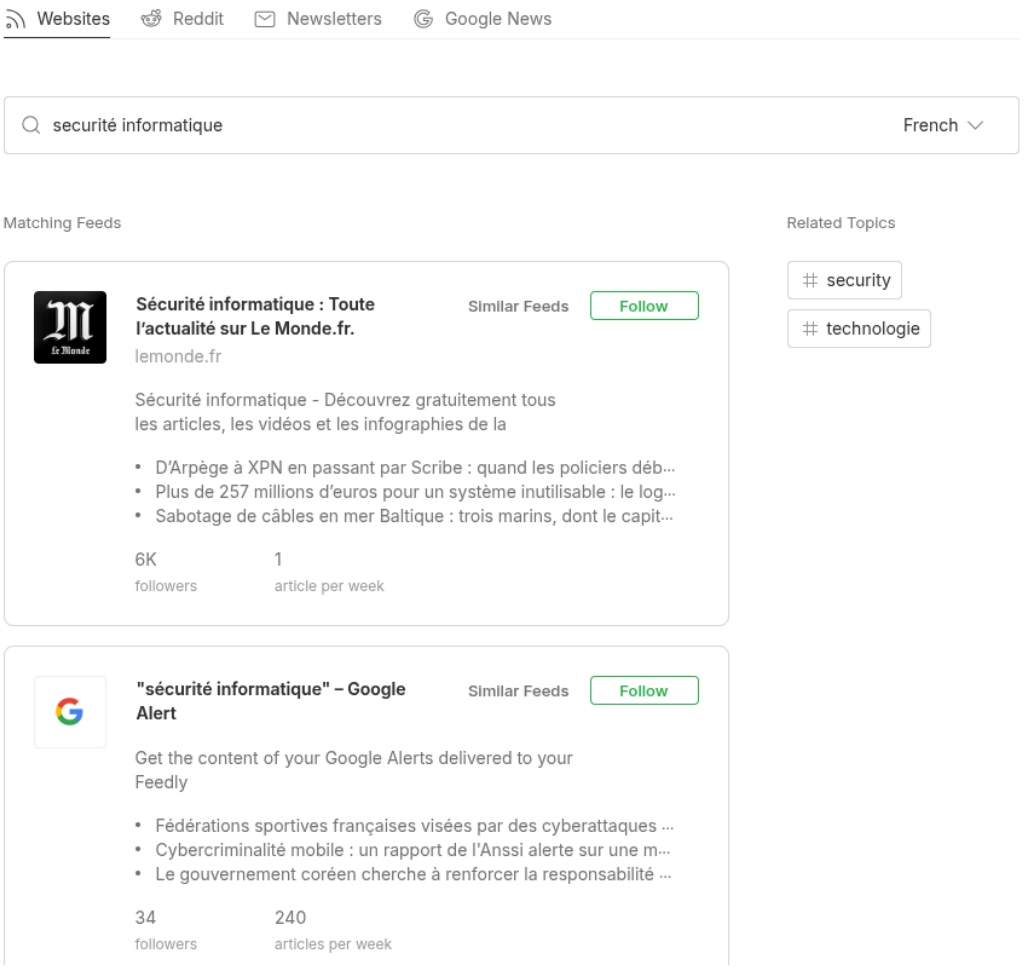
Dans la rubrique à gauche sur “ Follow Sources ”, on va ajouter l’ensemble des sources de notre tableau



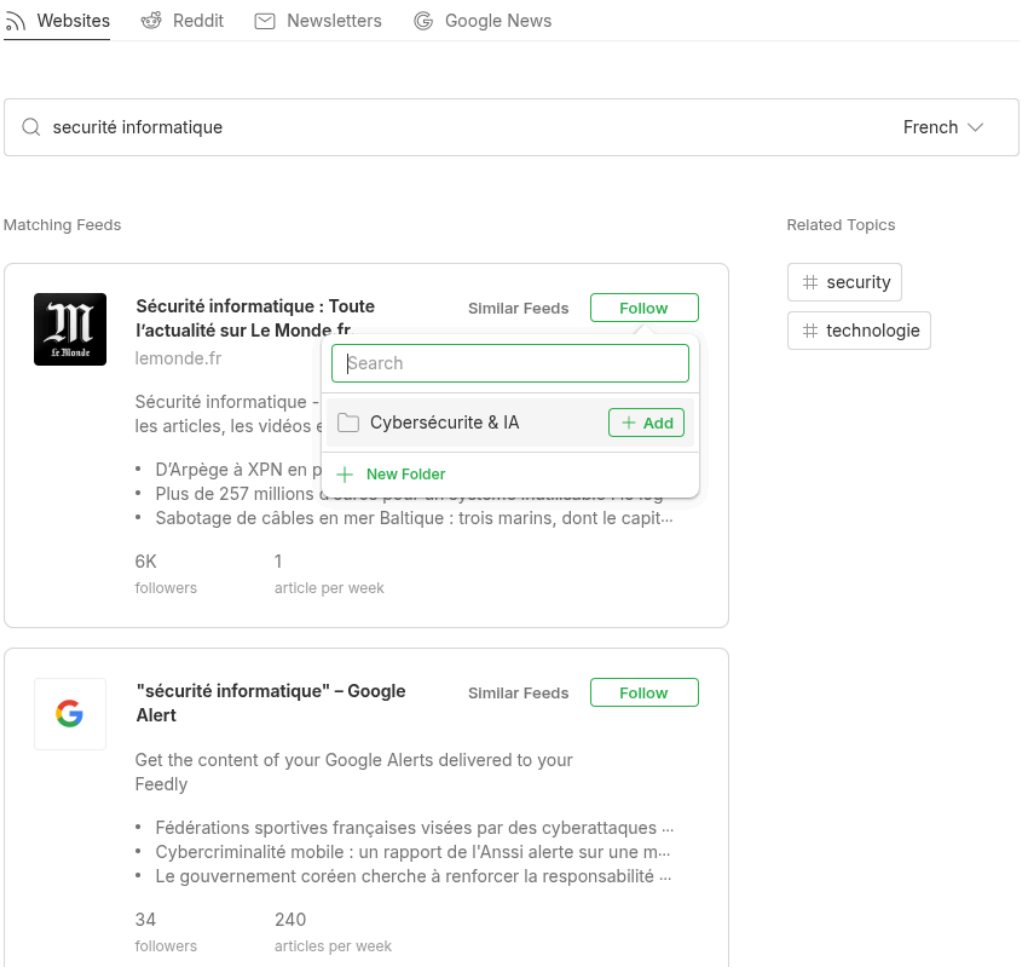
Une fois cliqué, vous êtes redirigé vers une nouvelle page ou vous pourrez alors renseigner le thème de vos veilles informationnelles via différentes méthodes (RSS, newsletter, alerte Google…) :



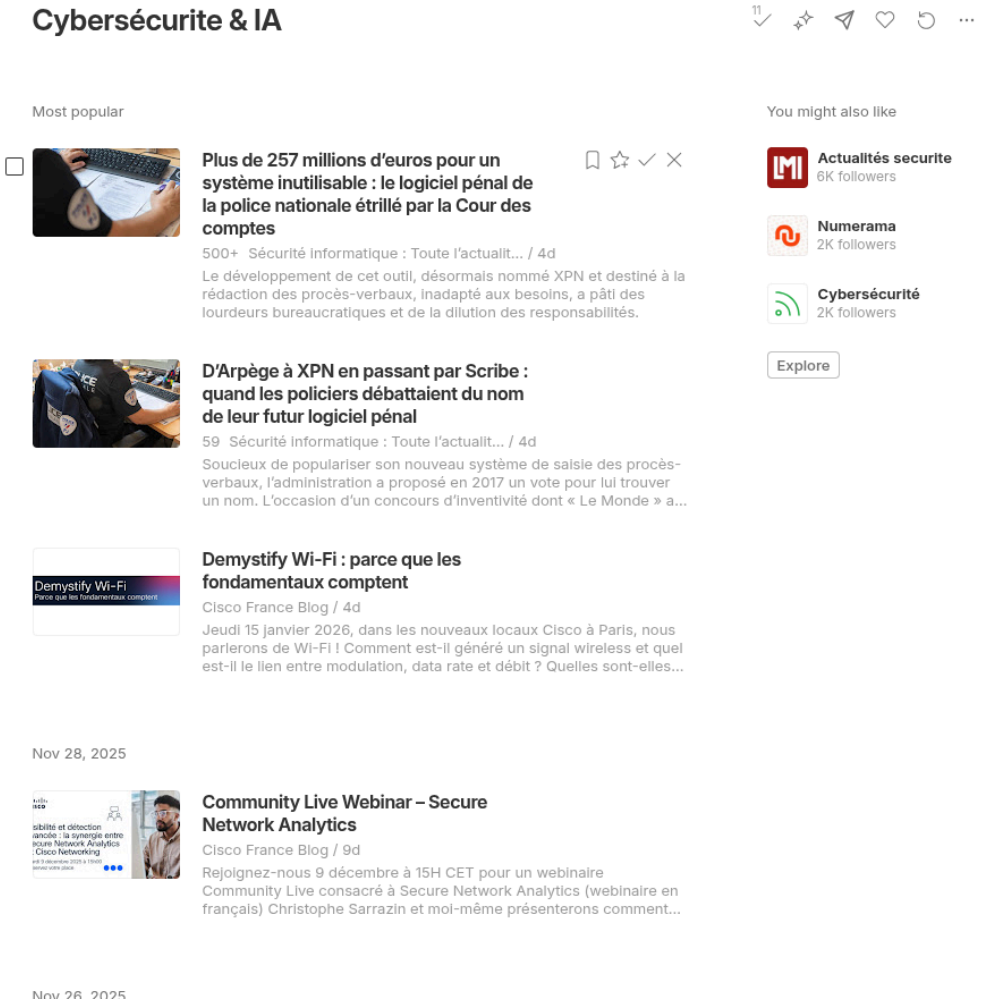
Par exemple, étant sur le thème de la cybersécurité, ainsi que sur le matériel informatique, on peut renseigner « sécurité informatique » pour arriver sur des blogs parlant de ce thème :



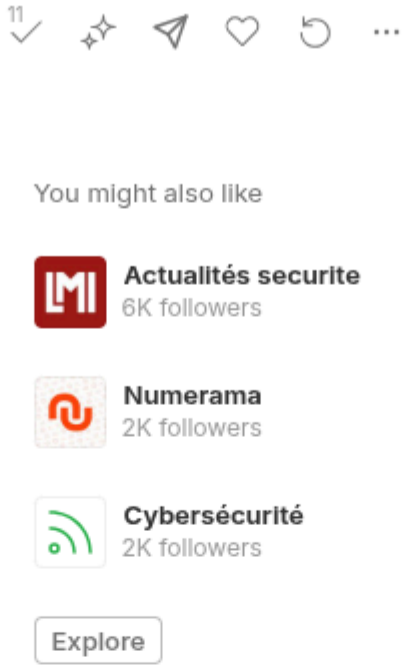
Il suffit plus que de sélectionner ce que l'on souhaite pour suivre ce contenu grâce au bouton *Follow* :



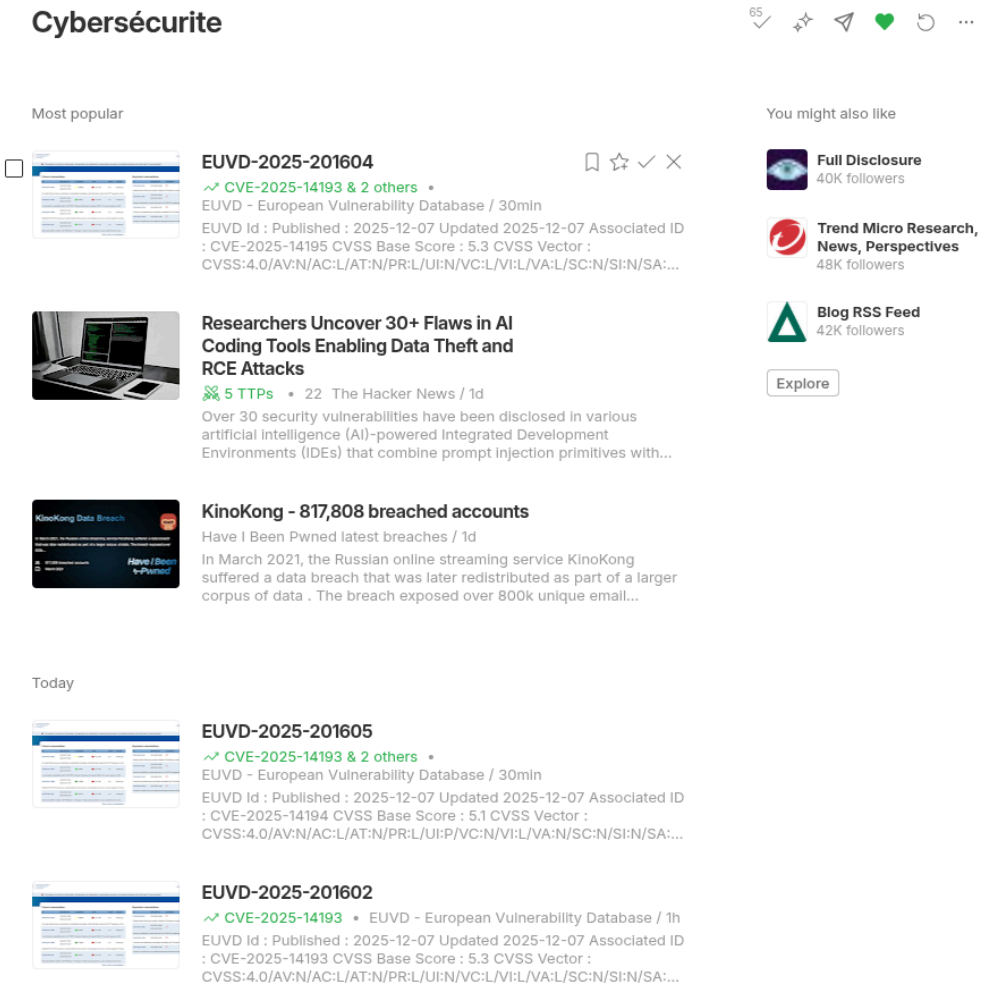
Créer un dossier avec New Folder cela permettra d'organiser plusieurs veilles informationnelles sur différents sujets. Une fois ceci fait, si on retourne dans notre dossier, on peut remarquer que l'on a plusieurs articles venant de ce site sur notre page d'accueil :



Nous avons aussi la possibilité d'ajouter de nouveau flux en lien avec notre thème à droite :



Il ne nous reste plus qu'à ajouter l'ensemble des sources que l'on souhaite pour avoir une veille bien complète et utilisable au quotidien pour rester informé sur les thèmes que l'on souhaite.
Feedly classe les articles pour vous informer sur le plus récent en utilisant principalement le tri chronologique par défaut, qui affiche les publications en fonction de leur date et heure. Pour garantir la pertinence, l'assistant IA Leo filtre et priorise le contenu, mettant en avant les sujets clés que vous suivez. Il est entraîné à masquer les doublons ou le bruit non pertinent. L'organisation en dossiers thématiques permet également de se concentrer sur l'actualité récente d'un domaine spécifique. En résumé, Feedly combine récence (chronologie) et pertinence (IA Leo) pour optimiser votre veille.
Ce qui donne ceci dans votre page d'accueil ou il suffira de cliquer sur l'article qui vous intéresse :



Bilan Technique de Mon Expérience de VeillePoints Forts Techniques (Bilan)

J'ai trouvé que la mise en place de ce dispositif de veille a été une réussite technique sur plusieurs aspects :

Aspect Technique	Description du Succès/Avantage
Centralisation des Sources (Feedly)	La plateforme Feedly m'a permis de consolider l'ensemble des flux d'information (RSS, sites spécialisés) dans un environnement unique, ce qui a considérablement évité la dispersion et optimisé mon temps de consultation.
Filtrage par IA (Leo Assistant)	L'intégration de l'assistant IA "Leo" est un atout majeur que j'ai beaucoup apprécié. Il a démontré sa capacité à réduire le "bruit informationnel", à prioriser les articles en fonction de mes thèmes de veille (Cybersécurité) et à identifier rapidement

	les tendances émergentes ou les vulnérabilités critiques.
Organisation Thématique	J'ai utilisé les "Folders" (Dossiers) dans Feedly pour structurer ma veille de manière logique (par exemple, un Dossier "Cybersécurité", un autre pour le "Matériel Informatique"), facilitant ainsi ma navigation et mon analyse ciblée.
Pertinence et Réactivité	Le dispositif m'a garanti une bonne réactivité face à l'actualité, assurant que les informations cruciales (nouvelles failles NVD, rapports ANSSI) me soient remontées en temps quasi réel grâce au tri chronologique et à la priorisation par Leo.
Accessibilité et Partage	L'interface ergonomique de Feedly et ses options de partage ont beaucoup simplifié la diffusion des informations pertinentes au sein de l'équipe ou pour la rédaction de mes synthèses.

Bien que l'expérience soit positive, je vois plusieurs pistes pour améliorer et faire évoluer techniquement mon système de veille :

Axe d'Amélioration	Proposition d'Évolution Technique	Objectif
Élargissement des Formats	J'aimerais intégrer des sources non-RSS : je pourrais configurer des alertes Google spécifiques pour les mots-clés très pointus ou ajouter des newsletters par e-mail dans un flux centralisé via un service tiers (si Feedly ne le gère pas nativement).	Mon objectif est de capturer des informations qui ne sont pas diffusées via des flux RSS traditionnels, notamment les analyses de fond ou les communications institutionnelles.

Automatisation des Alertes	Je pense configurer des **notifications personnalisées** basées sur des mots-clés hautement critiques (par exemple, "CVE-Année-Numéro", "Zero-Day", nom d'une technologie interne spécifique) pour recevoir une alerte immédiate en dehors de Feedly.	L'objectif est d'assurer la gestion des urgences et ma réactivité maximale face aux menaces critiques (priorisation de l'intervention).
Mesure de l'Efficacité (KPI)	Je devrai définir des indicateurs de performance (KPI) pour la veille : nombre d'articles critiques identifiés, temps moyen de réaction à une nouvelle vulnérabilité, taux de "bruit" filtré par Leo.	Je pourrai ainsi évaluer objectivement la qualité et l'efficacité de mon dispositif pour justifier les ressources que j'alloue à cette tâche.

Conclusion

En conclusion, la mise en place et l'optimisation de ce dispositif de veille technologique, axé sur la cybersécurité et s'appuyant sur des outils performants comme Feedly, s'est révélée être un succès majeur, transformant une contrainte d'apprentissage en un levier stratégique essentiel pour mon futur professionnel. En effet cela m'a appris d'acquérir de l'expérience mais aussi d'approfondir mes compétences :

- **Montée en compétences ciblée en Cybersécurité :** J'ai pu rester constamment informé sur les dernières failles, les nouvelles menaces (comme l'évolution des ransomwares) et l'actualité de la sécurité. Cela me permet de mieux comprendre ce qu'est une alerte NVD ou un rapport ENISA, enrichissant ainsi mon expertise métier pour le futur diplôme (BTS SIO option SISR).
- **Gestion efficace de l'information (et du temps) :** J'ai appris à trier et à prioriser les articles importants au milieu de la masse d'informations disponibles sur le web. Cela me rend plus efficace, me fait gagner du temps et me donne une méthode pour ne pas me laisser submerger par la surcharge informationnelle.
- **Développement de l'esprit critique :** Je m'entraîne régulièrement à évaluer la fiabilité des sources, à faire la différence entre une information sérieuse provenant d'une autorité reconnue et un simple article de blog ou une fausse alerte. C'est essentiel en sécurité pour prendre les bonnes décisions.
- **Amélioration de la réactivité et de la proactivité :** Cette veille m'a

sensibilisé à l'impératif de rapidité en sécurité. Je suis plus alerte et capable d'identifier une faille critique dès sa publication, ce qui est une compétence fondamentale pour anticiper les problèmes en tant qu'administrateur réseau.