Veille Cybersécurité

Comprendre les menaces technologiques et les solutions de demain.

01

BTS SIO

Sommaire

Veille Cybersécurité — Avril 2026

01 Titre

02 Sommaire

03 Le Paysage Actuel

04 IA Offensive vs Défensive

05 Rançongiciels 2.0

06 La Fin des Mots de Passe ?

07 Le Facteur Humain

08 Citation

09 Copy Fail — CVE 2026

10 Bonnes Pratiques

11 Claude Security

12 Glossaire Technique

Le Paysage Actuel

Pourquoi la cybersécurité est devenue un enjeu critique

10,5 T$

coût annuel mondial
de la cybercriminalité (2025, Cybersecurity Ventures)

+15 %

d'événements de sécurité
en France en 2024 (ANSSI)

1 / 11 s

une nouvelle attaque
par rançongiciel dans le monde (2021, Cybersecurity Ventures)

L'Intelligence Artificielle

L'IA Offensive (Attaque)

- **Phishing parfait** : emails sans fautes, ton crédible, très personnalisé.
- **Malwares polymorphes** : changent de signature pour échapper aux antivirus.
- **Découverte de failles** (0-day) : une IA peut auditer un code et trouver une faille critique en **~1 heure**.

L'IA Défensive (Protection)

- **SIEM/EDR augmentés** : surveillance 24/7, anomalie détectée en millisecondes.
- **Audit de code par IA** : **Claude Security** scanne et propose le correctif.
- **Tri automatique des alertes** : l'analyste se concentre sur le réel.

Rançongiciels 2.0

Avant, un rançongiciel ne faisait qu'une chose : bloquer vos fichiers contre une rançon.

Aujourd'hui, c'est la Double Extorsion :

- **Ils volent** vos données confidentielles.
- **Ils chiffrent** (bloquent) vos ordinateurs.
- **Sans paiement,** vos secrets sont publiés sur internet.

Cas Marquants

- **CHSF Corbeil-Essonnes** (2022) — LockBit 3.0, rançon 10 M$ exigée, refus de payer, données médicales publiées.
- **Colonial Pipeline** (USA, 2021) — DarkSide, oléoduc à l'arrêt 6 jours, 4,4 M$ payés (75 BTC).
- **MGM Resorts** (2023) — ALPHV/Scattered Spider, 100 M$ de pertes, casinos paralysés 10 jours.
- **Change Healthcare** (USA, 2024) — ALPHV/BlackCat, 22 M$ payés, données de **190 M** de patients exposées.

La Fin des Mots de Passe ?

Le mot de passe a fait son temps : trop faible, trop souvent réutilisé, trop souvent volé. Place au **Passwordless**.

- **Biométrie :** FaceID, empreinte digitale. Votre visage ou votre doigt remplace le mot de passe.
- **Passkeys :** une clé cryptographique stockée sur votre téléphone, impossible à voler par phishing.
- **MFA (Double Sécurité) :** deux preuves d'identité au lieu d'une seule (mot de passe + code SMS, ou app authenticator).



Le Facteur Humain

L'Hameçonnage

Faux emails et SMS qui imitent vos banques, La Poste, les impôts pour voler vos mots de passe.

Ingénierie Sociale

Les pirates manipulent vos émotions : urgence, peur, autorité pour vous faire cliquer sans réfléchir.

La Vigilance

Vérifiez l'expéditeur. Doutez des urgences. Ne cliquez jamais sur un lien suspect.

"La cybersécurité n'est pas un produit que l'on achète, c'est un processus continu."

— Bruce Schneier (Expert en sécurité)

Copy Fail · Quand l'IA trouve les failles avant nous

CVE-2026-31431 · CRITIQUE

LE SCOOP

Une IA a trouvé la faille

· Xint Code = scanner IA de sécurité
· ≈ 1h de scan sur le noyau Linux
· PoC : 732 octets de Python
· Découverte le 23 mars 2026

LA FAILLE

LPE = élévation de privilèges

· User normal → root en 1 commande
· Bug AF_ALG (crypto kernel)
· Présent depuis 2017 — 9 ans non vu
· Toutes les distros Linux touchées

CONSÉQUENCES & DEMO

Contrôle total de la machine.

Voici l'attaque, en direct :

▶ **tinyurl.com/copyfaildemo**

« Une seule prompt opérateur, ≈ 1h de scan. L'IA défensive ouvre une nouvelle ère pour la cybersécurité. »

Les 3 Piliers de l'Hygiène Numérique

1. Sauvegarder

Copies régulières, hors ligne ou cloud chiffré. Règle 3-2-1.

- **Veeam / Acronis** — sauvegarde entreprise
- **Cloud** — OneDrive, Backblaze, Wasabi
- **NAS** — Synology, QNAP (local)

2. Mettre à Jour

Patches dès leur sortie. Automatiser et centraliser.

- **GPO Windows** — déploiement AD
- **WSUS / Intune** — gestion MAJ parc
- **Ansible / WinGet** — scripts d'auto

3. Vérifier

Activer la double authentification (MFA) partout où c'est possible.

- **Authenticator** — Microsoft / Google (TOTP)
- **YubiKey** — clé physique FIDO2 / U2F
- **Authy** — code à usage unique multi-appareils

Claude Security

L'IA défensive d'Anthropic — l'autre face de la médaille

PUBLIC BETA · 2026

LE PRODUIT

Claude Security par Anthropic

· Scanner de code propulsé par Claude Opus 4.7

· Lit le code comme un chercheur en sécurité

· Suit les flux de données entre fichiers/modules

· Trouve des vulnérabilités cachées depuis des années

· Génère le patch — du scan au correctif en 1 session

· Scans planifiés, export CSV/Markdown, webhooks Slack/Jira

LE PIVOT

Anthropic devient acteur cyber

· L'IA qui crée du code sécurise aussi le code

· Réponse directe aux failles type Copy Fail

· Partenaires : CrowdStrike, Palo Alto, Wiz, SentinelOne

· Project Glasswing : modèle Mythos pour infra critique

« AI compresses the timeline between vulnerability discovery and exploitation »

— Anthropic, mai 2026

Bilan : l'IA est l'épée à double tranchant de 2026 — elle trouve les failles plus vite, mais peut aussi les corriger plus vite.

Glossaire Technique

Le vocabulaire de la cybersécurité — version BTS SIO

CVE
Common Vulnerabilities and Exposures — identifiant standardisé d'une faille (ex : CVE-2026-31431).

CVSS
Score de gravité d'une vulnérabilité, de 0 à 10. Au-dessus de 7 = critique.

MFA
Multi-Factor Authentication. Deux preuves d'identité (mot de passe + code SMS / app).

Phishing
Hameçonnage. Email ou SMS frauduleux qui imite une marque pour voler des identifiants.

Ransomware
Rançongiciel. Logiciel qui chiffre les fichiers et exige une rançon pour les déchiffrer.

SAST
Static Application Security Testing. Analyse du code source à la recherche de vulnérabilités.

Prompt Injection
Attaque qui détourne une IA en injectant des instructions cachées dans le contexte qu'elle lit.

LPE
Local Privilege Escalation. Faille qui permet à un utilisateur d'obtenir les droits administrateur.

Zero-Day
Faille inconnue de l'éditeur et donc non corrigée. Exploitable jusqu'au correctif.

PoC
Proof of Concept. Code de démonstration qui prouve qu'une faille est exploitable.