

N°61

PRIX : 24€ TTC

TRIMESTRIEL

NOVEMBRE > JANVIER 2026

Global Security Mag

THE LOGICAL & PHYSICAL SECURITY MAGAZINE

RETEX NIS 2, DORA, CRA, ISO 27001, RGPD, LA CONFORMITÉ ET LA CYBERSÉCURITÉ

Vers une sécurité numérique souveraine :
relier la réflexion stratégique à l'action collective

p. 46



Anne Le Hénanff
Ministre déléguée chargée de
l'Intelligence Artificielle et du
Numérique

**L'intelligence artificielle
au service du crime
organisé :** l'Europe
face à un dilemme
stratégique

p. 48



Séverine Meunier
Experte en Sécurité
Numérique et Intelligence
Appliquée

**ISO/IEC 27001
fête ses 20 ans :**
une norme,
une communauté,
une vision

p. 64



Emmanuel Garnier
Président Club 27001 et
Directeur Cybersécurité Orano

**Conformité et
Cybersécurité,**
piliers de la souveraineté
numérique européenne

p. 76



**Jean-Noël
de Galzain**
Founder and CEO,
WALLIX Group



OFFERT PAR



LEVAS SAS
CYBER INFO

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

Parlons de vos projets 2026

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

ÉDITO



LA CONFORMITÉ ET LA CYBERSÉCURITÉ

IL PEUT SEMBLER RASSURANT DE SE PENSER CONFORME, ET DE SE PENSER EN CYBERSÉCURITÉ.

La Conformité, c'est communément le fait de correspondre à une norme. Cela pourrait même se traduire par « être normal », ce qui peut rassurer certaines personnes, mais donner envie à d'autres personnes de se distinguer, de marquer leurs différences, d'être originales ou du moins de le paraître...

En matière de Cybersécurité, la Conformité devient de plus en plus la norme...

Une Organisation peut-elle se satisfaire d'être Conforme sans être en Cybersécurité ?

Les Règlements, les Directives, au niveau de l'Europe, les Lois de transposition et les Lois locales, en se multipliant, ont fait de la Conformité et la Cybersécurité, deux sœurs inséparables, deux piliers nécessaires pour lutter contre les cyberattaques incessantes à la fois dans le monde privé et professionnel.

Dans cette édition de Global Security Mag, vous trouverez des écrits passionnants.

Au plaisir !

Valentin Jangwa

COMPLIANCE AND CYBERSECURITY

IT MAY SEEM REASSURING TO THINK OF YOURSELF AS COMPLIANT AND CYBERSECURITY-CONSCIOUS.

Compliance is commonly understood as meeting a standard. It could even be translated as "being normal," which may reassure some people, but make others want to stand out, emphasize their differences, be original, or at least appear to be...

When it comes to cybersecurity, compliance is increasingly becoming the norm...

Can an organization be satisfied with being compliant without being secure?

Regulations, directives at the European level, transposition laws, and local laws have multiplied, making compliance and cybersecurity two inseparable sisters, two necessary pillars in the fight against incessant cyberattacks in both the private and professional worlds.

You will discover fascinating articles in this edition of Global Security Mag.

Enjoy!

Valentin Jangwa

N°61 NOVEMBRE>JANVIER 2026

globalsecuritymag.fr,
globalsecuritymag.com,
globalsecuritymag.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@globalsecuritymag.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 l'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,
Suzanna Nedelec, Anne Guyot,
Nicolas Liard, Christel Olsen,
Daniel Binsfeld et Valentin Jangwa,
In Memoriam, notre regretté Zbigniew
Kostur

SOMMAIRE



1	ÉDITO
4-5	AGENDA & CALENDRIER DES ÉVÈNEMENTS

DÉLÉGUÉ.E À LA PROTECTION DES DONNÉES

6-7	Valentin Thévenot
-----------	-------------------

FEMME ENGAGÉE DANS LA CYBER

8-10	Nolwenn Le Ster
------------	-----------------

POINT DE VUE

12-13	Kilian Chiarelli
-------------	------------------

rencontre aux asises de la cybersécurité

16-18	François Bidondo
20-23	Alain Bouillé

BOXE ET CYBERSÉCURITÉ

24-25	Alban Bennacer
-------------	----------------

THEMA

26-27	Élodie Le Saout
28-29	Florence Giuly-Davis
30-31	Benoit Grünemwald
33-34	Julien Bruant
35-36	Anne Leslie
37-38	Loïc Guézo
40-41	Gérôme Billois
44-45	Jean-Michel Mis

DOSSIER spécial

46-47	Anne Le Hénanff
48-50	Séverine Meunier
52-53	Franck Rouxel

ENTRETIENS

59-61	Odile Duthil
-------------	--------------

CLUB 27001

64-65	Emmanuel Garnier
66-67	Patrick Foubert & Mickaël Ferton

Publi-info

68-69	Davidson consulting
72-75	Scality
76-78	Wallix

L'expert OSINT

82-83	Baptiste Robert
-------------	-----------------

IA ET CYBERSÉCURITÉ

84-85	Jean-Luc Raymond
-------------	------------------

chronique technique

86-89	Nicolas Liard
-------------	---------------

Livre cyber

90-91	Gaëlle Picard-Abezis
92-93	Myriam Quémener & Amelie Köcke
94-95	Etienne De Sérerville
96-97	Renaud Tisserant & Mickaël Vigreux

LES NEWS DU CPI-B2B

98-99	Mountaha Ndiaye
100-101	Laurent Vanel

CHRONIQUE JURIDIQUE

102-103	Alexandra Iteanu
---------------	------------------

L'œil de l'expert

105-106	Jean-Pierre La Hausse De Lalouvière
---------------	-------------------------------------

SUMMARY



1	EDITO
4-5	AGENDA & EVENTS CALENDAR

DATA PROTECTION OFFICER

6-7	Valentin Thevenot
-----------	-------------------

CYBER WOMAN

8-10	Nolwenn Le Ster
------------	-----------------

INSIGHT

12-13	Kilian Chiarelli
-------------	------------------

meetings at Les Assises de la cybersécurité

16-18	François Bidondo
20-23	Alain Bouillé

BOXING & CYBERSECURITY

24-25	Alban Bennacer
-------------	----------------

THEMA

26-27	Élodie Le Saout
28-29	Florence Giuly-Davis
30-31	Benoit Grünemwald
33-34	Julien Bruant
35-36	Anne Leslie
37-38	Loïc Guézo
40-41	Gérôme Billois
44-45	Jean-Michel Mis

SPECIAL FILE

46-47	Anne Le Hénanff
48-50	Séverine Meunier
52-53	Franck Rouxel

INTERVIEW

59-61	Odile Duthil
-------------	--------------

CLUB 27001

64-65	Emmanuel Garnier
66-67	Patrick Foubert & Mickaël Ferton

Publi-Info

68-69	Davidson consulting
72-75	Scality
76-78	Wallix

OSINT EXPERT

82-83	Baptiste Robert
-------------	-----------------

AI & CYBERSECURITY

84-85	Jean-Luc Raymond
-------------	------------------

TECHNICAL TOPIC

86-89	Nicolas Liard
-------------	---------------

CYBER BOOK

90-91	Gaëlle Picard-Abezis
92-93	Myriam Quémener & Amelie Köcke
94-95	Etienne De Sérerville
96-97	Renaud Tisserant & Mickaël Vigreux

NEWS FROM CPI-B2B

98-99	Mountaha Ndiaye
100-101	Laurent Vanel

LEGAL TOPIC

102-103	Alexandra Iteanu
---------------	------------------

THE CYBER EXPERT

105-106	Jean-Pierre La Hausse De Lalouvière
---------------	-------------------------------------

> NOVEMBRE <

- **5 > 6 novembre - Paris**
Tech Show - Big Data & AI
Lieu Porte de Versailles
www.bigdataworld.fr/
- **10 > 13 novembre - Lisbonne (Portugal)**
Web Summit
<https://websummit.com/>
- **18 > 21 novembre - Paris**
Milipol
Villepinte
<https://www.milipol.com/>
- **18 > 20 novembre - Paris**
Salon des Maires
<https://www.salondesmaires.com/>
- **19 > 20 novembre - Dublin (Irlande)**
Salon Datacenters Ireland
<https://10times.com/datacentres-ireland>
- **19 > 20 novembre - Marbella (Espagne)**
IT & Cybersecurity Meetings - Réseaux, cloud, mobilité et cybersécurité
<https://link.veyou-group.com>
- **20 novembre - Londres (UK)**
Technology Live !
<https://a3communicationspr.com/homepage/events/technology-live/>
- **21 novembre - Online**
Conférence AFCDP
<https://universite-des-dpo-2025.afcdp.net/page/c101-accueil/>
- **24 novembre - Paris**
Cyber Night - la Nuit de la Cybersécurité
Lieu : Théâtre Mogador
www.republikgroup-it.fr/cybernight
- **24 > 26 novembre - Riyadh (Arabie Saoudite)**
Black Hat Middle East and Africa
Riyadh international convention and exhibition center
<https://athack.com/>
- **25 > 27 novembre - Londres (UK)**
IFSEC
ExCeL London
www.ifsec.co.uk
- **26 novembre - Paris**
Diner du Cercle de la sécurité
www.lecercle.biz
- **26 > 27 novembre 2025 au MEETT de Toulouse**
7^e édition du CBC Cybersecurity Business Convention
<https://www.opensource-experience.com/>

> DÉCEMBRE <

- **2 > 3 décembre - Reims**
Congrès du CESIN
<https://cesin.fr/>
- **2 > 4 décembre - Porte de Versailles - Paris**
TRUSTECH
<https://www.trustech-event.com/>
- **5 décembre - Stockholm (Suède)**
Data Center Forum
<https://www.datacenter-forum.com/events/stockholm/2025>
- **8 > 10 décembre - Las Vegas (USA)**
Gartner Identity & Access Management Summit
www.gartner.com/en/conferences/na/identity-access-management-us
- **8 décembre - Paris**
6^e du Cyberwomenday
<https://cyberwomenday-cefcys.com/>
- **les 10 et 11 décembre 2025 - Paris**
Cité des Sciences et de l'Industrie
<https://www.opensource-experience.com/>

> JANVIER <

■ 12 > 14 janvier 2026 - Dubaï (EAU)

Intersec
26e édition
www.intersecexpo.com

■ 15 janvier 2026 - Campus Cyber à Paris la Défense
Le panorama de la cybercriminalité du Clusif revient le jeudi 15 janvier 2026 et sera diffusé en direct et en accès libre.

Quels grands enjeux cyber ont ponctué l'année 2025 ? La réponse en images et en conférence avec les experts du Clusif.
 Les inscriptions ouvriront dès le début du mois de janvier !
<https://clusif.fr/agenda/conference-panocrim/>

■ 20 janvier 2026 - Paris 3^e - Espace Saint-Martin
GS Days - Journées Francophones de la Sécurité de l'Information et de la Cyber
16^e édition

Les GS Days, Journées Francophones de la Sécurité de l'Information et de la Cyber, sont organisées en un événement annuel exclusivement en français. Des Tables Rondes, des Conférences, ainsi que des démonstrations d'exploitation de failles informatiques, sont organisées en parallèle.

Ces Conférences abordent la sécurité sous un angle technique, organisationnel et juridique à destination des Expert.e.s sécurité, Administrateurs et Administratrices sécurité, RSSI, DSI, Responsables Cybersécurité...

Les démonstrations réalisées, en partie, en coopération avec les experts de l'ARCSI concernent ces deux typologies de public.

Plusieurs associations professionnelles reconnues sont partenaires de cet événement : L'AGORA RSSI, l'AGORA DSI, le CEFCYS, le Clusif, le Forum ATENA, eFutura, ISSA France, le Chapitre français de l'OWASP, l'ARCSI, le Club 27001, le CESIN, le Club EBIOS, la Fédération Française de la Cybersécurité, HEXATRUST, l'OSSIR, RD-SSI, CLUSIR NORD, l'AFCDP, la FIEEC...

En parallèle à cet événement, un espace sera aussi ouvert à quelques sponsors spécialisés.

Cybermalveillance.gouv.fr, notre parrain institutionnel sera de nouveau présent.

Lieu : Espace Saint-Martin, 75003 Paris
Renseignements : Valentin Jangwa
Tel. : +33 7 89 65 15 70
e-mail : vj@globalsecuritymag.com
Web : www.gsdays.fr

■ 21 > 23 janvier 2026 - Osaka (Japon)

Japan IT Week
www.japan-it-osaka.jp/en-gb.html

■ 26 - 28 janvier 2026 - Tel Aviv (Israël)

Cybertech Goblat Tel Aviv
 Lieu : Tel Aviv Convention Center
www.cybertechisrael.com/

■ 28 janvier 2026 - Helsinki (Finlande)
e-crime & cybersecurity Nordics

<https://akjassociates.com/>

■ 28 > 29 janvier 2026 - Paris

Cyber Show Paris
 Lieu : espace Champerret, Paris 17
<https://www.cybershowparis.fr/fr/>

■ 8 > 29 janvier 2026 - Porte de Versailles - Paris
Learning Technologies

www.learningtechnologiesfrance.com

VALENTIN
THÉVENOT

*Administrateur de l'AFCDP,
DPO et Chargé de Sécurité
du SI Banque BCP
Groupe BPCE*



APPRENDRE À MAÎTRISER L'OSINT POUR MIEUX PROTÉGER NOTRE VIE PRIVÉE, UN PARI GAGNANT ?

**Chercher la note d'un restaurant
avant de s'y rendre, éplucher
les informations légales d'une
entreprise, comparer les prix d'un
futur voyage, peut-être faites-vous
déjà de l'OSINT sans le savoir.**

**De son nom complet
« Open Source Intelligence »
(ndla : renseignement d'origine
sources ouvertes, en français),
l'OSINT est une véritable boîte à
outils de techniques qui, lorsqu'elles
sont affûtées par l'expérience,
peuvent être de véritables leviers
pour mieux protéger nos
données personnelles.**

UNE TECHNIQUE D'INVESTIGATION PAR RICOCHETS

Pendant la seconde guerre mondiale, les alliés étudiaient le prix des agrumes sur les marchés. Si ces prix venaient à fortement augmenter, cela pouvait signifier que les raids aériens menés sur les ponts de la région avaient été fructueux. En effet, un pont détruit signifiait souvent un approvisionnement moindre de certains produits ce qui les rendait mathématiquement plus chers.

Toutefois, corrélation n'implique pas causalité et c'est pour cette raison qu'il est crucial de croiser des sources de façon rigoureuse pour s'assurer de la fiabilité de l'information obtenue.

L'OSINT consiste donc à répondre à une hypothèse de travail par la collecte de données brutes, publiquement accessibles à tous. Chaque donnée, permet ensuite de pivoter vers une autre donnée par un effet de rebond et ce, successivement.

C'est en croisant les données ainsi obtenues que celles-ci acquièrent de l'information et donc de la valeur, ce qui permet de répondre à l'hypothèse de travail et possiblement de réorienter ses recherches et ses moyens, pour prendre de meilleures décisions.

Aujourd'hui, l'OSINT est utilisé par de nombreux professionnels tels que les journalistes, détectives privés, universitaires, recruteurs, mais aussi de façon malveillante par des cybercriminels et cambrioleurs pour repérer leurs prochaines cibles, ou encore dans le cadre de violences sexistes et sexuelles.

DES DONNÉES PUBLIQUES ET LICITES COMME BASE DE TRAVAIL

Si les données utilisées dans la pratique de l'OSINT peuvent être de nature très différentes, elles ont toutes en commun deux caractéristiques : elles doivent être publiques et licites. Une donnée qui aurait été obtenue en pénétrant indûment dans un système d'information mal verrouillé, en récupérant un fichier issu d'une fuite de données ou en violation de la vie privée, n'est donc pas admise dans le cadre d'une démarche OSINT. Il est par conséquent primordial que le cheminement intellectuel de l'enquête en OSINT fasse l'objet d'une traçabilité rigoureuse afin d'en garantir la licéité. Qu'il s'agisse de métadonnées de contenus multimédias, d'informations publiques de réseaux sociaux, de données mises en ligne par une administration ou de cartes satellitaires, les sources sont nombreuses. Pour autant, une bonne enquête OSINT repose avant tout sur la capacité de l'enquêteur à relier les points et à extraire la bonne information de façon rapide.

I KNOW WHERE YOUR CAT LIVES

En 2014, l'artiste et data analyst Owen Mundy créa un site qui localisait sur une carte les photos de chats librement accessibles sur les réseaux sociaux. Pour être répertoriés sur le site d'Owen, les internautes devaient avoir géolocalisé leur photo, l'avoir mise en public et l'avoir identifiée par un « tag » comme étant une photo de chat.

Malgré ces quelques conditions, ce ne sont pas moins de 6 millions de photos qui ont été republiées sur le site d'Owen. Par sa démarche, l'artiste cherchait à mettre en évidence l'étonnante facilité avec laquelle nombre de nos photos étaient en accès libre sur internet, créant ainsi un risque pour notre vie privée.

L'OSINT AU SERVICE DE LA CYBERSÉCURITÉ

Les organisations étant le reflet des individus qui la composent, l'exposition de la vie privée de collaborateurs clefs peut également amener des failles de sécurité pour l'entreprise elle-même. Des informations qui peuvent être utilisées pour des campagnes de hameçonnage ou permettre d'obtenir des informations sensibles non publiques.

En 2024, le journal « Le Monde » avait ainsi révélé que les trajets de course à pied des gardes du corps d'Emmanuel Macron, renseignés sur l'application Strava, permettaient d'en déduire les futurs déplacements du chef de l'État, une fois les lieux repérés et sécurisés. Alors, la prochaine fois que vous publierez une photo sur les réseaux, demandez-vous ce qu'elle dit de vous. ■

Si les données utilisées dans la pratique de l'OSINT peuvent être de nature très différentes, elles ont toutes en commun deux caractéristiques : elles doivent être publiques et licites.

AFCDP

NOLWENN
LE STER

COO Cybersecurity_
Almond-Amossys_
Présidente de la Commission
Cybersécurité de Numeum



LA FILIÈRE CYBER

LORS DE LA 25^E ÉDITION DES ASSISES DE LA
CYBERSÉCURITÉ À MONACO, NOLWENN LE STER A
ACCORDÉ UN ENTRETIEN À GLOBAL SECURITY MAG.
"EN RÉSUMÉ, CE QUI M'ANIME, C'EST LA FILIÈRE CYBER"

■ ■ **GS MAG :** *Nolwenn LE STER, bonjour. Global Security Mag est ravi de vous avoir en entretien. Pouvez-vous vous présenter et nous dire comment votre parcours professionnel vous a amenée à votre rôle actuel ?*

■ ■ **NLS :** Je suis Ingénieure Télécom. J'ai fait la belle école qui est l'IMT (Institut Mines-Télécom) Atlantique, il y a maintenant une grosse vingtaine d'années. Sans revenir sur l'ensemble de mon parcours, je pense que le point commun de toutes mes expériences, c'est d'avoir géré des transformations dans des environnements où l'innovation était un sujet important. J'ai démarré ma carrière dans une SSII (Société de Services en Ingénierie Informatique), ce qui correspond dorénavant à une ESN (Entreprise de Services Numériques). Ensuite, j'ai passé quinze ans chez SPIE ICS

et à l'aube de mes quarante ans, j'ai décidé de me consacrer exclusivement à la Cybersécurité. J'en faisais déjà un petit peu avant, mais là, j'ai décidé de le faire exclusivement parce qu'il me semblait qu'à ce moment-là de ma carrière, c'était important que je puisse aussi travailler non seulement pour mes clients, mais pour la société et pour mes enfants. J'ai trois enfants et donc j'ai choisi de rejoindre le groupe Capgemini où j'ai consolidé et piloté l'activité Cybersécurité pendant cinq ans. Et là, depuis un an, j'ai rejoint le groupe Almond, qui est un « pure-player » Cybersécurité, pour encore augmenter mon impact dans la filière Cybersécurité, cette fois-ci en l'exerçant au travers d'un « pure-player » basé en Europe, avec des ambitions de se développer en Europe pour consolider une plateforme de services européenne qui contribuerait aussi à faciliter l'accès aux acteurs de la tech européenne, à leur marché. Pour moi, c'est un projet personnel d'entreprise, c'est un projet de société pour la filière Cybersécurité.

J'ai la chance par ailleurs d'être la Présidente de la Commission Cybersécurité Numeum depuis maintenant cinq ans. C'est pour moi la possibilité de pouvoir avoir des échanges et coconstruire avec mes pairs autour d'initiatives comme Cyber4Tomorrow, qui est une plateforme web où on a essayé de rassembler des initiatives de Cybersécurité pour engager les professionnels de la Cyber à faire de la Cyber pour la société. En résumé, ce qui m'anime, c'est la filière Cyber.

■ ■ **GS MAG** : *Merci pour votre engagement. Nous reviendrons peut-être un jour là-dessus. Je vous dirai pourquoi. Alors, pouvez-vous nous parler plus spécifiquement de Almond, nous dire en quoi Almond est unique ? Quels sont les points différenciants ?*

■ ■ **NLS** : Almond est un groupe de Cybersécurité et J'aurais envie de dire de Cyber-Résilience. Je vais vous expliquer pourquoi. C'est un « pure-player » présent en France avec des implantations à Paris, à Nantes, Rennes, Strasbourg, Lyon. Nous avons également une activité sur la Suisse et des équipes techniques opérationnelles sur la Corée du Sud et le Canada pour assurer nos services en 24H/24 7J/7.

Nous sommes quatre cent cinquante. Notre offre de services est large. Notre ambition pour les ETI, c'est d'être leur partenaire privilégié depuis l'anticipation du risque cyber, la mise en place des mesures de protection, la détection, la remédiation et bien sûr la gouvernance. Et faisant tout cela, et pour répondre à votre question sur ce qui nous différencie, notre positionnement est celui de l'expertise, un positionnement premium également. Et donc sur chacune des briques que j'ai citées, on ne sait pas tout faire parfaitement, mais ce qu'on fait, on le fait avec un niveau d'expertise et de profondeur. Ça nous anime depuis vingt-cinq ans, date de création de l'entreprise, avec cet ADN tech, qui, je pense, est un deuxième point important après l'expertise. Notre ADN Innovation et Technique fait que Almond est unique. Pour illustrer cela, dix pour cent de notre chiffre d'affaires qui est investi en R&D (Recherche et Développement), ce qui nous permet aussi d'aller encore plus loin.

Cela nous amène au troisième point de différenciation qui est que nous faisons du service outillé et cela veut dire du service qui amène de nouvelles choses sur le marché. Typiquement, nous avons développé une solution de Cyber Range (Plateforme pour les simulations et l'entraînement) qui s'appelle Mantis, grâce à l'acquisition de Amossys, qui nous permet d'effectuer des exercices de crise augmentée, et en fait, et avec la technique du jumeau numérique. Il existe de nombreux cas d'usage. Il est ainsi possible d'entraîner des SOC (Security Operations Centers ou Centre des Opérations de Sécurité), cela permet de faire des exercices de crise augmentée, du « Breach And Attack simulation (BAS) » ou de tester ses défenses face aux cyberattaques. Tout cela est intégré dans nos services. Un autre exemple qui est selon moi une réussite entrepreneuriale, c'est que nous avons développé une solution d'analyse de vulnérabilités, en recourant au procédé d'une spin-off (ou scission) qui permet de transformer une division de la société en une société indépendante devenue la solution Board of Cyber.

Almond est lauréate du Grand Défi Cyber sur plusieurs projets France 2030. Et cela nous anime. Cela veut dire par exemple, qu'au quotidien, dans nos services, nous intégrons l'IA (Intelligence Artificielle) depuis plusieurs années. Cela nous permet aussi d'amener une vue assez unique, de conseil et benchmark à nos clients. Un quatrième point de différenciation, en lien avec ce que je disais sur l'explication de mon parcours et qui a aussi

contribué à cette ambition chez Almond, il me semble, c'est qu'au-delà de servir nos clients de la meilleure des façons, il est aussi utile et important de contribuer à animer l'écosystème de la Cyber.

Concrètement, cela veut dire qu'au quotidien, il est nécessaire d'être dynamique dans toutes les initiatives des réseaux qui existent, et ils sont nombreux, en participant par exemple, au Cercle d'excellence cyber, au sein de Numeum, au CESIN, à l'ACN (l'Alliance pour la Confiance Numérique) et d'autres, au Campus Cyber évidemment. Et plus largement, la volonté est d'œuvrer pour contribuer à ce que les solutions de la Tech européenne puissent trouver leur point d'équilibre plus vite en trouvant des clients. Je pense que les sociétés de services ont un rôle clé à jouer et Almond est engagée à cela.

>>>

>>> ■■ **GS MAG** : *Nos lecteurs, lectrices, c'est aussi l'écosystème des RSSI, des CISO, des DPO, DSI, Responsables Cyber, Responsables Cybersécurité. Quels seraient vos messages clés pour notre lectorat ?*

■■ **NLS** : Je trouve que le métier de RSSI ou CISO est complexe et pas facile.

Il y a des enjeux importants, et des injonctions paradoxales. On leur demande de savoir faire de nombreuses choses. Alors, le message clé, est de leur dire que le positionnement d'Almond_Amossys est d'être leur partenaire, d'essayer en miroir, de leur amener ce qui peut les aider à mieux vivre leur quotidien. Selon moi, les RSSI ou CISO ont besoin d'expertise, d'agilité, de proximité et d'excellence. Et j'espère que les équipes d'Almond arrivent à leur apporter cela, et dans tous les cas, c'est ce que nos clients nous disent quand ils nous choisissent.

■■ **GS MAG** : *Les aider à mieux vivre leur quotidien, vous avez dit ?*

■■ **NLS** : Les aider à vivre mieux leur quotidien et à gérer les injonctions paradoxales auxquelles ils et elles sont confronté.e.s.

Faire du réglementaire et de la technique, parler à un Board et à des équipes techniques, parler au business tout en étant contraints par des budgets. Donc beaucoup de sujets sur lesquels, le ou la RSSI / CISO, devrait être un Superman ou une Superwoman. Pour réussir à faire ses super missions, il ou elle a besoin d'être super entouré.e et donc, en s'adressant à des expert.e.s qui peuvent accompagner ces enjeux-là, qui ne sont pas les mêmes aujourd'hui et demain, en plus. Il est en plus nécessaire de s'adapter tout le temps.

■■ **GS MAG** : *Et comment chez Almond, vous les aidez par rapport à NIS 2, DORA, CRA, RGPD, ISO 27001... La conformité et la Cybersécurité ?*

■■ **NLS** : Nous les aidons concrètement en proposant des prestations de service pour accompagner nos clients à comprendre en quoi ils sont soumis à ces exigences et comment ils peuvent, ils doivent les décliner dans leurs organisations, dans leurs solutions techniques, dans toutes les dimensions. Donc ça, c'est un axe, j'ai envie de dire évident. Et un deuxième axe sur lequel j'espère que nous les aidons, c'est dans notre contribution active dans l'écosystème Cybersécurité. Almond fait aussi partie des acteurs consultés par les autorités sur les lois de transposition des Directives européennes, ou sur l'application de ces cadres réglementaires.

Et notre préoccupation, c'est de faire en sorte que l'application soit « opérationnalisable » et ne crée pas « d'usine à gaz » pour les Entreprises et Organisations. Et, in fine, d'éviter que cela ne devienne des freins à leur compétitivité, mais plutôt des accélérateurs de compétitivité. Je me permets de rappeler que cybersécuriser, cela veut dire favoriser le fait qu'on puisse numériser plus. Et numériser plus, digitaliser plus, ça veut dire prendre des avantages compétitifs ou en tout cas ne pas en perdre. C'est donc un enjeu hyper important pour l'autonomie stratégique européenne que nos Entreprises et Organisations soient hyper bien digitalisées ou numérisées, et ainsi hyper bien cybersécurisées.

Nos actions comportent ce qu'on appelle un effet « kiss cool », c'est-à-dire qu'avec notre expertise, nous essayons d'amener un regard objectif et pragmatique aussi aux Autorités afin que la façon dont les choses sont traduites dans les textes, soit concrètement « opérationnalisable » par les Entreprises et les Organisations. ■

Je me permets de rappeler que cybersécuriser, cela veut dire favoriser le fait qu'on puisse numériser plus. Et numériser plus, digitaliser plus, ça veut dire prendre des avantages compétitifs ou en tout cas ne pas en perdre.



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



A portrait of Kilian Chiarelli, a man with a beard and short dark hair, wearing a white button-down shirt. He is looking off to the side with a thoughtful expression, his hands clasped in front of him. The background is dark and out of focus.

KILIAN
CHIARELLI

*Ingénieur en Cybersécurité,
Crédit Agricole Personal
Finance & Mobility*

LA SÉCURITÉ OFFENSIVE AU CRÉDIT AGRICOLE PERSONAL FINANCE & MOBILITY : UNE APPROCHE PROACTIVE POUR RENFORCER LA RÉSILIENCE

Face à la multiplication et à la sophistication croissante des cyberattaques, les entreprises doivent aujourd'hui dépasser la simple posture défensive pour adopter une stratégie proactive.

C'est dans cette optique que le Crédit Agricole Personal Finance & Mobility (CA-PFM) a structuré une équipe dédiée à la sécurité offensive, chargée d'améliorer en continu la sécurité des systèmes du groupe.

L'objectif principal de cette démarche est simple : penser comme un attaquant pour mieux se défendre. En reproduisant les conditions réelles d'une attaque, les experts identifient les failles avant qu'elles ne puissent être exploitées, tout en renforçant la culture de sécurité au sein des équipes.

La sécurité offensive s'articule autour de trois missions complémentaires : la recette sécurité, la Red Team et le Bug Bounty. Chacune répond à un objectif précis mais concourt à un même but : renforcer la sécurité du système d'information du Groupe.

LA RECETTE SÉCURITÉ : GARANTIR LA CONFORMITÉ DES BONNES PRATIQUES

Première brique de la sécurité offensive, la recette sécurité intervient en amont des mises en production.

Face à la multiplication et à la sophistication croissante des cyberattaques, les entreprises doivent aujourd'hui dépasser la simple posture défensive pour adopter une stratégie proactive.

Elle consiste à vérifier l'application des bonnes pratiques de sécurité dans les projets applicatifs et les infrastructures. L'équipe s'assure que les configurations sont conformes aux politiques internes, que les dépendances logicielles sont maîtrisées et qu'aucune faille connue ne subsiste avant la mise en ligne.

Si le niveau de sécurité d'une application est jugé insuffisant, un exercice de Red Team interne peut être déclenché pour confronter les défenses dans des conditions réelles, tout en gardant un cadre maîtrisé.

Au-delà des aspects techniques, la recette sécurité est un levier de sensibilisation. Elle aide les équipes projet à adopter les bons réflexes et à renforcer la culture 'security by design'. Elle favorise une détection précoce des vulnérabilités, limitant les risques et les coûts de correction.

LA RED TEAM : TESTER LA RÉSILIENCE DU SYSTÈME D'INFORMATION

La deuxième mission, la Red Team, vise à simuler des attaques internes et externes réalistes pour évaluer la capacité de détection, de réaction et de remédiation des défenses en place. Ces tests d'intrusion complètent les audits externes en reproduisant des scénarios de compromission globale et des chaînes d'attaque complètes.

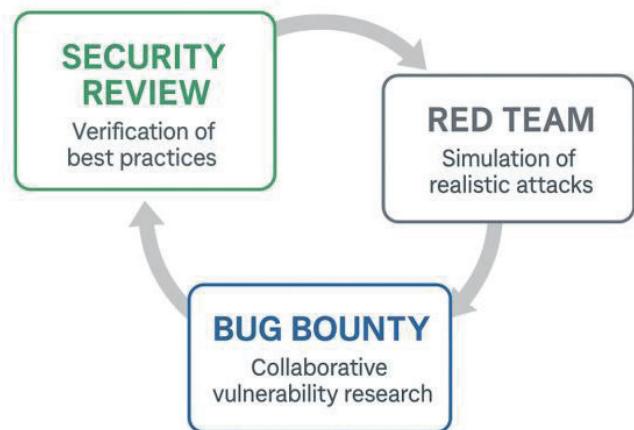
En agissant comme un adversaire déterminé, l'équipe identifie les faiblesses techniques et organisationnelles et améliore les processus de réponse à incident. Cette démarche, menée avec les équipes SOC et Blue Team, renforce la synergie entre les volets offensif et défensif de la cybersécurité.

LE BUG BOUNTY : LA FORCE DU COLLECTIF AU SERVICE DE LA SÉCURITÉ

Enfin, la troisième mission repose sur un modèle collaboratif : le Bug Bounty. Le Crédit Agricole Personal Finance & Mobility s'appuie sur la plateforme mondialement connue pour mobiliser une communauté de hackers éthiques certifiés. Ces chercheurs testent nos applications et infrastructures pour détecter les vulnérabilités parfois difficiles à identifier en interne.

Ce programme offre une expertise externe complémentaire et valorise la transparence et la collaboration dans la démarche de cybersécurité du groupe.

Security Offensive Lifecycle



VERS UNE CYBERSÉCURITÉ TOUJOURS PLUS PROACTIVE

Grâce à ces trois leviers — recette sécurité, Red Team et Bug Bounty —, le Crédit Agricole Personal Finance & Mobility adopte une approche globale et proactive de la sécurité offensive. L'enjeu est d'assurer une protection durable des données et des systèmes tout en renforçant la confiance des utilisateurs.

Les résultats se traduisent par une amélioration continue du niveau de sécurité et une meilleure coordination entre les entités techniques et métiers. Dans un contexte de menaces en constante évolution, cette stratégie proactive permet d'anticiper et de neutraliser les risques avant qu'ils n'affectent les utilisateurs.

En plaçant l'humain et l'anticipation au cœur de sa stratégie, l'entreprise confirme que la sécurité offensive est un levier essentiel pour renforcer sa posture de 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

16^e édition

GSDays

LES JOURNÉES FRANCOPHONES DE LA SÉCURITÉ

DE L'INFORMATION ET DE LA CYBER

20/01/26
Espace Saint-Martin - paris 3^e



Le Rubik's Cube de la Cybersécurité :
RSSI / CISO / DPO / DSI-CIO / COMEX / SOC / CERT / CSIRT...

INSCRIPTION SUR WWW.GSDAYS.FR





FRANÇOIS
BIDONDO

LORS DE LA 25^E ÉDITION DES ASSISES DE LA CYBERSÉCURITÉ,

François BIDONDO, Group CISO, Directeur Cybersécurité RATP Group, et Administrateur du CESIN, a accordé un entretien à Global Security Mag

■ ■ **GS MAG :** *François BIDONDO, bonjour, Global Security Mag est ravi d'avoir cet entretien avec vous. Pouvez-vous vous présenter et nous dire comment votre parcours professionnel vous a amené à vos rôles actuels à la RATP et puis au CESIN ?*

■ ■ **FB :** Merci pour votre question et pour l'opportunité de m'exprimer. J'ai un parcours finalement assez traditionnel puisque j'ai un diplôme d'Ingénieur en télécom à l'origine, donc plutôt une appétence pour la technologie, la technique.

Et finalement, la Cybersécurité n'était pas un sujet à l'époque où j'ai été diplômé en 2003. Et c'est un peu le hasard qui m'a amené vers cette direction, le hasard d'un stage de fin d'études autour de la sécurité des réseaux,

ça s'appelait comme ça à l'époque. Ce n'était pas un vrai métier, un métier à part entière. Et j'ai mis le pied dans cet écosystème à une époque où les enjeux commençaient à apparaître autour de la technologie et des aspects extrêmement pointus de sécurisation de nos systèmes. Et petit à petit, j'ai évolué dans cet écosystème en même temps que le sujet, puisque la Cybersécurité est devenue un enjeu d'entreprise à la fois technologique, mais aussi très intégrée avec les autres métiers des entreprises, le business, le juridique, les ressources humaines.

Et finalement, j'ai pu m'épanouir, apprendre et continuer à apprendre dans ces métiers en occupant différents rôles, très techniques au départ. Et petit à petit, avec le passage dans la banque chez BNP Paribas, dans l'industrie chez Alstom et aujourd'hui en tant que Chief Information Security Officer du groupe RATP, de pouvoir prendre en main des enjeux Cybersécurité de plus en plus importants et structurants dans les entreprises, en gardant ce lien avec

Venez nous apporter vos expériences, vous bénéficierez aussi de celles de tous les membres du CESIN, et c'est ainsi que nous serons plus forts et plus fortes face aux cybermenaces.

la technique qui est quand-même un socle important dans mon parcours, mais en m'ouvrant à d'autres enjeux pour les entreprises et en rencontrant d'autres métiers. Et un des fils conducteurs dans mon parcours, c'était la solidarité, la contribution et l'appui sur la communauté de la Cybersécurité que représente le CESIN. Je suis donc un adhérent de la première heure, de l'association et j'ai jugé cette année qu'il était temps de proposer ma candidature au Conseil d'Administration. J'ai eu la chance d'être élu et ça me permet aussi de redonner à cette communauté, ce qu'elle m'a apporté, de contribuer à son développement alors que de grands enjeux sont devant nous sur le sujet.

■ ■ GS MAG : *Vous avez abordé la deuxième question qui consiste à dire ce que vous apporte le fait d'être au CESIN. Et vous, qu'apportez-vous au CESIN ? Car j'ai cru comprendre qu'en tant que membre du CESIN, il est nécessaire de donner et de recevoir.*

■ ■ FB : Exactement, c'est un enjeu important au CESIN. On est là pour donner, recevoir, contribuer. Mais finalement, ce que m'apporte le CESIN, c'est d'abord de partager avec la communauté nos enjeux, de ne pas se sentir seul. Parce que parfois, c'est vrai que face à l'adversité, face aux cyberattaquants, face aux réglementations, face aux contraintes budgétaires, technologiques, on peut se sentir face à une montagne. C'est important de savoir qu'on n'est pas seul, de savoir que ces enjeux, ces objectifs et ces contraintes sont partagés et donc de voir comment d'autres peuvent les adresser, de pouvoir éventuellement les adresser à plusieurs, on est plus fort à plusieurs. Et c'est donc d'abord d'avoir, ce lieu d'échange pour partager, apprendre et finalement se rendre compte qu'on est face à des mêmes enjeux, des mêmes problématiques et de trouver les meilleures solutions.

Le CESIN, c'est un endroit où on retrouve des expertises de haut niveau et où on a la chance d'avoir des communautés spécialisées, des échanges avec l'écosystème, avec les startups, avec des acteurs de l'industrie et des éditeurs et des fournisseurs de services qui nous permettent aussi de bénéficier de cette veille, de ces échanges et de rester finalement informés par ce panel. La veille est importante dans notre métier et le CESIN est aussi un endroit où on peut travailler cette veille et obtenir ces informations. Et enfin, ça permet finalement de se remettre en question aussi, je dirais, c'est quelque chose d'important quand on voit arriver une nouvelle génération, de nouvelles problématiques, de nouveaux secteurs d'activité qui s'intéressent à la Cybersécurité, soit à cause de la réglementation, soit à cause simplement des enjeux de leurs métiers qui intègrent la numérisation. Cela nous permet aussi de nous questionner. Voilà ce que j'essaie d'apporter.

C'est au travers de mon parcours qui a mixé des postes d'expertise, des postes d'encadrement, de direction dans différents secteurs d'activité, c'est de pouvoir finalement adresser les sujets sous différents prismes. Le prisme d'entreprises très matures comme les banques où la réglementation est en place depuis longtemps, des prismes où les enjeux, comme dans l'industrie, sont plus récents, avec des systèmes souvent plus obsolètes, donc des enjeux vraiment différents.

Le Service Public aujourd'hui qui a toute mon attention sur la Cybersécurité de nos offres. Et donc en ayant cette expérience, j'essaie de l'apporter et d'en faire bénéficier toute la communauté, des plus récents membres aux plus anciens, parce que finalement, c'est tout l'intérêt. Aussi, mettre à profit ce que j'ai pu vivre, comme difficultés, comme enjeux, de fusions-acquisitions, d'événements spécifiques comme les Jeux olympiques et Paralympiques, c'est un dernier élément en date qui a bien mobilisé toute la communauté. Je partage volontiers ces expériences avec les membres du CESIN.

>>>

>>> ■■ **GS MAG** : *Alors justement, quel serait votre conseil aux CISO, RSSI face à cette future loi de transposition, NIS 2, CRA, DORA ? Que pouvez-vous dire en deux mots ?*

■■ **FB** : En deux mots : un, Confiance et deux, Opportunité. Effectivement, cette réglementation arrive et touche beaucoup de secteurs qui n'étaient pas précédemment sous le coup de la réglementation. Mais moi, j'y vois déjà un grand bénéfice, c'est-à-dire, faire monter tout l'écosystème en maturité. Les exigences portées par cette réglementation ne sont pas nouvelles.

Finalement, c'est beaucoup de bonnes pratiques, d'hygiène cybersécurité qui étaient déjà dans beaucoup de feuilles de route, dans beaucoup de stratégies cybersécurité dans les organisations. Là, c'est appuyé par la réglementation, donc c'est un levier supplémentaire et je trouve que c'est utile dans des moments où on doit aller négocier des moyens, de pouvoir compter sur ce levier de la réglementation. Je suggère donc de prendre cela comme une opportunité pour, encore une fois, valoriser notre métier, notre activité et ainsi pouvoir accélérer. C'est un élément supplémentaire pour convaincre et faire bouger les lignes. C'est quelque chose de positive.

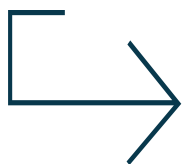
Le deuxième conseil serait de ne pas hésiter à en parler au CESIN. Et donc pour ceux qui ne sont pas encore membres, de nous rejoindre pour partager sur les implémentations, les différences sectorielles, éventuellement les différences d'implémentation entre les pays, puisqu'au niveau européen, les transpositions peuvent être différentes. Beaucoup de nos membres sont confrontés à cette multiplicité de transpositions, et se posent les mêmes questions d'implémentation et de la réglementation. Nous avons au sein du CESIN, selon moi, toutes les réponses à apporter pour aider nos collègues et nos confrères à mettre en place cette, cette réglementation du mieux possible.

■■ **GS MAG** : *Vous faites une belle transition sur notre dernière question qui est : en résumé, quel serait votre message clé pour motiver les RSSI, CISO à rejoindre le CESIN ?*

■■ **FB** : Il s'agit de rejoindre la communauté de personnes et des collaborateurs qui partagent les mêmes questions, intérêts, passions pour certains autour de la cybersécurité, de ces enjeux depuis des années. Le CESIN est un lieu d'échange formidable avec une source d'inspiration. Enfin, je rencontre des gens qui ont vécu des expériences, des projets incroyables. C'est à la fois une source d'inspiration et de remise en question permanente. Et je ne peux qu'encourager les gens à vivre ce que j'ai vécu, c'est-à-dire à intégrer ce club et pendant des années, progresser, apprendre et contribuer, puisque nous amenons aussi à cette communauté nos propres expériences. Alors, venez nous apporter vos expériences, vous bénéficierez aussi de celles de tous les membres du CESIN, et c'est ainsi que nous serons plus forts et plus fortes face aux cybermenaces. ■



Le CESIN, c'est un endroit où on retrouve des expertises de haut niveau et où on a la chance d'avoir des communautés spécialisées, des échanges avec l'écosystème, avec les startups, avec des acteurs de l'industrie et des éditeurs et des fournisseurs de services qui nous permettent aussi de bénéficier de cette veille, de ces échanges et de rester finalement informés par ce panel.



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



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

A portrait of Alain Bouillé, a middle-aged man with glasses, wearing a dark suit jacket over a light-colored shirt. He is smiling slightly. The background is a blurred green outdoor setting. To the right of the portrait, there is a decorative graphic of a cluster of small, overlapping squares in shades of gold and brown.

ALAIN
BOUILLÉ

*Délégué Général et
Porte-parole du CESIN*

LORS DE LA 25^E ÉDITION DES ASSISES DE LA CYBERSÉCURITÉ À MONACO, Alain Bouillé, Délégué Général et Porte-parole du CESIN a accordé un entretien à Global Security Mag.

■ ■ **GS MAG :** *Bonjour Alain Bouillé, Global Security Mag est ravi d'avoir cet entretien avec vous. Nous sommes dans le cadre des Assises de la cybersécurité, de la vingt-cinquième édition. Quelle est l'actualité du CESIN ?*

■ ■ **AB :** L'actualité du CESIN est comme l'actualité de la Cyber, elle est très riche. Il y a évidemment les sujets toujours prégnants de criminalité. Nous avons jusqu'ici, passé une année 2025 avec des attaques assez cinglantes, qui ont frappé des secteurs d'activité qui n'étaient pas habitués à cela. Je pense aux secteurs du Retail et du Luxe qui se sont fait attaquer, paradoxalement par des méthodes anciennes, et je pense en particulier à

l'ingénierie sociale dont Salesforce a été la cible, pour mieux attraper les données de ses clients. Et là, en effet, on a vu des fuites de données importantes et avec des méthodes qui sont relativement anciennes, comme l'ingénierie sociale. Les Entreprises et les Organisations ont tellement « blindé les portes et mis des verrous, comme le MFA et d'autres technologies, que les cyberattaquants n'essayent plus d'ouvrir la porte, mais demandent à quelqu'un de l'ouvrir pour eux. Et en même temps, il ne s'agit pas d'ignorer les cyberattaques boostées à l'IA (Intelligence Artificielle), mais ce qui a fait l'actualité, c'est l'ingénierie sociale. L'autre cyberattaque qui a marqué ces derniers temps, c'est celle encore liée à Salesforce, mais plutôt sous l'angle attaque logicielle. C'est-à-dire qu'un logiciel d'IA intégré dans l'outil Salesforce s'est fait pirater, avec pour effets, des jetons de connexion récupérés, etc. Et là, cela ne nous rajeunit pas, car on en revient à 2017 avec SolarWinds, cas dans lequel il

Le message que je passerais bien aux futurs membres, c'est de dire : Ne venez pas au CESIN que pour consommer. Il est aussi nécessaire de donner, pour qu'une Association comme la nôtre fonctionne. Nous restons très vigilants à cela, et il nous arrive régulièrement de refuser des dossiers de candidature en cas de doute sur ce point.

ne s'agissait plus d'attaquer les Entreprises et les Organisation directement, mais plutôt les outils qu'elles utilisent. Et comme presque tout le monde utilisait les mêmes logiciels, il a été plus facile, effectivement, de réaliser des cyberattaques de grande ampleur. C'est le sujet de la fameuse attaque par supply chain (chaîne d'approvisionnement). Le CESIN a sorti à l'occasion des Assises de la cybersécurité, un communiqué de presse sur le risque cyber lié aux fournisseurs. En effet, on peut prendre l'exemple des interactions entre les fournisseurs et un Service Marketing qui va envoyer à un sous-traitant son fichier client pas très bien protégé, pour organiser une opération de marketing, et les données clients se font pirater. En résumé, maintenant, deux tiers des cyberattaques ne se font pas frontalement sur l'Entreprise ou l'Organisation visée, mais via un fournisseur.

Dans ce communiqué de presse, le CESIN préconise un certain nombre de démarches pour sécuriser les fournisseurs, comme des questionnaires, des assessments ou évaluations. Nous avons réalisé plusieurs études sur ce sujet, avec Board of Cyber, qui apporte beaucoup de réponses à ces questions de la sécurité des fournisseurs. Mais il reste évidemment prégnant que le fait qu'il y ait autant de fournisseurs, devrait amener les dirigeants à se poser la question de savoir si tout externaliser comme ça, un peu n'importe comment, est bon pour la sécurité des données. Je suis convaincu que non. On ne peut pas assurer la sécurité de milliers de fournisseurs et avoir un œil sur les données en permanence. Donc cette question des cyberattaques qui ciblent les entités au travers des fournisseurs ou au travers des logiciels qu'ils utilisent, comme l'exemple de Salesforce, va être probablement la tendance. Cela a tellement bien marché avec Salesforce, qu'il n'y a pas de raison que les cyberattaquants s'arrêtent là. En résumé, notre actualité est d'abord centrée autour des cyberattaques via les fournisseurs.

Ensuite, vient l'actualité géopolitique. Oui, C'est un des thèmes des Assises de la Cybersécurité en 2025, et cela sera le thème du Congrès du CESIN. Il est certain que l'élection de Donald Trump a secoué un peu tout le monde. Mais enfin, on sait très bien que l'Amérique a toujours été dans une position de conquête et voir d'hégémonie.

Les outrances de Trump ont un peu réveillé les consciences. Et pour les chantres de la Souveraineté, dont je fais partie, c'est plutôt une bonne nouvelle. C'est également une bonne nouvelle pour le marché européen, je pense. Il y a une dynamique qui se met en place, il faut la saisir.

Si on analyse les partenariats du CESIN, on constate qu'il y a une vingtaine de sponsors, dont une dizaine d'éditeurs et une dizaine d'intégrateurs. Les intégrateurs sont pratiquement tous français, en revanche chez les éditeurs, nous avons cinquante pour cent d'entre eux hors Europe et cinquante pour cent Européens. On ne peut pas se passer des technologies américaines, c'est clair, ni des israéliennes. Mais comme il se trouve que ces deux pays sont quand-même en ce moment un peu secoués, l'un par la politique, l'autre par la guerre, cela fait réfléchir sur la capacité de ces pays à continuer à fournir des services de qualité de manière pérenne.

Le scénario de Trump qui coupe les vivres du Danemark en matière numérique, si le Danemark ne cède pas le Groenland aux États-Unis, est tout à fait réel. Si on revient à la Cyber, ma position, c'est de dire : on a un gros défaut dans la Cyber, c'est qu'on a beaucoup, et parfois beaucoup trop, de solutions embarquées pour protéger notre patrimoine. On nous l'a souvent reproché, on nous le reproche encore. Évidemment, les membres du CESIN essaient d'architecturer et de rationaliser tout cela. Cependant, en moyenne, dans les grandes Entreprises, ce sont plus de cinquante solutions qui sont installées et en moyenne nationale dans notre baromètre, plus de quinze

>>>

solutions. Cela veut dire, en effet, que nous sommes très fragmentés dans nos solutions, mais en même temps, cela implique que nous sommes très agiles. Et l'agilité, cela n'a pas de prix, parce que ça veut dire que demain, si on nous dit, pour une raison X ou Y, qu'il ne faut plus travailler avec les logiciels de tel ou tel pays, comme on nous l'a dit au moment de la guerre avec les Russes et l'Ukraine, pour s'agissant des logiciels russes dans nos infrastructures, nous savons faire. Changer un EDR (Endpoint Detection and Response ou service de détection et de réponse pour les terminaux), changer un antivirus, changer n'importe laquelle brique d'une solution cyber, c'est possible. Je ne dis pas que cela se fait sans douleur, mais c'est un projet avec un début, une fin, et un petit peu de moyens et on n'en parle plus. Vous demandez au DSI (Directeur ou Directrice des Systèmes d'Information) de changer de digital workplace ? Oui, c'est aussi un projet, mais il risque de durer dix ans.

Tout cela, pour dire que ces questions de Souveraineté, cela m'agace un peu que l'on nous donne des leçons sur le fait de savoir ce qu'est la Souveraineté, l'Autonomie stratégique, ou la Confiance numérique. La grande question, devrait être la liberté de choix et la garantie que « quand on va tourner le robinet, il y aura toujours de l'eau qui coulera ». Voilà pour « le coup de gueule ».



**le CESIN préconise
un certain nombre de
démarches pour sécuriser
les fournisseurs, comme
des questionnaires,
des assessments ou
évaluations.**



■ ■ **GS MAG :** *Cela nous amène au fait que dans la loi de transposition qui est en cours (Résilience des Infrastructures critiques et le Renforcement de la Cybersécurité, NIS 2, CRA, DORA), il y a justement des volets sur la sécurisation par rapport aux fournisseurs, par rapport à la Supply chain. Comment le CESIN a-t-il accompagné à ce jour, cette transposition qui n'est encore pas aboutie, par rapport aux institutions (l'ANSSI, le Sénat, l'Assemblée Nationale) ?*

■ ■ **AB :** Nous avons été auditionnés à plusieurs reprises, très en amont. Nous avons coopéré énormément avec l'ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information) dans les toutes premières rédactions du texte, avant même qu'il ne soit soumis au Parlement. Cela a été un gros travail qui a d'ailleurs été salué par l'ANSSI. Nous avons ensuite suivi toutes les étapes. Nous avons été auditionnés également par les Commissions du SENAT et de l'Assemblée Nationale.

Les différentes étapes sont bien sûr un peu mises à mal par l'instabilité gouvernementale, mais cela n'empêche pas le Parlement de continuer à travailler. Les Entreprises et Organisations ont très largement amorcé les travaux sans attendre que le texte soit effectivement voté. Donc, notre message à nos membres, c'est : ça ne sert à rien d'attendre. Ça ne sert à rien de repousser le tas de cailloux, parce qu'il sera plus gros et encore plus difficile à repousser dans six mois. Il faut se retrousser les manches et y aller.

Le CRA (Cybersecurity Resilience Act), je le mets un petit peu à part. Nous y avons contribué avec des propositions d'amendements au niveau européen. Ces propositions concernaient plutôt les logiciels SaaS qui n'y étaient pas très bien traités. Nous avons vu avec plaisir que nos propositions avaient été intégrées. Peut-être que d'autres ont eu la même idée en même temps. Le CESIN ne revendique pas la paternité de ces amendements, mais nous sommes contents car ce qu'on voulait y voir, y est maintenant. Je suis un petit peu choqué de la réaction des Entreprises qui fabriquent des logiciels, et qui disent : « Ah là là, vous nous mettez encore des bâtons dans les roues. » Je réponds, non, c'est la première fois que nous vous mettons des bâtons dans les roues. Il n'y a aucune réglementation sérieuse à ce jour, qui impose aux fabricants de logiciels d'intégrer la sécurité dans le développement. Alors évidemment, il y en a beaucoup qui le font. Tous les grands éditeurs intègrent de la sécurité dans leurs logiciels. Cependant, quand on voit la part de

vulnérabilités, qui augmente de manière exponentielle et que les RSSI ont du mal à traiter, on ne peut que se réjouir du renforcement de la réglementation en la matière. Nous sommes obligés maintenant d'avoir des outils pour faire le tri... Enfin, comme je le dis souvent, on a industrialisé la médiocrité. C'est-à-dire qu'effectivement, comme il n'y a aucune contrainte dans la sécurité des logiciels, on constate un paquet de vulnérabilités. Quand vous allez dans une collectivité locale ou un hôpital, qui ont acheté leur dernier logiciel pour différentes applications, telles que la Comptabilité ou les Ressources Humaines, et que vous faites le moindre audit de code, il apparaît que c'est un vrai gruyère en matière de sécurité. Il serait peut-être temps de « remettre l'église au milieu du village ». En conséquence, au CESIN, nous applaudissons des deux mains, évidemment, cette réglementation. Et encore une fois, je suis un peu choqué que cela surprenne les fabricants de logiciels, qu'on leur demande enfin d'être un peu sérieux sur la Cyber.

■ ■ **GS MAG** : *Quel est le message clé pour les lecteurs et lectrices de Global Security Mag, RSSI, CISO, pour les motiver à rejoindre le CESIN ?*

■ ■ **AB** : Le CESIN est une association qui réunit un écosystème de RSSI et CISO, et à ce jour, nous sommes mille deux cents. Il n'y a pas de numéros clausus à ce chiffre puisque des RSSI ou CISO sont nommés presque tous les jours, et on s'en félicite. Entre le mois de juin et le

mois de septembre, plus de cinquante RSSI ont rejoint le CESIN. Ce que procure cette Association, c'est la véritable entraide dans une profession qui reste quand-même en sous-effectif. Nous partageons aussi mutuellement les expériences et les avancées .

Nous fournissons à nos membres un service de veille, évidemment sans faire de la concurrence aux Entreprises qui commercialisent ce genre de service. Nous mettons en commun des veilles très professionnelles, afin de notamment les mettre à la disposition des plus modestes qui ne peuvent pas se payer ce type de veilles.

Il peut s'agir de veilles sur les vulnérabilités, sur les technologies, ou encore d'autres types de veilles. Le mot d'ordre au CESIN, c'est le partage pour l'entraide. Alors, plus nous serons nombreux, plus nous pourrions en effet partager. Le message que je passerais bien aux futurs membres, c'est de dire : Ne venez pas au CESIN que pour consommer. Il est aussi nécessaire de donner, pour qu'une Association comme la nôtre fonctionne. Nous restons très vigilants à cela, et il nous arrive régulièrement de refuser des dossiers de candidature en cas de doute sur ce point. Il arrive en effet que des gens souhaitent venir « en mode coucou » dans le lit du CESIN, en attendant que les œufs tombent... Pour que le CESIN fonctionne, il faut des apports de toutes parts. Pour aider à cela, nous avons créé un service de mentorat, pour aider et guider les débutants par des membres aguerris. ■

Nous avons coopéré énormément avec l'ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information) dans les toutes premières rédactions du texte, avant même qu'il ne soit soumis au Parlement.



ALBAN
BENNACER

*Avocat au Barreau de Paris,
Mandataire sportif, Membre de l'International
Sports Lawyer Association*

CYBERSÉCURITÉ ET BOXE : UN MÊME ART DE LA DISCIPLINE

Sur le ring comme dans le cyberspace, la victoire ne revient pas toujours au plus puissant, mais souvent au mieux préparé.

LA BOXE, SPORT D'ANTICIPATION ET DE
STRATÉGIE, OFFRE UNE MÉTAPHORE
ÉCLAIRANTE POUR COMPRENDRE LA
CYBERSÉCURITÉ MODERNE :

il ne suffit pas de frapper fort, de manière
approximative ; il faut aussi savoir
anticiper, se protéger, observer l'adversaire,
faire preuve de rapidité, de précision et
d'efficacité tout en respectant les règles.

Dans les deux cas, la conformité joue un
rôle central : elle définit le cadre du combat.

LA CONFORMITÉ : LE CADRE RÉGLEMENTAIRE DU RING

En boxe, les règles ont pour objet de garantir non seulement un combat équitable mais aussi l'intégrité et la sécurité des pratiquants. En cybersécurité, la conformité joue un rôle analogue : RGPD, NIS2, DORA, ISO 27001... ces « règles du jeu » posent un cadre protecteur des entreprises et de leurs clients.

Mais comme tout boxeur le sait, connaître les règles ne suffit pas. Encore faut-il les allier à la technique et à la préparation, physique et mentale en boxe, opérationnelle en entreprise.

Trop d'entreprises abordent la conformité comme une formalité, un contrôle avant le combat, un peu comme la pesée ou la visite médicale. Or, la conformité n'est pas une fin en soi : c'est une condition, qui réduit l'imprévu et protège durablement.

CYBERSÉCURITÉ : DE LA DÉFENSE À L'ANTICIPATION

Sur le ring, la garde est essentielle : un boxeur sans défense s'expose. Pourtant, une approche uniquement défensive ne suffit pas à remporter le combat.

De même, en cybersécurité, se contenter d'appliquer les exigences réglementaires ne suffit pas à contrer des menaces en constante évolution.

Les cybercriminels n'ont pas de règles, pas d'arbitre. Ils frappent là où la garde se baisse : un mot de passe faible, un correctif oublié, un collaborateur distrait.

L'entreprise doit donc adopter une approche proactive, tester sa résilience, simuler des attaques, entraîner ses équipes — tout comme un boxeur s'entraîne pour se préparer à l'adversité.

Surtout, à l'instar du boxeur, l'entreprise doit anticiper. Un pugiliste agile ne réagit pas seulement à l'attaque immédiate : il anticipe le coup suivant, ajuste sa défense, prépare le coup d'après. De la même manière, une organisation performante prévoit les scénarios d'attaque probables, adapte ses dispositifs et renforce ses défenses avant même d'être visée.

LE DÉFI : CONCILIER RIGUEUR ET AGILITÉ

Associer conformité et cybersécurité, c'est concilier deux logiques parfois opposées :

- la conformité impose la méthode, la documentation, la traçabilité — une rigueur quasi administrative ;
- la cybersécurité opérationnelle, elle, exige de la réactivité, de l'adaptation, du mouvement permanent.

Car tout comme un boxeur statique devient une cible facile, une entreprise figée dans ses processus est vulnérable. Le danger est alors de transformer la conformité en carcan.

Trop de procédures peuvent ralentir la détection ou la réponse aux incidents. À l'inverse, négliger la conformité, c'est tenter de se défendre sans maîtriser la technique. De la même manière qu'un boxeur qui ne sait pas parer ou esquiver peut recevoir un coup fatal, une entreprise qui néglige la préparation de sa cybersécurité s'expose à des sanctions et à la perte de confiance voire à une réputation entachée après une attaque mal parée.

Le véritable défi est donc d'intégrer la conformité dans le geste technique, de la rendre fluide, naturelle, comme un boxeur, par liaisons, intègre la défense dans chacun de ses mouvements, la préparation dans ses déplacements et l'anticipation dans sa prise d'information.

ENTRAÎNER LA CULTURE D'ENTREPRISE : LE SPARRING DU NUMÉRIQUE

La boxe ne s'apprend pas seul, la cybersécurité non plus. La sensibilisation, les audits, les exercices de crise jouent le rôle du sparring : ils révèlent les réflexes, les failles, les progrès.

Or, la conformité impose de prouver ces efforts : journaux d'événements, plans de continuité, rapports d'incidents. L'enjeu est de transformer ces obligations en outils d'amélioration continue.

Tout comme un boxeur apprend de ses séances de mise de gants et analyse ses propres combats pour mieux progresser, une entreprise mature ne se contente pas de cocher des cases : elle apprend à chaque round, affine sa posture, renforce sa défense.

L'ARBITRE INTÉRIEUR : L'ÉTHIQUE COMME LIGNE DIRECTRICE

Enfin, il existe un parallèle plus subtil : l'éthique. En boxe, tricher, c'est perdre l'honneur ; en cybersécurité, exposer des données et ignorer la conformité, c'est perdre la confiance.

La conformité ne doit donc pas être vue uniquement comme une contrainte extérieure, mais aussi comme l'expression d'une éthique interne. Elle définit la manière dont l'entreprise se comporte sur le ring numérique : respectueuse, disciplinée, responsable. ■

CONCLUSION : GAGNER, SI POSSIBLE AVANT LA LIMITE

La boxe enseigne la patience, la stratégie et le respect. Le maître mot du noble art est de « toucher sans être touché ».

La cybersécurité exige les mêmes vertus.

Associer conformité et cybersécurité, c'est apprendre à combattre dans un cadre exigeant, sans perdre en efficacité. C'est faire de la cybersécurité l'art de combattre sans encaisser de KO. Et lorsque ces deux dimensions s'équilibrent, l'entreprise est prête à affronter l'adversité numérique, sans crainte de l'inconnu.



ÉLODIE LE SAOUT

*Fondatrice, CEO,
Moïra Cybersecurity*

RETEX NIS2 AU NIVEAU EUROPEEN : LES PREMIERS ENSEIGNEMENTS DE LA MISE EN CONFORMITÉ

**APRÈS PLUSIEURS MOIS
D'APPLICATION DE LA DIRECTIVE NIS2,
LES PREMIERS RETOURS D'EXPÉ-
RIENCE RÉVÈLENT UNE TRANSFORMA-
TION PROFONDE DES APPROCHES DE
GOUVERNANCE DES RISQUES CYBER.
AU-DELÀ DE LA SIMPLE CONFORMITÉ
RÉGLEMENTAIRE, CETTE DIRECTIVE
CATALYSE UNE REFORTE STRUCTU-
RELLE DES DISPOSITIFS DE CYBERSÉ-
CURITÉ ORGANISATIONNELLE.**

La transposition de NIS2 dans les législations nationales européennes marque une étape décisive dans la maturation de la gouvernance cyber. Les premières phases de mise en conformité révèlent des enjeux inattendus et des opportunités stratégiques qui dépassent largement le cadre réglementaire initial. Cette évolution transforme progressivement la perception de la conformité, d'obligation subie en levier de performance organisationnelle.

LA CARTOGRAPHIE DES ENTITÉS : UN EXERCICE PLUS COMPLEXE QUE PRÉVU

L'identification du périmètre d'application de NIS2 s'est révélée bien plus complexe que ne le suggéraient les textes

réglementaires. Les critères de qualification des entités essentielles et importantes génèrent de nombreuses zones grises, particulièrement pour les organisations multi-sectorielles ou les filiales de groupes internationaux.

L'expérience terrain démontre que cette complexité initiale constitue paradoxalement un atout pour les organisations qui l'abordent méthodiquement. L'exercice de cartographie imposé par NIS2 force une analyse exhaustive des activités, des interdépendances et des vulnérabilités qui révèle souvent des risques méconnus ou sous-évalués dans les approches traditionnelles.

Les organisations ayant investi dans une analyse approfondie de leur périmètre d'application témoignent d'une amélioration significative de leur compréhension des enjeux de cybersécurité. Cette phase préliminaire, initialement perçue comme administrative, devient un véritable audit stratégique des vulnérabilités organisationnelles.

L'ÉMERGENCE D'UNE GOUVERNANCE PROPORTIONNÉE

L'exigence de mesures "appropriées et proportionnées" inscrite dans NIS2 impose une approche nuancée de la conformité qui tranche avec les logiques binaires traditionnelles. Cette proportionnalité, loin d'être un assouplissement, exige une justification rigoureuse de chaque choix technique et organisationnel.

Cette évolution transforme profondément le dialogue avec les autorités de contrôle. L'accent se déplace progressivement de la vérification de conformité formelle vers l'évaluation de la cohérence et de l'efficacité des dispositifs mis en place. Cette

transformation valorise l'expertise métier et la capacité d'analyse des risques au détriment des approches purement procédurales. Les retours d'expérience montrent que les organisations ayant développé une argumentation solide de leurs choix de sécurité bénéficient d'une relation plus constructive avec les régulateurs. Cette dynamique encourage une approche proactive de la conformité où l'anticipation remplace progressivement la réaction.

LA TRANSFORMATION DES MÉTIERS DE LA CYBERSÉCURITÉ

NIS2 accélère la transformation des profils et compétences attendus dans le domaine de la cybersécurité. L'exigence de formation et sensibilisation des organes dirigeants modifie fondamentalement les relations entre équipes techniques et instances décisionnelles.

Cette évolution se traduit par l'émergence de nouveaux rôles hybrides combinant expertise technique et capacité de communication stratégique. Les professionnels capables de traduire les enjeux techniques en risques business et de contextualiser les obligations réglementaires dans les réalités opérationnelles voient leur valeur ajoutée reconnue et valorisée.

L'obligation de notification rapide des incidents impose également une refonte des processus décisionnels internes. Les mécanismes traditionnels de validation hiérarchique s'avèrent inadéquats aux contraintes temporelles de la directive, nécessitant une délégation accrue et une responsabilisation des équipes opérationnelles.

LES ZONES D'OMBRE PERSISTANTES

Malgré les clarifications apportées par les autorités nationales, plusieurs aspects de NIS2 demeurent sujets à interprétation, générant une incertitude juridique que les organisations doivent apprendre à gérer. Cette ambiguïté concerne particulièrement les modalités pratiques d'application de certaines exigences dans des contextes organisationnels complexes.

La gestion des chaînes d'approvisionnement illustre parfaitement cette problématique. Si l'obligation d'évaluer et superviser les fournisseurs est claire dans son principe, sa mise en œuvre pratique soulève de nombreuses questions opérationnelles. Comment évaluer efficacement des milliers de fournisseurs ? Quels critères retenir pour prioriser les contrôles ? Comment maintenir cette surveillance dans la durée ?

L'absence de standards uniformisés au niveau européen génère également des divergences d'interprétation entre États membres qui compliquent la situation des groupes multinationaux. Cette fragmentation normative impose une approche différenciée de la conformité selon les juridictions, multipliant les coûts et la complexité organisationnelle.

L'OPPORTUNITÉ D'UNE CYBERSÉCURITÉ BUSINESS-ORIENTED

Au-delà des contraintes, NIS2 offre aux organisations l'opportunité de repenser leur approche de la cybersécurité dans une logique véritablement business-oriented. L'exigence de proportionnalité force un dialogue constructif entre équipes techniques et métiers pour identifier les mesures de sécurité les plus pertinentes. Cette convergence génère progressivement une culture commune où la cybersécurité n'est plus perçue comme une contrainte externe mais comme un enabler de la performance opérationnelle. Les organisations les plus avancées témoignent d'une amélioration de leur agilité et de leur capacité d'innovation grâce à une approche plus mature de la gestion des risques cyber.

L'obligation de reporting vers les instances dirigeantes transforme également la nature des échanges sur la cybersécurité. Les discussions évoluent progressivement des aspects purement techniques vers une analyse stratégique des risques et opportunités, enrichissant la réflexion décisionnelle globale.

VERS UNE MATURITÉ COLLECTIVE

Les premiers mois d'application de NIS2 révèlent l'émergence d'une dynamique collaborative inédite entre organisations d'un même secteur. La complexité commune des enjeux de conformité favorise le partage d'expériences et le développement de bonnes pratiques sectorielles. Cette mutualisation des efforts se traduit notamment par la création de groupes de travail techniques et l'élaboration de référentiels partagés. Cette dynamique collective accélère significativement la montée en maturité des organisations et optimise l'allocation des ressources dédiées à la conformité.

L'implication croissante des associations professionnelles dans l'accompagnement à la conformité crée également un écosystème de support qui facilite l'appropriation des exigences réglementaires par les organisations de taille intermédiaire traditionnellement moins outillées.

CONCLUSION : UNE TRANSFORMATION EN COURS

Les premiers retours d'expérience de la mise en conformité NIS2 dessinent les contours d'une transformation profonde et durable des approches de cybersécurité organisationnelle. Cette évolution dépasse largement le cadre réglementaire pour catalyser une refonte culturelle et opérationnelle des dispositifs de gestion des risques cyber.

Si certaines zones d'incertitude persistent et nécessitent encore des clarifications, la dynamique globale témoigne d'une maturation accélérée de l'écosystème de cybersécurité européen. Les organisations qui sauront tirer parti de cette transformation pour renforcer leur résilience et leur compétitivité développeront un avantage stratégique durable dans un environnement numérique de plus en plus exigeant. ■

FLORENCE
GIULY-DAVIS

*Présidente et fondatrice
de l'agence de relations
publiques PR Paradigm*



CYBERSÉCURITÉ : AVEC NIS2, LE SILENCE DES ENTREPRISES EN CAS D'ATTAQUE N'EST PLUS UNE OPTION

**Cet automne, la France vit une
échéance clé : la transposition
de la directive européenne NIS2
dans le droit national.**

Après son adoption par le Sénat et le vote en commission spéciale à l'Assemblée nationale début septembre, le texte entre dans sa phase finale avant l'adoption définitive et la publication des décrets et arrêtés d'application. C'est une étape décisive. En effet, il ne s'agit plus de débats politiques, mais de mise en œuvre concrète. Pour des milliers d'organisations, publiques comme privées, la conformité devient une réalité opérationnelle, avec son lot de décisions à prendre et de pratiques à instaurer.

Avec cette directive, l'objectif affiché par l'Union européenne est de renforcer la résilience numérique du continent face à l'intensification et à la sophistication des cyberattaques. Mais NIS2 va bien au-delà de la technique. Elle impose de nouvelles règles de gouvernance, des obligations de gestion des risques et surtout une transparence renforcée. Les incidents significatifs devront être notifiés rapidement et les manquements pourront être sanctionnés. Autrement dit, la directive ne transforme pas seulement la manière de sécuriser, elle change aussi la manière de parler de sécurité. Elle oblige les organisations à rendre des comptes et à s'exposer. C'est un changement culturel profond qui s'impose, car au-delà de protéger leurs systèmes, il s'agit pour les Organisations de cultiver à la fois crédibilité et confiance vis-à-vis de toutes les parties prenantes, clients et partenaires compris.

C'est un changement culturel profond qui s'impose, car au-delà de protéger leurs systèmes, il s'agit pour les Organisations de cultiver à la fois crédibilité et confiance vis-à-vis de toutes les parties prenantes, clients et partenaires compris

Avec l'introduction de la réglementation NIS2, se mettre en règle ne se résumera donc plus à simplement cocher des cases. Il faudra affirmer publiquement une posture, celle d'une organisation qui assume ses responsabilités et qui prend au sérieux la menace numérique. Elle revient à assurer aux clients qu'ils peuvent confier leurs données en confiance, à rassurer les partenaires sur leur solidité et à donner des gages aux autorités quant à la maturité de leur gouvernance. Dans un environnement où la confiance peut vaciller au moindre incident, ce message n'a rien d'accessoire. La conformité cesse d'être une simple question juridique ou technique pour devenir une composante de la réputation et de l'image de marque d'une organisation.

La directive introduit également une obligation qui bouleverse la gestion des crises, la notification rapide des incidents significatifs. Jusqu'ici, la plupart des entreprises réagissaient aux cyberattaques par une discrétion assumée qui impliquait si possible le silence ou, au mieux, une communication minimale. Mais cette logique n'est plus tenable. Les attaques doivent désormais être assumées. Là où la discrétion servait de bouclier, NIS2 impose une nouvelle ère de transparence.

Clairement, ce basculement marque un tournant. Les cyberattaques ne sont plus seulement des problèmes techniques à résoudre dans l'ombre, elles deviennent des événements publics qui appellent une réponse claire et assumée. Désormais, le silence ne protège plus et la communication devient une partie intégrante de la sécurité numérique. Un incident ne se gère plus uniquement avec des équipes techniques, il se joue aussi dans l'espace public. Les régulateurs demanderont des comptes, les partenaires chercheront des garanties, les médias relaieront l'information. Dans ce contexte, chaque mot compte. Une réponse trop tardive ou maladroite peut endommager durablement une réputation. À l'inverse, une parole claire et cohérente peut rassurer et démontrer la solidité de l'organisation.

C'est ici que les communicants jouent un rôle décisif. Leur mission n'est pas de maquiller la réalité, mais d'aider l'entreprise à trouver la juste ligne, parler avec transparence sans dramatiser, être précis sans tomber dans un jargon hermétique. Trop technique, le discours perd son audience ; trop vague, il mine la confiance. Beaucoup d'organisations continuent d'investir massivement dans la technologie tout en sous-estimant l'importance de cette dimension. Pourtant, un incident ne se limite pas aux pare-feu et aux centres de données. Il se joue aussi dans l'espace public où la voix des relations publiques façonne la perception et peut préserver ou fragiliser la confiance.

Réduire NIS2 à une simple obligation de gestion de crise serait une vision étroite. La directive peut devenir une opportunité. Les entreprises qui choisissent de partager leurs démarches, de mettre en valeur leurs progrès ou de mener des initiatives pédagogiques construisent un récit positif. Elles ne subissent pas la réglementation, elles la transforment en levier de confiance. C'est ce que l'on peut appeler une communication cyber-responsable, une communication transparente sans être alarmiste et pédagogique sans être naïve.

Dans un environnement saturé d'annonces et de discours convenus, cette transparence sincère fait la différence. Elle donne aux organisations une voix crédible, capable de rassurer leurs parties prenantes et d'installer une relation durable de confiance. En définitive, NIS2 rappelle une évidence trop souvent oubliée, la sécurité ne protège pas seulement des systèmes. Elle protège aussi des relations, la réputation, la crédibilité, la confiance. La technologie défend les données tandis que la communication défend la confiance. C'est à la rencontre des deux que se construit désormais la résilience. ■



BENOIT
GRÜNEMWALD

*Directeur des Affaires
publiques, ESET France.*

LAZARUS ET LES DRONES EUROPÉENS : ENQUÊTE SUR UNE CYBERMENACE GÉOPOLITIQUE

Depuis plusieurs années, le groupe de cyberespionnage Lazarus, affilié à la Corée du Nord, mène des campagnes ciblées contre des entreprises stratégiques dans le monde entier. Récemment, les chercheurs d'ESET ont mis en lumière une nouvelle offensive du groupe, baptisée « Operation DreamJob », visant des sociétés européennes impliquées dans la fabrication de drones militaires. Pour mieux comprendre les enjeux de cette campagne, nous avons posé six questions clés aux experts d'ESET.

POURQUOI LAZARUS S'INTÉRESSE-T-IL AUX ENTREPRISES EUROPÉENNES DU SECTEUR DES DRONES ?

L'intérêt de Lazarus pour les technologies de drones s'inscrit dans une stratégie plus large de développement militaire nord-coréen. Les entreprises ciblées par cette campagne sont toutes actives dans la défense, et deux d'entre elles sont directement impliquées dans la conception ou la fabrication de composants pour UAV (Unmanned Aerial Vehicles). Ce ciblage suggère que le régime cherche à acquérir des savoir-faire industriels pour améliorer ses propres capacités de production de drones, notamment en s'inspirant de modèles occidentaux.

QUELLE EST LA MÉTHODE D'ATTAQUE UTILISÉE DANS CETTE CAMPAGNE ?

Operation DreamJob repose sur une ingénierie sociale sophistiquée. Les victimes reçoivent des offres d'emploi alléchantes, accompagnées de documents piégés et de logiciels trojanisés, comme des lecteurs PDF ou des plug-ins pour Notepad++. Une fois ouverts, ces fichiers déclenchent l'installation de malwares, notamment le RAT (Remote Access Trojan) ScoringMathTea, qui permet aux attaquants de prendre le contrôle total de la machine infectée. Cette approche, déjà utilisée dans des campagnes précédentes, reste efficace malgré sa médiatisation.

QUELS SONT LES OUTILS TECHNIQUES DÉPLOYÉS PAR LAZARUS DANS CETTE OPÉRATION ?

Les chercheurs d'ESET ont identifié une série de droppers, loaders et downloaders utilisés pour introduire les malwares dans les systèmes ciblés. Parmi eux, des projets open source trojanisés comme MuPDF, TightVNC Viewer ou des plugins pour WinMerge et Notepad++. Le groupe utilise également des techniques de DLL proxying pour charger ses malwares de manière furtive. Le payload principal, ScoringMathTea, est capable d'exécuter une quarantaine de commandes, allant de la collecte d'informations système à l'exécution de nouveaux malwares.

QUEL EST LE LIEN ENTRE CETTE CAMPAGNE ET LE CONFLIT RUSSO-UKRAINIEN ?

Les entreprises visées produisent des équipements militaires actuellement déployés en Ukraine, dans le cadre du soutien européen à Kiev. Au moment des attaques, des soldats nord-coréens étaient présents en Russie, ce qui laisse penser que Lazarus cherchait à obtenir des informations sur les systèmes occidentaux rencontrés sur le champ de bataille. Cette hypothèse est renforcée par le fait que l'un des droppers utilisés dans l'attaque contient le mot « drone » dans son nom interne, suggérant un intérêt spécifique pour cette technologie.

COMMENT LAZARUS PARVIENT-IL À CONTOURNER LES SYSTÈMES DE SÉCURITÉ ?

Lazarus mise sur la diversité et la polymorphie de ses outils. En trojanisant des projets open source et en modifiant leurs exports pour les adapter au chargement de DLL malveillantes, le groupe parvient à échapper aux détections classiques. Les malwares ne sont jamais présents en clair sur le disque, mais chargés en mémoire après déchiffrement. Cette approche permet de maintenir une présence furtive tout en conservant une signature reconnaissable, facilitant l'attribution par les chercheurs.

QUELLES SONT LES IMPLICATIONS POUR LA SÉCURITÉ DES ENTREPRISES EUROPÉENNES ?

Cette campagne souligne la perméabilité des secteurs sensibles face aux attaques par ingénierie sociale. Malgré la médiatisation des méthodes de Lazarus, la sensibilisation des employés reste insuffisante. Les entreprises du secteur de la défense, et en particulier celles impliquées dans les drones, doivent renforcer leurs protocoles de sécurité, former leurs équipes à détecter les signaux d'alerte et surveiller activement les menaces émergentes. Car si Lazarus a déjà démontré son intérêt pour ces technologies, il est probable que d'autres offensives suivront.

EN GUISE DE CONCLUSION, QUELS ENSEIGNEMENTS TIREZ-VOUS DE CETTE OPÉRATION ?

L'opération DreamJob menée par Lazarus en 2025 illustre une convergence entre cyberespionnage et enjeux géopolitiques. En ciblant des entreprises européennes du secteur des drones, le groupe nord-coréen chercherait à combler ses lacunes technologiques par le vol de propriété intellectuelle. Face à cette menace persistante, la vigilance et la coopération internationale restent les meilleurs remparts. ■

Une recherche à retrouver dans son intégralité et en accès libre sur :

<https://www.welivesecurity.com/en/eset-research/gotta-fly-lazarus-targets-uav-sector/> Comprenant des IOCs et une description MITRE ATT&CK

L'intérêt de Lazarus pour les technologies de drones s'inscrit dans une stratégie plus large de développement militaire nord-coréen.



HS2

Hervé Schauer Sécurité



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



JULIEN
BRUANT

*Directeur général LSTI
Groupe apave*

RETEX NIS 2, DORA, CRA, ISO 27001, RGPD, LA CONFORMITÉ ET LA CYBERSÉCURITÉ

■ ■ **GS MAG** : *Selon vous, quels sont les défis lorsqu'il s'agit d'associer la Conformité à la Cybersécurité ?*

■ ■ **LSTI** : Le défi principal, c'est de réussir à faire cohabiter deux logiques différentes. D'un côté, la conformité repose sur des normes et des obligations. De l'autre, la cybersécurité doit rester agile et réactive face à des menaces en constante évolution.

Le rôle de l'organisme de certification spécialisé en cyber est justement de créer ce pont entre conformité et cybersécurité. La conformité fixe un cadre qui peut rapidement être perçu comme une simple obligation administrative. L'intervention d'un organisme de certification permet de redonner du sens : nous venons valider non seulement le respect des référentiels, mais aussi la capacité de l'organisation à transformer ces exigences en véritables pratiques de sécurité de l'information.

■ ■ **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 une Conformité et une Cybersécurité, au mieux possible ? Et pour quelles raisons ?*

■ ■ **LSTI** : Nous observons qu'un nombre croissant d'entreprises opte pour une stratégie de certification sur la norme ISO/IEC 27001. En effet, cette norme s'impose depuis vingt ans comme un socle de référence sur la sécurité de l'information, et dont les exigences sont reprises dans la plupart des cadres réglementaires et directives (NIS2, eIDAS, DORA, CRA, RGPD, HDS, ...).

Aujourd'hui, elle est de plus en plus exigée par les grands donneurs d'ordre, notamment pour gérer le risque numérique dans la chaîne de sous-traitance.

>>>

>>> En pratique, cette certification offre une base structurée pour mettre en place les dispositifs (tactiques) assurant d'un niveau de maturité en sécurité de l'information en fonction d'une gestion des risques propres à l'entreprise.

La certification ISO/IEC 27001 répond à la fois aux enjeux d'optimisation de la conformité, constitue pour le marché un élément de preuve et de confiance, et renforce la sécurité même de l'activité de l'entreprise. Elle constitue en quelque sorte la base d'un plan de bataille pour la sécurité de l'information !

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

■ ■ LSTI : Les réglementations, directives et politiques cyber sont essentielles pour renforcer la robustesse des entreprises face à la menace cyber, pour améliorer la résilience des solutions, protéger les données et accompagner la digitalisation de l'économie.

LSTI, en tant qu'organisme de certification, est activement impliqué dans les groupes de travail, tant sur la partie technique et normative que dans les échanges avec les autorités qui définissent la politique globale de cybersécurité.

Nous sommes également membre fondateur de l'ACAB'c, l'association des organismes de certification sur la confiance numérique en Europe, ce qui nous permet de dialoguer avec nos pairs au niveau européen.

Enfin, notre rôle en tant qu'organisme de certification est d'auditer et de certifier les entreprises sur les référentiels applicables, en évaluant la mise en œuvre de ces nouvelles exigences.

L'objectif est de transformer ces sujets de conformité parfois complexes en mises en œuvre concrètes garantissant un niveau de sécurité de l'information pour les organisations. ■

A PROPOS DE LSTI

LSTI, filiale du groupe Apave est un organisme indépendant d'évaluation de la conformité spécialisé dans la cybersécurité et la certification des services de confiance. LSTI est reconnu comme un organisme certificateur majeur en France et en Europe pour l'évaluation des prestataires de services de confiance dans le contexte du règlement eIDAS, des référentiels cyber de l'ANSSI et de la norme ISO/IEC 27001.

www.lsti-certification.fr/fr/

À PROPOS DU GROUPE APAVE

Apave est un groupe international de plus de 150 ans spécialisé dans la gestion des risques techniques, humains, environnementaux et numériques. Entreprise indépendante avec un chiffre d'affaires de 1,4Md€ en 2024, Apave compte aujourd'hui 17 500 collaborateurs dont 12 000 ingénieurs et techniciens, 130 agences en France, 170 sites de formation en France et à l'étranger qui forment plus de 630 000 stagiaires par an. Apave est présent à l'international dans plus de 60 pays. ■

www.apave.com



La certification ISO/IEC 27001 répond à la fois aux enjeux d'optimisation de la conformité, constitue pour le marché un élément de preuve et de confiance, et renforce la sécurité même de l'activité de l'entreprise.



ANNE
LESLIE

*Head of Cloud Risk
EMEA IBM_Membre du
CEFCYS*

NIS2 ET L'IMPÉRATIF DE RÉPONSE ET REPRISE APRÈS INCIDENTS : FAIRE DE LA CONFORMITÉ UNE VÉRITABLE CAPACITÉ OPÉRATIONNELLE LA CONFORMITÉ ET LA CYBERSÉCURITÉ

La directive sur la sécurité des réseaux et de l'information (NIS2) est bien plus qu'une mise à jour réglementaire – c'est un test de résistance pour la résilience numérique de l'Europe. En vigueur depuis octobre 2024, NIS2 élargit considérablement le champ des exigences : gouvernance, gestion des risques liés aux fournisseurs, continuité d'activité, et bien sûr, notification, réponse et reprise après incidents. Elle souligne qu'une politique sur papier ne saurait remplacer des capacités réelles, éprouvées et pleinement opérationnelles. C'est dans ce contexte que la réponse aux incidents devient un révélateur clé de maturité opérationnelle.

LE DÉFI : SIGNALER UN INCIDENT EST COMPLEXE – Y RÉPONDRE ET SE RELEVER L'EST ENCORE DAVANTAGE

NIS2 impose des délais stricts pour la notification des incidents – un premier signalement dans les 24 heures, suivi de mises à jour détaillées et d'un rapport final. Mais l'horloge de la conformité ne suspend pas le chaos. Quand les systèmes tombent en panne ou que des données sont compromises, la vraie question n'est pas « Pouvons-nous envoyer un rapport ? » mais bien « Comment capitaliser sur notre maîtrise des incidents pour renforcer la confiance ? ».

>>>

>>> Nombre d'organisations abordent la notification d'incidents comme une formalité administrative, alors qu'il s'agit en réalité d'un levier stratégique. C'est la partie visible d'une capacité bien plus profonde : détecter, hiérarchiser et répondre sous pression. Et cette capacité ne s'improvise pas en pleine crise.

POURQUOI IL FAUT VALIDER LES HYPOTHÈSES

La plupart des plans de réponse et de reprise après incidents sont parfaits... sur le papier. Mais la réalité est désordonnée. Les vecteurs d'attaque ne suivent pas les manuels, et les dépendances insoupçonnées surgissent au pire moment. C'est pourquoi les tests ne sont pas facultatifs – ils sont essentiels.

Les exercices de simulation sur table sont un bon début, mais insuffisants. La vraie résilience vient de simulations qui mettent à l'épreuve les systèmes et les équipes, révèlent les angles morts et valident les hypothèses. Qui appelle qui à 2h du matin ? Comment escalader la situation si le canal de communication principal est hors service ? Que se passe-t-il si votre « fournisseur critique » est lui aussi en crise ? Ce ne sont pas des scénarios hypothétiques – ce sont des réalités inévitables.

LA PRATIQUE RENFORCE LA CONFIANCE SOUS PRESSION

La gestion des incidents est un effort collectif. Et comme tout effort, la performance sous pression dépend de l'entraînement. L'objectif n'est pas la perfection, mais des réflexes opérationnels. Quand les rôles, responsabilités et chemins décisionnels sont répétés, les équipes peuvent agir avec assurance plutôt que de débattre dans le noir.

Les organisations qui réussiront seront celles capables d'opérationnaliser leurs plans, pas seulement de les documenter. Cela implique de concevoir pour la

flexibilité : canaux de communication alternatifs, cadres décisionnels validés à l'avance, et chemins d'escalade qui fonctionnent même quand l'organigramme ne le permet pas.

Développer ces réflexes nécessite plus que des exercices annuels. Il faut intégrer les simulations dans le rythme opérationnel – de manière transversale : entre fonctions, pays et de plus en plus, entre secteurs. Car dans une économie hyperconnectée, un incident ne vous concerne jamais uniquement vous.

À QUOI RESSEMBLE L'EXCELLENCE

Des tendances se dessinent parmi les organisations qui voient NIS2 comme une opportunité plutôt qu'une contrainte :

- **Validation continue** – tests réguliers des hypothèses de détection, de réponse et reprise.
- **Diversité des scénarios** – allant des ransomwares aux compromissions de la chaîne d'approvisionnement, pas seulement les exercices « faciles ».
- **Processus intégrés de reporting** – afin que la conformité ne nuise pas à la gestion de crise.
- **Exercices collaboratifs** – avec fournisseurs, régulateurs et pairs, car le risque systémique appelle une réponse et reprise systémique.

PERSPECTIVES

NIS2 fixe un standard, mais le véritable facteur différenciant est culturel : il s'agit d'ancrer la résilience – en matière de réponse et de reprise – au cœur des capacités de l'organisation, et non de la réduire à une simple exigence de conformité.

Car lorsque l'incident inévitable surviendra, le succès ne se mesurera pas à la rapidité du signalement, mais à l'efficacité avec laquelle l'impact aura été contenu et les activités rétablies. ■

En vigueur depuis octobre 2024, NIS2 élargit considérablement le champ des exigences : gouvernance, gestion des risques liés aux fournisseurs, continuité d'activité, et bien sûr, notification, réponse et reprise après incidents.

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*



RETEX NIS 2, DORA, CRA, ISO 27001, RGPD, LA CONFORMITÉ ET LA CYBERSÉCURITÉ

■ ■ **GS MAG** : Selon vous, quels sont les défis lorsqu'il s'agit d'associer la Conformité à la Cybersécurité ?

■ ■ **LG** : Associer Conformité et Cybersécurité est un défi majeur en soi : il faut aligner des cadres réglementaires stricts sur un paysage de cybermenaces en constante évolution.

L'émergence de l'IA agentique complexifie cette association. Le "digital workspace" devient "agentique", où les agents IA agissent pour les humains. Chaque collaboration (humaine ou IA) comporte un risque de données.

Les agents IA consomment, génèrent et manipulent des données, élargissant la surface de menace et introduisant de nouvelles attaques comme l'injection de prompt.

Le paysage réglementaire (NIS2, DORA, CRA, RGPD) imposant des exigences strictes, le défi est de traduire ces règles en mesures concrètes. La "conformité de façade" n'est pas une option. Seule une sécurité intrinsèque est essentielle à la survie numérique.

■ ■ **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 une Conformité et une Cybersécurité, au mieux possible ? Et pour quelles raisons ?

■ ■ **LG** : Pour une cyber-résilience et une protection des données optimales dans cet environnement agentique, les organisations doivent articuler leur stratégie autour de la gouvernance et d'une gestion rigoureuse des risques tout au long du cycle de vie, en s'appuyant sur des normes comme l'ISO 27001.

Sur le plan tactique, les fondamentaux tels que l'EDR, le MFA et le chiffrement restent des piliers essentiels. Les SOC, enrichis par l'IA, doivent analyser en temps réel, hiérarchiser les alertes et proposer des actions correctives (MITRE ATT&CK).

>>>

>>> L'évolution vers l'espace de travail agentique exige trois capacités fondamentales :

1. Mapping des menaces d'interactions :

Par exemple aujourd'hui détecter et arrêter les exploits d'injection de prompt avant qu'ils n'atteignent l'utilisateur ou l'agent IA.

2. Mapping des risques de données :

Avoir une visibilité unifiée sur les données (structurées/non structurées, SaaS, cloud, collaboration). Classer, contrôler l'accès, surveiller l'utilisation et appliquer des politiques de gouvernance automatiquement, y compris pour l'accès des IA.

3. Contrôles et passerelles adaptés aux agents :

Une "passerelle d'agent" agit comme un plan de contrôle pour les agents IA, appliquant les politiques de données, empêchant l'exposition non autorisée et surveillant l'activité. A noter qu'ici, l'utilisation du protocole de contexte de modèle (MCP) permet aux agents d'IA de différents écosystèmes (par exemple de tiers) d'interagir, de façon sécurisée, par des mécanismes unifiés, pour l'accès aux données ou l'exécution d'actions.

Une approche "Human – IA Centric" est donc désormais primordiale, pour protéger à la fois les collaborateurs et les agents IA.

Tout s'accélère. Il existe déjà des solutions techniques éprouvées, étendues désormais par des agents IA. Par exemple, la solution Human Communications Intelligence (HCI) de Proofpoint¹, basée sur l'IA agentique, transforme les communications humaines en renseignements exploitables.

Elle détecte, raisonne et prévient les risques (fautes professionnelles, menaces internes) en temps réel, passant d'une conformité post-incident à une prévention proactive, en interprétant l'intention humaine...

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

■ ■ **LG** : L'adaptation est une constante. Face à l'évolution rapide des technologies et des réglementations, une approche proactive est indispensable. Concernant l'IA, le CLUSIF a d'ailleurs publié un "Modèle de Politique de Sécurité des Systèmes d'Information (PSSI) pour l'Intelligence artificielle" en février 2025². Ce modèle est crucial pour encadrer le développement et l'utilisation sécurisée de l'IA.

L'IA offre des opportunités fantastiques pour automatiser et renforcer la conformité (audits, détection de menaces pour NIS2/DORA, gestion d'incidents pour CRA), réduisant les erreurs humaines. Mais elle introduit aussi de nouveaux risques.

Le rapport "Voice of the CISO 2025" de Proofpoint³ a révélé que 61 % des RSSI français s'inquiètent du risque de perte de données clients via les outils publics d'IA générative. Les vulnérabilités (biais, hallucinations, attaques adverses comme l'injection de prompt) nécessitent des adaptations réglementaires (RGPD, NIS2) pour évaluer les risques spécifiques à l'IA, augmentant les coûts et posant des questions de responsabilité.

L'évolution des normes sera une intégration IA-centrique. L'IA incite à réviser le CRA et DORA pour inclure des exigences de transparence et d'explicabilité, induites par des approches hybrides homme-IA. Les outils traditionnels ne suffisent plus ; il faut protéger humains et agents IA. Cela implique une visibilité unifiée et des contrôles adaptés aux agents.

En somme, une nouvelle ère arrive, où l'IA transforme fondamentalement la façon de travailler et de se défendre. Mais une question s'impose : jusqu'où peut-on déléguer sans perdre le contrôle, surtout lorsque des agents IA agissent en notre nom ? ■

Les agents IA consomment, génèrent et manipulent des données, élargissant la surface de menace et introduisant de nouvelles attaques comme l'injection de prompt.

1 <https://www.proofpoint.com/fr/products/digital-communications-governance>

2 <https://clusif.fr/publications/pssi-ia/>

3 <https://www.proofpoint.com/fr/newsroom/press-releases/proofpoint-2025-voice-ciso-report>



ÉCHANGER ET AGIR ENSEMBLE POUR LA CONFIANCE DANS LE NUMÉRIQUE

Le Clusif est l'association de référence de la cybersécurité en France. Reconnu d'utilité publique par l'Etat, sa mission consiste à favoriser les échanges d'idées et de retours d'expérience. Les membres du Clusif sont issus de tous les secteurs économiques.

REJOIGNEZ-NOUS !

Et contribuez à l'ensemble de nos activités :

Le Panorama de la cybercriminalité

Les conférences

Le podcast

Les publications

Les études sur les pratiques de sécurité

Les exercices de crise et les défis cyber étudiants

Nos nombreuses contributions auprès des métiers hors cyber, des pouvoirs publics



GÉRÔME
BILLOIS

*PARTNER CYBERSECURITY
& DIGITAL TRUST_
WAVESTONE*



RETEX NIS 2, DORA, CRA, ISO 27001, RGPD, LA CONFORMIT  ET LA CYBERS CURIT 

Le principal d fi r side dans la multiplication des textes r glementaires et des exigences qui se recourent partiellement, varient selon les secteurs et les niveaux (national, europ en, international... et les th matiques : infrastructure critique, r silience, produit, privacy...). Pour les grands acteurs mondiaux, il n'est pas rare d' tre suivis par plusieurs dizaines, voire centaines de r gulateurs, et de devoir se conformer   des centaines, parfois des milliers, d'obligations diff rentes.

  cela s'ajoute un contexte g opolitique complexe, marqu  par des tensions et une remise en question de la d pendance num rique : certaines zones imposent d sormais leurs propres solutions technologiques ou crit res de conformit . Ces  l ments sont parfois r glementaires et ajoutent un niveau de complexit  additionnel en n cessitant des mises en  uvre de technologies contraignantes.

Ces  volutions, et les exigences des r gulateurs lors d'audits, viennent souvent bousculer les programmes de cybers curit  d j  en place, obligeant les organisations   revoir leurs priorit s et   mieux int grer les exigences de conformit  dans leurs plans d'action op rationnels.

Les  quipes de cybers curit  doivent rationaliser toutes ces exigences et augmenter la souplesse de leurs approches pour prendre en compte ces  l ments de mani re r active, sans pour autant perdre le cap de leur strat gie. C'est un peu la quadrature du cercle par moment !

■ ■ GS MAG : Selon vous, quels sont les défis lorsqu'il s'agit d'associer la Conformité à la Cybersécurité ?

■ ■ GB : Le principal défi réside dans la multiplication des textes réglementaires et des exigences qui se recoupent partiellement, varient selon les secteurs et les niveaux (national, européen, international... et les thématiques : infrastructure critique, résilience, produit, privacy...). Pour les grands acteurs mondiaux, il n'est pas rare d'être suivis par plusieurs dizaines, voire centaines de régulateurs, et de devoir se conformer à des centaines, parfois des milliers, d'obligations différentes.

À cela s'ajoute un contexte géopolitique complexe, marqué par des tensions et une remise en question de la dépendance numérique : certaines zones imposent désormais leurs propres solutions technologiques ou critères de conformité. Ces éléments sont parfois réglementaires et ajoutent un niveau de complexité additionnel en nécessitant des mises en œuvre de technologies contraignantes.

Ces évolutions, et les exigences des régulateurs lors d'audits, viennent souvent bousculer les programmes de cybersécurité déjà en place, obligeant les organisations à revoir leurs priorités et à mieux intégrer les exigences de conformité dans leurs plans d'action opérationnels.

Les équipes de cybersécurité doivent rationaliser toutes ces exigences et augmenter la souplesse de leurs approches pour prendre en compte ces éléments de manière réactive, sans pour autant perdre le cap de leur stratégie. C'est un peu la quadrature du cercle par moment !

■ ■ 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 une Conformité et une Cybersécurité, au mieux possible ? Et pour quelles raisons ?

■ ■ GB : Les organisations les plus matures ont tendance à structurer leur propre framework interne, qui agrège et relie les différentes exigences réglementaires afin de disposer d'une base de travail unique et cohérente dans le temps. Certaines mettent également en place des « compliance towers » ou des « remediation centers », chargés de piloter la conformité et de gérer les actions correctives, notamment lors des contrôles des régulateurs. Ce modèle centralisé permet de conserver une vision d'ensemble, le cap de la stratégie et une cohérence entre les différentes entités, mais requiert un haut niveau d'expertise et de coordination. À l'inverse, des structures plus petites ou plus décentralisées adoptent souvent une approche locale de la conformité, chaque pays ou entité gérant ses

obligations et son niveau de risque. C'est particulièrement le cas sur NIS 2 avec les divergences fortes d'approche entre pays européens. Cette stratégie, bien que plus risquée en matière d'homogénéité, reste parfois la seule option réaliste compte tenu des moyens disponibles. Elle requiert cependant la mise en place d'un mécanisme de gestion de crise à l'échelle du groupe en cas de problème de conformité. En effet les impacts d'une non-conformité locale pouvant rapidement être visible à l'échelle internationale et vont requérir une réponse coordonnée.

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

■ ■ GB : Pour les équipes cybersécurité, cette adaptation constante n'a rien de nouveau : le domaine évolue en permanence, tant sur le plan technologique que réglementaire, et les organisations sont désormais rompues à cet exercice, toujours complexe, de veille et d'ajustement continu.

Les dernières évolutions récentes concernent surtout l'intelligence artificielle, avec l'apparition de frameworks et de politiques de sécurité spécifiques précisant les nouveaux risques et les mesures associées, notamment pour l'IA générative et agentique. Cela conduit à la mise à jour des processus et à la mise en place de nouveaux outils plateformes de sécurité dédiées. L'enjeu a été de s'assurer que les multiples IA créées par les métiers seront suffisamment sécurisées et ...conforme, en particulier en Europe avec l'IA Act mais les réglementations internationales se multiplient. A moyen terme il y a un enjeu autour du développement d'IA et de datalake pour la cybersécurité sur lesquels il y a beaucoup d'expérimentations et qui pourront simplifier grandement la conformité en permettant une vue en temps réel du niveau de l'organisation.

S'agissant du quantique, nous en sommes encore à la phase amont de définition de la stratégie et de la gouvernance, sans modification majeure des politiques ou référentiels existants à date. Cela va arriver d'ici quelques mois. Mais contrairement à l'IA, il s'agit davantage d'un projet de migration technologique, avec des impacts limités sur le business à court terme. Les exigences réglementaires sont pour l'instant assez simples, donnant des dates de migration réalistes mais nécessitant des actions dès 2026.

De manière générale, toute stratégie cyber solide inclut désormais un chantier "Emerging Threats & Regulations", actif pendant toute la durée de la stratégie, permettant de maintenir une ligne budgétaire et un organe de gouvernance pour faire les actions urgentes d'évaluation et de priorisation face aux nouvelles menaces mais aussi de s'assurer de la mise à jour régulière des référentiels et politiques de sécurité à l'échelle de toute l'organisation. ■



Plateforme IAM SaaS européenne au service des enjeux business

• IAM •

• IGA •

• Fédération •

• CIAM •

• SSO •

• MFA •

• Employés •

• Partenaires •

• Clients •

• Citoyens •

• Objets
connectés

www.memory.eu



HEXATRUST

CLOUD CONFIDENCE & CYBERSECURITY

ET SI VOUS REJOIGNIEZ EN 2026 L'ASSOCIATION DES LEADERS EUROPÉENS DE LA CYBERSÉCURITÉ ET DU CLOUD DE CONFIANCE ?

Dans un contexte géopolitique incertain, il est plus que jamais nécessaire de se rassembler autour d'un collectif engagé au service d'un écosystème tech français et européen, protecteur de vos données.

Rejoindre Hexatrust, c'est faire entendre votre voix et intégrer une communauté dynamique et innovante, pour faire rayonner ensemble le savoir-faire européen.

L'UNION FAIT LA FORCE



Défendre

Agir pour nos adhérents et anticiper les défis réglementaires de demain.



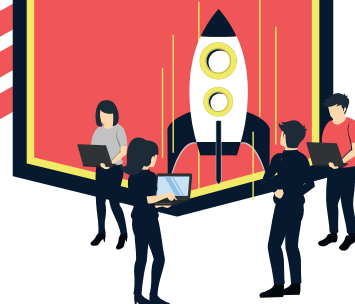
Représenter

Porte-parole de la filière et accélérateur du développement des entreprises du numérique de confiance.



Promouvoir

Valoriser l'excellence française et européenne du numérique de confiance.



Rejoignez la communauté du numérique de confiance
WWW.HEXATRUST.FR | CONTACT@HEXATRUST.FR

A portrait of Jean-Michel Mis, a middle-aged man with short grey hair and glasses, wearing a dark suit, light blue shirt, and dark tie. He is smiling and looking towards the camera. The background is a blurred indoor setting with warm lighting. To the right of the portrait, there is a decorative graphic consisting of numerous small squares in various shades of gold and brown, some of which are larger and more prominent, creating a pixelated or mosaic-like effect.

JEAN-MICHEL
MIS

*ANCIEN DÉPUTÉ
PRÉSIDENT
VIA PUBLICA Conseils*

DE LA PROTECTION DES OIV À LA RÉSILIENCE SYSTÉMIQUE : UN CHANGEMENT D'ÉPOQUE

Pendant près d'une décennie, la politique française de cybersécurité s'est structurée autour d'une priorité claire : protéger les Opérateurs d'Importance Vitale (OIV). Cette stratégie fondatrice a permis de bâtir un socle solide face à la montée des menaces numériques.

En tant qu'ancien député et ancien vice-président du groupe d'études « Cybersécurité et Souveraineté numérique » de l'Assemblée nationale, aujourd'hui consultant auprès d'acteurs publics et privés, j'ai suivi l'émergence d'un modèle nouveau : celui d'une résilience numérique élargie.

Avec NIS 2, DORA et le Cyber Resilience Act, nous entrons dans une phase où la cybersécurité n'est plus l'affaire d'un cercle restreint mais d'un écosystème national complet : infrastructures publiques, collectivités, santé, industries, cloud, prestataires technologiques, entreprises de toutes tailles.

UN CADRE COHÉRENT AVEC ISO 27001 ET LE RGPD

Cette transformation s'inscrit dans un cadre réglementaire et normatif cohérent, qui ne remplace pas mais complète l'existant.

- ISO 27001, dont la version 2022 modernise les contrôles et renforce la dimension opérationnelle, demeure le socle international de gestion des risques et de gouvernance de la sécurité.
- Le RGPD, dont l'application et la jurisprudence se consolident à l'échelle européenne, reste la pierre angulaire de la protection des données et de la notification des incidents.
- NIS 2 et DORA introduisent une obligation de résultat en matière de continuité, de maîtrise de la chaîne d'approvisionnement et de pilotage au niveau dirigeant.

Ainsi, les organisations peuvent s'appuyer sur leurs fondations ISO 27001 / RGPD tout en intégrant les exigences nouvelles : maturité renforcée, industrialisation de la réponse, gouvernance exécutive et coopération renforcée.

UNE MOBILISATION ÉLARGIE SUR TOUT LE TERRITOIRE

L'intégration dans le champ réglementaire de nouveaux secteurs — hôpitaux, collectivités, opérateurs territoriaux, prestataires — reflète une réalité : la continuité de la vie économique et des services publics repose désormais sur un tissu numérique distribué.

Partout en France, des dynamiques positives se déploient : mutualisations, centres cyber régionaux, montée en compétence, partage d'expertise. Cette évolution témoigne de la capacité du pays à structurer une réponse collective, progressive et pérenne.

La nomination d'Anne Le Hénanff au gouvernement, ancienne rapporteure du titre « cybersécurité et infrastructures critiques » à l'Assemblée nationale, constitue à cet

égard un signal politique fort : la cybersécurité n'est plus un sujet purement technique, elle devient un levier de souveraineté, de continuité républicaine et de résilience nationale, piloté au plus haut niveau de l'État.

LE RÔLE STRUCTURANT DE L'ANSSI

Dans cette phase, l'ANSSI joue un rôle pivot. Aux missions régaliennes — protection de l'État, qualification de l'expertise — s'ajoute désormais une mission structurante : accompagner l'élévation du niveau de sécurité dans l'ensemble du paysage économique et institutionnel.

UNE DYNAMIQUE EUROPÉENNE AFFIRMÉE

Comme le souligne Henna Virkkunen, Commissaire chargée de la souveraineté technologique :

"We have to be prepared for many different kinds of threats. That's why we must closely cooperate together."

L'Europe fait de la cybersécurité un pilier de sa souveraineté numérique, dans une logique de cohérence, d'intégration et de coopération.

UN RENDEZ-VOUS PARLEMENTAIRE EN JANVIER

Le projet de loi de transposition, adopté au Sénat et en commission à l'Assemblée nationale, sera débattu à l'Assemblée nationale selon l'annonce du gouvernement.

La France entrera dans une ère où la cybersécurité devient un socle commun, partagé par l'ensemble des acteurs économiques et publics. Nous passons d'un modèle défensif ciblé à un modèle de résilience distribuée, mobilisant gouvernance, gestion du risque, protection des données, continuité d'activité et coopération territoriale.

C'est un moment structurant pour notre pays comme pour l'Europe, et une étape essentielle vers un numérique plus sûr, plus stable et je l'espère plus souverain. ■

Avec NIS 2, DORA et le Cyber Resilience Act, nous entrons dans une phase où la cybersécurité n'est plus l'affaire d'un cercle restreint mais d'un écosystème national complet

ANNE
LE HÉNANFF

*Ministre déléguée chargée
de l'Intelligence Artificielle
et du Numérique*



PAR SÉVERINE MEUNIER

VERS UNE SÉCURITÉ NUMÉRIQUE SOUVERAINE : RELIER LA RÉFLEXION STRATÉGIQUE À L'ACTION COLLECTIVE

Dans le débat sur la défense et la souveraineté, Anne Le Hénanff s'est imposée au fil des années comme une voix singulière, exigeante et lucide. Rapporteuse pour avis à la commission de la Défense nationale et des forces armées, elle plaide pour une approche de la sécurité qui dépasse les frontières traditionnelles entre militaire et civil, entre technique et politique.

SON FIL CONDUCTEUR ?

Construire une autonomie stratégique européenne fondée sur la capacité à produire, à protéger et à décider.

Cette vision résonne particulièrement avec les transformations en cours dans le champ de la sécurité numérique. Ce domaine, souvent réduit au "cyber", mérite au contraire une approche systémique : il s'agit moins de protéger des machines que de garantir la fiabilité de nos décisions, la résilience de nos institutions et la confiance dans nos outils. Dans ce champ, la souveraineté ne se mesure pas en lignes de code mais en capacité collective à comprendre, anticiper et agir.



Construire une autonomie stratégique européenne fondée sur la capacité à produire, à protéger et à décider.

Anne Le Hénanff met en garde contre les dépendances technologiques qui grignotent notre autonomie décisionnelle. Cette réflexion rejoint mes travaux sur la détection des signaux faibles et l'analyse comportementale : la véritable vulnérabilité ne vient pas seulement des failles techniques, mais de notre difficulté à percevoir les interconnexions invisibles — entre infrastructures, données, comportements et influence informationnelle. La sécurité numérique, c'est avant tout une écologie de la lucidité.

La députée* défend également une approche équilibrée du continuum entre innovation civile et défense. Là encore, la frontière s'estompe : les technologies issues du monde civil — intelligence artificielle, cloud, traitement massif de données — irriguent désormais la stratégie militaire.

Cette porosité, si elle est encadrée, devient un levier : elle favorise la coopération, stimule la recherche et accélère la montée en compétences. Mais elle suppose un cadre éthique, une gouvernance et une capacité à penser la temporalité longue, au-delà des cycles politiques ou industriels.

DANS LE CHAMP DE LA SÉCURITÉ NUMÉRIQUE, CETTE VISION APPELLE UNE VIGILANCE PARTAGÉE

Renforcer la culture de sécurité dans les collectivités, valoriser le rôle des réservistes numériques, intégrer davantage de profils féminins et pluridisciplinaires : autant d'enjeux que je constate aussi sur le terrain. La sécurité ne se décrète pas depuis le sommet, elle se construit à tous les niveaux — dans les administrations, les entreprises, les écoles, les territoires.

L'UN DES APPORTS MAJEURS D'ANNE LE HÉNANFF EST DE REPLACER L'HUMAIN AU CŒUR DE LA RÉFLEXION STRATÉGIQUE

Elle parle de mémoire, de conditions de service, de justice : des mots rares dans un univers souvent dominé par la technique. Cette approche rejoint ma conviction : la sécurité numérique doit rester un projet de société, pas seulement un sujet d'ingénieurs. Elle engage nos valeurs, notre rapport à la confiance et notre manière de transmettre.

En reliant nos champs d'action — défense, renseignement, innovation, protection des données —, une perspective se dessine : celle d'une sécurité numérique souveraine, pensée comme une continuité entre la maîtrise technologique et la responsabilité collective. Dans un monde où la donnée devient un espace de confrontation, notre résilience dépendra autant de notre capacité à innover que de notre aptitude à relier.

La défense de demain ne sera pas seulement celle des armes, mais celle de la cohérence : cohérence entre les institutions et les citoyens, entre la technologie et l'éthique, entre l'information et la décision. Anne Le Hénanff nous rappelle que la souveraineté n'est pas une posture mais une pratique ; qu'elle se cultive dans le quotidien des politiques publiques, des infrastructures et des consciences.

À l'heure où la sécurité numérique devient la colonne vertébrale de nos démocraties, il ne s'agit plus seulement de se protéger, mais de se projeter. Réconcilier la stratégie et l'humain, la défense et la donnée, le discernement et la vitesse : voilà sans doute le défi du temps présent. Et c'est à cette jonction, entre vision et action, que se joue désormais notre véritable autonomie. ■



SÉVERINE
MEUNIER

*Experte en Sécurité
Numérique et Intelligence
Appliquée*

L'INTELLIGENCE ARTIFICIELLE AU SERVICE DU CRIME ORGANISÉ : L'EUROPE FACE À UN DILEMME STRATÉGIQUE

**L'INTELLIGENCE ARTIFICIELLE
N'EST PLUS UN SIMPLE
ACCÉLÉRATEUR ÉCONOMIQUE :
ELLE EST DEVENUE UN
MULTIPLICATEUR OPÉRATIONNEL
POUR LE CRIME ORGANISÉ.**

Mais en Europe — et singulièrement
en France — répondre avec les mêmes
outils se heurte à des garde-fous juridiques et
éthiques stricts. Entre efficacité criminelle
et respect des droits fondamentaux,
comment concilier sécurité et démocratie ?

CONTEXTE : L'IA COMME CATALYSEUR DU CRIME ORGANISÉ

Les organisations criminelles exploitent aujourd'hui l'IA pour automatiser des fraudes, créer des contenus falsifiés et optimiser la logistique de leurs trafics. Des deepfakes aux systèmes de phishing ultra-personnalisés, en passant par l'automatisation de circuits financiers opaques, la technologie devient un multiplicateur de capacités pour des réseaux qui opèrent à l'échelle mondiale. Europol et d'autres instances internationales alertent sur la vitesse et l'efficacité de ces nouveaux modes opératoires.

Contrairement à certaines représentations, l'usage criminel de l'IA ne transforme pas les trafics classiques — drogues, traite, contrefaçon, contrebande — qui demeurent majoritairement analogiques. La véritable évolution se situe dans les marges financières : fraude, escroqueries, faux ordres, détournements, micro-blanchiment.



Ces segments, plus discrets mais stratégiques, absorbent aujourd'hui l'essentiel des innovations liées à l'IA. C'est sur cette composante "crime économique", souvent sous-estimée, que repose désormais une part croissante du financement des organisations criminelles.

L'IA transforme le crime organisé en une machine agile et adaptative, capable d'opérer plus vite que la plupart des institutions publiques.

L'IA ne crée pas un crime organisé augmenté : elle amplifie le crime organisé déjà rentable.

ÉTAT DES LIEUX : COMMENT LES RÉSEAUX CRIMINELS « APPRENNENT » ET AGISSENT

1. Phishing et fraude automatisés :

L'IA permet de générer des messages multilingues hyper-personnalisés, testés et ajustés en continu selon les réponses des victimes.

2. Faux identitaires et extorsion :

La génération audio et vidéo facilite les usurpations de voix ou de visages à des fins d'extorsion ou de chantage.

3. Blanchiment sophistiqué :

Les modèles d'IA orchestrent des chaînes financières complexes, avec comptes factices et micro-transferts, rendant le suivi des fonds difficile.

4. Adaptation tactique en temps réel :

Grâce à l'IA et à l'analyse OSINT, les réseaux ajustent leurs actions en fonction des mesures de police ou des fermetures de plateformes.

DES CHIFFRES CONFIRMENT CETTE DYNAMIQUE :

EPPO: 2 666 enquêtes en cours pour 24,8 milliards d'euros de préjudice, dont 13,15 milliards liés aux fraudes à la TVA. <https://www.eppo.europa.eu/en/media/news/2024-annual-report-eppo-leading-charge-against-eu-fraud>

OLAF: 871,5 millions d'euros de fonds détournés identifiés et 43,5 millions d'euros de dépenses frauduleuses évitées. https://anti-fraud.ec.europa.eu/media-corner/news/olaf-exposes-fraud-involving-over-eu870-million-2025-06-16_fr

Ministère de l'Intérieur: 348 000 atteintes numériques enregistrées, dont 226 300 atteintes aux biens, principalement des escroqueries.

Source : Ministère de l'Intérieur, janvier 2025

<https://www.interieur.gouv.fr/actualites/communiques-de-presse/publication-du-rapport-annuel-relatif-a-cybercriminalite>

Ces données confirment une tendance profonde :

la fraude est devenue un moteur financier majeur, stable et peu risqué pour les organisations criminelles, bien plus que certains trafics traditionnels.

Ces tendances montrent que l'IA n'est pas seulement un outil : elle va devenir une compétence stratégique pour le crime organisé.

Le futur du crime est moins technologique qu'adaptatif : l'IA accélère ce qui fonctionnait déjà.

MODE OPÉRATOIRE : UNE ORGANISATION NUMÉRIQUE ET MODULAIRE

Les réseaux criminels structurent désormais leurs activités comme de véritables chaînes de production numériques :

• Spécialisation des rôles :

développeurs de malware, opérateurs de comptes, gestionnaires de marketplaces illicites.

• Exploitation des vulnérabilités des systèmes :

manipulation de données ou attaques sur des modèles d'IA pour contourner les défenses.

• Réactivité accrue :

adaptation rapide aux mesures des forces de l'ordre grâce à l'analyse automatisée de données ouvertes.

Cette modularité confère aux organisations criminelles une résilience opérationnelle et un avantage stratégique difficile à contrer avec les méthodes traditionnelles.

Au-delà de la seule modularité, l'IA renforce la capacité des réseaux à exploiter des « signaux faibles » : comportements atypiques, réactions émotionnelles, horaires de réponse, traces OSINT.

Loin d'un mythe technologique, il s'agit d'une optimisation incrémentale : tester, mesurer, ajuster. Cette logique quasi-industrielle n'augmente pas la criminalité en volume, mais en efficacité, rendant certains schémas d'escroquerie plus difficiles à détecter pour les dispositifs de conformité.

Le crime organisé ne devient pas numérique : il devient hybride. Et c'est pire.

>>>

>>> LE DILEMME EUROPÉEN ET FRANÇAIS : POURQUOI NOUS NE POUVONS PAS « JOUER LE MÊME JEU »

En Europe, et en France en particulier, les autorités font face à un paradoxe : elles disposent de moyens légaux et techniques limités pour utiliser l'IA à des fins offensives ou d'infiltration.

CONTRAINTES MAJEURES

- **Réglementation sur l'IA (AI Act) :**
interdiction de certaines manipulations et limitations strictes pour la surveillance automatisée.
- **Protection des données (GDPR) :**
encadrement rigoureux de la collecte et du traitement des informations personnelles.
- **Cadres procéduraux stricts :**
création de faux profils ou infiltration de forums illicites nécessite autorisation judiciaire.
- **Culture démocratique et droits fondamentaux :**
toute action intrusive doit être proportionnée et contrôlée, sous peine de rendre les preuves irrecevables.

Ces contraintes limitent l'usage de certaines armes technologiques que les criminels utilisent sans scrupules, créant un décalage tactique significatif

CRIMINALITÉ ANALOGIQUE

Une part importante du crime organisé continue pourtant de prospérer par des moyens strictement analogiques : transport physique, messageries humaines, réseaux relationnels, comptabilité hors-système. Comme le rappellent de nombreux praticiens, "le meilleur moyen d'échapper à la surveillance numérique reste de ne pas être numérique". La sophistication technologique ne concerne qu'une fraction du paysage criminel.

Le futur du crime est
moins technologique
qu'adaptatif : l'IA accélère
ce qui fonctionnait déjà.

PARADOXE EUROPEEN

L'Europe a développé le meilleur cadre éthique du monde... mais pas la meilleure vitesse d'exécution.

■ **L'enquêteur Quentin Mugg ancien enquêteur à l'OCRGDF et auteur de Argent sale : la traque, le rappelle dans plusieurs de ses travaux :** les courtiers criminels demeurent depuis des décennies les véritables moteurs invisibles du blanchiment, bien plus que les innovations technologiques récentes. Il décrit cette hégémonie discrète, fondée sur des réseaux de confiance, des flux non bancarisés et des systèmes comme le Hawala, qui continuent de fonctionner parfaitement en marge de toute surveillance numérique.

Ce contraste souligne un point essentiel : l'IA renforce la fraude observable, mais une large partie des flux criminels reste invisible par nature, non pas par technologie.

Mais l'enjeu principal n'est pas technologique : il est écosystémique.

L'IA n'invente pas le crime. Elle optimise un système qui existe déjà depuis longtemps, structuré par des réseaux d'intermédiaires qui maîtrisent l'art de la discrétion et de l'exploitation des failles.

L'essor de l'intelligence artificielle bouleverse profondément les modes opératoires du crime organisé. Loin des représentations classiques centrées sur la violence, les armes ou les marquages territoriaux, la criminalité contemporaine s'appuie désormais sur une logique industrielle, fondée sur la donnée, l'automatisation et l'externalisation. L'IA devient un levier, un amplificateur et, de plus en plus, un architecte invisible des attaques numériques, des fraudes massives, de la pédocriminalité en ligne ou du blanchiment financier.

■ **Au cœur de cette transformation se trouve une réalité encore trop peu comprise :** l'économie criminelle repose moins sur ses exécutants que sur ses facilitateurs. Ce ne sont pas les profils voyants qui structurent l'écosystème, mais ceux qui orchestrent, conseillent, anonymisent, connectent, forment, optimisent. Ces intermédiaires — brokers, développeurs, logisticiens, blanchisseurs, ingénieurs IA — façonnent l'infrastructure du crime moderne.

■ **Parmi eux, une catégorie se distingue par son ancienneté et son rôle déterminant :** les "courtiers criminels". Comme le rappelle un article récent du Nouvel Obs, ces acteurs n'ont rien d'un phénomène émergent : ils constituent depuis des décennies la charpente silencieuse de la criminalité organisée. Leur fonction n'est pas de prendre des risques, mais de rendre le système fluide, rentable et surtout invisible.



LES COURTIER CRIMINELS : UNE HÉGÉMONIE SILENCIEUSE QUI PRÉCÈDE L'IA

Longtemps ignorés des politiques publiques, les courtiers criminels opèrent dans l'ombre comme les véritables ingénieurs de résilience du crime organisé. Leur rôle s'étend bien au-delà du blanchiment traditionnel :

- Ils assurent la circulation et la conversion des flux illicites ;
- Ils connectent les groupes entre eux ;
- Ils fournissent l'infrastructure logistique, technique et financière dont les criminels ont besoin ;
- Ils opèrent à la frontière du légal et de l'illégal, exploitant les angles morts réglementaires.

Ils préexistent à l'IA, mais l'IA multiplie leur puissance. Elle leur offre une capacité nouvelle à :

- Cartographier automatiquement les vulnérabilités d'un système ;
- Industrialiser des escroqueries à grande échelle ;
- Automatiser la création d'identités synthétiques, de contenus prétextes ou de deepfakes crédibles ;
- Diversifier les flux financiers en s'appuyant sur des intermédiaires dématérialisés ;
- Faciliter l'exploitation sexuelle des mineurs en ligne via des outils de diffusion et de camouflage.

L'IA devient ainsi l'outil parfait pour un intermédiaire discret : un multiplicateur d'efficacité sans exposition.

"Les courtiers criminels restent l'infrastructure la plus résiliente du blanchiment : aucune IA ne concurrence un système qui n'a jamais été numérique prospérer sans être vu."

Comparaisons internationales

- **Royaume-Uni :**
le cadre CHIS (Covert Human Intelligence Sources) autorise sous supervision l'infiltration, offrant plus de marges de manœuvre.
- **États-Unis :**
moins de restrictions sur l'expérimentation, avec des agences capables d'« active defense » mais sous débats sur les droits civiques.
- **Japon :**
législation d'active cyberdéfense permettant des actions proactives sur infrastructures adverses.

En comparaison, l'Europe favorise la protection des droits et la transparence, mais au prix d'une prudence qui réduit sa capacité à contrer rapidement l'IA malveillante.

Propositions : réduire le déséquilibre tout en respectant l'État de droit

1. Mandats IA spécialisés :

autorisations judiciaires encadrées pour certaines opérations IA ciblées, avec durée et périmètre limités.

2. Sandboxes techniques :

environnements sécurisés pour tester des modèles IA en conditions contrôlées, en partenariat public-privé.

3. Centres d'expertise IA-forensics :

analystes, data scientists et juristes formés pour investigations techniques légales.

4. Coopération internationale renforcée :

partage d'indicateurs et outils forensiques en temps réel.

5. Outils de détection partagée :

bases d'IOCs, détection de deepfakes, watermarking vérifiable pour neutraliser les campagnes criminelles.

6. Expérimentations légales pilotes :

infiltration passive de forums ou tests encadrés de détection de fraudes IA pour évaluer l'efficacité avant généralisation.

Ces mesures permettent de réduire l'écart technologique avec les criminels tout en respectant la législation et les principes démocratiques.

CONCLUSION PROSPECTIVE

Même si Le crime organisé maîtrise l'IA — c'est un fait. L'IA ne reconfigure pas encore le crime organisé : elle amplifie surtout la composante frauduleuse, celle qui s'appuie sur des flux officiels, des identités légitimes et des comportements détectables.

Le cœur des trafics, lui, demeure encore fondamentalement humain, relationnel, territorial.

L'Europe et la France doivent répondre de manière proactive, mais encadrée, pour ne pas laisser un avantage stratégique aux contrevenants. La solution réside dans l'adaptation des cadres légaux, le développement de capacités techniques spécialisées et la coopération internationale.

L'Europe peut protéger ses citoyens tout en restant fidèle à ses principes : sécurité, transparence et respect des droits fondamentaux

Le véritable enjeu stratégique pour l'Europe consiste donc à anticiper les usages criminels en testant des solutions encadrées et, à absorber cette criminalité financière augmentée, tout en continuant à surveiller des réseaux analogiques qui échappent entièrement au numérique. Cette double vigilance sera déterminante pour préserver sécurité, état de droit et équilibre démocratique.. ■

FRANCK
ROUXEL

*CISO
Cofondateur
AGORA RSSI CISO
Vice-Président FFCYBER*



DE LA CONTRAINTE RÉGLEMENTAIRE À L'AVANTAGE STRATÉGIQUE : ANTICIPER LA LOI SUR LA RÉSILIENCE COMME LEVIER D'ANTIFRAGILITÉ

La proposition de loi relative à la résilience des infrastructures critiques et au renforcement de la cybersécurité, déposée le 10 septembre 2025, dessine les contours d'une transformation profonde de notre approche de la cybersécurité. Bien qu'encore en discussion parlementaire, ce texte révèle une tendance lourde : comment les organisations peuvent-elles anticiper et transformer ces futures contraintes en véritables leviers de création de valeur ?

DU PÉRIMÈTRE DÉFENSIF À LA RÉSILIENCE SYSTÉMIQUE

Le projet de loi préfigure une rupture conceptuelle : **la résilience comme principe organisateur.**

Les futurs "plans de résilience opérateur" devraient remplacer les plans de protection actuels, intégrant une analyse systémique des dépendances, y compris extra-territoriales. L'obligation envisagée d'analyser "les risques liés à la dépendance envers des fournisseurs propriétaires" offre déjà une grille de lecture : celle de cartographier et maîtriser ses chaînes de valeur numériques.

Cette exigence de transparence technologique, si elle est adoptée, représente une opportunité pour développer **une souveraineté informationnelle pragmatique.**

Les entreprises qui anticipent ces obligations en repensant dès maintenant leurs architectures prennent une longueur d'avance stratégique.



L'ANTIFRAGILITÉ CRÉATRICE : SE PRÉPARER SANS ATTENDRE

Avec des amendes potentielles de 10 millions d'euros ou 2% du chiffre d'affaires mondial envisagées dans le texte, les organisations ont le choix : attendre la promulgation pour une conformité passive, ou anticiper par l'antifragilité créatrice.

Prenons l'obligation pressentie de notification des incidents sous 24 heures. L'organisation antifragile n'attend pas le vote : elle développe dès maintenant des capacités de détection qui dépasseront le cadre réglementaire. Ces systèmes deviennent des **accélérateurs d'apprentissage organisationnel**, transformant chaque incident actuel en préparation aux exigences futures.

Les tests de résilience opérationnelle évoqués dans le projet deviennent, pour les pionniers, des laboratoires d'innovation anticipée. Ces simulations permettent d'expérimenter de nouvelles architectures et de développer une culture de la résilience avant même que la loi ne l'impose.

LA DONNÉE VIVANTE : PRÉPARER LA CONFORMITÉ DYNAMIQUE

Le projet introduit **le concept de conformité évolutive** : des référentiels qui s'adapteront aux menaces émergentes. Cette approche pressentie résonne avec le paradigme de la donnée vivante - une information qui évolue et maintient sa pertinence dans des contextes changeants.

Les organisations visionnaires développent dès aujourd'hui des systèmes de conformité auto-adaptatifs :

- **Des pipelines** conçus pour ajuster leurs paramètres selon les futures évolutions réglementaires
- **Des architectures** anticipant les changements normatifs à venir
- **Des processus** apprenant déjà des incidents pour renforcer leur conformité future

Cette approche proactive transforme la réglementation annoncée : de contrainte future, elle devient dès maintenant un guide pour l'excellence opérationnelle.

CRÉATION DE VALEUR ANTICIPÉE

L'impact économique de cette préparation dépasse le simple évitement de futures sanctions :

VALEUR OPÉRATIONNELLE IMMÉDIATE :

Les capacités développées en anticipation améliorent déjà l'efficacité. Les analyses de dépendances optimisent les chaînes d'approvisionnement actuelles.

VALEUR COMMERCIALE DIFFÉRENCIANTE :

Anticiper la conformité devient un argument commercial. Les organisations proactives rassurent leurs clients sur leur capacité d'adaptation.

VALEUR STRATÉGIQUE D'ANTICIPATION :

Comprendre les orientations réglementaires permet des décisions d'investissement éclairées et une navigation agile dans l'incertitude législative.

VALEUR ÉCOSYSTÉMIQUE PRÉCOCE :

Les mécanismes de partage envisagés incitent à créer dès maintenant des réseaux de résilience collaborative.

DU CISO AU CHIEF RESILIENCE OFFICER : UNE ÉVOLUTION À ANTICIPER

Cette proposition de loi accélère une mutation déjà perceptible : celle du RSSI vers le Chief Resilience Officer. Les organisations clairvoyantes n'attendent pas la promulgation pour faire évoluer cette fonction.

Le futur CRO devra orchestrer une symphonie complexe mêlant enjeux techniques, organisationnels, réglementaires et géopolitiques. Les entreprises qui recrutent et forment dès maintenant ces talents hybrides prennent une avance décisive sur leurs concurrents qui attendront la contrainte légale. ■

CONCLUSION : L'ANTICIPATION COMME AVANTAGE COMPÉTITIF

Cette proposition de loi ne doit pas être vue comme une épée de Damoclès mais comme une boussole stratégique. Les organisations antifragiles n'attendent pas le vote final : elles transforment dès aujourd'hui chaque orientation pressentie en levier d'innovation.

Dans ce "numérique de l'incertitude", la capacité à anticiper et transformer les futures contraintes réglementaires en avantages immédiats devient la marque distinctive des organisations véritablement antifragiles. L'heure n'est pas à l'attentisme mais à l'antifragilité créatrice qui transforme chaque signal réglementaire en opportunité d'évolution - car c'est dans cette anticipation que réside l'essence même de la résilience stratégique.



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

LE RENDEZ-VOUS INCONTOURNABLE DES EXPERTS DE LA CYBERSÉCURITÉ

220 exposants spécialisés

Editeurs de solutions, startups innovantes, banques, assurances, etc.

Des conférences sur mesure

- L'impact des réglementations européennes sur les acteurs publics et privés français : vers une mise en conformité différenciée ?
- Chaînes industrielles délocalisées, sécurités dispersées : où commence votre périmètre cyber ?



Challenge capture the flag

Venez tester vos compétences, affronter d'autres challengers et décrocher votre place parmi les meilleurs.

Nouveauté : verticale spatial

Jeudi 27 novembre, une édition satellite du CYSAT

Remise de prix Cyberstars

**TÉLÉCHARGEZ GRATUITEMENT
VOTRE BADGE VISITEUR
CBC-CONVENTION.COM**



Suivez-nous [in](#) @CBC - Cybersecurity Business Convention

ÉDITION

#5

**OPEN SOURCEZ
VOS SOLUTIONS IT**

**OPEN
SOURCE
EXPERIENCE**

PARIS

**10 & 11
DÉCEMBRE 2025**

NOUVEAU LIEU
- CITÉ DES SCIENCES
ET DE L'INDUSTRIE

90 EXPOSANTS 130 CONFÉRENCES 150 SPEAKERS

Inscription gratuite à partir de septembre sur
www.opensource-experience.com

Suivez-nous



#OSXP2025

Un événement



organisé par



Aux mêmes dates
et lieu que



DEVOPS REX
LA CONFÉRENCE DEVOPS
FRANCOPHONE

100% retour d'expérience



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





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

nēosoft

 cabinet-gtec.fr

 contact@cabinet-gtec.fr

**Prenez
RDV**





ODILE
DUTHIL

*Directrice Cybersécurité,
Groupe Caisse
des Dépôts, et
Présidente Clusif*

L'ASSOCIATION CLUSIF : LA CONFIANCE NUMÉRIQUE

■ ■ **GS MAG :** *Odile DUTHIL, bonjour. Global Security Mag est ravi d'avoir cet entretien avec vous. Pouvez-vous vous présenter et nous dire comment votre parcours professionnel vous a amenée à votre rôle actuel au sein de la Caisse des Dépôts et à la Présidence Clusif ?*

■ ■ **OD :** Je suis Ingénieure en télécommunications. Diplômée d'une école qui s'appelle l'ENSEA (École Nationale Supérieure de l'Électronique et de ses Applications). Et à la sortie de mon diplôme d'ingénieur, j'ai intégré une entreprise qui à l'époque s'appelait France Télécom, en tant qu'experte sur la partie radio, c'est-à-dire, ce qui se passe entre le mobile et le réseau. J'ai mené ma carrière au sein de cette Société qui était devenue Orange, pendant vingt-cinq ans. J'ai travaillé sur beaucoup de systèmes, à la fois dans la partie réseau, mobile et fixe, 2G, 3G, 4G, 5G, des plateformes de services avec notamment la plateforme télé Orange TV (le nom actuel).

Et j'ai aussi œuvré dans une partie des Systèmes d'Information. J'ai donc un parcours technique, et j'ai progressé dans l'entreprise jusqu'à devenir Manager de Managers. Je suis arrivée à la Cybersécurité par la sécurité des réseaux, qui est aussi une matière connexe à la Cybersécurité, car elle en reprend aussi les fondamentaux. J'ai travaillé beaucoup avec l'État. Au bout de vingt-cinq ans, j'ai eu l'opportunité de changer de domaine parce que je voulais évoluer vers la partie Cybersécurité, mais pas forcément rester dans le domaine des télécommunications. J'avais une appétence pour le domaine bancaire, alors, j'ai postulé il y a un peu plus de cinq ans, en 2020, à la Caisse des Dépôts pour être Adjointe du Directeur Cybersécurité. Et j'occupe maintenant le poste de Directrice Cybersécurité depuis avril 2024.

>>>

>>> La filière Cybersécurité à la Caisse des Dépôts représente une équipe d'environ soixante-dix personnes qui se répartissent sur le SOC (Security Operations Center ou Centre des Opérations de Sécurité) et le CERT (Computer Emergency Response Team ou Centre d'Alerte et de Réaction aux Attaques), donc dans la partie opérationnelle, et qui sont rattachées à la DSI.

Moi j'ai une équipe d'une trentaine de personnes, à la fois pour la partie Gouvernance, donc une équipe de RSSI qui accompagnent les Directions métiers, et une partie d'experts Cybersécurité qui travaillent sur la fuite de données, la gestion des habilitations, l'IAM (Identity and Access Management ou la Gestion des Identités et des Accès), tout ce qui est utilisation des outils de Cybersécurité. Il y a une troisième équipe qui travaille sur la partie fraude, cartographie des risques, la veille et la gestion de crise, puisqu'on s'est réorganisé à l'aune de la réglementation DORA. Mon rôle à la Caisse des Dépôts, c'est la maîtrise des risques SI (Systèmes d'Information) et SSI (Sécurité des Systèmes d'Information).

Voilà pour la partie parcours professionnel. Concernant mon parcours associatif, je suis au Conseil d'Administration du Clusif (l'Association Reconnue d'Utilité Publique, et de référence pour la Sécurité de l'Information et du Numérique) depuis un peu plus de deux ans. Je suis aussi membre du CESIN (Le Club des Experts de la Sécurité de l'Information et du Numérique) en tant que RSSI. J'ai été très active. Par exemple, avec une Avocate spécialisée dans le Numérique et la Cybersécurité (Garance MATHIAS) qui est aussi au Conseil d'Administration du Clusif, nous avons porté le Groupe de Travail DORA du Clusif. J'ai monté l'Espace Sécurité Offensive du Clusif avec une personne (Hocine MAHTOUT) qui est dans mon équipe à la Caisse des Dépôts.

J'avais donc déjà une implication forte, et quand s'est présentée l'opportunité de candidater pour la présidence, cela m'a semblé naturel.



**L'Association a obtenu
le statut de la Reconnaissance
d'Utilité Publique (RUP)
depuis novembre 2024.**

■ ■ **GS MAG :** *Alors justement nous allons nous concentrer sur le Clusif. Vous venez d'être élue, félicitations. Quelles sont vos ambitions et quelles sont les perspectives que vous avez pour le Clusif ?*

■ ■ **OD :** Pour l'Association Clusif, la ligne directrice est de porter la Confiance Numérique. C'est le fait de pouvoir travailler en confiance et que pour chaque entreprise, on préserve l'intégrité de ses données, l'intégrité de ses activités, pour elle et pour ses utilisateurs, pour ses clients. C'est quelque chose d'important. Dans nos membres, nous avons deux collèges, un collège acteurs et un collège utilisateurs. Nous avons donc ce creuset au Clusif, entre des sociétés qui proposent des solutions et d'autres qui les utilisent. Mais le Clusif n'est pas un lobby. Nous ne défendons pas d'intérêt particulier, car nous sommes au service de l'intérêt général, surtout en tant qu'Association Reconnue d'Utilité Publique.

Le Clusif a pour mission de fournir des grilles de lecture pour décoder les meilleures solutions, les meilleures problématiques, les bonnes pratiques à mettre en œuvre pour l'écosystème en Cybersécurité. Notre ambition est dans le fait que nous représentons une Association de professionnels et nous nous adressons à des professionnels, pour faire monter en compétence, en maturité, l'écosystème Cyber. C'est la ligne directrice. Alors pour ce faire, la confiance Numérique, ce n'est pas uniquement Paris, mais c'est partout.

C'est ainsi que nous avons un réseau de Clusir (entités régionales), qui sont des partenaires avec lesquels nous travaillons, et qui sont des Associations locales ou régionales. Nous en avons certaines à l'international, la Suisse et l'Italie au moins. Et l'idée, c'est d'avoir un travail en commun, un partage de connaissances, une articulation, de renforcer ce travail ensemble au niveau Paris et Régions. C'est important parce qu'il y a aussi une vraie dynamique régionale qu'il est intéressant d'accompagner. L'Association a obtenu le statut de la Reconnaissance d'Utilité Publique (RUP) depuis novembre 2024. C'est extrêmement important, et nous sommes très fiers d'avoir ainsi une place très particulière dans l'écosystème Cyber, car nous représentons la seule Association ayant ce statut. La RUP, c'est un certain nombre de cadres et d'obligations, bien sûr, mais cela nous donne aussi des possibilités. Ce sont ces opportunités que j'aimerais aussi développer au travers d'appels à projets et en s'appuyant sur le mécénat de compétences, comme ce statut nous le permet.

Concrètement, cela veut dire que nous pouvons faire des appels à projets et que des personnes qui sont, par exemple, dans une société de Consultants, adhérente au Clusif, peuvent donner du temps, pro bono, à titre gracieux, pour mener une partie des projets et être des acteurs. C'est gagnant-gagnant. Parce que pour le collaborateur qui, en général, a beaucoup d'expérience, cela lui donne une opportunité de faire quelque chose pas forcément avec une rentabilité financière et cela est gagnant pour les projets, puisque c'est financé. Voilà les grands axes de cette nouvelle mandature.

■ ■ **GS MAG : Nous sommes en pleine Assises de la cybersécurité. Quel message clé vous auriez à donner aux RSSI, CISO, DPO, Responsables cyber, Responsables Cybersécurité pour rejoindre le Clusif ?**

■ ■ **OD :** Cette année, j'ai eu la chance d'être coprésidente des assises pour la vingt-cinquième édition, 2025. Nous avons voulu, avec Lois Samain, donner la ligne directrice FuturS. Se tourner vers le futur dans tous nos défis. Il s'agit de la Cybersécurité au service des métiers et de la création de valeur.

C'est-à-dire que maintenant, le ou la RSSI est finalement à la croisée des chemins entre des ruptures technologiques, je pense à l'IA, au quantique, au Cloud, aux nouvelles réglementations, je pense à NIS 2, DORA, CRA, dans un contexte juridique déterminé, et avec des problématiques de Souveraineté Numérique, puisque nous évoluons dans un monde géopolitique pour le moins chamboulé. Nous sommes au cœur de ces problématiques, Et c'est aussi quelque chose qu'on trouve aux Assises, évidemment. Ce sont des thématiques qui sont abordées parce qu'on a voulu les mettre en exergue. Ce sont aussi des choses sur lesquelles nous travaillons au Clusif et qu'on peut trouver, encore une fois avec cet aspect un peu unique, qui est de travailler sur des dossiers entre des acteurs et des utilisateurs.

Au Clusif, nous organisons aussi des conférences thématiques. Par exemple, une Conférence sur le post-quantique, le chiffrement post-quantique, et le 23 octobre, une Conférence très intéressante dans ce contexte géopolitique, sur la Confiance Numérique. Nous établissons au Clusif, beaucoup de livrables, beaucoup de publications. Les adhérents forment des Groupes de Travail et œuvrent sur différentes problématiques. Lors de cette 25^{ème} édition des Assises, nous revenons sur la Cybersécurité dans le monde industriel, puisqu'il y a des thématiques qui sont un peu spécifiques. Mais nous avons aussi des livrables sur DORA, sur la Souveraineté Numérique.

Nous avons mis en place un modèle de PSSI (Politique de Sécurité des Systèmes d'information) sur l'IA. Nous pouvons travailler sur des thématiques en commun. Et nous avons également des Espaces spécifiques qui fonctionnent très bien. **Pour l'Espace RSSI, où on est en petit comité, avec des règles de Chatham House, ce qui permet de discuter sur des sujets de fond, sur des problématiques rencontrées, et partager entre responsables de la sécurité numérique.** Nous avons aussi l'Espace consacré à Sécurité Offensive, où on parle plutôt de tests techniques et en particulier des méthodes où on se met à la place de l'attaquant, en utilisant les mêmes moyens pour tester la robustesse de nos systèmes d'information. Ce sont des méthodes un peu novatrices et sur lesquelles il est toujours intéressant d'échanger, mais qui s'adressent effectivement à une population peut-être un peu plus technique dans la matière Cybersécurité. Voilà, en résumé ce qu'on trouve au Clusif.

L'Association Clusif, une référence dans la Sécurité de l'Information et du Numérique, est un lieu avec un esprit d'échange, de partage. Un endroit où on se parle beaucoup, on se challenge, on confronte les idées et je pense que c'est cela qui fait progresser. Nous y partageons évidemment les bonnes pratiques. ■

L'Association Clusif est un lieu avec un esprit d'échange, de partage. Un endroit où on se parle beaucoup, on se challenge, on confronte les idées et je pense que c'est cela qui fait progresser. Nous y partageons évidemment les bonnes pratiques.

Cyber/IA expo

3 FÉVRIER 2026

PALAIS DES CONGRÈS - PARIS

Cyber-IA expo est organisé par **Beyond Event**
avec **Les Assises de la cybersécurité** et les **RIAMS**.

contact@ia-cyber.com

ia-cyber.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



EMMANUEL
GARNIER

*Président Club 27001 et
Directeur Cybersécurité
Orano*

ISO/IEC 27001 FÊTE SES 20 ANS : UNE NORME, UNE COMMUNAUTÉ, UNE VISION

LE 16 OCTOBRE 2025, LA NORME ISO/IEC 27001 A CÉLÉBRÉ SES 20 ANS. À CETTE OCCASION, LE CLUB27001 A ORGANISÉ UN ÉVÉNEMENT NATIONAL SIMULTANÉ DANS SES GROUPES RÉGIONAUX : PARIS, LYON, NANTES, RENNES ET TOULOUSE.

**Plus de
270 participants**

— adhérents, animateurs,
contributeurs et membres du comité
d'administration — se sont réunis
pour marquer ce jalon
majeur de la cybersécurité.

**Le 16 octobre 2025, la norme ISO/IEC
27001 a célébré ses 20 ans.**

À cette occasion, le Club27001 a organisé un événement national simultané dans ses groupes régionaux : Paris, Lyon, Nantes, Rennes et Toulouse. Plus de 270 participants — adhérents, animateurs, contributeurs et membres du comité d'administration — se sont réunis pour marquer ce jalon majeur de la cybersécurité.

UNE NORME EN CONSTANTE ÉVOLUTION

Publiée pour la première fois en 2005, la norme ISO/IEC 27001 a connu trois versions successives. Loin d'être figée, elle s'est imposée comme un langage commun et un standard incontournable pour la gestion de la sécurité de l'information (SMSI). Son adoption croissante témoigne de son utilité : selon une étude de l'AFNOR publiée le jour de l'anniversaire, le nombre de certifiés est passé de 200 en 2008 à plus de 1 000 en 2023.

LE CLUB27001 : UNE AVENTURE HUMAINE

Fondé sur les bases de la British Standard BS7799, le Club27001 est devenu une association en 2008. Dès ses débuts, il a été animé par des figures emblématiques comme Hervé Schauer et Éric Doyen, qui ont contribué à diffuser la culture de la norme en France. Le Club repose sur un modèle unique : des binômes d'animateurs — souvent un RSSI et un consultant ou auditeur — qui incarnent son ADN. Et ce, toujours sans sponsor, par choix.

Aujourd'hui, le Club compte près de 600 adhérents, majoritairement individuels, répartis dans plusieurs groupes régionaux :

- Paris : ~200 membres

- Nantes : ~130 membres
- Rennes : >100 membres
- Lyon : ~90 membres
- Toulouse : >80 membres
- Marseille : en cours de relance

Le Club s'est aussi ouvert à l'international, avec des membres en Belgique, Suisse, Luxembourg et Canada.

DES INITIATIVES CONCRÈTES

Outre ses réunions régionales, le Club organise une conférence annuelle, adossée aux GS Days, et anime plusieurs groupes de travail :

- Un livre blanc sur les outils de gestion des SMSI
- Un GT sur les réglementations (ex. NIS 2)
- Un GT sur les bonnes pratiques terrain (ISO 27002)
- Un GT sur les processus issus d'autres normes

ENTRETIEN AVEC LE PRÉSIDENT DU CLUB27001 :

« La norme ISO 27001, c'est une aventure humaine avant tout »

À l'occasion de cet anniversaire, nous avons rencontré le président du Club27001, engagé depuis les débuts de l'association. Il revient sur son parcours, les évolutions du Club et sa vision pour l'avenir de la cybersécurité.

■ ■ GS MAG : *Vous souvenez-vous de vos premières rencontres avec le Club27001 ?*

Oui, très bien. Les premières réunions étaient animées par des pionniers comme Hervé Schauer — dont les sociétés ont formé de nombreux professionnels à la norme — et Éric Doyen, toujours présent dans le conseil d'administration depuis l'origine. Il a été président pendant de nombreuses années, et aujourd'hui vice-président. À l'époque, ces réunions n'avaient pas de statut officiel, et il n'était pas toujours simple d'y participer, surtout pour certaines catégories de professionnels. Il fallait parfois justifier une demi-journée d'absence, ce qui n'était pas évident.

■ ■ GS MAG : *Comment avez-vous évolué au sein du Club ?*

J'ai été vice-président pendant huit ans, puis président depuis bientôt onze ans. Je garde un excellent souvenir de notre première conférence

ISO 27001 d'une journée à La Défense, dans le cadre d'un événement cyber qui n'existe plus aujourd'hui. C'était une étape importante.

■ ■ GS MAG : *Vous avez aussi mené des projets de certification ?*

Oui, j'ai été convaincu très tôt par l'intérêt d'une norme internationale en cybersécurité. En 2009, après un projet de 18 mois, mon GIE de l'époque a été certifié ISO 27001 par LSTI. Nous avons renouvelé la certification deux fois, et elle a été maintenue jusqu'à la fin du GIE en 2014.

■ ■ GS MAG : *Un souvenir marquant à partager ?*

J'ai récemment réécouté notre passage dans le podcast NoLimitSecu, enregistré en février 2016. On y retrouve Hervé Schauer, Éric Doyen, Carl Roller — notre trésorier fidèle depuis des années — et moi-même. C'est un beau moment d'échange et de transmission.

■ ■ GS MAG : *comment décririez-vous l'esprit du Club ?*

C'est avant tout du bénévolat et de l'investissement. Les administrateurs sont le cœur, les animateurs les poumons, les contributeurs des groupes de travail les muscles, et les membres qui partagent leurs retours d'expérience sont le sang. Une belle analogie proposée par notre secrétaire, Étienne Gérain.

■ ■ GS MAG : *Et pour les 20 prochaines années ?*

Ce 16 octobre 2025, nous avons organisé un événement national unique, qui a rassemblé plus d'acteurs de la norme que jamais auparavant en France. Je serai probablement en fin de carrière pour les 40 ans de la norme, mais j'espère être invité ! Je pense que les prochaines années s'écritront moins en termes de conformité et d'exigence. Et si la véritable maturité consistait à faire de la cybersécurité un réflexe de confiance et un moteur d'innovation ?



PATRICK
FOUBERT

Club 27001



MICKAËL
FERTON

LIVRE BLANC NIS 2 DU CLUB 27001

CONVERGENCES ET ENJEUX DE CONFORMITÉ ENTRE NIS 2 ET ISO 27001

**À L'APPROCHE DE LA
TRANSPOSITION EN FRANCE
DE LA DIRECTIVE EUROPÉENNE
NIS 2, LE CLUB 27001 PUBLIE
UN LIVRE BLANC POUR GUIDER
LES ENTITÉS ESSENTIELLES,
IMPORTANTES ET SOUS-
TRAITANTES CRITIQUES**

UNE DIRECTIVE EXIGEANTE, UNE RÉPONSE PRAGMATIQUE

Cette première version est le fruit d'un travail collaboratif d'experts issus de l'industrie, du juridique, des services et de la cybersécurité, ce document introduit la directive en la croisant avec les normes ISO/IEC 27001 et 27002.

UN GUIDE CONÇU POUR RATIONALISER LES EFFORTS

Le livre blanc rappelle que la certification ISO 27001, bien que structurante, ne suffit pas à elle seule : NIS 2 impose des exigences plus fortes sur certains aspects (notification d'incidents, responsabilité du dirigeant, sanctions jusqu'à 10 M€ ou 2 % du CA mondial, contrôle renforcé de la chaîne d'approvisionnement, etc). Cependant, les entités déjà certifiées couvrent près de 80 % des mesures attendues, selon l'analyse croisée du Club.

Cette première version est le fruit d'un travail collaboratif d'experts issus de l'industrie, du juridique, des services et de la cybersécurité, ce document introduit la directive en la croisant avec les normes ISO/IEC 27001 et 27002.

UNE INTELLIGENCE COLLECTIVE AU SERVICE DE LA CYBERSÉCURITÉ

Au-delà du contenu, ce projet illustre l'intelligence collective du Club 27001, qui a réuni RSSI, auditeurs, juristes et praticiens autour d'un objectif commun : proposer un guide vivant, pragmatique et utile pour anticiper la directive et renforcer la résilience numérique des organisations. Les membres du Groupe de Travail NIS 2 du Club27001 travaillent d'ailleurs déjà sur une version 2 de ce livre blanc, au travers de fiches considérant les différentes exigences de la transposition française.

VERS UNE CYBERSÉCURITÉ EUROPÉENNE PLUS MATURE

Chaque fiche de la version 2 du livre blanc NIS 2 du Club 27001 sera conçue comme un outil opérationnel et non un simple résumé réglementaire.

Son objectif : rendre la directive actionnable pour les RSSI, DSI et dirigeants, en traduisant chaque exigence en mesures concrètes et vérifiables.

Toutes les fiches suivront une structure commune :

- le principe NIS 2 concerné et ses références ISO/IEC 27001-27002,
- les mesures de mise en œuvre et leur niveau de complexité,
- les éléments de preuve attendus lors d'un audit,
- enfin, l'avis du Club 27001, qui éclaire la valeur ajoutée d'une approche certifiée ISO 27001.

Cette architecture permet une lecture "Lead Implementer" et "Lead Auditor", conciliant opérationnel et conformité.

Elle illustre la vision collective et pragmatique du Club : croiser les expertises — techniques, juridiques, managériales — pour construire un langage commun entre réglementation et terrain.

Un travail collaboratif au service d'une cybersécurité européenne plus mature et partagée.

Cette première version du livre blanc est disponible au téléchargement (réservée aux adhérents).

Vous souhaitez faire part de vos remarques ? Vous souhaitez rejoindre l'un de nos groupes de travail ? Consultez le site internet du Club 27001 (www.club-27001.fr), rubrique « Groupes de travail ».



RETEX NIS 2, DORA, CRA, ISO 27001, RGPD, LA CONFORMITÉ ET CYBERSÉCURITÉ

> SELON VOUS, QUELS SONT LES DÉFIS LORSQU'IL S'AGIT D'ASSOCIER LA CONFORMITÉ À LA CYBERSÉCURITÉ ?

Le principal enjeu réside, selon moi, dans la capacité à aligner les approches : deux langages, deux rythmes.

La conformité repose souvent sur des référentiels juridiques, normatifs ou réglementaires (DORA, ISO 27001, NIS2, DORA, RGPD par exemple), tandis que la cybersécurité se traduit plutôt par des mesures techniques et opérationnelles.

La temporalité n'est pas la même non plus, les audits sont d'avantages périodiques alors que la menace cyber est continue.

Faire converger ces deux logiques exige donc une capacité à faire communiquer deux écosystèmes qui ne s'imbriquent pas naturellement - c'est là que les consultant(e)s ont toute leur valeur.

Pourtant, ces approches se nourrissent mutuellement, et c'est ce qui leur donne toute leur cohérence. On peut les comparer à un gouvernail et un moteur : l'un ne sert à rien sans l'autre. L'un donne la direction, l'autre la propulsion.

Sans conformité, la cybersécurité manque de cadre ; sans cybersécurité, la conformité perd en impact.

Rappeler les valeurs métier et les enjeux business de l'organisation est par exemple une bonne manière de recentrer le débat : cela permet de rassembler les deux écosystèmes autour d'un objectif commun, celui de départ.

> COMMENT LES SOLUTIONS DE VOTRE ENTREPRISE PERMETTENT-ELLES AUX ORGANISATIONS D'ATTEINDRE UNE POSTURE DE CONFORMITÉ ET CYBERSÉCURITÉ, LA MEILLEURE POSSIBLE ?

Davidson Consulting, et plus largement tout organisme de conseil, permet d'apporter un regard externe sur la conformité et la cybersécurité au sein des organisations.

C'est un regard nourri par la multiplicité des secteurs d'intervention clients et par le travail réalisé pour acquérir et développer la compétence.

Pour parler de nous, nous aidons les organisations à cartographier leurs obligations et à traduire les textes (NIS2, DORA, RGPD, CRA, Cyber Act, etc.) afin de connaître les périmètres d'applicabilité et les exigences opérationnelles qui en découlent. Cela passe par des diagnostics de maturité, des analyses d'écart et la définition d'une feuille de route claire entre les obligations réglementaires et la réalité du terrain.

Nous accompagnons également la mise en conformité technique et organisationnelle : modification des politiques de sécurité, renforcement des processus IAM/PAM, accompagnement segmentation et micro-segmentation, durcissement des environnements critiques, gestion des incidents cyber, etc.

Enfin, nous déployons des mécanismes de supervision et de pilotage pour transformer la conformité en démarche continue : tableaux de bord consolidés, suivi des indicateurs de sécurité, finalement une bonne démarche SMSI.

Notre force tient surtout à la transversalité de nos équipes : des experts GRC, des chefs de projet, des architectes sécurité et des analystes SOC/CSIRT qui interviennent directement auprès de nos clients mais tous reliés par Davidson.

> QUELLES SONT LES ÉVOLUTIONS PRÉVUES POUR VOS SOLUTIONS ?

Depuis la création de Davidson en 2005, nous avons toujours privilégié une approche agnostique pour accompagner nos clients pour l'étude et le choix de leurs solutions, au plus près de leurs besoins, sans parti pris et en toute indépendance.

En parallèle, notre démarche R&D nous a permis de tester et de rester connectés aux technologies émergentes, afin d'identifier celles qui apportent — ou apporteront dans un futur proche — une réelle valeur à nos clients.

L'année 2025 marque un tournant stratégique pour Davidson : nous renforçons nos investissements dans les partenariats.

Nous croyons notamment beaucoup à l'analyse de risque quantitative ET dynamique. Basée sur l'identi-

Lucas Perez (Davidson consulting)
highlights the challenge of aligning compliance (legal frameworks like NIS2, CRA, DORA, GDPR, ISO 27001...) with continuous cybersecurity. Davidson bridges this gap by mapping obligations, conducting maturity audits, and implementing technical safeguards (IAM, incident response). Their holistic approach—combining GRC experts, SOC analysts, and security architects—ensures ongoing compliance and risk management. In 2025, they focus on dynamic risk analysis, sovereign solutions, and AI-driven detection to enhance organizational resilience.

fication en temps réel et automatique des actifs, cette solution couplée à l'analyse statistique (simulations Monte Carlo + FAIR), renouvelle en profondeur l'évaluation de la sécurité et la lecture financière du risque.

Nous poursuivons également des travaux sur les solutions souveraines, managées ou non, convaincus que la souveraineté numérique sera l'un des leviers clés de la résilience des organisations dans les années à venir.

Et bien sûr, l'IA — difficile de ne pas en parler — fait également partie de nos travaux R&D, avec un focus sur un RAG interne et des cas d'usage autour de la donnée et des mécanismes de détection.



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)



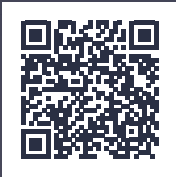
Le meilleur de la cyber-résilience.

ARTESCA  **Veeam**
UNIFIED SOFTWARE APPLIANCE

Backup + stockage objet.
Dans une seule appliance.

Zero Trust.

Zéro compromis.



scality.com/fr



JÉRÔME LECAT, CEO, SCALITY, A ACCORDÉ UN ENTRETIEN À GLOBAL SECURITY MAG, LORS DE LA 10^E ÉDITION DU SCALITY DAY, ET DE L'ANNIVERSAIRE DES 15 ANNÉES DE SCALITY.

“ Une chose qui a été dite par plusieurs de nos clients sur scène aujourd'hui, c'est qu'en fait, quand on choisit une solution, il y a la technique, mais il y a surtout la relation avec le fournisseur. ”

“ Nos clients plébiscitent Scality dans la relation et sont prêts à recommander Scality autour d'eux. ”



> JÉRÔME LECAT, BONJOUR. GLOBAL SECURITY MAG EST RAVI DE VOUS AVOIR EN ENTRETIEN. NOUS SOMMES EN PLEIN SCALITY DAY ET LE RYTHME DE L'INNOVATION DE SCALITY EST ASSEZ IMPRESSIONNANT. POUVEZ-VOUS NOUS PARLER DES ACCORDS DE PARTENARIAT QUE VOUS AVEZ EUS AVEC LE KAZAKHSTAN ? QUEL EST LE CONTEXTE ET QUELS SONT LES ENJEUX ?

Alors effectivement, c'est le dixième Scality Day et cette année, on a décidé de faire un événement international à Paris. Cinq cents personnes enregistrées, plus de trois cents personnes qui sont venues de vingt pays différents, de la Hollande à l'Arabie Saoudite, des États-Unis au Sri-Lanka, de l'Inde, de l'Azerbaïdjan au Kazakhstan, bref, un peu de partout dans le monde. Tout d'abord, nous sommes super contents de pou-

voir fêter les dix ans de Scality Day, en même temps que les quinze ans de Scality, avec nos clients et nos partenaires du monde entier. Nous avons trois pays où nous nous développons beaucoup cette année : l'Arabie Saoudite, l'Inde et le Kazakhstan. Et on a choisi de mettre en valeur le Kazakhstan cette année au Scality Day, parce qu'en allant là-bas, j'ai été vraiment fasciné par le dynamisme de ce pays, la volonté d'aller de l'avant. Ils viennent de, d'ouvrir leur premier super computer pour l'Intelligence Artificielle, cette semaine par le Président Tokaïev. Et c'est vraiment un pays qui a une dynamique incroyable et qu'en fait, on connaît très mal en Europe.

Je pense que la plupart de vos lecteurs et lectrices ne savent même pas placer le Kazakhstan sur une carte, alors que le Kazakhstan, c'est un pays qui, en superficie, est presque aussi grand que l'Inde. En ce qui concerne la nature du partenariat, tout d'abord, nous avons une dizaine de clients déjà existants au Kazakhstan. Une équipe de Scality là-bas et c'est vraiment notre base de développement pour l'Asie centrale. Nous avons aussi des clients dans d'autres pays d'Asie centrale, mais notre base de développement, c'est le Kazakhstan. Nous avons été impressionnés par l'accueil qui nous a été réservé, notamment par Asset ISSEKESHEV (Chairman of the Board of Trustees Qaztech Alliance) et son organisation Qaztech Alliance of Technology Companies, Scality est membre, et qui est peut-être un mélange comme ce que serait la French Tech en France ou France Digitale. C'est, en résumé, une Organisation qui œuvre pour la promotion du digital au sein du Kazakhstan.

> SCALITY FAIT DES ALLIANCES ET IL Y A NOTAMMENT UNE ALLIANCE RÉCENTE AVEC L'INRIA (INSTITUT NATIONAL DE RECHERCHES EN SCIENCES ET TECHNOLOGIES DU NUMÉRIQUE) DANS LE CADRE DE FRANCE 2030. NOUS PARLONS BEAUCOUP EN CE MOMENT DE LA SOUVERAINETÉ NUMÉRIQUE. SCALITY A DONC FAIT UNE ALLIANCE AVEC L'INRIA, POUR STOCKER DES DONNÉES DE MANIÈRE SÛRE ET ÉCO-RESPONSABLE. POUVEZ-VOUS NOUS EN PARLER ?

Effectivement, la Souveraineté est un sujet qui est très important pour nos clients dans le monde entier. Il ne faudrait pas croire que la souveraineté, c'est juste un concept français. Nos clients, ce sont des Grandes

Entreprises et Organisations, ce sont des Opérateurs de Cloud, ce sont des Gouvernements.

Nous avons des contrats avec des Gouvernements dans trente-cinq pays. Et s'ils font des contrats avec nous pour déployer des infrastructures qu'ils contrôlent, c'est bien pour des problématiques de Souveraineté, et aussi de performance et de coût, mais avant tout, de Souveraineté. Ce qu'on fait avec l'Inria, c'est effectivement un projet France 2030. Le projet s'appelle CyberT.

Nous avons trois projets avec l'Inria. Pour l'un, il s'agit d'utiliser de l'Intelligence Artificielle pour faire de la maintenance prédictive. En fait, quand on regarde les cas qui font que nos systèmes ne fonctionnent plus, ne servent plus de données ou n'écrivent plus de données, et quand c'est un humain qui regarde, on se dit qu'on aurait pu prédire le phénomène quelques jours avant. Et on se dit qu'avec ce qui existe aujourd'hui en IA, une IA devrait pouvoir prédire cela. Mais c'est un problème éminemment complexe.

Nos systèmes remontent des milliers, littéralement des milliers d'informations par seconde. Et ce n'est pas évident de faire un système d'IA qui va regarder des milliers d'informations par seconde. On fait des « snapshots » ou photos instantanées, on regarde des informations à l'échelle de cinq minutes, parce qu'on pense que c'est suffisant. Mais on est en train de travailler avec l'Inria, un projet de recherche multi-années, pour être capable de concevoir un système qui fait ça. Et nous avons montré sur scène la première version de ce système qui va être déployé dès le premier trimestre 2026. C'est un premier projet.

Le deuxième projet, toujours en utilisant de l'IA, est de se demander si on ne pourrait pas, en regardant les patterns (schémas) d'accès et les patterns réseau sur nos systèmes, détecter des attaques avant même qu'elles soient nocives. C'est un domaine de recherche beaucoup plus fondamental. Autant la maintenance prédictive, nous savons tous que ça va marcher parce que ça marche dans d'autres industries, ça marche dans les avions, ça marche dans les gros systèmes industriels et nous sommes assez similaires à cela.

Autant, arriver à détecter des attaques sur des patterns sans savoir ce qu'on cherche, c'est un problème beaucoup plus compliqué. Nous travaillons dessus avec une équipe de l'Inria qui s'appelle PIRAT (Protection de l'Information et Résistance aux Attaques) qui a des très bonnes idées.

Nous sommes entrain de tester ça sur nos systèmes en faisant des simulations, en partenariat aussi avec nos clients, pour être capables de faire de la détection en avance des attaques. Et puis la troisième chose, >>>

>>> c'est avec une équipe qui a développé une API (Application Program Interface ou Interface de Programmation d'Applications) qui s'appelle Power API. Et l'idée, c'est d'être capable de mesurer en temps réel la consommation énergétique des serveurs qui sont déployés avec nos logiciels. Et le but, c'est de pouvoir facilement faire un bilan carbone sur des systèmes Scality.

Cela nous sert à optimiser les systèmes d'un point de vue bilan carbone et à être capables de faire des recommandations à nos clients. Et cela permet à nos clients de sortir des bilans carbone plus précis et plus rapidement avec moins de travail.

> QUELLE EST LA VISION SUR LES PROCHAINES ALLIANCES STRATÉGIQUES DE SCALITY ?

Nous continuons à développer, je dirais, à intensifier des choses qu'on fait déjà depuis plusieurs années. D'abord, Scality offre du logiciel qui est toujours déployé sur des serveurs. On travaille énormément avec trois constructeurs de serveurs qui étaient là aujourd'hui tous les trois : HPE, Lenovo et Supermicro. Nous avons fait de très gros déploiements. Je parle de plusieurs centaines de pétaoctets avec chacun d'entre eux. Et les clients sont venus et ont témoigné sur scène. Vous avez pu voir Iron Mountain et Core42 qui ont présenté à tour de rôle le déploiement de plus d'une centaine de pétaoctets. C'est un type d'alliance qui est très important parce qu'on optimise en fait l'interaction entre notre software et leurs serveurs. Le deuxième type d'alliance, c'est tout ce qui concerne la Cybersécurité, avec en particulier, et ils sont aussi présents aujourd'hui, deux logiciels de backup qui sont Veeam et Commvault, avec qui nous faisons beaucoup d'optimisation pour que les logiciels interagissent très bien, notamment avec notre produit ARTESCA, qui est notre produit spécifique pour le backup.

Vous avez pu entendre des clients qui expliquent à quel point c'est facile de déployer. C'était notamment le cas d'Aerospacelab aujourd'hui, par exemple, ARTESCA avec Veeam. Nous avons d'autres clients qui déploient Commvault à très grande échelle. Il s'agit à la fois de partenariats, mais c'est aussi d'engagements de formation mutuelle, afin que Veeam et Commvault sachent comment nos logiciels fonctionnent, et que nous sachions comment fonctionnent les leurs. Nous avons formé nos équipes de customer success pour connaître ces logiciels et être capables d'aider les clients dans des problématiques qui dépasseraient largement les problématiques de Scality et qui seraient plus liées à ces logiciels. Donc c'est quelque

chose de très forte pour le travail commun. Et puis, le troisième type de partenariat est autour de l'Intelligence Artificielle, notamment avec WEKA et NVIDIA, qui ont présenté aujourd'hui. Avec WEKA, nous avons fait une intégration logicielle, avec un connecteur spécifique pour WEKA et nous sommes capables d'offrir une performance exceptionnelle sur WEKA. De notre point de vue, c'est aujourd'hui la solution de stockage la plus rapide sur le marché pour l'Intelligence Artificielle, bien plus rapide que tous ses concurrents. Et c'est la raison pour laquelle nous travaillons avec eux. Nous avons déjà réalisé vingt-cinq déploiements dans le monde avec WEKA. C'est un partenariat qui, à la fois technologiquement, et aussi dans la valeur délivrée aux clients, fonctionne très bien. Et puis avec NVIDIA, vous avez vu Serge Palaric, Vice-Président Alliances, Global CSP & ISV EMEA aujourd'hui sur scène, nous développons des projets autour de leur concept AI DP. Nous pensons que de plus en plus, l'IA va être déployée à l'Edge ou en périphérie, et nous travaillons avec NVIDIA sur des concepts autour de cela.

> QUELS SERAIENT VOS MESSAGES CLÉS POUR NOS LECTRICES ET LECTEURS, RSSI, CISO, DPO, DSI, RESPONSABLES CYBER ET RESPONSABLES CYBERSÉCURITÉ ?

Une chose qui a été dite par plusieurs de nos clients sur scène aujourd'hui, c'est qu'en fait, quand on choisit une solution, il y a la technique, mais il y a surtout la relation avec le fournisseur. Et plusieurs des clients ont dit : « OK, la solution de Scality, d'un point de vue technique, fonctionne extrêmement bien. On observe un MTBF (Mean Time Between Failure ou Temps Moyen de Fonctionnement entre Défaillances hors de tout arrêt volontaire ou programmé) de l'ordre de six ans, ce qui est extrêmement bon ». Mais ils ont dit en fait, « encore plus important, la relation qu'on a avec les équipes de Scality, que ce soient les équipes avant-ventes ou les équipes support, customer success, est vraiment excellente. » Et d'ailleurs, nous avons annoncé ce matin que dans une étude faite par Net Promoter Score, qui est une étude extrêmement exigeante, Scality ressort avec un Net Promoter Score de quatre-vingt-cinq, ce qui montre bien que **nos clients plébiscitent Scality dans la relation et sont prêts à recommander Scality autour d'eux.** L'autre chose, c'est que Scality continue à investir considérablement dans la sécurité. On est maintenant certifié ISO 27001. On fait des Pentests ou Tests d'intrusion de nos logiciels. C'est un investissement constant. J'ai envie de dire que c'est une évidence, mais je ne suis pas sûr que tous nos concurrents investissent autant dans ce sens.

At Scality's 10th Scality Day, CEO Jérôme LECAT emphasized client trust and global growth, especially in Kazakhstan, where Scality supports AI and digital initiatives. Partnerships with Inria (AI for predictive maintenance, cybersecurity, carbon tracking), NVIDIA, and WEKA advance sovereign, secure, eco-friendly data storage.

Clients praise Scality's technology and exceptional support, reflected in an 85 Net Promoter Score. Focus remains on security (ISO 27001) and strategic alliances.



SCALITY

CONTACTS :

Jérôme LECAT, CEO, Scality

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



RETEX NIS 2, DORA, CRA, ISO 27001, RGPD : CONFORMITÉ ET CYBERSÉCURITÉ, PILIERS DE LA SOUVERAINETÉ NUMÉRIQUE EUROPÉENNE

> SELON VOUS, QUELS SONT LES DÉFIS LORSQU'IL S'AGIT D'ASSOCIER LA CONFORMITÉ À LA CYBERSÉCURITÉ, NOTAMMENT PAR RAPPORT À L'IDENTITÉ NUMÉRIQUE ?

Historiquement, la cybersécurité a permis le bon fonctionnement des PC contre les virus ou les applications malveillantes, la sécurité des réseaux interconnectés via le firewall ou l'UTM et ses fonctions protection réseau. La stratégie cyber consistait à faire de la « protection périmétrique » des flux entrants et sortants. Aujourd'hui, avec l'explosion de la mobilité des utilisateurs, l'interconnexion aux réseaux industriels et aux applications cloud, les enjeux de cybersécurité se sont déplacés vers les utilisateurs et les machines. L'approche ZeroTrust est devenue un standard d'architecture pour reprendre le pouvoir sur les accès numériques. La gestion des identités et des accès est devenue le pivot de la stratégie cyber qui sous-tend la résilience de l'activité des organisations et des entreprises.

Par ailleurs, nous évoluons dans un contexte mondial profondément transformé par la montée en puissance de l'IA et une dépendance accrue aux géants extra-européens du numérique. Cette situation crée une tension entre la nécessité de respecter le cadre réglementaire européen fondé sur la protection des données, et la pression exercée par des solutions technologiques débridées.

Pour relever ce défi, nous avons besoin de bâtir un espace numérique de confiance reposant sur trois piliers :

- Une régulation commune assumée, garantissant la protection des identités et la conformité avec les standards européens ;
- Des capacités industrielles et technologiques souveraines, pour maîtriser nos infrastructures et nos données ;
- Une stratégie homogène de résilience numérique capable de faire face aux menaces de cyberattaques, en soutenant l'innovation.

Aujourd'hui, l'Europe ne dispose pas encore des infrastructures numériques souveraines nécessaires pour assurer pleinement son autonomie et sa compétitivité. La maîtrise de nos identités numériques et de nos données est donc essentielle pour conserver les clés de notre avenir numérique.

> COMMENT VOTRE ENTREPRISE CONTRIBUE-T-ELLE À RÉPONDRE À CES DÉFIS ?

WALLIX est un éditeur leader européen des logiciels de cybersécurité des Identités et des Accès (IAM), visionnaire du Gartner, présent dans 16 pays avec un réseau de revendeurs et intégrateurs déployé dans une centaine sur les cinq continents. Notre ambition est double :

- proposer une plate-forme innovante de gestion des accès identifiés, et des accès numériques à privilège,
- construire un acteur industriel européen pérenne dans la cybersécurité, qui permette aux entreprises et aux organisations de regagner en autonomie stratégique, à l'abri des lois extra-européennes.

Les solutions de WALLIX redonnent aux organisations le contrôle des accès numériques des utilisateurs humains et non humains aux actifs critiques et aux données sensibles, pour résister aux cyberattaques, se mettre en conformité et améliorer l'efficacité opérationnelle.

La vision stratégique de WALLIX repose donc sur trois piliers :

- La souveraineté des données;
- La souveraineté technologique, grâce à une plateforme modulaire WALLIX One, fondée sur les principes du Zero Trust, couvrant l'ensemble des besoins en IAM et PAM ;
- La souveraineté opérationnelle en plaçant la gouvernance du client au cœur de la démarche, soutenue par un écosystème solide de partenaires et d'experts dans 100 pays.

WALLIX One réunit dans une même approche modulaire, simple et évolutive, l'ensemble des fonctions clés de l'Identity Security :

- Authentification robuste (multi-facteurs)
- Contrôle des privilèges (PAM) pour maîtriser les accès sensibles,
- Gouvernance des identités et des accès (IGA) pour assurer conformité et traçabilité.

Architecture « tout-en-un » s'appuyant sur le principe du moindre privilège et la vérification systématique de chaque accès, qu'il s'agisse d'un utilisateur, d'un système ou d'un service.

> COMMENT VOTRE ORGANISATION S'ADAPTE-T-ELLE AUX ÉVOLUTIONS PERMANENTES DES DIRECTIVES, RÈGLEMENTS, LOIS DE TRANSPPOSITION ET TECHNOLOGIES ?

La mission de WALLIX est claire : protéger les identités des utilisateurs humains et non humains et leurs accès aux infrastructures critiques et aux données sensibles des organisations afin de leur permettre d'évoluer librement et en confiance dans un monde numérique.

Pour cela, nous nous engageons à offrir des solutions de la plus haute qualité, alliant innovation, robustesse et conformité.

WALLIX a obtenu les certifications ISO 27001 et SOC2 pour élever le niveau de qualité de ses services et solutions.

Historiquement certifiées par l'ANSSI en France, la solution WALLIX PAM a été certifiée par le BSI en Allemagne, attestant de la conformité de nos logiciels aux plus hauts standards européens de sécurité informatique, tels que définis par le BSI et l'ANSSI.

Nous concevons des produits de cybersécurité de haut niveau, destinés à assurer la résilience de nos clients. Dans une logique de qualité et de confiance numérique à l'échelle européenne, WALLIX poursuit une stratégie de certification selon les standards nationaux les plus exigeants.

La souveraineté devient ainsi un choix rationnel, durable et stratégique, permettant de concilier exigence de sécurité, indépendance technologique et optimisation budgétaire pour nos clients.

Précisons également que WALLIX investit fortement dans la sensibilisation et l'éducation à travers WeEdu, un programme destiné aux Ecoles et aux Universités en Europe pour former les futurs responsables informatiques et experts de nos entreprises, et participer ainsi à élever le niveau de résilience de la société.

>>>

>>>

Jean-Noël de Galzain, CEO of WALLIX, highlights the shift from perimeter security to identity-centric cybersecurity (Zero Trust) due to mobility, cloud, and AI. Europe faces tension between regulatory compliance (GDPR, NIS2) and reliance on non-European tech. WALLIX addresses this with a sovereign, modular IAM/PAM platform (WALLIX One), offering robust authentication, privilege management, and identity governance. Certified by ANSSI, BSI, ISO 27001, and SOC2, WALLIX ensures data sovereignty, operational resilience, and regulatory alignment. The company also invests in education (WeEdu) and global partnerships, making digital sovereignty a strategic, sustainable, and cost-effective reality for European organizations.

**CONTACTS :**

Jean-Noël de Galzain
Founder and CEO, WALLIX Group

Courriel : info@wallix.com

PRIVILEGED ACCESS / WORKFORCE ACCESS / ACCESS GOVERNANCE



wallix

Évoluez librement dans un monde numérique plus sûr

Libres et maîtres de vos systèmes, avec WALLIX vous opérez dans des environnements numériques et industriels où la sécurité ne freine pas vos activités. WALLIX sécurise les identités et accès afin de protéger vos actifs critiques face aux cybermenaces et de fluidifier vos interactions avec vos fournisseurs et vos clients. Leader Européen de la gestion des comptes à privilèges, WALLIX simplifie la mise en œuvre de la conformité et améliore l'efficacité opérationnelle des entreprises.

Avec WALLIX, vous bâtissez un monde numérique plus sûr pour innover, collaborer et grandir sans compromis.

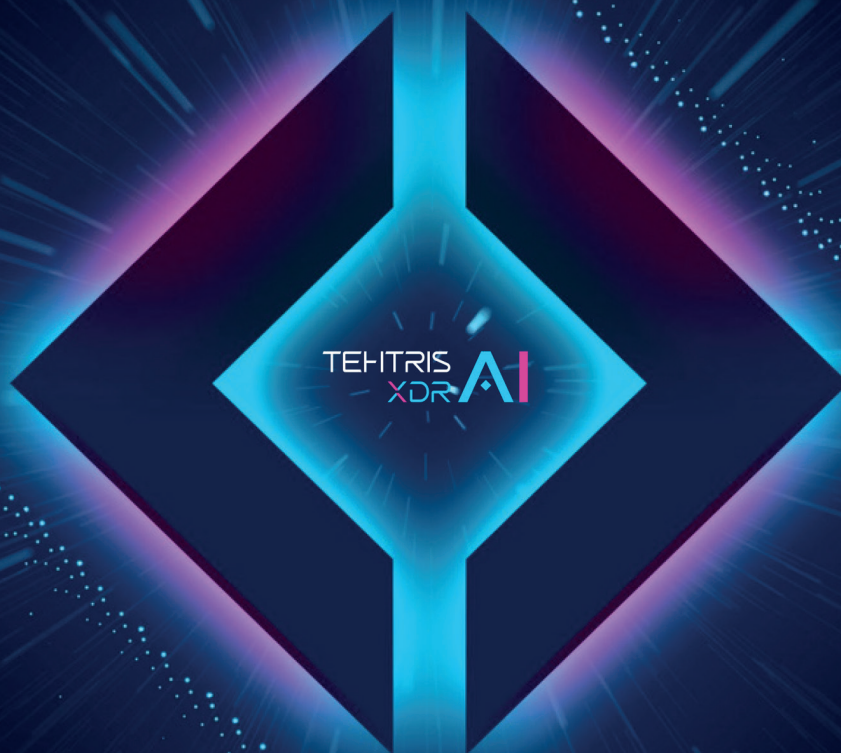
www.wallix.com

<TEHTRIS>

FACE THE UNPREDICTABLE

Devenez le gardien du cyberspace.

TEHTRIS
WITH XDR AI



DÉTECTEZ ET NEUTRALISEZ
AUTOMATIQUEMENT LES
CYBERATTAQUES EN TEMPS RÉEL,
QUELLE QUE SOIT VOTRE ORGANISATION.



business@tehtris.com
tehtris.com



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





BAPTISTE
ROBERT

CEO de Predictalab

L'EXPERT OSINT

■ ■ **GS MAG** : *Baptiste Robert, bonjour. Global Security Mag. Nous sommes ravis de vous avoir en entretien. Pouvez-vous vous présenter?*

La question des traces laissées par les membres de l'Exécutif, mais également par les collaborateurs, elle est extrêmement importante et elle peut avoir des conséquences directes sur la Cybersécurité, mais également sur la Sûreté.

■ ■ **BR** : Je me suis fait connaître il y a maintenant une petite dizaine d'années en tant que hacker, puisque j'ai réussi à trouver dans plusieurs applications gouvernementales des failles de sécurité que j'ai révélées à l'époque sur les réseaux sociaux, notamment sur Twitter. Et j'ai été fortement médiatisé à cette occasion-là. J'ai travaillé sur des applicatifs gouvernementaux indiens, français, américains, du Vatican également, russes, chinois. Donc, j'ai fait un bon tour du monde. Et suite à cette médiatisation, j'ai passé beaucoup de temps dans les médias, dans la presse écrite, en télévision, à faire de la sensibilisation sur les aspects cyber. Mais j'ai également passé pas mal de temps à faire des conférences, que ce soit pour la sensibilisation du grand nombre, donc des conférences publiques, mais aussi des conférences privées pour des entreprises, pour faire

de la sensibilisation cyber dans les entreprises, ce qui reste une activité que je fais encore actuellement. Je donne entre trente et quarante conférences par an. Il y a cinq ans, j'ai décidé avec un associé qui est toulousain, de créer une société qui s'appelle Predictalab. Et après avoir travaillé sur le sujet de la désinformation, nous avons décidé de créer cette société spécialisée en OSINT, l'Open Source Intelligence, Renseignement d'origine Source Ouverte en français. Et l'idée était d'être un expert, un référent dans le domaine de l'Open Source Intelligence. Predictalab agit sur trois verticales différentes. Une première qui va être sur la question des analyses, des empreintes numériques. Nous travaillons avec des Responsables, des hauts dirigeants, des membres de Comités Exécutifs, pour faire leur empreinte numérique. Globalement, nous allons répondre à une question qui est très simple, c'est de dire : qu'est-ce qui traîne sur moi sur Internet ? Qu'est-ce qui est critique ? Qu'est-ce que je dois enlever et comment je dois l'enlever ? Et sur ces problématiques, nous aidons le Dirigeant ou la Dirigeante, en lui faisant un audit complet de tout ce qui traîne sur lui ou elle, et surtout en l'accompagnant, en supprimant pour lui ou elle ce qui doit être supprimé. Nous savons que très souvent, quand on a des responsabilités, quand la vie va très vite, on a souvent tendance à mélanger sa vie privée et sa vie personnelle. Et c'est l'ordre des choses, mais à un certain niveau, il est important de faire la séparation des

deux. Nous faisons aussi des enquêtes dirigées où on va répondre à des problématiques, faire de l'investigation classique, travailler avec des avocats, des enquêteurs privés. Nous travaillons parfois avec le secteur public pour faire de l'investigation. Nous avons une deuxième verticale consacrée à de la formation. Nous formons des équipes d'investigation, des équipes spécialisées, du secteur public ou du secteur privé, à faire de l'enquête sur Internet, à utiliser l'OSINT et un tout ce qui est relatif à cela, toutes les capacités de l'OSINT.

La troisième verticale est une classique d'édition de logiciels. Nous créons des produits associés à l'OSINT. Nous avons plusieurs solutions qui sont disponibles sur Internet. Par exemple, Predictasearch.com, qui est un moteur de recherche inversé pour les adresses électroniques, numéros de téléphone, pseudonymes et noms. Typiquement, en résumé : vous soumettez une adresse électronique et en trente secondes, nous allons vérifier sur une centaine de sites internet les comptes associés à cette adresse électronique. Et donc en trente secondes, vous allez avoir une empreinte numérique de la personne très rapidement et cela permet à l'enquêteur qui part d'une seule adresse électronique d'obtenir plein d'informations associées, un nom, prénom, un pseudonyme, des adresses IP, même des mots de passe parfois, pour aller chercher toutes ces informations. Nous avons d'autres solutions, on a Predictagraph, Predictagraph.com, stealers.ai, qui nous permettent de compléter nos offres et d'avoir une synergie entre les différents produits. Certains sont publics, d'autres sont moins publics car réservés à des gens dont c'est le métier, donc un métier un peu plus spécifique. Globalement, c'est l'activité de Predictalab. Donc il s'agit d'être un expert, un référent en la matière de l'OSINT pour rayonner sur cette question par les conférences, mais également de pouvoir former le plus grand nombre, de pouvoir fournir les outils adaptés de nos jours sur cette question, et de pouvoir appuyer la demande d'investigation, puisque ça nous permet également d'avoir un feedback, un retour direct de nos produits, car les utilisateurs, les consommateurs de nos produits, les premiers consommateurs, sont en fait en interne.

■ ■ **GS MAG** : *Pouvez-vous nous donner deux ou trois spécificités qui rendent Predictalab unique ? Des points clés ?*

■ ■ **BR** : Les points clés de Predictalab, c'est que quand vous allez sur le marché mondial de l'OSINT, vous allez souvent trouver des sociétés qui font un petit bout, qui font soit de la formation, soit autre chose. L'idée de Predictalab, et c'est ce qui rend Predictalab unique, c'est d'être un concentré d'expertise. Nous avons à l'intérieur de Predictalab, tout le cycle global. Si vous avez n'importe quelle question relative

à l'OSINT, nous pouvons probablement, et même sûrement y répondre. Que cela soit à propos de la formation, sur de l'enquête, sur du produit, nous savons faire. Et le but de Predictalab, et cela est aussi unique, c'est que nous sommes peu de personnes, mais nous sommes extrêmement productifs. Nous sommes à ce jour, un effectif d'une dizaine de personnes avec un noyau dur de personnes qui travaillent extrêmement rapidement et qui ont des expertises très pointues. L'idée de Predictalab, c'est de nous voir comme une « Squad » ou une équipe de personnes extrêmement qualifiées qui vont être très productifs et directement au point.

■ ■ **GS MAG** : *Pouvez-vous nous donner quelques messages clés pour nos lectrices et lecteurs qui sont aussi des RSSI, des CISO, des DSI, des Responsables Cyber et Cybersécurité, des DPO ?*

■ ■ **BR** : La question de l'empreinte numérique est très importante pour les Responsables, notamment les Responsable Cyber et Cybersécurité, et aussi pour les Responsables Sûreté. La question des traces laissées par les membres de l'Exécutif, mais également par les collaborateurs, elle est extrêmement importante et elle peut avoir des conséquences directes sur la Cybersécurité, mais également sur la Sûreté. Cela est donc un sujet qu'il faut prendre à bras le corps. On sait aujourd'hui que la Cybersécurité est un vrai sujet sur lequel il faut investir, mais ce sujet de l'empreinte numérique, c'est un sujet qu'il faut attaquer en priorité. Très souvent, cela permet aussi d'amener d'autres sujets. On sait que la Cybersécurité nécessite d'aller en Comex (Comité Exécutif) pour convaincre les Dirigeants qu'on a envie d'attaquer ce sujet. Vous pouvez par exemple leur montrer leurs empreintes numériques, leurs multiples informations sur Internet. Ensuite, leur expliquer en quoi cela peut les mettre en danger, eux, leurs familles, leurs enfants, leurs parents... C'est en général une très bonne illustration qui permet d'amener d'autres sujets, de dire : Vous voyez, la Cybersécurité, c'est important, il faudrait peut-être y mettre des fonds. Donc la sécurisation de l'empreinte numérique des Dirigeants, c'est un « quick win » résultat probant rapide, c'est ainsi plus facile de faire passer des messages et amener d'autres sujets. Chez Predictalab, une solution qui s'appelle Stealers.ai permet d'être alerté en direct quand des collaborateurs vont se faire hacker et s'il y a des identifiants liés à l'Entreprise ou l'Organisation et qui traînent sur Internet. Notre idée chez Predictalab, et cela s'explique aussi par mon background ou parcours, c'est de se mettre dans la peau des cyberattaquants et savoir comment ils procèdent, comment ces gens-là aujourd'hui attaquent les sociétés et quelles sont les procédures utilisées par ces personnes, afin de pouvoir contrer ces procédures. ■



JEAN-LUC
RAYMOND

Journaliste Tech

L'IA AU DÉFI DE LA GESTION DES VULNÉRABILITÉS

**AU SOPHI.A SUMMIT,
SAP EXPOSE LES
PROMESSES ET LIMITES
DES MODÈLES DE LANGAGE
FACE À L'EXPLOSION DES
FAILLES LOGICIELLES.**

UNE PRESSION CROISSANTE SUR LES CHAÎNES DE SÉCURITÉ

Lors de l'édition 2025 de ce rendez-vous international qui a rassemblé à Nice Sophia Antipolis des chercheurs et experts mondiaux de l'intelligence artificielle, Merve Sahin, chercheuse et ingénieure au sein de l'équipe Product Security de SAP, a explicité la tension qui pèse sur la gestion des vulnérabilités. Elle rappelle que chaque faiblesse dans l'architecture, l'implémentation ou la configuration d'un logiciel peut compromettre la confidentialité, l'intégrité ou la disponibilité d'un système, avec des effets pouvant aller de la fuite de données aux interruptions d'activité. Dans un contexte où les vulnérabilités recensées augmentent fortement et où les délais de correction se mesurent parfois en mois, les équipes AppSec recherchent des leviers pour accélérer la détection et la remédiation.

Dans un contexte où les vulnérabilités recensées augmentent fortement et où les délais de correction se mesurent parfois en mois, les équipes AppSec recherchent des leviers pour accélérer la détection et la remédiation.

IA ET DÉTECTION : AVANCÉES RAPIDES, MATURITÉ LIMITÉE

Les outils SAST, qui analysent statiquement le code, demeurent largement utilisés, mais génèrent encore trop de faux positifs. L'espoir suscité par les grands modèles de langage s'accompagne donc d'une prudence méthodologique. Les recherches compilent plus de quarante ensembles de données et aboutissent à des résultats contradictoires. Dans certaines expériences, les modèles identifient des vulnérabilités non détectées par les SAST classiques, mais leur taux de faux positifs peut grimper jusqu'à 85 %, un niveau incompatible avec les contraintes des pipelines de développement continus. De plus, l'absence d'explicabilité pose un problème majeur. Là où une règle SAST est lisible et modifiable, l'interprétation produite par un modèle peut paraître convaincante tout en étant fautive, obligeant les analystes à renforcer leur vigilance au lieu de la réduire.

PRIORISATION : DES SIGNAUX ENCORE TROP FAIBLES

La priorisation des vulnérabilités, déterminante pour les RSSI, reste difficile à automatiser. Les modèles parviennent à prédire certains paramètres du score CVSS, comme le vecteur d'attaque ou la complexité, mais échouent dès que les critères dépendent du contexte applicatif. Sahin souligne la nécessité de benchmarks mieux construits pour évaluer la capacité réelle de l'IA à trier efficacement les risques.

REMÉDIATION : L'IA SURPREND PAR SA QUALITÉ

La réparation automatisée apparaît comme l'usage le plus prometteur. En collaboration avec l'université du Nouveau-Brunswick (Canada), SAP a analysé 75 cas réels issus de la base NVD, chacun associé à une vulnérabilité détectée par un SAST. Les modèles

reçoivent le fichier vulnérable annoté et doivent produire un correctif ensuite validé par des tests. Certains modèles atteignent 86 % de corrections valides, dépassant parfois la qualité des correctifs humains, notamment sur des injections SQL où l'IA applique systématiquement les requêtes préparées plutôt que des «échappements» partiels. Cette capacité à proposer des correctifs plus complets et plus structurés ouvre des perspectives concrètes pour réduire la dette de sécurité.

UN POTENTIEL RÉEL, MAIS UNE SUPERVISION INDISPENSABLE

Aussi, les limites demeurent évidentes. Les modèles peuvent supprimer des blocs de code utile, introduire des régressions ou générer des modifications excessives. Leur variabilité, même à paramètres identiques, interdit pour l'instant leur usage autonome. Les pistes les plus ambitieuses reposent sur les approches agentiques capables d'orchestrer l'analyse, d'exécuter du code et de vérifier automatiquement les correctifs. Les annonces récentes de Google et OpenAI vont dans cette direction, mais aucune évaluation indépendante ne permet encore de juger leur robustesse.

UNE TRANSFORMATION INÉVITABLE, MAIS PROGRESSIVE

Les recherches de Merve Sahin montrent que l'IA n'a pas vocation à remplacer les experts en cybersécurité, mais qu'elle peut devenir un levier décisif, particulièrement dans la remédiation. La détection et la priorisation devront encore gagner en fiabilité avant de s'intégrer pleinement aux chaînes de sécurité. Pour les RSSI, la question n'est pas de savoir si ces outils s'imposeront, mais comment s'y préparer sans fragiliser la qualité globale des systèmes. L'IA accélère déjà certaines tâches critiques; il appartient désormais aux organisations de définir les conditions permettant d'en tirer un bénéfice durable. ■



NICOLAS
LIARD

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

COMMENT L'AUTOMATISATION ET L'INTELLIGENCE ARTIFICIELLE

SONT AU SERVICE DE LA MISE EN CONFORMITÉ

**LONGTEMPS PERÇUE COMME UNE
CONTRAINTE ADMINISTRATIVE,
ELLE S'IMPOSE DésORMAIS
COMME UN PILIER DE LA CONFIANCE
NUMÉRIQUE ET UN LEVIER DE
TRANSFORMATION STRUCTURELLE.**

La multiplication des cadres réglementaires – NIS 2, DORA, Cyber Resilience Act, RGPD, ISO 27001 – a considérablement accru la complexité du paysage normatif européen. Chaque texte impose de nouvelles obligations : contrôle, traçabilité, gestion documentaire, et audits réguliers.

Face à cette densité réglementaire, les entreprises doivent revoir leur approche : la conformité ne peut plus être une opération ponctuelle, elle doit devenir un processus dynamique, intégré et mesurable en continu.

C'est précisément dans ce contexte que l'automatisation et l'intelligence artificielle (IA) prennent toute leur valeur : non comme gadgets technologiques, mais comme instruments de rationalisation, d'efficacité et de gouvernance intelligente.

L'intelligence artificielle révolutionne la gestion de la conformité, transformant une contrainte administrative en levier de performance.

AUTOMATISER POUR MAÎTRISER : LA NAISSANCE D'UNE CONFORMITÉ AUGMENTÉE

L'automatisation appliquée à la conformité s'appuie sur une logique simple : décharger les équipes des tâches répétitives et structurantes, tout en améliorant la fiabilité et la cohérence des processus.

L'intelligence artificielle, en particulier, apporte une dimension nouvelle : la capacité d'analyser, de corrélérer et d'interpréter des volumes massifs de données réglementaires et opérationnelles, pour aider à la décision et anticiper les écarts de conformité.

Deux exemples concrets illustrent cette évolution : Hexadiag, développé par le groupement Hexatrust repose sur un principe d'auto-évaluation guidée : à partir de questionnaires dynamiques et de référentiels intégrés (NIS 2, DORA, ISO 27001), l'outil génère une cartographie de maturité et une feuille de route priorisée. L'entreprise obtient ainsi une vision claire de ses écarts et de ses objectifs, sans nécessiter un audit préalable lourd. Cette approche standardisée offre un gain de temps considérable et une première brique de pilotage stratégique.

De son côté, Optivalue de Smart Global Governance franchit une étape supplémentaire en intégrant l'automatisation documentaire et la logique d'IA. La plateforme assure la gestion continue des preuves de conformité, la production automatisée des rapports d'audit et l'accompagnement vers les certifications.

Elle identifie les écarts entre politiques internes et exigences normatives, puis propose des mesures correctives adaptées. La gouvernance, gestion des risques et conformité (GRC) forme les socles des stratégies de sécurité modernes. En s'appuyant sur l'IA, les plateformes GRC analysent en temps réel les risques et automatisent les workflows de conformité, réduisant ainsi la charge administrative tout en garantissant le respect des réglementations sectorielles, comme SOX ou HIPAA.

Ce type de solution marque la transition vers une conformité dite "intelligente", capable d'apprendre et de s'ajuster à mesure que l'organisation évolue.

LES FONDATIONS TECHNIQUES D'UNE CONFORMITÉ INTÉGRÉE

Si les outils d'auto-diagnostic constituent la surface visible de cette transformation, la véritable révolution se joue en profondeur, au sein des infrastructures de cybersécurité.

Dans un paysage numérique en constante évolution, marqué par la multiplication des cybermenaces et l'exigence croissante de conformité réglementaire (RGPD, NIS2, ISO 27001, etc.), les organisations se tournent vers des solutions innovantes pour sécuriser leurs infrastructures. Parmi les outils incontournables, le SIEM (Security Information and Event Management) joue un rôle central en collectant et corrélant les logs et événements de sécurité en temps réel. Grâce à l'intelligence artificielle, ces systèmes ne se contentent plus de signaler des incidents : ils anticipent les menaces via des analyses >>>

>>> prédictives et automatisent la génération de rapports de conformité, facilitant ainsi les audits et la détection des écarts aux politiques de sécurité. De leur côté, les solutions de Data Security Posture Management (DSPM) et de Cloud Security Posture Management (CSPM) permettent de cartographier et protéger les données sensibles dans les environnements cloud. L'IA y joue un rôle clé en classifiant automatiquement les données (via le traitement du langage naturel) et en corrigeant dynamiquement les configurations non conformes, alignées sur les benchmarks CIS ou les normes NIST. L'Identity and Access Management (IAM), souvent couplé au Privileged Access Management (PAM) garantissent ainsi le respect du principe du moindre privilège, une exigence majeure des normes ISO 27001 et NIS2. La gestion des vulnérabilités, quant à elle, s'appuie sur l'IA pour prioriser les correctifs en fonction de l'impact potentiel des failles, automatisant les scans et optimisant la conformité aux standards PCI DSS ou ISO 27001. Un grand nombre d'autres solutions de sécurité pourraient être évoquées ici qui prennent une nouvelle dimension grâce à l'intelligence artificielle et permettent une conformité

intégrée tels que les EDR, NDR, SASE, DLP, UEBA etc ... L'intégration de l'IA dans ces solutions ne se limite pas à renforcer la sécurité : elle transforme la manière dont les organisations abordent la conformité, en automatisant les processus, en détectant proactivement les menaces et en réduisant les risques liés aux erreurs humaines. Une révolution indispensable pour faire face aux défis cyber d'aujourd'hui et de demain.

DES BÉNÉFICES TANGIBLES, MAIS PAS SEULEMENT

L'intelligence artificielle révolutionne la gestion de la conformité, transformant une contrainte administrative en levier de performance. Les gains sont immédiats et mesurables : les délais et coûts liés aux audits sont réduits de moitié, voire des deux tiers, grâce à l'automatisation de la collecte des preuves et à la génération instantanée de rapports. Fini les semaines de préparation fastidieuse, place à une conformité quasi temps réel. Mais l'IA ne se contente pas d'accélérer les processus.

Elle en améliore aussi la fiabilité en appliquant des règles homogènes et reproductibles, éliminant ainsi les biais humains et les divergences d'interprétation entre audi-

teurs. Chaque action de sécurité devient traçable, offrant une visibilité stratégique aux décideurs via des tableaux de bord dynamiques. Ces outils permettent de suivre, en un clin d'œil, l'état de conformité par norme, par entité ou par région — un atout majeur pour les organisations multinationales. Au-delà de ces avancées opérationnelles, c'est toute la culture de la conformité qui se métamorphose.

Exit l'exercice ponctuel et subis, place à un

indicateur clé de performance et de résilience, valorisable auprès des régulateurs, des partenaires et même dans les appels d'offres. La conformité n'est plus un mal nécessaire, mais un avantage concurrentiel.

Pourtant, cette automatisation n'est pas sans risques. À force de déléguer la surveillance et l'analyse aux algorithmes, une dérive subtile mais dangereuse guette

L'intelligence artificielle, en particulier, apporte une dimension nouvelle : la capacité d'analyser, de corréler et d'interpréter des volumes massifs de données réglementaires et opérationnelles, pour aider à la décision et anticiper les écarts de conformité.

les organisations : celle de la « vibe compliance ». Par analogie au « vibe coding » — cette pratique où les développeurs codent par intuition sans maîtriser la logique sous-jacente — la « vibe compliance » désigne une conformité de façade. Tout semble en ordre, les indicateurs sont au vert, mais personne ne comprend plus vraiment le sens des contrôles ni la logique qui les sous-tend. Les dangers sont multiples. D'abord, une perte de compréhension : les équipes, habituées à des processus automatisés, peinent à expliquer la raison d'être d'un contrôle ou d'une mesure. Ensuite, une dépendance aveugle aux algorithmes : une erreur de paramétrage ou un biais dans le modèle peut fausser l'ensemble du reporting, sans que personne ne s'en aperçoive. Enfin, et surtout, un flou sur la responsabilité : en cas de non-conformité détectée trop tard, qui sera tenu pour responsable ? L'outil, l'intégrateur, ou l'organisation elle-même ?

Ces défis soulignent une réalité incontournable : l'IA ne doit pas remplacer le jugement humain, mais l'éclairer. La conformité automatisée, aussi performante soit-elle, ne peut être légitime que si elle reste sous la supervision d'experts, dans un cadre de gouvernance transparent et documenté. Les technologies sont des outils puissants, mais c'est à l'humain de leur donner du sens — et d'en assumer la responsabilité. L'enjeu n'est pas de choisir entre automatisation et expertise, mais de créer une synergie où l'IA amplifie les capacités humaines, sans jamais les remplacer. Car une conformité qui ne repose que sur des algorithmes, aussi sophistiqués soient-ils, reste une illusion. La vraie résilience s'appuie sur l'alliance de l'intelligence artificielle et de l'intelligence critique

CONFORMITÉ AUGMENTÉE : QUAND L'IA ET L'EXPERTISE HUMAINE S'ALLIENT POUR UNE GOUVERNANCE RESPONSABLE

À l'ère de la transformation numérique, la conformité n'est plus une simple case à cocher, mais un écosystème dynamique, où l'intelligence artificielle et l'expertise humaine doivent trouver un équilibre subtil.

L'IA n'est plus un simple exécutant, mais un copilote stratégique. Elle assiste les RSSI, les Délégués à la Protection des Données (DPO) et les responsables conformité dans leurs prises de décision, sans pour autant les remplacer. Son rôle ? Analyser des montagnes de données, détecter des anomalies et suggérer des actions, tout en laissant aux experts le soin de valider, ajuster et interpréter. Les professionnels de la conformité voient ainsi leur mission évoluer : ils deviennent des « entraîneurs d'IA », garants de la qualité des modèles, de la pertinence des indicateurs et de la transparence des processus.

L'enjeu est de taille : une automatisation bien maîtrisée permet de passer d'une conformité statique, souvent perçue comme une contrainte, à une conformité vivante, mesurable et explicable. Capable de s'adapter en temps réel aux évolutions des menaces et des réglementations, elle offre aux organisations une agilité sans précédent.

Mais attention : cette mutation ne peut être vertueuse que si elle reste gouvernée, auditée et centrée sur l'humain. Car au fond, la conformité ne se résume pas à une question technique. C'est un engagement éthique et responsable.

L'IA, aussi puissante soit-elle, n'est qu'un outil au service de cette mission. Son rôle est d'amplifier la portée de la conformité, pas d'en effacer la dimension humaine. La technologie doit éclairer la conscience, pas la remplacer. Dans un monde où les enjeux de cybersécurité et de protection des données n'ont jamais été aussi critiques, cette alliance entre l'IA et l'expertise humaine n'est pas un luxe — c'est une nécessité.

L'avenir de la conformité se dessine donc à l'intersection de l'innovation et de l'éthique. La conformité de demain sera augmentée, mais gouvernée ; intelligente, mais explicable ; automatisée, mais responsable.

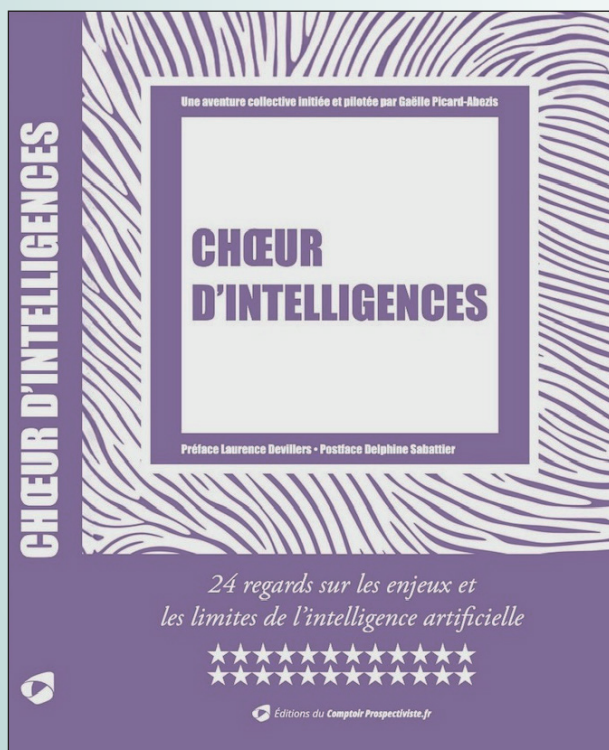
C'est dans cet équilibre subtil entre l'expertise humaine et la puissance des machines que réside la clé de la confiance numérique européenne. Une confiance qui ne se décrète pas, mais se construit — jour après jour, entre transparence, responsabilité et innovation. ■

GAËLLE
PICARD-ABEZIS



*Fondatrice Galléan,
Initiatrice et Pilote du livre*

LIVRE CYBER : *CHŒUR D'INTELLIGENCES*



■ ■ **GS MAG :** *Quel est le contexte et quels sont les enjeux de votre livre ?*

■ ■ **GPA :** J'ai voulu que cet ouvrage soit une exploration à 360° mais surtout qu'il dépasse les clivages ! De l'industrie du jeu vidéo aux algorithmes financiers, de l'éthique en cosmétique aux deepfakes, de l'imaginaire des enfants à la cybersécurité souveraine : *Chœur d'intelligences* explore l'IA là où elle opère vraiment. Cette cartographie inédite révèle des connexions insoupçonnées et des enjeux cruciaux que les débats mainstream, souvent superficiels, ignorent totalement.

L'ambition ? Dépasser la simple vulgarisation technique. Chercheurs, artistes, start-uppeurs, avocats, spécialistes de la data, doctorants et enseignants s'unissent pour interroger les promesses, les dérives et les paradoxes de cette technologie qui transforme notre société.

Pourquoi ce livre arrive-t-il au bon moment ?

Parce qu'en 2025, nous ne pouvons plus nous contenter d'approches approximatives. L'IA transforme déjà notre rapport à la création littéraire, à la prise de parole publique, à l'écologie, à la justice. Ce livre donne enfin la parole à ceux qui la vivent de l'intérieur.

Et c'est là sa force : **24 contributions expertes qui osent se confronter**. Des visions parfois opposées qui s'enrichissent mutuellement. Des doutes qui éclairent autant que les certitudes. Des débats qui avancent parce qu'ils assument la complexité et refusent les réponses simplistes. Contrairement aux ouvrages techniques froids ou aux essais alarmistes, *Chœur d'intelligences* offre ce qui manque cruellement : **une compréhension globale, nuancée et honnête des mutations en cours**. Chaque auteur apporte sa perspective unique. À chaque lecteur d'en faire sa propre synthèse.

■ ■ GS MAG : En quoi votre livre peut-il aider les RSSI, les CISO, et les DPO ?

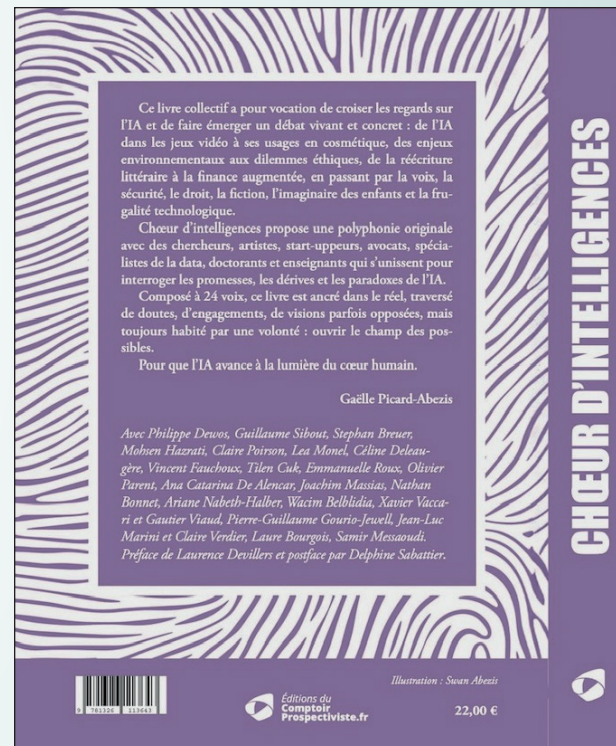
■ ■ **GPA** : Rares sont les livres où une polyphonie d'auteurs se réunit pour explorer les enjeux majeurs et pluriels de notre époque. *Chœur d'intelligences* couvre de nombreux secteurs d'activité, tout en abordant de front les questions d'éthique, de réglementation et les perspectives d'évolution de l'IA. Pour un RSSI qui maîtrise ses sujets et leurs enjeux, la veille permanente ne suffit pas : il faut aussi cultiver la curiosité du moment présent pour mieux se projeter dans l'avenir. Ce livre est là pour éveiller, ouvrir le débat et interroger.

Quelques thématiques et extraits qui pourraient retenir leur attention :

Pierre-Guillaume Gourio-Jewell, co-fondateur d'**Open Sezam**, interroge le lien entre IA, morale et éthique : *« Derrière chaque filtre se cache une hiérarchie de valeurs. Et cette hiérarchie n'est jamais universelle. Une entreprise peut juger prioritaire de protéger la réputation de ses partenaires ; une administration peut privilégier l'ordre public au détriment de la liberté d'expression. »* **Claire Poirson**, fondatrice du cabinet **FIRSH** et pionnière sur la question des deepfakes à travers le lab innovation international qu'elle a créé, et **Léa Monel** nous interpellent sur ce phénomène tout en rappelant un paradoxe fondamental : *« Le deepfake est en soi libre et constitue un outil moderne d'expression d'une liberté fondamentale : la liberté d'expression. »* Enfin, **Jean-Luc Marini**, Directeur de recherche d'**OpenStudio**, et **Claire Verdier**, Data Scientist, proposent des pistes concrètes vers une IA frugale : *« L'adoption d'une IA plus frugale constitue un début de réponse pour réduire l'impact environnemental de l'IA. »* et je ne dévoile pas le chapitre de **Samir Messaoudi** CEO de Kunayo sur la Cyber ...

■ ■ GS MAG : Quels sont vos messages pour nos lectrices et lecteurs (RSSI / CISO / DSI / CIO / DPO / Responsables Cyber et Cybersécurité...) ?

■ ■ **GPA** : Ce livre invite, avec humilité, à se questionner et à se projeter. Je sais que leurs fonctions, oh combien stratégiques, autour de la sécurité, de la sûreté et de la cybersécurité s'exercent avec cette curiosité naturelle et cet esprit critique permanent. Comme l'évoque **Olivier Parent** co-fondateur du **Comptoir Prospectiviste** : *« Ne devrions-nous pas être attentifs à ne pas faire de l'IA un pharmakon moderne, à ne pas en faire le bouc émissaire qui se verrait condamné à supporter nos comportements et usages pas toujours responsables ? »*. ■



*Magistrate et
Spécialiste du Droit
du Numérique et de
la Cybersécurité*



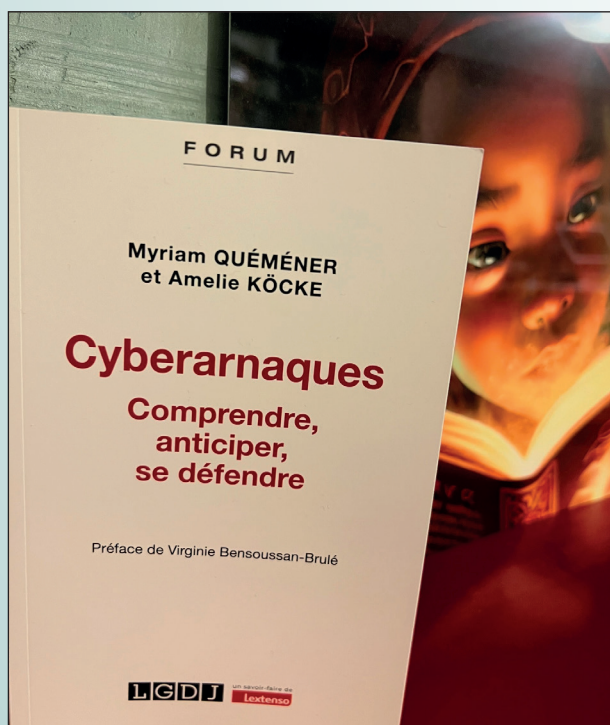
MYRIAM QUÉMÉNER

*Experte en
criminalité
financière*



AMELIE KÖCKE

LIVRE CYBER : CYBERARNAQUES, COMPRENDRE, ANTICIPER, SE DÉFENDRE



■ ■ **GS MAG :** *Quel est le contexte et quels sont les enjeux de votre livre ?*

■ ■ **MQ & AK :** Nous sommes parties du constat que les cyberfraudes étaient en pleine expansion et visaient aussi bien les entreprises, les collectivités territoriales et les citoyens. Les cybercriminels se sont adaptés à leurs cibles avec par exemple du phishing de mieux en mieux réalisé et avec des logos bien imités. Les cyberfraudes sont en fait une manifestation de la cybercriminalité qui est de plus en plus une délinquance financière. Dans ce contexte, notre livre éclaire la mutation rapide des menaces: industrialisation des attaques, professionnalisation des réseaux, et exploitation des innovations technologiques pour tromper plus vite, plus loin et à moindre coût.

L'IA générative change l'échelle : courriels et sites frauduleux sans faute, automatisation des approches, personnalisation des arnaques grâce aux données publiques. Les deepfakes de voix et de visage permettent des usurpations d'identité crédibles, de la fraude au président aux ordres de virement urgents,

en passant par la manipulation d'opinion. Les cryptomonnaies, elles, offrent aux fraudeurs des rails de paiement pseudonymes, accélérant escroqueries, ransomwares et «rug pulls». Le spoofing (affichage d'un numéro ou d'une identité légitime) amplifie l'effet de confiance et contourne les réflexes de vigilance.

Les enjeux sont multiples : économiques, juridiques et humains. Notre ouvrage déploie la cartographie des scénarios, du phishing aux deepfakes, des faux ordres de virement aux arnaques d'investissement en cryptomonnaies. Ce livre qualifie également les infractions qui s'y rattachent (escroquerie, usurpation d'identité, blanchiment, accès frauduleux) et dresse le portrait des acteurs de la riposte. Nous explorons une jurisprudence prise entre innovation et vide normatif et plaidons pour une coopération renforcée entre sphères publique et privée. Partage de signaux, plateformes sécurisées, harmonisation transfrontalière: seule cette alliance permettra de poursuivre efficacement les fraudeurs et de restaurer la confiance numérique.

■ ■ GS MAG : *En quoi votre livre peut-il aider les RSSI, les CISO, et les DPO ?*

■ ■ MQ & AK : Ce livre d'un format peu encombrant est en sorte un guide de bonnes pratiques pour les RSSI, les CISO et les DPO. Cet ouvrage propose des clefs afin de se protéger contre les fraudes numériques, se prémunir contre ces pièges qui sont aujourd'hui très diversifiés et parfois démultipliés par le biais du recours à l'Intelligence artificielle. Ce livre fait aussi des préconisations pour avoir les bons réflexes et donne aussi des adresses et références afin de contacter les services compétents pour traiter par exemple les plaintes relatives aux fraudes et escroqueries commises en ligne.

Nous présentons des scénarios types, fraude au président, phishing ciblé, spoofing d'identité, deepfakes vocaux ou vidéo, escroqueries aux cryptomonnaies, avec des signaux faibles et des modes opératoires. Nous abordons également les autorités d'enquête et de poursuite compétentes et les canaux de signalement. Nous synthétisons la jurisprudence notamment en matière de fraude au paiement en ligne récente qui précise les responsabilités utiles pour calibrer les contrôles. Enfin, nous décryptons les nouveaux cadres légaux et réglementaires en vigueur, afin d'aider RSSI, CISO et DPO à transformer la conformité en levier opérationnel.

■ ■ GS MAG : *Quels sont vos messages pour nos lectrices et lecteurs (RSSI / CISO / DSI / CIO / DPO / Responsables Cyber et Cybersécurité...) ?*

■ ■ MQ & AK : Le message principal consiste à s'informer sur les modes opératoires et se méfier des annonces alléchantes. Il est préférable d'aller sur les sites connus et ne pas cliquer sur des mails d'inconnus.

Pour toutes celles et ceux qui portent la responsabilité du numérique, l'essentiel est d'entretenir une connaissance à jour des fraudes et de leurs évolutions. Les techniques changent vite, l'IA facilite les imitations et les usurpations, et il faut garder un regard attentif sur ce qui paraît trop crédible ou trop urgent.

La sensibilisation gagne à être continue. Quelques repères simples, partagés régulièrement, permettent à chacun de reconnaître un signal faible, de poser une question, de demander une vérification. La vigilance devient un réflexe collectif plutôt qu'un rappel ponctuel.

La coopération fait véritablement la différence. Quand les équipes échangent leurs observations, quand les partenaires se tiennent informés, les fraudes perdent de leur effet de surprise. Mieux vaut un doute exprimé tôt qu'un incident découvert tard. La confiance se construit en circulant, calmement, l'information utile.

Face aux deepfakes et aux messages travaillés par l'IA, le jugement humain reste central. Un second regard, une confirmation par un autre canal, un temps de recul suffisent souvent à dévoiler la supercherie. Ce livre veut nourrir ces réflexes sobres et partagés. Il ne promet pas l'absence d'attaques, mais une capacité renforcée à les reconnaître vite, à les contenir et à préserver l'essentiel. ■



*Ecrivain Officier Central de
Sécurité chez IBM France*

ETIENNE DE SÉRÉVILLE

LIVRE CYBER : CYBERSÉCURITÉ DES INFRASTRUCTURES CRITIQUES, APPLIQUER ET METTRE EN ŒUVRE NIS2



■ ■ **GS MAG :** *Quel est le contexte et quels sont les enjeux de votre livre ?*

■ ■ **EDS :** Le livre s'inscrit dans le double contexte de la dépendance accrue de nos sociétés aux technologies numériques et de menaces cyber permanentes. La transformation numérique de nos activités s'accélère encore dans tous les processus industriels et de service, intégrant les nouveautés technologiques comme l'intelligence artificielle et le quantique, ou plus simplement la facturation électronique obligatoire à partir de 2026.

Parallèlement, sur une scène internationale conflictuelle, les pays européens font face à des opérations adverses dans le cyberspace visant à saboter leurs activités sensibles. Les cyberattaques visant les infrastructures critiques (énergie, santé, transports, eau, télécommunications, finance, etc.) sont nombreuses, continues et parfois très furtives, comme le soulignent les rapports des agences spécialisées.

Ce livre vise à répondre à des enjeux pédagogiques en renforçant la culture et la connaissance des objectifs, des orientations et du futur de la cybersécurité. Il met en lumière l'enjeu sectoriel, en rappelant la diversité des domaines concernés et la nécessité d'adapter les approches de sécurité à leurs spécificités techniques et organisationnelles. Il souligne l'importance stratégique de la cybersécurité pour la continuité des activités vitales de nos sociétés face aux menaces hybrides, illustrée par des exemples de crises cyber déjà survenues.

Il porte aussi un enjeu pratique d'implémentation de technologies de sécurité et de mise en oeuvre des meilleures pratiques actuelles de sécurité, alignée avec la Directive Network Information Security 2 (NIS2). Il aborde aussi l'enjeu technologique, en explorant l'intégration des innovations et les dépendances nécessitant la sécurisation des chaînes logistiques numériques.

■ ■ GS MAG : *En quoi votre livre peut-il aider les RSSI, les CISO, les DSI, les CIO, les DPO, les Responsables Cyber et Cybersécurité ?*

■ ■ EDS : Ce livre constitue un guide stratégique et opérationnel destiné aux responsables sécurité confrontés à la complexité croissante de la protection des infrastructures critiques. Il s'inscrit dans le mouvement de renforcement réglementaire européen, en s'appuyant sur la directive NIS 2, qui imposent des exigences de gouvernance, de gestion des risques et de résilience numérique, comme le Digital Operational Resilience Act (DORA) pour le secteur financier et le Cyber Resilience Act (CRA) pour les produits comportant des éléments numériques.

L'ouvrage permet d'aider les responsables à identifier les systèmes d'information sensibles, à distinguer ceux relevant du périmètre réglementaire et ceux à exclure, à analyser les menaces auxquelles ils sont exposés et leurs vulnérabilités, et à mettre en oeuvre une démarche structurée d'appréciation et d'analyse des risques fondée sur les principales méthodes et norme internationale (EBIOS-RM, ISO 27005:2022, NIST SP 800-30). Il expose des principes de gouvernance, les mécanismes de protection et de défense, ainsi que les mesures de résilience, de continuité d'activité et de gestion de crise adaptées aux systèmes d'informations spécifiques de pilotage des infrastructures critiques. Le livre fournit ainsi aux décideurs une vision intégrée de la cybersécurité, reliant exigences réglementaires, réalités techniques, mesures organisationnelles et enjeux stratégiques.

■ ■ GS MAG : *Quels sont vos messages pour nos lectrices et lecteurs (RSSI / CISO / DSI / CIO / DPO / Responsables Cyber et Cybersécurité...) ?*

■ ■ EDS : Le premier message porté par ce livre est la portée stratégique de la cybersécurité : arrêt d'activités essentielles pour les citoyens, perte de confiance dans le numérique, dégradation de l'image de l'entité, risques juridiques et financiers majeurs. La cybersécurité n'est plus une option, mais un impératif stratégique pour garantir la continuité des infrastructures critiques et la sécurité nationale. Dans un contexte de numérisation accélérée, la dépendance des organisations à leurs systèmes d'information rend toute vulnérabilité exploitable et tout incident potentiellement systémique.

D'autre part, il faut souligner la nécessité d'une approche fondée sur la maîtrise des risques : les moyens sont limités, les journées ne font que 24h. Comprendre les menaces, identifier les vulnérabilités et évaluer les impacts est indispensable pour prioriser les efforts et adapter les mesures de sécurité. Le livre met en avant les principaux référentiels – NIS 2, LPM 2018, ISO 27001:2022-AnnexeA, NIST CSF 2 – comme leviers de structuration, de cohérence et de sécurité minimale à mettre en oeuvre.

Un troisième message important concerne la gouvernance de la cybersécurité : celle-ci doit être intégrée aux processus de décision stratégique de l'entité, soutenue par la direction générale afin d'anticiper les menaces dans des activités fortement dépendante du numérique. La sécurité n'est pas seulement une affaire technique, mais un facteur de résilience organisationnelle et de performance durable.

Enfin, le livre invite à développer une culture partagée de cybersécurité, fondée sur la formation, la coopération et la vigilance collective. La protection des infrastructures critiques repose sur la capacité des acteurs à anticiper, détecter, réagir et apprendre en continu face à un paysage des menaces en constante évolution. ■

*Président Inaty
Associé de Qorum
Secur'Num
Architecte en
Cybersécurité*



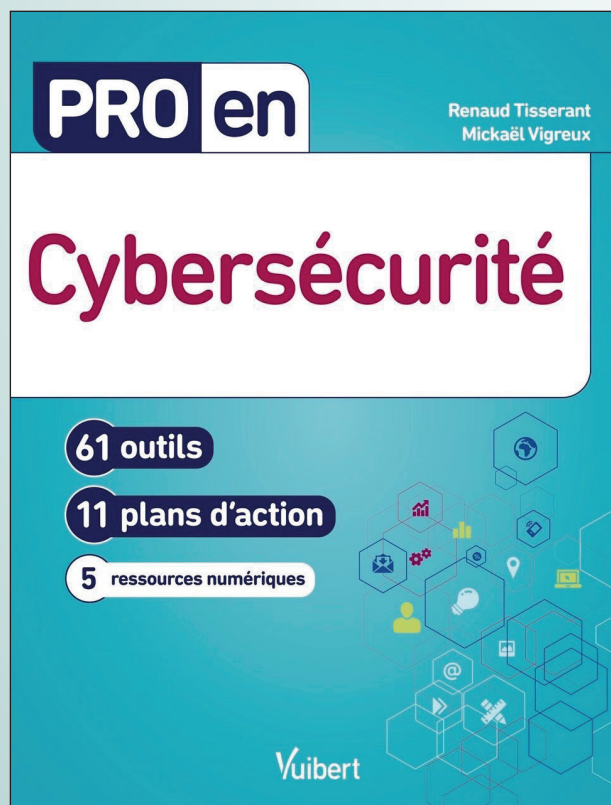
RENAUD TISSERANT



*Responsable
Commercial
de l'Afnic
Expert en
visibilité et
stratégie Web*

MICKAËL VIGREUX

LIVRE CYBER : *PRO EN CYBERSÉCURITÉ /* *PRÉFACE ANNE LE HÉNANFF*



■ ■ **GS MAG :** *Quel est le contexte et quels sont les enjeux de votre livre ?*

■ ■ **RT & MV :** « Pro en Cybersécurité » s'inscrit dans un contexte où la cybersécurité est devenue une priorité stratégique pour les organisations et pour la protection de nos infrastructures et de nos données.

Face à la montée des attaques - menées par des acteurs étatiques, mafieux, cybercriminels opportunistes ou encore des groupes hacktivistes - la protection des infrastructures et des données n'est plus négociable.

La pression réglementaire s'intensifie, du RGPD à NIS 2, en passant par DORA et le Cyber Resilience Act (CRA). Cette évolution rapide impose une veille continue, une anticipation des obligations actuelles et à venir afin d'avoir une mise en conformité proactive - plutôt que subie - de l'ensemble des organisations.

Pour y répondre, l'ouvrage propose 61 fiches outils et 11 plans d'action. Méthodes pas à pas, check-lists et scénarios de réponse aux incidents y offrent des repères concrets pour comprendre, anticiper et réagir face aux risques cyber. Surtout, le livre rappelle tout au long de la lecture que la cybersécurité n'est plus de la responsabilité unique d'un cercle de spécialistes :

elle relève désormais d'une responsabilité collective, du comité exécutif aux équipes opérationnelles, en passant par les équipes terrain, les acteurs étatiques et les partenaires.

■ ■ **GS MAG** : *En quoi votre livre peut-il aider les RSSI, les CISO, les DSI, les CIO, les DPO, les Responsables Cyber et Cybersécurité ?*

■ ■ **RT & MV** : Le livre s'adresse aussi bien aux RSSI, CISO, DSI, CIO, DPO et autres responsables d'organisations dans leur quotidien.

Il propose surtout une approche pragmatique, avec un jargon limité, afin de permettre aux profanes de comprendre les enjeux, d'acquiescer les bonnes pratiques essentielles et de passer à l'action.

Il est autant l'ouvrage pour une personne du sérail que le guide de survie que l'on pourra offrir à ses responsables pour les sensibiliser au sujet et leur donner les codes afin de comprendre les enjeux, les contraintes et les opportunités de la cybersécurité.

Cela doit leur permettre d'emmener l'ensemble des parties prenantes à passer de spectateurs à acteurs et partenaires proactifs.

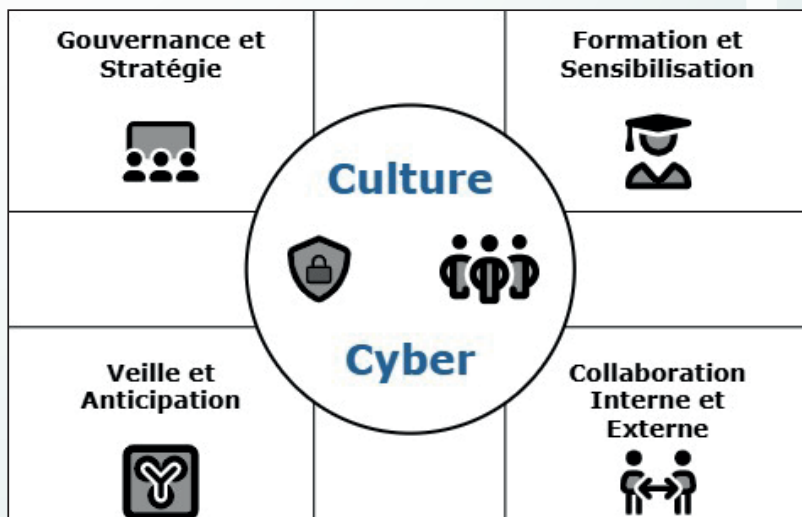
Les ressources fournies, incluant les contributions de douze expertes et experts, donnent une vision à 360 degrés sans entrer dans le dur de la technologie.

Il est impératif que le sujet soit appréhendé par l'ensemble des équipes et organes dirigeants. Cela passe par des actions d'information et de sensibilisation, auxquelles des supports comme « Pro en Cybersécurité » contribuent.

■ ■ **GS MAG** : *Quels sont vos messages pour nos lectrices et lecteurs (RSSI / CISO / DSI / CIO / DPO / Responsables Cyber et Cybersécurité...) ?*

■ ■ **RT & MV** : Les messages sont nombreux, mais nous souhaitons en partager trois :

- 1. La donnée la plus sûre est celle que l'on n'a pas ou à laquelle on n'a pas accès** : la sobriété numérique (isolation des archives, suppressions à la date d'obsolescence des anciennes données, etc.) et de bonnes pratiques (principe du moindre accès, isolation et compartiments étanches entre les composants de votre infrastructure, etc.) sont des fondements limitant l'impact d'un incident.
- 2. Les réglementations comme NIS 2, DORA et le CRA** ne doivent pas être appréhendées comme des contraintes mais comme des opportunités pour améliorer la sécurité globale, la compétitivité et apporteront alors un véritable avantage concurrentiel.
- 3. La cybersécurité est une responsabilité partagée, commune et intriquée** entre l'ensemble des acteurs internes et externes d'une organisation : des équipes métier au PDG, des fournisseurs aux clients - autant partenaires que vecteurs de risques -, mais aussi l'écosystème numérique français et européen. ■



MOUNTAHA
NDIAYE

*EMEA Director
Ecosystem Sales and
Programs Hyland_CPI-B2B*



RETEX NIS 2, DORA, CRA, ISO 27001, RGPD, LA CONFORMITÉ ET LA CYBERSÉCURITÉ

■ ■ **GS MAG** : Selon vous, quels sont les défis lorsqu'il s'agit d'associer la Conformité à la Cybersécurité ?

■ ■ **MN** : L'association de la conformité et de la cybersécurité représente un choc de cultures. D'un côté, la conformité impose des cadres stricts – RGPD, NIS2, DORA, ISO 27001 ou le futur Cyber Resilience Act – autant de référentiels qui structurent et responsabilisent

De l'autre, la cybersécurité opérationnelle doit contrer des menaces évolutives et imprévisibles. Le risque est de tomber dans une approche « boîte à cocher », en se concentrant sur la conformité formelle plutôt que sur la protection réelle.

Le défi consiste donc à aligner ces deux dimensions : faire de la conformité un levier de résilience, et non une contrainte. Cela requiert un changement de paradigme. Historiquement, nous protégeons avant tout un périmètre : nous bâtissons des murailles techniques autour du système d'information, à la façon d'un château-fort. Mais cette mentalité périmétrique ne suffit plus à l'ère du cloud et de la donnée volatile.

Aujourd'hui, le véritable « périmètre » de sécurité, c'est l'information elle-même. Nous devons donc protéger chaque donnée, où qu'elle se trouve, plutôt que de compter uniquement sur des frontières réseau. En recentrant la sécurité sur l'information – et non sur de simples périmètres – nous répondons aux exigences de conformité tout en renforçant notre capacité de défense face aux cybermenaces.

■ ■ **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 une Conformité et une Cybersécurité au mieux possible ? Et pour quelles raisons ?*

■ ■ **MN** : Nous avons adopté une approche « data-centric » de la cybersécurité. Concrètement, nous classons rigoureusement les informations selon leur sensibilité, avec pour chaque catégorie des protections adaptées. Par exemple, lors d'une collaboration avec l'armée française, nous avons chiffré tous les documents sensibles et restreint les accès aux seuls habilités. Même en cas d'intrusion, la donnée critique restait illisible : un garde-fou indispensable à une époque où les périmètres techniques ne suffisent plus.

Nous appliquons également le principe Zero Trust – ne jamais faire confiance par défaut, toujours vérifier – qui réduit la surface d'attaque en n'autorisant que les accès légitimes. Cette démarche répond aussi bien aux obligations réglementaires (contrôle des accès d'ISO 27001) qu'aux impératifs de sécurité opérationnelle.

Nous intégrons la sécurité et la conformité dès la conception : plutôt que d'ajouter des contrôles après coup, nous incluons d'emblée les exigences légales dans les processus. Ainsi, les systèmes sont conformes et résilients par conception, sans nécessiter de coûteux correctifs ultérieurs.

Enfin, nous faisons collaborer étroitement juristes et techniciens. En cassant les silos, nous créons une synergie : la conformité guide les améliorations de sécurité, et la cybersécurité garantit une protection concrète des actifs, rendant la conformité réellement vivante et efficace.

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

■ ■ **MN** : Les cadres réglementaires et technologiques évolueront sans cesse, mais notre mission reste la même : protéger le capital informationnel. Pour y parvenir, nous maintenons une veille proactive sur chaque nouvelle obligation, en la considérant comme une occasion de renforcer notre dispositif. La récente PSSI-IA nous sert par exemple de guide pour adapter nos pratiques autour de l'intelligence artificielle, tandis que l'ère du quantique est anticipée : nous testons dès aujourd'hui le chiffrement post-quantique afin que nos données demeurent sûres demain.

S'adapter, c'est aussi faire évoluer en continu les compétences et la culture internes. Nous investissons donc dans la formation permanente des équipes et dans le partage d'expérience au sein de la communauté cyber pour garder une longueur d'avance. Enfin, nous abordons le changement avec un esprit visionnaire : plutôt que de le subir, nous cherchons à l'anticiper. En misant sur l'innovation et sur l'écoute des signaux faibles, nous transformons l'incertitude en une dynamique positive d'amélioration continue de la cybersécurité.

C'est dans cet esprit que nous avons conçu notre nouvelle plateforme Hyland Content Innovation Cloud (CIC), forgée entièrement sur une base agentique. Elle permet d'orchestrer, en temps réel, des agents intelligents capables d'interagir avec l'information, d'en évaluer le contexte et de déclencher automatiquement les protections adéquates. La sécurité ne se contente plus d'observer : elle agit, prévient et s'adapte à la vitesse de la donnée. ■

L'association de la conformité et de la cybersécurité représente un choc de cultures.

LAURENT
VANEL

*Directeur Technique des
Solutions d'Infrastructures
chez IBM France_Cybersécurité
secteur santé*



CYBERSÉCURITÉ DANS LE SECTEUR DE LA SANTÉ : CONSTATS ET DÉFIS

IL Y A QUELQUES ANNÉES,
ON AVANÇAIT DE MANIÈRE
PROVOCATRICE QUE LA
QUESTION N'ÉTAIT PLUS SI L'ON
SERAIT ATTAQUÉ, MAIS QUAND
ET COMMENT RÉAGIR.
AUJOURD'HUI, CE CONSTAT EST
DEvenu RÉALITÉ :
LE SECTEUR DE LA SANTÉ,
AVEC SES INFRASTRUCTURES
CRITIQUES ET SES DONNÉES
SENSIBLES, N'ÉCHAPPE PAS
AUX CYBERATTAQUES,
DÉSORMAIS UNE MENACE
SYSTÉMIQUE.

L'explosion des **dispositifs médicaux connectés** accroît la vulnérabilité des établissements. Si les dossiers médicaux électroniques sont souvent bien protégés, de nombreux dispositifs restent exposés, qu'ils soient anciens ou conçus sans sécurité intégrée. Cette fragilité peut être partiellement compensée par des **solutions de gestion centralisée des appareils**, semblables aux systèmes utilisés pour sécuriser smartphones et tablettes. Elles permettent de contrôler les mises à jour, configurer les paramètres de sécurité, surveiller les vulnérabilités et appliquer des correctifs à distance.

Les systèmes de santé modernes sont caractérisés par **une interopérabilité complexe** entre appareils, applications et réseaux. Chaque connexion représente une surface d'attaque, et assurer une communication sécurisée en toutes circonstances constitue un défi permanent.

Le **manque de compétences spécialisées** aggrave le problème : de nombreux établissements ne disposent pas des ressources internes pour surveiller, évaluer ou répondre efficacement aux cyberattaques. Le coût des violations de données reste particulièrement élevé dans ce secteur. À cela s'ajoute **une pression réglementaire accrue**, avec des cadres comme le HIPAA, le RGPD et les normes relatives aux dispositifs médicaux, imposant une vigilance constante sur la protection des informations sensibles.

STRATÉGIES ET BONNES PRATIQUES

Plusieurs approches sont essentielles :

- L'architecture **Zero Trust** qui consiste à ne jamais faire confiance automatiquement et à vérifier en continu identités et permissions.
- Le principe de **Secure-by-Design** qui recommande d'intégrer la sécurité dès la conception des dispositifs médicaux, y compris les mises à jour et la robustesse des systèmes.
- L'**intelligence artificielle** et l'**automatisation** qui permettent la **détection des attaques en temps réel** et la **restauration automatique de copies saines des données**, limitant ainsi l'impact sur les systèmes et les patients.
- La surveillance continue, le patch management et une **gouvernance forte** — politiques claires, plans de réponse aux incidents et audits.

SÉCURITÉ DES PATIENTS ET FORMATION

La cybersécurité dépasse le cadre informatique : elle protège directement la **sécurité des patients**. Une attaque sur un dispositif médical peut avoir des conséquences graves sur leur vie. La sécurité doit être intégrée à la **stratégie globale de transformation numérique**, et non reléguée au service informatique. Le secteur doit investir dans la **formation** de profils spécialisés en cybersécurité et IA, incluant des programmes pour personnes en reconversion ou jeunes éloignés du système scolaire.

CONFORMITÉ ET HÉBERGEMENT DES DONNÉES

La protection des données repose sur des normes strictes : elles doivent être hébergées par des structures certifiées, et tous les acteurs, y compris les fournisseurs cloud et les prestataires externes, doivent s'y conformer. Le RGPD et les directives nationales sur la sécurité des systèmes critiques encadrent l'ensemble du secteur.

TENDANCES ET PERSPECTIVES

Le secteur reste une **cible privilégiée**, combinant données sensibles, délais critiques et infrastructures complexes héritées de systèmes anciens. Les **ransomwares** dominent les attaques : récemment, une nouvelle version de **LockBit** a été identifiée, alors que l'on pensait le problème maîtrisé, illustrant la nature **sans fin de cette lutte**, où les cybercriminels exploitent les avancées de l'IA pour déployer des attaques toujours plus sophistiquées.

Les vulnérabilités varient selon les régions, le niveau d'investissement numérique et la gouvernance IT. Les attaques via des tiers ou fournisseurs externes augmentent, rendant la sécurité de la **chaîne logistique** indispensable. L'automatisation, la détection en temps réel et la restauration rapide des données sont désormais **cruciales** pour limiter l'impact des attaques, assurer la continuité des soins et protéger les informations sensibles.

En France, **348 000 atteintes numériques** ont été recensées en 2024¹, soit une hausse de 74 % sur cinq ans, soulignant l'urgence de stratégies robustes et globales pour sécuriser les systèmes de santé et la vie des patients. ■

Les systèmes de santé modernes sont caractérisés par une interopérabilité complexe entre appareils, applications et réseaux.

¹ Source: https://www.interieur.gouv.fr/actualites/communiqués-de-presse/publication-du-rapport-annuel-relatif-a-cybercriminalite?utm_source=chatgpt.com

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*



CYBERSÉCURITÉ : QUAND LA NORME DEVIENT LA LOI

**LA CYBERSÉCURITÉ S'EST TRANSFORMÉE EN UN VÉRITABLE
LABYRINTHE RÉGLEMENTAIRE : RGPD, NIS2, DORA, CRA, AI ACT...
SANS PARLER DES RÉFÉRENTIELS ET CERTIFICATIONS (ISO 27001,
SECNUMCLOUD, EUCS...).**

Face à cette prolifération, les professionnels du secteur peinent parfois à distinguer ce qui relève d'une obligation légale, d'une bonne pratique, ou d'une simple recommandation.

Cette coexistence entre le "droit dur" (hard law), composé de règles juridiquement obligatoires, et le "droit souple" (soft law), constitué de recommandations, lignes directrices ou standards de bonnes pratiques, contribue à complexifier la lecture du cadre normatif applicable en matière de cybersécurité.

Le "droit souple" n'a pas de valeur contraignante au sens strict, mais il exerce une force normative indirecte : il influence les décisions du juge judiciaire et des autorités de contrôle et constitue une garantie de sécurité juridique pour les acteurs économiques.

Si le droit souple se développe autant en cybersécurité, c'est parce que les entreprises font face à une inflation de textes législatifs sans toujours savoir comment les appliquer concrètement.

Le Principe d'accountability du RGPD illustre cette difficulté : il fait reposer sur les organismes et non plus sur le régulateur, la responsabilité d'être conforme aux lois en vigueur, en documentant cette conformité en interne.

Les normes et référentiels viennent apporter un peu plus de sécurité juridique, avec un tampon non pas du régulateur mais d'organismes dit « certificateurs ».

Ces normes ne sont donc pas des lois, mais elles peuvent influencer des juges ou des autorités de contrôle (1), elles peuvent également devenir la loi des parties si elles sont intégrées ou visées au contrat (2).

ISO, ANSSI, CIS, SecNumCloud, HDS... Tous se présentent comme des gages de sécurité, mais aucun n'a, à lui seul, valeur de loi.

1_ LA NORME N'EST PAS LA LOI

Le marché de la cybersécurité est désormais saturé de référentiels et standards : ISO, ANSSI, CIS, SecNumCloud, HDS... Tous se présentent comme des gages de sécurité, mais aucun n'a, à lui seul, valeur de loi.

Au côté des guides et bonnes pratiques de l'Agence Nationale de Sécurité des Systèmes d'Information (ANSSI), les référentiels les plus répandus sont ceux édictés par l'Organisation Internationale de Normalisation (ISO) et la Commission Électrotechnique Internationale (IEC) et qualifié de « normes ISO ».

La norme ISO/IEC 27001, par exemple, tient en une trentaine de pages et définit les exigences pour instaurer un système de management de la sécurité de l'information (SMSI). Elle impose une logique de gestion des risques, d'amélioration continue et de documentation des mesures de sécurité, mais son application reste volontaire.

Aucune entreprise n'est juridiquement tenue de s'y conformer. Pourtant, le juge ou l'expert judiciaire s'y réfère de plus en plus souvent pour apprécier la "règle de l'art" en matière de sécurité.

Ainsi, en cas d'incident ou de litige (en malfaçon par exemple), l'absence de conformité à ces référentiels peut être interprétée comme un manquement à l'état de l'art, notamment pour les prestataires informatiques ou hébergeurs de données sensibles.

Il en va de même pour les autorités de contrôle comme la CNIL, qui contrôlent les organismes, et qui souvent, demandent à ce que soient respectées leurs recommandations (soft law) comme gage de bonnes pratiques ... sous peine de sanction. Il est alors fortement recommandé de se conformer au Guide de Sécurité de la CNIL, ou à la norme ISO27001, pour prouver le respect de l'obligation de sécurité imposée par l'article 32 du Règlement UE n°2016/679 dit « RGPD ».

On voit donc aujourd'hui que même si ces normes et recommandations ne sont pas des Lois, leur non-respect risque tout de même de mener indirectement à des sanctions judiciaires, ou administratives.

2_ LA NORME PEUT ÊTRE LA LOI DES PARTIES

Lorsqu'une norme est intégrée ou visée dans un contrat, elle acquiert une valeur contractuelle, c'est-à-dire une valeur juridique contraignante entre les parties signataires du contrat.

La norme pourra être formellement intégrée au contrat. Elle sera alors annexée. Mais le plus souvent, dans les contrats entre professionnels, la norme sera très précisément identifiée aux articles du contrat, et viser. L'effet juridique sera le même que dans le premier cas. Le non-respect de la norme équivaudra à un manquement au contrat. Bien évidemment, le plus souvent, ce sera le client qui aura intérêt à intégrer ou viser une norme au contrat qui le lie à un prestataire.

En mentionnant par exemple la conformité à ISO 27001 ou SecNumCloud dans un cahier des charges ou un DPA (Data Processing Agreement), le prestataire s'engage contractuellement à respecter les exigences correspondantes.

Dès lors, le non-respect de la norme peut constituer un manquement contractuel, voire un manquement à une obligation de résultat.

Mais ce levier contractuel a ses limites : certaines entreprises, désireuses de rassurer leurs clients ou d'obtenir un marché stratégique, acceptent des exigences disproportionnées (par exemple, certification ISO 27001 "complète" pour un simple développement logiciel, ou SecNumCloud pour un hébergeur tiers).

Cette surenchère normative expose les prestataires à un risque de non-conformité contractuelle, voire à une mise en cause de responsabilité en cas d'incident.

En pratique, tout est une question d'équilibre et de rapport de force : la norme peut sécuriser la relation contractuelle lorsqu'elle est bien calibrée, ou au contraire devenir une source de contentieux si elle est appliquée sans discernement.

En conclusion, le *soft law* s'impose aujourd'hui comme une porte de sortie face à une inflation réglementaire qui n'est pas toujours très claire sur les engagements techniques et organisationnels exigés des organisations et des entreprises. Mais les normes sont elles-mêmes parfois rédigées en termes généraux et donc sujet à interprétation.

La vraie maturité « cyber » consistera à choisir les bons référentiels, au bon niveau, pour les bons risques, compris de tous, client et prestataire, sans tomber ainsi dans une conformité de façade qui peut créer plus d'insécurité juridique qu'elle n'en résout.

C'est à cette condition que la norme renforce la sécurité... sans devenir la loi par défaut. ■



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

JEAN-PIERRE
LA HAUSSE
DE LALOUVIÈRE

*Président eFutura
Directeur Général
France Intalio*



eFutura, ASSOCIATION PROFESSIONNELLE INDÉPENDANTE

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

Les adhérents rejoignent **eFutura** pour participer à l'évolution des normes au niveau Français (AFNOR Normalisation et AFNOR Certification), Européen (CEN et ETSI) et International (ISO) : Archivage électronique, Cyber-sécurité, Facture électronique, Gestion de Documents, Gouvernance de l'information, Numérisation, Intelligence artificielle.

Nous réalisons des événements, Petits-déjeuners, Dîners-conférences, Tables-rondes et Webinaires dans différents domaines complexes générés par la transition numérique.

Enfin, eFutura est un Think Tank de réflexion sur les enjeux sociétaux du numérique.

La Cybersécurité est un axe fondamental pour la sécurité des acteurs économique face aux menaces multiples qui ne cessent de croître : états, mafias, individus.

Les Cyberattaques ne préviennent pas : elles frappent, bloquent, volent et détruisent.

Phishing, Ransomwares, Malware, Attaques DDoS, usurpations d'identité, Vol de données, fraudes à l'IA... chaque jour, elles gagnent en fréquence et en sophistication.

>>>

>>> En 2023, 330 000 attaques ont visé des PME et ETI françaises, pour un coût moyen de 130 000 € chacune. Une seule intrusion peut arrêter vos opérations, vider vos comptes, exposer vos données et briser la confiance de vos clients.

Nous sommes tous des cibles potentielles. Mais les dirigeants d'entreprises ont une responsabilité particulière : responsabilité juridique, sanctions, réputation compromise.

En Europe, des réglementations, directives, normes ont été, sont mises en place pour contraindre les états membres et donc les entreprises à mettre en place des mesures de sécurité afin de garantir une résilience opérationnelle face aux incidents majeurs, et sanctionner sévèrement la non-conformité :

- **Cyber Security Act** qui définit le cadre de la cybersécurité en Europe,
- **DORA** (Digital Operational Resilience Act) pour le secteur financier européen et ses sous-traitants,
- **Directive NIS 2** (Network and Information Security Directive) pour la gouvernance de la cybersécurité. Elle concerne les entités des secteurs jugés essentiels ou importants soit environ 15.000 organisations en France dans 18 secteurs d'activité. Mais attention, les sous-traitants peuvent également être concernés,
- **Règlement CRA** (Cyber Resilience Act) pour les produits numériques (logiciels, objets connectés, ...),
- **Directive REC** (Résilience des Entités Critiques) pour la gestion des menaces physiques des infrastructures critiques,
- **ISO 27001**, systèmes de management de la sécurité de l'information (SMSI).

Ces réglementations, directives, normes ne sont pas faites pour pénaliser les entreprises mais au contraire, pour prévenir des dangers qui eux vont grandement les pénaliser le jour où elles seront attaquées !

Associer la conformité à la cybersécurité est donc essentielle. Cela passe notamment par la formation en cybersécurité des dirigeants, par la mise en place d'une veille technologique et réglementaire, par le choix de solutions conformes et souveraines.

Chez eFutura, nous sommes totalement sensibilisés et engagés dans les réflexions et dans la diffusion d'informations pour la mise en place de stratégies Cyber. Un Groupe de Travail composé de membres divers : éditeurs de logiciels, hébergeurs, consultants, associations spécialisées réalise un livret Cyber à destination des directions et des COMEX qui ont besoin de mieux comprendre les enjeux des régulations européennes, des risques, des sanctions ... auxquelles leur organisation doit faire face. Il sera disponible gratuitement en téléchargement sur le site www.efutura.fr en décembre 2025. Il est préfacé par le Général Marc WATIN-AUGOUARD, créateur de Forum InCyber.

La cybersécurité n'est plus une option. Ce doit être une décision stratégique au niveau des COMEX !

La Cybersécurité est un axe fondamental pour la sécurité des acteurs économique face aux menaces multiples qui ne cessent de croître : états, mafias, individus.

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

TeaLenium

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

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

PRIVILEGED ACCESS / WORKFORCE ACCESS / ACCESS GOVERNANCE



wallix

Évoluez librement dans un monde numérique plus sûr

Libres et maîtres de vos systèmes, avec WALLIX vous opérez dans des environnements numériques et industriels où la sécurité ne freine pas vos activités. WALLIX sécurise les identités et accès afin de protéger vos actifs critiques face aux cybermenaces et de fluidifier vos interactions avec vos fournisseurs et vos clients. Leader Européen de la gestion des comptes à privilèges, WALLIX simplifie la mise en œuvre de la conformité et améliore l'efficacité opérationnelle des entreprises.

Avec WALLIX, vous bâtissez un monde numérique plus sûr pour innover, collaborer et grandir sans compromis.

www.wallix.com