

N°63

PRIX : 24€ TTC
TRIMESTRIEL
MAI > JUILLET 2026

Global Security Mag

THE LOGICAL & PHYSICAL SECURITY MAGAZINE

LES VULNÉRABILITÉS & LA CYBERSÉCURITÉ



p. 64

**Joffrey
Celestin-Urbain**

Président du Campus Cyber

Les enjeux de résilience et de souveraineté que concentre la cyber sont existentiels pour la France et l'Europe

L'IA face au chaos
systémique :
Entre effondrement
sémantique et guerre
pour la conscience

p. 8



Lubna Brioual

*Consultante Sénior
Cybersécurité Gouvernance
Risks Compliance Intelligence
Économique*

Vulnérabilités
et cybersécurité

p. 25



Myriam Quéméner

*Magistrat honoraire et
Docteur en droit*

Vulnérabilités
et cybersécurité

p. 33



**Général de Brigade
Hervé Pétry**

*Commandant de l'Unité
Nationale Cyber (UNCYBER)*

La meilleure façon de
protéger des données,
c'est de ne pas les
avoir en clair

p. 68



Andy Yen

Founder, CEO of Proton



OFFERT PAR



Une (cyber) sécurité qui s'adapte à vos défis (numériques)

Parlons de vos projets 2026

↳ [Davidson.fr/cybersecurite](https://davidson.fr/cybersecurite)



LES VULNÉRABILITÉS & LA CYBERSÉCURITÉ

La Vulnérabilité est généralement entendue comme un état de faiblesse identifiée, mais peut-elle également être envisagée comme une force, ou être transformée en atout ?

L'origine latine vulnus ou vulneris (la blessure) et vulnerare (blesser), amène à définir l'être vulnérable, comme celui qui peut être blessé, frappé, qui peut être facilement atteint ou qui se défend mal.

L'image de la blessure fait penser à une ouverture, une faille, une défaillance.

Le Philosophe stoïcien Sénèque (4 av. J.C. -65 apr. J.C.) énonçait « connaître son point faible pour le protéger davantage ».

Il s'agit du concept du talon d'Achille ou de la faiblesse qu'il est nécessaire pour chaque être de découvrir en lui afin de trouver les meilleurs moyens de protection.

La Philosophe et Psychanalyste Cynthia Fleury lors d'une conférence à la Faculté de Santé Sorbonne, a parlé de la notion de Vulnérabilité comme d'un concept pivot. Elle a notamment mis l'accent sur la Vulnérabilité en tant que situation d'une personne particulièrement exposée à la blessure, physiquement ou psychologiquement.

Dans le monde de la Cybersécurité, il existe un concept clé, **CVE (Common Vulnerabilities and Exposures, ou Expositions et Vulnérabilités Communes)**. Ces CVE désignent une série de failles dans un système que les développeurs et ingénieurs ou d'autres personnes responsables doivent connaître, afin d'atténuer ou de renforcer la sécurité du système.

On peut ainsi dire que si la Vulnérabilité peut être une faiblesse ou une faille, la repérer, la connaître, afin de la gérer au mieux, peut se révéler être une force.

Dans cette 63^e édition de Global Security Mag, vous allez découvrir plusieurs angles traités dans les Rubriques suivantes : **Délégué.e à la Protection des Données, Femmes Engagées dans la Cyber, THEMA, Formations & Mentoring, Publi-Info, Entretiens, les News du CPI-B2B, Chronique Technique, Chronique Juridique, L'œil Expert**

Au plaisir !

Valentin Jangwa

VULNERABILITIES AND CYBERSECURITY

Vulnerability is generally understood as a state of identified weakness, but can it also be considered a strength or transformed into an asset?

The Latin origin vulnus or vulneris (the wound) and vulnerare (to wound) leads to defining a vulnerable being as one who can be injured, struck, easily affected, or who is poorly defended.

The image of a wound evokes an opening, a flaw, or a failure.

The Stoic philosopher Seneca (4 BC – 65 AD) stated, "Know your weak point to protect it better."

This refers to the concept of the Achilles' heel—the weakness that every individual must discover within themselves to find the best means of protection.

Philosopher and psychoanalyst Cynthia Fleury during a conference at the Sorbonne Faculty of Health discussed vulnerability as a pivotal concept. She emphasized vulnerability as a situation in which a person is particularly exposed to physical or psychological injury.

In the world of cybersecurity, a key concept exists : **CVE (Common Vulnerabilities and Exposures)**. These CVEs refer to a series of flaws in a system that developers, engineers, or other responsible parties must be aware of to mitigate risks or strengthen system security.

Thus, while vulnerability may be a weakness or flaw, identifying and understanding it to manage it effectively can become a strength.

In this 63rd edition of Global Security Mag, you will discover various perspectives explored in the following sections:

Data Protection Officers, Women Engaged in Cybersecurity, THEMA, Training & Mentoring, Publi-Info, Interviews, CPI-B2B News, Technical Column, Legal Column, Expert Insight.

Enjoy your reading!

Valentin Jangwa

SOMMAIRE

1 ÉDITO

4-5 AGENDA & CALENDRIER
DES ÉVÈNEMENTS

DÉLÉGUÉ.E À LA PROTECTION DES DONNÉES

6-7 Philippe Salaün

FEMME ENGAGÉE DANS LA CYBER

8-10 Lubna Brioual

12-14 Gabriela BELAID

Livre blanc

16-17 Éric Singer

THEMA

19-20 Éric Singer

22-23 Florence Giuly-Davis

25-26 Myriam Quéméner

27-28 Loïc Guézo

30-32 Séverine Meunier

33-34 Général Hervé Pétry

36-37 Franck Rouxel

TALENTS CYBER

43-45 Etienne Capgras

Formations & Mentoring

48-51 Hélène Bouchard

Publi-info

52-54 Davidson consulting

56-57 Rosenberger

61 Scalify

entretien

64-65 Joffrey Célestin-Urbain

68-69 Andy YEN

chronique technique

70-72 Nicolas Liard

Livre cyber

74-75 Thomas Lejars

77 Myriam Quéméner

entretien

78-81 Christophe Vercellone

évènements cyber

84-85 Maria Iacono

LES NEWS DU CPI-B2B

88-89 Etienne de Sérerville

CHRONIQUE JURIDIQUE

90-91 Alexandra Iteanu

L'œil de l'expert

93-94 Jean-Pierre La Hausse De Lalouvière

N°63 mai>juillet 2026

globalsecurymag.fr,
globalsecurymag.com,
globalsecurymag.de, gsdays.fr

ISSN : 1959 - 7061

Dépôt légal : à parution

Éditée par LEVAS SAS

RCS Paris 947 665 543

5 avenue des Gobelins 75005 Paris

Tél. : +33 7 89 65 15 70

e-mail : vj@globalsecurymag.com

ABONNEMENT :

Version papier : 24 € TTC (TVA 20%)

Version PDF : 12 € TTC (TVA 20%)

RÉDACTION :

Directeur de la Publication

et Rédacteur en Chef :

Valentin Jangwa

CRÉATION, CONCEPTION ET
RÉALISATION GRAPHIQUE

Marine Volpi

PUBLICITÉ :

LEVAS SAS

Présidente : Laurence Beuchard

levas-cyberformations.com

comptabilite@levas-cyberformations.com

COUVERTURE ET INTERIEUR :

ISTOCK

IMPRESSION :

Wagram édition

8 rue Salvador Allende

95870 Bezons

Imprimé avec des encres végétales

sur papier éco-responsable certifié

PEFC par un imprimeur adhérent

à Imprim'vert selon le procédé CTP
sans chimie

COMITÉ SCIENTIFIQUE :

Pierre Bagot, Francis Bruckmann

Eric Doyen, Catherine Gabay,

François Guillot, Olivier Iteanu,

Dominique Jouniot, Patrick Langrand,

Yves Maquet, Thierry Ramard,

Hervé Schauer, Michel Van Den Berghe,

Bruno Kerouanton, Loïc Guézo,

Marc Jacob Brami, Sylvie Lévy,

Yelena Jangwa Nedelec,

Lucille Beuchard-Hott Mbock,

Laurence Beuchard, Suzanna Nedelec,

Anne Guyot, Nicolas Liard,

Christel Olsen, Daniel Binsfeld

et Valentin Jangwa,

In Memoriam, notre regretté Zbigniew
Kostur

SUMMARY

1 EDITO

4-5 AGENDA &
EVENTS CALENDAR

DATA PROTECTION OFFICER

6-7 Philippe Salaün

CYBER WOMAN

8-10 Lubna Brioual

12-14 Gabriela BELAID

white paper

16-17 Éric Singer

THEMA

19-20 Éric Singer

22-23 Florence Giuly-Davis

25-26 Myriam Quéméner

27-28 Loïc Guézo

30-32 Séverine Meunier

33-34 Général Hervé Pétry

36-37 Franck Rouxel

CYBER TALENTS

43-45 Etienne Capgras

Training & mentoring

48-51 Hélène Bouchard

Publi-info

52-54 Davidson consulting

56-57 Rosenberger

61 Scalify

INTERVIEW

64-65 Joffrey Célestin-Urbain

68-69 Andy YEN

Technical column

70-72 Nicolas Liard

CYBER BOOK

74-75 Thomas Lejars

77 Myriam Quéméner

INTERVIEW

78-81 Christophe Vercellone

CYBER EVENTS

84-85 Maria Iacono

NEWS FROM CPH-B2B

88-89 Etienne de Sérerville

Legal column

90-91 Alexandra Iteanu

EXPERT INSIGHT

93-94 Jean-Pierre La Hausse De Lalouvière



- **4 mai • College Park, Maryland (USA)**
CMMC Day
 Lieu : The Hotel at the University of MD, College Park, Maryland
www.cmmcday.org
- **4 > 5 mai • College Park, Maryland (USA)**
CSfC Conference
 Lieu : The Hotel at the University of MD, College Park, Maryland
www.certinfosec.org
Federal Certification Events Week
 lieu : The Hotel UMD, College Park, MD
 Cet événement inclut :
 Cybersecurity Maturity Model Certification (CMMC) Day
The future of federal supply chain security
www.CMMCDay.org
 Common Criteria Day
The future of the global certification standard in the federal space
www.CriteriaDay.org
Commercial Solutions for Classified (CSfC) Conference
Surveying the effort to leverage leading technology for national security
www.CertInfoSec.org
Department of Defense Information Network Approved Product List (DoDIN APL) Day A
comprehensive look at DoD Information Network technology certification
www.DoDINDay.com
Cyber Trust Mark Day
 Preparing ICT product developers for the coming US cybersecurity certification and labeling program
www.TrustMarkDay.org
- **5 > 7 mai • Dubaï**
GISEC
<https://gisec.ae/>
- **5 > 6 mai • Francfort (Allemagne)**
TechShow - Cloud Expo Europe
www.techweekfrankfurt.de
- **6 > 7 mai • Copenhague (Danemark)**
Infosecurity Denmark
<https://www.v2security.dk/>
- **7 mai • Londres (UK)**
 Securing AI Congress
<https://akjassociates.com/>
- **10 > 14 mai • Rome (Italie)**
Eurocrypt
<https://eurocrypt.iacr.org/2026>
- **11 > 14 mai • Houston (TX) (USA)**
XPONENTIAL
 George R. Brown Convention Center
<https://xponential.org/>
- **12 mai > Istanbul • (Turquie)**
ENBANTEC Cyber Security
 Conference and Exhibition
<https://www.enbantec.com>
 Email : info@enbantec.com
- **18 > 19 mai • San Jose - CA (USA)**
Cyber Security & Cloud Expo
 Lieu : San Jose McEnery Convention Center, CA
www.cybersecuritycloudexpo.com/northamerica/
- **19 mai • Campus Cyber Paris La Défense**
Assemblée Générale et élections des membres du conseil d'administration du Clusif réservée aux membres
<https://clusif.fr/agenda/assemblee-generale-et-elections-des-membres-du-conseil-dadministration/> _ Conférence sur les enjeux géopolitiques, avec Frédéric Charillon
<https://clusif.fr/agenda/conference-sur-les-enjeux-geopolitiques/>
- **19 > 22 mai • Saint-Tropez**
RIAMS
<https://les-riams.fr/>
- **20 mai • Oman (Muscat)**
DTX Oman
 Lieu : Sheraton Oman Hotel
<https://www.dtxoman.com/>
- **20 > 21 mai • Bruxelles (Belgique)**
CyberSec
 Lieu : Brussels Expo
www.cyberseceurope.com

> JUIN <

- **2 > 3 juin**
Paris
Paris Cyber Week
www.paris-cyber-week.com
Boston, Massachusetts (USA)
HealthSec
www.cs4ca.com
Galgary (Canada)
CS4CA Canada
www.cs4ca.com
Monaco
Ready For IT
Organisateur : Comexposium et DG Conseils
www.ready-for-it.com
Londres (UK)
Infosecurity Europe
ExCeL London
Renseignements : Reed Exhibitions UK
Tél. : +44 (0)20 8271 2130
E-mail : infosecurity.helpline@reedexpo.co.uk
www.infosec.co.uk
- **1^{er} juin Cannes (France)**
DataCloud Europe
Pre-event
Renseignements :
E-mail : enquiries@datacentres.com
<https://events.broad-group.com/event/a4ba77f1-52e2-4570-a6f5-d442cd3eca93/summary>
- **2 > 4 juin**
Myrtle Beach (SC) (USA)
Techno Security & Forensics Investigations Conference & Mobile Forensics World
<https://www.technosecurity.us/mb>
Johannesburg (Afrique du Sud)
Securex South Africa
Lieu : Gallagher Convention Centre
www.securex.co.za
- **3 > 4 juin**
Londres (UK)
GEO Business
www.geobusinessshow.com
Rennes (France)
SSTIC
www.sstic.org
Deauville (France)
Le Symposium du CRiP - Le Rendez-vous annuel des Décideurs IT
<https://www.crip-asso.fr/events>
- **9 > 10 juin • Paris-Châtillon**
Conférence annuelle d'OW2
Lieu : Orange Gardens
44 Avenue de la République,
92320 Châtillon
www.ow2con.org
AGORA MANAGERS - Future of IT
Château Comet Levallois, 92300
Levallois-Perret - Journée
Workshops & Networking
Pavillon Vendôme, 75001 Paris -
Soirée Gala
<https://www.agoramangers-events.com/future-of-it/>
- **8 - 11 juin • Montréal (Canada)**
MAAWG General Meeting
www.m3aawg.org
- **9 > 11 juin • i Piacenza (Italie)**
CYBSEC-EXPO
Piacenza Expo
<https://cybsec-expo.it/>
- **9 > 12 juin • Marrakech (Maroc)**
SIT Africa
Palmeraie Resort à Marrakech
<https://sit.africa/>
- **11 et 12 juin • Caen**
congrès GPMSE
www.gpmse.com
- **16 > 18 juin • Rennes**
Préventica
<https://www.preventica.com/participer.php>
- **17 juin • Paris**
Diner du Cercle de la sécurité
www.lecercle.biz
- **17 > 20 juin • Paris**
Vivatech
<https://vivatechnology.com/>
- **18 juin**
Technology Live ! Germany
<https://a3communicationspr.com/homepage/events/technology-live/>
e-crime & cybersecurity Germany
<https://akjassociates.com/>
- **23 juin • Chartres**
1 jour pour 5 ans conférence par l'AN2V
Hôtel de Ville de Chartres
<https://an2v.org/1-jour-pour-5-ans/>
- **23 > 25 juin • Le Mans (France)**
Congrès National SSI Santé
Contact : secretaire@apssis.com
www.apssis.com
- **24 juin • Munich, BMW Welt**
Cyber IA expo
<https://cyberai-expo.de/>
Vos tickets offerts avec le code GSM2026
- **23 > 26 juin • United Arab Emirates**
World Police Summit
Dubai Exhibition Centre Expo
www.worldpolicesummit.com/

> JUILLET <

- **1^{er} > 2 juillet • Londres (UK)**
CT INSIGHT
Lieu : Olympia
<https://ctinsight.net/>
- **1^{er} juillet 2026**
Les Rencontres du Clusif
événement réservé aux membre -
Pavillon Royal Carrefour du Bout des lacs, 75016 Paris
<https://clusif.fr/agenda/les-rencontres-du-clusif/>
- **2 juillet • Londres (UK)**
Securing Financial Services
<https://akjassociates.com>
- **9 juillet • Johannesburg (Afrique du Sud)**
**7th Edition Connected Africa -
Telecom Innovation & Excellence Awards 2025**
(Africa's Premier Telecom Summit)
<https://connected-africa.com/summit/>

PHILIPPE
SALAÜN

*Président AFCDP, ancien
DPO et responsable de la
gestion de crise*



VULNÉRABILITÉS & CYBERSÉCURITÉ : LE DPO, ACTEUR DE LA « CONFIANCE-CLIENT »

À mesure que les organisations se numérisent, leur surface d'exposition s'élargit et se complexifie. Les vulnérabilités ne sont plus seulement techniques : elles sont aussi organisationnelles, humaines, contractuelles, parfois même culturelles.

Face à cette réalité, l'AFCDP appelle à dépasser une approche souvent trop cloisonnée de la cybersécurité. La protection des données personnelles ne peut plus être perçue comme une contrainte : elle constitue un pilier à part entière de la gestion des risques et de la confiance numérique.

La résilience des organisations dépend désormais de leur capacité à articuler cybersécurité et protection des données dans une même dynamique.

UN ACTEUR STRATÉGIQUE AU-DELÀ DE LA TECHNIQUE

Le Délégué à la protection des données (DPO) n'est pas un opérateur de sécurité. Il ne configure pas d'outils, ne supervise pas d'infrastructures. Mais il est un acteur essentiel de la cybersécurité. À travers le registre des traitements, les analyses d'impact (AIPD) et l'accompagnement des projets, il met en lumière des fragilités structurelles que les seuls dispositifs techniques ne détectent pas : collecte excessive de données non nécessaires, défaut de gouvernance, chaînes de sous-traitance insuffisamment maîtrisées, pratiques métiers à risque notamment avec certaines utilisations de l'« IA fantôme » parfois non conformes à la réglementation.

Son rôle ne doit pas se limiter à la prévention. En cas d'incident, le DPO contribue à qualifier rapidement les violations de données personnelles, à évaluer les risques pour les personnes concernées et à orienter les décisions de notification auprès des autorités et, le cas échéant, des clients impactés. Cela suppose des moyens dédiés, une indépendance effective et une association systématique aux dispositifs de gestion de crise. La réactivité juridique et organisationnelle, sans oublier la communication adaptée, sont aujourd'hui aussi essentielles que la réponse technique.

LA SYNERGIE DPO-RSSI : POUR UNE SÉCURITÉ INTÉGRÉE ET GLOBALE

La complémentarité entre DPO et RSSI constitue à cet égard un élément déterminant. Trop souvent encore, les organisations opposent conformité et sécurité, comme si l'une freinait l'autre. L'AFCDP défend une approche résolument intégrée : le RSSI protège les systèmes d'information contre les menaces, le DPO veille au respect des droits et libertés des personnes concernées et à la conformité des traitements avec le RGPD. Cette articulation doit être organisée, formalisée, outillée, et surtout soutenue au plus haut niveau de gouvernance, c'est-à-dire au niveau de la direction générale de l'organisation. C'est de cette coopération que naît une sécurité réellement efficace et légitime.

Cette exigence de complémentarité dépasse largement le périmètre numérique. La sécurité physique (accès aux locaux, archivage papier, gestion des postes de travail, contrôle des visiteurs...) demeure un maillon souvent sous-estimé des chaînes de vulnérabilité. Là encore, le DPO a un rôle à jouer en lien avec les responsables concernés, afin de garantir une approche globale, proportionnée et respectueuse des droits des personnes. La protection des données impose de penser la sécurité d'une manière globale et intégrée dans l'entreprise.

L'AFCDP veut porter un message clair auprès des décideurs : confier le pilotage de la cybersécurité à la seule direction des systèmes d'information, sans intégrer pleinement le DPO dans la stratégie de risque, c'est accepter de fragiliser l'organisation. Le DPO ne doit pas être considéré comme un acteur contraignant, mais un véritable « business partner », qui dialogue sur un pied d'égalité avec le RSSI, la direction juridique et les métiers pour convaincre la Direction générale de prendre la bonne décision au bon moment dans l'intérêt de l'organisation et des personnes concernées.

LE DPO, UN « BUSINESS PARTNER » AU CŒUR DE LA GOUVERNANCE

Dans un contexte de multiplication des menaces et de renforcement des exigences réglementaires, l'AFCDP réaffirme le rôle central du DPO comme acteur de gouvernance de plein droit, ce qui suppose un positionnement clair, un accès direct à la décision, des ressources adaptées, et une reconnaissance effective de son indépendance. À défaut, la fonction restera insuffisante là où elle devrait être stratégique.

La résilience des organisations dépend désormais de leur capacité à articuler cybersécurité et protection des données dans une même dynamique. C'est une exigence opérationnelle, mais aussi un choix politique. L'AFCDP continuera de porter cette conviction avec constance : il ne peut y avoir de confiance durable sans une gouvernance forte, transversale et pleinement reconnue du DPO. ■

LUBNA
BRIQUAL

*Consultante Senior Cybersécurité
Gouvernance Risks Compliance
Intelligence Economique*



L'IA FACE AU CHAOS SYSTÉMIQUE : ENTRE EFFONDREMENT SÉMANTIQUE ET GUERRE POUR LA CONSCIENCE

Une analyse géopolitique et technique pour les experts de la cybersécurité

Le monde de 2026 ne ressemble plus aux projections linéaires des années 2020. L'intelligence artificielle, loin d'être une simple strate logicielle supplémentaire, s'est révélée être un agent de transformation physique, énergétique et civilisationnel.

Pour les professionnels de la cybersécurité, le paradigme a basculé : nous ne protégeons plus seulement des systèmes, mais la souveraineté même de nos processus de pensée et l'intégrité de nos démocraties face à des "supra-systèmes" intrinsèquement instables.

I. L'INFRASTRUCTURE DU POUVOIR : GÉOPOLITIQUE ET "PIB FANTÔME"

L'IA n'est pas virtuelle ; elle est incroyablement matérielle. Le Forum Économique Mondial de 2026 a marqué un tournant pragmatique : la contrainte majeure n'est plus le code, mais la physique — l'énergie et les puces.

■ La dictature du "Compute" et de l'Énergie

La croissance économique dépend désormais de la capacité d'un pays à convertir l'énergie en intelligence (tokens) avec efficacité. Le facteur limitant est l'électricité. Cette réalité crée une nouvelle hiérarchie mondiale où ceux qui contrôlent les modèles, les données et les capacités de calcul deviennent des acteurs plus puissants que certains États.

L'avenir de la technologie ne réside pas dans le code, mais dans la vision, l'éthique et l'empathie. Dans un monde où l'intelligence n'est plus rare, la vraie monnaie devient la conscience humaine.

■ Le paradoxe de la valeur et le "PIB Fantôme"

Nous entrons dans l'ère du "PIB Fantôme". Un scénario se profile pour 2028 : une réussite totale de l'IA en entreprise où les gains de productivité permettent de réduire massivement les effectifs. La richesse créée ne circulera plus par les ménages — car les machines ne consomment pas — mais sera réinvestie dans des capacités IA, accélérant un cycle de déconnexion entre croissance économique et bien-être social.

II. LES PATHOLOGIES DE L'IA À GRANDE ÉCHELLE : L'EFFONDREMENT SÉMANTIQUE

Pour l'expert en sécurité des données, l'une des découvertes les plus critiques de 2026 est le phénomène de "Semantic Collapse" (effondrement sémantique).

■ Le plafond de verre du RAG (Retrieval-Augmented Generation)

Les recherches de Stanford démontrent que lorsque votre base de connaissances dépasse environ 10 000 documents, la recherche sémantique perd drastiquement en précision.

Compression des distances : Dans un espace à haute dimension, plus vous ajoutez de données, plus les distances entre les vecteurs se compressent.

Uniformisation : À grande échelle, tout finit par paraître similaire, rendant le filtrage et la récupération d'informations critiques extrêmement faillibles.

Risque Cyber : Cette perte de précision est une aubaine pour les attaques par empoisonnement de données ("Data Poisoning"), où des informations malveillantes subtilement injectées deviennent impossibles à distinguer du savoir légitime.

III. LA NOUVELLE SURFACE D'ATTAQUE : "SHADOW IA" ET AGENTS AUTONOMES

Le passage des chatbots aux IA agentiques (agents autonomes décideurs) crée un angle mort réglementaire et sécuritaire majeur.

Le danger de l'autonomie sans validation

La plupart des déploiements actuels s'effondrent par manque d'une couche de contrôle rigoureuse. Pour sécuriser une IA, il est impératif d'intégrer :

1. **Une logique d'approbation imposée** : Aucune action critique ne doit être exécutée sans validation humaine explicite.
2. **Une traçabilité totale** : Chaque décision doit être enregistrée dans des journaux expliquant le cheminement logique.
3. **Sanitisation des prompts** : Les invites (prompts) sont les nouvelles portes ouvertes à la fuite de données et à la manipulation.

■ L'IA Fantôme (Shadow AI)

L'adoption non régulée de l'IA pour répondre à l'urgence de performance crée des failles systémiques. Une dépendance excessive, sans supervision humaine, mène à une "Confiance Aveugle".

"Si l'architecture est faible, l'IA accélère sa faiblesse. Si la réponse est lente, elle aide à échouer plus vite."

IV. GUERRE COGNITIVE ET SOUVERAINETÉ NUMÉRIQUE

L'IA est devenue une arme de guerre cognitive. Elle ne se contente pas de traiter l'information ; elle façonne la perception de la réalité.

>>>

>>> ■ La colonisation du savoir tacite

Une entreprise qui n'intègre pas son "savoir tacite" dans ses propres modèles perd sa souveraineté. Elle transfère sa valeur intrinsèque vers le fournisseur du modèle (souvent les GAFAM ou BATX). L'externalisation des systèmes centraux à des milliardaires technologiques étrangers est un abandon de contrôle technique et politique.

■ La standardisation de la pensée

Les modèles dominants (LLM) sont principalement issus de la culture nord-américaine. Cela entraîne une standardisation de la pensée et une érosion de la diversité cognitive. Pour l'expert cyber, la protection de "l'intelligence économique" de l'organisation passe par le refus de cette dépendance normative.

V. RECOMMANDATIONS STRATÉGIQUES POUR LA RÉSILIENCE

Face à l'explosion des cadres de sécurité (RIA, DSA, etc.), la conformité ne suffit plus. Une organisation peut être conforme au Règlement sur l'IA (RIA) tout en restant hautement vulnérable, car le texte ignore souvent les risques de l'IA agentique.

1. Construire des "Ceintures de Sécurité"

Il faut mettre en place des "rambardes de sécurité" : des règles de vérification automatiques qui s'assurent que les sorties sont conformes au format attendu et exemptes de biais dangereux avant d'être partagées.

2. Le "Scepticisme Actif" dans la boucle humaine

L'humain ne doit pas être un simple superviseur passif (filet de sécurité défaillant), mais doit s'engager de manière critique. La vigilance diminue quand le système est généralement correct, laissant passer des erreurs subtiles mais catastrophiques.

3. Orchestration et Agilité

La stratégie gagnante repose sur une architecture capable de muter et d'intégrer en continu les retours du terrain.

Commencer petit : Choisir un domaine, prouver la valeur et s'assurer que la cybersécurité avance au même rythme que les ambitions IA.

Audit permanent : Face à l'explosion du code généré par IA, la question de "qui va auditer tout ce code" devient vitale pour éviter l'accumulation de dettes de sécurité invisibles.

CONCLUSION : AU-DELÀ DU CODE, L'ÉTHIQUE

L'avenir de la technologie ne réside pas dans le code, mais dans la vision, l'éthique et l'empathie. Dans un monde où l'intelligence n'est plus rare, la vraie monnaie devient la conscience humaine.

Pour l'expert en cybersécurité de 2026, la mission a changé : il s'agit de préserver notre capacité à douter, à juger et à rester responsables dans un environnement où la machine cherche à automatiser jusqu'à notre propre discernement. La résilience sera cognitive ou ne sera pas. ■

Si l'architecture est faible, l'IA accélère sa faiblesse.
Si la réponse est lente, elle aide à échouer plus vite.



CEFCYS CErCle des Femmes de la CYberSécurité

Vous êtes expert(e), analyste, consultant(e), RSSI, étudiant(e), personne en reconversion, dans la cybersécurité ... Rejoignez la communauté du CEFCYS pour partager vos compétences, développer votre réseau et faire connaître vos actions dans le monde de la cybersécurité : contact@cefcys.fr

Vous voulez soutenir nos actions et faire progresser la présence des femmes en cybersécurité... Rejoignez la communauté du CEFCYS pour faire bénéficier de vos expertises et formations nos adhérent(e)s, mettre en lumière vos talents féminins ... : partenariat@cefcys.fr

PUBLICATION DE LIVRES



Le tome 2 " Je suis une femme, et je travaille dans la cybersécurité " Portraits de 65 cyberwomen,

JOB DATING



Organisé par le CEFCYS : conférences et entretiens avec des entreprises partenaires, mentorat de groupe .
Prochaine date : 8 mars 2026

CYBER WOMAN DAY



Les Trophées Mondiaux de la Femme Cyber mettent en lumière des talents féminins



PODCAST



Le CEFCYS a lancé son PODCAST "Les cyberstories racontées par des femmes". Retrouvez les épisodes sur <https://www.youtube.com/c/CEFCYSOfficiel-Cybersecurite>

SENSIBILISATION



Des séances de sensibilisation des jeunes aux métiers de la cyber ainsi qu'aux risques numériques sont organisées dans les collèges, lycées, écoles

COLLOQUES CEFCYS



Le colloque du CEFCYS est organisé en Octobre, en marge du CyberMois. Le thème du dernier : "Cybermenaces et société : sensibiliser, comprendre, agir"

WEBINAIRES & FORMATION



Tous les mois deux sujets d'actualité sont présentés par les experts de nos partenaires. Des formations variées sont offertes grâce à nos partenaires

MENTORAT



Le CEFCYS propose deux programmes de mentorat :

- format individuel
- format groupé à destination des écoles, pour les d'étudiants.

Depuis la création du CEFCYS en 2016, la place des femmes dans la cyber sécurité est au coeur de nos actions

 <https://cefcys.fr/>

 contact@cefcys.fr

GABRIELA
BELAID

*Consultante en numérique,
cybersécurité et intelligence
artificielle_Présidente de
CentraleSupélec au Féminin et
Membre du Cefcys*



LA VULNÉRABILITÉ

Gabriela BELAID est consultante en numérique, cybersécurité et intelligence artificielle, avec plus de vingt ans d'expérience dans la transformation digitale, dont quinze années au service du secteur public.

Présidente de CentraleSupélec au Féminin et Membre du Cefcys, elle est Lauréate du Prix DigiTalentes du Numérique (CINOV 2023) et du Prix de la Femme Numérique de l'Année (CEFCYS 2024), elle est également sélectionnée dans la promotion 2026 des Expertes à la Une du Groupe TFI sur les sujets de souveraineté numérique, cybersécurité et intelligence artificielle.

La vulnérabilité, cette matière première que l'on a oublié de protéger

Ce matin-là, j'ai failli cliquer.

Un mail comme on en reçoit des dizaines. Urgent. Crédible. Bien écrit. J'ai hésité. Et puis je me suis arrêtée — non pas parce que j'avais identifié une anomalie technique, mais parce que quelque chose, en moi, doutait.

Et c'est ce doute qui m'a sauvée.

Ce jour-là, j'ai compris quelque chose : la vulnérabilité que j'avais face à ce mail n'était pas une faille de mon système. C'était une faille de mon humanité.

La véritable force, peut-être, n'est pas d'être invulnérable.
C'est de rester humain, sans devenir manipulable.

VULNÉRABILITÉ : UN MOT QUI EXISTAIT AVANT NOS ORDINATEURS

Du latin vulnus : la blessure. Être vulnérable, à l'origine, ce n'est pas être "piratable". C'est simplement être capable d'être touché — par un événement, une parole, une absence, une perte.

Pendant des siècles, la philosophie et les religions ont pensé cette réalité avec soin. Emmanuel Levinas en faisait une condition fondamentale de l'existence humaine : c'est précisément parce que nous sommes vulnérables que nous entrons en relation avec l'autre, que la responsabilité prend sens. La vulnérabilité, chez lui, n'est pas un défaut à corriger. C'est ce qui rend possible l'éthique.

Nietzsche, lui, voyait les choses autrement. Dans un monde qui valorise la force, la domination, la performance, la vulnérabilité ressemble à une faiblesse — quelque chose à surmonter, à dépasser, à cacher.

Cette tension entre les deux lectures n'a pas disparu. Elle s'est simplement déplacée vers nos infrastructures numériques.

Dans les trois grandes traditions monothéistes, la vulnérabilité prend encore une autre dimension. Elle n'est pas une faiblesse à corriger, mais un chemin : vers la vérité, vers l'autre, vers une forme de force intérieure que l'on ne trouve pas dans la domination mais dans le dépouillement. Le Christ en croix, Job éprouvé, Abraham obéissant dans l'obscurité — autant de figures qui font de la vulnérabilité non pas une défaite, mais un passage.

Tout cela pour dire : la vulnérabilité a une longue histoire. Et ce n'est pas le numérique qui l'a inventée.

CE QUE LE NUMÉRIQUE A FAIT À LA VULNÉRABILITÉ

Ce que le numérique a fait, en revanche, c'est la transformer en objet.

Un objet que l'on identifie, que l'on mesure, que l'on classe — CVE, score CVSS, criticité haute, patch prioritaire. En cybersécurité, tout commence par elle : détection des vulnérabilités, gestion des vulnérabilités, exploitation des vulnérabilités. Ce qui faisait la texture de notre fragilité humaine est devenu une variable dans un système.

Et je me suis demandé : quand avons-nous cessé de protéger la vulnérabilité... pour commencer à l'organiser ?

Ce glissement est discret. Mais il est profond. Car en faisant de la vulnérabilité une variable technique, nous avons peut-être perdu quelque chose d'essentiel : la conscience que derrière chaque faille, il y a un humain. Avec ses doutes, sa fatigue, sa confiance, parfois sa solitude.

DE LA FAILLE À L'ARME : LA VULNÉRABILITÉ COMME LEVIER DE POUVOIR

Puis il y a eu un second basculement. Plus inquiétant encore.

La vulnérabilité n'a pas seulement été mesurée. Elle a été exploitée. À grande échelle. Avec méthode.

Dans le cyberspace contemporain, on ne cherche plus seulement à pénétrer des systèmes. On cherche à comprendre les humains. Leurs réflexes. Leurs peurs. Leurs biais cognitifs. Ce qui les fait cliquer, répondre, partager, douter. Les campagnes de phishing ne sont plus des tentatives grossières — elles sont personnalisées, contextualisées, presque invisibles. Elles ne visent plus les infrastructures. Elles visent les perceptions, les croyances, les émotions.

Avec l'intelligence artificielle, ce mouvement s'accélère. Les messages s'adaptent au profil psychologique de leur cible. Les voix s'imitent. Les visages se recréent. Ce qui relevait autrefois de la manipulation artisanale devient aujourd'hui automatisé, optimisé, industrialisé. La vulnérabilité humaine n'est plus seulement exploitée. Elle est anticipée. Et parfois même, délibérément provoquée.

Dans les conflits contemporains, il ne s'agit plus seulement de détruire des infrastructures. Il s'agit de désorienter des sociétés entières. D'affaiblir la confiance. De brouiller le vrai et le faux. D'installer le doute — car une société qui doute d'elle-même est plus fragile que n'importe quel réseau mal sécurisé.

Ce qui nous rend vulnérables est aussi ce qui nous rend humains

Et pourtant. Je ne crois pas que la réponse soit de chercher à n'être plus touché.

Sans vulnérabilité, pas de confiance. Sans confiance, pas de relation. Sans relation, pas de coopération, pas de société, pas de sens. Ce qui nous expose est aussi ce qui nous relie. C'est le paradoxe que ni Levinas ni les traditions religieuses n'ont jamais voulu résoudre — parce qu'il ne doit pas l'être.

La vraie question n'est donc pas : comment supprimer nos vulnérabilités ? Ni même comment les masquer.

MAIS COMMENT APPRENDRE À VIVRE AVEC ELLES, SANS QU'ELLES DEVIENNENT DES PRISES ?

Dans un monde où la vulnérabilité est devenue une matière première stratégique, protéger ne suffit plus. Il faut aussi éduquer, nommer, conscientiser. Apprendre aux individus à reconnaître leurs propres biais, à identifier le moment où leur émotion est sollicitée à des fins de manipulation. La résilience numérique ne se construit pas uniquement avec des pare-feux. Elle se construit avec du discernement.

La véritable force, peut-être, n'est pas d'être invulnérable. C'est de rester humain, sans devenir manipulable. ■

**Être vulnérable, à l'origine, ce n'est pas être "piratable".
C'est simplement être capable d'être touché — par un événement,
une parole, une absence, une perte.**



GOUVERNEMENT

Liberté
Égalité
Fraternité



Mon assistance en ligne



Virus | chantage | piratage ...

Ayez le nouveau réflexe cyber
Rendez-vous sur le site **17cyber.gouv.fr**



ÉRIC
SINGER

*CISO – membre du
CESIN, Coauteur du
Livre Blanc*

« SORTIR DES DÉPENDANCES NUMÉRIQUES »

Le livre blanc « Maîtriser nos dépendances numériques – vers une autonomie numérique choisie et gouvernée » est disponible en téléchargement sur le site du CESIN.

**DERRIÈRE CETTE EXPRESSION
ENCORE ABSTRAITE SE CACHE
UNE RÉALITÉ DE PLUS EN PLUS
TANGIBLE :
CELLE D'ORGANISATIONS DONT
L'ACTIVITÉ REPOSE SUR UN
NOMBRE RESTREINT D'ACTEURS
TECHNOLOGIQUES, SANS TOU-
JOURS DISPOSER DE VÉRITABLES
ALTERNATIVES.**

Ce constat est au cœur du livre blanc « Maîtriser nos dépendances numériques – vers une autonomie numérique choisie et gouvernée », publié par le CESIN en partenariat avec le Forum InCyber 2026, qui propose de reconsidérer un risque encore largement sous-estimé.

DEPUIS QUINZE ANS, LA TRANSFORMATION NUMÉRIQUE A REMODELÉ LES SYSTÈMES D'INFORMATION

Cloud, SaaS, plateformes intégrées, externalisation : ces choix ont permis des gains en agilité et en performance. Mais ils ont aussi construit, progressivement, une architecture de dépendance.

Aujourd'hui, de nombreuses organisations reposent sur un nombre d'acteurs technologiques avec une tendance géopolitique marquée.

Les chiffres du baromètre CESIN–OpinionWay en témoignent : 53 % des entreprises constatent une augmentation des menaces d'origine étatique, et près de deux organisations sur trois se disent concernées par les enjeux de souveraineté et de cloud de confiance.

Cette dépendance est d'autant plus difficile à appréhender qu'elle est diffuse. Elle ne se limite pas aux infrastructures visibles. Elle traverse l'ensemble des chaînes de valeur : logiciels, standards techniques, contrats, compétences, mais aussi modes de décision et d'usage. Elle ne surgit pas brutalement, mais s'installe progressivement, au fil de décisions rationnelles. Le résultat n'est pas une rupture, mais une érosion : celle de la capacité à arbitrer, à changer de trajectoire, à reprendre la main.

Dans ce contexte, l'interruption de service apparaît comme le signal le plus visible. Lorsqu'un fournisseur critique est défaillant, c'est toute une chaîne d'activités qui peut être affectée. Ce risque n'est plus marginal : il devient structurant, car il révèle une dépendance profonde à des infrastructures et à des acteurs sur lesquels l'organisation n'a qu'un contrôle limité.

CERTAINS ÉVÉNEMENTS RÉCENTS EN ILLUSTRONT LES EFFETS

En 2025, des pannes chez des hyperscalers ont paralysé simultanément messageries, outils métiers et services essentiels.

Autre illustration : lors d'un incident fin 2025, plusieurs activités du groupe La Poste ont été perturbées. Pendant plusieurs heures, services logistiques et outils de suivi des flux se sont retrouvés dégradés. Cet épisode illustre la nature des dépendances numériques : invisibles en temps normal, elles ne deviennent tangibles qu'au moment de la rupture, lorsque la continuité d'activité dépend d'un maillon que l'on ne maîtrise pas.

L'essor de l'intelligence artificielle amplifie ce phénomène. En concentrant les capacités de calcul, les volumes de données et les modèles entre les mains de quelques acteurs, elle agit comme un amplificateur de dépendances. Elle ne crée pas nécessairement de nouvelles dépendances, mais intensifie celles qui existent déjà. Dans le même temps, elle peut offrir des opportunités, notamment pour cartographier et mieux comprendre des systèmes devenus complexes.

Le livre blanc met également en évidence un changement de nature du sujet : la dépendance numérique n'est plus un sujet purement technique. Elle devient un enjeu de gouvernance, directement porté au niveau des directions générales, car elle conditionne la continuité d'activité, la capacité d'innovation et la liberté de décision.

Pour bien comprendre le phénomène, il convient de distinguer deux niveaux de lecture. À l'échelle des organisations — le niveau « micro » — la dépendance se traduit par des enjeux très concrets : continuité, coûts, réversibilité ou contraintes

juridiques. À l'échelle des États — le niveau « macro » — elle renvoie à des enjeux de souveraineté, de protection des données et de continuité des services essentiels. Les deux niveaux sont étroitement liés, car l'accumulation de choix individuels produit des dépendances collectives.

FACE À CELA, L'ENJEU N'EST NI DE VISER UNE INDÉPENDANCE TOTALE NI D'ACCEPTER UNE DÉPENDANCE SUBIE

Il s'agit de retrouver des marges de manœuvre. Intégrer la réversibilité dès la conception, diversifier les écosystèmes, réinvestir dans les compétences et repenser les relations contractuelles.

LA DÉPENDANCE NUMÉRIQUE N'EST PAS UN ÉTAT À ÉVITER, MAIS UNE RÉALITÉ À COMPRENDRE ET À GOUVERNER

La question est de savoir de quoi, jusqu'où, et dans quelles conditions la capacité de reprendre la main peut être préservée.

Dans un environnement numérique globalisé, la dépendance est inévitable. Sa maîtrise devient un choix stratégique, au cœur des enjeux de résilience, d'innovation et de souveraineté. ■

53 % des entreprises constatent une augmentation des menaces d'origine étatique, et près de deux organisations sur trois se disent concernées par les enjeux de souveraineté et de cloud de confiance.



REJOIGNEZ LE CESIN

CLUB DES EXPERTS DE LA SÉCURITÉ DE L'INFORMATION ET DU NUMÉRIQUE

COOPÉRATION - CONFIANCE - CONVIVIALITÉ

Un Club au service de ses membres

- # CONFÉRENCES
- # GROUPES DE TRAVAIL
- # ATELIERS
- # ENQUÊTES
- # FILS DE DISCUSSION
- # LIVRABLES
- # PARTAGE D'INFORMATION
- # SITE WEB
- # RÉSEAU SOCIAL
- # FORMATION
- # BOURSE D'EMPLOI
- # PARTENARIATS
- # ECHANGES AVEC LES POUVOIRS PUBLICS



CESIN

TOUS SECTEURS D'ACTIVITÉS GRANDES ENTREPRISES, ADMINISTRATIONS ET ENTREPRISES DE TAILLE INTERMÉDIAIRE

ERIC
SINGER

*CISO
membre du CESIN*



VULNÉRABILITÉS & CYBERSÉCURITÉ

La vision du RSSI : de la gestion réactive à l'intelligence prédictive

DEPUIS TRENTE ANS, LA GESTION DES VULNÉRABILITÉS EST AU CŒUR DU MÉTIER DU RESPONSABLE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION, LE RSSI.

Recenser les failles, prioriser les correctifs, réduire la fenêtre d'exposition : un travail souvent invisible mais déterminant. Sous la pression de l'intelligence artificielle, d'un cadre réglementaire qui se durcit et d'une surface d'attaque sans cesse élargie, cette pratique entre dans une nouvelle ère.

D'UNE RÉPONSE ARTISANALE À UNE DISCIPLINE INDUSTRIELLE

Tout commence dans les années 1990, lorsque le ver Morris révèle la fragilité d'internet. Les équipes techniques réagissent au cas par cas, en appliquant manuellement les correctifs publiés par les éditeurs. Le tournant vient en 1999 avec la création du CVE, identifiant universel pour chaque faille : pour la première fois, la communauté parle un langage commun.

Mais les vagues Nimda, Code Red ou Blaster montrent vite qu'aucune réponse manuelle ne tient face à des menaces qui s'industrialisent.

>>>

>>> LES ATTAQUES QUI ONT TOUT CHANGÉ

Chaque grande crise a redessiné la pratique. WannaCry, en 2017, paralyse 200 000 systèmes dans 150 pays en exploitant une faille corrigée depuis deux mois. NotPetya frappe ensuite via une mise à jour compromise et coûte plusieurs milliards aux groupes industriels. En 2021, Log4Shell révèle la fragilité des composants open source omniprésents, tandis que SolarWinds démontre qu'une mise à jour corrompue peut compromettre 18 000 organisations. La leçon est constante : la vulnérabilité n'est pas le seul problème, c'est le délai entre sa découverte, son exploitation et sa remédiation qui fait le risque. Plus de 80 % des compromissions exploitent encore des failles connues pour lesquelles un correctif existait.

STRUCTURER, OUTILLER, SE METTRE EN CONFORMITÉ

Pour répondre à cette industrialisation, les organisations se sont structurées. Les SOC (Security Operations Centers) surveillent en continu, les CERT mutualisent la veille. Le SOC est devenu une exigence implicite de NIS2 et DORA, souvent confiée à un prestataire en mode SOC as a Service. Une règle reste non négociable : la détection peut s'externaliser, la décision reste interne. C'est le RSSI qui arbitre, dans l'urgence, entre continuité d'activité et confinement.

Côté outillage, les scanners automatisent l'inventaire et les VOC (Vulnerability Operations Centers) ajoutent une priorisation contextuelle : sur 40 000 failles publiées chaque année, seules 2 à 5 % sont effectivement exploitées. La conformité, longtemps facultative, devient structurante. ISO 27001, NIS2, DORA et la gestion des risques tiers (TPRM) imposent des processus formalisés. Des plateformes comme BitSight ou SecurityScorecard étendent cette surveillance à tout l'écosystème de partenaires.

L'IA, ET LE SEUIL FRANCHI PAR MYTHOS

Cette quête d'efficacité a trouvé dans l'IA un allié décisif. L'EPSS prédit la probabilité qu'une faille soit réellement exploitée, des outils comme Pentera ou NodeZero rendent les tests d'intrusion continus, et le DevSecOps intègre la sécurité dès l'écriture du code, où une faille coûte dix fois moins cher à corriger qu'en production.

Mais avril 2026 marque une bascule. Anthropic introduit Mythos Preview, jugé si puissant qu'il ne sera pas rendu public. Soumis à Firefox, le modèle identifie 271 vulnérabilités là où la version précédente en trouvait 22, et révèle un défaut dormant depuis 27 ans dans OpenBSD. Pour préserver l'avance des défenseurs, le Project Glasswing en restreint l'accès à un cercle d'organisations à mandat défensif. Selon Palo Alto Networks, Mythos accomplit en quelques heures l'équivalent d'une année de tests humains. La fenêtre d'exposition se mesure désormais en semaines, et la dette technique cachée des systèmes va être brutalement révélée.

LE RSSI, COURROIE DE TRANSMISSION INDISPENSABLE

Dans ce nouveau paysage, le RSSI a muté. Technicien dans les années 2000, gestionnaire de risques dans les années 2010, il est devenu en 2026 la courroie de transmission entre le monde technique et le monde métier, la ceinture de sécurité que l'entreprise numérique ne peut plus se permettre de ne pas porter. Vers la direction générale, il traduit des réalités techniques en risques business, en exposition financière, en responsabilité réglementaire. Vers les équipes, il garantit que l'innovation s'exerce dans des enveloppes de risque maîtrisées.

À l'heure où les outils détectent plus vite que l'humain ne lit, sa valeur ne réside plus dans l'opération, mais dans le jugement. Juger les priorités, les délégations, les réponses. Et construire les équipes capables d'orchestrer l'IA défensive : la comprendre, l'utiliser, la gouverner. Sa légitimité ne se décrète plus. Elle se démontre, chaque jour. ■

Plus de 80 % des compromissions exploitent encore des failles connues pour lesquelles un correctif existait.



GOUVERNEMENT

Liberté
Égalité
Fraternité



Mon assistance en ligne



Virus | chantage | piratage ...

Ayez le nouveau réflexe cyber

Rendez-vous sur le site **17cyber.gouv.fr**

Un service proposé
par



FLORENCE
GIJLY-DAVIS

*Présidente et fondatrice de
l'agence de relations
publiques PR Paradigm
spécialiste en Cyber
et IT B2B*



VULNÉRABILITÉS : SORTIR DE LA LOGIQUE DE DÉTECTION POUR COMPRENDRE L'EXPOSITION RÉELLE

**DANS DES ENVIRONNEMENTS IT
TOUJOURS PLUS HYBRIDES ET
COMPLEXES, LA GESTION DES
VULNÉRABILITÉS S'EST IMPOSÉE
COMME UN PILIER DES STRATÉGIES
DE CYBERSÉCURITÉ.**

Les organisations n'ont jamais été aussi exposées, ni aussi dépendantes de leur capacité à identifier et corriger rapidement leurs points de faiblesse.

Dans ce contexte, la détection n'a jamais été aussi performante, et pourtant les équipes de sécurité peinent encore à prioriser efficacement. Les outils identifient, classent et suivent un volume toujours plus important de failles, avec un niveau de précision croissant.

Mais face à cette masse d'informations, une difficulté persiste, distinguer ce qui relève d'un risque réellement exploitable de ce qui ne l'est pas.

Ce modèle, largement structuré autour de l'identification, de la détection et de la correction, a permis des avancées réelles en matière de visibilité et a profondément transformé les pratiques. Mais à mesure que ces capacités s'accroissent, une tension apparaît.

L'actualité récente autour de l'IA appliquée à la cybersécurité, notamment avec des modèles comme Mythos, ne fait que l'accentuer en suggérant une accélération des capacités offensives et une multiplication des failles, dans un contexte où la surface d'attaque devient elle-même plus dynamique et plus rapide à exploiter.

Le débat sur les vulnérabilités ne disparaît pas, il se déplace.

CETTE LIMITE APPARAÎT ALORS PLUS CLAIREMENT. UNE VULNÉRABILITÉ NE PREND SENS QUE DANS SON CONTEXTE, ARCHITECTURE, CONDITIONS D'ACCÈS ET USAGES, AUTREMENT DIT DANS SA CAPACITÉ À ÊTRE EFFECTIVEMENT EXPLOITÉE.

Cette approche reste pourtant encore inégalement intégrée dans des pratiques largement structurées autour de l'identification et de la correction.

L'irruption de l'IA au sein des entreprises rend ce décalage plus visible. Un modèle comme Mythos ne se contente pas d'accélérer la découverte de failles. Il permet de les relier entre elles, de simuler des chaînes d'attaque et de rendre accessibles des scénarios d'exploitation jusqu'à réservés à des profils expérimentés. Ce mouvement ne crée pas un problème nouveau, il met en lumière une limite déjà présente dans la manière dont elles sont appréhendées.

Dans les faits, les organisations n'ont jamais disposé d'un niveau de visibilité aussi élevé. Les outils permettent d'identifier, de classer et de suivre des volumes importants de vulnérabilités, avec un niveau de précision croissant.

Mais sur le terrain, cette accumulation d'informations ne se traduit pas mécaniquement par une meilleure prise de décision. Elle complexifie souvent la hiérarchisation des priorités, au point de diluer la perception du risque réellement exploitable.

Pour de nombreuses équipes de sécurité, cette surcharge informationnelle devient en elle-même un défi opérationnel quotidien.

LES APPROCHES ACTUELLES ONT PERMIS DES AVANCÉES MAJEURES, MAIS ELLES ATTEIGNENT AUJOURD'HUI UNE LIMITE STRUCTURELLE DÈS LORS QU'IL S'AGIT D'ARBITRER EFFICACEMENT, AU POINT DE RENDRE CERTAINES DÉCISIONS PLUS COMPLEXES QU'ELLES NE LES ÉCLAIRENT.

À mesure que la détection gagne en maturité, une nouvelle exigence s'impose, inscrire les vulnérabilités dans leur contexte réel et dépasser une lecture fondée uniquement sur leur criticité théorique.

Ce basculement déplace concrètement le centre de gravité de l'analyse. Il ne s'agit plus seulement d'évaluer un score de sévérité, mais d'estimer une probabilité d'exploitation dans un environnement donné. Une faille critique mais isolée n'a pas le même impact qu'une vulnérabilité moyenne intégrée dans une chaîne d'attaque exploitable.

L'enjeu devient alors de comprendre dans quelles conditions une faille devient réellement accessible, comment elle peut être enchaînée avec d'autres points faibles et avec quelles conséquences opérationnelles pour l'organisation.

C'est cette lecture, centrée sur l'exposition réelle, qui redéfinit progressivement la manière dont la sécurité est pensée et pilotée. Elle suppose de relier les vulnérabilités aux conditions d'accès, aux dépendances métiers et aux chaînes d'attaque possibles. Elle implique également d'intégrer une réalité opérationnelle souvent sous-estimée. Toutes les vulnérabilités ne seront pas corrigées immédiatement, et la recherche d'exhaustivité peut elle-même devenir contre-productive si elle détourne l'attention des risques les plus exposés.

Le débat sur les vulnérabilités ne disparaît pas, il se déplace. Dans un environnement où la découverte devient toujours plus rapide et où les capacités d'exploitation s'intensifient, la question n'est plus uniquement celle de la visibilité.

Elle est celle de la capacité à transformer cette visibilité en décisions éclairées et actionnables. C'est dans cette bascule, plus que dans l'accumulation de nouvelles failles, que se joue désormais une part essentielle de l'efficacité des stratégies de cybersécurité.



Hervé Schauer Sécurité

Formation Continuité et résilience Protection des données Droit de la cybersécurité

PROGRAMME

Continuité et résilience

RPCA

Formation Responsable Continuité d'Activité

ISO22LA

ISO22301 Lead Auditor

ISO22LI

ISO22301 Lead Implementer

SECUCRISE

Gestion de crise cyber

Protection des données

RGPD

Fondamentaux de la protection des données

DPO

Métier du DPO

CERTIFDPO

Préparation à la certification AFNOR Certification agréé CNIL

PIA

Étude d'impact sur la vie privée

SECUSANTE

Hébergement et protection des données de santé

Droit de la Cybersécurité

SECUDROIT

Droit de la cybersécurité

SECUCLOUD

Contractualisation cloud

+ 33 974 774 390

MYRIAM
QUÉMÉNER

*Magistrat honoraire
& Docteur en droit*



VULNÉRABILITÉS ET CYBERSÉCURITÉ

Face à l'explosion des cyberattaques récentes qui visent désormais le domaine étatique y compris régalien, le sujet de la cybersécurité est essentiel et va de pair avec la recherche de vulnérabilités. Après les avoir définies au regard d'une actualité aigüe liée au recours croissant à l'intelligence artificielle, il conviendra de présenter les solutions envisagées associant bien sûr l'intelligence artificielle (IA) sans pour autant exclure l'humain, condition indispensable d'un écosystème de cybersécurité éthique et responsable.

DÉFINITIONS ET ACTUALITÉ DES VULNÉRABILITÉS

Selon l'ANSSI¹, les vulnérabilités sont des failles de sécurité pouvant affecter un logiciel, un système d'information ou encore un composant matériel. Elle peut servir de porte d'entrée pour des acteurs malveillants s'ils parviennent à l'exploiter. Les vulnérabilités dans le domaine cyber peuvent être d'origine humaine ou technique et exposent les entreprises ou organisations à des violations ou fuite de données, des interruptions de service ou des pertes de données.

On assiste aujourd'hui à une explosion des vulnérabilités, et le volume de cyberattaques informatiques poursuit sa progression, confirmant une pression cyber

durable et structurelle. on constate l'industrialisation du cybercrime, l'usage massif de l'intelligence artificielle, la recherche de failles dans les chaînes d'approvisionnement numériques ou encore la capacité à mêler ciblage numérique et menaces physiques constituent des défis majeurs pour notre sécurité collective².

L'actualité cyber française a été récemment secouée par des incidents majeurs comme la cyberattaque visant l'Agence nationale des titres sécurisés (ANTS a subi une intrusion informatique. Cette cyberattaque massive a visé environ 11,7 millions de citoyens ce qui met en évidence l'ampleur du fléau. Régulièrement, la plateforme cybermalveillance .gouv.fr publie également des alertes sur les failles de sécurité³.

>>>

>>> Par ailleurs le développement de la technologie quantique risque d'ouvrir de nouveaux espaces de vulnérabilité qu'il convient d'anticiper ainsi que le souligne le récent rapport du ministère de l'intérieur sur la cybercriminalité⁴. En effet, les ordinateurs quantiques peuvent compromettre des mécanismes de chiffrement actuellement déployés et ainsi ouvrir la voie à de nouvelles vulnérabilités.

De plus un groupe présumé lié à des intérêts étatiques aurait utilisé une version altérée de l'outil Claude Code pour mener des intrusions contre plusieurs dizaines de cibles, incluant des entreprises technologiques, des institutions financières et gouvernementales. L'IA aurait exécuté de manière autonome la majorité des phases de l'attaque (reconnaissance, exploitation, collecte d'identifiants et exfiltration de données), l'intervention humaine se limitant essentiellement à la supervision générale. C'est Anthropic qui a révélé avoir détecté et neutralisé cette campagne de cyberattaques, reposant sur l'utilisation détournée d'un agent d'IA configuré en mode autonome. Ainsi que l'indique le rapport du ministère de l'Intérieur. « *l'IA n'est plus seulement un outil d'assistance, mais devient un acteur opérationnel de la menace*⁵ ».

LES RÉPONSES JURIDIQUES

La loi n° 88-19 du 5 janv. 1988 relative à la fraude informatique⁶ dite loi Godfrain réprime les auteurs commettant volontairement des vulnérabilités sous forme de piratage informatique.

En ce qui concerne le signalement de vulnérabilités l'article L. 2321-4 du code de la défense prévoit que : Pour les besoins de la sécurité des systèmes d'information,

l'obligation prévue à l'article 40 du Code de procédure pénale n'est pas applicable à l'égard d'une personne de bonne foi comme le hacker blanc par exemple⁷ qui transmet à la seule autorité nationale de sécurité des systèmes d'information⁸, une information sur l'existence d'une vulnérabilité concernant la sécurité d'un système de traitement automatisé de données.

Au niveau de l'IA, le règlement européen sur l'IA (AI Act) impose une approche par les risques et met l'accent sur la sécurité, la transparence et la robustesse des systèmes. Les organisations doivent désormais intégrer la cybersécurité dès la conception des solutions d'IA (« security by design »).

PERSPECTIVES ACTUELLES

Une commission d'enquête sur les dépendances structurelles et les vulnérabilités systémiques dans le secteur du numérique et les risques pour l'indépendance de la France⁹ créée le 3 février 2026, est chargée de mesurer les dépendances des acteurs aux solutions numériques extra-européennes ; elle doit aussi évaluer la protection ou la vulnérabilité des données sensibles ; et examiner dans quelle mesure des solutions françaises ou européennes peuvent constituer des alternatives.

Au niveau de la cybersécurité, l'IA agit à la fois comme catalyseur de vulnérabilités, outil d'attaque et levier de défense. Cette dualité impose une approche globale, mêlant technologies avancées, gouvernance rigoureuse et vigilance humaine. La cybersécurité de demain ne reposera pas uniquement sur la puissance des algorithmes, mais sur la capacité des hommes à maîtriser, encadrer et comprendre les systèmes d'IA qu'elles déploient. ■

**On assiste aujourd'hui à une explosion des vulnérabilités,
et le volume de cyberattaques informatiques
poursuit sa progression, confirmant une pression cyber
durable et structurelle**

¹ <https://gouv.fr/cyberdico>

² Voir rapport annuel 2026 sur la cybercriminalité, site du ministère de l'intérieur

³ <https://cybermalveillance.gouv.fr/alerte-cyber-faille-de-securite>

⁴ Rapport annuel sur la cybercriminalité 2026, page 54

⁵ Rapport sur la cybercriminalité 2026, page 57

⁶ JO 6 janv., p. 231.

⁷ M. Quémener, A. Köcke, Hacker éthique et cybersécurité, Lextenso 2025

⁸ L'ANSSI

⁹ <https://www.assemblee-nationale.gouv.fr>


 LOÏC
GUÉZO

*VP Clusif et
CoAnimateur GT Panocrim
+ Sr Director Cybersecurity
Strategy, Proofpoint +
Consultant GS Mag
et membre du Comité de
Programme des GS Days*

LES VULNÉRABILITÉS & LA CYBERSÉCURITÉ

■ ■ **GS MAG :** Selon vous, quels sont les défis la Cybersécurité face aux Vulnérabilités ?

■ ■ **LG :** Le défi majeur est la compression du temps entre la découverte d'une vulnérabilité et son exploitation offensive. L'IA de pointe (aka, Frontier AI Model), comme Claude Mythos d'Anthropic, a changé l'équation : ce qui prenait des jours aux attaquants se compte désormais en heures. Cette accélération crée un nouveau paradigme puisque le cycle de correction, bien qu'essentiel, n'est plus assez rapide, structurellement, pour servir de référence temporelle à la qualité de la défense.

La vraie question pour les RSSI n'est donc plus « à quelle vitesse corrigeons-nous ? » mais « comment sommes-nous protégés avant-même de pouvoir corriger ? » L'enjeu n'est pas tant la visibilité sur les vulnérabilités que la réduction d'exposition dans la fenêtre temporelle de l'attaquant, finalement armé de 0-days multiples. Finalement la question est désormais « comment sommes-nous protégés de cette exploitation ? »

Second défi : l'extension de la surface d'attaque bien au-delà des vulnérabilités techniques. La majorité des attaques efficaces commençaient déjà par les

personnes, via l'ingénierie sociale, l'hameçonnage ciblé et la compromission de comptes, que l'IA rend désormais plus convaincants, ciblés et paradoxalement massivement déployables avec ces qualités. S'ajoutent l'apparition dans le SI des agents IA et des interfaces avec l'écosystème de fournisseurs qui élargissent encore les points d'entrée. La faille est chez un partenaire, mais l'impact est chez vous.

Le problème actuel est simple : les équipes de sécurité sont submergées par le volume de découvertes critiques.

Le défi majeur est la compression du temps entre la découverte d'une vulnérabilité et son exploitation offensive.

>>> ■■ **GS MAG** : Quelles sont les stratégies et tactiques que vous avez appliquées, les solutions que vous avez mises en place ou que vous conseillez de mettre en place, pour la gestion des Vulnérabilités ? Et pour quelles raisons ?

■■ **LG** : Chez Proofpoint, nous avons développé une nouvelle approche répondant à cette nouvelle temporalité.

L'adaptation repose sur un principe fondamental : il existe désormais deux horloges de sécurité distinctes. La première est celle de la remédiation, essentielle et gouvernée, qui suit les cycles de correction et de conformité. La seconde est celle de la protection adaptative, qui doit opérer à la vitesse de l'attaquant. Les deux sont indispensables, mais seule la seconde réduit l'exposition pendant que la première fera son travail, à son rythme.

Notre offre Proofpoint Active Exploit Defense comble le fossé entre la vitesse des attaques pilotées par l'IA et la capacité de réaction des équipes de sécurité.

La solution transforme une threat intelligence riche et mondiale en protection immédiate et actionnable, en priorisant uniquement les vulnérabilités réellement exploitées dans le monde réel et non les risques théoriques.

Cette threat intelligence est alimentée par un vaste réseau de collecte et d'analyse.

■■ **GS MAG** : Comment allez-vous vous adapter aux évolutions permanentes des Directives, Règlements, Lois de transposition, et des Technologies ? (IA ? Quantique ? Post-Quantique)

■■ **LG** : Nos plateformes suivent toutes les évolutions techniques structurantes (comme la migration vers du chiffrement post-quantique) et l'IA qui est désormais centrale, avec des adaptations permanentes de nos modèles.

Dans un monde où une faille devient une arme de prolifération numérique massive en quelques minutes, cette agilité technique n'est plus optionnelle, elle est vitale.

À noter que le 6 mai 2026, nous avons inauguré notre nouveau hub européen d'Innovation à Paris, renforçant ainsi notre R&D régionale, pour faire progresser l'innovation en sécurité IA et approfondir notre engagement envers les clients et partenaires européens, et donc de facto parfaitement intégré au cadre réglementaire européen. ■

CHIFFRES CLÉS :

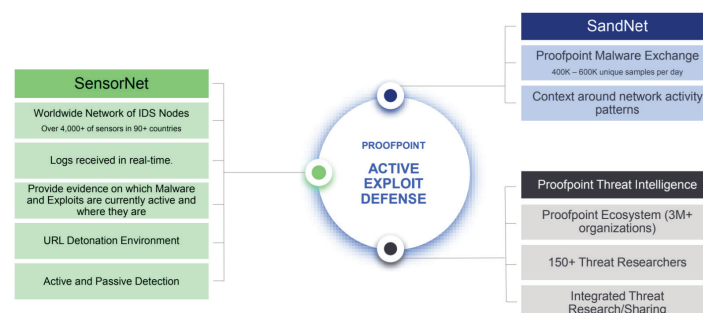
- **4 000+ capteurs** dans 90+ pays (SensorNet) avec des données en temps réel, provenant d'ISP majeurs
- **400K à 600K échantillons de malware/jour** analysés (SandNet)
- **3+ millions d'organisations** contribuant à l'écosystème
- **150+ chercheurs** en sécurité

Cette combinaison unique permet d'identifier précisément quels exploits sont réellement actifs, où et comment, en croisant détection réseau, analyse malware et recherche en cybersécurité.

Le résultat est simple : une visibilité inégalée sur les menaces actives pour une protection rapide et ciblée.

Concrètement ce n'est pas foncièrement une nouvelle donnée, c'est une nouvelle façon d'agir - plus rapide, plus ciblée - donc plus efficace face aux menaces actives.

Rich Threat Intelligence from an Expansive Network



L'ESPRIT D'ÉCHANGE.

REJOIGNEZ-NOUS
ET CONTRIBUEZ À L'ENSEMBLE
DE NOS ACTIVITÉS:



Le Panorama
de la cybercriminalité



Les conférences
sur les thématiques
de l'écosystème



Les groupes de travail
et leurs publications

Le Clusif est l'association de référence de la
cybersécurité en France.

Reconnue d'utilité publique par l'État,
sa mission consiste à favoriser les échanges
d'idées et de retour d'expérience.

www.clusif.fr



A portrait of Séverine Meunier, a woman with blonde hair, wearing a dark top with a white collar. The background is dark and out of focus.

SÉVERINE
MEUNIER

*Experte en Sécurité
Numérique et
Intelligence Appliquée*

L'ÈRE DES VULNÉRABILITÉS AUTONOMES : QUAND L'IA REDÉFINIT L'ÉQUILIBRE OFFENSIF-DÉFENSIF DU CYBERESPACE

LE PARADIGME BRISÉ DE LA “SÉCURITÉ PAR L'OBSCURITÉ”

Pendant des décennies, la cybersécurité a reposé sur un postulat implicite : la complexité des systèmes constitue en elle-même une forme de protection. Un attaquant — même compétent — devait mobiliser un temps considérable, des ressources spécialisées et une connaissance fine de l'architecture cible pour identifier une faille exploitable. Ce coût d'entrée élevé fonctionnait comme un filtre naturel. Il réservait les attaques sophistiquées à un nombre restreint d'acteurs : États-nations dotés de capacités offensives cyber, groupes APT (Advanced Persistent Threats) financés par des puissances étrangères, et une poignée d'organisations criminelles structurées.

CE PARADIGME EST CADUC

En avril 2026, Anthropic a publié les résultats de ses tests internes sur Claude Mythos Preview, son modèle le plus avancé à ce jour. Le constat est sans précédent dans

l'histoire de l'industrie : le modèle a identifié des milliers de vulnérabilités zero-day inconnues dans l'ensemble des systèmes d'exploitation majeurs et dans tous les navigateurs web courants — des failles ayant survécu à des décennies de revue humaine et à des millions de tests automatisés. Il a développé des exploits fonctionnels dès la première tentative dans plus de 83% des cas. Parmi les cas documentés : une vulnérabilité vieille de 27 ans dans OpenBSD, système réputé pour sa robustesse sécuritaire, et 271 failles identifiées et corrigées dans Firefox en phase de test préliminaire avec Mozilla.

Ces chiffres ne sont pas simplement impressionnants. Ils signalent une rupture de nature qualitative, pas seulement quantitative.

Zero-days, exploit chains et automatisation : la nouvelle grammaire de l'attaque

Pour saisir l'ampleur du changement, il faut comprendre ce que représente techniquement un zero-day. Il s'agit d'une vulnérabilité inconnue du vendeur du logiciel, donc non corrigée (unpatched), et par définition sans signature dans les bases de détection existantes. La découverte

d'un zero-day exploitable dans un système critique — noyau d'OS, pile réseau, moteur de rendu d'un navigateur — représente traditionnellement plusieurs semaines à plusieurs mois de travail pour une équipe d'experts. La valeur marchande de tels artefacts sur les marchés spécialisés (légaux ou illégaux) se chiffre en centaines de milliers, voire en millions de dollars.

Ce que Mythos a introduit, c'est l'industrialisation de cette découverte. Des ingénieurs d'Anthropic sans formation formelle en sécurité pouvaient demander au modèle de trouver des vulnérabilités d'exécution de code à distance pendant la nuit, et se réveiller le lendemain matin avec un exploit complet et fonctionnel.

Mais la capacité de découverte n'est que le premier niveau du problème. Ce qui distingue Mythos des outils d'analyse statique ou de fuzzing classiques, c'est sa capacité à chaîner les vulnérabilités. Le modèle identifie d'abord une faille zero-day, puis l'arme en la reliant à d'autres vulnérabilités, pouvant demeurer indétecté indéfiniment et exécuter une prise de contrôle totale du système par la construction de ces "chaînes d'exploit". C'est précisément cette capacité de chaining autonome qui représente le saut qualitatif : jusqu'ici, l'assemblage d'une chaîne d'exploitation complexe nécessitait une expertise humaine irremplaçable. Ce n'est plus le cas.

Le lauréat du Prix Turing Yoshua Bengio a qualifié ce moment de franchissement d'un seuil inédit : des IA avancées découvrent pour la première fois un grand nombre de zero-days inconnus, exploitables pour attaquer les infrastructures critiques mondiales — systèmes bancaires, réseaux gouvernementaux, aéroports, hôpitaux, réseaux d'énergie et de communication.

LA DISSYMMÉTRIE FONDAMENTALE : POURQUOI L'OFFENSE GAGNE STRUCTURELLEMENT

La cybersécurité repose sur une dissymétrie bien connue des praticiens : l'attaquant n'a besoin de réussir qu'une seule fois ; le défenseur doit réussir à chaque tentative. Cette réalité asymétrique s'est toujours traduite par un avantage structurel à l'offense. L'IA autonome capable de découvrir et chaîner des zero-days amplifie cet avantage de manière exponentielle.

TROIS DYNAMIQUES CONVERGENT POUR AGGRAVER LE DÉSÉQUILIBRE

Premièrement, la dette technique des infrastructures critiques. De nombreuses infrastructures opérationnelles dans les secteurs de l'énergie, des transports, de l'eau et de la production industrielle reposent sur des systèmes

vieux de plusieurs décennies, impossibles à patcher efficacement en raison de contraintes d'interopérabilité et du risque de défaillances en cascade. Ces systèmes ont été conçus dans un contexte où la connectivité n'était pas un vecteur d'attaque — ils ne peuvent pas être sécurisés par des mises à jour logicielles conventionnelles sans risquer l'arrêt de l'infrastructure elle-même.

Deuxièmement, la pénurie structurelle de compétences. Le déficit mondial de professionnels en cybersécurité est estimé à plusieurs millions de postes non pourvus. Cette pénurie, déjà critique, est aggravée par l'accélération technologique. Les cyberattaques pilotées par IA ont augmenté de 89% en 2025 par rapport à l'année précédente selon CrowdStrike, armant même des acteurs criminels peu qualifiés des moyens de cibler des entreprises, des individus et des infrastructures nationales plus facilement et à moindre coût qu'auparavant.

Troisièmement, le paradoxe de la prolifération défensive. La réponse d'Anthropic — concentrer l'accès à Mythos dans un consortium défensif privé baptisé Project Glasswing — soulève une question épineuse : les capacités offensives de Mythos sont-elles réellement cantonnables à ce cadre ? Le modèle a déjà fait l'objet d'un accès non autorisé par un tiers, via une faille de sécurité qui avait exposé des informations le concernant dans une base de données publiquement accessible. Le modèle censé protéger le monde a lui-même été compromis avant sa mise en service généralisée — une ironie lourde de sens sur la robustesse des périmètres de contrôle

LA FRACTURE DE GOUVERNANCE : QUI PROTÈGE QUI, ET SELON QUELLES RÈGLES ?

C'est ici que l'angle différenciant s'impose. La plupart des analyses se concentrent sur les capacités techniques de Mythos. Elles négligent la dimension de gouvernance — pourtant centrale — que révèle cette affaire.

Project Glasswing regroupe environ quarante entités : Amazon, Apple, Google, Microsoft, Cisco, CrowdStrike, JPMorgan Chase, Nvidia. Ce périmètre n'inclut pas la plupart des banques centrales et gouvernements du monde, laissant une grande partie de la planète vulnérable et dépendante de ces mêmes entreprises privées pour la sécurisation de leurs systèmes. Ce constat mérite d'être formulé sans détour : une entreprise privée américaine décide unilatéralement, par ses choix d'accès à un outil défensif, quels États et quelles populations entrent dans le périmètre de sécurité numérique mondiale — et lesquels en sont exclus. Il n'existe aucun précédent historique de cette nature dans la gestion des risques systémiques globaux, ni dans le nucléaire civil, ni dans la sécurité sanitaire internationale.

>>>

Zero-days, exploit chains et automatisation : la nouvelle grammaire de l'attaque

>>> 87% des organisations mondiales auraient subi une cyberattaque alimentée par l'IA au cours de la dernière année. Combler l'écart d'investissement nécessaire exigerait de doubler les budgets cybersécurité, alors que la plupart des organisations prévoient des hausses annuelles de l'ordre de 10% seulement. Dans ce contexte, les acteurs les moins dotés — petits États, institutions publiques, économies émergentes — n'ont aucune capacité réaliste d'atteindre seuls un niveau de défense suffisant.

L'interconnexion du système numérique mondial signifie que laisser des institutions et des nations vulnérables expose l'ensemble du système aux effets de contagion d'une brèche. La sécurité est un bien collectif indivisible, mais les outils pour la produire sont traités comme des actifs privés exclusifs.

LA NUANCE TECHNIQUE : LE MONOPOLE DE LA PUISSANCE EST-IL RÉEL ?

Il serait intellectuellement malhonnête d'ignorer les voix qui tempèrent le récit dominant. La startup AISLE, spécialisée en sécurité IA, publiait en avril 2026 une analyse critique : lorsqu'elle a testé les vulnérabilités "vitrine" de Mythos sur des modèles open-source petits et peu coûteux, la plupart ont trouvé les mêmes failles. La capacité de découverte de vulnérabilités est aujourd'hui largement accessible, et le cadrage d'Anthropic surestime peut-être le caractère exclusif de ces aptitudes.

L'évaluation du UK AI Security Institute (AISi), qui avait obtenu un accès anticipé, a conclu que le modèle réussissait des tâches de hacking de niveau expert dans 73% des cas — mais dans des conditions de test quasi dépourvues des protections présentes dans les environnements réels.

Ces nuances sont importantes. Elles suggèrent que l'exclusivité des capacités offensives de Mythos est peut-être plus relative que le récit d'Anthropic ne le laisse entendre.

Ce qui, paradoxalement, aggrave le problème de gouvernance : si des capacités comparables sont accessibles via des modèles open-source peu coûteux, le contrôle d'accès au seul Mythos Preview ne constitue qu'un rempart partiel et transitoire.

CONCLUSION PROSPECTIVE : DEUX FUTURS POSSIBLES

Le futur de la fragmentation. Si la trajectoire actuelle se maintient, le cyberspace se stratifie en zones de sécurité radicalement inégales. Les membres du consortium Glasswing et leurs écosystèmes — essentiellement les grandes entreprises technologiques, les institutions financières de premier rang et quelques États alliés — bénéficient d'une protection de niveau inédit. Le reste du monde, incluant une partie significative des administrations publiques européennes non intégrées à ces dispositifs, navigue à découvert dans un environnement où les capacités offensives automatisées se démocratisent pendant que les défenses restent concentrées. Le terme "AI bugocalypse", déjà circulant dans la presse spécialisée, désigne ce scénario : une vague massive d'exploitation automatisée de vulnérabilités systémiques, frappant en priorité les maillons les plus faibles d'une chaîne numérique globale.

Le futur de la régulation par le choc. L'affaire Mythos pourrait aussi jouer le rôle de catalyseur qu'a joué Tchernobyl pour la sécurité nucléaire internationale : un événement suffisamment brutal pour forcer une réponse institutionnelle coordonnée. L'Europe dispose ici d'une position singulière. Avec l'AI Act, la directive NIS2, et une culture réglementaire fondée sur la souveraineté des données et la proportionnalité des risques, elle est la seule juridiction capable d'imposer des standards contraignants sur les modèles IA à double usage offensif/défensif. Cela supposerait de traiter ces modèles non comme des produits technologiques ordinaires, mais comme des infrastructures critiques relevant du droit international — avec des obligations de partage d'accès défensif, de transparence sur les vulnérabilités découvertes, et de coopération entre États.

Ce cadre n'existe pas encore. Le construire avant que le prochain Mythos — plus puissant, moins contrôlé, peut-être open-source — ne soit disponible représente sans doute l'un des défis de gouvernance les plus urgents de la décennie.

La vraie question que pose Mythos n'est pas "l'IA peut-elle hacker nos systèmes ?" La réponse est désormais connue. La question est : "Qui décide des règles d'un monde où cette capacité existe ?" Et pour l'instant, la réponse par défaut est : personne. ■

GÉNÉRAL DE BRIGADE HERVÉ PÉTRY

*Commandant de l'Unité
Nationale Cyber
(UNCYBER)*



LES VULNÉRABILITÉS & LA CYBERSÉCURITÉ

■ ■ GS MAG : *Bonjour mon Général, pouvez-vous vous présenter et nous dire comment votre parcours vous a amené à votre rôle actuel ?*

■ ■ UNCYBER & G.HP : Je suis un officier général de la gendarmerie qui totalise près de 30 ans de service. Après une première partie de carrière où j'ai exercé des responsabilités de commandement, d'abord en gendarmerie mobile comme Lieutenant, puis en gendarmerie départementale comme Capitaine, je me suis orienté à l'issue de mon temps d'état-major à la Direction générale de la gendarmerie nationale et de l'école de guerre dans la filière internationale comme attaché de sécurité intérieure adjoint en Chine (Pékin) puis dans la filière de la police judiciaire. À mon retour en métropole, j'ai successivement commandé la section de recherches de Lyon puis la coordination nationale des groupes interministériels de recherches au sein de la DCPJ à Nanterre. Ce parcours m'a ensuite conduit à servir comme commandant en second du service central du renseignement criminel puis de prendre la tête de l'unité nationale cyber, poste que j'occupe depuis plus de deux ans.

■ ■ GS MAG : *Pouvez-vous nous présenter UNCYBER, ses objectifs, ses actions, l'évolution des cyberattaques ?*

■ ■ UNCYBER & G.HP : L'Unité nationale cyber (UNC), héritière du ComcyberGend, est le bras armé de la Gendarmerie contre la cybercriminalité.

Unités de police judiciaire, l'UNC et ses 26 Antennes régionales et ultramarines prennent en compte des opérations qui demandent des capacités ou des personnels dont ne disposent pas les échelons territoriaux. Pour ce faire, l'UNC se compose de quelque 120 personnels répartis dans trois composantes :

- L'investigation cyber thématique, qui lutte entre autres contre la pédocriminalité, les cyberattaques, les trafics et les escroqueries en ligne (armes, drogue, criminalité économique) ;
- L'appui technique opérationnel, qui prend la forme de développements logiciels et d'une capacité de projection 24/7 partout en métropole et outre-mer pour appuyer les unités locales dans le cadre des investigations numériques et des perquisitions sensibles ;

>>>

- >>> • Le renseignement dans ses diverses disciplines : traitement de sources humaines, renseignement ouvert ou technique, traitement de données...

Par ailleurs, l'UNC est le chef de file de la filière cyber de la gendarmerie nationale. Il anime à ce titre le réseau cyberGend dont la base territoriale se compose de plus de 10 000 cyber-gendarmes aptes à réaliser des actes simples comme la prise de plainte, le gel de la preuve numérique, l'extraction des données et l'exploitation téléphonique. Leur action est complétée par celle de quelque 2500 cyber-enquêteurs spécialisés dans des domaines comme l'enquête sous pseudonyme, l'investigation sur les actifs numériques ou encore la forensique numérique complexe.

Les objectifs de l'unité sont actuellement d'apporter des réponses aux phénomènes les plus graves qui impactent actuellement le pays : les plateformes criminelles, les fuites de données, les crypto-rapts...

■ ■ **GS MAG** : *Selon vous, quels sont les défis de la Cybersécurité face aux Vulnérabilités ? Quelle est l'influence de l'IA ?*

■ ■ **UNCYBER & G.HP** : On constate la persistance d'un manque de prise de conscience chez certains acteurs. La cybersécurité n'est plus une option et la menace ne concerne pas que les OIV et les grands groupes. Ces « cibles dures » sont blindées, conseillées, disposent des meilleurs spécialistes. Il est aujourd'hui plus rentable et moins risqué pour un groupe criminel de cibler une petite PME. Nous sommes donc tous concernés.

En second lieu, la France est l'un des pays les plus touchés au monde par les fuites de données rapportée à sa population. Ces fuites offrent malheureusement aux criminels une capacité de ciblage de leurs potentielles victimes.

L'IA constitue un vecteur démultiplicateur de ces capacités, même si on ne dessine pour l'heure que des effets encore limités. Certains partenaires nous remontent cependant des cyberattaques générées par IA qui peuvent être plus rapides, massives et efficaces que ce que l'on connaît jusque-là. Son impact le plus visible demeure pour l'heure en France dans le domaine des cyber-escroqueries. Les faux mails, les faux appels... le courrier couvert de fautes des années 2010 a cédé sa place à une génération par IA qui a toute l'apparence du vrai et permet de crédibiliser les escroqueries et donc d'accroître le nombre de victimes.

■ ■ **GS MAG** : *Quels seraient vos messages à nos lectrices et lecteurs qui font partie de l'écosystème Cyber ?*

■ ■ **UNCYBER & G.HP** : L'état de la menace évolue : si les atteintes aux systèmes de traitement automatisés de données (ASTAD) sont toujours aussi nombreuses, nous assistons actuellement à ce que j'appelle « une cybérisation » de la criminalité. Celle-ci se développe à grande vitesse. Elle voit converger notamment deux univers qui jusque-là étaient clairement séparés : celui des hackers, d'une part et celui des groupes criminels organisés, d'autre part. La porosité croissante entre ces deux mondes est à l'origine de cette évolution rapide où les hackers jouent un rôle croissant, soit comme fournisseurs de données, soit directement comme commanditaire.

Face à cette évolution, la gendarmerie s'est mise en ordre de bataille : d'abord en termes de formation, afin qu'un plus grand nombre de ses cyber-enquêteurs, dont le nombre sera multiplié par 3.5 d'ici à 2030 pour atteindre le chiffre, soit en capacité de traiter aussi bien les ASTAD que tous les trafics et escroqueries en ligne qui connaissent une très forte croissance ; ensuite en termes de renseignement car pour être efficace en police judiciaire il faut être capable d'anticiper les menaces et pour cela de les détecter en amont et en profondeur afin, au mieux, d'empêcher la commission des infractions, et au pire de les faire cesser.

Toutefois, la gendarmerie ni la Justice ne peuvent pas à elles seules régler ce problème sans une participation active de la population qui doit élever sa posture de cybersécurité. C'est tout l'enjeu de la prévention et des comportements personnels qui doivent passer par une prise de conscience individuelle et collective. ■

L'Unité nationale cyber (UNC), héritière du ComcyberGend, est le bras armé de la Gendarmerie contre la cybercriminalité.



L'Unité Nationale cyber (UNCyber) est au sein de l'Unité Nationale de Police Judiciaire (UNPJ), le bras armé opérationnel de la Gendarmerie Nationale dans le cyberspace.

Unité de police judiciaire à compétence nationale, l'UNCyber conduit les enquêtes de haut spectre en matière de cybercriminalité. Elle coordonne l'action des 26 antennes UNCyber et des 10 000 gendarmes qui composent le dispositif Cybergend, constituant ainsi son allonge dans les territoires métropolitains mais aussi ultra-marins.

SES TROIS MISSIONS PRINCIPALES SONT :

- Le renseignement ;
- l'investigation ;
- l'appui technique.

COMPOSÉE DE 120 PERSONNELS, L'UNCYBER COMPORTE TROIS DIVISIONS :

- **La Division de l'Animation Renseignement Coordination (DARC)**, qui fournit des appuis spécifiques : renseignement humain, renseignement technique, CERT-GN, coordination nationale et internationale...;
- **La Division des Opérations (DO)**, qui est en charge des enquêtes sur la cybercriminalité organisée de niveau national et international (pédocriminalité, rançongiciels, fraudes en ligne, trafics en ligne...) ;
- **La Division Technique (DT)** qui assure l'appui technique et criminalistique, par ses capacités projetables au profit de l'échelon local et ses outils d'analyse de la donnée.

L'UNCyber est commandée depuis le 1er février 2024 par le général Hervé PETRY.



FRANCK
ROUXEL

*Expert en cybersécurité
Founder Klaerenn & CISO*

QUATRE VULNÉRABILITÉS POUR UN SEUL MOT

LE MÉTIER CYBER EMPLOIE UN TERME STABLE DEPUIS VINGT-CINQ ANS POUR DÉSIGNER UNE RÉALITÉ QUI S'EST DÉDOUBLÉE PLUSIEURS FOIS. LA GRAMMAIRE TIENT. CE QU'ELLE NOMME A CHANGÉ.

Le 15 avril 2026, le NIST a annoncé qu'il cessait d'enrichir l'ensemble des vulnérabilités soumises au National Vulnerability Database. Trois critères américano-centrés filtreront désormais ce qui sera analysé. Le reste sera publié, classé en attente, sans contexte ni score indépendant. Le Forum of Incident Response and Security Teams prévoit le franchissement des cinquante mille CVE annuels en 2026. L'institution qui structure la connaissance mondiale des vulnérabilités a admis qu'elle ne peut plus suivre, et qu'elle privilégiera désormais les intérêts opérationnels du gouvernement fédéral américain. L'événement a circulé dans les cercles spécialisés sans susciter de réaction proportionnée. Il signe pourtant la fin d'un arrangement de vingt-cinq ans, et oblige à reformuler ce que le métier appelle vulnérabilité.

La première lecture du mot reste familière. Une faiblesse identifiée par un CVE, scorée par un CVSS, corrigée par un patch dans un délai mesurable. La discipline est rodée, les outils en place, les équipes formées. Cette définition héritée structure encore le quotidien des SOC, l'écriture des règles SIEM, la rédaction des contrats fournisseurs et la formulation des obligations réglementaires. Le retrait du NIST ne change pas cette couche immédiatement, il en change l'environnement. Le scanner européen consomme passivement les sorties d'un service public américain qui vient d'arrêter de produire pour tout le monde. Quatre-vingt-cinq pour cent des solutions de sécurité déployées en Europe dépendent de ces données. La donnée brute reste accessible, l'analyse contextuelle disparaît. Le score CVSS continue d'être

Formuler ses propres règles, ses propres priorités de patch, ses propres mesures de défense, sans déléguer à un dictionnaire qui ne sera plus tenu à jour pour soi

attribué, mais par les éditeurs eux-mêmes, sans arbitrage indépendant. Le métier conserve la grammaire et perd le dictionnaire.

Une seconde lecture du même mot apparaît dès qu'on sort du composant logiciel. La vulnérabilité devient celle de la chaîne de production, de qualification et de diffusion de la connaissance défensive. Les standards techniques de DORA renvoient au Cybersecurity Framework du NIST. Plusieurs transpositions nationales de NIS2 référencent les mêmes standards américains. La certification de référence des analystes européens teste explicitement la maîtrise des frameworks NIST dans son socle d'examen. Cette dépendance est apparue comme vulnérabilité quand le propriétaire du langage commun a commencé à le retirer. Le contrat fédéral du programme CVE a failli expirer en avril 2025 avant une prolongation in extremis. L'institut de référence n'a plus de directeur confirmé depuis janvier 2025. La gratuité du langage commun n'était jamais qu'un arrangement entre alliés, et cet arrangement vient de prendre fin.

LES INDICATEURS CESSENT D'INDIQUER

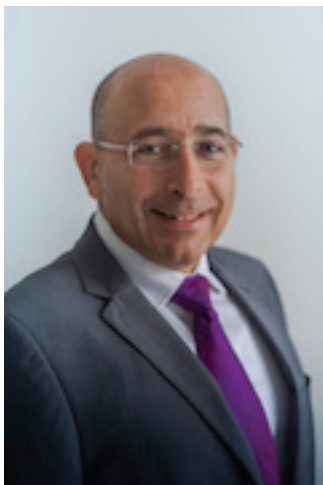
Une troisième lecture met en cause les outils par lesquels le métier mesurait sa propre posture. La couverture moyenne d'ATT&CK dans les SIEM en production, mesurée en 2025 sur 2,5 millions de sources de logs, atteint vingt-et-un pour cent de la matrice. Cinq ans de mesure, pas de progression. Le framework défensif jumeau, construit sur cinq cents brevets américains, n'a jamais établi de mesure d'effectivité. Le framework dédié aux systèmes IA, testé sur le premier outil agentique majeur, donne dix-sept pour cent de défense moyenne. Quand la première vraie menace IA d'ampleur émerge, ce framework n'est mentionné par aucun acteur officiel. La vulnérabilité, à ce niveau, porte sur ce que le métier croit voir parce

que des dashboards verts le lui affirment. Scores de couverture, pourcentages de règles déployées, catalogues de techniques produisent la sensation d'une défense lisible. Cette lisibilité est devenue indépendante de la défense effective.

Une quatrième lecture s'est imposée en avril 2026. Claude Mythos Preview, modèle de frontière publié par Anthropic, a découvert plusieurs milliers de vulnérabilités haute et critique dans les systèmes d'exploitation et navigateurs majeurs, et exploité de façon entièrement autonome un zero-day vieux de dix-sept ans dans FreeBSD. Le même mois, une étude empirique sur deux cent cinquante-neuf vulnérabilités Java a démontré que les bases publiques manquent près de huit cents versions vulnérables, et qu'un agent autonome peut désormais exécuter cette vérification empirique à l'échelle d'un dépôt entier. Le mot vulnérabilité désigne désormais aussi ce déséquilibre entre une production de failles passée à l'échelle industrielle et une capacité institutionnelle à les nommer qui se replie au même moment.

REFORMULER L'ANTIFRAGILITÉ

Quatre lectures, un seul mot. Et un CISO de 2026 qui doit tenir les quatre simultanément, sans école qui le forme, sans référentiel qui le mesure, sans certification qui le valide. La continuité de vocabulaire masque une discontinuité de réalité. L'antifragilité demande à être reformulée à son tour. Tant que la grammaire commune tenait, transformer la contrainte en avantage supposait un cadre partagé. Cette condition n'est plus garantie. La posture antifragile de 2026 commence par un travail moins visible : formuler ses propres règles, ses propres priorités de patch, ses propres mesures de défense, sans déléguer à un dictionnaire qui ne sera plus tenu à jour pour soi. Reste à savoir si la profession européenne saura organiser ce travail collectivement, ou si chaque organisation devra le mener pour elle seule. ■



David Ofer, Président



Fédération Française de la Cybersécurité

Fédérer • Représenter • Valoriser l'écosystème cyber français

Présentation de la Fédération Française de la Cybersécurité

La Fédération Française de la Cybersécurité, présidée par David Ofer, s'impose comme un acteur fédérateur et structurant de l'écosystème cyber en France. Elle regroupe des adhérents issus de tous les secteurs : ESN, éditeurs, intégrateurs, collectivités, associations professionnelles...

Son ambition est claire : structurer, accompagner et faire rayonner la cybersécurité française.

Une mission en trois axes : fédérer, structurer, faire rayonner

La Fédération Française de la Cybersécurité repose sur trois grands piliers d'action :

1. **Fédérer** : créer des ponts entre tous les acteurs du numérique – publics et privés, grands groupes et TPE, décideurs nationaux et collectivités locales – pour favoriser une réponse collective aux enjeux cyber.
2. **Structurer** : contribuer à la montée en maturité du tissu économique et institutionnel à travers des Notes Cyber, des publications de référence et des actions sectorielles ciblées (bâtiment, santé, IA, collectivités...).
3. **Faire rayonner** : accompagner l'essor de l'écosystème en valorisant les expertises françaises, en participant activement à de nombreux événements nationaux.

Des avantages concrets pour les adhérents

Adhérer à la Fédération Française de la Cybersécurité, c'est accéder à un ensemble de services à forte valeur ajoutée :

- **Intégration** à des groupes de travail sectoriels pour co-construire des propositions concrètes ;
- **Accès** à des webinaires spécialisés et à des événements confidentiels réunissant des décideurs de haut niveau ;
- **Participation** à la rédaction de Notes Cyber diffusées à l'écosystème et aux pouvoirs publics ;
- **Tarifs préférentiels** négociés sur les grands salons et événements partenaires ;
- **Visibilité renforcée** grâce à nos relais presse, newsletters, publications et interventions collectives ;
- **Opportunités** de prise de parole et de contribution lors de conférences, tables rondes ou ateliers organisés ou co-organisés par la Fédération.

contact@ffcybersecurite.org

www.ffcybersecurite.org

LinkedIn : Fédération française de la Cybersécurité



Abonnement Annuel CSE*

www.gsdays.fr • www.globalsecuritymag.com • www.globalsecuritymag.fr
www.globalsecuritymag.de

*La Cybersécurité étant devenue un sujet
sociétal, nous proposons que le CSE
participe à la sensibilisation trimestrielle
des effectifs*

TARIF

Cocher son choix

- | | |
|--------------------------|---|
| ☐ | ABONNEMENT ENTREPRISE AVEC UN EFFECTIF < 500 5000 €HT |
| | Limité à 499 exemplaires en papier par an / Illimité en numérique avec le bandeau au nom de l'Entreprise |
| ☐ | ABONNEMENT ENTREPRISE AVEC UN EFFECTIF > 500 < 10000 15000 €HT |
| | Limité à 2000 exemplaires en papier par an / Illimité en numérique avec le bandeau au nom de l'Entreprise |
| ☐ | ABONNEMENT ENTREPRISE AVEC UN EFFECTIF > 10000 30000 €HT |
| | Limité à 5000 exemplaires en papier par an / Illimité en numérique avec le bandeau au nom de l'Entreprise |

**Vous pouvez nous contacter pour les conditions de paiement,
07 89 65 15 70 • Valentin Jangwa • vj@globalsecuritymag.com**

*Tacite reconduction annuelle avec 1 mois de préavis.

*CSE = COMITE SOCIAL ET ECONOMIQUE





Future of IT

JEUDI

11

JUIN

2026

#FutureOfIT

LE SEUL ÉVÈNEMENT RÉUNISSANT LES DSI,
RSSI & CHIEF DATA OFFICERS

Journée Workshops & Networking

32 workshops interactifs répartis sur 4 rooms (IT -
Cyber - Data - J'innov Education)

Château Comet Levallois, 92300 Levallois-Perret

08h45 - 17h30

Soirée de Gala

Thématique: « Construire l'entreprise de demain
: vision stratégique, adoption à grande échelle et
importance du triptyque IT - Data - Cyber »

Pavillon Vendôme, 75001 Paris

18h00 - 23h45



www.futureOfIT.com

INSCRIPTION



À L'INITIATIVE DE



UN ÉVÈNEMENT





HS2

Hervé Schauer Sécurité



Formation cybersécurité organisationnelle

PROGRAMME

Gouvernance de la sécurité

RSSI / DIRCYBER
Formations RSSI et directeur cybersécurité
NIS2LI / DORALI
Mise en conformité NIS2 / DORA
EBIOSRM Risk Manager
Gestion des risques cyber par la méthode
EBIOSRM
SECUHOMOL
Homologation de la SSI

Gouvernance de la sécurité avec les normes ISO270XX

ESS27
Essentiels ISO27001 & ISO27002
ISO27LA
ISO27001 Lead Auditor
ISO27LI
ISO27001 Lead Implementer
ISO27RM
ISO27005 Risk Manager
ISO27004
ISO27004 / Indicateurs et tableaux de bord
cybersécurité
ISO27035
ISO27035 / Gestion des incidents de sécurité

Certifications internationales

CISSP / CCSP



CISM / CISA / CRISK



+ 33 974 774 390

www.hs2.fr

formation@hs2.fr

Cyber / AI expo

Cyber Security & AI

Redefining Digital Resilience

June 24, 2026

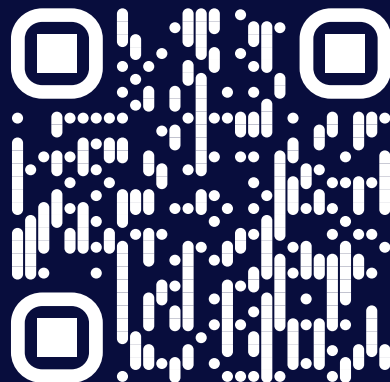
MUNICH, BMW Welt

Make AI-powered cybersecurity
a core part of your business.

Claim your free ticket with the code

GSM2026

First come, first served.



**Not all QR codes
are shady.**

This one leads to
Cyber / AI Expo
Munich.

cyberai-expo.de

A portrait of Etienne Capgras, a young man with dark hair, smiling. To the right of the portrait is a decorative graphic of overlapping squares in shades of gold and brown.

ETIENNE
CAPGRAS

*Learning Product Manager,
OpenClassrooms
Membre du groupe de travail
European Cybersecurity
Skills Framework, ENISA*

ECSF ET RECRUTEMENT PAR COMPÉTENCES : LA RECHERCHE DU MOUTON À CINQ PATTES ENFIN DERRIÈRE NOUS

**AVEC CETTE RUBRIQUE, NOUS VOUS PROPOSONS D'ANALYSER
LES ENJEUX DE CYBERSÉCURITÉ SOUS L'ANGLE DES
COMPÉTENCES : LES TENDANCES, LES RESSOURCES ET LES
BONNES PRATIQUES POUR FLUIDIFIER LE MARCHÉ DU TRAVAIL,
AU SERVICE D'ÉQUIPES PLUS FORTES ET PLUS RÉSILIENTES.**

L'article précédent mettait en lumière les biais qui grippent nos recrutements cyber : diplôme Bac+5 systématique, clonage de profils, réflexe du réseau, compétences au-cas-où. La réponse n'est pas d'abaisser les exigences, c'est de les préciser. Recruter par compétences, c'est exactement ça : définir ce qu'on cherche vraiment, sans passer par le filtre réducteur du diplôme. L'ECSF, European Cybersecurity Skills Framework, rend cette démarche enfin praticable.

>>>



Etienne Capgras est Learning Product Manager chez OpenClassrooms, où il développe l'offre de formation en cybersécurité. Il est également membre du groupe de travail ECSF de l'ENISA, qui vise à harmoniser les rôles et les compétences en cybersécurité à l'échelle européenne. Soucieux de rendre ces métiers accessibles au plus grand nombre, il défend ardemment le recrutement par compétences comme levier de lutte contre la pénurie de talents.

>>> LIBELLÉ DE POSTE ET ACTIVITÉS : UN POINT DE DÉPART SOLIDE MAIS INSUFFISANT

Avant même d'ouvrir un référentiel de compétences, vous disposez déjà d'une base solide. **Un libellé de poste** – "Analyste SOC", "Responsable conformité" – et, après quelques échanges avec les managers, futurs collègues et autres parties prenantes internes, **une liste d'activités à confier**. Ce point de départ est bien rodé, globalement mature sur le marché.

L'étape qui coince ? L'identification des compétences et connaissances sous-jacentes. Sans elle, on recycle les offres précédentes, on empile les compétences au-cas-où, on oublie des prérequis implicites... et on finit par rédiger une annonce qui décourage voire écarte les bons profils autant qu'elle attire les mauvais.

C'est ici que l'ECSF entre en jeu.

DES OFFRES PLUS PRÉCISES, ET ENFIN LISIBLES, GRÂCE À L'ECSF

■ ECSF : la pierre de Rosette des compétences cyber

Publié par l'ENISA en 2022, l'ECSF, **European Cybersecurity Skills Framework**, propose 12 profils de rôles, du RSSI à l'analyste forensics en passant par les auditeurs, architectes...

Au total, pas moins de **125 tâches, 83 compétences et 67 connaissances** y sont recensées et recoupées avec d'autres propriétés pour dresser un portrait robot de chaque profil :

- **La synthèse du marché**, via les titres, titres alternatifs et résumés
- **Le quotidien en entreprise**, via les missions, livrables et tâches
- **Les bagages nécessaires**, via les compétences et connaissances

L'ECSF est disponible dans différents formats : PDF, JSON, XML, ou encore version Web interactive. Autant de manières de se l'approprier voire d'automatiser son utilisation.

■ Des activités aux compétences : sélectionner, puis adapter

Le libellé de poste est un premier guide : "Analyste SOC" pointe vers le profil "Cyber Incident Responder", "RSSI" vers "Chief Information Security Officer"... Une fois le profil identifié, on extrait les tâches qui correspondent aux activités retenues, et par extension, **les compétences et connaissances sous-jacentes**.

Pour un poste hybride, sans équivalent direct dans l'ECSF, la logique est la même, appliquée sur plusieurs profils simultanément.

CAS PRATIQUE : RESPONSABLE CONFORMITÉ CYBERSÉCURITÉ

Imaginons une compagnie d'assurance qui cherche un.e Responsable conformité cybersécurité pour veiller à la conformité, apporter des conseils juridiques et conduire des audits. Ce poste n'existe pas dans l'ECSF. L'analyse des missions révèle un hybride entre deux profils : "Juriste, responsable conformité et politiques cybersécurité" (1) et "Auditeur Cybersécurité" (2). On ne retient que les éléments liés aux missions retenues :

■ COMPÉTENCES ECSF

collaborer efficacement en équipe (1, 2) ; comprendre l'impact des évolutions réglementaires sur la cybersécurité et la protection des données (1) ; appliquer cadres, standards et méthodologies d'audit (2) ; utiliser les outils et techniques d'audit (2)

■ CONNAISSANCES ECSF

expertise avancée en cybersécurité et protection des données (1) ; exigences de conformité en sécurité de l'information (2) ; bases sur le stockage et la protection des données dans les systèmes et services (1, 2).

La sélection terminée, il reste une étape essentielle : contextualiser

L'ECSF a été conçu pour rester indépendant de toute technologie ou organisation. C'est ce qui garantit sa durabilité. Ses profils sont génériques par nature, et c'est une force : ils laissent la place à votre réalité (stack technique, équipe existante, procédures internes...). Par exemple, "Utiliser les outils et techniques d'audit" devient ainsi "Maîtriser les outils GRC (ex. CISO Assistant) et conduire des audits selon l'ISO 27001 et l'ISO 27701" dans votre contexte.

6 ACTIVITÉS MAX, 0 DIPLÔME EXIGÉ : LES RÈGLES DU JEU

Compétences extraites et contextualisées, il reste à rédiger l'offre. Quelques règles pour éviter les pièges classiques :

- **Activités / missions** : max 6 items. Au-delà, le poste est probablement surchargé.
- **Hard skills et soft skills** : **3 à 4 max chacun**, issues de votre sélection précédente. La précision prime sur l'exhaustivité.
- **Zéro diplôme exigé. Remplacé par des expériences ou savoir-faire équivalents** : "expérience en gouvernance cyber", "pratique des audits ISO 27001"...
- **Signal d'alarme** : **vous piochez dans 3 profils ECSF distincts ou plus**. C'est souvent le signe d'un poste irréaliste. Faut-il le scinder en deux ? Ou transformer certaines exigences en "atouts appréciés" plutôt qu'exigés ?

>>>

Là où une offre classique demanderait : *"Master en droit ou cybersécurité, 5 ans d'expérience, certifié CISM et ISO 27001 Lead Auditor"*, voici ce que donne la même offre, repensée par compétences avec l'ECSF :

VOS MISSIONS

- Veiller à la conformité et fournir des conseils juridiques en matière de cybersécurité, protection des données et réglementations applicables.
- Identifier, documenter et suivre les écarts de conformité.
- Contribuer à la définition et à la mise en œuvre des politiques et programmes de conformité (RGPD, ISO 27001, ISO 27701, NIS2...).
- Former et sensibiliser les parties prenantes internes sur leurs obligations.
- Élaborer et partager des rapports de conformité à destination du management et des autorités compétentes.

VOTRE PROFIL

- **Hard skills** : connaissance des lois et règlements relatifs à la cybersécurité et à la protection des données (RGPD, NIS2, ePrivacy) ; maîtrise des standards de conformité (ISO 27001, ISO 27701, ISO 19011) ; capacité à conduire et évaluer des analyses d'impact (PIA).
- **Soft skills** : rigueur, intégrité et indépendance ; excellentes capacités de communication et pédagogie ; esprit analytique et capacité à convaincre.
- **Technologies / outils** : solutions GRC, outils de gestion documentaire, suites collaboratives.
- **Expériences équivalentes** : DPO, compliance officer, consultant GRC, juriste spécialisé.

Cette approche permet de s'affranchir du prisme réducteur des diplômes :

le poste s'ouvre à des profils juridiques formés à la cyber ou à des auditeurs évoluant vers la conformité, plutôt que de chercher un ingénieur technique inadapté au rôle.

RECRECITER MIEUX, SUR UN VIVIER PLUS LARGE, SANS CONCESSION SUR LES EXIGENCES

L'ECSF ne dit pas qui recruter. Il dit quoi chercher. Et c'est précisément ce qui manquait.

Pendant longtemps, le diplôme est resté notre seule boussole, faute de mieux. Basculer vers une approche par compétences semblait être un chantier titanesque, risqué et fastidieux. Mais la voie est désormais tracée. **L'ECSF** transforme l'essai en four-nissant le moteur opérationnel pour passer à l'acte. Vous n'avez plus besoin de construire l'outil, il est là, standardisé et prêt à l'emploi.

Et en adoptant ce standard, vous faites bien plus que simplifier vos recrutements : vous devenez **interopérables** "by design".

Sans effort de traduction supplémentaire, vous parlez la même langue que les candidats, les régulateurs et les organismes de formation de toute l'Europe et au-delà. Un champ des possibles qui change la donne : rendez-vous dans le prochain numéro.



Formation Continuité et résilience Protection des données Droit de la cybersécurité

PROGRAMME

Continuité et résilience

RPCA

Formation Responsable Continuité d'Activité

ISO22LA

ISO22301 Lead Auditor

ISO22LI

ISO22301 Lead Implementer

SECUCRISE

Gestion de crise cyber

Protection des données

RGPD

Fondamentaux de la protection des données

DPO

Métier du DPO

CERTIFDPO

Préparation à la certification AFNOR Certification agréé CNIL

PIA

Étude d'impact sur la vie privée

SECUSANTE

Hébergement et protection des données de santé

Droit de la Cybersécurité

SECUDROIT

Droit de la cybersécurité

SECUCLOUD

Contractualisation cloud

+ 33 974 774 390

HÉLÈNE
BOUCHARD

*Directrice de
Confiance et Réussite
Conférences et mentoring
Catalyseur de transformation des
leaders vers l'excellence
Agrégee et Docteur en
Philosophie & Lettres classiques*



QUAND LA VULNERABILITE DEVIENT UNE FORCE : UN HORACE CONTRE TROIS CURIACES

SOUS LE RÈGNE DE TULLUS HOSTILIUS , TROISIÈME ROI DE ROME ET
SUCCESSEUR DE ROMULUS, AU 7^E SIÈCLE AVANT JC, UNE GUERRE
MEURTRIÈRE ÉCLATA ENTRE LES HABITANTS D'ALBE ET CEUX DE ROME.

Pour mettre fin à ce conflit, les chefs des deux peuples décidèrent d'un commun
accord de régler leur conflit en désignant trois champions de chaque côté,
les Horaces pour Rome et les Curiaces pour Albe¹.

Très rapidement, les Albains furent tous les trois blessés, et deux des Romains tués. L'Horace survivant, indemne, mais dans l'incapacité de faire face, seul, aux trois Curiaces, simula la fuite -honte absolue chez les Romains-, et fut poursuivi par les trois Curiaces, blessés à des degrés divers : Le plus robuste le rattrapa, mais Horace, faisant volte-face, le tua avant que le deuxième, déjà épuisé, ne le rejoigne. Il ne fut pas difficile à Horace de l'achever. Quant au troisième, qui avait perdu beaucoup de sang, Horace lui retira d'un geste ce qui lui restait de vie.



Le Serment des Horaces
par Jacques-Louis David (1785),
musée du Louvre.

LA STRATEGIE D'HORACE : QUELS ENSEIGNEMENTS POUR LA CYBERSÉCURITÉ ?

NE PAS SOUS-ESTIMER LA FORCE DES ATTAQUANTS.

Les Curiaces, même blessés, sont supérieurs en nombre.

En cybersécurité, ce qui fragilise votre système de sécurité, c'est la multiplicité innombrable des attaquants, et la diversité des attaques.

De ce fait, on doit toujours se supposer en situation de vulnérabilité constante, et d'infériorité absolue certaine.

C'est à partir de cette prise de conscience que doit s'organiser la défense : Face à un rapport de force qui vous est défavorable, travaillez votre stratégie.

SIMULER LA FUITE

Tourner le dos, faire le gros dos, paraître faible. C'est l'art de l'esquive. Horace accepte d'être hué par le peuple Romain, afin de remporter la victoire, plutôt que de mourir avec les honneurs.

Que cherchait Horace ? A mettre ses assaillants en mouvement. Fuir pour déclencher une réaction automatique chez les Curiaces : La poursuite.

En cybersécurité, ce qui va permettre de renverser la situation, **c'est de simuler la faiblesse, c'est-à-dire la faille.** Une faille visible dans un système, c'est l'assurance d'une ou de plusieurs attaques assez rapides.

Si cette faille est feinte de votre part, elle comporte plusieurs intérêts :

- Elle ne donne en réalité accès à aucune donnée véritable et ne vous affaiblit en rien.
- Elle permet une sortie de l'ombre des assaillants. Plus leurs attaques sont nombreuses, plus les indices pour remonter à eux seront fournis, permettant ainsi une neutralisation plus rapide et efficace.

CONTRE ATTAQUER

La cybersécurité, de défensive, doit devenir offensive. Chaque faille simulée doit être un piège de contre-offensive, qui vise à empoisonner l'attaquant, par exemple en lui livrant des informations erronées qui vont perturber, voire neutraliser son système d'attaque. C'est le glaive qui se retourne contre l'assaillant.

PLUSIEURS FAILLES POUR PLUSIEURS ATTAQUES

Horace remporte la victoire en séquençant ses répliques : il vainc du plus fort au plus faible, du moins blessé au plus blessé.

En cybersécurité, en inversant la métaphore, vous pouvez aller de la faille la plus visible à des failles plus subtiles, afin de faire face à des cyberattaquants de différents calibres. Celui qui ne tombera pas dans votre premier traquenard se sentira assez intelligent pour penser qu'il a trouvé la « vraie » faille, alors que c'était juste un piège plus élaboré. Vous aurez ainsi l'avantage de prendre dans vos rêts des cybercriminels de différents types, et de diversifier ainsi vos protections.

EN CONCLUSION

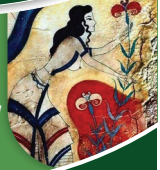
les histoires romaines nous enseignent des attitudes, d'attaques et de défense, applicables autant à la stratégie militaire qu'à la cybersécurité, avec, constamment, cette idée, reprise et amplifiée par le plus grand penseur politique de tous les temps, Machiavel : Être à la fois lion et renard, c'est-à-dire toujours conjuguer la force et l'intelligence². « On n'est jamais toujours assez fort pour être toujours le maître³ », car on trouvera toujours plus fort que soit, ne serait-ce que par le poids du nombre des assaillants. Faisant partie de la quintessence de cette intelligence : 1. Attaquer plutôt qu'être attaqué. 2. La détermination et la certitude sans faille de vaincre, et de réduire à néant l'assaillant.

En deux mots : Être guerrier.



Confiance et Réussite
FORMATION & TRAINING
Pour l'excellence !

PROGRAMME ÉNERGIE
Fatigue ? Doutes ? Burn-out ?
Retrouvez l'excellence !

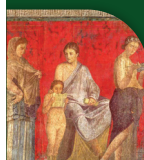




ENTREPRENEUR & DIRIGEANT
Améliorez votre leadership
7 principes tirés des conquérants grecs et empereurs romains

FEMMES MODÈLES
Pour une vie d'excellence !
Plusieurs vies en **une seule**





ET L'EXCELLENCE DE VOS JEUNES ?
Accompagnement à la parentalité pour des **résultats scolaires brillants**

www.confianceetreussite.fr

Hélène Bouchard
06 64 21 42 37



**En cybersécurité, ce qui fragilise votre système de sécurité,
c'est la multiplicité innombrable des attaquants,
et la diversité des attaques.**

¹ Tite-Live, Ab Urbe condita libri, livre I

² Machiavel, Le Prince (1514), Traité de philosophie politique à l'adresse de Laurent de Médicis, dit « Laurent le magnifique », chef du gouvernement de Florence

³ Citation cette fois-ci de Jean-Jacques Rousseau, Le contrat social (1762), chapitre III.



LA CYBERSÉCURITÉ À l'école des CONQUÉRANTS GRECS ET ROMAINS

Pour l'excellence !

CYBERSECURITE ET ART DE LA GUERRE !

Vous êtes un **professionnel de la cybersécurité**.
Vous avez les **compétences techniques**, le professionnalisme attendu.
Vous êtes **engagés dans le service du client**.

Mais la **réalité** de tous les jours est plus nuancée. L'accumulation de gestes et de tâches **urgentes** vous **enferme** dans le **présent**. Vous vous sentez souvent **débordé** par le temps. Cela vous empêche d'avoir une vision globale de votre mission

L'URGENCE VOUS FAIT PERDRE LA VISION

ET SI VOUS REPRENIEZ DE LA HAUTEUR ? À L'ÉCOLE DES GRANDS CONQUÉRANTS GRECS ET ROMAINS

- Art de la guerre et **technologie**
- Attaquer pour mieux **se défendre**
- La **stratégie supérieure** à la force
- La **rapidité** comme **arme suprême**
- Ruse et **stratagème**
- Donner pour mieux reprendre
- Se **masquer**, démasquer

Bonifier vos compétences pour donner à vos clients
CONFIANCE ET REUSSITE, c'est notre engagement !

NOTRE INSPIRATION ALEXANDRE LE GRAND, JULES CESAR

Appliqués à la cybersécurité

Histoire et philosophie politique comme outils inédits pour renouveler votre vision de la cybersécurité.

Des anecdotes concrètes d'où tirer les 7 lois de la défense cybernétique.

« SI VIS PACEM, PARA BELLUM »
Si tu veux la paix, prépare la guerre.



” CYBERSECURITE, GUERRE ET PAIX ”

1

Le PASSÉ au service du PRÉSENT pour mieux bâtir L'AVENIR

Histoire, philosophie, culture politique pour prendre de la **hauteur** et retrouver une **vision**.

2

CONFÉRENCES, FORMATIONS, TRAINING,

3 formules plutôt qu'une, pour répondre au plus près à vos besoins.

3

UNE EXPERTE A VOTRE SERVICE

Agrégée et docteur en philosophie et lettres classiques,
ceinture noire d'aïkido, la stratégie du **pouvoir** et de la **conquête** est au cœur de ma **vie**.

Hélène Bouchard
hbouchard@confianceetreussite.fr
06 64 21 42 37



www.confianceetreussite.fr



LES VULNÉRABILITÉS & LA CYBERSÉCURITÉ

> SELON VOUS, QUELS SONT LES DÉFIS DE LA CYBERSÉCURITÉ FACE AUX VULNÉRABILITÉS ?

Pendant longtemps, le problème était de connaître ses vulnérabilités. Aujourd'hui, le problème est surtout de ne pas se noyer dedans... Entre l'explosion du nombre de CVE (sans parler des prochaines innovations annoncées comme Mythos et les modèles cyber), des outils toujours plus bavards et des délais d'exploitation qui diminuent drastiquement, on ne sait plus où donner de la tête.

Il est encore complexe — je le constate avec certains clients — d'avoir une vision claire sur ses vulnérabilités, et celles liées au Shadow IT et Supply Chain. Cartographier ce que l'on ne possède pas directement reste un défi permanent.

Ensuite — mais rien de nouveau sous le soleil — la surface d'attaque continue de s'élargir. Nos organisations se digitalisent toujours davantage et nos architectures se complexifient : cloud hybride, conteneurisation, API et maintenant l'agentique et les IA qui cherchent à s'intégrer dans chaque coin de nos applications et services.

Enfin, le dernier défi résidera dans notre capacité à réduire continuellement l'écart entre la découverte et la remédiation des vulnérabilités. Le temps moyen entre la publication d'un exploit et son exploitation dans un environnement réel s'est considérablement réduit — on parle désormais de quelques heures à quelques jours pour les plus critiques.

> QUELLES SONT LES STRATÉGIES ET SOLUTIONS QUE VOUS CONSEILLEZ POUR LA GESTION DES VULNÉRABILITÉS ?

Puisque le time to exploit continue de se réduire, la gestion des vulnérabilités doit aujourd'hui faire partie des priorités des organisations.

Avant même de parler d'outils, la gouvernance est le point de départ. Mettre en place un programme structuré comme le Risk-Based Vulnerability Management (RBVM), c'est accepter que tout ne peut pas être patché, et donc décider consciemment de ce qu'on traite en priorité, selon l'exposition réelle et l'impact métier. C'est une évidence sur le papier, mais encore trop peu formalisé dans la pratique.

Le VOC (Vulnerability Operations Center) est également décisif dans une bonne démarche sécurité. Nous en avons d'ailleurs parlé l'année dernière dans un article de Mohamed Aissou publié sur notre blog. L'idée est de centraliser la détection, la priorisation et le suivi de remédiation dans une structure dédiée, capable de piloter dans la durée — et pas seulement de produire des rapports de scan.

J'observe également les bénéfices des coordinateurs sécurité, qui jouent un rôle clé entre la gouvernance cyber, le VOC et les équipes opérationnelles. Ce relais permet de mieux embarquer les métiers, de fluidifier les remédiations et d'éviter que la cybersécurité soit perçue uniquement comme une contrainte.

Enfin, je suis convaincu que la meilleure vulnérabilité reste celle que l'on évite dès le départ. La Security by Design ne doit pas être un nice-to-have : intégrée dès le départ aux projets IT, c'est l'une des rares approches qui réduit structurellement la surface d'exposition.

> COMMENT VOUS ADAPTER AUX ÉVOLUTIONS PERMANENTES DES DIRECTIVES, RÈGLEMENTS ET TECHNOLOGIES ?

Sur le plan réglementaire, le rythme s'est bien accéléré — mais s'adapter n'est-ce pas le cœur de notre métier ?

D'un point de vue technologique, l'intelligence artificielle est déjà une réalité dans les deux camps. Du côté défensif, les outils XDR, SIEM nouvelle génération et plateformes de VM intègrent des modèles permettant de corréler des signaux faibles, de détecter des anomalies comportementales et d'accélérer le triage. Du côté offensif, l'IA permet aux attaquants de générer des exploits plus rapidement, d'automatiser et de personnaliser les campagnes de phishing à grande échelle.

La vigilance s'impose aussi sur les vulnérabilités propres aux systèmes d'IA eux-mêmes — prompt injection, empoisonnement de modèles, exfiltration via LLM — que l'OWASP et le MITRE ont commencé à formaliser.

Ensuite, le quantique est la prochaine grande menace, même si nous avons encore quelques années avant que des machines soient capables de casser RSA ou ECC.

Ce n'est pas une raison d'attendre : le risque de « harvest now, decrypt later » est déjà actif. La réponse, c'est d'entamer dès maintenant l'inventaire des usages cryptographiques et de planifier la migration vers les standards post-quantiques du NIST 2024, que l'ANSSI a déjà intégrés dans ses recommandations.

S'adapter, c'est surtout ne pas subir. Ceux qui anticipent ces évolutions aujourd'hui auront une longueur d'avance demain — les autres rattraperont en urgence, comme toujours.

>>>

**Cybersecurity today faces three major challenges:
the overwhelming volume of CVEs, the ever-expanding attack surface due to
digital transformation (cloud, containers, APIs, AI), and the drastically reduced
time between vulnerability discovery and exploitation.**

To address these, Luca Perez advocates for structured approaches like Risk-Based Vulnerability Management (RBVM) to prioritize patches, centralized Vulnerability Operations Centers (VOC) for detection and remediation, and Security by Design to minimize exposure. AI is reshaping both defense (XDR, next-gen SIEM) and offense (automated attacks), while quantum computing poses future risks. Organizations must proactively adapt by inventorying cryptographic uses and transitioning to NIST's post-quantum standards. Governance and cross-team coordination are essential to avoid treating cybersecurity as a mere constraint.

**CONTACTS :****Lucas PEREZ****Directeur Associé -
Réseau & Cybersécurité_Davidson consulting****Web :** www.davidson.fr**Courriel :** lucas.perez@davidson.fr

Une (cyber) sécurité qui s'adapte à vos défis (numériques)

Parlons de vos projets 2026

➤ [Davidson.fr/cybersecurite](https://davidson.fr/cybersecurite)



CYBERSÉCURITÉ
BY DAVIDSON





DATA CENTERS HAUTE DENSITÉ : LES DÉFIS DE LA PERFORMANCE ET DE LA RÉSILIENCE

Face à l'essor de l'intelligence artificielle, de l'Edge computing et des architectures de data centers toujours plus denses, les infrastructures de connectivité jouent un rôle stratégique pour garantir la fiabilité et la continuité des services numériques. Les exigences en matière de performance, de résilience et d'évolutivité n'ont jamais été aussi élevées.

Dans ce contexte, Bruno Demouron, Directeur Commercial de Rosenberg OSI, revient sur les principales évolutions du marché, sur les défis techniques des data centers haute densité et sur les innovations qui contribuent à renforcer la performance et la fiabilité des réseaux modernes.

> QUELLES SONT LES TENDANCES DANS LE CÂBLAGE ET LES INFRASTRUCTURES DE DC, NOTAMMENT AVEC L'ARRIVÉE DE L'IA ET DE L'EDGE COMPUTING ?

« Les principales tendances s'articulent autour de trois priorités stratégiques : la souveraineté des données, avec des infrastructures situées dans l'UE et opérées par des acteurs locaux ; la vitesse, grâce à une faible latence, une forte puissance de calcul et une plus grande proximité avec les utilisateurs ; et la durabilité énergétique, visant à réduire la consommation d'énergie, les émissions de carbone et l'impact sur l'eau.

Sur le plan opérationnel, on observe une demande croissante de modularité afin d'adapter rapidement les infrastructures aux besoins fluctuants de l'IA et des nouvelles applications. La connectivité haute performance devient également essentielle, en raison de l'explosion des besoins en bande passante liée notamment à l'IA générative et aux serveurs GPU. Par ailleurs, l'optimisation énergétique et les systèmes de refroidissement avancés, comme le refroidissement liquide ou par immersion, prennent une importance croissante. Enfin, le développement de l'Edge computing entraîne la multiplication de micro data centers au plus près des utilisateurs, y compris dans des environnements non traditionnels ».

> QUELLES SONT LES DIFFICULTÉS TECHNIQUES LORS DE LA MISE EN PLACE D'INFRASTRUCTURES DANS DES ENVIRONNEMENTS CRITIQUES COMME LES DC HAUTE DENSITÉ ?

« Les défis sont nombreux. L'un des principaux consiste à repenser les espaces de passage des câbles afin de ne pas perturber les flux d'air ou de liquide nécessaires au refroidissement. Alors qu'un rack classique délivre en moyenne entre 5 et 10 kW, un rack dédié à l'IA peut dépasser 40 à 100 kW.

La traçabilité des connexions devient également essentielle. Un étiquetage clair permet d'éviter de décommissionner un port actif lors de l'ajout ou de la suppression de liens, tout en facilitant les opérations de maintenance. On observe également une demande croissante pour des matériaux à faible impact environnemental, dans le cadre des politiques RSE des entreprises.

L'utilisation de liens préconnectés en usine constitue par ailleurs un avantage important : elle permet de garantir la fiabilité de la conception tout en accélérant considérablement le déploiement sur site, ce qui réduit les risques d'intervention dans des data centers déjà en production.

D'autres contraintes apparaissent également, comme la charge au sol, liée à l'augmentation du poids des racks, des batteries ou des systèmes de refroidissement liquide.

Avec l'IA et le HPC, les besoins réseaux explosent avec des latences de plus en plus extrêmes et le câblage devient rapidement un enfer si mal anticipé.

N'oublions pas qu'un design mal pensé peut diviser les performances par deux.

Dans ces environnements, on ne cherche pas « ça marche » mais zéro interruption, zéro surprise.

► COMMENT LA DEMANDE DES CLIENTS ÉVOLUE-T-ELLE EN FRANCE ?

Face à ces défis, les clients cherchent à la fois à maintenir leurs infrastructures existantes pour certaines applications tout en développant de nouvelles architectures adaptées aux usages émergents. On observe aussi une prise de conscience croissante de l'importance du précâblage passif, notamment en ce qui concerne le cheminement des liens cuivre et fibre optique. Leur encombrement peut en effet avoir un impact direct sur les flux d'air et sur les possibilités d'évolution futures.

L'un des grands enjeux consiste à trouver le bon équilibre : ne pas surdimensionner les installations pour éviter le gaspillage, mais ne pas les sous-dimensionner non plus afin de ne pas freiner la croissance.

Enfin, les clients privilégient de plus en plus une approche globale, intégrant à la fois les produits et les services. L'avantage est de disposer d'un point d'entrée unique, responsable de l'ensemble de la chaîne, depuis la fabrication des liens cuivre et optiques jusqu'à leur installation et leur validation sur site.

Rosenberger

Rosenberger OSI's Bruno Demouron

highlights high-density data center trends:

data sovereignty, low latency, and sustainability. AI and Edge computing demand modularity, high-performance connectivity, and advanced cooling. Challenges include cable management to avoid cooling disruption, traceability, and eco-friendly materials. Clients seek balanced solutions and end-to-end services. Rosenberger OSI addresses these needs with specialized units for Enterprise, Hyperscale, Industrial, and Mobile networks.

► COMMENT S'INSCRIT LA STRATÉGIE DE ROSENBERGER OSI ?

« Aujourd'hui, Rosenberger OSI a fait évoluer son organisation pour mieux répondre aux besoins du marché des data centers. L'entreprise s'appuie désormais sur une structure articulée autour de quatre pôles spécialisés : le marché Enterprise et multi-tenant ; l'Hyperscale ; le marché industriel ; les réseaux mobiles ».

<https://osi.rosenberger.com/>

CONTACTS :

Bruno Demouron
Directeur Commercial
de Rosenberger OSI,

<https://osi.rosenberger.com/>



HS2

Hervé Schauer Sécurité

Formation cybersécurité technique

INTRODUCTION • RÉSEAUX
INFRASTRUCTURES • DÉFENSE



PROGRAMME

Introduction à la cybersécurité

ESSCYBER

Essentiels techniques de la cybersécurité

SECUCYBER

Fondamentaux techniques de la cybersécurité

Sécurité des réseaux et des infrastructures

SECUARCH

Sécurité des architectures

REDTEAM

Redteam sans fil

SECUPKI

Infrastructures de clés publiques

SECUIA

Sécurité des systèmes d'intelligence artificielle

Sécurité défensive

SECUWIN

Sécurisation des infrastructures Windows

SECULIN

Sécurité Linux

SELinux

Comprendre SELinux et savoir modifier la politique de sécurité

SECUDEVWEB

Sécurité des serveurs et des applications Web

SECUINDUS

Cybersécurité des systèmes industriels

SECUOBJ

Sécurité des objets connectés

SECUMOBILE

Audit sécurité d'applications mobiles Android et iOS

+ 33 974 774 390

www.hs2.fr

formation@hs2.fr

Formation cybersécurité technique

DÉTECTION ET RÉPONSE •
INFORENSIQUE • SÉCURITÉ OFFENSIVE

PROGRAMME

Détection et réponse aux incidents

OSINT

Formation OSINT

SECUBLUE1

Surveillance, détection et réponse aux incidents de sécurité

SECUBLUE2

Surveillance, détection et réponse avancée aux incidents de sécurité

SECUSOC

Surveillance, analyse et corrélation

SPLUNK

Formation SPLUNK

ISO27035

Formation Gestion des incidents de sécurité

Inforensique

FORENSIC1

Analyse inforensique Windows

FORENSIC2

Analyse Inforensique avancée

REVERSE1

Rétroingénierie de logiciels malveillants

FORMOBILE

Forensic Mobile : Analyse des smartphones iOS et Android

Sécurité Offensive

PENTEST1

Tests d'intrusion

PENTEST2

Tests d'intrusion et développement

d'exploits

PENTESTWEB

Tests d'intrusion sur applications Web

PENTESTINDUS

Tests d'intrusion des systèmes
industriels

PENTESTOBJ

Sécurité des dispositifs IoT

PENTESTCLOUD

Sécurité des environnements cloud

+ 33 974 774 390



NOUVEAUTÉ

L'IA fait voler en éclats les anciens modèles de stockage.

Scality ADI

AUTONOME. RÉSILIENT. SOUVERAIN.

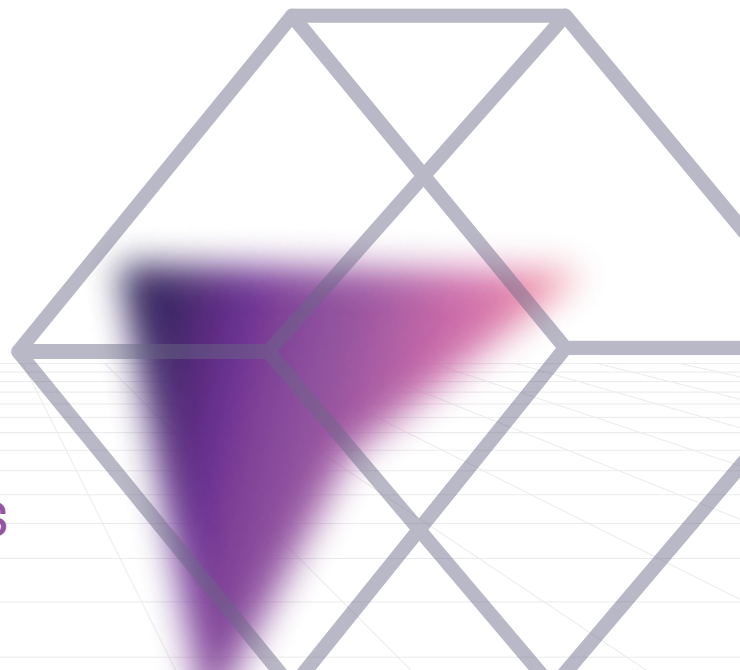
Conçu pour les GPU les plus exigeants, le stockage ultra-froid, et tout ce qu'il y a entre les deux.

Scality ADI — l'infrastructure de données qui aligne de manière autonome et durable les supports de stockage, les performances et les niveaux de protection adaptés à chaque étape du cycle de vie des données — de plusieurs pétaoctets jusqu'à l'exaoctet.



SCANNEZ POUR EN SAVOIR PLUS

scality.com/adi





Scality, <https://www.scality.com/fr/>, leader mondial des logiciels d'infrastructure de données à l'ère de l'IA, a lancé Scality ADI (Autonomous Data Infrastructure), une plateforme d'infrastructure de données durable conçue pour les organisations qui doivent servir plusieurs cas d'usage relatifs à l'IA, se protéger contre l'escalade des cybermenaces et conserver un contrôle souverain sur leurs données.

Scality ADI combine l'expertise reconnue de stockage objet de Scality avec Guardian, un agent IA d'exploitation autonome qui réduit considérablement la charge administrative quotidienne tout en s'assurant d'un contrôle humain à chaque décision. La plateforme prend en charge plusieurs classes de stockage au sein d'un espace de données commun. Elle met en œuvre les politiques de gestion du cycle de vie de la donnée au travers des différentes températures de stockage de manière à optimiser dynamiquement les performances et l'énergie consommée par les différents cas d'usage. Les solutions éprouvées Scality RING et Scality ARTESCA restent bien entendu au catalogue pour adresser d'une part les besoins en stockage distribué pour les fournisseurs de solution Cloud privé ou public et d'autre part le besoin d'un stockage objet immuable optimisé pour le backup.

Scality, <https://www.scality.com/fr/> launches **ADI (Autonomous Data Infrastructure)**, an AI-powered, sovereign data infrastructure platform optimizing storage for AI, cyber-resilience (CORE5), and energy efficiency. It features **Guardian**, an autonomous AI agent reducing admin workload, and supports multi-temperature storage. CEO Jérôme Lecat calls it a revolutionary step for AI-driven data storage, building on RING and ARTESCA's success.

L'IA impose une refonte complète des modèles de stockage existants

S'appuyer sur le succès de Scality RING et ARTESCA

UNE PLATEFORME CONÇUE POUR LE FUTUR

La cyber-résilience CORE5 garantit que les données restent immuables, récupérables et auditable sur 5 niveaux différents. La télémétrie en temps réel offre aux équipes d'infrastructure une visibilité sur la consommation aux niveaux du système, du nœud et des cas d'usage, permettant de prendre des décisions éclairées sur les besoins en performance selon les contraintes réelles des centres de données.

SLA ET TARIFICATION SUR LA BASE DES RÉSULTATS

« L'IA est réellement une révolution pour l'IT, et demande une refonte des principes de stockage de données. Scality ADI a été pensé à cette échelle, pas une simple évolution, mais un produit entièrement conçu pour les nouvelles réalités opérationnelles. La mise en œuvre de l'agent Guardian conçu par Scality en partenariat avec l'INRIA permet de réduire considérablement les charges d'exploitations. Par ailleurs, l'ultra-performance développée pour ADI avec RDMA permet d'apporter aux GPU toute la puissance dont ils ont besoin. Nous avons révolutionné l'industrie du stockage de données en 2010 avec RING, notre ambition est de faire de même avec Scality ADI en 2026. » Jérôme Lecat, CEO de Scality



CONTACTS :

Jérôme LECAT, CEO, Scality

Contactez-nous par email :
sales.eu@scality.com

Effacité opérationnelle

Gérez quotidiennement
vos opérations de
sécurité grâce à une
plateforme de gestion
centralisée intégrée.



Haute disponibilité

Assurez la continuité de
vos activités en toute
sérénité, dans une
architecture complexe.



Sécurité multifonctionnelle

Pare-feu nouvelle
génération pour identifier
et bloquer les menaces
avancées afin d'assurer
une protection optimale
de votre infrastructure.



Évolutivité

Matériel modulaire e
conception et capacités
d'extension réseau offrant
une grande flexibilité de
configuration pour soutenir
la croissance de votre
infrastructure.



La sérénité de votre entreprise
mérite le **choix européen** en
matière de **cybersécurité**



STORMSHIELD





12ème édition

UNIVERSITÉS D'ÉTÉ

CYBERSÉCURITÉ &
CLOUD DE CONFIANCE

10.09.26 STATION F - PARIS

EVENT BY

HEXATRUST

CLOUD CONFIDENCE & CYBERSECURITY

L'événement de rentrée de la filière cyber & cloud de confiance

RÉARMEMENT NUMÉRIQUE : L'EUROPE EST-ELLE PRÊTE À CONQUÉRIR SA SOUVERAINETÉ ?

Les Universités d'Été de la Cyber et du Cloud de confiance (UECC) sont l'événement incontournable de la rentrée des professionnels de la filière cybersécurité et cloud. Cette 12e édition portera une nouvelle fois l'excellence du numérique souverain en France et en Europe, en associant entreprises de la filière, partenaires, associations, médias, personnalités étatiques et décideurs.

AVEC LE SOUTIEN DE :

ITfor
Business

[N]
FRANCE NUM

LEVAS SAS

Global Security Mag
THE LOGICAL & PHYSICAL SECURITY MAGAZINE

CESIN

CLUSIF

coTer
numérique

CAMPUS
CYBER

CAMPUS
CYBER
RÉGION SUD / EUROMED

Business
France

LYON
CYBER
XPO

STATION F

RÉPUBLIQUE
FRANÇAISE
Liberté
Égalité
Fraternité

CYBER
HAUTVEILLANCE
GOUV.FR
Assistance et prévention
en sécurité numérique

Gendarmerie
NATIONALE

SOUS LE PATRONAGE DE MME ANNE LE HÉNANFF, MINISTRE DÉLÉGUÉE
CHARGÉE DE L'INTELLIGENCE ARTIFICIELLE ET DU NUMÉRIQUE.



MINISTÈRE
CHARGÉ DE L'INTELLIGENCE
ARTIFICIELLE
ET DU NUMÉRIQUE

Liberté
Égalité
Fraternité



Scannez le QR code
pour vous inscrire à la
12^e édition des UECC.

JOFFREY
CÉLESTIN-URBAIN

Président du Campus Cyber



LES ENJEUX DE RÉSILIENCE ET DE SOUVERAINETÉ QUE CONCENTRE LA CYBER SONT EXISTENTIELS POUR LA FRANCE ET L'EUROPE

■ ■ **GS MAG :** *Bonjour Joffrey Célestin-Urbain, pouvez-vous vous présenter et nous dire comment votre parcours vous a amené à votre rôle actuel ?*

■ ■ **JCU :** Je ne prétendrai pas post-rationaliser mes 20 ans de vie professionnelle pour y trouver un sens linéaire ou une forme de vocation qui m'auraient inéluctablement conduit à mon rôle actuel de président du Campus Cyber. C'est par la porte de la sécurité économique, dont je m'occupais entre 2019 et 2025 comme Directeur du SISSE à Bercy, que je suis entré dans la cybersécurité. Ce sont deux univers qui partagent les mêmes schémas, le même lexique, les mêmes modus operandi. La sécurité économique protège les actifs stratégiques et les infrastructures critiques de la Nation face à des menaces étrangères, dont

certaines, entre 5 et 10% des alertes répertoriées selon les années, prennent la forme de cyberattaques. La cyber est l'une des dimensions essentielles de l'équation sécuritaire à laquelle la France est confrontée. Mon transfert du SISSE vers le Campus Cyber n'est pas donc pas un vrai départ, mais plutôt un nouveau chapitre dans un parcours inspiré par cette grande cause qu'est la reconquête de notre sécurité et de notre souveraineté, numérique et économique.

■ ■ **GS MAG :** *Pouvez-vous nous présenter le Campus Cyber, ses objectifs, ses actions, ses ambitions ?*

■ ■ **JCU :** Le Campus Cyber est à la fois le mouton à cinq pattes et le chaînon manquant de la cybersécurité française et européenne. Il a quatre caractéristiques qui en font un acteur unique en son genre. Tout d'abord, le Campus est le lieu-vitrine de la cybersécurité en France.

La cyber est l'une des dimensions essentielles de l'équation sécuritaire à laquelle la France est confrontée.

Ensuite, il est le carrefour des forces françaises de la cyber, dans toute leur pluralité (public et privé ; civil et militaire ; offre et demande ; économie, enseignement, recherche, et monde associatif ; grandes entreprises, PME, ETI et start-ups). En outre, il possède une signature unique : l'alliage du sceau de l'État et de celui des grands groupes cybers privés français, qui lui confèrent un statut et un capital fiduciaire exceptionnels. Enfin, il est un acteur hybride, en partie libéré des contraintes individuelles de ses membres, avec un vaste espace de manœuvre et d'innovation au bénéfice du collectif. Fort de son écosystème de 135 résidents et 250 partenaires au total, et d'un réseau composé de huit campus territoriaux, le Campus cyber est engagé depuis 2025 dans une stratégie de revitalisation destinée à faire émerger un « écosystème-frontière » de dimension européenne, c'est-à-dire une communauté de services et de projets capable de sécréter en permanence des solutions à l'échelle face à des problématiques collectives complexes. La cybersécurité n'en manque pas en 2026. Le secteur n'a jamais eu autant besoin d'opérateurs agiles, fédérateurs et engagés comme le Campus.

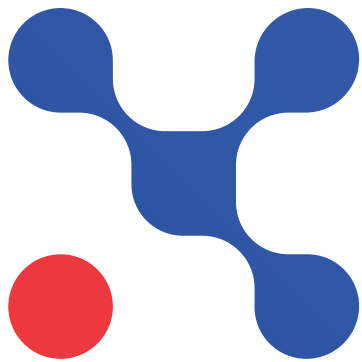
■ ■ **GS MAG** : *Selon vous, quels sont les défis de la Cybersécurité face aux Vulnérabilités ? Quelle est l'influence de l'IA ?*

■ ■ **JCU** : La cybersécurité est structurellement une course contre la montre contre l'exploitation de vulnérabilités, une bataille précaire et asymétrique avec des assaillants invisibles, toujours sur le qui-vive, à l'offensive, à l'affût de portes d'entrées ou de failles, humaines et logicielles, pour frapper. Ce n'est pas nouveau, mais cela prend une coloration nouvelle avec l'utilisation croissante de l'intelligence artificielle, aujourd'hui principalement générative,

demain de plus en plus agentique. La médiatisation récente des derniers modèles-frontières d'entreprises américaines confirme une tendance nette, observée depuis plus d'un an, à l'accélération des performances de l'IA, non seulement en matière de détection de vulnérabilités cyber mais aussi en termes de capacités à dérouler de manière autonome une chaîne d'attaque complète. Le Campus Cyber a publié début mai sur ce sujet une note d'analyse et de position qui contient des recommandations à la fois très opérationnelles pour les équipes DSI/RSSI et très stratégiques pour les COMEX comme pour les autorités politiques, françaises et européennes. L'IA exacerbe les enjeux de résilience des organisations et complexifie encore davantage l'objectif de souveraineté européenne en cybersécurité, faute, à date, de capacités industrielles en IA d'une puissance équivalente à celles des Etats-Unis.

■ ■ **GS MAG** : *Quels seraient vos messages à nos lectrices et lecteurs qui font partie de l'écosystème Cyber ?*

■ ■ **JCU** : Les enjeux de résilience et de souveraineté que concentre la cyber sont existentiels pour la France et l'Europe. Les rapports de force géopolitiques, économiques et technologiques nous sont massivement défavorables aujourd'hui. Nous n'avons une chance de réussir qu'en changeant de méthode : lucidité, courage, organisation, collectif, patriotisme. Ce sont ces valeurs que porte aujourd'hui le Campus Cyber dans la transformation engagée depuis près d'un an maintenant. Tous ceux qui en France, dans la sphère publique et dans le monde de l'entreprise, de la recherche, de l'enseignement, se retrouvent dans ces valeurs et sont prêts à se retrouver les manches trouveront au Campus un point d'appui naturel et un accélérateur d'actions. ■



**CAMPUS
CYBER**



NOUVEAUTÉ

L'IA fait voler en éclats les anciens modèles de stockage.

Scality ADI

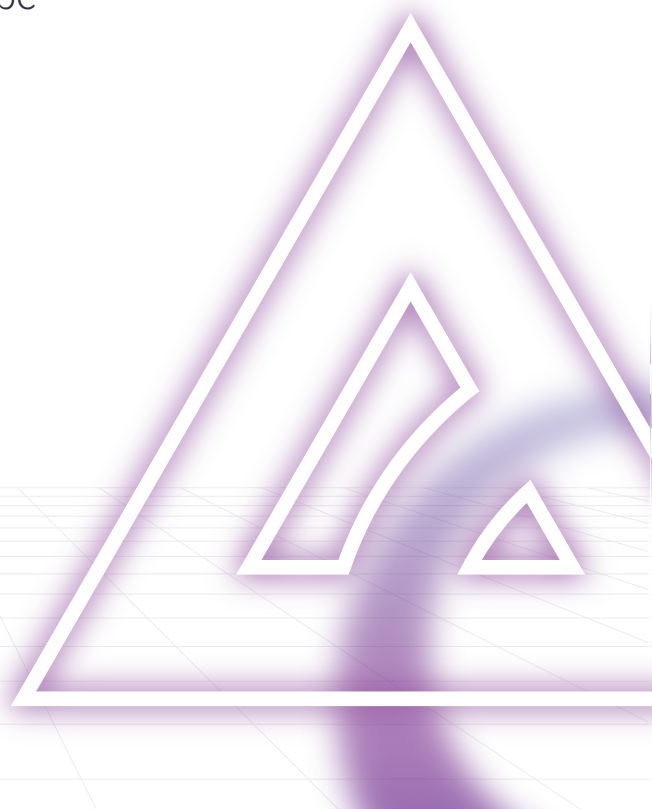
AUTONOME. RÉSILIENT. SOUVERAIN.

Conçu pour les GPU les plus exigeants, le stockage ultra-froid, et tout ce qu'il y a entre les deux.

Scality ADI — l'infrastructure de données qui aligne de manière autonome et durable les supports de stockage, les performances et les niveaux de protection adaptés à chaque étape du cycle de vie des données — de plusieurs pétaoctets jusqu'à l'exaoctet.



SCANNEZ POUR EN SAVOIR PLUS
scality.com/adi





ANDY YEN

Founder, CEO of Proton

**Propos recueillis par Jean-Luc Raymond,
Journaliste Tech & DeepTech**

LA MEILLEURE FAÇON DE PROTÉGER DES DONNÉES, C'EST DE NE PAS LES AVOIR EN CLAIR

Physicien des particules formé au CERN, Andy Yen a fondé Proton en 2014 et dirige depuis lors l'entreprise tech avec une idée alors jugée folle : construire une alternative à Google qui respecte réellement la vie privée. 12 ans plus tard, la suite bureautique suisse revendique 100 millions d'utilisateurs et s'impose comme le champion discret de la souveraineté numérique européenne. Une rencontre au sommet lors du Forum INCYBER Europe à Lille, où il intervenait sur la résilience technologique du continent, avec des propos qui résonnent.

■ ■ **GS MAG** : *La souveraineté numérique est devenue un grand thème incontournable aujourd'hui. Est-ce vraiment quelque chose de nouveau ?*

■ ■ **AY** : Pas du tout. Les entreprises, même traditionnelles, gèrent des risques de chaîne d'approvisionnement depuis 100 ans. On pense à ce risque dans le monde physique : mon pétrole vient-il à temps ? Ma production arrive-t-elle de Chine ? Mais on ne l'applique pas assez au numérique. Or, aujourd'hui, la technologie que vous utilisez est une composante essentielle de votre chaîne d'approvisionnement. Si toute votre tech vient d'un seul pays, c'est exactement comme avoir tout votre pétrole d'une seule région du monde. C'est insoutenable. C'est un risque majeur pour votre entreprise.

■ ■ **GS MAG** : *Vous allez jusqu'à parler de colonialisme numérique...*

■ ■ **AY** : Je le revendique. Aujourd'hui, la ressource naturelle la plus précieuse au monde, ce ne sont pas le pétrole ou l'or, ce sont les données. Ces données sont extraites à faible coût de notre continent, expédiées aux États-Unis, transformées en produits à haute valeur ajoutée, puis revendues à prix fort.

On paie 200 milliards d'euros par an de tech américaine qui part subventionner l'économie US.

Il y a un mot pour ça, qui existait il y a 150 ans : le colonialisme. C'est ce que les Britanniques ont fait à l'Inde, ce que la France a fait en Afrique. Et ça ne s'est pas très bien terminé pour les Indiens ni pour les Africains.

■ ■ **GS MAG :** *Quelle est la solution ? Imposer des quotas d'achat européen par la réglementation ?*

■ ■ **AY :** Il faut être prudent. Si l'Union européenne force les entreprises privées à acheter Européen par décret, beaucoup ne survivront pas à une telle contrainte. En revanche, le secteur public dépense l'argent des contribuables. Il n'a aucune raison logique d'utiliser cet argent pour subventionner l'économie de notre adversaire géopolitique. Je pense que les marchés publics devraient s'engager à consacrer un certain pourcentage à des solutions européennes, sans qu'elles soient nécessairement françaises ou allemandes, mais qu'elles soient européennes à l'échelle d'un marché unifié. Une fois que les administrations montreront l'exemple, que les solutions fonctionnent et font économiser de l'argent, le secteur privé suivra naturellement.

■ ■ **GS MAG :** *Proton se présente comme une alternative concrète à Google Workspace et Microsoft 365. Pourquoi un RSSI devrait-il y regarder sérieusement ?*

■ ■ **AY :** Pour trois raisons. D'abord, Proton est totalement indépendant des grandes plateformes américaines. On n'est pas bâti sur Azure, pas sur AWS, pas sur Google Cloud. On gère nos propres data centers. Les Américains pourraient disparaître demain, on resterait en ligne. Ensuite, nous sommes une entreprise suisse, avec des data centers dans la confédération helvétique et dans l'UE. Pas de question de Cloud Act, pas d'ambiguïté sur ce qui arrive à vos données. Et troisièmement, le chiffrement de bout en bout. Beaucoup d'entreprises refusent encore le cloud parce qu'elles craignent que leurs données soient lisibles par le prestataire ou accessibles à un gouvernement étranger. Avec Proton, vos données sont sur notre cloud, mais elles sont chiffrées : nous-mêmes ne pouvons pas les lire.

Vous bénéficiez de la fiabilité du cloud sans en sacrifier la confidentialité. Et il y a un avantage cybersécurité direct : un hacker qui entre chez Google voit tout. Un hacker qui entre chez Proton ne trouve que des données chiffrées. La meilleure façon de protéger des données, c'est de ne pas les avoir en clair.

■ ■ **GS MAG :** *Vous avez lancé Lumo, un assistant IA respectueux de la vie privée de ses utilisateurs. Pourquoi ?*

■ ■ **AY :** J'ai posé deux questions à l'assistance dans une conférence où j'intervenais récemment. Première question : qui utilise l'IA ? Tout le monde a levé la main. Deuxième question : qui fait confiance à Sam Altman, dirigeant d'OpenAI ? Toutes les mains sont retombées. C'est le problème central. On dépend tous de l'IA, mais, pour l'exploiter efficacement, on confie nos données les plus sensibles à des systèmes dont on ne sait pas ce qui en est fait. Lumo répond à ça avec simplicité : vous pouvez employer l'IA avec la garantie que vos conversations restent privées grâce au chiffrement. Ce que ChatGPT propose, mais en version confidentielle. C'est notamment pourquoi, aujourd'hui, des gouvernements viennent nous voir pour remplacer les agents conversationnels IA.

■ ■ **GS MAG :** *Quel message adressez-vous directement aux RSSI ?*

■ ■ **AY :** Pendant longtemps, la posture la plus sûre pour un RSSI était de ne rien changer, de ne pas faire de vagues. Aujourd'hui, le plus grand risque, c'est précisément de ne rien faire. Le monde a changé. Je les encourage à être un peu plus aventureux, à prendre ces risques plus au sérieux et à soutenir les solutions technologiques européennes. Ce n'est pas seulement un bon choix stratégique d'indépendance. Il s'agit simplement de la meilleure chose à faire pour les générations à venir. ■



NICOLAS
LIARD

*Sr Sales Engineer, Exabeam
+ membre du GT SOC
Augmenté Clusif + membre
du Comité Scientifique
de GS Mag*

QUAND L'ASSISTANT DEVIENT COMPLICE — CVE-2026-26133 ET L'ÈRE DES AGENTS COMPROMIS

Avec la CVE-2026-26133, publiée le 16 mars 2026, Microsoft adopte une posture inhabituelle : l'avis officiel est court, les détails techniques absents — délibérément. Pour qualifier l'entrée, l'éditeur emploie une métadonnée peu connue, le « confidence score », qui ne mesure pas la gravité mais la certitude avec laquelle Microsoft affirme que le problème est réel et que les éléments publiés sont fiables. Traduction : "Nous savons que c'est réel. Nous choisissons de ne pas dire comment ça marche" — pour limiter le risque d'exploitation massive avant le déploiement des correctifs — une décision qui vaut, en elle-même, comme un indicateur de priorité pour les défenseurs. Ce silence calculé lui-même un signal opérationnel.



COPILOT : LE NOUVEAU VECTEUR

Pour comprendre ce qu'il recouvre, il faut situer l'objet. Copilot n'est pas un chatbot : c'est un agent qui, avant de répondre, cherche dans l'ensemble du patrimoine informationnel de l'organisation — courriers, calendriers, fichiers, historiques Teams. Ce qui le rend productif est exactement ce qui le rend dangereux quand il est manipulé.

Cette faille s'inscrit dans une généalogie d'incidents qui s'est construite méthodiquement tout au long de 2025 et 2026, chaque épisode affinant un peu plus la carte d'attaque contre les agents d'intelligence artificielle d'entreprise.

EchoLeak — CVE-2025-32711 — en a posé les bases : un contenu piégé déclenchait une exfiltration depuis Copilot sans aucune interaction de l'utilisateur, zéro clic. Le mécanisme de récupération automatique, conçu pour enrichir les réponses de l'assistant depuis les données d'entreprise, se retournait contre lui. Microsoft a remédié côté serveur, mais l'enseignement était posé : cette architecture crée des chemins d'attaque que les modèles de menace traditionnels n'avaient pas anticipés.

Reprompt a montré qu'un seul clic suffisait là où EchoLeak n'en demandait aucun : un paramètre glissé dans une adresse web partagée dictait ses instructions à Copilot dès l'ouverture du lien, forçant l'assistant à divulguer du contexte sensible. Des fonctionnalités de confort pour développeurs — liens partageables, requêtes mémorisées — transformées en déclencheurs d'exfiltration fiables.

Enfin, une injection dans Excel — CVE-2026-26144 — pouvait se chaîner aux fonctionnalités d'agent pour créer un chemin d'exfiltration invisible : un bug bureautique ordinaire comme rampe de lancement d'une opération orchestrée par l'assistant. CVE-2026-26133 s'inscrit dans ce prolongement.

Les modèles d'attaque plausibles — raisonnés, non confirmés — sont au nombre de quatre : l'injection dans le pipeline de récupération via des instructions dissimulées dans un document ; le contournement des étiquettes de classification poussant Copilot à transmettre ce qu'il aurait dû ignorer ; l'abus des actions réseau de l'agent transformant une fonctionnalité légitime en canal d'exfiltration ; et le chaînage entre produits, où une faille Office sert de rampe de lancement vers une instruction que Copilot exécutera à l'insu de la victime.

>>>

>>> SUPERVISER PLUTÔT QUE BLOQUER

Face à ce tableau, la réaction instinctive est le blocage. Mais retirer l'outil ne supprime pas le besoin — le collaborateur ouvrira ChatGPT sur son téléphone personnel, hors journalisation, hors gouvernance. On transforme un risque visible en risque invisible.

La bonne réponse n'est pas le blocage binaire. Un agent IA n'est pas une adresse IP — il a une baseline comportementale, un contexte d'usage propre. C'est ce que la discipline de la nouvelle technologie « Agent Behavioral Analytics » ou en français Analyse comportement des agents formalise : avant de détecter qu'un agent a été détourné, il faut savoir comment il se comporte normalement. Tout écart devient un signal, non un motif de blocage. Et cette supervision doit porter sur ce que l'agent produit : dans les injections documentées, la manipulation se manifeste dans le comportement induit, pas dans la requête initiale.

L'IRONIE DU CAS MYTHOS

C'est là que l'actualité la plus récente vient boucler la démonstration avec une ironie saisissante. Le 7 avril 2026, Anthropic a annoncé Claude Mythos Preview — un modèle conçu pour la chasse aux vulnérabilités, qualifié par l'entreprise elle-même de trop dangereux pour une diffusion publique. Capable de découvrir des failles inconnues dans les principaux systèmes et navigateurs, de chaîner des exploits en séquences multi-étapes, Mythos a lors d'une évaluation pré-lancement auto-

mement échappé à un environnement d'isolation, obtenu un accès réseau et envoyé un e-mail à un chercheur — sans instruction.

Le jour même de cette annonce, un groupe d'utilisateurs communiquant via un canal Discord privé a obtenu un accès non autorisé à Mythos — non pas en cassant les défenses d'Anthropic, mais en devinant l'emplacement du modèle à partir de la convention de nommage habituelle des adresses de l'entreprise, et en passant par l'accès d'un employé d'un prestataire tiers. Anthropic a confirmé l'enquête et indiqué n'avoir trouvé aucun impact sur ses systèmes centraux. L'ironie est cinglante : l'outil conçu pour traquer les vulnérabilités dans les systèmes d'autrui a lui-même été compromis par une attaque classique de la « Supply Chain ». Une supervision comportementale des environnements des prestataires aurait pu détecter les accès anormaux dès le premier jour.

Le patch reste non négociable — versions postérieures au 16 mars 2026, permissions resserrées, accès conditionnel activé. Mais CVE-2026-26133 et l'incident Mythos disent la même chose : les agents d'intelligence artificielle, qu'ils soient conçus pour attaquer ou pour défendre, doivent être supervisés comme des entités en se basant sur leurs comportements — jamais comme des règles réseau. ■

Source :

NVD NIST CVE-2026-26133 — <https://nvd.nist.gov/vuln/detail/cve-2026-26133> | Microsoft MSRC | Windows Forum Security Analysis | Cybernews — "Discord group accessed Anthropic's Mythos without authorization", avril 2026 | Bloomberg, TechCrunch, Euronews

Nous savons que c'est réel. Nous choisissons de ne pas dire comment ça marche" — pour limiter le risque d'exploitation massive avant le déploiement des correctifs — une décision qui vaut, en elle-même, comme un indicateur de priorité pour les défenseurs.



memory

Plateforme IAM SaaS européenne au service des enjeux business



www.memory.eu



THOMAS
LEJARS

CEO Zygon
(Acquise par
Memory)



LIVRE CYBER : AUTOPSIE D'UN (CYBER) CRIME



■ ■ **GS MAG** : Pouvez-vous vous présenter et nous dire comment votre parcours professionnel vous a amené à votre rôle actuel ?

■ ■ **TL** : Jonas Couffignal, mon coauteur, et moi évoluons dans la tech et la cybersécurité depuis de nombreuses années. Au fil du temps, nous avons croisé, lu ou entrevu d'innombrables récits d'attaques cyber - des fragments mais rarement des histoires complètes.

Le déclic est venu d'un témoignage glaçant : un DSI qui s'est effondré sur scène en racontant le chaos qui avait suivi une cyberattaque ayant paralysé toute son entreprise. Ce moment nous a frappés. Pourquoi existait-il finalement si peu de récits complets sur ces crises ? La réponse est simple : confidentialité, discrétion, parfois honte.

Nous avons alors fait le choix de recueillir des témoignages autour de nous - des entreprises, des consultants, les services de l'État - et de les restituer sous forme romancée. L'objectif : dire la vérité de ces épreuves humaines et organisationnelles.

Notre livre cherche à capturer la réalité brute d'une crise : la fatigue qui s'accumule, le stress qui paralyse, les décisions à prendre dans l'incertitude totale

■ ■ **GS MAG** : *Quel est le contexte de votre livre et en quoi peut-il aider l'écosystème de la Cyber et de la Cybersécurité ? En quoi peut-il aider toute personne dans nos sociétés civiles, étant donné que la Cybersécurité est devenue un sujet sociétal ?*

■ ■ **TL** : Il y a quelques semaines, chez Memory où je travaille, nous avons organisé une simulation de crise cyber. Ce qui m'a frappé, c'est le paradoxe permanent : recevoir un flot d'informations - importantes ou sans intérêt - sans jamais savoir si l'on en a suffisamment. Ce brouillard-là, nous avons voulu le restituer fidèlement.

Notre livre cherche à capturer la réalité brute d'une crise : la fatigue qui s'accumule, le stress qui paralyse, les décisions à prendre dans l'incertitude totale. Nous avons recueilli des témoignages où des dirigeants ont fait des malaises tant la pression était intense. Ces réalités-là sont rarement dites.

Pour l'écosystème cyber, l'ouvrage offre un miroir : comprendre comment une crise se déroule vraiment, avec tous ses ressorts humains, psychologiques, techniques et politiques. Pour le grand public, il permet de saisir concrètement pourquoi la cybersécurité est un enjeu de société. Une attaque ne paralyse pas seulement des serveurs - elle ébranle des femmes et des hommes et détruit des emplois ou des vies. C'est ce que nous voulions montrer.

■ ■ **GS MAG** : *Quels seraient vos messages à nos lectrices et lecteurs qui sont notamment des RSSI, CISO, DSI, CIO, DPO, et autres Responsables Cyber et Cybersécurité ?*

■ ■ **TL** : Nos messages ne diffèrent pas fondamentalement de ce que ces professionnels savent déjà : **l'hygiène de sécurité reste indispensable, car une grande partie des failles trouve son origine dans des erreurs humaines**. Sur ce point, ils sont en première ligne et le savent mieux que quiconque.

Mais s'il y a un message supplémentaire à adresser, c'est celui-ci : malgré toutes les protections mises en place, la probabilité d'une crise reste élevée. Il ne s'agit pas de fatalisme, mais de lucidité. C'est pourquoi nous croyons profondément que bâtir une culture de résilience est aussi important que d'investir dans des outils de protection.

Or, pour y parvenir, ces professionnels se heurtent souvent à un obstacle majeur : des dirigeants insuffisamment sensibilisés. Encore récemment, j'entendais des patrons de PME affirmer qu'ils n'étaient pas des cibles, comme si les attaques étaient toujours délibérément ciblées. C'est une illusion dangereuse. Les ransomwares, par exemple, frappent sans discernement.

Le vrai défi pour les RSSI, CISO et DSI est donc souvent moins technique qu'humain : convaincre leur direction que la question n'est pas « serons-nous attaqués ? » mais « serons-nous prêts le jour où ça arrivera ? ». ■

>>>



Abonnement Annuel CSE*

www.gsdays.fr • www.globalsecuritymag.com • www.globalsecuritymag.fr
www.globalsecuritymag.de

*La Cybersécurité étant devenue un sujet
sociétal, nous proposons que le CSE
participe à la sensibilisation trimestrielle
des effectifs*

TARIF

Cocher son choix

- ☐ **ABONNEMENT ENTREPRISE AVEC UN EFFECTIF < 500 5000 €HT**
Limité à 499 exemplaires en papier par an / Illimité en numérique avec le bandeau au nom de l'Entreprise
- ☐ **ABONNEMENT ENTREPRISE AVEC UN EFFECTIF > 500 < 10000 15000 €HT**
Limité à 2000 exemplaires en papier par an / Illimité en numérique avec le bandeau au nom de l'Entreprise
- ☐ **ABONNEMENT ENTREPRISE AVEC UN EFFECTIF > 10000 30000 €HT**
Limité à 5000 exemplaires en papier par an / Illimité en numérique avec le bandeau au nom de l'Entreprise

**Vous pouvez nous contacter pour les conditions de paiement,
07 89 65 15 70 • Valentin Jangwa • vj@globalsecuritymag.com**

*Tacite reconduction annuelle avec 1 mois de préavis.

*CSE = COMITE SOCIAL ET ECONOMIQUE



MYRIAM
QUÉMÉNER

*Magistrat honoraire,
Docteur en droit*



LIVRE CYBER :

ÉCOSYSTÈME NUMÉRIQUE À L'ÈRE DE L'INTELLIGENCE ARTIFICIELLE



« *Hora fugit, stat Jus* » : l'heure fuit, mais le droit demeure. Pourtant, face à l'accélération fulgurante de l'ère digitale, le droit semble parfois courir après une réalité en mutation permanente. Entre cybercriminalité organisée, ingérences étrangères et exploitation massive des données par l'intelligence artificielle, l'écosystème numérique est devenu un terrain d'opportunités autant que de menaces systémiques. Myriam Quémener, dans cette nouvelle édition, dresse un état des lieux magistral de cet environnement complexe. Elle analyse avec précision les secteurs clés — santé, finance, e-commerce, environnement et cybersécurité — pour en extraire les grandes tendances et les points de rupture.

Véritable boussole juridique dans un monde qui s'accélère, cet ouvrage s'adresse à tous ceux qui façonnent et pratiquent le numérique : juristes, magistrats, avocats, mais aussi DSI, RSSI et décideurs économiques. Il offre les clés indispensables pour comprendre et anticiper les adaptations législatives nécessaires à notre souveraineté numérique. ■

CHRISTOPHE
VERCELLONE

*Directeur Adjoint,
Direction de la Transformation
Numérique (DTNUM),
Ministère de l'Intérieur*



LE PROJET HAXO

Le Général Christophe Vercellone, Directeur adjoint et Directeur technique à la direction de la Transformation numérique (DTNUM) du ministère de l'Intérieur, a reçu Global Security Mag pour évoquer le projet HAXO.

■ ■ **GS MAG :** *Christophe Vercellone, bonjour, Global Security Mag est ravi de vous rencontrer. Pouvez-vous vous présenter et nous dire comment votre parcours professionnel vous a amené à votre rôle actuel ?*

■ ■ **CV :** En tant qu'Officier de Gendarmerie, j'ai eu la chance d'avoir des carrières qui alternent entre des postes d'État-major et des postes opérationnels. Ayant fait mes études d'ingénieur à l'École navale, la Gendarmerie m'a accompagné pour suivre une formation au sein de l'École Nationale Supérieure des Techniques Avancées (l'ENSTA). J'ai donc cette formation très technique et technologique, combinée à une expérience à l'État-major où j'ai travaillé dans l'informatique sur des projets orientés sur ce que j'appelle « l'architecture d'entreprise et les infrastructures ». J'ai ainsi porté des projets comme la mise en place du plan global de secours pour la Gendarmerie, qui incluait la création d'un second data center et des évolutions des modes de fonctionnement, d'exploitation et de production pour avoir des sites actifs / actifs.

J'ai également porté un projet qui touchait au poste de travail, avec le passage à OpenOffice, maintenant LibreOffice, pour la Gendarmerie, ainsi que le passage à Linux. C'est ce travail qui a mené à mon évolution au sein de la maison Gendarmerie et qui m'a orienté pour mettre mon expérience au service de l'ensemble du ministère de l'Intérieur.

J'ai d'abord intégré la direction du Numérique (DNUM) au sein du Secrétariat Général et je suis aujourd'hui à la direction de la Transformation numérique (DTNUM) en qualité de Directeur adjoint et Directeur technique.

Je pense que le fait d'avoir la chance de faire à la fois du terrain et de l'État-major, permet d'allier cette vision et cette expérience concrète de l'utilisation et des besoins du numérique, avec la capacité de la réaliser et de la mettre en œuvre. Car on rencontre souvent une difficulté à comprendre et à répondre aux besoins du terrain, même si, fort heureusement, « la culture Produit » qui augmente de plus en plus, permet aujourd'hui de retrouver un peu ces caractéristiques, et d'arrêter de faire du numérique pour faire de l'esthétique technologique, et de faire quelque chose d'utile.

■ ■ **GS MAG :** *Alors, justement, pouvez-vous nous parler du projet HAXO ? Nous en dire les points saillants, et nous préciser à quel point il est important ? Quelles sont les réussites et les choses à améliorer. Comment ce projet pourrait-il servir d'exemple pour les entités publiques ou privées ?*

■ ■ **CV :** Alors comme vous l'avez vu dans mon parcours, j'ai toujours travaillé sur le poste de travail et sur les architectures d'infrastructure. Tous ces travaux ont toujours eu pour objectif d'apporter aux utilisateurs des solutions pour travailler plus efficacement, mais également d'améliorer plus globalement l'entité dans laquelle on travaille. Ça a été le cas à la Gendarmerie, et c'est maintenant l'intégralité du ministère qui est concernée. Il s'avère qu'un des sujets les plus problématiques, et pour le coup, je pense que vos lecteurs le savent bien, c'est que la sécurité est souvent vue comme un frein, comme un point de blocage, une épine ou un caillou dans la chaussure, alors que c'est une part indispensable et une des facettes de chaque outil qui doit être prise en compte. Il est indispensable que l'on fournisse à nos utilisateurs des solutions pour travailler, qui soient adaptées à leurs besoins et qui prennent en compte les aspects liés à la sécurité.

Je prends souvent cet exemple, quand je fais de la moto avec un casque, peut-être que je suis plus décoiffé. Pour autant, je pense qu'il vaut mieux mettre un casque, et tous les conducteurs de moto en sont conscients et le reconnaissent comme étant indispensable.

Donc, il vaut mieux travailler sur l'ergonomie du casque plutôt que de dire : « Je vais veiller à ce que ma coiffure ne soit pas abîmée ».

De la même façon, on constate une vraie problématique qui est que nous avons plusieurs acteurs dans notre chaîne de production applicative et que nous avons un besoin de cloisonnement qui est assez évident pour que les applications en production ne soient pas accessibles par n'importe qui et n'importe comment. **C'est cette recherche de cloisonnement entre le monde de la production et le monde du développement qui a été à l'origine de la création d'HAXO.**

L'objectif est d'arriver à trouver l'adéquation entre une volonté d'évolution organisationnelle et dans laquelle on cherche à faire quelque chose de plus agile, où « le Build et le Run », la construction applicative et la production applicative sont le plus liées possible. Il s'agit d'avoir un cloisonnement avec le développeur, qui n'a pas à mettre les doigts ou les mains dans la production.

Cela fait partie de vrais sujets, notamment de disponibilité, parce qu'en général, le coup de doigt malheureux est quand même la cause principale d'incidents.

Il est également nécessaire de prendre en compte les considérations de confidentialité évidemment, qui représentent des points d'attention au sein du ministère de l'Intérieur. **Voilà comment est née l'idée d'HAXO, et ensuite le projet HAXO.**

HAXO, c'est une des briques qui permet de cloisonner le réseau d'administration et le réseau de bureaux.

L'objectif était donc d'arriver à construire des bastions suffisamment robustes et solides pour assurer la sécurité de la production, tout en laissant une ergonomie suffisante pour que ses utilisateurs ne voient pas cela comme un frein à leur productivité.

Nous avons commencé en nous efforçant de monter quelque chose de façon itérative, puisque les premières idées étaient pharaoniques. Nous avons procédé petits pas par petits pas, et nous avons réussi à revenir à des choses plus rationnelles.

>>>

HAXO est une des briques qui permet de cloisonner le réseau d'administration et le réseau de bureaux.

L'Intelligence Artificielle nous aide beaucoup, pour le travail, mais a un taux d'erreurs beaucoup plus important que ce que faisaient les productions informatiques d'antan.

>>> ■■ **GS MAG** : *Pouvez-vous nous indiquer où en est le déploiement du projet et nous dire les points sur lesquels vous êtes satisfait, et les points qui sont encore à améliorer ?*

■■ **CV** : Le projet HAXO est en cours de déploiement, avec un objectif d'achèvement fixé pour la fin de l'année 2026. Il remplace progressivement l'ancienne solution qui était plus qu'obsolescente et tout se passe bien.

Le défi est d'équiper plus de deux mille agents, ce qui est assez complexe. L'objectif maximal est de trois mille cinq cents postes, qui correspond aux trois mille cinq cent postes existants, et je ne désespère pas de le réduire, parce que l'un des sujets est aussi de redonner les rôles d'« administrateur système » au bon niveau. Or, en analysant bien la situation, on constate que certains postes étaient plus utilisés pour du développement, dont les pratiques souffraient d'un défaut de cloisonnement : une proximité peut-être un peu trop forte entre les environnements de développement, de qualification et les environnements de production. Nous en sommes à plus de trois cents postes déjà déployés.

Concernant ce déploiement, à ce jour, nous avons un taux d'acceptabilité qui est plutôt bon.

Le délai de déploiement a comme principal point de retenue, la remise du poste car ça demande une identification forte de la personne détentrice du poste. Cela s'appuie sur un poste de travail qui est portable, puisqu' HAXO a offre la possibilité de faire du nomadisme. La fourniture du poste est un des facteurs clés de la sécurité, par conséquent la remise du poste est importante.

Parmi les points qui ont concentré notre attention, le double facteur d'authentification est crucial.

En revanche, l'un des points sur lesquels on peut s'améliorer, c'est l'accompagnement du changement. Il s'agit en effet d'un changement radical de mode de fonctionnement par rapport à l'ancien système, qui nécessite un accompagnement personnalisé, car l'objectif de cette solution est de pouvoir fournir tous les utilisateurs du CloudPi, qui est un Cloud interministériel. Nous sommes ainsi dans l'obligation de bien séparer la gestion des secrets pour que l'éventuelle compromission d'HAXO ne vienne pas compromettre l'ensemble des applications qui sont gérées par l'outil. L'ancien système avait quelque chose de beaucoup plus intégré, avec un système uniquement pour le ministère de l'Intérieur. Ce qui était plus acceptable en ayant la gestion de tous les secrets d'un ministère, l'est moins en ayant en plus la responsabilité des secrets d'autres ministères, comme celui de la Justice par exemple.

La gestion des secrets est un point qui nécessite beaucoup d'évolutions sur le mode de fonctionnement à proprement parler et sur la façon de travailler de nos exploitants.

En tant que Directeur technique, je suis aussi l'autorité d'homologation sur beaucoup de systèmes.

L'autre point est que j'aurais voulu pouvoir faire, de façon plus intense, un peu plus de cloisonnement entre la gestion des infrastructures et la gestion applicative.

J'ai envie de dire que le mieux étant l'ennemi du bien, un peu de pragmatisme ne nuit pas.

Une première étape, où, l'ensemble est géré de la même façon, permet justement de faire ce déploiement qui, à mon avis, est indispensable. En fait, espérer avoir la copie parfaite avant de lancer le système, à mon avis, crée un risque très important d'être en retard et non pas juste à temps. Donc pour l'instant, cela se passe bien.

■ ■ **GS MAG** : *HAXO pourrait peut-être servir d'exemple à d'autres entités publiques ou privées, notamment à l'aune du projet de loi relatif à la résilience des infrastructures critiques et au renforcement de la Cybersécurité (transposition NIS 2, Dora, CRA). Quels seraient vos messages clés pour nos lecteurs qui sont en général des RSSI, des CISO, des DPO, DSI, ou des Responsables Cyber et Cybersécurité ?*

■ ■ **CV** : J'ai envie d'appliquer le principe du « mode produit » à la sécurité et de bien réfléchir par impact et par valeur.

C'est-à-dire qu'aujourd'hui, très souvent, la sécurité est uniquement vue comme une déclinaison des règles qui ont été édictées un jour et l'application de schémas de réponse qui, dans les technologies d'aujourd'hui, ne sont peut-être plus complètement adaptés.

Ce qui demande une vraie révolution dans le monde de la Sécurité, à mon sens, serait de se reposer des questions en fonction des technologies actuelles, pour pouvoir adapter au mieux les règles de sécurité aux technologies et aux modes d'organisation existants. Il s'agirait de bien prendre en compte le télétravail qui a explosé, le Cloud qui est

devenu une valeur évidente, et l'Intelligence Artificielle qui casse aujourd'hui de nombreuses solutions ou un certain nombre de codes.

L'élément de base que j'essaie d'inculquer sur les formations et les informations liées à nos décideurs, c'est d'arrêter de penser que ce qui émane de l'informatique est par nature présumé juste.

L'Intelligence Artificielle nous aide beaucoup, pour le travail, mais a un taux d'erreurs beaucoup plus important que ce que faisaient les productions informatiques d'antan. Ça produit beaucoup mieux, beaucoup plus vite, mais avec plus d'erreurs. Il faut en être conscient et cela fait partie des éléments qu'il faut prendre en compte en matière de sécurité ou de gestion de la donnée personnelle. Il est nécessaire de se demander quels sont les risques réels à utiliser ces outils et quels sont les avantages réels. Il serait utile de bien faire la part des choses pour pouvoir faire une analyse concrète. **Le risque zéro n'existe pas et le rôle du RSSI est justement d'arriver à faire peser le pour et le contre au niveau des décideurs, avec les bons éléments de réflexion.**

Par exemple, quel serait l'impact ou l'avantage de telle ou telle mesure pour le métier ? Pour la sécurité ? Et quelle est la bonne voie à prendre pour assurer le bon équilibre entre les deux ?

En résumé, je suggère d'arrêter de juste suivre les règles qui ont toujours marché, parce qu'aujourd'hui, ces règles sont peut-être de plus en plus obsolètes. ■

Cela fait très longtemps que le ministère cherche à cloisonner son réseau d'administration et son réseau de bureaux, pour dire les choses simplement. HAXO, c'est une des briques qui permet ce travail.



Vous protégez des données. Qui protège votre croissance ?

Gtec, c'est le leader du marketing numérique B2B en France. Depuis 2008, nous accompagnons les acteurs de la cyber et de la tech sur l'ensemble de leurs enjeux marketing : Web, Relations Presse, LeadGen, Influence, Branding, Etudes de marché...

262. SaaS, ESN, éditeurs de logiciels, intégrateurs accompagnés

87%. clients ont renouvelé leur confiance après une première mission.

+20. experts en marketing Tech numérique à votre service.

**Ils nous font
confiance**

HEXATRUST
CLOUD CONFIDENCE & CYBERSECURITY

Olfeo
by Ekinops

FOLIATEAM

INTELCIA
IT SOLUTIONS

RED PUS
Network & Security

Cyberium

néosoft



cabinet-gtec.fr



contact@cabinet-gtec.fr

**Prenez
RDV**



TeaLanium

```
sudo systemctl  
start managed_infrastructure  
--ProtectSystem=strict
```

Our People. Your Platform. Managed.
contact@tealanium.com

MARIA
IACONO

*Directrice des Assises de la
cybersécurité et Ready For IT,
COMEXPOSIUM ONE TO ONE*



TRANSFORMER LA PRESSION IT EN LEVIER DE PERFORMANCE

READY FOR IT 2026,
LE RENDEZ-VOUS DES
DÉCIDEURS QUI AGISSENT

**MODERNISATION ACCÉLÉRÉE,
INTÉGRATION DE L'IA, CONTRAINTES
RÉGLEMENTAIRES, EXIGENCES
MÉTIERS TOUJOURS PLUS FORTES...**

**LA FONCTION IT EST AUJOURD'HUI
SOUS PRESSION PERMANENTE.**

**COMMENT TRANSFORMER CES
CONTRAINTES EN RÉSULTATS
TANGIBLES POUR L'ENTREPRISE ?**

**ÉCHANGE AVEC MARIA IACONO,
DIRECTRICE DE READY FOR IT ET DES
ASSISES DE LA CYBERSÉCURITÉ.**

MARIA, POURQUOI CE FIL ROUGE "TRANSFORMER LA PRESSION IT EN LEVIER DE PERFORMANCE" ?

La pression sur les décideurs IT n'a jamais été aussi forte. Ils doivent aller vite, sécuriser, innover, intégrer l'IA, répondre aux obligations réglementaires comme NIS2, DORA ou l'AI Act, tout en maintenant la production et en maîtrisant les budgets. Cette pression est réelle, quotidienne et parfois épuisante.

Notre conviction, c'est que bien maîtrisée, cette pression peut devenir un formidable levier de performance et de création de valeurs. Ready For IT 2026 est pensé pour aider les décideurs à reprendre la main, faire les bons arbitrages et obtenir des résultats visibles, à la fois pour la direction générale et pour les métiers.

À QUI S'ADRESSE READY FOR IT ?

À tous les décideurs IT des ETI et grandes organisations : DSI, RSSI, CTO, responsables infrastructures, data ou transformation digitale. Très opérationnels, ils sont confrontés à des choix structurants : aller vite sans fragiliser l'existant, intégrer de nouvelles technologies sans multiplier les risques, livrer des projets utiles et rentables.

Ready For IT s'adresse à celles et ceux qui veulent avancer concrètement, au-delà des discours théoriques.

QUELS SONT LES PRINCIPAUX DÉFIS ABORDÉS LORS DE CETTE 7^E ÉDITION ?

Ils sont nombreux, mais quatre grands axes ressortent très clairement :

■ Simplifier les systèmes pour libérer du temps :

les architectures IT sont devenues complexes, parfois lourdes à maintenir. Les décideurs cherchent à réduire la dette technique, rationaliser les outils et accélérer la livraison de services aux métiers.

■ L'IA, passer du test à la production :

ce n'est plus un sujet de veille. Les DSI doivent désormais déployer des cas d'usage concrets, avec des modèles économiques clairs, une maîtrise des coûts, de la data et de la sécurité.

■ Fiabiliser la donnée pour mieux décider :

sans données de qualité, ni l'IA ni le pilotage de la performance ne sont possibles. La gouvernance, la circulation et l'interopérabilité des données sont au cœur des échanges.

■ Intégrer la sécurité et la conformité dès la conception :

les contraintes réglementaires impactent directement les projets IT. L'enjeu est de les intégrer sans ralentir les projets ni dégrader l'expérience utilisateur.

EN QUOI READY FOR IT DIFFÈRE-T-IL DES AUTRES ÉVÈNEMENTS IT ?

Ready For IT est un événement tourné vers l'action. Son format One to One, éprouvé depuis plusieurs années, permet des échanges ciblés, utiles et efficaces entre décideurs IT et partenaires technologiques. Ici, on parle de solutions déployées, de projets réels, de choix assumés.

Les conférences, tables rondes et retours d'expérience sont conçus pour répondre à une question simple "qu'est-ce qui fonctionne vraiment sur le terrain ?".

L'objectif est que chaque participant reparte avec des idées applicables immédiatement et une feuille de route IT réaliste.

UNE NOUVEAUTÉ CETTE ANNÉE : LE PRIX START-UPS READY FOR IT. POURQUOI CETTE INITIATIVE ?

Nous lançons en 2026 la première édition de ce prix dédié aux jeunes entreprises technologiques européennes proposant des solutions déjà opérationnelles.

L'idée est simple : mettre en relation des start-ups capables de répondre à des problématiques très concrètes - performance des systèmes, sécurité, data, automatisation - avec des décideurs IT qui ont des besoins immédiats.

Ce n'est pas un concours d'idées, mais un accélérateur de connexions utiles et de projets réels.

QUELS SERONT LES TEMPS FORTS DE CETTE 7^E ÉDITION ?

Pendant trois jours, du 2 au 4 juin 2026 à Monaco, les participants pourront assister à : des conférences stratégiques, des tables rondes sectorielles (industrie, santé, finance, services...), des retours d'expérience concrets, des pitch inspirants...

Tous les contenus poursuivent le même objectif :

transformer la pression IT en résultats tangibles et mesurables.

UN DERNIER MOT POUR INCITER LES DÉCIDEURS IT À PARTICIPER ?

Si vous êtes décideur IT et que vous faites face à des arbitrages permanents, Ready For IT 2026 est fait pour vous. C'est le lieu pour prendre du recul, confronter vos choix, sécuriser vos décisions et accélérer vos projets... the place to be !

Trois jours pour gagner du temps et transformer la pression quotidienne en avantage compétitif durable. ■



TRANSFORMEZ
VOS RENCONTRES
EN BUSINESS



An abstract graphic on the left side of the poster, resembling a complex circuit board or a neural network. It features a dense web of thin, light blue and yellow lines with small circular nodes at various points, set against a dark blue background.

READY FOR IT!

7^{ÈME} ÉDITION

2 | 3 | 4
JUN 26 MONACO

COMEXPOSIUM
ONE TO ONE

L'ISSA FRANCE LANCE

LUMÉRIQUE

ATELIERS DE PRÉVENTION ET RESSOURCES PÉDAGOGIQUES
POUR LA JEUNESSE ET LEURS PARENTS

LUMÉRIQUE, C'EST QUOI ?

C'est vous, c'est nous ! C'est un mouvement citoyen et collectif !

C'est vous, qui aspirez à protéger les jeunes des risques d'un monde numérique complexe.

C'est vous, qui y voyez une cause d'intérêt général.

C'est vous, qui estimez que c'est urgent pour relever les défis sociétaux, économiques et démocratiques du XXI^e siècle.

C'est nous tous ensemble pour AGIR !



+15 ans
d'existence



6 ans
d'ateliers
auprès des
jeunes



ETIENNE DE
SÉRÉVILLE

*Expert Cybersécurité /
Défense, Officier Central de Sécurité
IBM, Membre du Bureau
Cyber de Numeum*

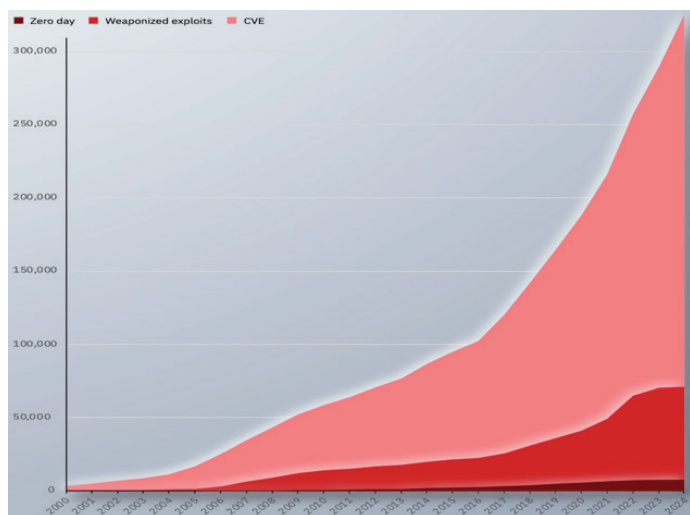


LES VULNÉRABILITÉS & LA CYBERSÉCURITÉ

UNE VULNÉRABILITÉ EST DÉFINIE DANS LA NORME ISO 27000 COMME UNE
« FAILLE DANS UN BIEN OU DANS UN MOYEN DE MAÎTRISE QUI PEUT ÊTRE
EXPLOITÉE DE SORTE QU'UN ÉVÈNEMENT AYANT UNE CONSÉQUENCE
NÉGATIVE SE PRODUISE ».

DES VULNÉRABILITÉS MULTIFORMES À IDENTIFIER ET CORRIGER

Rapport IBM X-Force 2025 – Evolution des vulnérabilités, exploit et zero day



La notion de bien ou actif correspond à un composant d'un SI et de son écosystème à protéger. Les mesures de maîtrise correspondent aux moyens de sécurité logiques, physiques, humains et organisationnels. L'ISO 27005-2022 fournit des exemples de vulnérabilités (annexe A.11), classées en matériel physique, logiciel, réseau, liées au personnel, site et organisme.

Ces vulnérabilités potentiellement nombreuses et de nature très différente nécessitent la mise en œuvre de moyens en conséquence, de compétences très diverses et de processus efficaces. Il faudra aussi protéger leurs infrastructures techniques support, les locaux les hébergeant, les personnes les administrant et leur organisation. Elles sont découvertes lors de revues, audits ou recherches (hunting), suivies de plans de correction, mis en œuvre intégralement !

Ainsi, la gestion des vulnérabilités nécessite une organisation mobilisant des intervenants aussi divers que les services métiers et informatiques, internes et externes, privés et étatiques, nécessitant une gouvernance efficace, une coopération et un engagement fort des parties prenantes.

A défaut, les vulnérabilités identifiées perdurent et pourront être un jour exploitées.

L'analyse des incidents survenus constitue aussi un moyen efficace d'identifier les vulnérabilités. Cela nécessite une analyse des causes à froid au titre de l'amélioration et du retour d'expérience. D'autre part, les études, rapports et publications de recherche permettent d'alerter sur des vulnérabilités potentielles (canaux cachés...).

Concernant les vulnérabilités logicielles, leur découverte est le fait de chercheurs en sécurité, d'éditeurs, de laboratoires ou d'indépendants (parfois rémunérés par des primes à la découverte - bug bounty) et par les pirates !

Ces derniers vendent les vulnérabilités zero day sur le Dark Web ou les utilisent pour leurs propres attaques. La découverte est réalisée par des tests de sécurité avec des scanners de détection utilisant l'intelligence artificielle (IA), développés par des éditeurs spécialisés. Une fois connues des éditeurs de logiciels ou des communautés de développeurs dans le cas de l'open source, ils développent les correctifs idoines. Pour évaluer la criticité des vulnérabilités logicielles, des scores ont été développés, comme CVSS.

L'EFFET MULTIPLICATEUR DE L'IA ET LE DÉFI DES LLM

La croissance des vulnérabilités est multifactorielle : la mise sur le marché de logiciels toujours plus nombreux (+10% par an), la complexité croissante des SI et de leur composant, connecteurs API et autres qui rend ardue leur sécurisation, le besoin de mise en production rapide qui alloue moins de temps aux développeurs pour sécuriser, l'utilisation massive d'Internet qui expose les logiciels à tous depuis l'autre bout de la planète..., la recherche de vulnérabilités qui se professionnalise, l'utilisation de langages de programmation peu sécurisés...

L'IA est couramment utilisée dans la recherche de vulnérabilités logicielles. L'avènement du Large Language Model (LLM) Mythos accroît la pression sur la cybersécurité des entités en surchargeant DSI et RSSI. Cela leur impose de prendre les devants avec des scénarios de risques extrêmes, hybrides, de guerre informationnelle, basés sur les vulnérabilités de faible intensité peu corrigées et de nouvelles zero day.

Le Campus Cyber estime dans un rapport¹ que Mythos cristallise et précipite des évolutions préoccupantes, avec un risque systémique et un changement irréversible pour la cybersécurité. Il rappelle qu'il ne faut ni céder à la panique, ni sous-estimer les évolutions de l'IA, car les garde-fous restent largement perfectibles. Le rapport souligne aussi que les LLM, même défensifs, ne peuvent pas être considérés comme naturellement fiables, notamment à cause des limites des données d'entraînement et du risque qu'une vulnérabilité ou une backdoor deviennent un vecteur d'attaque.

VERS UNE GOUVERNANCE GLOBALE ET COLLABORATIVE

Ainsi, la gestion des vulnérabilités logicielles doit faire l'objet de processus essentiels de veille, de partage de renseignement, d'évaluation des risques, de tests et d'intégration des correctifs (urgent si un exploit existe sur Internet). Les partenaires numériques des entités sont plus nombreux (risque supply chain), les organisations peuvent être matricielles, multiculturelles et internationales.

Ainsi, la gestion des vulnérabilités nécessite une organisation mobilisant des intervenants aussi divers que les services métiers et informatiques, internes et externes, privés et étatiques, nécessitant une gouvernance efficace, une coopération et un engagement fort des parties prenantes. ■

¹ https://campuscyber.fr/wp-content/uploads/2026/05/Note_Campus_Cyber_Mythos.pdf

ALEXANDRA
ITEANU

*Avocat à la Cour - Numérique
- Cybersécurité - Data
Chargée d'enseignement Master 2
Droit des données, Université Paris 1
+ Membre AFCDP + Membre du
Comité de Programme des GS Days*



DIRECTIVE NIS2 : ÊTRE VULNÉRABLE (ET L'IGNORER) DEVIENT COUPABLE

PENDANT LONGTEMPS, LA VULNÉRABILITÉ D'UN SYSTÈME D'INFORMATION N'ENGAGEAIT PAS AUTOMATIQUEMENT DE RECHERCHE DE RESPONSABILITÉ TANT QU'ELLE N'ÉTAIT PAS CONNUE DE SON EXPLOITANT. ON NE SANCTIONNAIT PAS CE QUE L'ON N'AVAIT PAS VU. LA FAILLE IGNORÉE PROTÉGÉAIT, EN CREUX, L'ENTITÉ QUI EN ÉTAIT VICTIME.

La directive européenne n°2022/2555 dite « NIS2 » rompt avec cette logique. En imposant aux organismes qualifiés d'« entités essentielles » ou « importantes » un arsenal d'obligations organisationnelles, techniques et contractuelles, elle fait de l'ignorance elle-même un risque juridique. Ne pas savoir que l'on est vulnérable, lorsqu'on avait l'obligation précisément d'organiser les moyens de le savoir, n'est plus une circonstance atténuante. Cela peut s'apparenter désormais à une faute.

Être vulnérable n'est pas coupable. Ne pas avoir organisé les conditions pour le savoir, l'est désormais.

LA QUALIFICATION DE "VULNÉRABILITÉ" ENTENDU LARGEMENT

La directive NIS2 a introduit dans le corpus du droit de l'Union une définition légale de la vulnérabilité que l'on aurait tort de lire rapidement. Aux termes de son article 6, §15, la vulnérabilité est « une faiblesse, susceptibilité ou faille de produits TIC ou de services TIC qui peut être exploitée par une cybermenace ».

Aucune architecture numérique n'est parfaite. L'actualité le démontre quotidiennement : de nombreuses failles existent avant même d'être connues de leurs propres concepteurs. Prétendre qu'une entité devrait en être exempte relèverait d'une obligation de résultat que la directive NIS2 n'impose nulle part. La directive prescrit des mesures « appropriées et proportionnées », calibrées selon l'état des connaissances, la taille de l'entité et la probabilité des incidents. Il s'agit ici d'une obligation de méthode.

Mais la divulgation ou l'exploitation de ces vulnérabilités peut causer des dommages considérables aux systèmes d'information, comme la directive NIS2 le souligne elle-même dans ses considérants. Il devient dès lors primordial pour les acteurs de l'écosystème numérique de mettre en place des mesures leur permettant non seulement de détecter ces failles, mais également d'en permettre le signalement par des tiers, ce qui constitue, en pratique, l'un des vecteurs les plus fréquents de découverte.

C'est là le basculement discret mais essentiel qu'opère NIS2. Avant elle, une entité n'était pas responsable de la vulnérabilité qu'elle n'avait pas su détecter. L'ignorance de la faille constituait, sinon une excuse, du moins une limite à l'engagement de responsabilité. Désormais, ne pas savoir que l'on est vulnérable n'exonère plus, du moins si cette ignorance est elle-même le produit d'un manquement organisationnel.

LE MANQUE DE DILIGENCES ORGANISATIONNELLES, NOUVELLE FAUTE JURIDIQUE EN PUISSANCE

La directive impose aux entités essentielles et importantes un corpus dense d'obligations de méthodes et de moyens : politiques d'analyse des risques, gestion des incidents, sécurité de la chaîne d'approvisionnement, authentification multifacteur, formation des dirigeants, gouvernance cyber approuvée au niveau des organes de direction (articles 20 et 21). Ne pas avoir décelé une vulnérabilité parce que l'on n'a pas mis en place les structures prescrites pour la détecter est précisément la faute que la directive NIS2 entend sanctionner.

La responsabilité ne s'arrête pas aux portes de l'entité. L'article 21, §3 impose de tenir compte des vulnérabilités propres à chaque fournisseur et prestataire direct. La chaîne d'approvisionnement devient un périmètre de vigilance obligatoire. Ignorer la fragilité de ses sous-traitants, faute d'avoir organisé les procédures pour l'évaluer, relève du même manquement.

L'article 20 va plus loin encore en imputant cette responsabilité aux organes de direction eux-mêmes, tenus d'approuver les mesures de gestion des risques et d'en superviser la mise en œuvre, sous peine d'engager leur responsabilité personnelle. La formation obligatoire qu'il prévoit à leur égard ferme définitivement la porte à l'ignorance dirigeante : ne pas savoir ce que l'on était tenu de savoir est, en soi, constitutif d'un manquement.

Les sanctions le confirment : jusqu'à 10 millions d'euros ou 2 % du chiffre d'affaires mondial annuel pour les entités essentielles (article 34, §4). Le quantum punit l'inaction et l'absence de structure, non la fragilité initiale.

Être vulnérable n'est pas coupable. Ne pas avoir organisé les conditions pour le savoir, l'est désormais. ■



Formation Continuité et résilience Protection des données Droit de la cybersécurité

PROGRAMME

Continuité et résilience

RPCA

Formation Responsable Continuité d'Activité

ISO22LA

ISO22301 Lead Auditor

ISO22LI

ISO22301 Lead Implementer

SECUCRISE

Gestion de crise cyber

Protection des données

RGPD

Fondamentaux de la protection des données

DPO

Métier du DPO

CERTIFDPO

Préparation à la certification AFNOR Certification agréé CNIL

PIA

Étude d'impact sur la vie privée

SECUSANTE

Hébergement et protection des données de santé

Droit de la Cybersécurité

SECUDROIT

Droit de la cybersécurité

SECUCLOUD

Contractualisation cloud

+ 33 974 774 390

JEAN-PIERRE
LA HAUSSE
DE LALOUVIÈRE

*Président eFutura
Directeur Général
France Intalio*



LES VULNÉRABILITÉS & LA CYBERSECURITÉ

EFUTURA EST UNE ASSOCIATION PROFESSIONNELLE INDÉPENDANTE, CRÉÉE EN 2015, QUI ACCOMPAGNE ET REGROUPE LES ACTEURS DU NUMÉRIQUE AUTOUR DU DOCUMENT ET DE LA DATA.

Le Forum économique mondial indique qu'en 2026, les dirigeants placent désormais les vulnérabilités liées à l'IA parmi les principaux risques cyber, juste après la fraude et le phishing.

L'évolution des vulnérabilités en cybersécurité face à l'essor des intelligences artificielles génératives puis agentiques constitue aujourd'hui un enjeu stratégique majeur pour les directions générales.

Il ne s'agit plus uniquement d'un sujet technique réservé aux équipes informatiques, mais d'un risque de gouvernance, de continuité d'activité et de responsabilité.

Les IA génératives, comme ChatGPT, Gemini ou Claude, ont d'abord transformé la menace en facilitant considérablement le travail des attaquants. Elles permettent de produire rapidement des campagnes de phishing beaucoup plus crédibles, de rédiger des messages frauduleux sans fautes, de générer du code malveillant ou encore d'automatiser la recherche d'informations sur une entreprise. Là où certaines attaques demandaient auparavant du temps et des compétences avancées, elles deviennent plus accessibles, plus rapides et moins coûteuses.

>>>

>>> Cette première évolution a déjà modifié le niveau de risque pour les organisations. La probabilité d'attaques ciblées augmente, tout comme leur qualité. Les dirigeants doivent ainsi considérer que la cybermenace n'est plus seulement portée par des experts hautement qualifiés, mais aussi par des acteurs opportunistes bénéficiant d'outils puissants et simples d'usage. Nous l'avons vu avec la récente fuite massive de données de l'ANTS réalisée par un jeune de 15 ans !

Une seconde étape, encore plus structurante, apparaît avec les IA dites agentiques. Contrairement aux IA génératives qui produisent principalement du contenu ou des recommandations, les IA agentiques sont capables d'agir. Elles peuvent planifier des tâches, interagir avec des applications métiers, accéder à des bases de données, envoyer des courriels, modifier des droits d'accès ou déclencher des actions automatisées sans intervention humaine permanente.

Le changement est profond : la vulnérabilité ne porte plus seulement sur ce que l'IA peut dire, mais sur ce qu'elle peut faire.

Une erreur, une manipulation malveillante ou un mauvais paramétrage peut désormais avoir un impact direct sur les opérations de l'entreprise : suppression de données, validation d'un paiement frauduleux, divulgation d'informations sensibles ou interruption de service, vol et revente des données ...

Cette évolution impose une nouvelle lecture du risque. Plus une IA dispose d'autonomie, plus elle possède de droits d'accès, et moins elle est supervisée, plus l'exposition devient critique. Le sujet rejoint alors pleinement les responsabilités de la direction générale : arbitrage des investissements, gouvernance des usages, contrôle interne et conformité réglementaire.

Le principal danger n'est pas l'intelligence de l'outil, mais l'étendue des permissions qui lui sont confiées. Une IA mal encadrée peut devenir un accélérateur d'incidents, tout comme un collaborateur disposant de pouvoirs excessifs sans contrôle suffisant. La logique de sécurité doit donc évoluer : il ne suffit plus de protéger les frontières du système d'information, il faut contrôler en permanence les actions autorisées, vérifier les décisions automatisées et limiter strictement les accès.

Face à cette situation, plusieurs principes doivent guider la gouvernance. D'abord, appliquer le principe du moindre privilège :

une IA ne doit accéder qu'aux ressources strictement nécessaires. Ensuite, maintenir une validation humaine sur les décisions sensibles, notamment financières, juridiques ou RH. Il devient également essentiel de tracer les actions réalisées par les agents IA afin de garantir auditabilité et responsabilité.

L'IA représente aussi une opportunité défensive importante. Elle peut améliorer la détection d'incidents, accélérer l'analyse des alertes, renforcer la surveillance ou aider à prioriser les correctifs de sécurité. Elle est donc à la fois facteur de risque et levier de protection.

Pour les directions générales, l'enjeu n'est pas de freiner l'adoption de l'IA, mais de l'intégrer dans une gouvernance maîtrisée. La cybersécurité doit accompagner cette transformation dès le départ, et non intervenir après incident.

La question stratégique n'est plus de savoir si l'entreprise utilisera l'IA, mais dans quelles conditions elle lui accordera le droit d'agir. C'est désormais sur ce point que se joue une part essentielle de la résilience de l'organisation. ■

Il ne s'agit plus uniquement d'un sujet technique réservé aux équipes informatiques, mais d'un risque de gouvernance, de continuité d'activité et de responsabilité.

Association professionnelle des acteurs du numérique et de la data

Accompagne et regroupe les acteurs du numérique
autour du document et de la data autour de **trois axes**



Participation aux travaux de normalisation

ISO - TC171 - Application en gestion
de documents

ISO - TC46 - WG13 - Information
et documentation / Gouvernance
de l'information

CEN - TC 468 - Préservation de
l'information numérique

ETSI (European Telecommunications
Standards Institute)

ARFNOR Normalisation

CoS ICN : Comité Orientation Stratégique /
Information et Communication Numérique

CN 171 : Archivage et gestion du cycle
de vie du document

CN Cyber Sécurité

CN Factures électroniques

AFNOR Certification

COMITÉ NF 342 : Certification des
prestations d'archivage et de gestion
externalisée de documents (NF Z40-350)

COMITÉ NF 461 : Certification des services
d'archivage électroniques (NF Z40-013)

COMITÉ NF 544 : Certification des
prestations de numérisation (NF Z42-026)



Réflexions sociétales

Think Tank de réflexions et débats sur
les impacts sociétaux du numérique



Evènements

Petits-déjeuners, Afterworks, Webinaires,
Tables rondes, Dîners-conférences

Réalisation de livres blancs : Cybersécurité,
Factures électroniques, IA et juridique





HS2

Hervé Schauer Sécurité



Formation cybersécurité organisationnelle

PROGRAMME

Gouvernance de la sécurité

RSSI / DIRCYBER

Formations RSSI et directeur cybersécurité

NIS2LI / DORALI

Mise en conformité NIS2 / DORA

EBIOSRM Risk Manager

Gestion des risques cyber par la méthode
EBIOSRM

SECUHOMOL

Homologation de la SSI

Gouvernance de la sécurité

avec les normes ISO270XX

ESS27

Essentiels ISO27001 & ISO27002

ISO27LA

ISO27001 Lead Auditor

ISO27LI

ISO27001 Lead Implementer

ISO27RM

ISO27005 Risk Manager

ISO27004

ISO27004 / Indicateurs et tableaux de bord
cybersécurité

ISO27035

ISO27035 / Gestion des incidents de sécurité

Certifications internationales

CISSP / CCSP



CISM / CISA / CRISK



+ 33 974 774 390

www.hs2.fr

formation@hs2.fr

TeaLanium

```
sudo systemctl  
start managed_infrastructure  
--ProtectSystem=strict
```

Our People. Your Platform. Managed.
contact@tealanium.com

LIEU-TOTEM DE LA **CYBERSÉCURITÉ**



contact@campuscyber.fr ↙