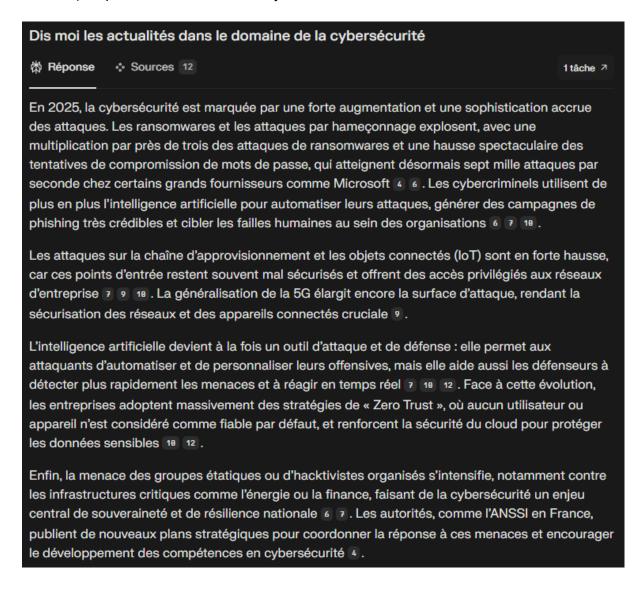
# Veille technologique - Cybersécurité & Nouvelles technologies

Pour ma veille, j'ai utilisé Perplexity AI, une IA connectée au web qui me résume l'actualité. Grâce à une automatisation sur mon téléphone, je reçois deux fois par semaine (lundi et vendredi) un point sur l'actualité de la cybersécurité.



voici un exemple de réponse que me renvoie perplexity, on peut voir que je peux consulter les sources utilisé pour produire cette réponse

# IA & Cybersécurité : une arme à double tranchant

Côté attaques :

Phishing amélioré par IA

- Création de malwares polymorphes
- Génération de deep fakes (voix, vidéos)

#### Côté défense :

- Détection de comportements anormaux
- Réponse automatisée aux incidents (ex : blocage IP)
- Systèmes adaptatifs qui apprennent des attaques passées

L'IA est aussi très utile pour analyser les logs et le trafic réseau en temps réel.

# Informatique quantique : un risque pour le chiffrement

Quand elle sera suffisamment puissante, l'informatique quantique pourra casser les systèmes de chiffrement actuels.

Cela menace:

- Les transactions bancaires
- Les certificats numériques
- Les communications sécurisées (TLS/SSL)

#### Les réponses aux menaces quantiques

Cryptographie post-quantique:

Des algorithmes conçus pour résister aux attaques quantiques :

- CRYSTALS-Kyber. C'est un algorithme de chiffrement post-quantique qui permet à deux parties d'échanger une clé secrète de façon sécurisée, Il repose sur des mathématiques complexes appelées réseaux euclidiens
- Classic McEliece. Cet algorithme se base sur des codes correcteurs d'erreurs, une technique mathématique éprouvée depuis des décennies. Même si ses clés publiques sont assez grandes, il offre une très bonne sécurité et une grande rapidité de déchiffrement

- Rainbow. C'est un algorithme de signature post-quantique basé sur des équations polynomiales multivariées, un domaine mathématique difficile à inverser, même pour un ordinateur quantique.il a finalement été écarté du processus de standardisation à cause de vulnérabilités découvertes, notamment des attaques permettant de récupérer la clé privée.
- SPHINCS+. C'est un algorithme de signature post-quantique basé sur des fonctions de hachage. Contrairement à d'autres algorithmes, il n'utilise pas de structures mathématiques complexes, ce qui le rend plus simple à analyser.

# Cryptographie quantique (QKD):

- Utilise les lois de la physique quantique pour sécuriser l'échange de clés de chiffrement. Son principe repose sur le fait que toute tentative d'interception modifie l'état des particules utilisées (comme des photons), ce qui rend toute attaque détectable.
- Le problème est que cette méthode reste coûteuse et difficile à déployer

### Conclusion

L'IA et l'informatique quantique sont en train de transformer la cybersécurité. Il est donc essentiel de suivre ces évolutions pour anticiper les menaces et adapter les méthodes de protection.