# Focus Cybersécurité | octobre 2025

Yannick Pech

## Entre fuites massives, dépendances systémiques, vulnérabilités critiques et quête de maturité cyber

Dans le sillage du mois précédent, celui d'octobre 2025 s'avère être funestement normal dans le panorama de la cybersécurité : multiplication des failles logicielles critiques, fuites de données sensibles touchant France Travail ou la région Hauts-de-France, panne proto-systémique d'Amazon Web Services (AWS) et publication d'un rapport mondial de Keeper Security mettant en lumière le fossé entre les discours et leur application concrète. Dans ce contexte, la perspective du Forum InCyber 2026 rappelle que la résilience et la confiance numériques devront être au cœur de la coopération européenne.

### *Vulnérabilités et alertes : une pression constante sur les défenses*

Les bulletins d'alerte du **CERT-FR (ANSSI)** confirment la fragilité croissante des environnements numériques. Les failles découvertes ce mois-ci — dans les technologies de serveurs web **Apache Tomcat**, **Xen**, et **WSUS** (Windows), ou la solution française VPN **TheGreenBow** — sont exploitées quasi immédiatement y compris après publication des correctifs par ailleurs parfois encore incomplets, comme pour Windows Server Update Service (WSUS).

La chaîne d'exploitation s'accélère : des outils d'IA sont systématiquement utilisés pour scanner automatiquement les infrastructures non mises à jour, tandis que les campagnes de phishing ciblées exploitent les annonces de vulnérabilités pour tromper les administrateurs. La **défense en profondeur** (DiD) repose en effet toujours plus sur des **boucles de correction continues**, des **alertes comportementales en temps réel**, et une **hygiène numérique collective** intégrant fournisseurs et prestataires.

**Une tendance se fait jour :** le modèle de sécurité périmétrique s'efface au profit d'une logique de **cyber-résilience intégrée** où anticipation, automatisation, et coordination entre parties prenantes deviennent incontournables.

### *France Travail : une fuite de données à l'échelle nationale*

L'attaque contre **France Travail** — et son prestataire **Cap emploi** — illustre la vulnérabilité des systèmes publics interconnectés. Dévoilée début octobre et faisant suite à au moins deux précédentes atteintes, elle a conduit à l'**exfiltration de données personnelles** portant sur plusieurs dizaines de millions d'usagers : noms, prénoms, adresses, identifiants, numéros de sécurité sociale, coordonnées téléphoniques et électroniques. Les **mots de passe et informations bancaires** ne seraient pas compromis, selon les premiers constats officiels.

La **CNIL** évoque jusqu'à **43 millions de profils concernés**, soit la quasi-totalité des demandeurs d'emploi recensés sur vingt ans. L'origine probable : un **compte d'agent usurpé** chez Cap emploi, dépourvu d'authentification multi-facteurs. Cette compromission souligne le risque majeur lié aux **droits hérités** et aux **chaînes de sous-traitance** dans les systèmes d'information publics.

Au-delà des impacts techniques, cette crise interroge la **gouvernance de la donnée publique** et la **transparence institutionnelle** : notification à la CNIL, accompagnement des usagers, et prévention contre les campagnes de phishing ciblées.

**Enjeu central :** reconstruire la confiance dans les services publics numériques en imposant une politique d'accès fondée sur le **principe du moindre privilège**, le **chiffrement** systématique, l'imposition de **l'authentification forte** (multifacteurs d'authentification — MFA) et le **suivi des anomalies** en continu.

### *Lycées des Hauts-de-France : l'Éducation nationale dans le collimateur*

Le 17 octobre, la région **Hauts-de-France** a été frappée par une **attaque informatique paralysant plus de 250 lycées**. Le réseau interne de gestion a été rendu inaccessible, forçant la mise hors ligne des serveurs régionaux pendant plusieurs jours.
Cette attaque — d'origine encore non formellement identifiée — aurait mobilisé un **rançongiciel** ciblant les serveurs d'authentification et les espaces partagés.

La région a activé son **plan de continuité numérique** et suspendu temporairement certains services cloud externes, avec l'appui de l'**ANSSI** et du **C3N** (Centre de lutte contre les criminalités numériques de la gendarmerie nationale).

Cet incident souligne la fragilité des infrastructures éducatives, souvent sous-équipées au regard des exigences de sécurité, et rappelle que la **cybersécurité territoriale** constitue un enjeu de service public essentiel.

### *La panne d'AWS soulève — encore — la question de la dépendance technologique et de la souveraineté numérique des Européens*

Mi-octobre, une **panne mondiale** d'Amazon Web Services (**AWS**) a provoqué la coupure ou la dégradation temporaire de centaines de services numériques — sites médias, solutions SaaS (*Software as a Service*), plateformes institutionnelles et services cloud publics. Si la situation a été rétablie en moins d'une journée, l'incident a exposé la **dépendance critique de l'Europe** à un nombre limité de fournisseurs américains.

Cette dépendance touche la France en plein cœur : nombre de services publics ou d'entreprises stratégiques reposent sur des **infrastructures cloud hors de tout contrôle souverain**, où les données, leurs confidentialité et disponibilité sont **soumises à des juridictions extra-européennes**, notamment américaines.

Les initiatives comme **Gaia-X**, **SecNumCloud** ou **IRIS²** tentent de bâtir un socle européen de confiance, mais leur adoption reste limitée face à la puissance économique et technologique des *hyperscalers*. La panne d'AWS illustre aussi la faiblesse des stratégies multi-cloud : beaucoup d'organisations restent *de facto* mono-dépendantes à des entreprises étrangères oligopolistiques et souvent de même nationalité. Pourtant, de nombreux acteurs français (CleverCloud, Scaleway, Outscale, OVH…) ou européens pourraient constituer des alternatives sérieuses.

**Enjeu majeur :** sans maîtrise de ses infrastructures, l'Europe reste exposée à un **risque de dépendance systémique**. **La souveraineté numérique** ne peut se résumer à une réglementation ; elle **doit s'incarner** d'une part, dans **des choix politiques** volontaristes et, d'autre part, des **capacités industrielles et technologiques**.

### *Keeper Security livre un rapport édifiant sur la quête de maturité cyber*

Le **rapport mondial 2025** intitulé « *Global Cybersecurity Insights* » et publié le 30 octobre 2025 par **Keeper Security** met en évidence un **écart préoccupant** entre **les ambitions affichées** et **leur mise en œuvre opérationnelle** dans les organisations. Malgré l'adoption généralisée de cadres comme le **Zero Trust** (modèle basé sur la méfiance par défaut à l'endroit de tout utilisateur interne ou externe à un réseau informatique) ou la **gestion des accès privilégiés (PAM)**, près de **40 % des entreprises** reconnaissent ne pas appliquer de dispositifs **d'authentification forte** (MFA) **de manière systématique** sur leurs comptes administrateurs.

Les freins identifiés sont les suivants :

- manque de ressources humaines qualifiées ;
- complexité des environnements hybrides (cloud + *on-premise*) ;
- priorités concurrentes et dette technique accumulée ;
- sous-évaluation du risque lié aux identités numériques.

Keeper Security souligne que **l'identité et son authentification devient le pivot central de la cybersécurité actuelle** :

« *La protection des identités et des privilèges n'est plus une option, c'est l'ossature même de la résilience numérique*. »

Le rapport appelle à une **discipline opérationnelle accrue** : mise en œuvre mesurable, supervision en temps réel, audit continu et intégration de l'IA défensive dans la détection des anomalies.

**Constat global :** la maturité cyber ne se décrète pas ; elle s'évalue sur la base d'indicateurs concrets, d'un niveau de culture de sécurité et de pratiques éprouvées.

## *Tendances : l'IA offensive et la complexité croissante du risque*

- **IA malveillantes** : des modèles génératifs servent désormais à créer des campagnes de phishing hyper-personnalisées, à imiter des voix ou à forger des contenus de désinformation crédibles.
- **Attaques hybrides** : les groupes cybercriminels combinent désormais intrusions techniques, manœuvres d'ingénierie sociale et campagnes d'influence.
- **NIS2 et souveraineté** : la transposition de la directive européenne impose une professionnalisation rapide des fonctions de cybersécurité dans les entreprises, notamment pour la gestion de crise et le *reporting*.
- **Cybersécurité de proximité** : soutenus par l'ANSSI, les **CSIRT régionaux** développent leurs activités pour accompagner les PME et collectivités locales dans la détection et la réponse. Ils mutualisent toujours plus leur travail avec celui des CSIRT privés d'entreprises (Airbus, Thales, Capgemini…)
- **Risque de saturation** : sans accompagnement adapté, la multiplication des obligations réglementaires risque d'épuiser les petites structures — nécessitant des outils mutualisés et des offres de services partagées.

## *Perspective : vers un modèle européen de confiance numérique ?*

L'année 2026 s'annonce charnière pour la cybersécurité européenne. Le **Forum InCyber Europe 2026**, prévu du **17 au 19 mars à Lille Grand Palais**, aura pour thème :

« *De la résilience à la confiance : l'Europe face au choc cyber.* »

Cette édition mettra l'accent sur :

- l'**interopérabilité entre CERT** (*Computer Emergency Response Team*) **nationaux et régionaux** ;
- la **sécurité de l'IA et des modèles génératifs** ;
- la **normalisation des indicateurs de confiance** (labels, certifications, audits croisés).

En toile de fond, l'objectif est clair : **construire une cyber-gouvernance européenne** où la transparence, la vérification et la coopération remplacent la méfiance et l'isolement.

## En résumé

1. **Alerte continue :** les vulnérabilités s'enchaînent et se propagent plus vite qu'elles ne se corrigent ; la gestion du risque cyber devient un exercice de vitesse et de coordination.
2. **France Travail, symbole d'une fragilité publique :** un incident majeur qui questionne la chaîne de sous-traitance et la sécurité de l'authentification.
3. **Lycées des Hauts-de-France attaqués :** les collectivités et établissements scolaires deviennent des cibles privilégiées.
4. **AWS en panne : dépendance structurelle de l'Europe** — une crise révélatrice de la nécessité d'une souveraineté cloud et d'alternatives industrielles.
5. **Enquête de Keeper Security, signal mondial à l'adresse des organisations :** entre culture du Zero Trust et inertie opérationnelle, les écarts se creusent ; la rigueur d'exécution devient un enjeu stratégique. La maturité cyber ne se proclame pas, elle s'éprouve.
6. **Mutation du risque :** l'IA démultiplie les vecteurs d'attaque ; les défenses doivent intégrer l'automatisation, la veille, la poursuite de la sensibilisation et, au-delà, la formation.
7. **Cap sur 2026 :** le Forum InCyber de Lille 2026 portera l'ambition d'une cybersécurité européenne de confiance et de souveraineté mutualisée.

### Sources


VeilleCyber.fr — *Actualités cybersécurité, octobre 2025* https://veillecyber.fr/

France Travail — *Cyberattaque : soyez vigilants* https://www.francetravail.fr/candidat/soyez-vigilants/cyberattaque-soyez-vigilants.html

CNIL — *Fuite de données France Travail : enquête et recommandations* https://www.cnil.fr/fr/france-travail-la-cnil-enquete-sur-la-fuite-de-donnees-et-donne-des-conseils-pour-se-proteger

CERT-FR (ANSSI) — *Bulletins de sécurité, octobre 2025* https://www.cert.ssi.gouv.fr/actualite/

La Voix du Nord — *Cyberattaque contre les lycées des Hauts-de-France : 250 établissements paralysés*
https://www.lavoixdunord.fr/2025/10/18/cyberattaque-lycees-hauts-de-france

Hauts-de-France.fr — *Incident de cybersécurité dans plusieurs lycées de la région Hauts-de-France*
https://www.hautsdefrance.fr/incident-de-cybersecurite-dans-plusieurs-lycees-de-la-region-hauts-de-france/

Keeper Security — *Global Cybersecurity Insights Report 2025* (30 octobre 2025)
https://www.prnewswire.com/news-releases/keeper-security-research-captures-global-cybersecurity-insights-from-practitioners-302599175.html

Fortinet, *Le modèle de sécurit Zero Trust*
https://www.fortinet.com/fr/resources/cyberglossary/what-is-the-zero-trust-network-security-model

InCyber Europe 2026 — *Programme et thématique annoncés*
https://europe.forum-incyber.com

Yannick PECH est docteur en sciences de l'information-communication, spécialiste du renseignement et de la cybersécurité, certifié *pentester* junior. Chargé de cours en géopolitique, intelligence économique, sécurité numérique et OSINT dans le supérieur privé et public, chercheur au CEREGE de l'IAE de Poitiers, ancien veilleur-analyste et réserviste opérationnel de l'armée de Terre, il est désormais officier de la Réserve citoyenne de cyberdéfense au sein de la gendarmerie d'Occitanie. Il prépare actuellement les certifications EBIOS-RM et ISO-27001.