

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**.

Dis moi les actualités dans le domaine de la cybersécurité



Réponse



Sources 12

1 tâche ↗

En 2025, la cybersécurité est marquée par une forte augmentation et une sophistication accrue des attaques. Les ransomwares et les attaques par hameçonnage explosent, avec une multiplication par près de trois des attaques de ransomwares et une hausse spectaculaire des tentatives de compromission de mots de passe, qui atteignent désormais sept mille attaques par seconde chez certains grands fournisseurs comme Microsoft ^{4 6}. Les cybercriminels utilisent de plus en plus l'intelligence artificielle pour automatiser leurs attaques, générer des campagnes de phishing très crédibles et cibler les failles humaines au sein des organisations ^{6 7 18}.

Les attaques sur la chaîne d'approvisionnement et les objets connectés (IoT) sont en forte hausse, car ces points d'entrée restent souvent mal sécurisés et offrent des accès privilégiés aux réseaux d'entreprise ^{7 9 18}. La généralisation de la 5G élargit encore la surface d'attaque, rendant la sécurisation des réseaux et des appareils connectés cruciale ⁹.

L'intelligence artificielle devient à la fois un outil d'attaque et de défense : elle permet aux attaquants d'automatiser et de personnaliser leurs offensives, mais elle aide aussi les défenseurs à détecter plus rapidement les menaces et à réagir en temps réel ^{7 18 12}. Face à cette évolution, les entreprises adoptent massivement des stratégies de « Zero Trust », où aucun utilisateur ou appareil n'est considéré comme fiable par défaut, et renforcent la sécurité du cloud pour protéger les données sensibles ^{18 12}.

Enfin, la menace des groupes étatiques ou d'hacktivistes organisés s'intensifie, notamment contre les infrastructures critiques comme l'énergie ou la finance, faisant de la cybersécurité un enjeu central de souveraineté et de résilience nationale ^{6 7}. Les autorités, comme l'ANSSI en France, publient de nouveaux plans stratégiques pour coordonner la réponse à ces menaces et encourager le développement des compétences en cybersécurité ⁴.

voici un exemple de réponse me revoie 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 **deepfakes** (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
- Classic McEliece
- Rainbow
- SPHINCS+

Cryptographie quantique (QKD) :

- Utilise des **photons polarisés**
 - Détecte toute **interception**
 - Mais reste **coûteuse** et difficile à déployer
-

Conclusion

L'IA et l'informatique quantique **transforment la cybersécurité**.

Il est essentiel de suivre ces évolutions pour **anticiper les menaces** et adapter les **méthodes de protection**.