SANS SÛRETÉ,
IL N'Y A PAS DE STRATÉGIE DURABLE.

BAROMÈTRE MENSUEL DE LA MENACE

OCTOBRE 2025 #1

SYNTHÈSE EXÉCUTIVE

Octobre 2025 marque une escalade majeure des menaces. Les attaques par ransomware progressent de 48% avec 801 incidents mondiaux. En France, une attaque par phishing paralyse 80% des lycées d'une région. Un commando organisé dérobe 88 millions d'euros en sept minutes au Musée du Louvre. L'Europe enregistre des hausses spectaculaires : +180% au Portugal, attribution formelle d'attaques du GRU russe. La supply chain mondiale est compromise : F5 Networks piraté, 23 millions de données de Vietnam Airlines exfiltrées. Dans 25% des incidents, les données sont volées en moins de cinq heures. Double tendance : professionnalisation de la criminalité (cyber et physique) et autonomisation des profils de menace.

RANSOMWARES	EUROPE	VECTEUR N°1	EXFILTRATION
+48%	**+180%**	**60%**	**<5h**
Progression annuelle	Portugal (6 mois)	Attaques via phishing	25% des incidents

Note méthodologique : *CRITIQUE = menace immédiate ou acteur étatique sophistiqué ; ÉLEVÉ = impact financier majeur ou tendance structurelle ; MOYEN = impact sectoriel spécifique.*

FAITS MAJEURS DU MOIS

France

CRITIQUE Paralysie de 80% des lycées des Hauts-de France par ransomware

10 octobre | Une attaque ransomware Qilin a paralysé 80% des lycées publics des Hauts-de-France. Vecteur d'intrusion : email de phishing ciblant les boîtes académiques. Impact : coupure complète des réseaux informatiques, interruption des cours dans plusieurs centaines d'établissements. Les groupes Qilin, Akira et Sinobi totalisent près de 40% des attaques ransomware mondiales en octobre.

→ **ENSEIGNEMENT :** Le phishing demeure le vecteur d'intrusion principal (60% des attaques). Les collectivités territoriales constituent des cibles prioritaires.

CRITIQUE Vol de 88 millions d'euros au musée du Louvre en sept minutes

19 octobre | Vol de huit joyaux de la Couronne par un commando organisé. Mode opératoire : nacelle sur un camion dérobé neuf jours auparavant, quatre individus masqués, exfiltration par scooters haute puissance. Bilan : quatre suspects mis en examen, objets non récupérés. Un prérapport de la Cour des comptes révèle que, dans le secteur concerné, un tiers des salles ne dispose d'aucune caméra de surveillance, malgré un budget de fonctionnement annuel de 323 millions d'euros.

→ **ENSEIGNEMENT :** Les retards dans la mise aux normes de sûreté constituent une vulnérabilité critique, même avec des budgets conséquents.

CRITIQUE Démantèlement d'un projet d'attentat impliquant trois femmes

10 octobre | Mise en examen de trois femmes âgées de 18, 19 et 21 ans pour projet d'attaque visant des terrasses de cafés et une salle de concert. Premier projet d'action violente impliquant des femmes depuis plusieurs années. Le procureur national antiterroriste confirme six projets déjoués depuis début 2025, avec un niveau d'alerte maintenu à “Urgence attentat“.

→ **ENSEIGNEMENT :** Évolution vers des profils jeunes (moins de 21 ans) à radicalisation rapide, sans liens directs avec des structures organisées.

EUROPE

CRITIQUE Attribution formelle au GRU russe d'attaques contre des organisations françaises

Avril 2025 (rappel contextuel) | L'ANSSI a officiellement attribué une série d'intrusions informatiques au GRU (renseignement militaire russe) via le groupe APT28/Fancy Bear. Ces opérations, actives depuis 2021, ont visé une dizaine d'organisations françaises incluant administrations publiques et entreprises privées. Entre janvier et mars 2025, la France a enregistré plus de 845 incidents ciblant prioritairement les secteurs de l'énergie, des télécommunications et des transports.

→ **ENSEIGNEMENT :** La menace étatique persiste avec des campagnes d'intrusion de longue durée visant les infrastructures critiques françaises.

ÉLEVÉ Explosion des cyberattaques en Europe : Portugal +180%, 384 attaques en Allemagne/UK/Italie

Octobre 2025 | Le Portugal enregistre 14 incidents majeurs sur six mois, soit une hausse de 180%, avec le groupe AKIRA comme menace principale. À l'échelle européenne, l'Allemagne (151 attaques), le Royaume-Uni (141) et l'Italie (92) concentrent 384 incidents par ransomware. L'ENISA confirme que l'administration publique demeure le secteur le plus touché (38,2% des attaques), tandis que les secteurs de la santé et de l'énergie connaissent la plus forte progression.

→ **ENSEIGNEMENT :** Intensification géographiquement généralisée. Les économies en transformation numérique accélérée sont particulièrement exposées.

MONDE

CRITIQUE Compromission d'un leader mondial de la cybersécurité

Mi-octobre | F5 Networks, géant américain de la cybersécurité, a révélé qu'un acteur étatique a maintenu un accès prolongé à ses systèmes, dérobant des portions du code source BIG-IP ainsi que des informations relatives à des vulnérabilités non divulguées. La compromission a entraîné une perte de capitalisation boursière de près de deux milliards de dollars en une semaine.

→ **ENSEIGNEMENT :** Les attaques par la chaîne d'approvisionnement (supply chain) exposent simultanément l'ensemble de l'écosystème client.

MOYEN Fuite de 23 millions d'enregistrements clients de Vietnam Airlines

14 octobre | Vietnam Airlines a notifié à ses clients qu'une intrusion sur une plateforme tierce a conduit à l'exfiltration de 23 millions d'enregistrements couvrant la période de novembre 2020 à juin 2025. Les données compromises incluent informations personnelles, coordonnées et historiques de vol. L'incident s'inscrit dans une série d'attaques visant le secteur aérien, notamment Oracle E-Business Suite dont l'exploitation d'une vulnérabilité zero-day a touché plusieurs compagnies et universités.

→ **ENSEIGNEMENT :** Le secteur du transport aérien fait face à une recrudescence d'attaques. La dépendance aux plateformes tierces constitue un maillon faible.

ACTIONS PRIORITAIRES

- **Renforcer la formation anti-phishing :** 60% des intrusions débutent par un email compromis. Déployer des campagnes de simulation régulières auprès de l'ensemble des collaborateurs.
- **Auditer la chaîne de sous-traitance critique :** Cartographier l'ensemble des prestataires ayant accès aux systèmes d'information. Vérifier leurs certifications de sécurité et exiger des garanties contractuelles.
- **Tester le dispositif de réponse à incident :** dans 25% des incidents, l'exfiltration des données s'effectue en moins de cinq heures. Organiser des exercices de crise validant les procédures d'escalade et les contacts d'urgence.
- **Réviser les investissements sécuritaires :** s'assurer que les budgets alloués se traduisent par des capacités opérationnelles déployées. Privilégier une approche par les risques.