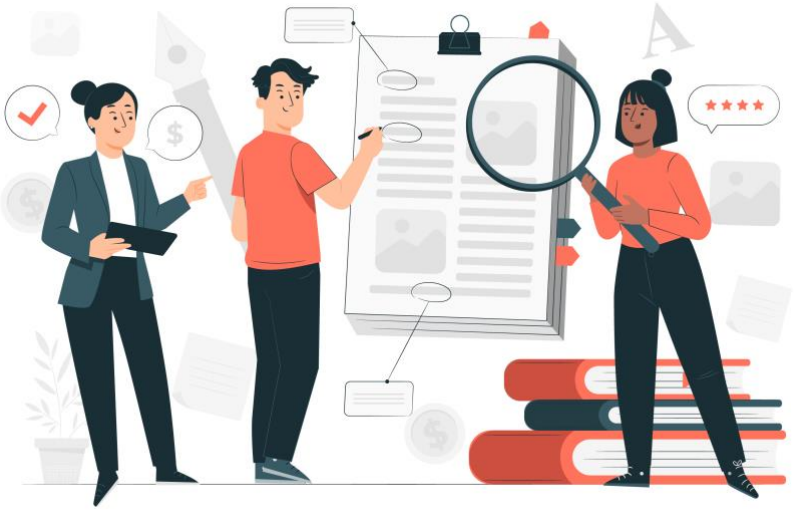
TD 2

LA VEILLE INFORMATIQUE



16 OCTOBRE 2025

WALID DJEGHIOUR

Étape 1

Grille de comparaison des outils :

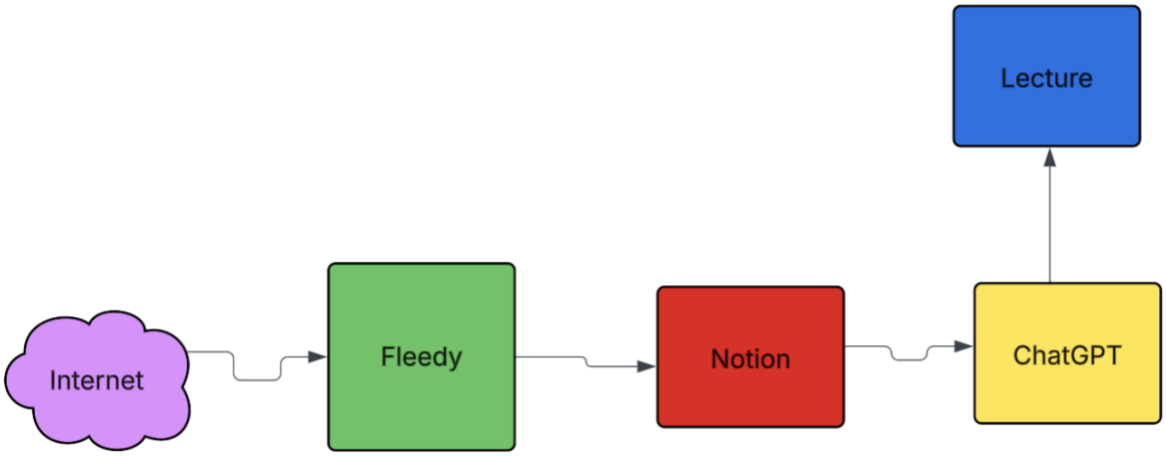
Outil	Type d'outil	Objectif principal	Points forts	Limites	Coût
Feedly	Agrégateur RSS	Collecter automatiquement des articles depuis plusieurs sources	Centralise les infos, IA Léo pour filtrer les contenus pertinents	Léo IA payant, peu d'automatisation gratuite	Gratuit / Payant
Inoreader	Agrégateur RSS	Collecte et classement des articles avec des filtres avancés	Très bon filtrage, compatible avec Notion et Zapier	Interface dense, certaines fonctions payantes	Gratuit / Payant
n8n	Outil d'automatisation	Connecte et automatiser plusieurs outils (Feedly, Notion, etc.)	Personnalisable, open source	Configuration complexe, nécessite du temps	Gratuit
Notion	Base de données / gestion de contenu	Classer et résumer les articles	Organisation claire, IA intégrée pour synthèse	Import manuel, dépend d'autres outils pour la collecte automatique	Gratuit / Payant
ChatGPT	Intelligence artificielle	Synthétiser et reformuler les articles	Résumés clairs, ajoute du contexte	Pas de collecte automatique	Gratuit / Payant
Make	Outil d'automatisation	Connecte et automatiser plusieurs outils (Feedly, Notion, etc.)	Très visuel, complet	Version gratuite limitée	Gratuit / Payant
Gemini	Intelligence artificielle	Résumer et analyser du contenu web	Bonne compréhension du texte, rapide	Moins personnalisable que ChatGPT	Gratuit / Payant

Étape 2

Outil choisi : Feedly :

J'ai choisi Feedly, un agrégateur de flux RSS qui centralise automatiquement les nouvelles publications de sites spécialisés (blogs, actualités, chaînes YouTube, etc.). C'est un outil simple à utiliser, très efficace pour organiser une veille informatique. Il permet de créer des catégories, d'ajouter des flux RSS et de marquer les articles intéressants pour les lire plus tard.

Schéma de ma veille informationnelle :



Mon schéma représente l'organisation de ma veille technologique à l'aide des outils Feedly, ChatGPT et Notion.

- Internet est la source principale d'informations (sites spécialisés, blogs, forums, actualités techniques…).

- Feedly centralise automatiquement ces informations grâce aux flux RSS que j'ai configurés (Cisco Security Blog, Docker, RDR-IT, Active Directory, etc.).

- ChatGPT m'aide à résumer et reformuler les articles importants afin d'en extraire les points essentiels et de mieux les comprendre

- Notion sert à classer et archiver les synthèses d'articles par thématique (Sécurité, Virtualisation, Réseaux…).

- Enfin, la partie **Lecture** correspond à ma consultation personnelle hebdomadaire où je relis les synthèses stockées dans Notion pour me tenir à jour.

Fréquence d'utilisation :

- Tous les 2 - 3 jours : consultation rapide des articles récupérée par Feedly .

Outils utilisés

- **Feedly** = collecte automatique des articles via flux RSS
- **Notion** = classement des articles par thématique
- **IA intégrée de Notion** = Résume
- **ChatGPT Pro =** Synthétise **+** reformulations

Démarche :

Je consulte Feedly pour voir les nouveaux articles dans mes thématiques de veille :

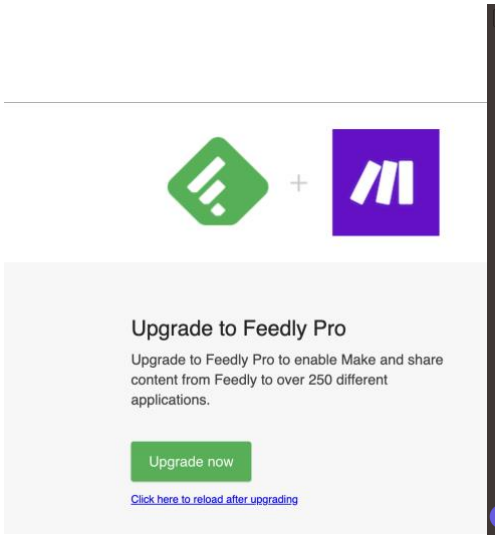
- Sécurisation des infrastructures
- Docker
- Active Directory
- Réseaux Cisco

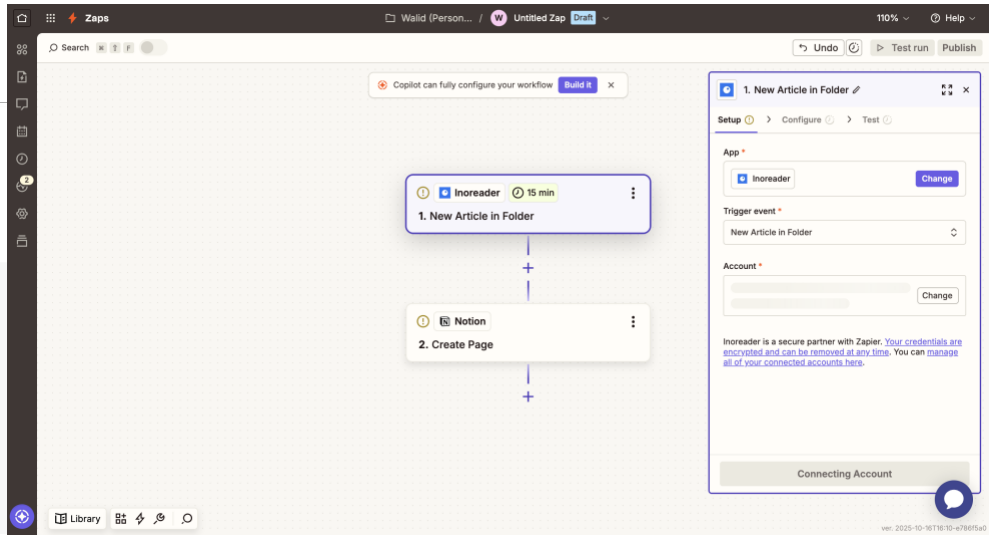
Lorsque Léo IA de Feedly me recommande un article, je le marque en "à lire plus tard".

- Je classe ensuite l'article dans la catégorie correspondante

Transfert vers Notion :

- Une fois l'article sélectionné, je le copie colle manuellement dans ma base Notion.
- Les outils d'automatisation tel que zappier ,n8n ou encore make sont payant.
- Nous pouvons le voir avec l'une des 2 images en dessous lorsque j'ai essayé de lier Feedly à Make





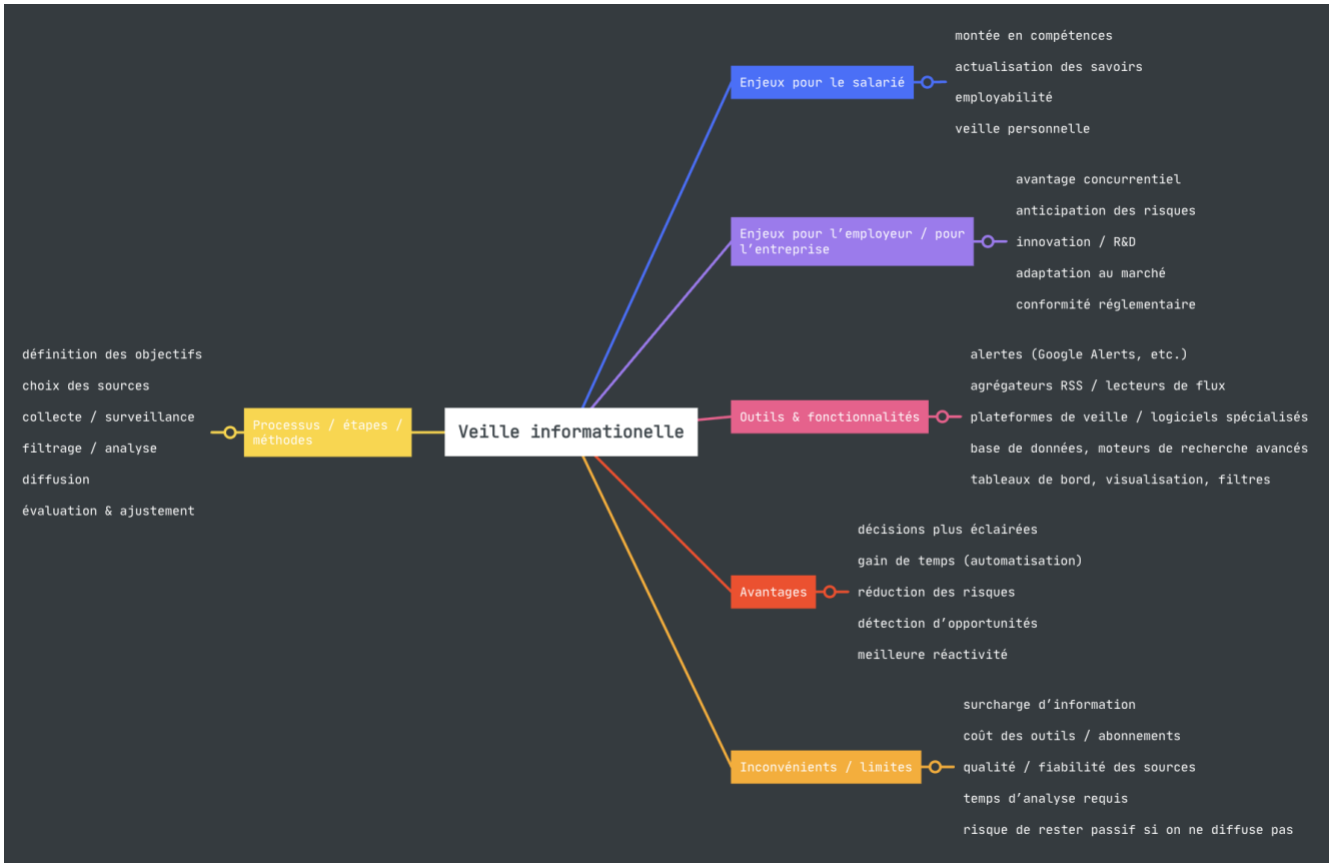
Synthèse et reformulation avec l'IA :

- Dans Notion j'utilise l'IA intégrée pour générer un résumé.
- Ensuite, j'envoie ce résumé à ChatGPT, qui reformule le texte, clarifie les passages techniques et peut ajouter des éléments de contexte (par exemple, des exemples d'application ou des définitions utiles).

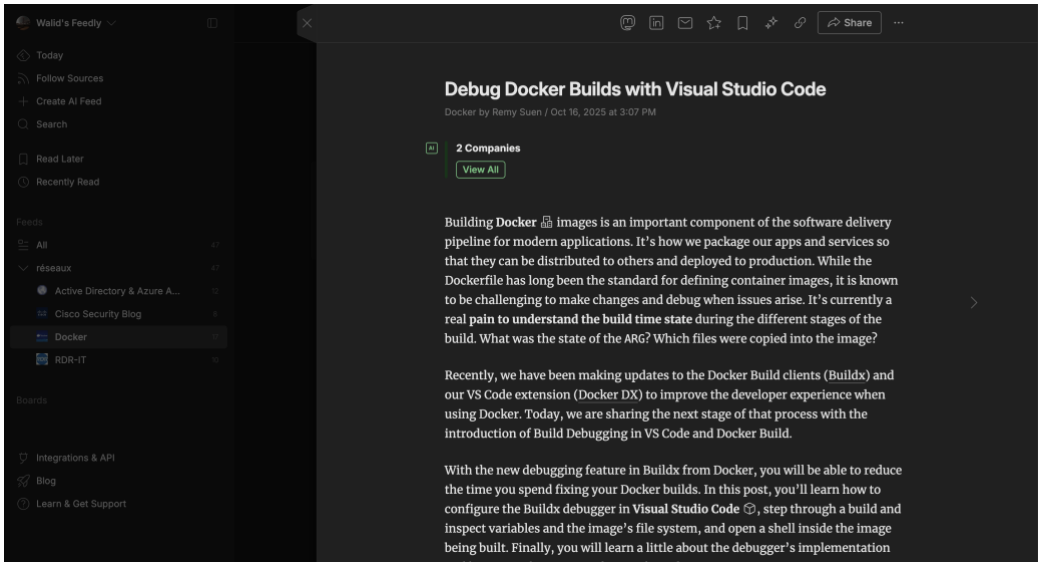
Lecture, enrichissement et archivage :

- Une fois par semaine, je relis les synthèses finales
- Si l'article est pertinent, je le classe dans son dossier correspondant (ex. Réseaux, Docker, AD).
- Lorsque l'article est obsolète ou peu intéressant, je le supprime afin de garder une veille claire, pertinente et à jour.
-

Schéma

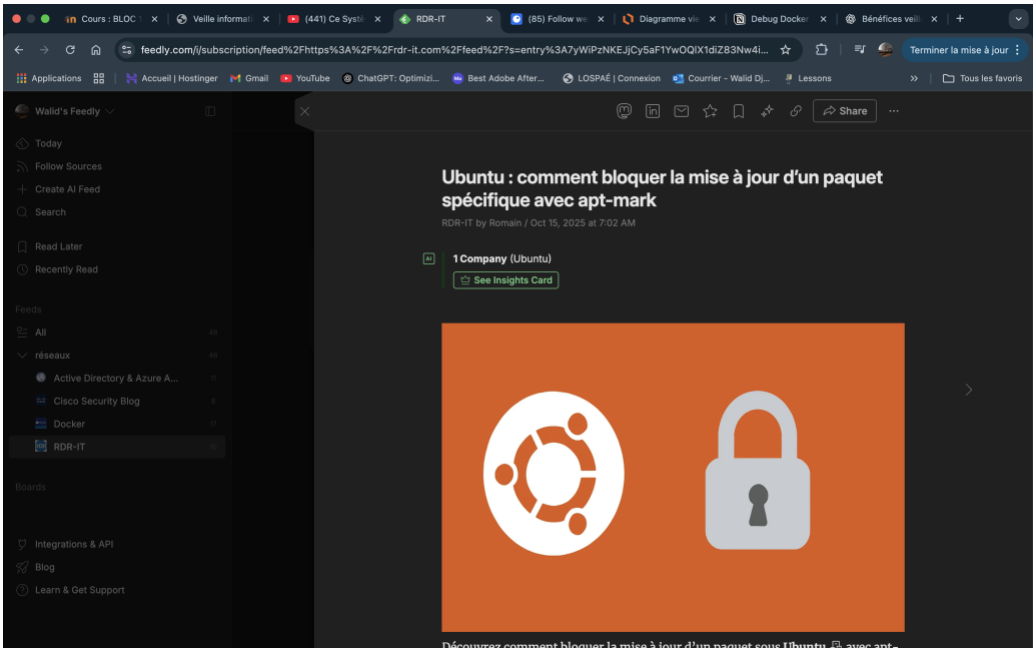


Virtualisation avec Docker :



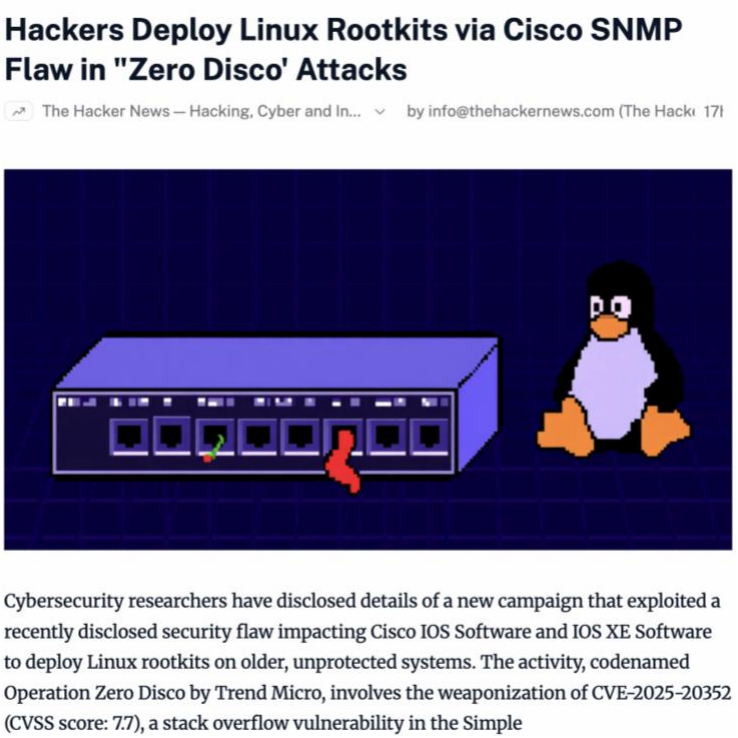
- Article: *Debug docker build whit visual studio code*

Réseaux RDR – IT :



- Article : Ubuntu : comment bloquer la mise à jour d'un paquet spécifique avec apt-mark

Réseaux Cisco security :



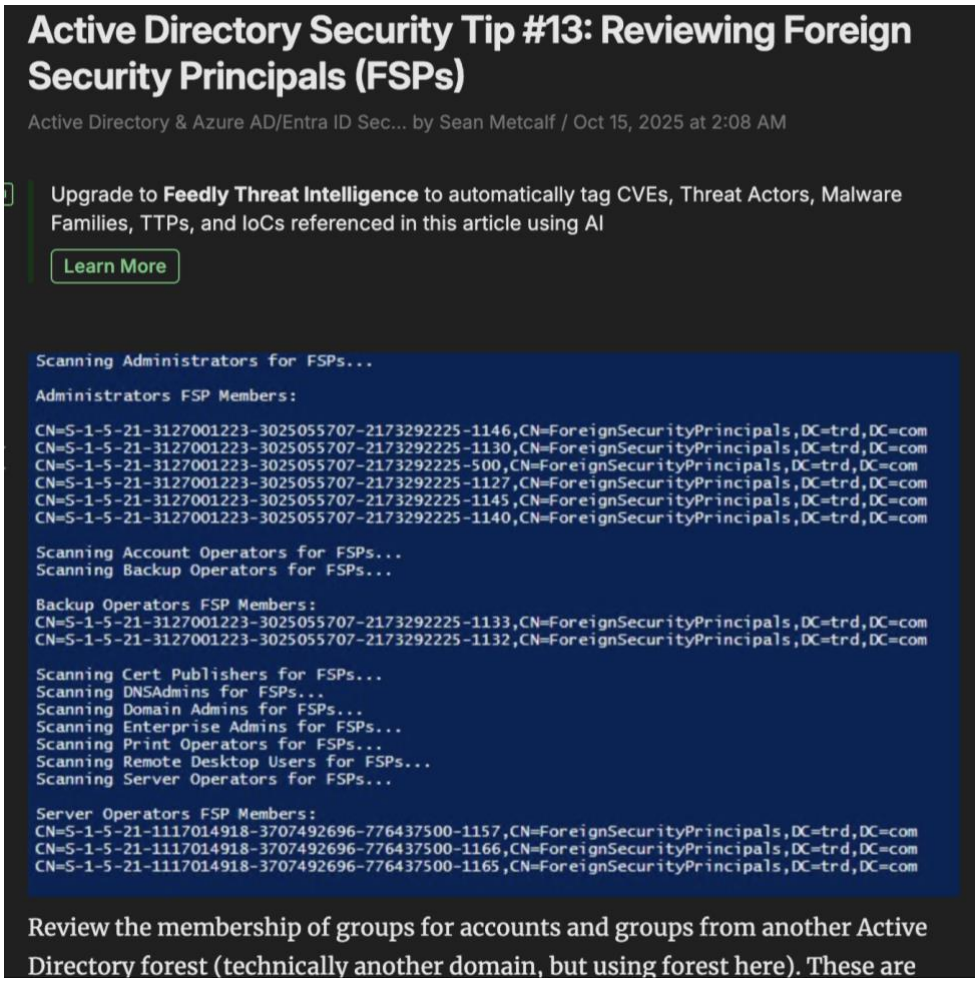
Hackers Deploy Linux Rootkits via Cisco SNMP Flaw in "Zero Disco' Attacks

The Hacker News — Hacking, Cyber and In... by info@thehackernews.com (The Hacki 17h

Cybersecurity researchers have disclosed details of a new campaign that exploited a recently disclosed security flaw impacting Cisco IOS Software and IOS XE Software to deploy Linux rootkits on older, unprotected systems. The activity, codenamed Operation Zero Disco by Trend Micro, involves the weaponization of CVE-2025-20352 (CVSS score: 7.7), a stack overflow vulnerability in the Simple

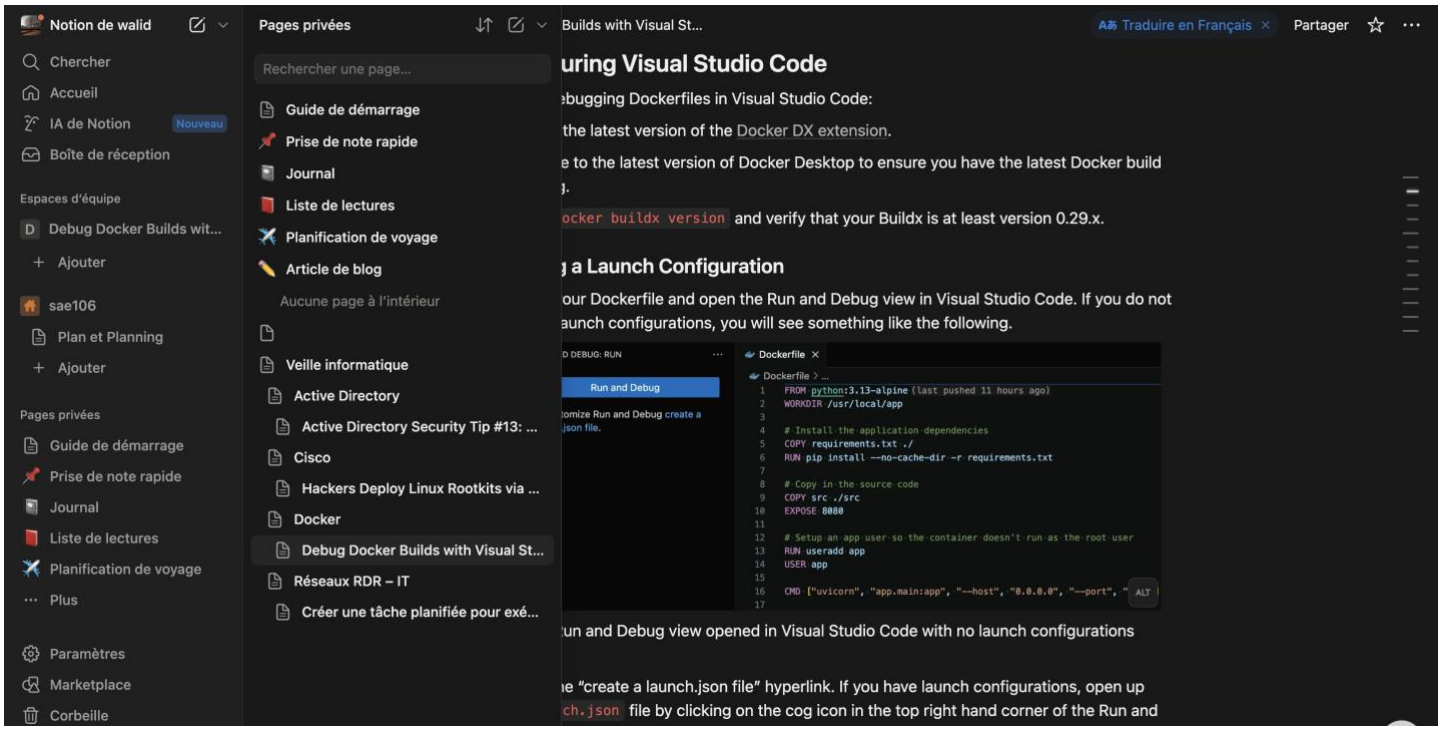
- Article : Hackers Deploy Linux Rootkits via Cisco SNMP Flaw in "Zero Disco' Attacks

Active Directory :



- Article : Active Directory Security Tip #13: Reviewing Foreign Security Principals (FSPs)

Organisation Notion :



- Mon espace Notion est organisé de manière claire afin de faciliter la gestion et le suivi de ma veille informatique**.**

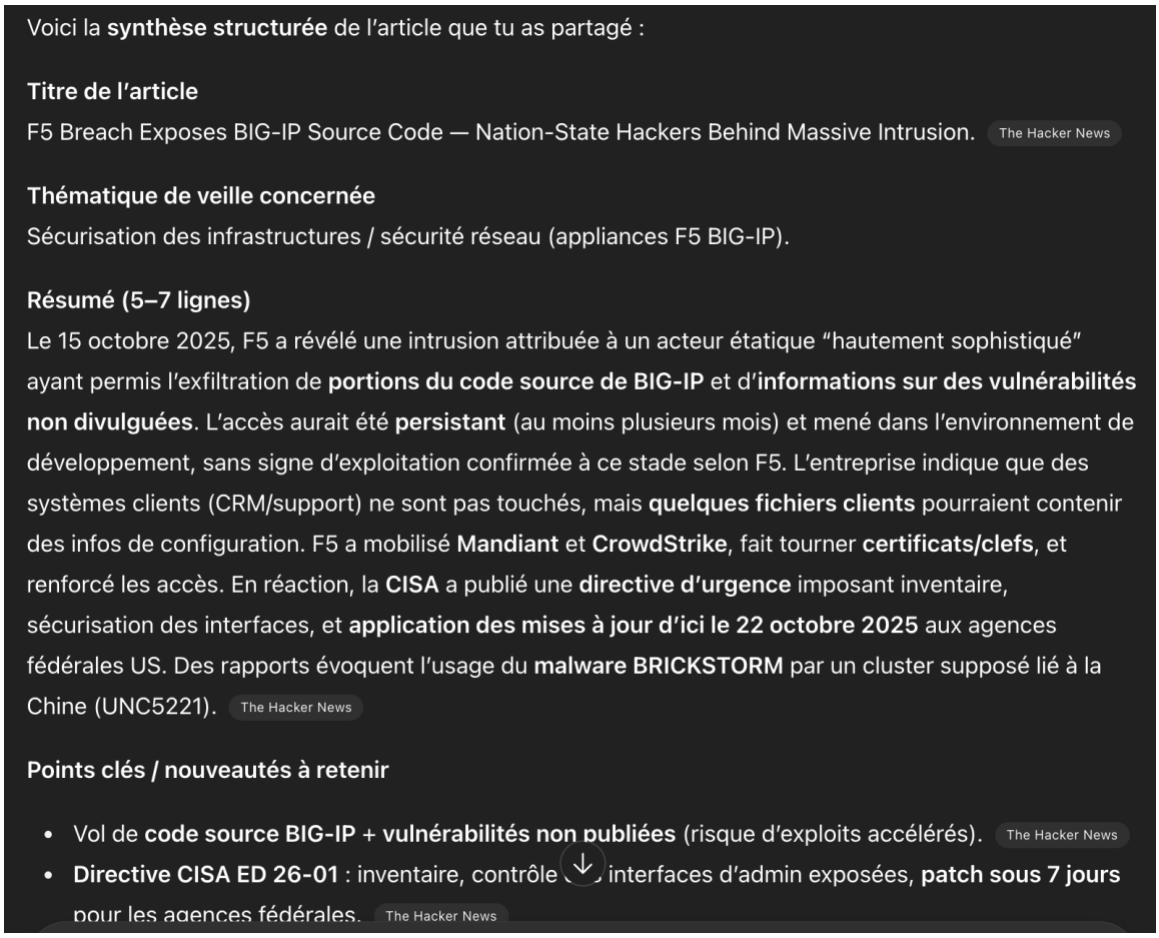
- Chaque dossier correspond à une thématique spécifique comme *Docker*, *Active Directory*, *Cisco* ou *Réseaux RDR – IT*.
  Les articles collectés depuis Feedly sont copiés et classés dans la section correspondante de Notion.
-

  Ensuite, j'utilise ChatGPT pour générer une synthèse complète et reformulée de chaque article, ce qui me permet d'en comprendre rapidement les points essentiels sans tout relire.

Voici un prompt type que je crée pour ChatGPT afin qu'il me synthétise un article :

Je suis étudiant en BTS SIO option SISR et je réalise une veille informatique sur plusieurs thématiques comme la cybersécurité, la virtualisation, les réseaux et les systèmes. Voici un article que j'ai trouvé via Feedly et que je souhaite synthétiser pour mon dossier de veille. Fais une synthèse claire et structurée de cet article en suivant ces points : Titre de l'article Thématique de veille concernée Résumé général de l'article en 5 à 7 lignes, avec les idées principales et les informations techniques importantes. Points clés ou nouveautés technologiques à retenir.

Résultat du prompt :



Voici la **synthèse structurée** de l'article que tu as partagé :

Titre de l'article

F5 Breach Exposes BIG-IP Source Code — Nation-State Hackers Behind Massive Intrusion. The Hacker News

Thématique de veille concernée

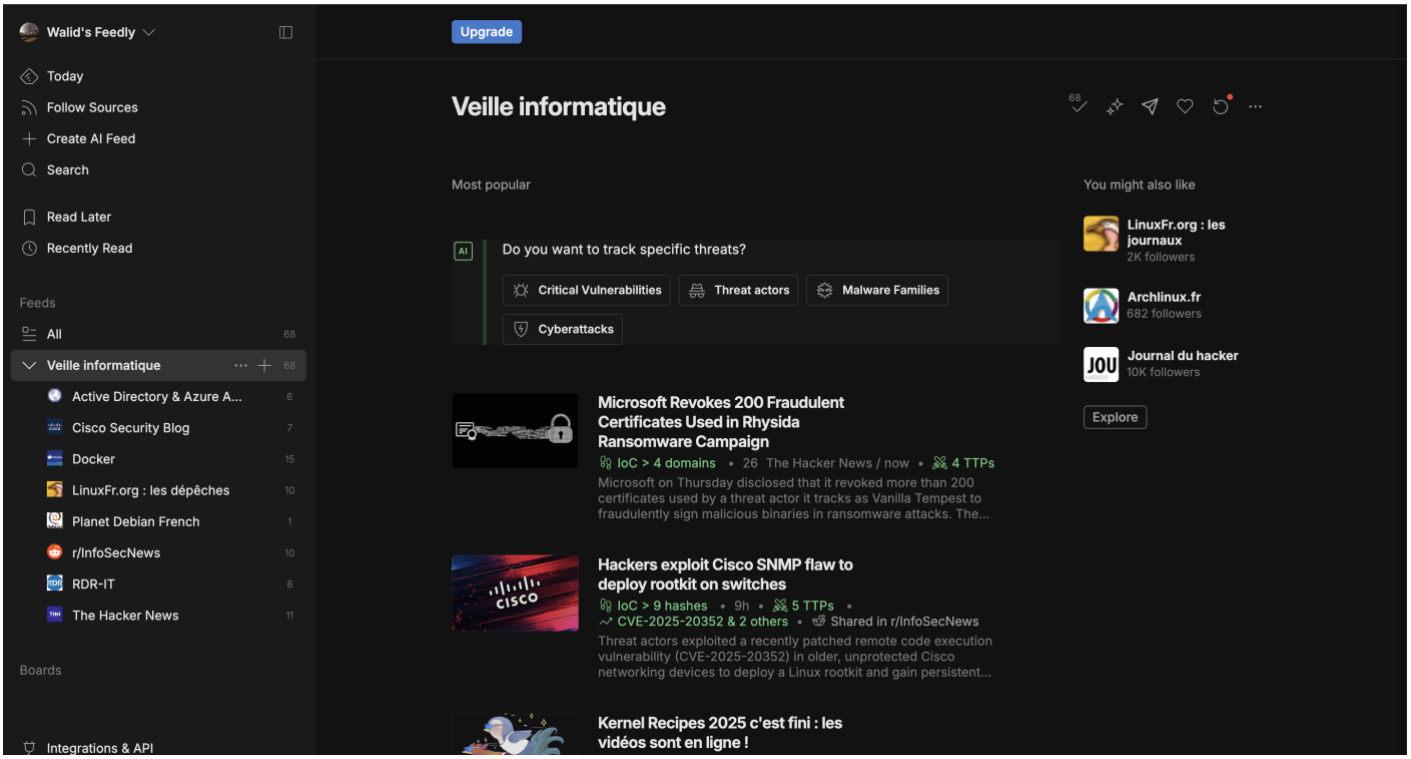
Sécurisation des infrastructures / sécurité réseau (appliances F5 BIG-IP).

Résumé (5–7 lignes)

Le 15 octobre 2025, F5 a révélé une intrusion attribuée à un acteur étatique "hautement sophistiqué" ayant permis l'exfiltration de **portions du code source de BIG-IP** et d'**informations sur des vulnérabilités non divulguées**. L'accès aurait été **persistant** (au moins plusieurs mois) et mené dans l'environnement de développement, sans signe d'exploitation confirmée à ce stade selon F5. L'entreprise indique que des systèmes clients (CRM/support) ne sont pas touchés, mais **quelques fichiers clients** pourraient contenir des infos de configuration. F5 a mobilisé **Mandiant** et **CrowdStrike**, fait tourner **certificats/clefs**, et renforcé les accès. En réaction, la **CISA** a publié une **directive d'urgence** imposant inventaire, sécurisation des interfaces, et **application des mises à jour d'ici le 22 octobre 2025** aux agences fédérales US. Des rapports évoquent l'usage du **malware BRICKSTORM** par un cluster supposé lié à la Chine (UNC5221). The Hacker News

Points clés / nouveautés à retenir

- Vol de **code source BIG-IP + vulnérabilités non publiées** (risque d'exploits accélérés). The Hacker News
- **Directive CISA ED 26-01** : inventaire, contrôle [illegible] interfaces d'admin exposées, **patch sous 7 jours** pour les agences fédérales. The Hacker News



Voici comment est organisé mon espace Feedly :