N°59
PRIX : 24€ TTC
TRIMESTRIEL
MAI > JUILLET 2025

Global Security Mag

THE LOGICAL & PHYSICAL SECURITY MAGAZINE

Dossier spécial

LES NOUVELLES TECHNOLOGIES (IA, QUANTIQUE, SASE, SOAR, XDR, ZERO TRUST...) ET 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

Interviews

Maria Iacono
Directrice des Assises de la Cybersécurité et Ready For IT, Comexposium One to One

Gérôme Billois
Membre du CA Clusif et CoAnimateur GT Panocrim + Partner Cybersecurity and Digital Trust, Wavestone + Auteur : CYBERATTAQUES, les Dessous d'une Menace Mondiale

OFFERT PAR

FÉDÉRATION FRANÇAISE DE LA CYBERSÉCURITÉ
FFCYBER

LA SOUVERAINETÉ AU COEUR DE NOTRE ADN

LLMaaS

Mistral AI

OUTSCALE KUBERNETES AS A SERVICE

Cloud Public SecNumCloud 3.2

VISA DE SÉCURITÉ ANSSI

OUTSCALE

outscale.com

EDITO

LE RÔLE PRINCIPAL DE LA CYBERSÉCURITÉ EST DE GARANTIR LA CONFIDENTIALITÉ, L'INTÉGRITÉ, ET LA DISPONIBILITÉ DES INFORMATIONS OU DES DONNÉES.

Les évolutions permanentes des Nouvelles Technologies (IA, QUANTIQUE, SASE, SOAR, XDR, ZERO TRUST...) sont-elles des menaces ou des opportunités pour la Cybersécurité ?

Il est établi que l'Information est une notion fondamentale et structurelle pour les interactions entre les individus dans nos sociétés, pour les Entreprises, les Organisations, les États, les Infrastructures, les Réseaux de Communication, les Systèmes Informatiques et Systèmes d'Informations.

L'Information est donc un enjeu essentiel, comme le rappelle l'Historien Yuval Noah Harari dans son livre « NEXUS » où il raconte comment les révolutions de l'Information ont transformé nos sociétés.

Des livres anciens à l'Intelligence Artificielle, l'Information est devenue à tel point sensible, qu'elle est l'un des enjeux primordiaux des luttes d'influence, des batailles géopolitiques et concurrentielles dans l'économie.

Le Chercheur David Colon, dans la nouvelle édition de son livre intitulé « La Guerre de l'Information », parle notamment de Cyberguerre et de Désinformation.

Les Nouvelles Technologies sont un vecteur clé de l'Information, elles accompagnent la transformation numérique, et leurs évolutions permanentes exigent une capacité d'adaptation continue. Les opportunités générées ne sont pas sans impliquer de vrais défis, notamment en matière de Cybersécurité.

Les différentes pages qui vont suivre ne vous laisseront pas sans réflexions.

Valentin Jangwa

THE MAIN ROLE OF CYBERSECURITY IS TO ENSURE THE CONFIDENTIALITY, INTEGRITY, AND AVAILABILITY OF INFORMATION OR DATA

Are the permanent evolutions of New Technologies (AI, QUANTIQUE, SASE, SOAR, XDR, ZERO TRUST...) threats or opportunities for Cybersecurity?

As a matter of fact, Information is a fundamental and structural notion for interactions between individuals in our societies, for Companies, Organizations, States, Infrastructures, Communication Networks, Computer Systems and Information Systems.

Information is therefore an essential issue, as historian Yuval Noah Harari reminds us in his book "NEXUS", in which he recounts how information revolutions have transformed our societies.

From ancient books to Artificial Intelligence, Information has become so sensitive that it is one of the key issues in the struggle for influence, and in geopolitical and competitive battles in the economy.

Researcher David Colon, in the new edition of his book entitled "Information Warfare", speaks of Cyberware and Disinformation in particular.

New technologies are a key vector of information, accompanying the digital transformation, and their constant evolution demands a capacity for continuous adaptation.

The opportunities generated are not without their challenges, especially in terms of cybersecurity.

The following pages will leave you with plenty to think about.

Valentin Jangwa

N°59 MAI>JUILLET 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 Imprim'vert selon le procédé CTP sans chimie

16e édition

GS Days

LES JOURNÉES FRANCOPHONES DE LA SÉCURITÉ DE L'INFORMATION ET DE LA CYBER

20/01/26

Espace Saint-Martin · paris 3e

PROGRAMME À VENIR

INSCRIPTION SUR WWW.GSDAYS.FR

SOMMAIRE

SUMMARY

>MAI<

■ **3 > 4 mai • Madrid (Espagne)**
Eurocrypt
www.eurocrypt.iacr.org/2024

■ **5 mai • Arlington Gateway, VA (USA)**
CMMC Day
Westin Arlington Gateway, VA
www.cmmcday.org

■ **6 mai • Maryland (USA)**
CSfC Conference
The Hotel at the University of MD, College Park, Maryland, USA
www.certinfosec.org

■ **6 mai • Maryland (USA)**
Federal Certification Events Week
The Hotel UMD, College Park, MD
Cet événement inclut :
Cybersecurity Maturity Model Certification (CMMC) Day

The future of federal supply chain security
www.CMMCDay.org

Common Criteria Day
The future of the global certification standard in the federal space
www.CriteriaDay.org

Commercial Solutions for Classified (CSfC) Conference
Surveying the effort to leverage leading technology for national security
www.CertInfoSec.org

Department of Defense Information Network Approved Product List (DoDIN APL) Day
A comprehensive look at DoD Information Network technology certification
www.DoDINDay.com

Cyber Trust Mark Day
Preparing ICT product developers for the coming US cybersecurity certification and labeling program
www.TrustMarkDay.org

■ **6 > 8 mai • Dubaï**
GISEC
www.gisec.ae/

■ **7 mai • Munich (Allemagne)**
Technology Live ! Germany
www.a3communicationspr.com/homepage/events/technology- live/

■ **7 > 9 mai • Taipei (Taïwan)**
Secutech
www.secutech.com

■ **13 > 15 mai • Barcelone (Espagne)**
Barcelona Cybersecurity Congress
www.barcelonacybersecuritycongress.com/

The IOT Solutions World Congress (IOTSWC)
www.iotsworldcongress.com/

■ **13 > 16 mai • Marrakech (Maroc)**
SIT Africa
Palmeraie Resort à Marrakech
https://sit.africa/

■ **13 > 15 mai • United Arab Emirates**
Wolrd Police Summit
Dubai Exhibition Centre Expo 2020
www.worldpolicesummit.com/

■ **14 > 15 mai • Copenhague (Danemark**
Infosecurity Denmark
www.v2security.dk/

■ **14 > 16 mai • Deauville (France)**
Le Symposium du CRiP
Le Rendez-vous annuel des Décideurs IT
www.crip-asso.fr/events

■ **15 mai • Munich (Allemagne)**
Technology Live ! France
www.a3communicationspr.com/homepage/events/technology-live/

■ **19 > 22 mai • Saint-Tropez**
RIAMS
www.les-riams.fr/

■ **19 > 22 mai • Houston (TX) (USA)**
XPONENTIAL
George R. Brown Convention Center
www.auvsi.org/events/xponential/auvsi-xponential-2025

■ **20 > 21 mai • Las Vegas (USA)**
Industrail Cyber Show
www.akjassociates.com/

■ **20 > 22 mai • Monaco**
Ready For IT
Organisateur : Comexposium et DG Conseils
www.ready-for-it.com

■ **21 > 22 mai • Bruxelles (Belgique)**
CyberSec
Lieu : Brussels Expo
www.cyberseceurope.com

■ **21 > 23 mai • Berlin (Allemagne)**
GITEX Europe
www.gitex-europe.com/

■ **21 > 23 mai • Piacenza (Italie)**
CYBSEC-EXPO
Piacenza Expo
www.cybsec-expo.it/

■ **23 mai • Online**
Conférence AFCDP
www.universite-des-dpo-2025.afcdp.net/page/c101-accueil/

■ **27 mai - Paris**
e-crime;& cybersecurity France
www.akjassociates.com/

> JUIN <

- **2 juin • Paris**
  USI
  https://www.usievents.com/fr/
- **2 > 4 juin • Paris**
  Paris Cyber Week
  www.paris-cyber-week.co
- **2 > 5 juin • Vancouvert (Canada)**
  MAAWG General Meeting
  www.m3aawg.org
- **3 > 4 juin • Boston, Massachusetts (USA)**
  HealthSec
  www.cs4ca.com
- **3 > 5 juin • Londres (UK)**
  Infosecurity Europe
  ExCeL London
  Renseignements :
  Reed Exhibitions UK
  Tél. : +44 (0)20 8271 2130
  E-mail :
  infosecurity.helpline@reedexpo.co.uk
  www.infosec.co.uk
- **3 > 5 juin • Cannes (France)**
  DataCloud Europe
- **3 juin Pre-event**
  Renseignements :
  E-mail : enquiries@datacentres.com
  www.events.broad-group.com/event/a4ba77f1-52e2-4570-a6f5-d442cd3eca93/summary
- **3 > 5 juin • Wilmington, NC (USA)**
  Techno Security & Forensics Investigations Conference & Mobile Forensics World
  https://www.technosecurity.us/mb
- **3 > 5 juin • Johannesburg (Afrique du Sud)**
  Securex South Africa
  Lieu : Gallagher Convention Centre
  www.securex.co.za
- **4 > 5 juin**
  Marseille
  AccesSecurity
  Parc Chanot
  http://accessecurity.fr/

  Francfort (Allemagne)
  TechShow - Cloud Expo Europe
  www.techweekfrankfurt.de

  Londres (UK)
  GEO Business
  www.geobusinessshow.com

  Santa-Clara - CA (USA)
  Cyber Security & Cloud Expo
  www.cybersecuritycloudexpo.com/northamerica/
- **4 > 6 juin • Rennes (France)**
  SSTIC
  www.sstic.org
- **10 > 11 juin • Galgary (Canada)**
  CS4CA Canada
  www.cs4ca.com
- **10 > 12 juin • Paris**
  Préventica
  https://www.preventica.com/participer.php
- **11 > 14 juin • Paris**
  Vivatech
  https://vivatechnology.com/
- **16 > 17 juin • Paris**
  Les Universités CRIP
  https://www.crip-asso.fr/events
- **17 > 20 juin • Marrakech (Maroc)**
  SIT AFRICA - CyberSecurity Forum
  https://sit.africa/
- **17 > 18 juin • Paris-Châtillon**
  Conférence annuelle d'OW2
  Orange Gardens
  44 Avenue de la République,
  92320 Châtillon
  www.ow2con.org
- **18 > 19 juin • Londres (UK)**
  SCTX - Counter Terror Expo
  Lieu : ExCel London
  Contact : Nicola Greenaway
  Tel. : + 44 (0) 208 542 9090
  Fax : + 44 (0) 208 542 9191
  E-mail : ngreenaway@niche-events.com
  https://ctexpo.co.uk/
- **24 juin • Munich (Allemagne)**
  e-crime & cybersecurity Germany
  https://akjassociates.com/
- **24 > 26 juin • Le Mans (France)**
  Congrès National SSI Santé
  Contact : secretaire@apssis.com
  www.apssis.com
- **25 juin • Paris**
  Diner du Cercle de la sécurité
  www.lecercle.biz

> JUILLET <

- **5 juillet • Londres (UK)**
  Securing Financial Services
  https://akjassociates.com
- **24 juillet • Johannesburg (Afrique du Sud)**
  7th Edition Connected Africa- Telecom Innovation & Excellence Awards 2025 (Africa's Premier Telecom Summit)
  https://connected-africa.com/summit/

PAUL-OLIVIER GIBERT

Président, AFCDP et POG – consulting

IA CONVERSATIONNELLE

UN DÉFI URGENT POUR LA PROTECTION DES DONNÉES PERSONNELLES

COMMENT INSTAURER LA CONFIANCE SANS FREINER LE PROGRÈS ?

L'intelligence artificielle conversationnelle bouleverse notre quotidien. Outils de rédaction, assistants juridiques, chatbots intégrés aux services clients : ces technologies séduisent par leur efficacité. Pourtant, derrière leur apparente convivialité, ces IA posent des défis majeurs en matière de protection des données personnelles.

En tant que Délégués à la Protection des Données (DPD/DPO), nous voulons alerter : l'usage non encadré de ces outils peut sérieusement compromettre le respect des droits fondamentaux des individus.

DES COLLECTEURS DE DONNÉES AUSSI DISCRETS QU'EFFICACES

Les IA conversationnelles traitent des volumes massifs de données – noms, coordonnées, informations bancaires, détails de santé ou opinions personnelles – issues de leurs interactions avec les utilisateurs. Ces informations ne sont pas seulement utilisées pour améliorer les performances de l'IA.

Elles sont aussi stockées, parfois indéfiniment, souvent en dehors de l'Union européenne, dans des conditions peu claires. Et lorsqu'un utilisateur partage une donnée sensible sans y penser – une situation médicale, une difficulté professionnelle – il n'imagine pas toujours que cette donnée puisse nourrir un modèle utilisé à grande échelle.

LE MIRAGE DU CONSENTEMENT ÉCLAIRÉ

Bien trop souvent, l'utilisateur ignore ce qu'il accepte. Les politiques de confidentialité sont longues, techniques, et peu accessibles. Le consentement, pourtant pierre angulaire du RGPD lorsque d'autres bases légales ne sont pas pertinentes, devient une formalité.

Or, sans information compréhensible et transparente, ce consentement n'a aucune valeur réelle.
Il est temps de reconnaître que l'illusion d'une simple « conversation » masque en réalité une extraction massive d'informations.

La menace n'est pas théorique. Fuites de données, erreurs de configuration, attaques informatiques, profilage abusif ou biais algorithmiques sont déjà documentés. Dans certains cas, ces outils sont même intégrés dans des environnements professionnels sensibles – cabinets médicaux, services juridiques, administrations – exposant des informations confidentielles à des risques considérables.

UN CADRE JURIDIQUE EN RETARD SUR LA TECHNOLOGIE

Le RGPD constitue un socle solide, mais insuffisant face à la complexité de ces nouveaux systèmes. Les frontières entre responsables de traitement et sous-traitants s'estompent.

L'exercice des droits (accès, rectification, suppression) devient incertain, voire impossible. Pire : certaines entreprises contournent les exigences réglementaires en externalisant l'hébergement des données hors UE, échappant de facto à la surveillance des autorités.

NOS RECOMMANDATIONS POUR UNE IA RESPONSABLE

Face à ces constats, l'AFCDP appelle à une action coordonnée de l'ensemble des parties prenantes.

1. **Transparence totale :**
   les éditeurs d'IA doivent informer clairement sur les données collectées, leur finalité et leur durée de conservation.
2. **Consentement effectif :**
   les utilisateurs doivent pouvoir accepter ou refuser, en connaissance de cause, l'usage de leurs données.
3. **Sécurité renforcée :**
   chiffrement, authentification forte, contrôle des accès doivent devenir des standards.
4. **Encadrement strict dans les organisations :**
   adoption de politiques d'utilisation, sensibilisation des collaborateurs, audits réguliers, et implication systématique des DPO dans le déploiement.
5. **Soutien à des solutions souveraines :**
   promouvoir des alternatives éthiques et locales, mieux alignées avec le droit européen et les attentes sociétales.

FAIRE LE CHOIX D'UNE SOCIÉTÉ NUMÉRIQUE DE CONFIANCE

La question n'est pas de s'opposer au progrès, mais de choisir le type de société numérique que nous voulons construire. Une société où l'innovation technologique se développe dans le respect des droits fondamentaux. Où la confiance des citoyens n'est pas sacrifiée sur l'autel de la performance algorithmique.

Les IA conversationnelles ne sont pas neutres. Elles sont façonnées par les choix de ceux qui les conçoivent, les déploient et les utilisent. À nous de faire en sorte que ces choix soient guidés par l'éthique, la transparence et le respect de la vie privée.

DOROTHÉE DECROP

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

GS MAG : *Bonjour Dorothée Decrop, pouvez-vous vous présenter et nous dire comment votre parcours professionnel vous a amenée à votre rôle actuel chez HEXATRUST ?*

DD : Défendre les intérêts collectifs a toujours été cœur de mon engagement. J'ai accompagné pendant plus de 15 ans des chefs d'entreprises au sein d'associations professionnelles patronales françaises et européennes pour défendre leurs intérêts dans le cadre de politiques publiques au sein des filières de recyclage et des services de mobilité. Dans ce cadre, j'ai contribué à plusieurs chantiers de transformation numérique de l'Etat, notamment la mise en place du SIV, la sécurisation des échanges en EDI dans les serveurs du ministère de l'Intérieur.

J'ai également œuvré à la montée en compétence de la prévention des risques professionnels en entreprise pour un programme qui touchait 400 000 salariés. Désireuse d'approfondir ma réflexion sur l'impact du numérique dans le lobbying, j'ai suivi un master en Management et gestion des organisations, enrichissant ainsi ma vision stratégique et mon goût pour l'entrepreneuriat.

Une expérience en start-up centrée sur la valorisation du capital immatériel des organisations a renforcé ma conviction : je veux travailler sur les questions du numérique et au service d'intérêts collectifs.

C'est dans ce contexte qu'Hexatrust s'est imposé comme une évidence, résonnant avec mon parcours et mes aspirations avec beaucoup d'intensité.

GS MAG : *Pouvez-vous nous parler de vos différents engagements, chez HEXATRUST, et comme Auditrice de la 87ème session en Intelligence Économique et Stratégique à l'Institut des Hautes Études de Défense Nationale IHEDN ?*

DD : Souvent certains disent vouloir avoir un impact, mais ne s'exposent pas. Mes engagements ne sont possibles que parce que je suis soutenue par une équipe de grande qualité, des adhérents exigeants et des élus engagés à nos côtés. Mes missions s'articulent autour de 3 axes : défendre les intérêts de nos membres dans les évolutions réglementaires, les représenter au sein des écosystèmes associatifs, privés et publics comme les Comités Stratégiques de Filière, nos ministères de tutelle ou le Campus Cyber et les promouvoir en France et à l'étranger.

La diversité de nos parties prenantes nourrit une réflexion stratégique qui trouve, au travers de notre présence sur plus de 15 événements par an, le lancement de nouveaux services comme l'HexaSearch, la production d'amendements parlementaires ou d'un Livre Blanc sur le Zero Trust, une déclinaison opérationnelle.

Notre fil directeur chez Hexatrust est plutôt simple sans être simpliste : promouvoir un écosystème d'entrepreneurs français et européens innovants, œuvrant pour un numérique de confiance aux valeurs européennes et au bénéfice de leurs utilisateurs.

Chez Hexatrust, l'intelligence économique se trouve au cœur de nos défis. La protection de l'information stratégique dans les organisations, l'autonomie stratégique de notre pays, la maîtrise de nos infrastructures sont des

questions aux répercussions multiples pour le quotidien de nos concitoyens qui nous animent tous les jours. Par exemple, l'impact des lois extraterritoriales sur la gestion de nos entreprises européennes devient un enjeu de préoccupation de premier ordre aux conséquences encore trop sous-estimées. Il me paraissait donc évident de poursuivre cette réflexion au sein de l'IHEDN, référence en la matière, afin de solidifier mes compétences dans ce domaine, de développer de nouveaux réflexes et de coconstruire avec les autres auditeurs et auditrices, partageant les mêmes préoccupations, une forme de filtre de sécurité utile à nos filières.

GS MAG : *Le contexte géopolitique semble avoir des répercussions sur les Nouvelles Technologies et la Cybersécurité. Qu'en pensez-vous ?*

DD : Les nouvelles technologies et les questions de cybersécurité sont devenues les terrains virtuels d'une nouvelle guerre économique aux conséquences bien réelles. Le contexte géopolitique est source de questionnement mais également riche d'opportunités. L'opportunité réside dans l'action.

De plus en plus d'acteurs s'interrogent désormais sur leur politique d'achat et ses conséquences. Nous avons lancé pour les aider deux nouveaux services : l'HexaDiag et l'HexaSearch, pour promouvoir une économie circulaire numérique.

Il faut sortir du French Bashing systématique qui nous coûte en compétitivité. Au contraire, il est important de prendre conscience que La France et l'Europe regorgent de start-ups et d'entreprises innovantes, primées pour leurs avancées technologiques, impliquées dans des programmes d'envergure comme France 2030 ou Horizon 2020, et prêtes à conquérir les marchés internationaux. Mais pour transformer ces pépites en marques globales reconnues, leur passage à l'échelle doit être collectivement soutenu, structuré et accompagné.

Ce défi ne repose pas uniquement sur les entrepreneurs. L'ensemble des acteurs économiques, privés et publics, ont un rôle clé à jouer en leur apportant des commandes d'ampleur. L'exportation de nos technologies passe d'abord par un ancrage fort sur notre propre marché. Soutenir nos champions en France, c'est aussi leur donner les moyens de réussir à l'international.

Ce passage à l'échelle doit s'inscrire dans une stratégie assumée, un "plan de bataille" articulé autour de synergies nationales et européennes. Chaque euro investi est un pas vers l'autonomie stratégique

Investir dans des solutions de cybersécurité et de numérique de confiance issues de l'écosystème français et européen, comme celles développées par les membres d'Hexatrust, dépasse le simple enjeu du numérique. C'est aussi un choix économique et stratégique, qui favorise la souveraineté, l'innovation et la résilience de nos entreprises.

La protection des données doit être au cœur de nos stratégies. En matière d'intelligence économique, les risques liés à la manipulation de l'information et à l'espionnage restent encore trop peu abordés. Or, la maîtrise de sa politique cloud et de ses infrastructures numériques est aujourd'hui un levier de performance autant qu'un impératif de sécurité.

Enfin, soutenir nos entreprises, c'est aussi avoir un impact direct sur l'emploi et notre modèle social. Faire confiance aux acteurs français et européens, c'est assurer la montée en puissance de nos innovations, la valorisation de nos diplômes, et renforcer notre modèle économique et social.

Chaque décision d'achat dans le domaine du numérique et de la cybersécurité est un acte stratégique. L'idée n'est pas de substituer des acteurs extra-européens au simple profit d'acteurs européens mais passera par une conduite du changement pour transformer nos usages numériques responsables de demain pour prendre en compte notre écosystème. Il s'agit non seulement de garantir la protection de nos infrastructures et de nos données, mais aussi d'accélérer l'émergence de champions technologiques capables de rivaliser à l'international. Soutenons-les, structurons leur passage à l'échelle et bâtissons ensemble la souveraineté numérique de demain.

GS MAG : *En tant que Rôle Modèle, quels sont vos messages pour encourager les femmes à rejoindre le monde de la Cyber ?*

DD : Les métiers disponibles dans le monde de la Cyber ne sont pas encore tous bien identifiés. Il est important de les faire connaître dès le collège pour donner le goût aux jeunes filles d'intégrer le monde des sciences et renforcer la diversité des profils dans les équipes tech. Et puis à côté de ces profils plus techs de type développeuse, ingénieure, data scientist, il y a de nombreux métiers disponibles et accessibles à toutes dès aujourd'hui. Emparez-vous-en !

Si vous aimez les innovations technologiques, une filière dynamique et engagée aux multiples enjeux, vous serez au bon endroit. C'est la diversité des profils qui permettront à nos entreprises de créer de la valeur interne à l'organisation et, par conséquent, pour leurs clients, et devenir ainsi des champions reconnus. Il est important de ne pas se mettre de barrière et de faire ce qui nous fait vibrer.

"Les femmes qui ont changé le monde n'avaient pas besoin de permission." – Coco Chanel. ■

11ème édition

UNIVERSITÉS D'ÉTÉ

CYBERSÉCURITÉ & CLOUD DE CONFIANCE

9.09.25 | **STATION F - PARIS**

EVÉNEMENT ORGANISÉ PAR

HEXATRUST

CLOUD CONFIDENCE & CYBERSECURITY

L'ÉVÉNEMENT DE RENTRÉE DE LA FILIÈRE CYBER & CLOUD DE CONFIANCE

AVEC LE SOUTIEN DE

CAMPUS CYBER

CESIN

Global Security Mag
THE LOGICAL & PHYSICAL SECURITY MAGAZINE

IT for Business

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

GOUVERNEMENT
Liberté
Égalité
Fraternité

17 CYBER
Mon assistance en ligne

Un service proposé par

POLICE NATIONALE | Gendarmerie nationale | CYBER MALVEILLANCE .GOUV.FR

MANON DUBIEN

Vice-Présidente CEFCYS
Responsable du développement commercial cyber dans un Cabinet de Conseils

LES NOUVELLES TECHNOLOGIES (IA, QUANTIQUE, SASE, SOAR, XDR, ZERO TRUST...) ET LA CYBERSÉCURITÉ

GS MAG : *Bonjour Manon Dubien, pouvez-vous vous présenter et nous dire comment votre parcours professionnel vous a amenée à votre rôle actuel et au CEFCYS ?*

MD : Bonjour et merci pour cette invitation.
Je suis responsable du développement commercial dans un cabinet de conseils en cybersécurité.
Mon parcours mêle stratégie, accompagnement des décideurs et compréhension fine des enjeux cyber.
En 2019 rejoindre le CEFCYS a été une évidence : il est essentiel de donner plus de visibilité aux femmes dans ce secteur d'avenir.

GS MAG : *Pouvez-vous nous parler de vos différents engagements ?*

MD : J'accompagne les décideurs dans la mise en place de stratégies cyber en lien avec leurs enjeux.
Je m'engage activement pour inspirer, fédérer et promouvoir les talents féminins dans notre écosystème.
J'aime porter des actions concrètes et impactantes.

GS MAG : *Le contexte géopolitique semble avoir des répercussions sur les Nouvelles Technologies et la Cybersécurité. Qu'en pensez-vous ?*

MD : Les tensions géopolitiques accélèrent l'innovation technologique, mais amplifient aussi les risques. L'IA, le quantique, le Zero Trust ou encore le SOAR transforment nos défenses. Face à cela, la Cybersécurité ne peut être que stratégique, souveraine et collective. Elle exige une vision claire, ancrée dans l'anticipation et la résilience.

GS MAG : *En tant que Rôle Modèle, quels sont vos messages pour encourager les femmes à rejoindre le monde de la Cyber ?*

MD : La Cybersécurité a besoin de diversité. Il est temps de faire tomber les barrières. Osez, formez-vous, rejoignez des réseaux, prenez la parole. Les métiers sont multiples et ouverts à tous les parcours. La légitimité ne se demande pas, elle se vit. C'est ensemble, avec des profils variés, que nous construirons une cybersécurité durable. Tant que la cybersécurité restera un monde à majorité masculine, elle restera incomplète. ■

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 connaitre 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

JOBDATING

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

CYBER WOMEN DAY BY CEFCYS

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 partnaires

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

FLORENCE PUYBAREAU

Directrice Clusif

LA NOUVELLE DIRECTRICE Clusif

ARRIVÉE EN FÉVRIER À LA TÊTE DE L'ASSOCIATION FLORENCE NOUS RETRACE SON PARCOURS ET SES AXES DE TRAVAIL POUR LES PROCHAINS MOIS

FLORENCE, PEUX-TU NOUS DIRE QUELQUES MOTS SUR TON PARCOURS ET LA RAISON POUR LAQUELLE TU AS SOUHAITÉ REJOINDRE LE CLUSIF ?

Sans remonter trop loin dans ma carrière qui commence à dater, j'ai un passé de journaliste dans la presse écrite. D'abord dans des magazines informatiques puis dans la presse économique et ensuite professionnelle (gestion des risques, assurance, RH…). J'ai surtout abordé les sujets « techno » sous l'angle des grandes tendances, de l'évolution des marchés, de l'apparition (voire la disparition) des technologies numériques. C'est pourquoi, assez tôt, j'ai commencé à m'intéresser à « la sécurité informatique » mais c'est seulement à partir de 2010 que je me suis davantage orientée vers ce secteur. En 2016, j'ai abandonné ma carte de presse pour rejoindre DG Consultants (devenu Comexposium) , l'organisateur des Assises de la cybersécurité, de Ready For IT , de Finaki… J'étais en charge des contenus, donc

des conférences, des tables-rondes… C'est l'époque où nous avons créé le Before , l'avant-première des Assises, une journée complète où RSSI et experts cyber travaillent sur leurs problématiques du moment. C'était passionnant car j'étais vraiment au cœur des sujets d'actualité. Mais il me fallait un nouveau challenge et en 2023, je suis partie à Lille prendre la direction du Campus Cyber Hauts-de-France Lille Métropole qui venait d'être lancé (et qui était le premier à être labellisé en Région). Là encore, une très belle aventure car tout était à faire : il fallait trouver le modèle, fédérer l'écosystème local (qui est dynamique mais au début n'attendait pas grand-chose du Campus) et prouver aux instances publiques qu'elles avaient eu raison d'investir dans le projet. En 2 ans, avec l'équipe, nous avons su créer une belle dynamique et aujourd'hui ce Campus est devenu un des fleurons de la cyber régionale et même nationale.

Paris me manquait un peu et quand s'est présentée l'opportunité de rejoindre le Clusif, je me suis dis que c'était une nouvelle chance qui s'offrait à moi. Rejoindre une si belle Association, l'une des plus anciennes du secteur et qui venait d'obtenir la reconnaissance d'utilité publique (RUP) !

JUSTEMENT QUEL EST TON PLAN D'ACTION POUR LES PROCHAINS MOIS ET TES GRANDES PRIORITÉS ?

Cela fait à peine 2 mois que je suis arrivée et même si je connaissais déjà le Clusif (mais de l'extérieur et sans être adhérente), j'ai encore besoin de m'imprégner de la vie de l'Association, de son fonctionnement, de la richesse de son « offre ». J'ai été étonnée de la quantité de livrables que nous publions chaque année (24 en 2024 dont le fameux Panocrim), de la qualité des groupes de travail et d'une façon générale de la volonté de nombreux adhérents de participer à la vie de l'Association. Nous avons la chance de pouvoir croiser le regard des acteurs (offreurs de solutions et services) avec celui des utilisateurs mais dans une démarche d'intérêt général. C'est l'une des valeurs ajoutées du Clusif et c'est dans cet esprit de travail en collectif que je veux inscrire mon action. A l'instar du Président Benoît Fuzeau qui présentera son plan stratégique lors de l'Assemblée Générale du 13 mai. Pour ma part, je travaille actuellement sur quatre axes prioritaires avec l'équipe de permanents et les administrateurs : le développement du Clusif dans son écosystème et autour de son écosystème.

A savoir porter notre voix et nos expertises non seulement au sein de notre secteur mais aussi auprès des structures (associations professionnelles, fédérations, syndicats…) qui ont besoin d'information, d'éclairage sur la cybersécurité. Cela passe par des partenariats, des livrables , des événements communs…

Autre chantier : le rapprochement avec le réseau des Clusir les différentes associations régionales (en Métropole et dans les DROM) souvent très dynamiques et avec lesquelles nous souhaitons développer de nouvelles coopérations.

Troisième axe : l'accompagnement des adhérents à commencer par les nouveaux. Certains ne connaissent pas toutes les activités du Clusif, n'osent pas s'engager sur des groupes de travail ou participer aux Espaces. A nous de bien les «on boarder » et de leur présenter toute la palette des possibles et des sujets qu'ils soient techniques, stratégiques, de gouvernance…

Enfin, et ce n'est pas le moindre, il y a le chantier RUP. C'est une formidable opportunité pour le Clusif mais elle nous engage à différents niveaux et cela aura sans doute un impact sur la vie de l'Association. C'est un nouveau challenge, comme je les aime ! ■

je travaille actuellement sur quatre axes prioritaires avec l'équipe de permanents et les administrateurs : le développement du Clusif dans son écosystème et autour de son écosystème.

20 | 21 | 22
MAI 2025
MONACO

READY FOR IT!

Le grand saut des ETI
sera au cœur des réflexions
de cette 6ème édition

Rejoignez la communauté & rendez-vous du 20 au 22 mai à Monaco

pour l'événement incontournable des acteurs engagés
dans la transition et la sécurité numériques.

Vous avez des projets d'investissement en cours ou à venir ?

Pour vous inscrire, scannez ce QR code !

Les inscriptions sont ouvertes et soumises à validation

Suivez-nous ! ready-for-it.com · Ready For IT · RFIT_event

COMEXPOSIUM ONE TO ONE

MARIA IACONO

Directrice des Assises de la Cybersécurité et Ready For IT, Comexposium One to One

LE GRAND SAUT DES ETI : READY FOR IT 2025,

L'ÉVÉNEMENT INCONTOURNABLE POUR LES DSI

La transformation digitale est devenue un passage obligé pour les ETI françaises. Pourtant, franchir ce cap s'apparente souvent à un véritable saut dans l'inconnu : complexité technologique, manque de ressources, réglementation renforcée… Comment les DSI peuvent-ils structurer et accélérer cette mutation stratégique ?

Maria Iacono, Directrice des Assises de la cybersécurité et Ready For IT, nous éclaire sur les défis et solutions à venir.

MARIA, POURQUOI PARLE-T-ON DE "GRAND SAUT" POUR LES ETI EN 2025 ?

Les ETI sont à un tournant décisif. Elles n'ont plus d'autre choix que d'intégrer pleinement le numérique pour rester compétitives, sécuriser leurs systèmes et répondre aux nouvelles exigences réglementaires comme NIS2. Mais ce saut est vertigineux : il faut concilier innovation, cybersécurité, transition vers le cloud, IA… tout en composant avec des budgets contraints et un manque de talents spécialisés. Ce "Grand Saut", c'est l'enjeu central que nous explorerons à Ready For IT 2025.

QUELS SONT LES PRINCIPAUX FREINS RENCONTRÉS PAR LES DSI ?

Trois grands défis reviennent systématiquement :

1. **La complexité technologique**
   L'intégration de nouvelles solutions, notamment en cybersécurité et en cloud hybride, reste un casse-tête.
2. **Le facteur humain**
   Trouver et retenir des talents qualifiés est une difficulté majeure.
3. **La gouvernance et la réglementation**
   Avec des obligations comme NIS2, les entreprises doivent repenser leur stratégie IT pour garantir conformité et résilience.

>>>

>>> EN QUOI READY FOR IT EST-IL UN ACCÉLÉRATEUR POUR LES DÉCIDEURS IT ?

Ready For IT 2025, c'est bien plus qu'un évènement : c'est une véritable plateforme d'échanges et d'expertise. Pendant trois jours, du 20 au 22 mai à Monaco, les DSI, CTO, RSSI et Directeurs Innovation pourront rencontrer les meilleurs experts et prestataires pour structurer leur transformation numérique.

Grâce à un programme mêlant conférences, tables rondes et rendez-vous one-to-one, chaque participant repart avec une vision claire des tendances et des solutions adaptées à ses enjeux. C'est aussi l'occasion unique d'échanger avec des pairs confrontés aux mêmes problématiques et de partager les meilleures pratiques du secteur.

UN MOMENT CLÉ DE L'ÉVÉNEMENT SERA LA PRÉSENTATION DE L'ÉTUDE "LE GRAND SAUT"... POUVEZ-VOUS NOUS EN DIRE PLUS ?

Absolument ! Réalisée par PAC, cette étude dresse un état des lieux précis des défis et opportunités pour les DSI des ETI. Nous y abordons notamment :

- Les tendances technologiques à intégrer en priorité,
- L'impact des nouvelles régulations,
- Les stratégies gagnantes pour optimiser les investissements IT.

Sa présentation à Ready For IT sera l'occasion d'échanger autour de ses conclusions et de fournir aux décideurs des recommandations concrètes pour franchir ce cap en toute sérénité.

QUELS SERONT LES AUTRES TEMPS FORTS DE READY FOR IT 2025 ?

Cette année, plusieurs tables rondes et keynotes permettront d'explorer en profondeur les différentes facettes du "Grand Saut" :

■ **"Le Grand Saut des ETI : pourquoi maintenant ?"**
Animé par Éric Domage, avec Arnaud Philippe et Julien Villecroze

- **"Vers plus d'efficacité !"**
Animé par Véronique Loquet
- **"Vers plus d'agilité !"**
Animé par Mélanie Bénard-Crozat et Frédéric Charles

■ **"Préparer le Grand Saut" :**

- **Par la gouvernance**
Avec Géraldine Dequeker, Thierry Salon et Marie Ait-Daoud
- **Par la technologie**
Animé par Éric Domage
- **Avec les talents**
Avec Véronique Loquet et Sylvain Despas

UN DERNIER MOT POUR INCITER LES DSI À PARTICIPER ?

Si vous êtes DSI, CTO ou RSSI d'une ETI, Ready For IT 2025 est l'événement à ne pas manquer. C'est l'occasion idéale pour anticiper les mutations du numérique, échanger avec des experts et sécuriser votre transformation digitale.

Ne ratez pas ce rendez-vous stratégique à Monaco du 20 au 22 mai ! ■

il faut concilier innovation, cybersécurité, transition vers le cloud, IA... tout en composant avec des budgets contraints et un manque de talents spécialisés.

REJOIGNEZ LE CESIN

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

COOPÉRATION - CONFIANCE - CONVIVIALITÉ

Un Club au service de ses membres

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

CESIN

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

contact@cesin.fr - www.cesin.fr

ÉRIC SINGER

Responsable du Cursus Cybersécurité ESIEE - IT + Global CSO, Ingenico Auteur du Livre Blanc ZERO TRUST, CESIN - Forum InCyber

ALAIN BOUILLÉ

Délégué Général et Porte-parole CESIN

ZERO TRUST : NOUVEAU PARADIGME OU BUZZWORD ?

LA CYBERSÉCURITÉ NE PEUT PLUS ACCORDER DE CONFIANCE AVEUGLE

Dans le monde d'avant, il suffisait de construire des murs. Un pare-feu bien configuré, un VPN pour les accès distants, un Active Directory maîtrisé, et l'entreprise pouvait dormir sur ses deux oreilles, ou presque ! Les utilisateurs étaient à l'intérieur, les menaces à l'extérieur. Le monde numérique ressemblait à un château fort : il fallait empêcher l'ennemi de franchir le pont-levis.

Mais ce modèle a volé en éclats. Et avec lui, une certaine idée de la confiance.

Aujourd'hui, les utilisateurs sont nomades, les données dans le cloud, les partenaires interconnectés, les applications distribuées, les appareils hétérogènes. La surface d'exposition s'est démultipliée. Le périmètre est devenu flou, mouvant, parfois inexistant. Et les attaquants n'ont jamais été aussi professionnels, discrets, agiles. Ils s'infiltrent, se latéralisent, patientent. Ils exploitent le moindre excès de confiance.

Dans ce contexte, le modèle du **Zero Trust** peut être une approche qui peut être adoptée par les experts sécurité.

PLUS QU'UN CONCEPT, UN CHANGEMENT DE PARADIGME

Le terme "Zero Trust" est souvent mal compris. On l'associe à une défiance systématique, presque paranoïaque. En réalité, il ne s'agit pas de ne faire confiance à personne, mais de ne jamais accorder cette confiance **par défaut. Chaque accès doit être justifié, chaque requête vérifiée, chaque privilège limité, chaque session surveillée.** Le tout, en s'adaptant dynamiquement au contexte : qui se connecte, depuis où, à quoi, dans quelles conditions.

C'est une approche fondée sur la vérification permanente, la segmentation intelligente, et le contrôle contextuel. Un modèle pensé pour un monde distribué, en constante évolution, où le danger vient autant de l'intérieur que de l'extérieur.

UN CHEMIN PLUS QU'UN ÉTAT FINAL

Le Zero Trust n'est pas une case à cocher. Ce n'est pas une technologie que l'on achète, déploie, et qui règle tous les problèmes. C'est une trajectoire, un but à atteindre, un cheminement progressif.

Et c'est justement ce que montre le livre blanc publié par le CESIN, en partenariat avec le Forum InCyber : à partir de près de 200 témoignages de membres du club, tous experts cybersécurité dans leur organisation, il dresse un état des lieux réaliste et documenté de ce que le Zero Trust est (et n'est pas). On y découvre que beaucoup d'entreprises ont déjà engagé, souvent sans le formaliser ainsi, des démarches très proches de ce modèle : authentification multifacteur, micro-segmentation, gestion fine des identités, supervision continue, ZTNA (Zero Trust Network Access)… Le Zero Trust permet alors de donner du sens, une cohérence d'ensemble, une ambition à long terme à ces initiatives disparates.

UNE VISION STRATÉGIQUE, PAS UN PROJET IT

L'autre mérite du livre blanc est de rappeler une vérité essentielle : le Zero Trust n'est pas un chantier purement technique. Il touche à la gouvernance, à l'organisation, aux processus métiers. Il engage les RSSI, bien sûr, mais aussi les DSI, les directions métiers, les RH, les achats et bien entendu le COMEX.

Car adopter cette posture, c'est repenser la façon dont on attribue les droits, dont on gère les accès tiers, dont on cartographie les flux, dont on identifie les actifs critiques. C'est mettre fin à une certaine naïveté dans la gestion des privilèges. C'est considérer que personne — pas même un administrateur, un fournisseur, ou un partenaire de longue date — ne doit disposer d'un accès illimité ou non supervisé.

Et c'est aussi, parfois, avoir le courage de dire non. Non à un accès trop large. Non à une exception non justifiée. Non à une dérogation permanente.

L'ÉQUILIBRE ENTRE SÉCURITÉ, FLUIDITÉ ET CONFIANCE

Cela ne signifie pas bloquer les usages ou nuire à l'expérience utilisateur. Au contraire : bien mis en œuvre, le Zero Trust permet une sécurité plus granulaire, plus fluide, plus invisible. Moins de frictions inutiles, mais plus d'intelligence dans les contrôles. Moins de "tout ou rien", plus d'adaptation au risque réel.

En somme, plus de confiance… mais une confiance éclairée, construite, réévaluée.

UN CAP POUR L'AVENIR

Face à des cybermenaces toujours plus sophistiquées, face à des environnements IT toujours plus complexes, le Zero Trust n'est pas un luxe. C'est une nécessité. Pas une baguette magique, mais un cap stratégique.

Il ne s'agit pas de tout refaire. Il s'agit de faire mieux, de façon plus cohérente. De sortir des modèles hérités, des privilèges excessifs, des angles morts. Et de bâtir une cybersécurité adaptée aux réalités d'aujourd'hui.

En d'autres termes : ne plus faire de la confiance un point de départ, mais un objectif. ■

Le Zero Trust n'est pas une case à cocher. Ce n'est pas une technologie que l'on achète, déploie, et qui règle tous les problèmes. C'est une trajectoire, un but à atteindre, un cheminement progressif.

WOJTEK SOCHACKI

Maître International du Jeu d'Échecs
Responsable Détection SOC & Analyste CERT, Hermès

LE JEU D'ECHECS & LA CYBERSÉCURITÉ

Tout a commencé sur un échiquier. Une position tendue, une menace invisible, une erreur de calcul... et la partie bascule. Des années plus tard, face à des lignes de log etdes alertes en cascade, j'ai reconnu la même sensation : ce moment où tout se joue enquelques secondes.

Les échecs m'ont appris à voir au-delà des apparences, à anticiper, à reconnaître les motifs cachés. Ce jeu silencieux a façonné ma manière de penser la cybersécurité. Voici pourquoi.

DE L'IMPORTANCE DE LA TACTIQUE (MITRE ?!)

Aux échecs, chacun bâti sa stratégie, essaie de s'inspirer des grands principes positionnels tel que le contrôle du centre, l'utilisation de l'avant poste, le jeu contre un pion isolé etc…

Mais au moment critique de la partie, le succès de l'une des deux stratégies imaginées par les deux camps se fera de façon brutale et se réglera par une séquence de coups tactiques, nécessitant une bonne dose d'imagine et reconnaissance de patterns (afin de pouvoir réussir à placer sa "fourchette" ou "enfilade" prévue de longue date) mais aussi et surtout la précision du calcul plusieurs coups à l'avance qui permettra de vaincre son adversaire qui n'avait pas réussi à calculer aussi loin ou a oublié certaines "pointes" intermédiaires.

Il apparaît donc essentiel de s'améliorer en tant que joueur d'échecs sur la phase tactique du jeu qui peut compenser d'autres lacunes tels qu'un manque de connaissance des parties classiques de champions du passés (ou d'absence de lecture de rapports DFIR ou de veille pour l'analyste SOC/CERT), ou d'un repertoire d'ouverture limité (ou d'un manque de patching ou hardening des serveurs / absence de segmentation réseau qui n'auraient probablement pas menés à la position défavorable que l'on essaie de compenser).

La force d'un joueur d'échecs se mesure à l'aide du classement ELO, qui indique la probabilité qu'un joueur batte un autre en fonction de l'écart de classement.

On se rendra compte au passage que chaque domaine de la cybersécurité est souvent sous la responsabilité d'une équipe dédiée dans l'entreprise, (ainsi le patching / hardening des serveurs n'est souvent pas géré par les analystes du SOC/CERT. D'un point de vue échiquéen, cela voudrait dire que plusieurs équipes se relaient en fonction de la phase du jeu dans laquelle la partie se trouve et où l'intervention de l'analyste CERT ne se fait la plupart du temps qu'à des phases avancées du jeu ce qui pose des difficultés supplémentaires liées à la stratégie globale et la communication entre les équipes. Aux échecs, cette réduction de la surface d'attaque se traduit par une exécution d'un petit-roque afin d'enlever notre roi exposé (en direct sur internet) en vue de le positionner à l'abri sur un VLAN dédié derrière un firewall de pions.

Pour ce faire, il est alors important pour l'analyste cyber de s'entraîner tout d'abord à nommer ces patterns, à tendre vers son exhaustivité (c'est le projet du MITRE ATT&CK) / les voir en action et de voir les effets qu'ils génèrent (création de logs particuliers, comportements successifs générés) afin de pouvoir les reconnaîtres plus facilement à l'avenir et même idéalement à les empêcher tout simplement de pouvoir se produire.

Comme lorsqu'un joueur d'échecs pousse son pion en h3 pour éviter la technique T8045 - MITRE ATT&CK a.k.a "mat du couloir".

MESURER SON NIVEAU OU SA MATURITÉ

La force d'un joueur d'échecs se mesure à l'aide du classement ELO, qui indique la probabilité qu'un joueur batte un autre en fonction de l'écart de classement. La qualité, l'intensité ou la beauté d'une partie ne sera pas la même selon qu'elle oppose deux débutants ou deux champions.

Il faut donc améliorer le ELO de son équipe défensive cyber afin de réduire la probabilité qu'elle se fasse battre par un attaquant opportuniste. Les échecs sont un jeu où la chance n'a pas sa place, et cela devrait être aussi le cas en cybersécurité.

Les échecs sont un jeu objectif : lors de l'analyse post-mortem (ou forensics), on peut toujours retrouver la cause précise de la défaite. C'est ce même mécanisme d'essai/erreur qui permet de progresser. En cybersécurité, cela se traduit par les tests d'intrusion réguliers, qui challengent les analystes SOC afin de les forcer à s'améliorer pour la véritable "partie" à venir, contre un adversaire réel et malveillant, face auquel l'erreur n'est pas permise.

Aux echecs comme en cyber, lorsque le niveau des équipes est mature, il suffit d'un faux pas de l'attaquant ou d'un mauvais pour que l'équipe défensive puisse reprendre le dessus avec la détection de celle-ci et repousser l'assaut.

UN JEU EN PERPÉTUELLE ÉVOLUTION

Bien que les règles n'aient pas évolué depuis la fin du XVe siècle, le jeu d'échecs est en constante transformation. Il a été bouleversé par l'arrivée des premiers ordinateurs, puis des modules d'analyse, et plus récemment par les réseaux neuronaux.

Concrètement, cela s'est traduit par une montée spectaculaire du niveau moyen, une amélioration de la qualité des parties, et la réhabilitation de variantes théoriques longtemps considérées comme douteuses.

Le jeu n'est toujours pas résolu, et ne le sera probablement jamais totalement, tant le nombre de positions possibles dépasse notre capacité de stockage et de calcul. Une réalité qui rappelle étrangement celle du cyberespace... ■

CONCLUSION

Les parallèles entre les échecs et la cybersécurité ne sont pas de simples analogies. Ils révèlent une vérité plus profonde : les deux disciplines exigent rigueur, anticipation, adaptation, et apprentissage constant. Qu'il s'agisse de parer une menace ou de trouver le bon coup, tout repose sur une lecture fine des signaux faibles, une compréhension du contexte, et une capacité à transformer l'information en décision. Le jeu d'échecs, loin d'être un loisir abstrait, peut devenir un formidable terrain d'entraînement pour l'esprit cyber. Et peut-être, qu'en maîtrisant les codes de l'un, apprend-on à mieux défendre les lignes de l'autre ?

ELODIE LE SAOUT

Fondatrice, CEO, Moïra Cybersecurity
Cofondatrice & CTO, Smartnova

L'AUTOMATISATION AU SERVICE DE LA GOUVERNANCE

Les technologies soar (security orchestration, automation and response) transforment progressivement l'approche de la gouvernance des risques et de la conformité (grc). Au-delà de la simple automatisation technique, ces outils offrent un potentiel de transformation profonde des processus décisionnels et du pilotage des risques cyber.

L'évolution constante des menaces et la complexification du paysage réglementaire imposent aux organisations une refonte de leurs mécanismes de gouvernance des risques cyber. Dans ce contexte, les plateformes SOAR émergent comme des leviers stratégiques pour transformer l'approche traditionnelle de la GRC, souvent perçue comme statique et déconnectée des réalités opérationnelles.

LA CONVERGENCE NÉCESSAIRE ENTRE OPÉRATIONS ET GOUVERNANCE

Historiquement, un fossé séparait les équipes opérationnelles de sécurité et les fonctions de gouvernance des risques. Les premières agissaient dans l'urgence, guidées par des impératifs techniques, tandis que les secondes élaboraient des cadres formels parfois déconnectés des contraintes du terrain. Cette dichotomie, longtemps acceptée comme inévitable, devient intenable face à l'accélération des cycles d'attaque et à la pression réglementaire croissante.
Les plateformes SOAR offrent désormais la possibilité de combler ce fossé en créant un continuum entre la détection des menaces, la réponse opérationnelle et la gouvernance des risques. Cette convergence s'opère notamment par l'intégration des exigences de conformité directement dans les playbooks d'automatisation, transformant ainsi des obligations souvent perçues comme administratives en processus opérationnels concrets.
L'expérience montre que cette intégration directe des contraintes réglementaires dans les workflows de réponse aux incidents réduit significativement le risque de non-conformité tout en améliorant l'efficacité opérationnelle. La documentation automatique des actions entreprises, la traçabilité des décisions et la standardisation des réponses constituent des atouts majeurs face aux exigences croissantes des régulateurs en matière de démonstration de maîtrise des risques.

L'AUTOMATISATION DE LA VEILLE RÉGLEMENTAIRE ET NORMATIVE

La complexification du paysage réglementaire représente un défi majeur pour les responsables GRC. RGPD, NIS2, réglementations sectorielles, normes techniques : maintenir une veille exhaustive et actionnable sur cet écosystème mouvant devient une tâche titanesque pour les équipes dédiées.
Les solutions SOAR avancées intègrent désormais des capacités de veille automatisée, permettant d'identifier les évolutions normatives pertinentes pour l'organisation et d'évaluer leur impact sur les processus existants. Cette

automatisation de la veille réglementaire permet non seulement de réduire la charge cognitive des équipes GRC mais également d'accélérer significativement l'adaptation des contrôles aux nouvelles exigences.

La valeur ajoutée réside particulièrement dans la capacité à contextualiser ces évolutions réglementaires en fonction des spécificités de l'organisation. En croisant les nouvelles exigences avec la cartographie des actifs et des processus métiers, les plateformes SOAR permettent d'identifier précisément les zones d'impact et de prioriser les actions de mise en conformité en fonction des risques associés.

DES INDICATEURS DYNAMIQUES POUR UN PILOTAGE PROACTIF

Les approches traditionnelles de la GRC reposent souvent sur des évaluations périodiques qui, par nature, offrent une vision statique et rapidement obsolète de l'exposition aux risques. Dans un environnement de menaces évoluant en temps réel, cette approche présente des limitations évidentes que les technologies SOAR permettent désormais de surmonter.

L'intégration des flux de données de sécurité opérationnelle dans les tableaux de bord GRC transforme radicalement la nature du pilotage des risques. Les indicateurs statiques cèdent progressivement la place à des métriques dynamiques offrant une vision en temps réel de l'efficacité des contrôles et de l'exposition aux menaces émergentes.

Cette évolution vers un pilotage dynamique se traduit notamment par la définition d'indicateurs composites combinant données opérationnelles et exigences de gouvernance. Par exemple, le délai moyen de remédiation des vulnérabilités critiques peut être automatiquement contextualisé en fonction des obligations réglementaires applicables aux systèmes concernés, offrant ainsi une vision immédiatement actionnable pour les décideurs.

L'INTELLIGENCE ARTIFICIELLE COMME CATALYSEUR

Les avancées récentes en matière d'intelligence artificielle démultiplient le potentiel des plateformes SOAR dans le domaine de la GRC. Au-delà de l'automatisation des processus existants, ces technologies permettent désormais d'anticiper les évolutions du risque et d'optimiser proactivement les mécanismes de contrôle.

Les algorithmes d'apprentissage supervisé s'avèrent à cet égard particulièrement pertinents pour identifier les tendances émergentes et prédire les zones de vulnérabilité potentielle avant qu'elles ne se matérialisent. Cette capacité d'anticipation, lorsqu'elle est intégrée aux processus de gouvernance, permet ainsi d'adopter une posture véritablement proactive plutôt que simplement réactive. Les technologies de traitement du langage naturel offrent également des perspectives prometteuses pour l'analyse automatisée des textes réglementaires et leur traduction en exigences opérationnelles concrètes. Cette capacité d'interprétation contextuelle réduit considérablement le délai entre la publication d'une nouvelle réglementation et son implémentation effective dans les processus de l'organisation.

DÉFIS ET FACTEURS CLÉS DE SUCCÈS

Si les bénéfices potentiels des plateformes SOAR pour la GRC sont considérables, leur mise en œuvre efficace se heurte à plusieurs défis qu'il convient d'anticiper.

Le premier écueil concerne la qualité des données intégrées dans les workflows automatisés. La fiabilité des décisions générées par ces plateformes dépend directement de l'exactitude, de l'exhaustivité et de la pertinence des informations sur lesquelles elles s'appuient. Une gouvernance rigoureuse des données constitue donc un prérequis incontournable à tout projet d'automatisation de la GRC.

La dimension humaine représente un second défi majeur. L'automatisation ne saurait remplacer l'expertise et le jugement des professionnels de la GRC, particulièrement dans l'interprétation des exigences réglementaires et l'évaluation de leur applicabilité aux spécificités de l'organisation. Une approche équilibrée, combinant automatisation des tâches à faible valeur ajoutée et valorisation de l'expertise humaine pour les décisions complexes, s'avère généralement la plus efficace.

VERS UNE GRC AUGMENTÉE

L'intégration des technologies SOAR dans les dispositifs de GRC ouvre la voie à une gouvernance "augmentée" où l'automatisation intelligente libère les professionnels des tâches répétitives pour leur permettre de se concentrer sur les activités à forte valeur ajoutée.

Cette transformation ne se limite pas à une simple optimisation des processus existants mais constitue une refonte profonde de l'approche même de la gouvernance des risques. Dans ce nouveau paradigme, la GRC n'est plus perçue comme une fonction administrative distincte des opérations de sécurité mais comme un continuum intégré allant de la détection technique à la décision stratégique.

Les organisations ayant adopté cette approche témoignent d'une amélioration significative de leur capacité à maintenir une conformité démontrable dans un environnement réglementaire mouvant, tout en optimisant l'allocation de leurs ressources défensives face à un paysage de menaces en constante évolution. ■

ETIENNE
DE SÉRÉVILLE

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

NOUVELLES TECHNOLOGIES ET CYBERSÉCURITÉ : L'IA COMME ACCÉLÉRATEUR DE SÉCURITÉ

Les équipes de cybersécurité sont confrontées à des défis croissants actuellement : cyberattaques nombreuses et sophistiquées, vecteurs d'attaque multipliés, complexité des infrastructures, frontières floues, chaîne d'approvisionnement risquée.

Ainsi, les infrastructures critiques ont subi des fuites de données aux coûts très élevés : les organisations des secteurs de santé, financier, industriel, technologique et énergétique ont enregistré les coûts de fuites de sécurité les plus élevés, tous secteurs confondus. Comme le souligne le rapport annuel d'IBM, les violations de données ont atteint des niveaux records avec un coût mondial moyen en augmentation de 10 % en un an, atteignant 4,88 millions de dollars, soit la plus forte hausse depuis la pandémie.

Ces fuites s'inscrivent dans les attaques à but lucratif, parfois avec de multiples extorsions. Et pour autant, les entités des secteurs critiques ne sont pas non plus épargnées par les attaques à finalité de déstabilisation ou d'espionnage, comme le présente le récent panorama 2024 de l'ANSSI.

ALORS, COMMENT LES ENTREPRISES PEUVENT-ELLES MIEUX SE DÉFENDRE CONTRE CES CYBERATTAQUES PLUS PERSISTANTES ET COÛTEUSES ?

Une des solutions réside dans l'automatisation basée sur l'IA.

Deux organisations étudiées sur trois ont déclaré déployer l'IA et l'automatisation de la sécurité dans l'ensemble de leur organisation, soit une augmentation de près de 10 % par rapport à l'année précédente. Grâce à un déploiement fort des workflows IA de prévention, les entreprises ont enregistré en moyenne 2,2 millions de dollars de moins en coûts de violation que celles qui n'utilisaient pas ces workflows – les économies les plus importantes révélées par le rapport 2024 sur les coûts liés aux violations de données.

L'IA peut gérer les tâches répétitives et chronophages, comme la surveillance des journaux, l'analyse du trafic réseau, des activités systèmes et des actions utilisateurs inhabituelles, qui peuvent être automatisées, permettant ainsi de tirer parti de l'expertise humaine là où elle est la plus utile. De même, l'intégration de l'IA permet de réduire les interventions manuelles, sources potentielles de latence et d'erreurs. En accélérant l'exécution des actions de remédiation, l'automatisation garantit une réponse rapide et efficace.

L'IA traite des masses de données à grande vitesse, surpassant nos capacités humaines. Elle peut identifier des schémas, des anomalies et des menaces potentielles en temps réel, réduisant ainsi les délais de réponse aux incidents. En détectant et en alertant rapidement les équipes SOC, l'IA minimise les opportunités pour les attaquants. Ainsi, l'IA prend en charge le tri initial, la suppression des faux positifs et le traitement des incidents basiques, libérant ainsi les analystes des tâches répétitives. Désormais, la validation et l'interprétation des résultats de l'IA deviennent cruciales, posant la question de la formation et de l'évolution des analystes avec ces automatisations.

Les outils de sécurité basés sur l'IA automatisent la détection des menaces, filtrent les activités non menaçantes et réduisent ainsi les faux positifs. Cette efficacité permet aux équipes de cybersécurité d'allouer efficacement leurs ressources et aux analystes de se concentrer sur les véritables menaces. Cette optimisation accélère la détection, simplifie la réponse aux incidents et la reprise d'activité, réduisant ainsi les coûts liés aux violations de données.

Cependant, l'efficacité du SOC repose sur la capacité à développer et à améliorer continuellement les modèles d'IA. Cela exige des compétences spécifiques ainsi qu'un accès à des données pertinentes, fraîches et de qualité. Or, l'évolution des technologies et la complexité des tactiques d'attaque compliquent cette exigence, rendant indispensable une gestion rigoureuse des modèles pour assurer leur pertinence opérationnelle. L'exploitation optimale des outils du SOC passe aussi par l'élaboration de scripts et runbooks adaptés aux activités forensiques et à la gestion opérationnelle de la réponse.

Ainsi, anticiper va consister à automatiser la cybersécurité avec l'IA pour se renforcer face aux attaques cyber plus nombreuses et complexes, pour détecter et qualifier plus rapidement, réduire les faux positifs et accélérer les remédiations. Cependant, cette efficacité doit passer par la qualité des données d'entraînement, la formation des analystes et la gouvernance des modèles d'IA. ■

les violations de données ont atteint des niveaux records avec un coût mondial moyen en augmentation de 10 % en un an

JEAN-MARC JACQUOT

Fondateur, Expert-conseil et Cybersécurité, Nextaura et Lexaura
CoAnimateur du GT SASE/ SSE Clusif

IA ET CYBERSÉCURITÉ : UN DUO À DOUBLE TRANCHANT

QUAND L'IA S'INVITE DANS LES SOLUTIONS DE CYBERSÉCURITÉ

Avant que l'Intelligence Artificielle ne prenne le devant de la scène, la cybersécurité occupait déjà une place de choix parmi les sujets les plus débattus. Bien que le premier s'immisce partout, la cybersécurité est tellement transverse qu'il était impensable que ce combo ne devienne pas une vedette à lui seul.

Les éditeurs de solutions en cybersécurité l'ont bien compris, implémenter de l'IA dans leurs produits peut leur donner un avantage concurrentiel significatif. Toutefois, toutes les IA ne se valent pas : seul un modèle bien entraîné, intégré et contrôlé peut produire des résultats tangibles. Par exemple quand on parle d'analyser des logs de manière croisée, l'IA s'avère particulièrement pertinente avec sa capacité à analyser des masses de données de manière très efficace. Elle permet notamment de faire ressortir les signaux faibles qu'un système classique n'aurait pas détecté sous peine de générer trop de faux positifs.

AUTOMATISER LES TESTS DE SÉCURITÉ GRÂCE À L'IA

L'IA peut aussi être mise à profit pour tester les règles de vos pares-feux. En générant un jeu de test à partir de règles validées sur des environnements de production, puis en automatisant la récupération des règles en place, vous pouvez rejouer ce jeu de test à intervalles réguliers pour vous assurer que tout est conforme. Cela permet de détecter des erreurs humaines ou des règles trop permissives qui n'auraient pas dû être implémentées, le tout sans générer de trafic.

QUAND L'IA DEVIENT UNE MENACE POUR LA CYBERSÉCURITÉ

Au-delà de son utilisation pour renforcer la cybersécurité, l'intelligence artificielle soulève également ses propres enjeux en matière d'éthique et de sécurité. Elle peut être utilisée pour automatiser la génération de contenus malveillants, faciliter des attaques sophistiquées comme l'empoisonnement de données d'apprentissage, ou encore contourner les défenses traditionnelles. L'opacité de certains modèles, la difficulté à garantir l'intégrité des résultats, et la dépendance croissante à des services externes soulèvent des questions majeures de gouvernance, de traçabilité et de souveraineté numérique. À mesure que les modèles gagnent en puissance, leur supervision devient un enjeu stratégique majeur pour les entreprises.

Ces enjeux requièrent une expertise très spécialisée, de nouveaux métiers d'experts voient le jour et l'ensemble étant encore tellement récent qu'il est pour l'instant difficile de trouver des personnes véritablement qualifiées… une aubaine pour les esprits mal tournés ? Potentiellement…

DEEPFAKES, PHISHING ET USURPATION D'IDENTITÉ À GRANDE ÉCHELLE

Justement de l'autre côté du scope, les cybercriminels ont également bien compris qu'en couplant des solutions d'IA (par exemple Générative) avec de l'automatisation. Ils peuvent désormais mener des campagnes de phishing de masse, et envoyer des messages impeccables et très personnalisés, en reprenant les principes actuellement appliqués dans les campagnes marketing efficaces. En allant plus loin, ils peuvent également se faire passer pour presque n'importe qui ayant publié des vidéos sur les réseaux sociaux en répliquant leurs voix…

On s'approche rapidement de la possibilité de pouvoir faire pareil en temps réel avec la vidéo en direct.

VERS UNE CRISE DE CONFIANCE NUMÉRIQUE ?

La confiance dans ce que nous voyons ou entendons devient une question cruciale. Pourra-t-on encore faire confiance aux personnes que l'on voit en visio demain ? Pendant quelque temps encore, certains éléments de langage ou de posture permettront sans doute de différencier l'humain de la machine. Mais ce n'est probablement plus qu'une question de mois avant que ce genre de « détails » puisse aussi être répliqué. Cette crise de confiance ne peut que générer de nouvelles opportunités qui adresseront ces problématiques.

IDENTITÉS, GOUVERNANCE ET AVENIR DE LA CYBERSÉCURITÉ

Nous vivons une époque formidable dans laquelle l'authentification et la gestion des identités sont aujourd'hui au cœur des priorités des RSSI. Mais de manière générale, la cybersécurité reste un pilier incontournable de notre avenir numérique et elle a encore de beaux jours devant elle.

PS : Promis ce texte n'a pas été généré avec une IA Générative, mais peut-être m'a-t-elle quand même permis de l'améliorer… ■

toutes les IA ne se valent pas : seul un modèle bien entraîné, intégré et contrôlé peut produire des résultats tangibles.

STÉPHANE CALÉ

Administrateur Clusif

LES NOUVELLES TECHNOLOGIES (IA, QUANTIQUE, SASE, SOAR, XDR, ZERO TRUST...) ET LA CYBERSÉCURITÉ

En février 2023, un trio de chercheurs a réussi à décrypter une cinquantaine de lettres écrites par Marie Stuart entre 1578 et 1584. Ces lettres étaient principalement adressées à l'ambassadeur de France alors qu'elle était emprisonnée, par ordre de la reine d'Angleterre Élisabeth Ire.

L'INFORMATIQUE QUANTIQUE

Il en est ainsi de tous les secrets qui sont chiffrés, un jour, quelqu'un arrivera à les décrypter. Et c'est tout l'enjeu aujourd'hui de l'arrivée de l'informatique quantique. Car elle devrait permettre de résoudre des problèmes mathématiques insolubles avec nos moyens actuels et qui sont à la base des algorithmes à clé publique. Ainsi, par exemple, l'algorithme de Shor devrait permettre de factoriser de grands nombres premiers. Ce pilier des mathématiques, sur lequel reposent de nombreux algorithmes de chiffrement asymétriques, dont RSA, tient du fait qu'il est relativement simple de multiplier deux grands nombres premiers, mais très difficile de faire l'inverse, c'est-à-dire factoriser un nombre très grand en ses facteurs premiers.

Concernant la date à laquelle ces ordinateurs quantiques seront pleinement opérationnels, M. Jensen Huang (cofondateur et directeur général de NVIDIA) a déclaré : « Si vous disiez 15 ans, vous seriez probablement optimiste. Et si vous disiez 30, vous seriez pessimiste. Mais si vous optez pour 20 ans, je pense que beaucoup d'entre nous le croiraient ».

Ainsi, vos secrets, protégés avec les solutions actuelles, devraient pouvoir être lus dans un avenir proche. C'est pourquoi, il est important de commencer dès aujourd'hui à se préparer à cette rupture technologique. En 2017, le NIST (National Institute of Standards and Technology) a donc lancé un appel à projets pour sélectionner des algorithmes de cryptographie post-quantique, capables de résister aux attaques potentielles des ordinateurs quantiques. Le 13 août 2024, le NIST a publié les versions finales de ses trois premières normes de cryptographie post-quantique qui a été suivi le 11 mars 2025 par la publication de l'algorithme HQC pour l'encapsulation /échange de clés.

Mais le problème est que comme ce domaine de recherche est récent, il est très difficile d'être certain, malgré toutes les précautions qui ont été prises, que ces nouveaux algorithmes de chiffrement sont résistants aux attaques. Ainsi en juillet 2022, l'algorithme SIKE, codéveloppé par Microsoft et Amazon, qui avait été soumis à la compétition du NIST, a été cassé par deux chercheurs belges de l'Université Catholique de Louvain, en 1 heure, grâce à un ordinateur utilisant un processeur Intel Xeon E5-2630 sorti en 2013 …

l'algorithme de Shor devrait permettre de factoriser de grands nombres premiers.

QUELLES SOLUTIONS ?

Alors que faire ? L'ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information) nous alerte sur le fait que des attaquants pourraient dès aujourd'hui intercepter et stocker vos informations confidentielles chiffrées afin de pouvoir, dans quelques années, les décrypter (attaque dite « Store Now, Decrypt Later ») ou porter atteinte à leur intégrité (ex : modification d'une signature électronique). C'est pourquoi, l'ANSSI recommande :

- pour le chiffrement asymétrique de mettre en œuvre dès aujourd'hui, des mécanismes hybrides qui combinent l'utilisation d'algorithmes pré-quantiques reconnus avec des algorithmes post-quantiques. Car « cela permet de bénéficier à la fois de la forte assurance sur la résistance du premier contre les attaquants classiques et de la résistance conjecturée du second contre les attaquants quantiques ».
- pour le chiffrement symétrique d'avoir « le même niveau de sécurité que l'AES-256 pour les algorithmes de chiffrement par bloc et au moins le même niveau de sécurité que SHA2-384 pour les fonctions de hachage »

L'ANSSI recommande également de mettre en œuvre des infrastructures « cryptoagile », notion dont elle donne une définition : « la cryptoagilité signifie qu'en plus de la possibilité de faire des correctifs, les produits pourraient avoir la capacité de permettre des mises à jour d'algorithmes cryptographiques afin de réagir aux recommandations à venir et aux mises à jour de normes ».

Et le temps presse car le NIST (National Institute of Standards and Technology) a déjà indiqué qu'il considèrerait comme obsolète les algorithmes asymétriques RSA-2048 et ECC-25 à partir de 2030 et qu'ils seront complètement interdits à partir de 2035.

[1]https://www.histoire-et-civilisations.com/actualite/le-mystere-enfin-resolu-des-lettres-cryptees-de-marie-stuart-87972.php
[2]https://fr.wikipedia.org/wiki/Algorithme_de_Shor
[3]https://actualitecloud.com/jensen-huang-predit-les-ordinateurs-quantiques-pleinement-fonctionnels-arriveront-dans-20-ans/?utm_source=chatgpt.com
[4]https://en.wikipedia.org/wiki/NIST_Post-Quantum_Cryptography_Standardization
[5]https://www.solutions-numeriques.com/un-algorithme-de-chiffrement-post-quantique-casse-en-1-heure-avec-un-xeon-de-2013/
[6]https://cyber.gouv.fr/sites/default/files/2022/04/anssi-avis-migration-vers-la-cryptographie-post-quantique.pdf
[7]https://cyber.gouv.fr/sites/default/files/document/AvisdelANSSIsurlamigrationverslacryptographie.pdf
[8]https://nvlpubs.nist.gov/nistpubs/ir/2024/NIST.IR.8547.ipd.pdf

AYMERIC BERRENDONNER

CISO, Memority

SELON VOUS, LES NOUVELLES TECHNOLOGIES (IA, QUANTIQUE, SASE, SOAR, XDR, ZERO TRUST...) ET LA CYBERSÉCURITÉ

GS MAG : *Selon vous, quels sont les enjeux au sujet des Nouvelles Technologies (IA, QUANTIQUE, SASE, SOAR, XDR, ZERO TRUST...) en Cybersécurité ?*

AB : Quand on se pose cette question et qu'on souhaite y répondre objectivement, on se doit de garder en tête des principes essentiels : tout d'abord, les nouvelles technologies d'aujourd'hui seront les technologies obsolètes de demain. Nous parlons aujourd'hui d'XDR comme nous parlions hier d'EDR, avant-hier d'antivirus. Quand on parle d'IA aujourd'hui comme une nouvelle technologie, c'est en fait un vieux sujet. J'ai eu mon diplôme d'Ingénieur en Informatique en 2001 et l'une des deux spécialités que j'avais choisies était justement l'intelligence artificielle. Ce qui est nouveau aujourd'hui réellement, c'est l'accès démocratisé aux LLM et l'industrialisation d'algorithmes de Machine Learning. Mais que ce soit il y a 25 ans ou aujourd'hui, le but d'une technologie comme l'IA n'a pas changé : il est de faciliter l'exécution de tâches. Et c'est précisément ce qui m'amène à mon second principe.

La technologie est un outil, rien d'autre. L'enjeu se situe donc exclusivement dans l'usage qui en est fait. Un tournevis dans la main d'un menuisier aura une fonction. Dans la main d'un meurtrier, il en aura une bien différente. Et dans la main d'un comptable, il n'aura plus aucune utilité.
Des outils comme les SASE, SOAR, XDR seront pour les uns des outils adaptés de protection contre des menaces, et pour les autres, de nouveaux sommets à franchir, pour certains ils n'auront aucun intérêt.

Les usages n'ont d'ailleurs généralement qu'un seul but : faciliter l'activité. Que ce soit un business lucratif, une action humanitaire, un service essentiel d'intérêt public ou un cartel cybercriminel.

Enfin, même à l'échelle des organisations, il existe une sorte de pyramide de Maslow. Ainsi, parler de Zero Trust quand les bases de la gestion des identités et des accès ne sont pas en place, ce n'est pas adapté.

Cela étant dit, quels sont donc les enjeux ? La réponse est simple, il faut revenir systématiquement aux fondamentaux : bien comprendre le contexte, les usages, les besoins, nos objectifs. Puis, comprendre de quoi et de qui on doit se protéger ? Enfin quel est notre budget ?

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, afin de gérer au mieux les cybermenaces induites par les Nouvelles Technologies ? Et pour quelles raisons ?*

AB : En tant que professionnel de la cybersécurité, je propose d'aborder chaque technologie de manière holistique en se posant les questions suivantes :

- En quoi cette technologie est-elle une menace en elle-même ?
- En quoi cette technologie va-t-elle changer les usages, et quelle est la nouvelle posture de sécurité à adopter ?
- Est-ce que cette technologie me permet de m'aider à faire face aux menaces ?
- Et surtout : en quoi cette technologie peut-elle aider le business ?

A titre d'exemple, à l'heure à laquelle j'écris ces lignes, mon équipe finalise une « Artificial Intelligence Security Policy » additionnée de deux standards, l'un d'analyse de risque IA à destination de nos ingénieurs sécurité, et l'autre de sécurité de l'IA, à destination de l'ensemble de l'entreprise. Là où hier, nous ne diffusions que quelques bonnes pratiques d'usage des chatbots, pour éviter par exemple la fuite de données, à partir d'aujourd'hui l'ensemble des problématiques liées à l'IA seront structurées. Toujours l'usage d'IA externes bien sûr, mais également la gestion de la menace augmentée par l'IA, l'usage de modèles d'IA internes, l'usage de modèles d'IA pour enrichir l'offre à nos clients, l'IA en tant qu'outil de défense, les tests de robustesse de l'IA, ou encore la gestion de l'IA sous l'angle réglementaire en particulier celui des impacts sur les personnes.

Chaque professionnel de la cyber doit à mon sens adopter cette approche par les risques et les besoins.

GS MAG : *Quelles évolutions, à court, moyen ou long terme, voyez-vous dans ce domaine des Nouvelles Technologies ?*

AB : Pour moi les circonstances sont toujours à la source des évolutions technologiques. Et aujourd'hui les circonstances géopolitiques sont à tout point de vue exceptionnelles. Suivez la pyramide de Maslow évoquée précédemment et ayez confiance en l'instinct de survie.

Je pense qu'à moyen terme, deux sujets vont se renforcer : Tout d'abord les principes de Zero Trust. Je n'aime pas ce terme qui reste assez flou et est pourtant utilisé partout, mais nous observons aujourd'hui avec incrédulité un allié historique se retourner contre nous, c'est bien d'une crise de confiance qu'il est sujet ici, et à l'échelle des systèmes informatiques, ces sujets vont être de plus en plus pris au sérieux, rentrer dans les réflexes métier, devenir une évidence.

De la même manière, la protection de la donnée au plus près va être renforcée, avec des sujets comme le confidential computing, la généralisation du BYOK (Bring your own key) permettant un vrai chiffrement applicatif et certainement, parce que le besoin sera renforcé et donc les budgets de recherche iront avec, des avancées dans le chiffrement homomorphique. L'ensemble de ces sujets permettant de continuer à travailler avec des acteurs en qui on aura désormais moins confiance tout en maintenant un niveau de protection acceptable de nos données.

Enfin, parce que c'était déjà le cas, il faudra dès aujourd'hui maitriser plus que jamais la cartographie de ses données sensibles, avec désormais un facteur temps.

Là où on se posait une question « cette donnée est-elle sensible ? Si oui, je la chiffre » il faut dès aujourd'hui se poser une nouvelle question : « cette donnée sensible aujourd'hui aura-t-elle toujours la même valeur dans plusieurs mois ? Si oui, je la chiffre au plus tôt avec des algos post-quantiques ». ■

Mais que ce soit il y a 25 ans ou aujourd'hui, le but d'une technologie comme l'IA n'a pas changé : il est de faciliter l'exécution de tâches.

memority

L'IDaaS européen qui accélère votre business

- IAM
- IGA
- Fédération
- CIAM
- SSO
- MFA

- Employés
- Partenaires
- Clients
- Citoyens
- Objets connectés

www.memority.eu

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

SELON VOUS, LES NOUVELLES TECHNOLOGIES (IA, QUANTIQUE, SASE, SOAR, XDR, ZERO TRUST...) ET LA CYBERSÉCURITÉ

GS MAG : *Selon vous, quels sont les enjeux au sujet des Nouvelles Technologies (IA, QUANTIQUE, SASE, SOAR, XDR, ZERO TRUST...) en Cybersécurité ?*

LG : Toute nouvelle technologie IT présente irrémédiablement deux facettes : une première facette « fonctionnelle » et une seconde« cybersécurité ». Certaines nouvelles technologies comme le SASE, SOAR, XDR, ZERO TRUST sont intrinsèquement orientées cyber : c'est leur rôle que d'apporter un nouveau service cyber, de faciliter un service existant en l'automatisant, en étant plus en amont, etc. Reste à vérifier qu'elles n'introduisent pas une nouvelle vulnérabilité, typiquement par une faiblesse dans leur implémentation ! Pour l'IA et le quantique, les enjeux ne sont pas de même nature. Ces technologies impactent structurellement la cybersécurité.

Le calcul quantique remet en cause les schémas de cryptographiques actuels à base de clés publiques, sur lesquels s'appuie la confiance numérique, rien de moins. Et il ouvre, à marche forcée hybride d'ici 2030-2032, la transition vers une cryptographie post-quantique (c'est-à-dire résistante aux attaques de l'ordinateur quantique...).

L'IA d'un côté promet une simplification des travaux de détection d'attaques, de soutien aux analystes SOC... Mais s'avère en même temps support aux développements de phishing dans des contrées préservées jusque-là (ainsi entre 2023 et 2024, les attaques au Japon ont quasiment doublées, voire quintuplées via les URL malicieuses !) ou un brillant coach pour la génération de code malicieux. L'IA générative particulièrement présente un risque de sécurité important pour 64 % des RSSI français comme l'indique le dernier rapport Voice of the CISO de Proofpoint. Sans parler de ce qui concerne à plus proche distance les organisations : le développement d'un shadow IA, avec exfiltration de données sensibles, rapports à synthétiser ou à traduire vers des environnements incontrôlés.
Un grand classique finalement !

>>>

>>> **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, afin de gérer au mieux les cybermenaces induites par les Nouvelles Technologies ? Et pour quelles raisons ?*

LG : Pour le quantique, tout est parfaitement dit par l'ANSSI avec son guide de 2024. La particularité de cette transition nécessaire est la menace d'attaques rétroactives (dites SNDL « store now, decrypt later » et pratiquées de toute évidence par américains et chinois à grande échelle) qui nécessite une prise en compte de ce risque dès aujourd'hui (avant même de savoir si le développement d'un ordinateur quantique performant est réalisable !).

Pour l'IA, tout un pan de nouvelles analyses de risque est en train de se développer et de s'outiller (infrastructures, modèles, données d'entraînement, données de travail, prompts… sont concernés). À revoir sur le site Clusif, les extraits éclairants du dernier Panorama Annuel de la Cybercriminalité, aka PANOCRIM. Et les RSSI français sont bien avancés sur ces sujets et largement à l'écoute des opportunités que présentent l'IA, notamment lorsqu'il s'agit d'adresser les risques liés à l'humain. En 2024, le rapport Proofpoint indique également que 89% d'entre eux cherchaient déjà à déployer des capacités basées sur l'IA pour se protéger contre les erreurs humaines et les menaces centrées sur l'humain.

GS MAG : *Quelles évolutions, à court, moyen ou long terme, voyez-vous dans ce domaine des Nouvelles Technologies ?*

LG : Ces nouvelles technologies autour du quantique et de l'IA évoluent de façon très particulière : théorisées de longue date (avant les années 1980), elles émergent aujourd'hui, massivement opérationnelles 50 ans plus tard et de façon concomitante. Du jamais vu ! Au cœur des confrontations géopolitiques actuelles entre les USA, la Chine et la Russie. Sous des formes assez visibles comme la course aux composants électroniques, le meilleur modèle d'IA, mais aussi sous des formes diffuses comme l'empoisonnement des modèles de l'Ouest par des masses d'informations et de narratifs pro-russes…
Le « meilleur » reste à venir.

À court terme, le véritable enjeu reste de maîtriser les risques avérés et persistants. Le constat est qu'importe le vecteur d'attaque et les technologies utilisées, le facteur humain continue d'être une des plus grandes vulnérabilités des entreprises pour 82 % des RSSI français interrogés dans l'étude Proofpoint. Un chiffre qui ne cesse d'augmenter d'année en année puisqu'il était à 75 % en 2023. ■

Pour l'IA et le quantique, les enjeux ne sont pas de même nature. Ces technologies impactent structurellement la cybersécurité.

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

CLUSIF

GÉRÔME BILLOIS

Membre du CA Clusif et CoAnimateur GT Panocrim + Partner Cybersecurity and Digital Trust, Wavestone + Auteur : CYBERATTAQUES, les Dessous d'une Menace Mondiale

SELON VOUS,

LES NOUVELLES TECHNOLOGIES

(IA, QUANTIQUE, SASE, SOAR, XDR, ZERO TRUST...) ET LA CYBERSÉCURITÉ

Simultanément, l'IA commence à jouer un rôle significatif dans les outils et fonctions de sécurité.

GS MAG : *Selon vous, quels sont les enjeux au sujet des Nouvelles Technologies (IA, QUANTIQUE, SASE, SOAR, XDR, ZERO TRUST...) en Cybersécurité ?*

GB : Les nouvelles technologies en cybersécurité sont nombreuses et présentent des défis variés selon différentes perspectives. À court terme, il s'agit d'intégrer des solutions efficaces comme SASE et SOAR sans complexifier l'écosystème existant.

À long terme, des tendances majeures telles que l'IA, le quantique ou le Zero Trust redéfinissent durablement les approches de sécurité.Dans ce contexte où les RSSI utilisent souvent une multitude d'outils différents, la rationalisation des outils, des processus et des équipes est et restera essentielle pour les organisations, en réponse à une demande croissante d'efficacité et d'optimisation.

Les nouvelles technologies en cybersécurité sont nombreuses et présentent des défis variés selon différentes perspectives.

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, afin de gérer au mieux les cybermenaces induites par les Nouvelles Technologies ? Et pour quelles raisons ?*

GB : L'accélération et la sophistication des cybermenaces affectent particulièrement les nouvelles technologies et nécessitent de repenser les dispositifs classiques de gestion des risques. Avec l'avènement du quantique, le chiffrement tel que nous le connaissons est remis en question, nécessitant de nouveaux algorithmes. L'intelligence artificielle introduit des menaces spécifiques telles que l'empoisonnement de données et l'évasion, amplifiées par l'automatisation croissante des actions via l'IA agentique. Ces évolutions obligent également les régulateurs à renforcer leurs exigences pour encadrer l'utilisation des nouvelles technologies.Il est donc impératif de réinventer nos dispositifs de sécurisation, non seulement dans les processus mais aussi en identifiant les nouveaux risques et en mettant en place de nouvelles contre-mesures. Bien que cela demande des efforts importants, la filière cybersécurité est prête à faire face aux défis, permettant ainsi la réalisation du concept « Secure by design ». Il sera toutefois nécessaire de s'adapter en continu face à l'évolution rapide de ces technologies.

GS MAG : *Quelles évolutions, à court, moyen ou long terme, voyez-vous dans ce domaine des Nouvelles Technologies ?*

GB : Le domaine des technologies en cybersécurité évolue actuellement avec une tendance vers les solutions « good enough », privilégiant l'efficacité opérationnelle plutôt que la recherche du produit parfait « best of breed ». Cette approche se concrétise par le choix de plateformes de sécurité intégrant de multiples fonctionnalités, prisée par les RSSI. Simultanément, l'IA commence à jouer un rôle significatif dans les outils et fonctions de sécurité.

Bien qu'il soit crucial d'évaluer ses apports opérationnels, il est tout aussi important de considérer les risques associés. Des cas d'usage concrets émergent, notamment dans la classification des documents, l'enrichissement et la simplification des alertes du SOC, ainsi que la gestion des tiers. Ces technologies, présentes et futures, ont le potentiel de transformer radicalement la pratique de la sécurité informatique pour les équipes cyber.

SCALITY

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

Fédération Française de la Cybersécurité

Fédérer · Représenter · Valoriser l'écosystème cyber français

Une fédération au service des acteurs de la cybersécurité

La Fédération Française de la Cybersécurité (FFC) est une organisation indépendante qui rassemble les acteurs publics, privés, associatifs et académiques de la cybersécurité. Elle agit comme une plateforme de coopération à l'échelle nationale et territoriale, pour renforcer la structuration de l'écosystème cyber français et porter une voix collective.

Nos missions concrètes

- Publier chaque année la cartographie nationale de l'écosystème cyber
- Animer des groupes de travail sectoriels (santé, IA, cloud, territoires, souveraineté…)
- Diffuser des notes stratégiques et capsules d'analyse (AI Act, RSSI augmenté, NIS2, etc.)
-Organiser ou coanimer des webinaires et événements
- Représenter l'écosystème sur les grands salons (FIC, Ready for IT, CAP IT, GS Days…)

-La Fédération Française de la Cybersécurité organise également des événements conviviaux réservés à ses adhérents, afin de favoriser les échanges, le partage d'expérience et le renforcement des liens au sein de la communauté cyber.
- Accompagner les membres dans leur visibilité et leurs connexions stratégiques

Rejoignez la Fédération

- Bénéficiez d'un réseau structurant et fédérateur
- Profitez d'une mise en valeur sur les salons et médias partenaires
- Engagez-vous dans les réflexions sectorielles et les groupes de travail
- Valorisez vos actions et développez votre présence au cœur de l'écosystème cyber

📧 contact@ffcybersecurite.org

🌐 www.ffcybersecurite.org

🔗 LinkedIn : Fédération Française de la Cybersécurité

CÉDRIC CAILLEAUX

Membre Clusif
+ Chef d'Entreprise,
Axians Cybersecurity,
ex-RSSI

SELON VOUS, LES NOUVELLES TECHNOLOGIES (IA, QUANTIQUE, SASE, SOAR, XDR, ZERO TRUST...) ET LA CYBERSÉCURITÉ

GS MAG : *Selon vous, quels sont les enjeux au sujet des Nouvelles Technologies (IA, QUANTIQUE, SASE, SOAR, XDR, ZERO TRUST...) en Cybersécurité ?*

CC : Il est évident que l'évolution rapide des nouvelles technologies impacte profondément le domaine de la cybersécurité. L'intelligence artificielle, l'informatique quantique, le Zero Trust, les solutions SASE, SOAR et XDR entre autres redéfinissent la manière dont les organisations protègent leurs actifs numériques. Ces transformations impliquent des défis majeurs en matière de détection des menaces, d'automatisation de la réponse aux incidents et d'adaptation aux nouvelles menaces cybernétiques. Pour moi, en tant que dirigeant d'entreprise en cybersécurité chez Axians Cybersecurity, ces technologies représentent une opportunité d'innovation et de différenciation sur un marché en constante évolution.

L'intelligence artificielle (IA) révolutionne la cybersécurité en permettant une détection proactive des menaces grâce à l'analyse de grandes quantités de données en temps réel. Les solutions XDR et SOAR, largement adoptées dans les SOC modernes, facilitent la réponse aux incidents en automatisant les processus de détection et de remédiation. L'IA est désormais un moteur central du développement des outils de cybersécurité modernes. Elle permet d'analyser des volumes massifs de données en temps réel, d'identifier des menaces inconnues, de détecter des anomalies et de répondre plus rapidement et efficacement aux incidents. Les algorithmes d'IA peuvent apprendre de nouveaux comportements des attaquants et s'adapter aux stratégies en constante évolution, augmentant ainsi la capacité des systèmes de sécurité à protéger les infrastructures critiques face à des attaques sophistiquées. Plusieurs éditeurs intègrent déjà l'IA dans leurs solutions de cybersécurité afin d'identifier et stopper les menaces avant qu'elles n'affectent l'entreprise, en clair elle détecte des attaques en temps réel et génère des réponses automatiques aux incidents. Il est important pour nos organisations d'exploiter l'IA pour offrir une cybersécurité plus proactive, prédictive et adaptative, en permettant une gestion des risques plus fluide et une meilleure protection contre des attaques de plus en plus complexes. Mais l'IA ne profite pas uniquement aux défenseurs. Certains groupes cybercriminels ont intégré l'intelligence artificielle dans leurs attaques, notamment

pour développer des ransomwares, concevoir des scripts malveillants et mener des campagnes de spear-phishing mais également concevoir des attaques de type « deep-fake ». Ces derniers ont émergé comme une menace sérieuse dans le domaine de la cybersécurité. En utilisant des techniques de manipulation vidéo, audio ou d'images, les attaquants peuvent créer des contenus falsifiés très réalistes qui peuvent tromper des individus ou des organisations et je crains que cela ne soit plus que jamais préjudiciable en 2025.

Parallèlement, l'informatique quantique représente une double menace et une opportunité pour la cybersécurité. Les progrès réalisés par Google et IBM dans le domaine de la suprématie quantique soulèvent la question de la résistance des algorithmes cryptographiques actuels. D'ailleurs en 2024, l'ANSSI a recommandé aux organisations de se préparer à la transition vers des algorithmes post-quantiques. Certains états et groupes cybercriminels stockent d'ores et déjà des données chiffrées dans l'espoir de les déchiffrer une fois les capacités quantiques suffisantes.

Le paradigme Zero Trust devient incontournable dans un monde où les cyberattaques se multiplient. L'adoption des solutions SASE permet aux entreprises de sécuriser leurs infrastructures hybrides et le télétravail, tout en améliorant la flexibilité et la réactivité des équipes de cybersécurité. Mais après le Zero Trust, qui repose sur le principe de "Ne jamais faire confiance, toujours vérifier", plusieurs tendances émergent pour renforcer encore davantage la cybersécurité comme par exemple le Zero Trust Continu (ZT-C) qui pousse le concept plus loin en instaurant un contrôle dynamique et en temps réel basé sur l'analyse comportementale des utilisateurs et des systèmes comme l'IA comportementale ou l'UEBA (User and Entity Behavior Analytics) qui utilise également des techniques de Machine Learning pour créer des profils comportementaux basés sur les actions passées des utilisateurs.

Cependant, je crois que l'évolution du Zero Trust pourrait bien conduire vers une IA auto-défensive. Cette IA pourrait adapter en temps réel les politiques de sécurité en fonction des menaces émergentes. Plutôt que d'appliquer des règles statiques, un système d'IA pourrait apprendre et automatiser les ajustements des contrôles d'accès et de sécurité. Le Zero Trust n'est pas une fin en soi mais je vois cela plutôt comme une transition vers des modèles de sécurité plus dynamiques et adaptatifs. L'avenir reposera sans nul doute vers des approches plus intelligentes, contextuelles et autonomes, avec un contrôle granulaire des identités, des données et des accès en fonction du risque en temps réel.

L'intelligence artificielle (IA) révolutionne la cybersécurité

Je pense que dans mes fonctions, l'innovation technologique est un levier de différenciation stratégique. Certaines entreprises ont transformé le marché en développant des solutions basées sur l'IA capables d'automatiser la détection et la remédiation des menaces. L'évolution réglementaire, avec des cadres comme NIS 2 et DORA, pousse également les entreprises à renforcer la résilience de leurs infrastructures et à proposer des solutions conformes aux nouvelles exigences légales. Par ailleurs, la pénurie de talents dans le domaine de la cybersécurité constitue un défi majeur.

Les nouvelles technologies transforment profondément la cybersécurité et obligent les RSSI à repenser leurs stratégies de protection. Les entreprises du secteur doivent aussi innover pour répondre aux défis croissants. À mes yeux, la convergence entre ces deux visions, celle de la sécurité et de l'innovation, est essentielle pour construire un écosystème numérique résilient et sécurisé.

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, afin de gérer au mieux les cybermenaces induites par les Nouvelles Technologies ? Et pour quelles raisons ?*

CC : Aujourd'hui, les nouvelles technologies se développent à un rythme rapide, apportant des opportunités excitantes, mais aussi des cybermenaces de plus en plus complexes. Face à cette réalité, les entreprises, comme Axians, doivent déployer des stratégies solides pour protéger non seulement leurs actifs, mais aussi ceux de leurs clients.

Le rôle du RSSI est de protéger le patrimoine informationnel de son entreprise tout en facilitant l'innovation. Il met en place plusieurs actions pour réduire les risques liés aux cyberattaques. Par exemple, l'approche Zero Trust permet entre autres de limiter la propagation des attaques en segmentant les réseaux et en appliquant des contrôles d'accès stricts. Mais au-delà de la technologie, il est impératif de sensibiliser et former continuellement les employés aux bonnes pratiques en matière de cybersécurité, car l'erreur humaine est l'un des vecteurs d'attaque les plus exploités par les cybercriminels.

>>>

>>> La mise en place d'un centre opérationnel de sécurité (SOC) est une autre réponse efficace face aux cybermenaces. Il permet une surveillance en continu, une détection rapide des incidents et une réaction immédiate pour en limiter l'impact. Pour accroître son efficacité, il est essentiel d'intégrer une solution de Security Orchestration, Automation and Response (SOAR), qui permet d'automatiser la gestion des incidents, d'accélérer les processus de réponse et d'améliorer la collaboration entre les équipes de sécurité. L'enjeu principal du SOAR est de réduire le temps de réaction face aux cyberattaques en orchestrant différents outils de cybersécurité et en automatisant certaines tâches répétitives, libérant ainsi du temps pour les analystes SOC qui peuvent se concentrer sur des menaces complexes.

Les solutions de type Endpoint Detection and Response (EDR) et Extended Detection and Response (XDR) sont également devenues incontournables. Ces technologies offrent une visibilité accrue sur les activités suspectes et permettent une réponse rapide et automatisée aux incidents de sécurité. L'XDR se distingue notamment par sa capacité à corréler des données issues de multiples sources pour détecter les attaques sophistiquées que des outils classiques ne pourraient identifier individuellement.

Une équipe CSIRT (Computer Security Incident Response Team) doit être mise en place pour répondre aux incidents de manière organisée et efficace. Son rôle est d'analyser, contenir et éradiquer les menaces identifiées, tout en documentant les incidents pour en tirer des leçons et améliorer les dispositifs de protection. En parallèle, l'implication d'un CERT (Computer Emergency Response Team) interne ou externe est souvent nécessaire pour une approche plus globale. Ce dernier joue un rôle clé dans la coordination des réponses aux menaces à l'échelle nationale ou sectorielle, en collaborant avec d'autres entités pour partager des renseignements sur les menaces émergentes et les meilleures pratiques de défense.

Pour éviter les failles de sécurité, le RSSI doit également s'assurer que des audits de vulnérabilités sont réalisés régulièrement et que les correctifs de sécurité sont appliqués dès leur disponibilité. L'alignement sur les réglementations et normes en vigueur, comme l'ISO 27001, le RGPD ou encore la directive NIS2 et la réglementation DORA, permet de structurer les efforts de cybersécurité et d'assurer un niveau de protection adapté aux risques.

Chez Axians, l'accompagnement des clients est une priorité. Nombreuses sont les organisations qui ne disposent pas des compétences nécessaires en interne pour gérer efficacement leur cybersécurité. L'externalisation vers un prestataire de services de sécurité gérée (MSSP) leur permet d'accéder à une expertise pointue et de bénéficier de solutions avancées sans investir massivement dans des ressources internes. L'automatisation et l'intelligence artificielle sont également des leviers stratégiques pour ces entreprises. Grâce à ces technologies, la détection et l'anticipation des cyberattaques sont améliorées, offrant une réactivité accrue face aux menaces.

Pour répondre aux besoins spécifiques de chaque client, une approche personnalisée est essentielle. Une analyse approfondie des risques et du contexte de l'entreprise permet d'élaborer des stratégies sur mesure, adaptées aux contraintes opérationnelles et budgétaires. Parmi les méthodes utilisées, les tests d'intrusion et le Red Teaming jouent un rôle clé en simulant des cyberattaques réelles afin d'évaluer les points faibles des infrastructures informatiques et d'améliorer leur résilience.

Enfin, la cyber-résilience est un aspect clé. Se préparer à l'inévitable en mettant en place un plan de continuité d'activité (PCA) et des mécanismes de sauvegarde robustes est essentiel pour minimiser l'impact des cyberattaques. La capacité d'une entreprise à se remettre rapidement d'un incident est cruciale pour sa pérennité.

Dans un monde où les cybermenaces évoluent constamment, la collaboration entre entreprises et experts en cybersécurité est essentielle. Cette coopération permet d'adopter des solutions innovantes, réactives et adaptées aux besoins spécifiques de chaque organisation, tout en garantissant une cybersécurité efficace. L'objectif est de protéger les entreprises et d'accompagner leur transformation numérique sans freiner leur agilité ni leur compétitivité.

GS MAG : *Quelles évolutions, à court, moyen ou long terme, voyez-vous dans ce domaine des Nouvelles Technologies ?*

CC : La cybersécurité est en pleine révolution avec l'émergence de technologies toujours plus avancées, et je suis convaincu que l'intelligence artificielle (IA), qui occupe déjà une place centrale dans ce secteur, jouera un rôle encore plus déterminant dans les années à venir. Chaque jour, les menaces deviennent plus sophistiquées et complexes, mais l'IA offre des possibilités inédites pour anticiper, détecter et neutraliser ces attaques de manière plus proactive et efficace.

À court terme, l'IA est déjà utilisée pour améliorer la détection des menaces, en permettant des analyses de données en temps réel, souvent à une échelle impossible pour l'humain. Les systèmes d'EDR (Endpoint Detection and Response) et XDR (Extended Detection and Response), alimentés par l'IA, peuvent aujourd'hui détecter des anomalies dans les comportements des utilisateurs et des réseaux. Ces outils ne se contentent pas de réagir aux incidents, mais utilisent l'apprentissage automatique pour prédire de nouveaux types d'attaques en analysant des patterns complexes. Les cyberattaques de type Zero day, difficiles à détecter avec des systèmes traditionnels, peuvent ainsi être identifiées bien plus tôt grâce à cette capacité d'analyse comportementale avancée.

L'IA apporte également une réponse autonome aux attaques. Mais si on projetait un système capable non seulement de détecter un incident en temps réel, mais aussi d'y répondre de manière instantanée sans l'intervention humaine, cela permettrait de réduire considérablement le temps de réaction, en isolant un système compromis ou en bloquant l'accès d'un utilisateur suspect sans délai. Cette approche automatisée devient à notre époque cruciale face à la rapidité des cyberattaques modernes, comme les ransomwares, qui nécessitent une réponse quasi immédiate pour minimiser les impacts.

D'un point de vue stratégique, l'IA a la capacité de prédire les attaques avant même qu'elles ne surviennent. Au travers de de l'analyse prédictive, l'IA peut surveiller et analyser des données historiques pour identifier des motifs de comportements associés à des attaques imminentes. Cette approche permettrait aux entreprises de mieux se préparer et de renforcer leur défense avant que l'attaque ne devienne une menace réelle. L'anticipation devient ainsi un des atouts majeurs de l'IA, qui permet d'aller bien au-delà des stratégies de défense réactives traditionnelles.

De côté de l'authentification et la gestion des identités, je pense qu'ils bénéficieront également des avancées de l'IA. De nouvelles méthodes d'authentification biométrique, combinées à l'analyse comportementale, pourrait voir le jour en permettant par exemple de créer des profils utilisateurs dynamiques. L'IA pourra surveiller en permanence les actions des utilisateurs et ajuster les niveaux d'accès en fonction de leur comportement en temps réel, renforçant ainsi la sécurité du SI tout en garantissant une expérience fluide pour les utilisateurs légitimes.

Dans un avenir plus lointain, l'informatique quantique pourrait bouleverser la cybersécurité. Les ordinateurs quantiques ont la capacité de résoudre certains problèmes beaucoup plus rapidement que les ordinateurs classiques, menaçant ainsi de briser les systèmes de cryptographie actuels à plus ou longs termes. Sa combinaison avec l'IA pourrait jouer un rôle clé dans la cryptographie post-quantique, en aidant à développer de nouveaux algorithmes capables de résister aux attaques des ordinateurs quantiques. Il sera nécessaire de trouver un équilibre entre la puissance des ordinateurs quantiques et la capacité de l'IA à créer des mécanismes de défense adéquats. Mais au-delà de ses capacités de défense, l'IA pourrait aussi s'avérer un allié dans la simulation d'attaques. Tout comme les techniques utilisées par les équipes de Red Teaming, l'IA pourrait prendre en charge des tests d'intrusion à grande échelle.

Ces attaques simulées pourraient inclure des attaques avancées par IA, offrant une plateforme de test plus réaliste et plus évolutive pour évaluer la résilience des systèmes face à des menaces en constante évolution.

Les menaces internes, quant à elles, pourraient être mieux gérées grâce à l'IA. En analysant les comportements des employés et des utilisateurs, l'IA pourrait repérer les activités suspectes, comme des fuites de données ou des comportements malveillants. Cette capacité d'analyse comportementale permettrait de prévenir les attaques provenant de l'intérieur, un problème souvent difficile à détecter avec les méthodes classiques.

Enfin, l'IA permettra une gestion dynamique des risques et de la conformité. Alors que la régulation de la cybersécurité devient de plus en plus complexe et nombreuses (DORA, NIS2, REC, AI Act, ...), les systèmes intelligents pourront analyser en temps réel la conformité d'une entreprise aux exigences légales et réglementaires, et alerter instantanément en cas de non-conformité.

La mise en place d'un centre opérationnel de sécurité (SOC) est une autre réponse efficace face aux cybermenaces

Cela permettra non seulement de mieux se protéger contre les attaques, mais aussi de réduire les risques de sanctions en cas de violation des normes.

À long terme, l'IA promet donc de transformer considérablement la cybersécurité. Nous passerions d'un modèle IA générative vers un IA Autonome où les modèles pourraient être capables de prendre des décisions complexes avec un minimum d'intervention humaine pour finir vers l'Intelligence Artificielle Générale (IAG) où l'IA pourrait finalement effectuer n'importe quelle tâche cognitive aussi bien qu'un être humain. Et nous verrons apparaitre ainsi des SOC pilotés presque entièrement par IA, avec des réactions instantanées aux cyberattaques sans intervention humaine.

Je pense donc que l'IA deviendra non seulement comme c'est déjà le cas aujourd'hui à savoir une technologie permettant de détecter et de répondre aux menaces, mais aussi un acteur clé de l'anticipation, de l'automatisation et de l'adaptation des systèmes de sécurité. Cependant, si l'IA présente des avantages indéniables, elle soulève également des questions de gouvernance, d'éthique et de gestion des risques, car elle pourrait aussi devenir une arme entre les mains de cybercriminels. L'avenir de la cybersécurité sera donc une nouvelle fois un équilibre entre innovation technologique et vigilance constante face aux nouvelles menaces. ■

FRANCK LECUYER

Ingénieur Cybersécurité, UGAP
Correspondant DPO
Membre Clusif et CESIN
CoAnimateur du GT SOC Augmenté Clusif

SELON VOUS,

LES NOUVELLES TECHNOLOGIES (IA, QUANTIQUE, SASE, SOAR, XDR, ZERO TRUST...) ET LA CYBERSÉCURITÉ

GS MAG : *Selon vous, quels sont les enjeux au sujet de la Nouvelle Technologie VOC en Cybersécurité ?*

FL : Tout d'abord, il faut préciser ce que nous entendons par VOC. Le VOC n'est déjà pas une technologie. Nous sommes plutôt sur un service, un service dédié à la détection, la gestion et à la remédiation des vulnérabilités de sécurité.

Ce service n'est en soi, pas nouveau mais il a pris une dimension très importante ces 2 dernières années notamment avec l'évolution des menaces cyber et la forte nécessité d'avoir une posture proactive en matière de sécurité.

Cette gestion des vulnérabilités est d'autant plus nécessaire que les organisations sont de plus en plus exposées avec l'émergence des applications Saas, l'évolution constante vers des infrastructures hybrides notamment mais également la multiplication des objets connectés sur Internet (IOT : Internet Of Things).

Prenons l'exemple des objets connectés qui représentent un véritable défi pour des responsables de la sécurité des systèmes d'information (RSSI). Ces objets qui doivent être connectés sur Internet, ne sont parfois pas isolés du réseau de l'entreprise et sont souvent oubliés dans le processus de patch management. Cela peut être le cas d'un réfrigérateur connecté, d'un service de climatisation ou de chauffage pilotable à distance, des volets électriques via de la domotique. Ces objets présentent également des failles de sécurité et doivent être maintenus en condition opérationnel par le biais de patchs et/ou mises à jour.

Nous observons donc que les risques d'exposition se multiplient et les surfaces d'attaque de l'entreprise deviennent de plus en plus hétérogènes...

Le service VOC peut être interne à l'entreprise mais cela nécessite des moyens humains ce qui est un frein pour certains.

Ce service n'est en soi, pas nouveau mais il a pris une dimension très importante ces 2 dernières années notamment avec l'évolution des menaces cyber

GS MAG : *Quelles solutions de votre entreprise ou organisation permettent de gérer au mieux les cybermenaces grâce au VOC? Et pour quelles raisons ?*

FL : le prérequis indispensable dans la mise en place d'un service VOC est d'avoir au préalable défini une politique de gestion des vulnérabilités.

Elle fixe en effet les exigences de sécurité en matière de déploiement des mises à jour et définit la stratégie de gestion. Cela couvre un large panel d'actifs comme les systèmes d'exploitation, les firmwares des IOT, les composants réseau, les bases de données, les systèmes de communications unifiées…

Une fois cette politique définie, il est plus simple de mettre en place le service VOC.

Le service VOC peut être interne à l'entreprise mais cela nécessite des moyens humains ce qui est un frein pour certains. Il faut alors se tourner vers un service managé par un MSSP qui pilotera le service et assurera son bon fonctionnement.

L'organisation doit définir en amont la liste des assets à surveiller et indiquer leur criticité, la sensibilité des données, le type d'applications hébergé…

Le service VOC propose des scanners de vulnérabilité qui sont lancés à fréquence régulière en fonction des périmètres et dont les résultats sont analysés afin de définir avec l'organisation une feuille de route, un plan de remédiation avec des notions de priorités suivant l'exposition, l'exploitabilité de la faille et la difficulté à remédier.

L'inconvénient de ce type de scan est qu'ils ne sont pas à une fréquence très rapprochée. Pour pallier cette problématique temporelle, il est possible d'installer des agents sur les assets ce qui permet d'avoir des scans quotidiens et par conséquent de suivre plus précisément l'évolution des menaces sur le parc.

GS MAG : *Quelles évolutions, à court, moyen ou long terme, voyez-vous dans ce domaine du VOC ?*

FL : Tout d'abord, bien que nous puissions imaginer des passerelles naturelles entre le service SOC et celui du VOC, ce n'est pas forcément le cas, notamment parce que ce sont souvent des équipes différentes et que le service VOC est encore récent. Ce rapprochement entre ces services et la fluidité des échanges entre eux seront des enjeux importants à court terme.

Je pense également que le VOC intègrera, par le biais de ses outils, de l'intelligence artificielle et qu'intégré à un SOAR, il sera peut-être possible d'analyser l'impact d'une mise à jour, de patcher automatiquement sur des environnements de recette par exemple et de faire tous les contrôles post-opératoires de test de validation afin de faciliter le travail des équipes systèmes pour le déploiement futur en environnement de production.

Nous voyons bien que ce monde est en constante évolution et que le SOC « initial » augmente d'année en année en intégrant de nouvelles technologies, de nouveaux services comme le VOC.

C'est d'ailleurs un sujet traité par les membres du Clusif qui travaillent justement sur cette notion de SOC « augmenté ». Un podcast sur cette thématique est d'ailleurs disponible depuis début Avril sur ce sujet. Je vous invite à l'écouter en attendant la publication du document Clusif en 2026.

STÉPHANE LEMERLE

Membre Clusif
+ Directeur du Programme Domaine Souverain, Orange

SELON VOUS,

SOUVERAINETÉ NUMÉRIQUE ET LA CYBERSÉCURITÉ

L'intelligence artificielle (IA) souveraine devient un enjeu stratégique pour les Etats et les entreprises.

GS MAG : *Selon vous, quels sont les enjeux de la souveraineté numérique ?*

SL : la souveraineté numérique permet de garantir la sécurité, la continuité et l'autonomie stratégique d'une organisation dans la gestion de ses infrastructures, services et données, face à des menaces étrangères (notamment celles liées aux lois extraterritoriales comme le FISA et le Cloud Act). Elle favorise la liberté d'action et de décision d'une organisation, réduisant sa dépendance aux fournisseurs, services et infrastructures cloud non souveraines. Enfin, elle assure une conformité réglementaire et juridique, garantissant que les données sont traitées conformément aux lois locales, renforçant ainsi la confiance des clients et partenaires.

L'adoption du cloud est devenue une tendance majeure dans la transformation numérique, avec de nombreuses entreprises passant d'hébergements sur site à des solutions cloud dans une stratégie « cloud first ». Bien que cette évolution offre flexibilité et évolutivité, elle comporte des risques dus à des notions floues et mal définies.

Le Clusif souligne la distinction entre « confiance numérique », qui sécurise les données selon des normes strictes, et « souveraineté numérique », qui vise en plus, à garantir l'indépendance face à l'influence étrangère, essentielle pour les données stratégiques, contractuelles ou réglementaires.

Le Clusif souligne la distinction entre « confiance numérique », qui sécurise les données selon des normes strictes, et « souveraineté numérique »

GS MAG : *Quelles sont les stratégies et tactiques que vous conseillez d'appliquer pour répondre à ces enjeux ?*

SL : il est essentiel de réaliser une analyse des risques en tenant compte des menaces étatiques et des enjeux légaux. Le contexte géopolitique mondial engendre des incertitudes pour les entreprises utilisant des solutions de cloud non souveraines, rendant la maîtrise des données cruciale dans les discussions internationales.

Il est également nécessaire d'évoluer vers une meilleure gouvernance des données et une classification appropriée de l'information. Les données les plus sensibles, qualifiées de « souveraines », doivent être protégées contre les lois extraterritoriales, car leur divulgation ou indisponibilité peut avoir des impacts vitaux pour les entreprises ou organisations.

Les travaux du Clusif, accessibles en ligne, offrent 2 outils pour accompagner les RSSI, responsables des systèmes d'information, chefs de projets et acheteurs dans cette démarche.

Un guide technique complet :
Ce document analyse les enjeux du cloud, des risques stratégiques et opérationnels (espionnage, indisponibilité des services, saisie légale) aux questions de classification des données. Il propose une liste de critères différenciés pour évaluer les solutions selon des dimensions essentielles telles que la localisation des données, la nationalité des équipes techniques ou encore les certifications des hébergeurs.

Accéder au guide

Un questionnaire d'auto-évaluation personnalisé :
Identifiez et catégorisez vos besoins stratégiques, en fonction du niveau de confidentialité de vos données et des services utilisés. Ce questionnaire vous aide à orienter votre choix vers des offres d'hébergement adaptées, répondant à vos exigences en matière de sécurité et de confiance.

Accéder au questionnaire d'auto-évaluation

GS MAG : *Quelles évolutions, à court, moyen ou long terme, voyez-vous dans ce domaine ?*

SL : Une prise de conscience nationale et européenne émerge concernant la maîtrise des dépendances stratégiques numériques, notamment face aux GAFAM. Des stratégies variées, telles que le multicloud pour les données non souveraines et les solutions certifiées SecNumCloud ou ON PREM (ex : Cloud déconnecté) pour les données souveraines, sont mises en œuvre. Les services Cloud certifiés SecNumCloud se développent, garantissant une indépendance totale en transférant les données vers ces environnements.

L'intelligence artificielle (IA) souveraine devient un enjeu stratégique pour les Etats et les entreprises. L'accent doit être mis sur l'innovation technologique au niveau européenne/français et le soutien aux infrastructures de cloud souverain. La sensibilisation et la formation des professionnels seront cruciales pour une adoption sécurisée de l'IA, permettant ainsi aux entreprises et aux États de protéger leurs actifs numériques et de renforcer leur autonomie stratégique face aux défis géopolitiques. A noter dans ce domaine une première brique issue des travaux du Clusif (Modèle de Politique de Sécurité des Systèmes d'Information (PSSI) pour l'IA, accessible aux membres.

SÉVERINE MEUNIER

Directrice de Campagnes Stratégiques, Airbus Defence and Space, Officier de Réserve Opérationnelle, COMCYBER-MI, Spécialiste en e-criminalité OSINT/ Deepfakes et IA

AU-DELÀ DU CYBER : POURQUOI LA SÉCURITÉ GLOBALE EST L'ENJEU STRATÉGIQUE DE DEMAIN

Ces dernières années, le mot "cyber" est devenu omniprésent. Il est sur toutes les lèvres, dans tous les rapports stratégiques, et semble être devenu le cœur des enjeux de sécurité. Pourtant, cette focalisation presque exclusive sur la cybersécurité masque une réalité plus vaste : celle de la sécurité globale.

Si la cybersécurité est un pilier essentiel dans un monde numérisé, elle n'est qu'un maillon d'un écosystème plus complexe. La véritable résilience ne peut se construire sans une vision élargie qui intègre la sécurité physique, la surveillance périmétrique et surtout, la maîtrise du renseignement sous toutes ses formes. Comprendre cette complémentarité est crucial pour éviter l'illusion d'une protection totale fondée sur un seul domaine technologique.

Si la cybersécurité est un pilier essentiel dans un monde numérisé, elle n'est qu'un maillon d'un écosystème plus complexe.

I. LA CYBER : UN BUZZWORD NÉCESSAIRE MAIS RÉDUCTEUR

La multiplication des cyberattaques, des ransomwares aux campagnes de désinformation, a propulsé la cybersécurité au sommet des priorités publiques et privées. Cette prise de conscience est salutaire. Cependant, à force de tout ramener au "cyber", on en vient à oublier que cette composante n'est qu'un aspect d'une problématique plus large : celle de la sécurité globale.

Les buzzwords, par leur nature, simplifient et condensent des réalités complexes. "Cyber" est devenu un mot-valise qui englobe aussi bien la sécurité informatique que la souveraineté numérique, au risque de masquer d'autres vulnérabilités cruciales. Or, une faille physique dans une installation stratégique, une négligence dans la sécurité périmétrique ou une faiblesse dans le renseignement peuvent avoir des conséquences bien plus graves qu'une intrusion informatique isolée.

La sécurité globale : une approche systémique indispensable

La sécurité globale repose sur une approche holistique où chaque composante – cyber, physique, humaine et informationnelle – contribue à une résilience collective. Si l'un de ces éléments est négligé, l'ensemble du dispositif est fragilisé.

Sécurité physique et périmétrique

Dans des secteurs sensibles comme la défense ou les infrastructures critiques, la protection physique demeure fondamentale. Une cyberattaque sur un système industriel peut causer des dommages, mais une intrusion physique, un sabotage ou une faille humaine peuvent avoir des conséquences immédiates et irréversibles.

Des dispositifs comme la surveillance périmétrique avancée (par drones, capteurs ou imagerie satellitaire) permettent de détecter des menaces bien avant qu'elles n'atteignent le cœur numérique. La cybersécurité, aussi sophistiquée soit-elle, ne remplace pas la vigilance sur le terrain ni l'anticipation des menaces physiques.

Le renseignement : clé de l'anticipation stratégique

Si la cyberdéfense protège l'existant, le renseignement permet d'anticiper les menaces futures. Cette discipline dépasse largement le cadre numérique pour s'appuyer sur des sources ouvertes (OSINT), l'analyse des signaux faibles et l'exploitation de capteurs multiples (imagerie, acoustique, électromagnétique, etc.).

L'intégration de ces données hétérogènes permet d'identifier des menaces émergentes avant qu'elles ne deviennent tangibles. Par exemple, la détection d'activités inhabituelles sur un réseau électrique critique peut révéler une menace bien avant qu'une attaque cybernétique ne soit déclenchée.

L'importance des capteurs et de l'analyse des signaux faibles

L'une des limites de la focalisation sur la cybersécurité est qu'elle tend à ignorer la richesse des informations issues du monde physique. Pourtant, les avancées dans le domaine des capteurs permettent aujourd'hui de collecter et d'analyser des flux massifs de données en temps réel, offrant une vue globale des menaces potentielles.

Capteurs multiples : une approche multi-domaine

Dans un environnement complexe comme la défense multi-domaines (air, terre, mer, cyber, espace), il est essentiel de croiser les informations issues de capteurs variés :

- Capteurs électromagnétiques pour la détection de communications ou d'anomalies radar.
- Imagerie optique et infrarouge pour surveiller les mouvements physiques ou les installations sensibles.
- Systèmes acoustiques pour la surveillance sous-marine ou la détection de drones.

Ces données brutes, une fois agrégées et analysées, fournissent un tableau beaucoup plus complet des menaces que les seuls indicateurs cyber.

>>>

>>> L'analyse des signaux faibles : l'art de l'anticipation

L'analyse des signaux faibles consiste à détecter des indices précoces de menaces avant qu'elles ne deviennent visibles. Cette capacité est essentielle dans un monde où les attaques sont de plus en plus furtives et hybrides.

Par exemple, une légère augmentation du trafic autour d'un site sensible, associée à des échanges inhabituels sur des forums obscurs, peut indiquer une préparation d'attaque combinant intrusion physique et cyber.

Pourquoi une vision trop "cyber-centrée" est un risque

Focaliser les ressources et les discours sur la cybersécurité présente plusieurs dangers :

Une illusion de contrôle

Une infrastructure cyber protégée ne garantit pas l'invulnérabilité si les accès physiques sont vulnérables ou si les renseignements sur les menaces ne sont pas suffisamment exploités.

Un angle mort stratégique

Se concentrer exclusivement sur la cyberdéfense peut faire perdre de vue des menaces hybrides combinant sabotages physiques, attaques informationnelles et espionnage classique.

Une rigidité organisationnelle

Les équipes focalisées sur le cyber risquent de fonctionner en silos, sans intégrer les retours d'autres expertises (renseignement, terrain, surveillance physique).

Vers une sécurité globale intégrée et proactive

L'enjeu aujourd'hui est de dépasser les effets de mode pour revenir à une approche équilibrée où la cyber est une composante d'un système plus large. Cela implique :

Une coopération interdisciplinaire

Faire collaborer experts cyber, analystes du renseignement, spécialistes de la sécurité physique et opérateurs terrain.

Des systèmes multi-capteurs et multi-domaines

Développer des plateformes capables d'intégrer et d'analyser des données issues de différentes sources pour une vision globale et en temps réel.

Une vigilance continue sur les signaux faibles

Investir dans l'analyse prédictive pour détecter les menaces émergentes avant qu'elles ne deviennent critiques.

Conclusion : Ne pas céder aux sirènes du simplisme

Dans un monde marqué par des menaces hybrides et évolutives, il est temps de dépasser les buzzwords pour adopter une approche systémique et proactive. Car la sécurité de demain ne se gagnera pas uniquement derrière un écran, mais sur tous les terrains.

La cybersécurité est un enjeu majeur, mais elle ne doit pas devenir un écran de fumée masquant d'autres vulnérabilités essentielles. Une véritable résilience repose sur une sécurité globale intégrant le cyber, le physique et l'intelligence stratégique.

La multiplication des cyberattaques, des ransomwares aux campagnes de désinformation, a propulsé la cybersécurité au sommet des priorités publiques et privées.

RENSEIGNEMENT ET INTELLIGENCE ARTIFICIELLE : UN LEVIER STRATÉGIQUE POUR LA SOUVERAINETÉ FRANÇAISE DANS LA DÉFENSE MULTI-DOMAINE

À l'intersection du renseignement et des nouvelles technologies, la France s'appuie sur un écosystème industriel d'excellence pour préserver son autonomie stratégique et relever les défis de la guerre multi-domaines.

Le renseignement au cœur de la transformation militaire

Dans un monde où les lignes de front se déplacent aussi bien dans l'espace, le cyberespace que sur les champs de bataille traditionnels, le renseignement devient l'élément central de la supériorité opérationnelle. La rapidité d'acquisition et d'analyse de l'information est devenue une capacité aussi décisive que la puissance de feu.

Dans cette transformation, la France peut compter sur un tissu industriel dense et innovant, capable de répondre aux enjeux de la guerre multi-domaines (air, terre, mer, cyber, espace). Un acteur majeur de ce paysage se distingue particulièrement par son expertise dans l'aérospatial, les systèmes de renseignement avancés et les solutions de communication sécurisée.

Cet acteur, dont les activités s'étendent de l'observation satellitaire au traitement intelligent des données, joue un rôle clé dans le maintien de la souveraineté française.

I. DE L'ESPACE AU CYBER : MAÎTRISER L'ENSEMBLE DU SPECTRE INFORMATIONNEL

L'orbite comme poste d'observation avancé

Le renseignement spatial est un pilier stratégique pour anticiper les menaces et surveiller les zones de crise. Grâce aux constellations de satellites d'observation et d'écoute, la France dispose aujourd'hui de capacités de veille et de surveillance étendues, essentielles pour assurer l'autonomie décisionnelle.

Un acteur industriel de premier plan, fort d'une expertise reconnue dans la fabrication de satellites de nouvelle génération, est au cœur de cette capacité. Ses plateformes permettent de collecter des images haute résolution et des signaux électromagnétiques, même dans des environnements contestés. Ces informations sont ensuite traitées par des algorithmes d'intelligence artificielle capables d'identifier automatiquement des mouvements anormaux ou des changements stratégiques au sol.

Ces technologies offrent un avantage crucial : la capacité de passer de l'observation à l'action en temps réel, réduisant ainsi le cycle décisionnel pour les forces armées. À l'heure où d'autres puissances investissent massivement dans l'espionnage orbital, la France peut s'appuyer sur ces infrastructures souveraines pour garantir une surveillance continue de ses intérêts stratégiques.

La cybersécurité au service de la protection du renseignement

Dans un environnement où les cyberattaques constituent une menace permanente, la sécurisation des flux d'information est un impératif stratégique. L'un des principaux industriels français du secteur aérospatial a développé des systèmes de communication ultra-sécurisés, utilisés aussi bien pour les opérations militaires que pour la gestion des infrastructures critiques.

Ces solutions intègrent des technologies de chiffrement avancées et des architectures résilientes capables de fonctionner même en cas de dégradation sévère du réseau. Elles garantissent l'intégrité des échanges entre les différents théâtres d'opération, une capacité essentielle pour le renseignement multi-domaines où la coordination entre les forces est vitale.

>>>

>>> II. INTELLIGENCE ARTIFICIELLE ET RENSEIGNEMENT : L'ALLIANCE DE LA VITESSE ET DE LA PRÉCISION

Automatiser l'analyse : du volume à la valeur

L'augmentation exponentielle des données issues des satellites, des drones et des capteurs terrestres impose un traitement rapide et efficace. L'IA joue un rôle décisif en permettant d'extraire des informations exploitables en quelques secondes, là où l'analyse humaine nécessitait autrefois plusieurs heures, voire plusieurs jours.

Un leader français du secteur aéronautique et spatial a investi de manière significative dans le développement d'algorithmes capables d'effectuer une analyse comportementale automatisée. Ces solutions permettent, par exemple, de détecter des schémas inhabituels sur des images satellites, de cartographier en temps réel des zones d'intérêt ou de suivre les mouvements de flottes navales adverses avec une précision inégalée.

Ces capacités d'analyse augmentée sont essentielles pour anticiper les actions ennemies et ajuster les réponses opérationnelles. Elles renforcent également la protection des infrastructures françaises face aux cybermenaces et aux tentatives d'espionnage industriel ou militaire.

La prise de décision accélérée sur le terrain

Dans le cadre des opérations combinées, où la rapidité de réaction est déterminante, la capacité d'interpréter en temps réel les informations multi-sources est un facteur de supériorité. Grâce aux solutions développées par un acteur industriel de premier plan, les forces françaises disposent de systèmes embarqués permettant l'analyse immédiate des données recueillies sur le terrain.

Ces plateformes de commandement, intégrant l'IA et l'analyse prédictive, favorisent la coordination des unités déployées dans différents milieux. Elles permettent aux décideurs de disposer d'une vision globale et actualisée du théâtre d'opérations, garantissant ainsi une prise de décision éclairée et rapide.

III. LA SOUVERAINETÉ TECHNOLOGIQUE : UN ENJEU D'AUTONOMIE STRATÉGIQUE

Des capacités souveraines au cœur de la défense nationale

Dans un contexte de compétition accrue entre les grandes puissances, préserver une capacité autonome d'acquisition et de traitement du renseignement est un enjeu vital pour la France. Cela nécessite des investissements conséquents dans la recherche et le développement, mais aussi la protection des chaînes de valeur technologiques.

Un industriel français, en pointe sur les systèmes de renseignement et de communication, contribue activement à cette souveraineté en développant des solutions indépendantes des technologies étrangères. Cette approche garantit que les données sensibles collectées par les forces françaises restent sous contrôle national, un impératif face aux risques d'espionnage ou d'ingérence extérieure.

Coopération internationale et maîtrise des technologies critiques

Bien que la France défende son autonomie stratégique, elle reste un acteur majeur des collaborations européennes et internationales en matière de renseignement. Un acteur industriel majeur du secteur aéronautique et spatial joue un rôle clé dans plusieurs programmes multinationaux visant à renforcer l'interopérabilité entre les alliés.

Ces coopérations permettent de mutualiser les investissements dans des technologies de rupture – telles que l'IA, l'edge computing ou les systèmes quantiques – tout en garantissant un accès souverain aux informations critiques.

L'avenir du renseignement français : trois priorités stratégiques

Pour conserver sa place parmi les grandes puissances du renseignement, la France devra poursuivre trois axes majeurs :

1. Renforcer l'innovation souveraine : accroître les investissements dans l'IA embarquée et les capacités de renseignement spatial pour anticiper les menaces futures.

2. Garantir la résilience cybernétique : développer des infrastructures sécurisées et autonomes pour protéger les informations sensibles sur l'ensemble du spectre multi-domaines.

3. Former les talents de demain : attirer et retenir des experts en intelligence artificielle, cybersécurité et analyse stratégique pour maintenir l'excellence opérationnelle.

Conclusion : La souveraineté informationnelle est un enjeu crucial et est un levier de puissance décisif.

Dans un monde où l'information est une arme à part entière, la capacité à collecter, analyser et exploiter cette ressource en toute indépendance constitue un impératif stratégique.

La France, portée par un écosystème industriel dynamique et des solutions de pointe, est résolument engagée dans cette voie. Elle peut s'appuyer sur des acteurs capables de conjuguer maîtrise technologique, innovation rapide et protection des informations sensibles, relever les défis de la guerre multi-domaines et se positionner comme un acteur clé du renseignement du futur.

OSER L'ATYPISME : UN PARCOURS HORS NORMES AU CŒUR DE LA DÉFENSE

Quand l'audace et la confiance surpassent les diplômes, tout devient possible à condition de respecter les règles et l'exigence d'excellence qui garantissent la compétitivité et la crédibilité de l'entreprise.

Quand le parcours défie les conventions

Dans le monde de la défense, les profils qui occupent des postes stratégiques partagent souvent des trajectoires linéaires, marquées par des diplômes prestigieux et une progression méthodique. Pourtant, il existe des chemins de traverse, moins conventionnels mais tout aussi puissants, qui rappellent qu'au-delà des qualifications académiques, ce sont la vision, l'audace et la capacité à penser différemment qui font la différence.

Aujourd'hui à plus de 50 ans, évoluer dans un univers où les ingénieurs diplômés dominent n'est ni une évidence ni un hasard. C'est le fruit d'un parcours atypique, fait de paris audacieux, d'un engagement sans faille et de la conviction que chacun peut avoir un impact s'il ose, s'il travaille dur et s'il bénéficie de la confiance des bonnes personnes. Mais si l'audace est essentielle, elle ne saurait suffire sans une compréhension fine des règles et des exigences de l'entreprise.

Dans un secteur aussi sensible que la défense, l'innovation ne peut se concevoir sans un cadre rigoureux. Chaque décision, chaque initiative, doit s'inscrire dans un équilibre subtil entre créativité et respect des normes. C'est cette capacité à conjuguer l'audace et la discipline qui fait la différence, et qui permet à un parcours atypique de s'inscrire dans une trajectoire d'excellence durable.

Je ne me suis jamais reposée sur des acquis, j'ai dû faire preuve de persévérance, d'un travail constant et d'une énergie inépuisable pour atteindre mes objectifs. Je pense que tout ne découle pas de talent, mais d'une capacité à surmonter des obstacles, à se remettre en question et à repousser mes limites en permanence. Mon parcours, à la fois autodidacte et conventionnel, a la qualité de forger une résilience et une discipline à toute épreuve j'ai appris à gérer la pression, à travailler dans des environnements exigeants et à évoluer parmi des leaders et des experts qui me poussent à réfléchir, à innover et à me dépasser. Je suis personnellement très épanouie dans des environnements de haut niveau, car c'est dans ces contextes que je trouve la stimulation intellectuelle et le challenge qui nourrit mon ambition.

Cependant, un des plus grands défis auxquels j'ai été confrontée est de prouver ma légitimité, de trouver des interlocuteurs prêts à m'accorder leur confiance. Mon parcours montre des résultats concrets, mais la difficulté réside dans le fait de convaincre les autres de la valeur de l'approche non conventionnelle, sans toujours avoir la possibilité de tout expliquer en détail.

La confiance repose sur une compréhension fondamentale : ce n'est pas seulement le chemin que j'ai emprunté qui compte, mais la manière dont j'ai su tirer des leçons et me réinventer au fil des étapes. Mon expérience, forgée dans la rigueur et l'effort, en fait des atouts indéniables pour les équipes et les projets ambitieux, et ma capacité à produire des résultats est souvent le gage d'une réussite durable. C'est ce qu'Airbus Defence and Space a su détecter dans mon profil. J'ai intégré tout d'abord l'entité Cybersecurity où je travaillais avec les Institutions Européennes et le secteur public, pour ensuite passer à la Direction de Defence Digital France, l'un des clusters qui s'occupe du des systèmes d'information, ce qui me fait travailler avec des équipes mixtes : d'experts et de développement et contribuant à proposer notre solution Fortion® Massive Intelligence, qui permet aux entités de prise de décisions stratégiques en étant assistées par l'intelligence artificielle. Cette aide à la décision dans le cadre des opérations multi-domaines, en tenant compte des interactions complexes entre les instruments de pouvoir politiques, militaires, économiques, sociaux, informationnels, du renseignement, des forces de l'ordre et environnementaux. Il améliorera la capacité des entités à anticiper stratégiquement, à prendre des décisions plus rapidement que ses adversaires et à renforcer sa cohésion.

Notre monde évolue constamment, tout comme nos systèmes de renseignement. En raison des récents changements dans l'environnement stratégique, de la complexité croissante des menaces, de l'explosion des données, de l'implication accrue des forces occidentales dans des opérations hybrides/asymétriques et de l'inadéquation de l'architecture du renseignement héritée de la Guerre froide.

>>>

>>> L'itinéraire d'un esprit libre : sortir du cadre tout en respectant les règles

Dans un environnement aussi structuré que celui de la défense, où l'excellence technique et la rigueur sont des piliers incontournables, il peut sembler difficile pour un profil non-ingénieur de s'imposer. Pourtant, c'est précisément cette différence qui devient une force lorsqu'elle est portée par une capacité à penser autrement et à aborder les problématiques sous un angle innovant.

Ne pas avoir suivi le chemin classique n'a jamais été un frein. Au contraire, cela a été un moteur. Face aux profils formatés, un regard extérieur permet de poser des questions nouvelles, de remettre en cause des certitudes et d'apporter des solutions créatives.

Mais cette liberté de pensée doit s'accompagner d'une compréhension profonde des règles de l'entreprise : dans un secteur où chaque décision peut avoir des conséquences stratégiques majeures, il est impératif d'agir avec sérieux et responsabilité.

C'est précisément ce cadre exigeant qui permet à l'audace de se déployer efficacement. La créativité sans rigueur peut devenir un facteur de risque ; l'innovation encadrée, en revanche, devient un levier de compétitivité. Être un esprit libre ne signifie pas être un électron libre : cela signifie savoir évoluer avec agilité dans un cadre structuré, en respectant les exigences de qualité et de confidentialité qui sont au cœur de la mission de l'entreprise.

L'importance de la confiance : croire en soi, respecter l'exigence collective

Un parcours atypique ne peut s'épanouir sans un élément fondamental : la confiance. Celle que l'on a en soi, bien sûr, mais surtout celle que d'autres placent en vous. À plusieurs moments clés, l'opportunité d'évoluer s'est présentée non pas parce que les compétences étaient déjà parfaites, mais parce que quelqu'un a cru au potentiel, à la capacité d'apprendre et de s'adapter.

Recevoir cette confiance est un privilège, mais c'est aussi une responsabilité. Dans une entreprise qui exige exemplarité et compétitivité, la confiance se mérite chaque jour. Elle impose de respecter les procédures, de garantir l'intégrité des décisions et d'incarner les valeurs de l'organisation.

S'intégrer dans un cadre où l'excellence est la norme ne signifie pas renoncer à sa singularité : cela signifie comprendre que l'audace est d'autant plus précieuse lorsqu'elle s'accompagne d'une rigueur irréprochable. En respectant ces principes, il devient possible de construire une crédibilité durable et d'ouvrir la voie à d'autres profils atypiques.

Penser autrement : l'innovation par l'"out of the box", encadrée par l'exigence

Dans un secteur aussi exigeant et normé que la défense, la capacité à penser différemment est un atout stratégique. Les solutions aux défis complexes ne viennent pas toujours des approches classiques. C'est en cultivant un esprit critique et en acceptant de bousculer les habitudes que l'on parvient à ouvrir de nouvelles perspectives.

Mais cette pensée "out of the box" ne peut prospérer qu'au sein d'un cadre défini. Innover dans un secteur aussi sensible impose de respecter des protocoles stricts et de comprendre les impératifs de sécurité. Cette double exigence – créativité et discipline – est la condition sine qua non pour transformer des idées nouvelles en solutions opérationnelles fiables.

En apportant un regard extérieur et en osant poser des questions que d'autres ne se posent pas, il devient possible de dépasser les limitations imposées par les cadres traditionnels. Mais ce dépassement doit toujours s'inscrire dans une logique de responsabilité et d'excellence collective.

Ici je peux exploiter toutes les particularités de mes analyses en "étoiles", car elles me permettent de cartographier non seulement les comportements suspects dans le cyberespace, mais aussi d'identifier les points faibles d'un système et d'attaques avant de « lire » les signaux faibles par corrélation. Cette capacité à anticiper un éventuel passage à l'acte, est une ressource précieuse dans un environnement où les menaces sont parfois subtiles et diffuses. Cette capacité est également due depuis mon plus jeune âge à l'observation, à mes recherches et cartographies de tendances sur les différents comportements humains, et issue des multiples expériences, de travail sur les sciences cognitives, depuis de nombreuses années. Quand on travaille sur la e-criminalité et la lutte contre la e-pedocriminalité , croyez-moi que vous êtes vite mise en reflexe sur la capacité de l'humain a être capable du meilleur comme du pire.

L'audace encadrée : des opportunités pour tous, sous conditions

Ce parcours souligne aussi l'importance de respecter les règles et la discipline propres à une entreprise engagée dans des enjeux de défense nationale.

Une organisation telle qu'Airbus Defence and Space qui mise sur l'audace et la diversité des profils crée un cercle vertueux : en donnant leur chance à des parcours hors normes, elle stimule l'innovation, renforce sa capacité d'adaptation et devient plus agile face aux défis futurs. Mais cette ouverture repose sur un socle immuable : le respect des règles, la confidentialité et l'excellence opérationnelle.

Susciter des vocations : ouvrir la voie à d'autres parcours atypiques

Mon témoignage vise aussi à inspirer celles et ceux qui hésitent à sortir du cadre ou à se lancer dans des domaines qui peuvent sembler inaccessibles. La défense, avec ses exigences et ses normes, peut sembler réservée à une élite technique. Mais la réalité est plus nuancée : ce secteur a besoin de diversité, d'esprits audacieux et de personnes prêtes à relever des défis complexes avec une approche différente – tant qu'ils respectent les règles qui garantissent la sécurité et la crédibilité collective.

Conclusion : Tout est possible pour ceux qui osent, avec rigueur et responsabilité

Mon parcours en est la preuve vivante : il est possible de réussir sans suivre la voie tracée. Oser sortir des sentiers battus, croire en ses capacités et faire confiance aux autres sont des leviers puissants pour transformer un chemin atypique en une trajectoire d'exception.

Mais l'audace n'existe jamais en dehors d'un cadre : dans un secteur aussi stratégique que la défense, respecter les règles et incarner l'exemplarité sont des impératifs incontournables. C'est ce subtil équilibre entre innovation et rigueur, entre créativité et discipline, qui permet aux profils atypiques de s'inscrire durablement dans la réussite collective.

Dans un monde en perpétuel changement, ce sont les esprits libres et responsables qui façonnent l'avenir. Et il n'est jamais trop tard pour en faire partie.

Engagement Reserve Opérationnelle Spécialiste au COMCYBER MI

Le COMCYBER-MI est le Commandement du ministère de l'Intérieur dans le cyberespace, créé pour lutter contre la cybercriminalité et analyser les cybermenaces en temps réel, tout en collaborant avec d'autres entités pour renforcer la cyber-résilience des entreprises et des structures publiques et privées. L'organisation du COMCYBER-MI se veut mixte et pluridisciplinaire, mettant en œuvre un haut niveau d'expertise stratégique et technique, se nourrissant de la diversité des personnels qui le composent. Sous la direction du General Christophe Husson.

Le COMCYBER-MI est composé de personnels de différents corps et services du ministère (gendarmerie, police nationale, direction générale de la sécurité intérieure, préfecture de police de Paris, personnels civils).

Quelles sont ses missions ?

- **Coordonner** pour un dispositif cohérent, lisible et performant Le COMCYBER-MI agit aussi sur le plan capacitaire, en structurant le dispositif de réponse contre les cybermenaces dans un but de lisibilité et de performance. Il définit les moyens humains et matériels à mettre en œuvre au sein du dispositif cyber du ministère pour garantir une action performante.
- **Anticiper** pour mieux s'adapter : Pas de stratégie sans anticipation, le COMCYBER-MI évalue et analyse l'état de la menace cyber et s'assure du partage de l'information aux unités qui le composent. De la même manière, le COMCYBER-MI participe à l'évolution des cadres juridiques et réglementaires pour s'adapter aux nouvelles formes de cybercriminalité et aux modes d'actions des cybercriminels.
- **Appuyer** pour une offre de service complète intégrant un haut niveau de technicité et des compétences rares. Je les remercie car en appui que j'ai pu contribuer au même titre que d'autres réservistes opérationnelles à la sécurisation des JOP 2024, au CNSC.
- **Former** pour garantir un haut niveau de réponse du ministère
- **Prévenir** par l'infusion d'une culture cyber
- **Coopérer** pour endiguer une cybercriminalité sans frontière.

Mon engagement au COMCYBER-MI est une mission d'appui et de coopération entre services européens et internationaux qui est essentielle afin d'appréhender les réseaux cybercriminels de haut spectre, Europol, Eurojust Interpol etc. ...

Grace à des outils performants en matière d'OSINT, d'IA et de détection des deep fakes, et en collaboration avec divers acteurs du Ministère de l'Intérieur, ce commandement contribue activement à assurer la cybersécurité et à neutraliser les menaces. En tant que réserviste, ma capacité à exploiter mon profil atypique et à "penser en étoiles" me permet de contribuer à l'anticipation des cyberattaques, en apportant des solutions innovantes et proactives pour une défense numérique optimale.

Mon approche unique repose sur la capacité à exploiter mon profil Zèbre dans le cadre des missions de cyberdéfense, cette approche m'aide à mieux comprendre les schémas complexes des cybermenaces et à anticiper les stratégies des acteurs malveillants. .

En utilisant cette capacité à penser différemment, je peux participer activement à la prévention des attaques et renforcer les capacités de réponse du COM CyberMI, en identifiant des angles d'analyse inédits et en proposant des solutions innovantes pour améliorer la sécurité des systèmes et infrastructures.

Membre honoraire de L'Association Point de Contact : Un Pilier de Lutte et de Soutien

Depuis 25 ans, l'association Point de Contact lutte contre les cyberviolences et protège les citoyens dans l'espace numérique qui est membre du réseau InHope.

Point de Contact est une association dédiée à la lutte contre les cyberviolences et à la protection des droits humains sur Internet. Son objectif : offrir un espace numérique plus sûr en permettant à tout citoyen de signaler des contenus illicites ou des situations préjudiciables en ligne. Son action >>>

>>> s'étend sur plusieurs problématiques majeures, telles que l'exploitation sexuelle des mineurs, les violences sexistes et sexuelles, les discours haineux et l'extrémisme violent, entre autres. Par son engagement, l'association cherche à instaurer des mécanismes de prévention, tout en assurant le soutien juridique et psychologique aux personnes concernées. Je suivais déjà cette association pour laquelle j'étais déjà intervenue et quand elle m'a proposée de rejoindre leur membre et actio en tant que membre honoraire j'ai tout de suite répondu positivement.

En tant que membre français du réseau international INHOPE, Point de Contact participe activement à la lutte contre l'exploitation sexuelle des mineurs en ligne. L'association transmet les contenus pédo-criminels aux forces de l'ordre et aux services numériques, à des fins de retrait et de judiciarisation. Depuis 2020, Point de Contact a transmis pas moins de 60 000 contenus illicites, contribuant ainsi de manière déterminante à l'identification des victimes et à la lutte contre la diffusion de contenus criminels en ligne.

L'association adopte une approche globale pour lutter efficacement contre les cyberviolences. Consciente que cette problématique ne peut être résolue par la seule suppression de contenus, l'association mène des actions de sensibilisation et de formation à destination d'un public varié, conduit des travaux de recherche pour améliorer la connaissance des phénomènes cybercriminels, ou encore, s'engage activement dans des initiatives de plaidoyer. Elle apporte également un soutien aux victimes en leur fournissant des ressources et des informations spécifiquement adaptées à leurs besoins.

Soutenir Point de Contact, c'est contribuer concrètement à la construction d'un Internet plus sûr, bienveillant et inclusif. L'association invite les entreprises, les institutions et les professionnels du numérique à se joindre à ses actions, que ce soit en devenant membres, en participant à ses initiatives ou en lui apportant un soutien financier. Chaque engagement renforce son impact dans la lutte contre les cyberviolences : ensemble, mobilisons-nous pour un espace numérique plus sain et respectueux.

Site web : www.pointdecontact.net
Ecrire à l'équipe : https://www.pointdecontact.net/contact/

Membre du conseil d'administration de Women4Cyber France .

Women4Cyber est une fondation européenne à but non lucratif créée en 2019, dédiée à la promotion et à l'encouragement de la participation des femmes dans le domaine de la cybersécurité. Son objectif principal est de combler le fossé entre les genres parmi les professionnels de la cybersécurité en Europe, en encourageant et en soutenant l'acquisition de compétences par les femmes, qu'il s'agisse de formation initiale, de perfectionnement ou de reconversion vers des carrières en cybersécurité.

En France, l'association Women4Cyber France, créée en 2021, représente la fondation européenne sur le territoire national. Elle vise spécifiquement à promouvoir les métiers de la cybersécurité auprès des femmes et à encourager le recrutement des talents féminins par les acteurs du secteur.

Nous avons un programme de mentorat en tant que rôles Models, et avons un programme avec le ministère de l'éducation national (TalCyb) où nous accompagnons les conseillers d'orientations et les professeurs dans la connaissance des besoins des métiers émergents et les compétences nécessaires.

Les actions comprennent :

> **Initiatives de promotion :** Organisation d'événements et de tables rondes pour inspirer les jeunes filles, les étudiantes et les femmes en reconversion, en mettant en avant des modèles féminins dans la cybersécurité.

> **Programme de mentorat :** Mise en place d'un programme où des mentors, hommes ou femmes, accompagnent des femmes débutantes ou en reconversion pour les aider à intégrer plus rapidement le secteur de la cybersécurité. Face à la pénurie de talents dans ce domaine, Women4Cyber France s'efforce de réunir toutes les femmes et tous les hommes engagés autour du défi des compétences en cybersécurité, en créant un réseau actif au cœur des territoires.

> **Sensibilisation et promotion des meilleures pratiques :** Créer une prise de conscience sur l'importance de la diversité dans la cybersécurité et promouvoir des pratiques exemplaires.

> **Participation accrue des femmes dans l'éducation à la cybersécurité :** Encourager une plus grande implication des femmes dans les programmes éducatifs liés à la cybersécurité.

> **Promotion de modèles féminins visibles :** Mettre en avant des femmes leaders dans le domaine pour inspirer et motiver les nouvelles générations.

> **Développement de programmes de formation adaptés :** Proposer des formations sur mesure pour l'entrée dans le domaine, le perfectionnement ou la reconversion en cybersécurité.

> **Augmentation de la présence des femmes sur le marché de l'emploi en cybersécurité :** Faciliter l'accès des femmes aux opportunités professionnelles dans ce secteur.

> **Renforcement de la présence féminine dans la recherche et l'innovation en cybersécurité :** Encourager la contribution des femmes aux avancées technologiques et méthodologiques.

> **Engagement des femmes dans les défis et exercices cyber :** Favoriser la participation féminine aux compétitions et simulations en cybersécurité.

ET VOUS SÉVERINE PLUS PERSONNELLEMENT ?

AUJOURD'HUI, IL NE S'AGIT PLUS SEULEMENT DE PARLER DE SES COMPÉTENCES, MAIS AUSSI DE PROUVER SA LÉGITIMITÉ DANS UN ENVIRONNEMENT OÙ L'ON SE SENT PARFOIS MINORITAIRE.

LES CHIFFRES QUI INTERPELLENT

1 femme sur 3
ressent que son opinion n'est pas prise au sérieux en réunion, notamment lorsqu'elle est entourée d'hommes.

53% des hommes
de 25 à 34 ans sont convaincus que "les femmes sont psychologiquent plus fragiles que les hommes"

Ce type de déséquilibre peut non seulement renforcer un sentiment d'isolement, mais aussi freiner l'ambition ou la capacité à se projeter dans des rôles de leadership.

Ces données révèlent un problème systémique : les environnements dominés par une seule perspective ne permettent pas d'exploiter pleinement le potentiel des talents.

Que faire pour changer la donne ?

Diversifier les panels de recrutement et les jurys : lorsqu'un candidat ou une candidate voit une diversité dans l'audience, il/elle se sent davantage à sa place. Cela réduit les biais et renforce une évaluation plus équitable

Favoriser des environnements inclusifs : l'inclusion ne se limite pas à remplir des quotas, mais à créer des espaces où chaque voix est entendue, respectée et valorisée

Former à la déconstruction des biais inconscients : les expressions, les comportements et même les attitudes passives, comme celles illustrées ici (ennui, amusement), peuvent décourager des talents prometteurs

Miser sur des représentations fortes : plus les femmes sont visibles dans des positions de pouvoir, plus elles inspirent d'autres à suivre leurs traces. On ne peut être ce que l'on ne voit pas.
www.women4cyber.fr

PROMOUVOIR LES RÉSERVES AU SEIN DES ENTREPRISES : UN ENGAGEMENT DE VALEUR

GS MAG : *En quoi le GREADS représente-t-il un atout stratégique pour Airbus, tant au niveau de l'engagement civilo-militaire que dans le développement de projets structurants pour la défense nationale ?*

SM : Le Groupement des Réservistes des Entités Aéronautiques, Défense et Spatial (GREADS) est une initiative stratégique pour le groupe Airbus, englobant toutes ses filiales, ainsi que celles de MBDA et d'Ariane Group. Le GREADS inclut tous les salariés du groupe, qu'ils soient en CDI, CDD, alternance ou autres formes de contrat. Cette initiative vise à promouvoir l'esprit de défense au sein du groupe et à créer un pont entre le secteur civil et la défense nationale. À ce jour, l'initiative recense plus de 200 réservistes.

Le GREADS rassemble des réservistes issus de divers corps militaires et civils, notamment l'Armée de Terre, l'Armée de l'Air et de l'Espace, la Marine Nationale, la Gendarmerie Nationale, la Police Nationale, et y associe les pompiers volontaires. L'association englobe à la fois des réservistes opérationnels et citoyens, et facilite l'engagement de ces derniers au sein de la défense tout en leur permettant de maintenir leur activité professionnelle au sein d'Airbus. Elle a d'ailleurs été récompensée plusieurs fois par le Prix de la Réserve Militaire pour sa contribution exceptionnelle à la défense nationale.

Le GREADS offre aux employés d'Airbus un cadre structuré pour concilier leur travail dans le groupe avec leur engagement dans la réserve militaire. De nombreux salariés, qualifiés et recherchés par les armées, souhaitent servir leur pays, mais se heurtent souvent à un manque

>>>

>>> d'informations claires ou à des obstacles organisationnels. Le GREADS travaille à amoindrir ces barrières, en facilitant l'accès à l'information et en mettant l'engagement à servir dans la réserve à l'honneur. Ainsi, un réserviste travaillant au sein du groupe Airbus se voit aujourd'hui accorder 15 jours d'absence payée par an, permettant ainsi de participer activement à la défense nationale sans impact sur sa carrière civile

Cet accompagnement est d'autant plus crucial dans le contexte de la BITD française, où Airbus joue un rôle clé. Le GREADS permet à Airbus de bénéficier de l'implication de ses employés dans des domaines stratégiques tels que l'aéronautique, la défense spatiale et la cybersécurité. En tissant des liens solides entre les salariés et les armées, l'entreprise s'assure de mieux répondre aux besoins spécifiques du Ministère des Armées, enjeu essentiel pour développer des projets de défense de grande envergure. En facilitant les échanges d'informations entre les entités, le GREADS permet à Airbus de mieux comprendre les priorités du Ministère et d'adapter ses offres. Ce réseau d'informations contribue également à mieux anticiper les besoins futurs et à développer des projets structurants, en réponse aux exigences de la défense française.

> Plus les femmes sont visibles dans des positions de pouvoir, plus elles inspirent d'autres à suivre leurs traces.

Le GREADS joue également un rôle central dans la diversification et la mise en valeur des compétences au sein du groupe, notamment en matière de cybersécurité. Dans un environnement où la guerre numérique prend de plus en plus d'ampleur, l'intégration de ces aspects dans le secteur privé de la défense est primordiale pour favoriser l'innovation. Le GREADS soutient activement la représentation des femmes en leur offrant des opportunités pour se former et contribuer à des projets de haute technologie.

Les femmes, souvent sous-représentées dans la cybersécurité et dans les fonctions de défense numérique, trouvent dans le GREADS une plateforme pour s'engager pleinement dans des missions de défense nationale. Leur expertise enrichit les projets d'Airbus, en particulier ceux liés à la défense informatique, la protection des infrastructures critiques et la sécurité des systèmes militaires. Cet engagement favorise à la fois la promotion de l'esprit de défense au sein du groupe et l'ouverture à des compétences féminines essentielles dans le secteur de la cybersécurité.

AIRBUS DEFENCE AND SPACE MEMBRE DE L'ACN ALLIANCE POUR LA CONFIANCE NUMÉRIQUE ET CO PRÉSIDENTE DU GT CYBER SÉCURITÉ

L'Alliance pour la Confiance Numérique (ACN) est un syndicat professionnel clé dans le secteur numérique, visant à promouvoir la confiance et la sécurité des technologies de l'information. L'ACN regroupe des entreprises engagées dans la cybersécurité, la protection des données et la conformité numérique, en abordant des enjeux essentiels comme la réglementation, les standards de sécurité et la gestion des risques numériques.

Être membre de l'ACN permet à Airbus Defence and Space de jouer un rôle actif dans l'élaboration de politiques publiques, de participer à des groupes de travail sur des sujets stratégiques tels que la souveraineté numérique, la protection de la vie privée, ou encore les normes de sécurité des infrastructures critiques. Cette présence au sein de l'ACN est primordiale, car elle garantit que notre entreprise reste à la pointe des évolutions légales et technologiques tout en contribuant à façonner un cadre numérique sécurisé et fiable.

Je tiens à remercier Airbus Defence and Space de m'avoir permis de la représenter au sein de cette organisation, en prenant la Co-présidence du GT Cyber. L'écosystème et ses membres contribuent activement aux réflexions et aux travaux sur les enjeux cruciaux pour l'avenir de notre secteur tels que le cyber, la sécurité et l'IA.

L'ENGAGEMENT AU SERVICE DE LA NATION : L'IMPORTANCE DE PROMOUVOIR LES RÉSERVES AU SEIN DES ENTREPRISES

GS MAG : *Réserviste pour vous qu'est-ce que cela représente ?*

SM : Dans le cadre des évolutions sociétales et économiques actuelles, les entreprises ont un rôle crucial à jouer dans la valorisation et l'intégration des réservistes des différents ministères au sein de leurs équipes. Cette démarche ne se limite pas à un simple acte de responsabilité sociale, mais représente une véritable stratégie d'engagement et de cohésion. Que ce soit des jeunes talents en quête d'expérience ou des professionnels plus expérimentés, la réserve est un vecteur clé de développement, et l'entreprise, en tant qu'acteur majeur de la société, peut en faire un levier stratégique pour l'innovation et la compétitivité.

L'INTÉGRATION DES RÉSERVISTES DANS LES ENTREPRISES : UN ENJEU CLÉ POUR L'AVENIR

Les réserves opérationnelles des différents ministères, qu'elles soient liées à la défense, à la sécurité civile, ou aux ministères de l'intérieur et des finances, représentent un vivier de compétences exceptionnelles. Ces réservistes apportent des connaissances techniques pointues, des compétences en gestion de crises, ainsi qu'une éthique de travail axée sur la rigueur, l'intégrité et le service à la nation. Dans ce contexte, les entreprises ont tout à gagner à promouvoir l'intégration des réservistes au sein de leurs équipes, qu'ils soient jeunes ou plus expérimentés.

L'intégration de réservistes, qu'ils soient jeunes recrues ou cadres plus aguerris, permet de renforcer la compétitivité de l'entreprise tout en enrichissant son capital humain. Les qualités que possèdent ces réservistes — l'engagement, la résilience, la discipline — se révèlent particulièrement bénéfiques dans des secteurs où la gestion de projet, la sécurité, la gestion de crise et l'agilité sont essentielles.

JEUNES ET MOINS JEUNES : DES PROFILS COMPLÉMENTAIRES POUR L'ENTREPRISE

Les réservistes peuvent être jeunes ou moins jeunes, mais dans tous les cas, ils sont porteurs de valeurs et de compétences qui enrichissent les équipes professionnelles. Les jeunes réservistes, souvent en début de carrière, apportent un souffle nouveau à l'entreprise, avec leur dynamisme et leur volonté de s'impliquer dans des projets à forte valeur ajoutée. En parallèle, les réservistes plus expérimentés — souvent issus de carrières militaires, de la gendarmerie, de la police ou des services de renseignement — apportent une expertise et une capacité à gérer des situations complexes et à prendre des décisions dans des contextes tendus.

Ces profils apportent une complémentarité essentielle à toute entreprise. Ils bénéficient d'une formation poussée qui les prépare à des contextes de forte pression et de haute exigence. Ils sont habitués à travailler en équipe et savent gérer des situations complexes de manière pragmatique et rapide.

Une société qui soutient ses réservistes fait ainsi le choix d'une équipe plus forte, plus polyvalente, et plus résiliente face aux défis modernes.

UNE ENTREPRISE GAGNANTE SUR TOUS LES FRONTS

Promouvoir les réservistes dans les entreprises est bénéfique à plusieurs niveaux :

- **Renforcement de l'esprit d'équipe et des valeurs communes :** Les réservistes ont en commun des valeurs fortes d'engagement, de solidarité, et de responsabilité, qui se transposent directement dans la culture d'entreprise.
- **Amélioration des compétences transversales :** Les réservistes sont formés dans des domaines variés, allant de la gestion de crise à la planification stratégique. Cela enrichit les compétences des équipes et élargit la palette de solutions disponibles pour faire face aux enjeux contemporains.
- **Responsabilité sociale de l'entreprise (RSE) :** En soutenant les réservistes, une entreprise contribue à la sécurité nationale et à l'engagement citoyen. Cela renforce son image d'acteur responsable et engagé.
- **Avantages en termes d'innovation et de leadership :** Les réservistes apportent une vision différente des défis, une capacité à innover en période de crise, et une vision stratégique qui peut être bénéfique pour la direction. ■

Une société qui soutient ses réservistes fait ainsi le choix d'une équipe plus forte, plus polyvalente, et plus résiliente face aux défis modernes.

HS2

Hervé Schauer Sécurité

Formation cybersécurité technique

INTRODUCTION • RÉSEAUX
INFRASTRUCTURES • DÉFENSE

PROGRAMME

Introduction à la cybersécurité

ESSCYBER
Essentiels techniques de la cybersécurité

SECUCYBER
Fondamentaux techniques de la cybersécurité

Sécurité des réseaux et des infrastructures

SECUARCH
Sécurité des architectures

REDTEAM
Redteam sans fil

SECUPKI
Infrastructures de clés publiques

SECUIA
Sécurité des systèmes d'intelligence artificielle

Sécurité défensive

SECUWIN
Sécurisation des infrastructures Windows

SECULIN
Sécurité Linux

SELinux
Comprendre SELinux et savoir modifier la politique de sécurité

SECUDEVWEB
Sécurité des serveurs et des applications Web

SECUINDUS
Cybersécurité des systèmes industriels

SECUOBJ
Sécurité des objets connectés

SECUMOBILE
Audit sécurité d'applications mobiles Android et iOS

+ 33 974 774 390

www.hs2.fr

formation@hs2.fr

ANNE SOUVIRA

Commissaire Divisionnaire Honoraire Ancien Chef de la Mission « Cyber »de la Préfecture de Police de Paris (Ministère de l'Intérieur) à la DILT

LA LUTTE CONTRE LES ABUS SEXUELS SUR MINEURS (CSAM) : UN DÉFI NATIONAL ET INTERNATIONAL DE PRIORITÉ ENTRE PROTECTION DES ENFANTS ET LIBERTÉ INDIVIDUELLE DES ADULTES

Des serviteurs de l'Etat et des associations se dévouent à la protection de l'enfant, victime de l'indicible et de l'inaudible, alors que la société en dépit d'affaires judiciaires toujours plus abominables, semble ne toujours pas avoir comme priorité une lutte véritablement efficace contre le fléau national et international des abus sexuels sur mineurs qui ne fait déjà plus consensus en Europe alors même qu'en 2022 1,5 million d'abus sexuels sur mineurs ont été signalés dans l'UE.

>>>

>>>

I. UN PHÉNOMÈNE PÉDOCRIMINEL EN EXPANSION

Face à des acteurs engagés n'assurant qu'une insuffisante protection des plus vulnérables due par l'Etat, les parents et tout un chacun, malgré un renforcement des moyens humains privés et publics et leur souci d'améliorer les textes juridiques répressifs européens.

L'ampleur du phénomène toujours en expansion selon les sources officielles telles qu'EUROPOL ou cyber-malveillance, interroge alors que chaque image/ vidéo pédo-pornographique i.e. pedo-criminelle, représente un véritable enfant et victime et que le signalement doivent permettre de limiter la production et la diffusion de ces contenus.

Définition(s) du CSAM FR- UE, de la détention de matériel pedocriminel au live streaming.

La définition généralement admise du CSAM, l'exploitation sexuelle des mineurs consiste en des contenus qui montrent des images ou vidéos où les mineurs sont explicitement mis en scène sexuellement. Ces matériels sont achetés, échangés et détenus après que les victimes ont subi ces crimes sexuels. Ces victimes, du nourrisson à l'ado, peuvent être livrées contre de l'argent par les parents dans des pays pauvres, à des industriels de photos et vidéos qui en font commerce, parfois au sein même de l'Europe.

Les technologies facilitent une élévation de la gravité des faits à un point tel que les pedo-criminels et leurs pourvoyeurs, procèdent, sur commandes payantes, à des live-streaming de ces crimes indicibles. Selon le service central spécialisé, pendant 10 ans, un homme a envoyé plus de 50 000 euros vers les Philippines et le Kenya pour commander des shows, des viols d'enfants en direct, le plus souvent réalisés par leurs parents qui exécutent les scénarios et desiderata pédocriminels de l'internaute derrière son écran à l'autre bout du monde.

Il s'agit d'une véritable économie ! Les mineurs en sont les victimes participantes lorsqu'ils fournissent eux-mêmes des images via des échanges en ligne (ou hors ligne) lors de sextorsion . Ils tombent dans les pièges des prédateurs et fournissent des images/vidéos qui se retrouvent sur Internet voire rencontrent leurs prédateurs en physique après discussion dans un jeu video ou sur snapchat.

Sans oublier le revenge porn qui n'est plus réservé aux majeurs; le fait de publier ou de diffuser sur Internet un contenu intime d'une personne sans son consentement et dans le but de porter atteinte à sa dignité ce qui permet la récupération du matériel par les exploiteurs et son utilisation comme deep fake possiblement.

Alors même que la loi du 16 juillet 1949 interdit entre autre, l'exposition aux mineurs de contenus pornographiques et la réprimant sévèrement à l'article 227-24 du code pénal

Ces mêmes mineurs ont accès via les smartphones à la pornographie de plus en plus tôt en l'absence de maîtrise et de contrôle parental ou d'éducation à l'école.

Le consentement nécessaire des parents pour les mineurs à compter de 13 ans pour avoir accès aux réseaux sociaux et la preuve de l'âge restait une difficulté technique (économique ?) pour les grandes plates-formes et réseaux sociaux. Le référentiel de l'ARCOM paru le 11 octobre 2024, n'est toujours pas respecté par les services de communications en ligne et autres réseaux sociauxdont l'activité est en France ou en Europe. Aussi la loi SREN du 21 mai 2024 avait-elle donné à l'ARCOM le pouvoir d'ordonner aux Fournisseurs d'Accès Internet, le blocage des sites hors la loi, sans passer par une décision de justice.

1,5 million d'abus sexuels sur mineurs ont été signalés dans l'UE.

Elle peut également imposer des sanctions pécuniaires auxdits sites, pouvant aller jusqu'à 150 000€ ou 2% du chiffre d'affaires (ou 300 000€ ou 4% du chiffre d'affaires, pour les sites récidivistes). Depuis le 11 janvier 2025 un délai de trois mois de mise en conformité courait, soit au 11 avril 2025.

Les plates-formes n'ayant pas mis en œuvre la double authentification ou autre solution efficace, opérant dans des Pays européens ont reçu des courriers de prévenance pour une mise en conformité technique à juin 2025, selon Clara Chappaz la Ministre déléguée chargée de l'Intelligence artificielle et du Numérique.

Durant ces délais des solutions de génération de preuve dérogatoires de l'âge étaient acceptées à titre temporaire. Selon les statistiques disponibles d'Europol et celles de l'association Point de Contact ou du réseau INHOPE - mentionnés infra, la France est le 2ème pays hébergeur en Europe de contenus pedo-criminels après les Pays-Bas.

Statistiquement l'hébergeur OVH, grand partenaire de lutte contre les CSAM est le plus implanté sur le territoire. 91% des contenus pedo-criminels concernent des enfants/filles entre 3 et 13 ans. Selon le home affairs de l'UE, 85 millions de contenus CSAM ont été signalés dans le monde !

Pour EUROPOL, la stratégie d'action avec les services nationaux est développée dans le cadre du programme EMPACT (Cycle politique de l'UE) qui est un plan d'actions (opérationnelles, de renseignement criminel, capacitaire, stratégique, de prévention et partenariat) ; l'un de ces plans est dédié à la lutte contre les abus de mineurs en ligne. L'opération Cumberland menée le 26 février 2025 a mis en cause 273 suspects identifiés et 25 suspects arrêtés. « Le principal suspect, un ressortissant danois arrêté en novembre 2024, gérait une plateforme en ligne où il diffusait les contenus qu'il produisait grâce à l'IA. Suite à un paiement symbolique en ligne, des utilisateurs du monde entier pouvaient obtenir un mot de passe pour accéder à la plateforme et assister à des abus sexuels sur des enfants ».

En 2023 selon le rapport de l'association Loi 1901 point de contact.net (PDC), reconnue en 2025 trusted flagger, 7 437 contenus pedo-criminels ont été identifiés ; soit plus de 1 contenu illicite sur 2 signalés, qualifié tel et transmis aux éditeurs et plates-formes d'hébergement ou à PHAROS. En 2024, PDC a identifié et transmis à la plateforme PHAROS, 17 180 contenus pédo-criminels, soit une augmentation de 131%. Selon PHAROS, le retrait à la source de 30 408 contenus d'atteintes sexuelles sur mineurs a été demandé ou leur blocage dans l'Union Européenne au premier semestre 2024.

Il convient de noter que malgré la croissance de la pedo-criminalité, aucune statistique ministérielle n'est disponible semble-t-il sur l'exploitation des sexuelles des mineurs hormis sous l'angle du proxénétisme. Ceci met en évidence l'intérêt de l'implication des associations aux côtés des forces de l'Ordre.

Les Acteurs de l'État sont renforcés par des réseaux privés souvent mieux subventionnés à l'étranger en dépit d'avancées françaises certaines. La lutte réalisée par le ministère de l'Intérieur avec le renfort d'associations n'est pas toujours entendue ni subventionnée à la hauteur des enjeux techniques et des ressources humaines nécessaires.

> **Sous l'impulsion tenace du Commandant de Police Divisionnaire,** Véronique Béchu, chef de l'ancien groupe des mineurs victimes de l'OCRVP de la direction centrale de la police Judiciaire (DCPJ), le décret du 29 août 2023 crée l'Office des Mineurs (OFMIN) à la Direction nationale de la Police Judiciaire (DNPJ), nouvelle appellation de la DCPJ. La préfecture de Police de Paris (PP) quant à elle et sur le ressort de la petite couronne, dispose de la Brigade de protection de la famille (BPF) ex-Brigade de protection des Mineurs (BPM). La gendarmerie nationale occupe le poste d'adjoint de l'OFMIN et dispose parallèlement d'un groupe spécialisé qui gère pour le ministère de l'Intérieur, la base du CNAIP des images découvertes identifiées ou non qui mènent à des interpellations. Ce centre alimente la base ICSE gérée par Interpol, aux fins d'identification des mineurs victimes du monde entier par analyse et comparaison des images. Cette lutte ministérielle s'appuie sur les enquêteurs techniciens de l'office anti-criminalité (OFAC) qui reçoivent également les signalements sur PHAROS, de ceux de la BEFTI/BLCC de la PP et du centre de criminalité numérique (C3N) de la GN. Ces services sont partenaires de la société civile vu la charge de travail à partager. Ces fonctionnaires, investigateurs en cybercriminalité sont chargés d'analyser les contenus d'enfants abusés et d'enquêter sous pseudonyme pour infiltrer et participer aux échanges afin de démasquer les prédateurs ; aussi doivent-ils être spécialement l'objet d'attention en raison des possibles chocs post-traumatiques.

> **Les technologies facilitent une élévation de la gravité des faits à un point tel que les pédocriminels et leurs pourvoyeurs, procèdent, sur commandes payantes, à des live-streaming de ces crimes indicibles.**

> **Le réseau INHOPE, l'Association internationale des hotlines Internet créée en 1999** regroupe 55 hotlines de signalement de contenus illicites avec pour mission >>>

>>> soutenir et de permettre aux lignes d'assistance INHOPE d'identifier et de supprimer rapidement le matériel d'exploitation sexuelle d'enfants, du monde numérique. La France a présidé plusieurs années ce réseau jusqu'en 2023 dont le président était celui de l'association Pointdecontact.net (PDC). L'utilité de ce système international de signalements est démontrée chaque jour. Ainsi au cours du premier semestre de l'année 2024, la hotline polonaise Dyżurnet.pl a reçu 13 640 signalements concernant du matériel pedo-criminel potentiel (CSAM). dont 10 231 URL contenant du matériel pédo-criminel). La hotline britannique - Internet Watch Foundation (IWF), via INHOPE, a envoyé un total de 9 410 rapports concernant le contenu des serveurs polonais. Sur les 710 sites web, 434 étaient des sites CAP (pyramide d'abus sexuels sur des enfants) ce qui représente 61 % des sites web avec CSAM analysés par Dyżurnet.pl. 77 % d'entre eux se trouvent sur des serveurs situés dans la Fédération de Russie ce qui met fin quasiment fin à l'enquête (même avant la guerre). INHOPE fait partie du projet CPORT, portail qui permet aux forces de l'ordre d'accéder à l'ICCAM, la plateforme sécurisée centralisée utilisée par les hotlines INHOPE. Le portail facilite l'échange direct de données et d'informations entre les analystes du contenu des HOTLINES et les services répressifs afin de rationaliser le retrait de CSAM.

> **PointdeContact.net (PDC), association Loi 1901 a été créée en 1998** à la demande du gouvernement français. Aujourd'hui, après une période de trouble due à un financement peu pérenne, réorganisée et rééquilibrée grâce à des membres impliqués elle poursuit cette activité, parallèlement à l'élargissement aux cyber-violences, aux côtés des FDO. Elle reçoit les signalements de contenus illicites, les qualifie aux fins de retrait par les hébergeurs ou la plateforme gouvernementale de signalement PHAROS gérée par l'Office anti-criminalité (OFAC) de la DNPJ. Cette association a également créé la plateforme DISRUPT : le dispositif d'interruption de diffusion de contenus intimes qu'elle opère. Il faut mentionner qu'aujourd'hui son financement est principalement privé en dépit de la réalisation d'une mission intérêt général et que si les Forces de l'Ordre sont membres, c'est seulement en observateurs dans le cadre de partenariats. C'est pourquoi ce financement, qui a été parfois européen comme pour les autres associations de l'écosystème, doit être renforcé par des mécénats d'entreprise de type RSE, car ces contenus vont s'accroissant. La poursuite de sa mission nécessite de financer ses analystes de contenus illicites, leur formation et leur bien-être mental ainsi que les couteux logiciels techniques afférents.

> **L'écosystème associatif,** tel le 3018 de e-enfance.org (association RUP) et l'enfant bleu.org ou SOS enfance en danger, traite aux côtés de PDC, de problématiques de protection de l'enfance par le programme un internet sans crainte opéré via les ressources de sensibilisation de la SAS TRALALERE sans l'aspect signalement de contenus illicites.

> **Pour comparaison,** le National Center for Missing & Exploited Children (NCMEC), est une organisation non lucrative fondée en 1984 par le Congrès des États-Unis. « le CSAM n'est pas seulement une image, c'est une scène de crime » rappelle le 11 mars 2025 le NcMEC sur X. « Chaque repartage est une revictimisation ». Ce centre transmet un nombre innombrable de contenus aux pays concernés par les adresses IP localisées pour identifications et interpellations. C'est pourquoi chaque jour en France des interpellations ont lieu par les forces de l'Ordre et des affaires défrayant la chronique sont jugées. Les nouvelles dispositions américaines à la suite des élections présidentielles pourraient affecter ces coopérations internationales ce qui reste à surveiller, dans la mesure où aux Etats-Unis les fournisseurs de service étaient obligés de signaler les CSAM.

> **Il n'y a pas dans l'Union Européenne de hub de signalement central** tel celui du Ncmec dont dépend la lutte de l'UE contre les CSAM. Aussi la future législation euro-

INHOPE fait partie du projet CPORT, portail qui permet aux forces de l'ordre d'accéder à l'ICCAM, la plateforme sécurisée centralisée utilisée par les hotlines INHOPE.

péenne crée-t-elle un Centre européen de prévention et de répression des abus sexuels commis contre des enfants, qui recueillera les signalements des trusted flaggers et des fournisseurs de service (FS) et les adressera pour exploitations aux pays. Le fonctionnement reposera sur la vigilance des outils utilisés aux bonnes fins par les FS pour détecter les CSAM. Il éditera un rapport de transparence sur les processus de recherche, de signalement et de suppression des matériels pédo-criminels.

> **Les fournisseurs de services en ligne de communications électronique.** Si en France, les fournisseurs d'accès à l'Internet, les éditeurs qui contrôlent les contenus et hébergeurs qui ne contrôlent pas les contenus ou autres plates-formes intermédiaires, doivent respecter le principe de la neutralité du net, i.e. de garantir l'accès à l'Internet et la libre circulation des contenus sans discrimination, ils sont soumis aux obligations de l'article 6 de la Loi du 21 juin 2004 modifiée (LCEN) à savoir participer à la lutte notamment contre les CSAM. Ainsi, les hébergeurs ne sont pas tenus à une obligation de surveillance générale et illimitée dans le temps, ils doivent a posteriori, retirer promptement le contenu manifestement illicite qui tombe sous le coup de la Loi dès lors qu'ils en ont connaissance. Toutefois dans son arrêt du 15 janvier 2025 de la Cour de Cassation affirme que des obligations contractuelles peuvent être plus strictes que celle de la Loi, permettant la modération a priori pour détecter les posts frauduleux, satisfaisant ainsi aux obligations de l'article 6 supra. Au niveau européen, le Digital Service Act (DSA), règlement sur les services numériques maintient le principe de non responsabilité de ces fournisseurs de services numériques reprenant le droit français, tout en invitant les grandes plates-formes à prendre des mesures de modération a priori, afin de prévenir les risques systémiques de disséminations de contenus illégaux tels les CSAM, leur utilisation alliant rapidité de diffusion et communication de masse.

Les retraits administratifs et judiciaires de contenus illicites

La poursuite d'infractions très massives a conduit, comme dans d'autres domaines, à prendre des mesures administratives pour des raisons d'efficacité, de rapidité de réparation pour les victimes. Ainsi les demandes de déréférencement par les moteurs de recherches, le retrait ou blocage administratif auprès des éditeurs et hébergeurs de contenus illicites notamment pédocriminels, a été confié à l'OFAC avec des voies de recours contre un éventuel retrait abusif sous la houlette d'une personnalité qualifiée, laquelle apprécie a posteriori la décision susceptible d'être transmise à un juge et donc d'être annulée. Tout un chacun peut demander le retrait, sous conditions de forme, auprès de l'Autorité Judiciaire sur le fondement de l'ordonnance 145 du code de procédure civile selon des critères contraignants ou auprès des éditeurs puis hébergeurs. Mais mieux vaut utiliser pour retirer un CSAM, la loi du 24 août 2021 modifiant l'article 6.I.8 de la LCEN modifiée le 21 mai 2024 (devenu le 6-3) qui permet sur demande à l'Autorité judiciaire, au seul Président du tribunal judiciaire, d'enjoindre le retrait de contenu illicite à « toute personne» par la procédure accélérée au fond (ancien référé) afin de prévenir ou de faire cesser un dommage occasionné par un contenu d'un service de communication au public en ligne.

Ce système de responsabilité directe des éditeurs de contenus et indirecte des hébergeurs, protège la liberté de communication tout en la conciliant avec la sauvegarde de l'Ordre public qui est assurée avec efficacité en urgence soit par l'OFAC soit par le 1er Président du TJ. Dans le cas général, l'Autorité Judiciaire est destinataire des plaintes vu les articles 6-1 et 6-2 et 6-2-2 de la LCEN du 21 juin 2004 modifiée.

A noter que déjà le 3 octobre 2019 la CJUE dans un arrêt Facebook Ireland Ltd/Eva Glawischnig-Piesczek, jugeait légitime qu'un contenu illicite identique ou équivalent à un contenu déjà jugé illicite puisse être bloqué en Europe voire dans le monde entier même si l'hébergeur n'en avait pas connaissance.

Il convient de rappeler ici que le conseil constitutionnel a clairement indiqué que en 2011 que « ...ces dispositions assurent une conciliation qui n'est pas disproportionnée entre l'objectif de valeur constitutionnelle de sauvegarde de l'ordre public et la liberté de communication garantie par l'article 11 de la Déclaration des droits de l'homme et du citoyen de 1789 ». Ce qui permet que pendant les voies de recours toujours trop longues les contenus ne réapparaissent pas.

Selon le home- affairs de l'Union Européenne : Les prestataires de services en ligne jouent un rôle essentiel dans le signalement des abus sexuels commis contre des enfants en ligne. Malheureusement, le système actuel de notification volontaire n'est pas assez efficace. Actuellement, 95 % des signalements émanent d'un seul prestataire de services (Meta). En tant que société, il s'agit obliger toutes les entreprises technologiques en Europe à détecter et signaler aux autorités les abus sexuels commis contre des enfants en ligne. 76% des européens souhaitent que la détection, le signalement et le retrait de contenus CSAM soit automatisés.

Tous les principes semblent être en place et pourtant l'arsenal des textes répressifs de droit français sur le CSAM doivent être mieux soutenus par une véritable collaboration motu proprio des prestataires de services en lignes qui devraient modérer, retirer et déréférencer les CSAM Comme il leur est fait obligations.

>>>

>>> II. LES TEXTES RÉPRESSIFS FRANÇAIS COUVRANT LE SPECTRE DE LA LUTTE CONTRE LES CSAM SONT BATTUS EN BRÈCHES FAUTE D'UN TEXTE EUROPÉEN CONSENSUEL D'OBLIGATION DE MODÉRATION A PRIORI, TOUJOURS EN COURS DE DISCUSSION.

Faute de ce règlement, c'est un 3e règlement dérogatoire européen, qui permet de scruter les réseaux, des Etats-Membres se retranchant derrière le rejet des possibilités de technologies intrusives qui mettraient en cause les libertés individuelles des adultes, lesquelles passeraient donc avant la protection des mineurs victimes.

Des textes répressifs progressistes en France contre les CSAM et illustrés d'affaires judiciaires doublés des efforts conjugués de l'UE et de la France, des Pays-Bas et l'Italie pour faire aboutir le règlement européen qui remplacera le règlement temporaire dérogatoire ayant pris fin en décembre 2020 et prorogé deux fois jusqu'au 3 août 2026 pour débusquer les prédateurs d'enfants.

Lutter contre la pedocriminalité avec le droit existant en France avec l'aide des USA et des réseaux privés européens et le règlement prorogé au 3 août 2026

La dissuasion de textes répressifs aux quantums pourtant importants est relative notamment au regard de la détention d'images pedo-pornographiques, la diffusion de deepfakes jusqu'aux commandes de live streaming car les peines n'entravent pas l'accroissement de la pedo- criminalité, faute de moyens techniques de détection rapide.

> Le principe de protection des mineurs est posé par l'article 227-24 du code pénal qui reprend l'interdiction de l'article 14 de la loi du 16 juillet 1949 modifiée sur les publications destinées à la jeunesse, de l'interdiction de représentation pornographique lorsque le message est susceptible d'être vu par un mineur. « Le fait soit de fabriquer, de transporter, de diffuser par quelque moyen que ce soit et quel qu'en soit le support un message à caractère… pornographique, y compris des images pornographiques impliquant un ou plusieurs animaux, …ou de nature …à inciter des mineurs à se livrer à des jeux les mettant physiquement en danger, soit de faire commerce d'un tel message, est puni de trois ans d'emprisonnement et de 75 000 euros d'amende lorsque ce message est susceptible d'être vu ou perçu par un mineur.

Les infractions prévues au présent article sont constituées y compris si l'accès d'un mineur aux messages mentionnés au premier alinéa résulte d'une simple déclaration de celui-ci indiquant qu'il est âgé d'au moins dix-huit ans ». Ce qui met en évidence la nécessité de déclarer au fournisseur du service sa majorité par le procédé efficace qu'il est censé proposer.

De plus, depuis le 23 avril 2021 l'article 227-23 du code pénal réprime le fait, en vue de sa diffusion, de fixer, d'enregistrer ou de transmettre l'image ou la représentation d'un mineur lorsque cette image ou cette représentation présente un caractère pornographique est puni de cinq ans d'emprisonnement et de 75 000 euros d'amende. …. Le fait d'offrir, de rendre disponible ou de diffuser une telle image ou représentation, par quelque moyen que ce soit, de l'importer ou de l'exporter, de la faire importer ou de la faire exporter, est puni des mêmes peines ; Les peines sont portées à sept ans d'emprisonnement et à 100 000 euros d'amende lorsqu'il a été utilisé, pour la diffusion de l'image ou de la représentation du mineur à destination d'un public non déterminé, un réseau de communications électroniques.

Pour illustrer tristement ces infractions commises dans tous milieux sociaux, selon une affaire de l'OFMIN « Pendant 10 ans, il a envoyé plus de 50 000 euros vers les Philippines et le Kenya pour commander des shows. Ces shows sont des viols d'enfants en direct, le plus souvent réalisés par leurs parents qui exécutent les scénarios et desiderata pédo-criminels de l'internaute derrière son écran à l'autre bout du monde. »

Les articles 227-23-1 sollicitation par un majeur auprès d'un mineur de la diffusion ou la transmission d'images, vidéos ou représentations à caractère pornographique dudit mineur est puni de sept d'emprisonnement et de 100 000 euros d'amende et si circonstance aggravante 10 ans. Il s'agit ici des « nudes » que des enfants ou ados font avec leur webcam ou smartphone à la demande de leur « amoureux » ou autres et qui sont ensuite diffusés sur la toile et sont propices au harcèlement numérique ensuite.

L'article 227-22-1 du code pénal réprime le GROOMING : Le fait pour un majeur de faire des propositions sexuelles à un mineur de quinze ans ou à une personne se présentant comme telle en utilisant un moyen de communication électronique est puni de deux ans d'emprisonnement et de 30 000 euros d'amende.

Ces peines sont portées à cinq ans d'emprisonnement et 75 000 euros d'amende lorsque les propositions ont été suivies d'une rencontre. C'est par les possibilités de messagerie Chat des jeux vidéos ou autres, en ligne par exemple que les prédateurs entrent en contact avec les mineurs se faisant passer pour mineurs allant jusqu'à provoquer des rencontres dans la vie physique.Cf la vidéo les dangers d'Internet John de la préfecture de Police de Paris, libre de droits.

En septembre 2024, un ancien magistrat qui proposait sa fille de 12 ans sur un réseau de communication en ligne a été condamné en appel pour incitation à la commission d'un viol et incitation à la corruption de mineur.

> **La répression de certains deepfakes et infraction approchante.** Le phénomène de sextorsion via l'intelligence artificielle (IA) fait de plus en plus de victimes chez les mineurs. Les deepfakes,ou deep nudes images hypersexualisées, créées avec le visage d'une personne sur un corps qui ne lui appartient pas, générés par des IA, truquent des contenus audio et vidéo en utilisant des critères physiques, morphologiques et gestuels. Ils sont utilisés pour des infractions sexuelles, du revenge porn ou du chantage envers les mineurs.

En France : Les articles 226-8 du Code pénal et 226-8-1 répriment les montages vidéos diffusés sans consentement, s'il n'apparaît pas évident qu'il s'agit d'un montage ou s'il n'en est pas expressément fait mention. Les deepfakes sont poursuivis sous cette qualification pénale. Les sanctions pour diffusion de montages réalisés avec les paroles ou l'image d'une personne sans consentement peuvent aller jusqu'à un an de prison et 15 000 euros d'amende. C'est la Loi du 21 mai 2024 qui a élargi le périmètre par l'inclusion des traitements algorithmiques consistant en hypertrucages (ou deepfakes), qui sont des synthèses multimédias basées sur l'intelligence artificielle.

La publication de montages à caractère sexuel réalisés sans consentement est punie de 3 ans et 75 000€ d'amende si c'est une publication en ligne. (226-8-1) ce qui parait peu au vu de l'impact de la diffusion.

> **Le rapport SOCTA d'Europol de mars 2025** mentionne l'IA utilisée à des fins de création de matériel pédo-criminel. C'est justement selon la Tribune pour répondre à cette brèche nouvelle en matière de pédocriminalité que le sénateur des Hauts-de-Seine Xavier Iacovelli a déposé en février une proposition de loi, pour lutter contre la création de contenus pédo-criminels au moyen de l'intelligence artificielle générative.

> **Le règlement provisoire relatif aux CSAM** prorogé une deuxième fois en 2021 a été encore prorogé jusqu'au 3 avril 2026 en attendant un accord sur un texte définitif qui aurait dû être trouvé avant le 3 août 2024…

> **Actuellement, les efforts volontaires des opérateurs** visant à détecter les abus sexuels commis contre des enfants en ligne font l'objet d'une surveillance limitée au-delà des dispositions de ce règlement provisoire (Règlement (UE) 2021/1232 du Parlement européen et du Conseil du 14 juillet 2021 portant dérogation temporaire à certaines dispositions de la directive 2002/58/CE en ce qui concerne l'utilisation de technologies par les fournisseurs de services de communications interpersonnelles indépendants de la numérotation pour le traitement des données à caractère personnel et autres données aux fins de la lutte contre les abus sexuels commis contre des enfants en ligne (Texte présentant de l'intérêt pour l'EEE) puis de sa prolongation (Règlement (UE) 2024/1307 du Parlement européen et du Conseil du 29 avril 2024 modifiant le règlement (UE) 2021/1232 portant dérogation … aux fins de la lutte contre les abus sexuels commis contre des enfants en ligne (Texte présentant de l'intérêt pour l'EEE)

Ainsi ces fournisseurs de service sont tenus de retirer et signaler aux FDO les contenus relatifs au CSAM.

C'est pourquoi, « pour combattre ce fléau mondial, l'UE a proposé une législation qui nous aidera à détecter, signaler et prévenir les cas d'abus sexuels commis contre des enfants en ligne et à soutenir les victimes. Sans législation définitive Les entreprises technologiques ne pourront plus détecter, signaler et supprimer les contenus illicites dans les services de communication, qui sont aujourd'hui le moyen le plus efficace de diffuser des contenus à caractère pédopornographique et de piéger les enfants: En 2021, les communications électroniques étaient à l'origine de 80 % des signalements !

> Les peines sont portées à sept ans d'emprisonnement et à 100 000 euros d'amende

Toute infraction au DSA précité notamment sur les CSAM sera passible d'amendes jusqu'à 6% du chiffre d'affaires mondial ». Les très grandes plates-formes de plus de 45 millions d'abonnés respectent à peu près le DSA pour éviter le risque de procédures au lieu d'exercice de leur activité européenne ; mais au vu du cloud act elles sont en contradiction avec leurs maisons mères.

Le DSA a créé également une catégorie de signaleurs de confiance (trusted flaggers) des associations telles point-decontact.net, ou e-enfance désignées par l'ARCOM dont les alertes seront traitées en priorité ; Ils établiront un rapport annuel à l'ARCOM.

Reste à voir quelle articulation entre les hotlines les trusted Flaggers, PHAROS/OFAC et le futur centre européen de prévention et de répression des abus sexuels commis contre des enfants.

>>>

>>> Les difficultés à sortir le Règlement définitif qui fait douter de la volonté de certains pays de protéger les enfants avant leur liberté individuelle

La Proposition de RÈGLEMENT DU PARLEMENT EUROPÉEN ET DU CONSEIL établissant des règles pour prévenir et combattre les abus sexuels envers les enfants COM/2022/209 final, ne fait pas consensus en raison des moyens intrusifs qu'elle doit permettre de mettre en œuvre pour détecter les contenus images et textes dans les échanges. Or les abus sexuels sur mineurs constituent un problème croissant, tant en ligne que hors ligne. Rien qu'en 2022, 1,5 million d'abus sexuels sur mineurs ont été signalés dans l'UE.

> **En attendant un hypothétique accord consensuel,** la commission européenne poursuit la mise en œuvre de la stratégie de 2020 à 2025 de lutter notamment contre les CSAM ; le 6 février 2024, la Commission a adopté la proposition du parlement et du conseil pour une refonte de la directive 2011/93/UE visant à actualiser les règles de droit pénal relatif aux abus sexuels et à l'exploitation sexuelle des enfants. Les règles révisées élargissent la définition des infractions, introduisant des sanctions plus lourdes et des exigences plus spécifiques en matière de prévention et d'assistance aux victimes. Elles complètent la proposition de règlement présentée par la Commission en 2022, qui impose aux entreprises internet de détecter, signaler et supprimer les contenus pédopornographiques présents sur leurs services.

> **Pourquoi l'accord sur le règlement européen du parlement et du conseil proposé en 2022** n'est-il **pas encore adopté ?** Les pays discutent sur un enjeu pourtant prétendu consensuel ! La commission européenne indique que la proposition est nécessaire et proportionnée compte tenu du développement et des ordres de grandeur du CSAM.

> **Il est bloqué au Conseil européen** car les discussions sous la Présidence hongroise n'ont pas abouti notamment en raison de la résistance de l'Allemagne puis des Pays-Bas alors que la Finlande et la France étaient favorables avec notamment l'assurance du chiffrement de bout en bout des échanges scrutés. Tandis que la République Tchèque est défavorable au règlement pour des raisons économiques. Deux éditeurs de sites pornographiques établis en République tchèque, les sociétés Webgroup Czech Republic et NKL Associates sro, ont saisi le Conseil d'Etat contre l'application à leur encontre des pouvoirs de sanction de l'ARCOM '(Loi et décret d'application de 2024). Le Conseil d'État saisit donc la Cour de justice de l'Union européenne sur l'enjeu de l'application de la loi pénale, en particulier des dispositions relatives à la protection des mineurs. Il s'agit d'une question de principe importante sur la possibilité pour la France de faire respecter sa loi pénale par un service numérique établi dans un autre État de l'Union européenne. Autre exemple, le puissant site AYLO dont dépend notamment le site Pornhub qui diffuse des vidéos pornographiques et héberge des matériels pedo-criminels en streaming depuis sa création en septembre 2007.

> **Certains idéologues tentent de faire accroire que la génération d'images pedo-criminelles serait de la création artistique...** Or c'est également un commerce générant des profits très importants notamment dans certains pays même européens...

> **Certains Etats-Membres refusent la surveillance de masse dans l'analyse de détection par l'Intelligence artificielle** des contenus pedo-criminels sur les plates-formes telles Whatsapp ou Gmail dans les messages privés qui réduirait la liberté individuelle pour certains ou qui risquerait pour d'autres d'entamer la résilience de cybersécurité des messageries over the top (OTT).

> **L'obligation des messageries d'analyser le contenu des communications et de détecter le grooming en temps réels est critiquée** en ce que cela mettrait en cause les libertés fondamentales de nos sociétés démocratiques au-delà de la protection des enfants ainsi que le prétend le contrôleur européen de la protection des données personnelles. L'inquiétude semble plus du côté de la protection des données et de la vie privée plutôt que la protection de l'enfant.

> **Convaincre que de vrais enfants, parfois nourrissons, sont victimes et revictimisés** à chaque résurgence de leurs photos même si ce sont des deeps nudes, ne devrait pourtant pas se heurter aux idéologies mais atteindre la conscience de pères et de mères.

> **En attendant saluons les actions des FDO et de prévention** envers les enfants dans les écoles et collèges voire les entreprises et notamment celle d'ISSA France de Diane Rambaldini et Hadi El Khouri et leur projet Lumérique.

Toute infraction au DSA précité notamment sur les CSAM sera passible d'amendes jusqu'à 6% du chiffre d'affaires mondial »

> **Raphael Pairon, ancien enquêteur de la gendarmerie nationale à l'OFMIN :** « Voici un remarquable reportage sur la lutte contre l'exploitation sexuelle des enfants au niveau international, proposé sur Arte. Comment les services spécialisés, en France (notamment l'OFMIN) et à l'étranger combattent cette forme ultra-violente de criminalité et protègent les enfants victimes....

... et le débat : Sommes-nous prêts à sacrifier un peu de notre vie privée pour permettre de repérer les abus sexuels d'enfants sur les messageries internet qui ne seraient pas chiffrées ?

Chacun va donc voir midi à sa porte. L'IA va regarder ou non les échanges et la confiance dans le traitement des dossiers vers les prédateurs supposés, devra être assortie de garanties de discrétion et de discernement par les humains qui ont le courage de concourir à la lutte contre les Child Sexual Abuse Mineur. Espérons qu'on pourra concilier protection des enfants d'abord et protection de la vie privée des adultes ensuite.

Il faut ordonner nos priorités et donc accepter, pour protéger nos enfants, de peut-être diminuer notre sacro-sainte vie privée, que par ailleurs on dévoile allègrement. Mais ne donnerions-nous pas notre vie pour nos enfants ? Ne peut-on pas laisser s'effacer les idéologies devant la protection de nos enfants ? Pour que les prédateurs ne soient plus tranquilles...

Mais c'est d'abord à la population de prendre conscience de l'ampleur de ce phénomène, qui s'est accru avec le COVID..., qui peut toucher chacun sans le savoir ; l'Etat qui bénéficie du travail des nombreuses associations citées doit se donner les moyens et aider au financement des associations reconnues sérieuses. C'est une question de sécurité et d'éducation donc prioritaire.

Il faut se mettre au niveau des autres pays et ne pas hésiter à communiquer sur ce sujet, même s'il peut sembler dérangeant, comme le font l'OFMIN, le C3N et la BPF de la PP qui ont le courage chaque jour de faire les enquêtes, les interpellations de faits indicibles afin de déférer devant la Justice les prédateurs qui profitent de l'Internet et de son relatif anonymat.

Ce tour d'horizon de la lutte contre les CSAM doit nous interroger sur l'état de la société et sa véritable volonté de protection des enfants, dans une société les exposant de plus en plus à la pédo-criminalité, à la pornographie ou autres contenus illicites notamment via les services de communication au public en ligne. Et ce, en dépit de textes répressifs toujours plus fermes, mais les sanctions données sont-elles à la hauteur de la considération des petites victimes ?

Comme le dit le home-affairs de l'UE, « Nous avons tous la responsabilité de protéger nos enfants contre les prédateurs sexuels. Chaque action compte sous quelque forme que ce soit ». ■

SOURCES

[1] Child sexual abuse minors
[2] Agence Européenne de Police. https://www.europol.europa.eu/
[3] https://www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/rapport-activite-2024
[4] https://www.pointdecontact.net/wp-content/uploads/2023/05/FicheCSAM.pdf
[5] https://www.pointdecontact.net/bande-dessinee-sexting/
[6] https://www.pointdecontact.net/wp-content/uploads/2023/05/FicheGrooming.pdf
[7] https://www.renaissancenumerique.org/publications/protection-des-mineurs-en-ligne-avec-justine-atlan/
[8] https://www.arcom.fr/sites/default/files/2024-10/Arcom-Referentiel-technique-sur-la-verification-de-age-pour-la-protection-des-mineurs-contre-la-pornographie-en-ligne.pdf
[9] Autorité de Régulation de la communication audiovisuelle et numérique. L'ARCOM est une API autorité publique indépendante, responsable de la garantie de la liberté de communication audiovisuelle en France. Elle détient les mêmes pouvoirs qu'une AAI autorité administrative indépendante mais dispose, contrairement à cette dernière, de la personnalité morale et de ressources propres.
[10] https://info.haas-avocats.com/droit-digital/loi-sren-pouvoirs-renforces-de-larcom-sur-les-contenus-en-ligne#:~:text=Les%20conditions%20de%20mise%20en,pouvoirs%20accord%C3%A9s%20%C3%A0%20l'ARCOM.
[11] https://www.europol.europa.eu/media-press/newsroom?q=cyber https://www.europol.europa.eu/media-press/newsroom?q=child
[12] https://www.pointdecontact.net/rapport-annuel-2023/
[13] https://www.inhope.org/EN/the-facts
[14] https://www.clubic.com/actualite-555423-la-france-participe-a-l-arrestation-de-dizaines-de-trafiquants-qui-utilisaient-l-ia-pour-creer-du-contenu-pedocriminel.html
[15] Signaleur de confiance
[16] https://sante.gouv.fr/IMG/pdf/rapport_du_groupe_de_travail_sur_la_prostitution_des_mineurs.pdf
[17] Office central de répression des violences aux personnes
[18] https://www.legifrance.gouv.fr/loda/id/JORFTEXT000048007181/
[19] CNAIP Centre national d'analyse des images pédopornographiques. https://www.gendarmerie.interieur.gouv.fr/gendinfo/dossiers/criminalistique-le-futur-des-a-present/lutte-contre-les-pedocriminels-le-cnaip-bras-arme-de-la-gendarmerie
[20] Huit ans. C'est la peine de prison requise par la présidente du jury de Soissons contre un couple soupçonné d'avoir abusé sexuellement de leurs nièces et de leur fils. Leur interpellation, le 20 octobre 2024, par les militaires du groupement de gendarmerie départementale de l'Aisne, met fin à plus d'une année de traque, menée in extenso par les enquêteurs du Centre d'analyse des images
[21] https://www.interpol.int/fr/Notre-action/Bases-de-donnees/Base-de-donnees-internationale-sur-l-exploitation-sexuelle-des-enfants International Child Sexual Exploitation (ICSE) image and video database
[22] COMMUNICATION - COMMERCE ÉLECTRONIQUE - N° 7-8 - JUILLET-AOÛT 2024 -©LEXISNEXISSA
[23] Brigade d'enquête sur les fraudes aux technologies de l'information dénommée brigade de lutte contre le cybercriminalité
[24] La convention de cybercriminalité de Budapest permettait une certaine coopération policière. La nouvelle convention de cybercriminalité sous l'égide de l'ONU signée au Vietnam n'améliorera vraisemblablement pas la coopération.
[25] Plateforme d'harmonisation, de recoupement et d'orientation des signalements, www.internet-signalement.gouv.fr
[26] https://www.pointdecontact.net/disrupt/ https://www.linkedin.com/company/associationpointdecontact/posts/?feedView=all
[27] Communiqué de presse de la PP de 2019
[28] https://x.com/NCMEC/status/1899553832914280877
[29] COMMUNICATION - COMMERCE ÉLECTRONIQUE - N° 7-8 - JUILLET-AOÛT 2024 -©LEXISNEXISSA
[30] L. n° 2024-449, 21 mai 2024 visant à sécuriser et à réguler l'espace numérique, art. 4
[31] Cour de justice de l'union européenne
[32] https://home-affairs.ec.europa.eu/whats-new/communication-campaigns/euvschildsexual-abuse-campaign-prevent-and-combat-child-sexual-abuse_fr
[33] https://www.doctrine.fr/l/texts/codes/LEGITEXT000006070719/articles/LEGIARTI000043405758?version=LEGIARTI000043405758&sourcePage=Legislation&source=next_article
[34] https://www.dailymotion.com/video/xqla7e
[35] https://www.lefigaro.fr/flash-actu/un-ancien-magistrat-qui-proposait-de-violer-sa-fille-mineure-condamne-pour-la-troisieme-fois-20240930
[36] https://www.village-justice.com/articles/sextorsion-quand-utilisation-detruit-les-mineurs,48054.html
[37] https://www.latribune.fr/la-tribune-dimanche/societe/la-pedocriminalite-via-ia-sous-surveillance-1020178.html
[38] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02021R1232-20240515
[39] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32024R1307
[40] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52022PC0209
[41] https://www.conseil-etat.fr/actualites/acces-en-ligne-aux-contenus-pornographiques-le-conseil-d-etat-saisit-la-cour-de-justice-de-l-union-europeenne-de-l-enjeu-de-la-protection-des-mineurs
[42] https://fr.wikipedia.org/wiki/MindGeek
[43] https://www.arte.tv/fr/videos/113627-000-A/pedocriminels-la-traque/

L'ISSA FRANCE LANCE

LUMÉRIQUE

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

LUMÉRIQUE, C'EST QUOI ?

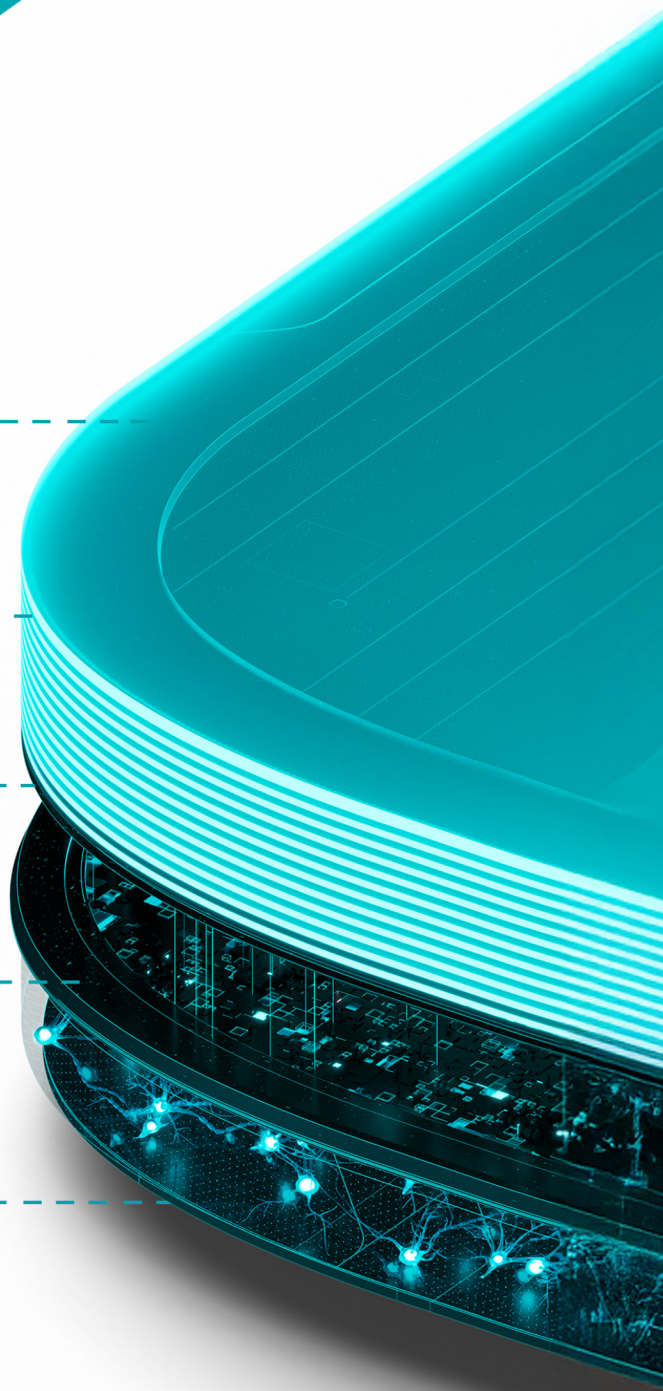
C'est vous, c'est nous ! C'est un mouvement citoyen et collectif !
C'est vous, qui aspirez à protéger les jeunes des risques d'un monde numérique complexe.
C'est vous, qui y voyez une cause d'intérêt général.
C'est vous, qui estimez que c'est urgent pour relever les défis sociétaux, économiques et démocratiques du XXIe 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

LES NOUVELLES TECHNOLOGIES (IA, QUANTIQUE, SASE, SOAR, aXDR, ZERO TRUST…) et la Cybersécurité

> LES HÔPITAUX SONT-ILS SI DIFFÉRENTS DES ENVIRONNEMENTS INDUSTRIELS ?

Pas tant que ça. En réalité, ils présentent des caractéristiques proches : hétérogénéité des équipements, contraintes réglementaires fortes, disponibilité 24/7, réseau multisite, coexistence d'anciens et de nouveaux systèmes. Comme dans une usine, on y trouve une grande diversité de systèmes, et comme dans l'industrie, une faille peut avoir un impact immédiat sur la production.

> POURQUOI PARLE-T-ON DE PLUS EN PLUS DE CYBERSÉCURITÉ DANS LES HÔPITAUX ?

Parce que les cyberattaques contre les établissements de santé se multiplient. Elles visent des systèmes critiques, souvent vieillissants, et des données médicales très lucratives. Une attaque peut paralyser un hôpital, retarder des soins ou provoquer des transferts d'urgence. La protection des actifs numériques est donc devenue une question de continuité des soins.

> QUE PEUT-ON FAIRE POUR PROTÉGER CES ENVIRONNEMENTS COMPLEXES SANS TOUT RECONSTRUIRE ?

Il ne s'agit pas de repartir de zéro, mais d'adopter une approche pragmatique. Isoler les systèmes critiques, appliquer le principe du moindre privilège, déployer une supervision comportementale, à partir des EPP + EDR, sauvegarder régulièrement, former le personnel aux bons réflexes (phishing, mots de passe, non partage des comptes…).

> EST-IL RÉALISTE DE VISER UNE SÉCURITÉ DE HAUT NIVEAU DANS LE SECTEUR DE LA SANTÉ ?

Oui, à condition de mutualiser les compétences et les outils. Tous les hôpitaux ne peuvent pas se doter d'un SOC (centre de supervision) ou d'une équipe dédiée. En revanche, ils peuvent s'appuyer sur des plateformes de sécurité pensées pour les environnements critiques, accompagnées de services d'analyse. Ils bénéficient ainsi d'un niveau de protection élevé, à coût maîtrisé. D'autre part, lors du choix de son partenaire, il faut considérer sa capacité à délivrer des solutions sur de nombreuses plateformes, tout en laissant le choix de l'hébergement. Cloud éditeur, cloud privé/public ou sur site. Peu de solutions offre ce niveau de flexibilité.

> LES SOLUTIONS DE CYBERSÉCURITÉ SONT-ELLES ADAPTÉES À LA DIVERSITÉ DES ÉQUIPEMENTS HOSPITALIERS ?

Certaines le sont, en particulier celles conçues pour des environnements industriels ou hybrides. Elles sont capables de fonctionner sur des postes anciens, d'intégrer des équipements médicaux sans les perturber et de s'insérer dans une architecture existante.

La légèreté, la compatibilité et la centralisation sont des critères essentiels. Il faut également considérer les fonctions permettant de répondre aux exigences d'une bonne hygiène : chiffrement, inventaire logiciel et matériel, gestion des vulnérabilités… En choisissant une solution couvrant un périmètre large, les établissements peuvent se rapprocher des bonnes pratiques sans multiplier les outils.

> RÉDUIRE LE NOMBRE D'OUTILS, EST-CE VRAIMENT UN AVANTAGE ?

Oui, c'est même un levier important d'efficacité. Moins de produits à acquérir et maintenir, engendre un coût global réduit et réduit la complexité opérationnelle pour les équipes. Elles gagnent de fait en expertise sur un nombre limité de solutions. Une solution bien intégrée permet une meilleure visibilité, une réponse plus rapide aux incidents, et une charge allégée. Il ne s'agit pas de tout faire d'un coup, mais de construire une sécurité adaptée, évolutive, réaliste. L'enjeu n'est pas de viser la perfection, mais la résilience. Un éditeur de qualité doit suivre la maturité de ses clients, tant en solutions qu'en services associés.

> QUEL EST LE MESSAGE PRINCIPAL À RETENIR ?

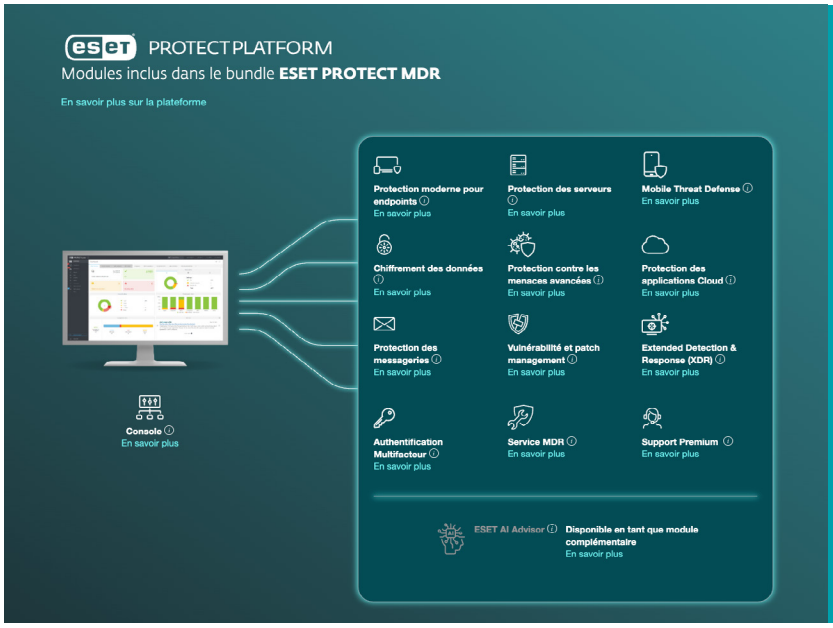
En s'appuyant sur des outils conçus pour des environnements critiques et les services qui les accompagnent, les établissements peuvent viser la résilience : sécuriser efficacement leurs systèmes sans compromettre leur fonctionnement. De plus, en limitant le nombre de prestataires, ils renforcent leur agilité – notamment en cas d'incident – tout en maîtrisant leur budget.

Hospitals and industrial environments share similar characteristics, such as diverse equipment, strong regulatory constraints, 24/7 availability, and the coexistence of old and new systems.

Cybersecurity in hospitals is increasingly important due to the rise in cyberattacks targeting critical systems and valuable medical data. These attacks can disrupt healthcare services and endanger patients.

To protect these complex environments without starting from scratch, hospitals should adopt a pragmatic approach: isolating critical systems, applying the principle of least privilege, deploying behavioral monitoring, regular backups, and training staff on best practices. Achieving high-level security in healthcare is realistic by mutualizing competencies and tools, such as Security Operation Centers (SOC) or dedicated teams, and using platforms designed for critical environments.

Effective cybersecurity solutions for hospitals must be adaptable to diverse equipment, lightweight, compatible, and centralized. Reducing the number of tools enhances efficiency, lowers costs, and simplifies operations. The goal is not perfection but resilience, ensuring hospitals can secure their systems effectively without compromising functionality. By relying on quality tools and services, hospitals can strengthen their agility and budget control, especially during incidents.



CONTACTS :
BENOIT GRÜNEMWALD
Directeur des affaires Publiques ESET France
Membre Clusif
Courriel : benoit.g@eset-nod32.fr

LES NOUVELLES TECHNOLOGIES (IA, QUANTIQUE, SASE, SOAR, XDR, ZERO TRUST...) et la Cybersécurité

> SELON VOUS, QUELS SONT LES ENJEUX AU SUJET DES NOUVELLES TECHNOLOGIES (IA, QUANTIQUE, SASE, SOAR, XDR, ZERO TRUST...) EN CYBERSÉCURITÉ ?

Le développement de nouvelles technologies comme l'IA ou l'informatique QUANTIQUE représente à la fois un formidable levier d'innovation et de compétitivité pour les organisations, mais aussi un défi majeur en matière de cybersécurité.

Le quantique, par exemple, ouvrira la voie à de nouveaux modèles économiques et à des avantages concurrentiels inédits. De la même manière que l'IA apporte déjà des gains d'efficacité dans de nombreux métiers et processus, sans parler des offres business qui se sont construites ou développées dans son sillon.

Mais ces avancées technologiques ont leur revers : l'arrivée du quantique remettra par exemple inévitablement en question nos mécanismes actuels de chiffrement, tandis que l'IA introduit déjà de nouvelles surfaces d'attaque et d'ambiguïté dans la chaîne de confiance.

Plus tôt ces technologies sont donc étudiées, contextualisées et comprises, plus tôt les organisations peuvent se positionner de manière éclairée sur leur utilisation.

Par exemple, nous avons très souvent constaté que l'IA était adoptée individuellement par beaucoup dans les organisations sans avoir eu en amont l'analyse approfondie de son impact sur les processus, les flux ou les responsabilités humaines de l'entreprise.

Le véritable défi est donc organisationnel : comment garder la maîtrise de son architecture de sécurité dans un écosystème mouvant et technologique par nature pour intégrer efficacement de nouvelles technologies.

Quant aux SASE, SOAR, XDR ou Zero Trust, elles sont avant tout des réponses fonctionnelles et méthodologiques à cette complexité croissante. Elles permettent de renforcer la visibilité, d'automatiser les actions de défense et d'améliorer l'orchestration des alertes. Mais leur efficacité dépend largement de leur intégration cohérente dans un cadre de gouvernance bien défini.

> QUELLES SOLUTIONS DE VOTRE ENTREPRISE OU ORGANISATION PERMETTENT DE GÉRER AU MIEUX LES CYBERMENACES INDUITES PAR LES NOUVELLES TECHNOLOGIES ? ET POUR QUELLES RAISONS ?

Chez Davidson, nous sommes partisans d'une approche centrée sur le pilotage par les risques, car toutes les organisations ne font pas face aux mêmes menaces, ni aux mêmes enjeux métiers. Cela implique une analyse continue et

contextualisée des surfaces d'exposition de nos clients, mais aussi une capacité à ajuster les priorités au fil des évolutions technologiques et organisationnelles.

La sensibilisation des collaborateurs reste, pour nous, un pilier fondamental : elle permet de maintenir un socle de maturité cyber sain et de développer un esprit critique indispensable surtout face à des outils et scénarios d'attaque de plus en plus sophistiqués.

L'IA, en particulier, commence déjà à bouleverser notre rapport à la véracité des informations et à la confiance que nous accordons à ce que nous voyons, lisons ou entendons.

Enfin, nous attachons une grande importance à la qualité des équipes de réponse à incident, capables d'assurer la détection, la remédiation et la résilience. (VOC/SOC/CERT/CSIRT).

> GS MAG : QUELLES ÉVOLUTIONS, À COURT, MOYEN OU LONG TERME, VOYEZ-VOUS DANS CE DOMAINE DES NOUVELLES TECHNOLOGIES ?

À court terme, l'intelligence artificielle va continuer de monter en puissance dans les organisations. Qu'il s'agisse de son intégration dans les outils du quotidien, de l'émergence d'assistants métiers spécialisés, ou encore de la création de nouvelles offres, l'IA va profondément transformer nos manières de travailler. Elle ne se contentera pas d'optimiser des tâches : dans certains cas, elle modifiera en profondeur la nature même du travail.

Dans le même temps, nous voyons déjà des approches comme le Zero Trust, le SASE ou les outils d'orchestration et d'automatisation devenir des standards opérationnels. Les environnements les plus matures les ont déjà intégrés, et les autres suivront rapidement, à court ou moyen terme.

À long terme, l'informatique quantique constitue une véritable rupture : sa capacité à casser les algorithmes de chiffrement actuels remet en cause des fondations entières de notre cybersécurité — de l'authentification aux échanges de données sécurisés.

Cette perspective impose de repenser nos architectures, en explorant des approches alternatives d'authentification qui ne reposent pas uniquement sur la cryptographie classique, ainsi que l'adoption progressive de standards post-quantiques.

Plus globalement, nous pensons que la cybersécurité devra devenir plus intuitive, contextualisée et métier-centric, pilotée par la donnée en temps réel.

The development of technologies like AI and quantum computing offers significant innovation and competitiveness but also poses major cybersecurity challenges.

Quantum computing will disrupt current encryption methods, while AI introduces new attack surfaces and trust issues. Organizations must study and integrate these technologies carefully to maintain control over their security architecture.

Approaches like SASE, SOAR, XDR, and Zero Trust enhance visibility, automate defenses, and improve alert orchestration, but their effectiveness depends on coherent integration within a well-defined governance framework.

At Davidson, we advocate for a risk-based approach, continuous analysis of exposure surfaces, and employee sensitization to maintain cyber maturity. Long-term, quantum computing will require rethinking cybersecurity foundations, while AI will transform work processes and necessitate intuitive, data-driven security solutions.

DAVIDSON
CONSULTING

CONTACTS :
Lucas Perez, Directeur Associé - Réseau et Cybersécurité, Davidson consulting
Web : www.davidson.fr
Courriel : lucas.perez@davidson.fr

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

Parlons de vos projets 2025

↘ Davidson.fr/cybersecurite

CYBERSÉCURITÉ
BY DAVIDSON

Entreprise B Certifiée

https://www.hyland.com/fr/company

LES NOUVELLES TECHNOLOGIES (IA, QUANTIQUE, SASE, SOAR, aXDR, ZERO TRUST…) et la Cybersécurité

> SELON VOUS, QUELS SONT LES ENJEUX AU SUJET DES NOUVELLES TECHNOLOGIES (IA, QUANTIQUE, SASE, SOAR, XDR, ZERO TRUST…) EN CYBERSÉCURITÉ ?

Ces nouvelles technologies en cybersécurité offrent des opportunités majeures pour renforcer les défenses des systèmes d'information, mais leur efficacité dépend étroitement de la structuration, sécurisation et gouvernance des informations non structurées. Ces contenus – documents, e-mails, messages – représentent la majorité des données en entreprise, mais sont souvent mal classifiés et peu protégés.

Or, pour que l'IA, Zero Trust ou XDR soient réellement efficaces, elles doivent s'appuyer sur des données bien indexées, enrichies de métadonnées pertinentes (sensibilité, propriétaire, cycle de vie). Sans cela, pas de politique d'accès granulaire, ni de détection fiable des risques. De même, les approches comme SASE ou SOAR, qui reposent sur une sécurité distribuée et interconnectée, nécessitent une vision unifiée des données et des politiques transverses, y compris pour les documents non structurés. Sur le plan réglementaire, la conformité (RGPD, DORA, HIPAA…) impose de localiser, classifier et protéger les contenus sensibles, ce qui requiert une gouvernance documentaire rigoureuse. Enfin, anticiper les menaces de demain, notamment liées au quantique, commence par sécuriser aujourd'hui les données critiques, en sachant ce qu'elles sont, où elles se trouvent et comment elles sont protégées.

> QUELLES SOLUTIONS DE VOTRE ENTREPRISE OU ORGANISATION PERMETTENT DE GÉRER AU MIEUX LES CYBERMENACES INDUITES PAR LES NOUVELLES TECHNOLOGIES ? ET POUR QUELLES RAISONS ?

Chez Hyland, notre plateforme Nuxeo joue un rôle clé dans la lutte contre les cybermenaces liées aux nouvelles technologies, en permettant de structurer, sécuriser et gouverner les contenus non structurés. Face à des approches comme l'IA, le Zero Trust ou le SASE, qui exigent une compréhension fine des données, Nuxeo automatise la classification, le tagging, la traçabilité et la gestion du cycle de vie des documents, qu'ils soient hébergés en local, sur le cloud ou en mode hybride.

Cette structuration en amont permet de nourrir efficacement les outils de cybersécurité en données fiables et d'appliquer des politiques d'accès dynamiques. La plateforme intègre en natif des fonctions de chiffrement, d'audit, de contrôle d'accès et de conformité réglementaire, tout en s'intégrant facilement aux solutions de sécurité du marché.

> GS MAG : QUELLES ÉVOLUTIONS, À COURT, MOYEN OU LONG TERME, VOYEZ-VOUS DANS CE DOMAINE DES NOUVELLES TECHNOLOGIES ?

Dans le domaine des nouvelles technologies en cybersécurité, les évolutions à venir – à court, moyen et long terme – convergent toutes vers un besoin accru de gouvernance intelligente des contenus. À court terme, l'IA sera utilisée de façon plus ciblée pour classifier automatiquement les documents et détecter les comportements à risque, à condition que les données soient enrichies et exploitables, comme le permet Nuxeo.

À moyen terme, la généralisation de Zero Trust et SASE exigera une vision granulaire des droits d'accès, nécessitant une structuration rigoureuse des contenus pour éviter les zones d'ombre.

À long terme, le calcul quantique remettra en question la cryptographie actuelle, forçant les organisations à identifier dès maintenant les données critiques à protéger.

Enfin, l'avenir passera par une intégration renforcée entre plateformes de contenu comme Nuxeo et les solutions de cybersécurité, grâce à l'automatisation, aux APIs ouvertes et à l'analyse avancée.

New cybersecurity technologies offer major opportunities to strengthen information systems, but their effectiveness depends on the structuring, securing, and governance of unstructured information.

These contents—documents, emails, messages—represent the majority of enterprise data but are often poorly classified and protected. For AI, Zero Trust, or XDR to be effective, they must rely on well-indexed data enriched with relevant metadata. Without this, granular access policies and reliable risk detection are impossible.

Regulations like GDPR, DORA, and HIPAA require locating, classifying, and protecting sensitive content, necessitating rigorous document governance. Hyland's Nuxeo platform plays a key role in addressing these challenges by automating the classification, tagging, traceability, and lifecycle management of documents, whether hosted locally, in the cloud, or in hybrid mode. This upfront structuring feeds cybersecurity tools with reliable data and enables dynamic access policies.

In the short term, AI will be used more precisely to classify documents and detect risky behaviors, provided the data is enriched and exploitable. In the medium term, the widespread adoption of Zero Trust and SASE will require granular access controls, necessitating rigorous content structuring. Long term, quantum computing will challenge current cryptography, forcing organizations to identify and protect critical data now. The future lies in stronger integration between content platforms like Nuxeo and cybersecurity solutions through automation, open APIs, and advanced analytics.

HYLAND™

CONTACTS :
Mountaha (Moun) NDIAYE
EMEA Director Ecosystem
Sales and Programs, Hyland
Courriel : Mountaha.Ndiaye@hyland.com

LES NOUVELLES TECHNOLOGIES (IA, QUANTIQUE, SASE, SOAR, aXDR, ZERO TRUST…) et la Cybersécurité

> SELON VOUS, QUELS SONT LES ENJEUX AU SUJET DES NOUVELLES TECHNOLOGIES (IA, QUANTIQUE, SASE, SOAR, XDR, ZERO TRUST…) EN CYBERSÉCURITÉ ?

Les nouvelles technologies transforment radicalement la cybersécurité, et c'est à la fois une opportunité et un défi. L'IA, par exemple, permet d'analyser des volumes de données gigantesques en un temps record et d'identifier des comportements suspects avant même qu'une attaque ne se produise. Mais elle est aussi exploitée par les cybercriminels, qui l'utilisent pour créer des attaques plus sophistiquées et difficilement détectables.

Le quantique, lui, remet en question nos standards de chiffrement actuels. C'est une bombe à retardement : dès que cette technologie sera suffisamment mature, certaines méthodes de protection utilisées aujourd'hui deviendront obsolètes du jour au lendemain. Il faut s'y préparer dès maintenant.

Enfin, l'approche Zero Trust devient incontournable. Les attaques sont de plus en plus ciblées, les frontières réseau n'existent plus vraiment avec le cloud et le télétravail… Il ne faut plus faire confiance par défaut à aucun utilisateur ou appareil. C'est une transformation majeure qui demande une remise en question des modèles traditionnels de cybersécurité.

> QUELLES SOLUTIONS DE VOTRE ENTREPRISE OU ORGANISATION PERMETTENT DE GÉRER AU MIEUX LES CYBERMENACES INDUITES PAR LES NOUVELLES TECHNOLOGIES ? ET POUR QUELLES RAISONS ?

Chez Exabeam, nous pensons qu'un changement de paradigme est nécessaire pour contrer ces nouvelles menaces.

■ **Sortir du cadre des règles statiques : l'analyse comportementale**

Historiquement, la détection des menaces repose sur des signatures et des règles statiques, souvent contournées par des attaquants qui savent s'adapter. Exabeam adopte une approche différente : plutôt que de surveiller uniquement

des événements isolés (tentatives de connexion échouées, exécutions de commandes suspectes), nous analysons en profondeur les comportements des utilisateurs et des machines.

Grâce à l'intelligence artificielle et au User & Entity Behavior Analytics (UEBA), notre solution établit une base de référence des comportements "normaux" et détecte toute déviation suspecte, même si elle semble légitime à première vue. Par exemple, une connexion depuis un pays inhabituel, avec des horaires et des habitudes qui ne correspondent pas à l'utilisateur, peut être immédiatement signalée comme suspecte, même si les identifiants utilisés sont valides.

■ Vers une cybersécurité multicouche : une seconde barrière essentielle

Les systèmes traditionnels partent du principe que si une connexion réussit à s'authentifier correctement, elle est fiable. Or, avec l'évolution des attaques et l'essor du Zero Trust, il devient impératif d'avoir une seconde ligne de défense, indépendante des mécanismes de protection initiaux.

C'est pourquoi nous intégrons une détection globale, capable d'identifier les attaques même après une compromission initiale. Cette approche permet de repérer des comportements anormaux post-authentification :

- Un employé qui commence à exfiltrer des volumes de données inhabituels.
- Un administrateur qui modifie ses accès sans raison apparente.
- Une machine qui se connecte à des ressources normalement hors de son périmètre.

En s'intégrant aux modèles Zero Trust, SASE et XDR, Exabeam assure une visibilité complète sur l'ensemble des environnements IT et cloud, permettant aux équipes SOC d'avoir une réponse rapide et automatisée face aux menaces avancées.

■ L'avenir de la cybersécurité : vers une détection et une réponse autonomes avec les agents IA

Le volume des cyberattaques et la complexité des environnements informatiques modernes rendent impossible une gestion entièrement manuelle des menaces. C'est pourquoi l'avenir de la cybersécurité repose sur des agents IA capables d'automatiser l'ensemble du cycle de réponse : détection, triage et remédiation.

Chez Exabeam, nous travaillons sur une nouvelle génération d'agents IA, capables de :

- Analyser en temps réel les événements de sécurité et de prioriser les alertes selon leur criticité.
- Corréler automatiquement les signaux faibles pour identifier les attaques furtives.
- Orchestrer une réponse dynamique : isoler un endpoint, bloquer un compte, lancer une enquête approfondie sans intervention humaine directe.

L'IA ne remplace pas l'humain, mais elle permet aux analystes SOC de se concentrer sur les incidents réellement critiques. En réduisant le bruit des fausses alertes et en accélérant les décisions de remédiation, cette approche diminue considérablement le temps de réponse et renforce la cybersécurité proactive.

> QUELLES ÉVOLUTIONS, À COURT, MOYEN OU LONG TERME, VOYEZ-VOUS DANS CE DOMAINE DES NOUVELLES TECHNOLOGIES ?

■ L'avenir de la cybersécurité : vers plus d'autonomie, d'intelligence et d'intégration

Les nouvelles technologies transforment profondément le paysage cyber, et les attaquants savent en tirer parti. L'évolution du cloud, de l'IA générative et de l'informatique quantique redéfinit les menaces et impose de repenser les approches de défense. Chez Exabeam, nous voyons plusieurs grandes tendances qui impacteront la cybersécurité à court, moyen et long terme.

■ À court terme : l'automatisation pour réduire la charge des SOC

Aujourd'hui, les équipes SOC sont saturées par un volume d'alertes trop élevé. L'augmentation de la surface d'attaque avec le cloud, le télétravail et les environnements hybrides génère des millions d'événements par jour, dont seulement une infime partie représente de véritables incidents.

L'automatisation et l'IA vont donc continuer à se généraliser pour :

- Réduire le bruit et prioriser intelligemment les alertes.
- Automatiser les réponses aux incidents sans intervention humaine pour les menaces courantes.
- Permettre aux analystes de se concentrer sur les attaques réellement sophistiquées.

■ À moyen terme : des agents IA pour des SOC autonomes

L'IA ne va pas seulement aider les analystes, elle va peu à peu devenir un véritable acteur de la cybersécurité, capable d'enquêter et de réagir en temps réel. Nous allons assister à l'émergence d'agents IA spécialisés, capables de :

- Corréler des signaux faibles pour identifier des attaques complexes en quelques secondes.
- Orchestrer la remédiation : désactiver un compte compromis, isoler une machine infectée, appliquer des règles de blocage sans intervention humaine.
- Apprendre en continu pour s'adapter aux nouvelles techniques des attaquants.

■ À long terme : une cybersécurité prédictive et post-quantique

L'arrivée de l'informatique quantique menace de rendre obsolètes les protections cryptographiques actuelles. Cela signifie que dans un avenir proche, des attaques pourront casser les clés de chiffrement et compromettre des systèmes aujourd'hui Considérés comme sécurisés.

Face à cette révolution, plusieurs évolutions majeures sont à prévoir :

- De nouveaux algorithmes de chiffrement résistants au quantique, que les entreprises devront adopter rapidement.
- Une cybersécurité plus prédictive, où l'IA et l'analyse comportementale permettront d'anticiper les attaques avant qu'elles ne surviennent.
- L'intégration de la cybersécurité à tous les niveaux : la protection ne se fera plus uniquement à travers des outils dédiés, mais sera directement intégrée aux infrastructures IT, aux logiciels et même aux objets connectés.

New technologies like AI and quantum computing are transforming cybersecurity, presenting both opportunities and challenges.

AI enables rapid analysis of vast data volumes to detect suspicious behaviors preemptively, but cybercriminals also exploit it for sophisticated attacks. Quantum computing threatens current encryption standards, requiring immediate preparation. The Zero Trust approach is becoming essential as attacks grow more targeted, and traditional network boundaries dissolve with cloud and remote work.

Exabeam advocates for a paradigm shift, moving away from static rules to behavioral analysis. Using AI and User & Entity Behavior Analytics (UEBA), Exabeam establishes a baseline of normal behavior and detects deviations, even if they appear legitimate. This multilayered approach ensures visibility and rapid response to advanced threats, integrating seamlessly with Zero Trust, SASE, and XDR models.

The future of cybersecurity lies in autonomous AI agents that automate detection, triage, and remediation, reducing noise from false alerts and enabling SOC teams to focus on critical incidents. Short-term, automation will alleviate SOC workloads. Medium-term, AI agents will become key actors in cybersecurity, capable of real-time investigation and response. Long-term, post-quantum cryptography and predictive security will be essential as quantum computing renders current protections obsolete. Integrating security at all levels, from IT infrastructure to connected devices, will be crucial.

exabeam™

INFORMATIONS PRATIQUES
Solutions / Conseils phares
Exabeam New-Scale SIEM, Exabeam Security Operations Platform
Matthieu POTIN, Regional Manager France
Courriel : Matthieu.potin@exabeam.com
+33 (0)6 08 01 57 37 • exabeam.com

exabeam™

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

LES NOUVELLES TECHNOLOGIES

(IA, QUANTIQUE, SASE, SOAR, aXDR, ZERO TRUST...) et la Cybersécurité

> SELON VOUS, QUELS SONT LES ENJEUX AU SUJET DES NOUVELLES TECHNOLOGIES (IA, QUANTIQUE, SASE, SOAR, XDR, ZERO TRUST...) EN CYBERSÉCURITÉ ?

L'heure n'est plus à la protection périmétrique : l'attaque est devenue algorithmique, furtive et autonome. Et notre défense doit suivre cette même logique. L'intelligence artificielle a radicalement élargi la surface d'attaque. Il devient de plus en plus réaliste d'imaginer des IA malveillantes capables d'identifier automatiquement des vulnérabilités, de planifier et de mener des campagnes d'attaques ultra ciblées, d'esquiver les mécanismes de défense et de récolter et exploiter les données des systèmes infectés et des renseignements open-source. Ce qui change, ce n'est pas seulement la nature des attaques, mais aussi leur cible : nous voyons émerger des offensives contre les « agents cyber » eux-mêmes – EDR, etc. Nous sommes e ntrés dans une nouvelle ère : celle du duel algorithmique, où l'IA offensive affronte une IA défensive. Et c'est un combat à armes égales... ou presque.

Ce bras de fer oblige les entreprises et les éditeurs à repenser en continu leurs approches de sécurité. Grâce à l'IA notamment, il existe un potentiel immense pour renforcer ces stratégies en automatisant la détection des menaces et en permettant une analyse des données en temps réel. Aujourd'hui des approches comme le Zero-Trust par exemple, nous ont également permis de renforcer ces barrières en réduisant la surface d'attaque grâce à une vérification continue.

Car ces mêmes technologies sont activement détournées par les cybercriminels. L'utilisation de l'IA continue de s'accélérer et prend même une tout autre dimension. Elle est exploitée pour créer des deepfakes ultra-réalistes, automatiser des campagnes de phishing à grande échelle et contourner les mesures d'authentification biométriques. Le Deepfake-as-a-Service (DfaaS) et les plateformes comme Haotian IA illustre cette menace croissante comme révélé dans le dernier rapport Threat Intelligence de TEHTRIS.

L'avènement de l'informatique quantique pourrait également compromettre les algorithmes de chiffrement actuels, nous obligeant à repenser nos stratégies de protection des données.

> QUELLES SOLUTIONS DE VOTRE ENTREPRISE OU ORGANISATION PERMETTENT DE GÉRER AU MIEUX LES CYBERMENACES INDUITES PAR LES NOUVELLES TECHNOLOGIES ? ET POUR QUELLES RAISONS ?

L'évolution constante des menaces et leur sophistication croissante accentuent **la cyber-fatigue des équipes SOC** et complexifient les environnements de sécurité. Notre priorité est donc d'apporter une **cybersécurité intégrée, intelligente et opérable,** pensée pour soulager les analystes et optimiser les déploiements.

2025 marque une véritable métamorphose pour TEHTRIS. Notre plateforme TEHTRIS XDR AI – dopée à l'IA propriétaire **CYBERIA** – a été entièrement repensée pour répondre aux nouvelles menaces, tout en mettant l'accent sur l'expérience utilisateur et l'efficacité opérationnelle.

Nos piliers d'innovation pour cette nouvelle version :

- **v14 :** une release majeure, conçue avec et pour les utilisateurs à travers nos ateliers de **co-design**
- **Deux innovations clés : un nouvel EDR et un nouvel XDR,** repensés pour offrir une détection augmentée, résiliente et intelligente
- **Un modèle de livraison en trois temps,** pour une adoption fluide
- **Implication stratégique de nos partenaires**
- **Support des environnements multi-tenants,** pour gérer en toute simplicité des contextes clients complexes (ex : MSSP, grandes organisations multi-entités)

Notre **nouveau EDR,** par exemple, est plus robuste et plus autonome. Au-delà d'une analyse multifactorielle pour une détection encore plus prédictive des menaces modernes, Il intègre des protections renforcées pour empêcher toute tentative de désinstallation ou de désactivation malveillante – une réponse directe aux nouvelles formes d'attaques ciblant les « agents cyber ».

Mais une protection complète ne s'arrête pas au poste de travail. Dans un monde **mobile-first,** où les smartphones et tablettes sont devenus des cibles privilégiées, notre solution **MTD (Mobile Threat Detection)** apporte une couche de sécurité dédiée : détection comportementale, identification de malwares, sécurisation des connexions réseau. L'objectif ? **Assurer une visibilité de bout-en-bout,** quel que soit le terminal.

Nous ne faisons pas qu'ajouter des couches technologiques : nous repensons en profondeur la façon dont elles sont **utilisées, comprises et intégrées** dans les opérations quotidiennes des SOC. C'est ça, la cybersécurité de demain : **augmentée, unifiée, et centrée sur l'humain.**

> QUELLES ÉVOLUTIONS, À COURT, MOYEN OU LONG TERME, VOYEZ-VOUS DANS CE DOMAINE DES NOUVELLES TECHNOLOGIES ?

À court terme, nous faisons face à une intensification de l'usage malveillant de l'IA. Les plateformes comme Deepfake-as-a-Service (DfaaS) permettent déjà à des acteurs peu qualifiés de lancer des campagnes sophistiquées, à grande échelle, et quasi indétectables. 2025 pourrait bien marquer un tournant : celui de l'automatisation complète du cybercrime. Phishing, spoofing vocal, bypass biométrique… tout devient industrialisable.

Nous entrons dans une guerre d'algorithmes, où les attaquants entraînent leurs IA pour déjouer nos défenses, pendant que les défenseurs doivent développer des IA plus rapides, plus fines, plus prédictives. C'est une course à l'armement numérique, qui exige des entreprises qu'elles automatisent autant leur détection que leur remédiation, sans sacrifier la lisibilité ni le contrôle humain.

À moyen terme, l'émergence de l'informatique quantique constitue une autre rupture majeure. Une fois opérationnelle à grande échelle, elle pourrait briser certains des fondements cryptographiques actuels. Les entreprises devront s'adapter très rapidement avec des approches post-quantum, dès aujourd'hui en phase de R&D active.

Enfin, à long terme, la fusion entre cybersécurité et intelligence contextuelle (géo-localisation, biométrie, IA comportementale, etc.) deviendra la norme. Il ne s'agira plus seulement de bloquer les menaces, mais d'anticiper les comportements, comprendre les contextes d'usage, et ajuster la posture de sécurité en temps réel.

L'avenir de la cybersécurité ne sera pas défensif. Il sera prédictif, éthique, et ultra-automatisé. Et ceux qui sauront conjuguer puissance technologique et responsabilité auront une longueur d'avance.

The era of perimeter protection is over; attacks are now algorithmic and autonomous.

AI has expanded the attack surface, enabling malicious AI to identify vulnerabilities, plan attacks, and evade defenses. This new era of algorithmic duels requires continuous adaptation. AI can strengthen defenses through automated threat detection and real-time data analysis. However, cybercriminals also exploit AI for deepfakes, phishing, and bypassing biometric authentication. Quantum computing may soon compromise current encryption methods. TEHTRIS's XDR AI platform, powered by proprietary AI CYBERIA, offers unified, automated threat detection and response, reducing SOC fatigue and enhancing visibility. The future of cybersecurity will be predictive, ethical, and highly automated.

TEHTRIS XDR AI PLATFORM

Une plateforme unifiée, automatisée, pilotée par notre IA propriétaire CYBERIA. Elle centralise la détection, la réponse, et la remédiation face aux menaces avancées sur l'ensemble des vecteurs : endpoints, réseaux, cloud, messageries, etc.

Objectif :
réduire la fatigue des équipes SOC tout en renforçant la visibilité et le contrôle.

- Refonte complète en 2025 (avec une version v14)
- Nouvelle ergonomie, pensée "SOC-first"
- Co-design client
- Multi-tenants : idéale pour les MSSP ou structures multi-entités

NOUVELLE GÉNÉRATION D'EDR (ENDPOINT DETECTION & RESPONSE)

Basée sur des modèles IA propriétaires renforcés et des analyses multifactorielles pour des détections encore plus rapides des menaces sophistiquées. Conçu pour résister aux attaques ciblant les agents de sécurité eux-mêmes. Empêche les désinstallations/désactivations malveillantes, tout en offrant une détection IA-augmentée, en temps réel.

MTD – MOBILE THREAT DETECTION

Solution dédiée aux appareils mobiles, devenue essentielle dans un monde "mobile-first".

- 3 niveaux de protection renforcée : OS, applications et réseaux
- Détection proactive des menaces (cyberespionnage, jailbreak/root, app/sites malveillants…)
- Sécurisation des connexions réseau
- Idéal pour les collaborateurs nomades et les environnements BYOD

NOS PRIORITÉS

- Enterprise-Grade Cyber Protection
- Réduction de la complexité opérationnelle
- Défense adaptative, assistée par IA
- Sécurité by design, à tous les niveaux de l'infrastructure

ALAIN
TER MARKOSSIAN

Director of Global solutions Engineering, TEHTRIS

LE DÉCOUPLAGE TECHNOLOGIQUE ET L'ANTICIPATION, DES CLÉS POUR LES RESPONSABLES CYBERSÉCURITÉ

Lors du Forum InCyber (FIC) 2025, Alain Ter Markossian, Director of Global Solutions Engineering, TEHTRIS, a accordé un entretien à Global Security Mag

GS MAG : *Merci de nous accorder ce temps. Pouvez-vous vous présenter et nous dire comment votre parcours vous a amené à votre rôle actuel ?*

ATM : J'ai 48 ans. J 'ai un parcours assez atypique et original lié au fait que je suis diplômé de géopolitique et relations internationales. J'ai ensuite intégré le Conseil Régional Provençal Côte d 'Azur où j'ai commencé l'Informatique au sens pur en faisant des systèmes d'informations géographiques, du mapping et de la cartographie numérique. C'est donc ainsi que j'ai fait mes premiers pas en tant qu'Informaticien. J'ai converti cela dans un diplôme d'Ingénieur et je me suis lancé dans un parcours plus orienté vers des éditeurs de logiciels. Cela correspondait à une volonté de ma part car c'était les années 2000 et l'essor de l'ensemble de l'édition avec l'arrivée d'Internet et du SaaS (Software as a Service). Mon parcours a commencé chez un éditeur français, Axway, où je me suis occupé au départ de ce qu'on appelait à l'époque des Technico-Commerciaux, qui sont ensuite devenus des Avant-Ventes, des Solutions Engineers.

>>>

>>> Il s'agit de toutes ces personnes qui ont à la fois une casquette technique pour pouvoir évangéliser ou vulgariser les problématiques techniques, et un sens commercial pour pouvoir aider les Commerciaux dans leurs démarches et parcours de Vente. Je suis resté très longtemps chez cet éditeur français dans le monde de la protection des transferts de données qui s'est ensuite spécialisé dans les API (Application Programming Interface ou Interface de programmation d'Application), la gestion des API, qui a révolutionné aussi notre monde. J'ai ensuite travaillé chez un Cloud Provider français, européen, OVHcloud. Et après cette expérience également dans l'Avant-Vente, j'ai dirigé une équipe d'Avant-Ventes chez un éditeur américain sur la Data Privacy, Data Governance, et GRC, OneTrust concernant tout le marché français et celui de l'Europe. Je suis arrivé chez TEHTRIS il y a environ deux ans, dans le but de monter et d'intégrer une équipe d'Avant-Vente internationale située dans différents pôles géographiques, à la fois l'Europe, l'Asie, et aussi le Moyen -Orient qui contient des leviers de croissance pour tous les acteurs européens de la Cyber.

J'ai tendance à souvent le répéter, mais je trouve que l'Avant-Vente est le plus beau métier dans l'édition du logiciel, puisqu'effectivement, on suit les évolutions technologiques en s'efforçant de montrer leurs valeurs et en les amenant aux clients.

GS MAG : *Pouvez-vous nous parler de TEHTRIS, et nous dire comment votre Organisation répond aux enjeux des nouvelles Technologies (IA, QUANTIQUE, SASE, SOAR, XDR, ZERO TRUST...) et de la Cybersécurité ? Qu'est-ce qui fait que TEHTRIS est unique ?*

ATM : TEHTRIS est un éditeur de logiciels français qui est sur le marché de la Cybersécurité depuis 15 ans, et c'est le premier éditeur français à avoir proposé une solution XDR (Extended Detection and Response ou Détections et Réponses étendues sur les menaces pour le poste de travail), c'est-à-dire une plateforme unifiée qui regroupe un arsenal de solutions de défense cyber et de gestion des incidents cyber. Donc à la fois un EDR (Endpoint Detection and Response ou Détections et Réponses sur les menaces pour le poste de travail) pour protéger les postes de travail et les serveurs, et également une protection des téléphones mobiles puisque nous attachons une importance forte sur le Cyberespionnage et le Cybersabotage, ce qui est une clé pour comprendre le côté unique de TEHTRIS dans ce monde de la protection cyber. Il s'agit là de notre spécialisation et notre ADN. En tant qu'éditeur européen d'offres de plateformes, nous avons différents modules qui vont se combiner pour apporter une optimisation face à la menace cyber. Nous utilisons l'IA pour orchestrer et automatiser. Effectivement, l'IA prend de plus en plus de place dans notre monde, que cela soit dans la Cyber ou dans l'IT (Information Technologies ou Technologies de l'Information) de façon générale, et les utilisations en sont plus que diverses. Chez TEHTRIS, nous avons développé notre propre IA qui va permettre d 'automatiser un ensemble de remédiations face à la menace cyber, et qui va aussi apprendre à partir du comportement dans son utilisation, c'est-à-dire qu'à partir de signaux faibles, on va pouvoir effectivement en tirer quelques menaces potentielles.

Et pour compléter cet arsenal, nous proposons aussi un SIEM (Security Information and Event Management ou Système de gestion des Informations et des Évènements de Sécurité) qui va permettre d 'avoir une approche tactique de l'ensemble de ces évènements, couplée avec l'IA.
Un autre point important à mentionner, est que nous avons aussi notre propre CTI (Cyber Threat Intelligence) qui permet d'avoir un état à un moment donné, et surtout le plus à jour de la menace cyber à travers le monde puisque nous avons le plus vaste réseau de honeypots (pots de miel ou pièges numériques), de faux serveurs déployés pour pouvoir attirer les attaquants et les identifier et bien évidemment proposer à nos clients, comme je le disais, l'état de l 'art de cette protection nécessaire le plus à jour possible. Tout cela permet d'anticiper la menace.

Le monde de la Cyber est en pleine mutation, beaucoup de choses ont été dites, on a aussi un contexte

Effectivement, l'IA prend de plus en plus de place dans notre monde, que cela soit dans la Cyber ou dans l'IT (Information Technologies ou Technologies de l'Information) de façon générale, et les utilisations en sont plus que diverses.

géopolitique qui est très changeant, avec différents points clés. Nous sommes dans l'attente de voir quelle stabilité, quel nouvel ordre cyber on aura, et je crois que tous les éditeurs devraient proposer à l'ensemble des Responsables Cyber, des outils d'anticipation, des outils de protection contre les vulnérabilités non identifiées. Donc pour ne pas se faire surprendre, il est nécessaire d'anticiper et se préparer au pire dans le monde de la Cyber.

Et je pense, tout en espérant le retour de la paix, que l'une des choses qui va se passer, que certaines personnes vont se retrouver dans une forme de cyber mercenariat et vont proposer leurs services pour exploiter faire des vulnérabilités Zéro-Day (non connues) via certains outils et peut-être apporter des menaces qui peuvent être mortelles, que cela soit pour des Entreprises et Organisations, ou bien pour des états qui peuvent se retrouver paralysés.

Donc les Responsables Cyber doivent se préparer à de tels scénarios d'anticipation critique par rapport à leurs parcs de solutions déployées. Et la prise en compte d'une certaine forme de Souveraineté Numérique en diversifiant les solutions adoptées, serait importante dans ce contexte géopolitique, et il semble nécessaire de se détacher de la dépendance technologique. Aller vers un découplage technologique me semble être une stratégie qui peut se révéler efficace.

GS MAG : *Il y a une loi française qui en cours d'élaboration pour transposer les Directives européennes, NIS 2 (Network and Information Systems ou Systèmes d'Information et Réseaux), CRA (Cyber Resilience Act ou Loi sur la Cyber-Résilience), DORA (Digital Operational Resilience Act ou Loi sur la Résilience opérationnelle numérique). Comment les solutions de TEHTRIS peuvent-elles aider à la fois à la Conformité et à la Cybersécurité ?*

ATM : C'est à la fois une chance et parfois un andicap en Europe, que de beaucoup légiférer. Les Anglo-Saxons légifèrent en général à posteriori, et les Européens légifèrent en général avant la menace. Mais je pense qu'il y a une chose qui est très importante, c'est que tout éditeur, notamment français ou européen et de plus en plus français devrait, dans ses solutions, intégrer la sécurité by design (dès la conception), comme cela est prescrit dans ces législations, et intégrer la Cybersécurité par design également, c'est-à-dire revoir les processus, en étant encore encore plus rigoureux dans l'ensemble de ces processus, sans aller au détriment de l'innovation ou vers son ralentissement. C'est une chose très difficile à manager pour les équipes d'Engineering, de pouvoir en même temps maintenir un rythme de sortie d'innovations et de fonctionnalités. C'est un vrai défi pour l 'ensemble des acteurs qui cherchent à rendre possible la Souveraineté numérique.

TEHTRIS est un éditeur de logiciels français qui est sur le marché de la Cybersécurité depuis 15 ans, et c'est le premier éditeur français à avoir proposé une solution XDR

En effet, en face, il y a une force de frappe toujours prête à se lever, un bouclier qui va sans cesse innover, aussi pour essayer de retarder et de lâcher le plus possible la concurrence. Et c'est là que les Européens doivent faire preuve également de tout leur savoir-faire d 'Ingénierie, c'est-à-dire innover tout en restant toujours dans le cadre de la Conformité et apporter de la valeur, car avec cela et en répondant aux besoins, c'est ce qui est primordial et qui fait la différence in fine entre un éditeur donné et un autre éditeur. Apporter de la valeur et répondre à un besoin qu'on aura peut-être identifié un peu en avance sera la clé du succès.

GS MAG : *Quels seraient vos messages clés à nos lectrices et lecteurs qui sont en général des RSSI, CISO, DSI, CIO, Responsables de la Cyber et de la Cybersécurité.*

ATM : Il me semble très important de faire un découplage technologique. Le bon adage populaire qui conseille de ne pas mettre tous ses œufs dans le même panier, semble à l'heure actuelle de plus en plus fonctionner, et sera peut-être une des clés. Puisqu'effectivement nous sommes dans une forme d'incertitudes dans le monde, anticiper et diversifier les technologies, en ayant différentes couches d'arsenal de protection, me semble être la bonne stratégie pour la Cybersécurité des Entreprises et Organisations. ■

DAVID CHASSAN

Directeur de la Stratégie, 3DS OUTSCALE, Dassault Systèmes

OUTSCALE, AVEC SA NOUVELLE OFFRE OKS, EST LE PARTENAIRE DE VOTRE TRANSFORMATION NUMÉRIQUE, AVEC LES PLUS HAUTS STANDARDS EN CYBERSÉCURITÉ.

Le lancement de la nouvelle offre OKS (OUTSCALE Kubernetes as a Service), a été l'occasion pour David Chassan d'accorder un entretien à Global Security Mag

GS MAG : *merci de nous accorder ce temps. Pouvez-vous vous présenter et nous dire comment votre parcours vous a amené à votre rôle actuel ?*

DC : Merci pour cet échange. Je suis David Chassan, Directeur de la Stratégie chez OUTSCALE, qui est une marque de Dassault Systèmes. J'ai un parcours qui a toujours été dans l'IT (Information Technology ou Technologies de l'Information, et j'ai démarré ma carrière professionnelle à l'issue d'une école de commerce, chez Sage. Puis j'ai évolué après dans les télécoms, et enfin chez OUTSCALE dès sa création un peu après 2010 en tant que Spin -off de Dassault Systèmes, pour en être son Cloud.

Nous fournissons des solutions de jumeaux virtuels aux Organisations, précisément dans la banque et la finance, le Heath care ou domaine de la Santé, et le domaine du secteur public.

GS MAG : *Pouvez-vous nous parler d'OUTSCALE et de sa nouvelle offre OKS ? Quel est le contexte et quels sont les enjeux notamment par rapport à la Souveraineté ou au Cloud de Confiance, et à la Cybersécurité ? Qu'est ce qui fait que cette offre OKS est unique par rapport à d'autres offres comme GKE (Google Kubernetes Engine), AKS (Azure Kubernetes Service), EKS (Amazon Elastic Kubernetes Service) ?*

DC : OUTSCALE en tant que marque de Dassault Systèmes, est d'abord le Cloud de l'ensemble des plateformes de Dassault Systèmes, principalement la 3D Experience Platform. C'est un ensemble qui rassemble de nombreux clients, dont Dassault Systèmes qui représente un peu plus de 350 000 clients à travers le monde, 45 millions d'utilisateurs.

Nous sommes l'opérateur Cloud de Dassault Systèmes, mais pas seulement, puisqu'on adresse également des clients en dehors de Dassault Systèmes, et principalement des institutions, des grandes entreprises et des entreprises aussi plus modestes. Et enfin, plus récemment, depuis deux ans, nous fournissons des solutions de jumeaux virtuels des Organisations, précisément dans la banque et la finance, le Heath care ou domaine de la Santé, et le domaine du secteur public.

Lorsque OUTSCALE est née pour être à la fois la plate-forme de Cloud et l'opérateur Cloud de Dassault Systèmes, Nous avons eu pour intention de protéger les données et la propriété intellectuelle de nos clients. Et c'est donc un asset extrêmement fort sur lequel OUTSCALE est née, et globalement, au sein de Dassault Systèmes, Il s'agit aussi de servir la Nation, de servir l'Europe. Et à travers cet ADN qui nous anime depuis le début, nous avons aujourd'hui un contexte où le Président des Etats-Unis, Donald Trump, a sonné à nouveau « un wake-up call » ou appel à se réveiller auprès de tout le monde, que cela soit les citoyens, les entreprises, les Institutions. On s'aperçoit que dans le monde de la Défense, Il paraît une évidence, et l'actualité récente va en ce sens, que la Souveraineté est essentielle. Elle anime toutes les industries, toutes les activités, et finalement, la Souveraineté est à la fois de choisir ses dépendances, mais aussi d'avoir toute la transparence nécessaire auprès des clients que l'on sert. C'est là où on adresse tout le concept de Cloud de Confiance.
Pour autant, globalement, dans toutes les Entreprises, on s'aperçoit qu'il y a un aspect de Multi-Cloud qui est opéré. Pour des données qui ne sont pas sensibles, des applications qui ne sont pas sensibles, je peux choisir mes Clouds de commodité, qu'ils soient français, européens ou américains ou chinois. En revanche, quand il s'agit de données sensibles, protéger les data et la propriété intellectuelle, le Cloud Souverain est essentiel. Il n'y a pas de débat, en fait. Donc, dans cette démarche, et dans la suite de ce qu'on avait amené en octobre dernier avec LLM as a service dans le cadre d'un partenariat industriel avec Mistral AI, nous avons fait l'acquisition d'une société qui s 'appelle Satelliz, il y a tout juste un an, et qui a l'expertise Kubernetes.

En ayant ces équipes, nous lançons OUTSCALE Kubernetes as a Service (OKS), qui est une plateforme managée, sécurisée et souveraine. Et c'est ce en quoi cette offre est vraiment unique aujourd'hui sur le marché. C'est-à-dire qu'OKS est un cluster qui est dédié par client.

Un cluster rassemble le Control Plane de Kubernetes, ses Workload Nodes et ses Conteneurs. Ce cluster est déployé et dédié par client. Il est entièrement cloisonné. Il y a une réelle étanchéité et il est déployé sur le Cloud SecNumCloud. Ainsi, en quelques minutes, un client peut disposer de son cluster Kubernetes et l'opérer comme il le souhaite. C'est en cela que c'est intéressant pour un client d'allier à la fois la Sécurité et la Souveraineté de ce service Kubernetes, et aussi de disposer de l'agilité et de l'élasticité du Cloud Public qui est lui-même qualifié SecNumCloud. De ce point de vue, c'est très intéressant, de façon qu'un client, en revenant dans le cadre que je vous donnais tout à l 'heure, du Multi-Cloud, peut opérer en étant sur le standard d'usage Kubernetes, déployer à la fois de la commodité et de la Souveraineté, puisque c'est un standard parfaitement Open Source.

>>>

>>> Si on compare avec d'offres, il est vrai qu'on va retrouver le K dans l'ensemble des offres des spécialistes Kubernetes. Il est essentiel de préserver ce K, car c'est le standard qui est intégré dans notre offre OKS. Là où OKS est unique, c'est que contrairement à toutes les offres qu'on peut retrouver sur le marché, il n'y a pas de mutualisation au sein du Cluster, le Control Plane est vraiment dédié au client et déployé de façon étanche pour chacun des clients et ce point est essentiel car c'est un déploiement qui est dédié sur un Cloud SecNumCloud. Le Cloud OUTSCALE est qualifié 3.2 dans sa dernière version qui apporte ainsi des différenciations essentielles par rapport à l'ancienne version sur laquelle nous étions aussi qualifiés. On retrouve le plus haut niveau de Cybersécurité imposé par l'ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information).

Cette qualification est extrêmement exigeante et c'est la raison pour laquelle, ce Graal est difficile à obtenir par rapport à un ensemble de Cloud Opérateurs, car il faut répondre à ces exigences de Cybersécurité et aussi, à une nouvelle exigence dans la version 3.2, qui est l'immunité à des lois extraterritoriales. Un autre dernier élément qui est intéressant cette version 3.2, c'est le principe de composition. C'est-à-dire que nous-mêmes, en tant qu'Opérateur Cloud, nous adressons aussi des clients qui sont des éditeurs de logiciels, qui peuvent, eux aussi, avoir cette démarche de qualification SecNumCloud sur la partie éditeur de logiciels, tout en s'appuyant sur notre Cloud qui est déjà qualifié 3.2. Alors, dans ce principe de composition, l'ANSSI propose de considérer le Cloud qui est déjà 3.2 dans la qualification d'un logiciel SaaS et de qualifier ensuite la couche supérieure à adresser. Voilà donc des éléments essentiels qui différencient des autres offres Kubernetes qu'on peut retrouver sur le marché.

GS MAG : *Sachant que la loi de transposition sur la Cyber-Résilience est en discussion en ce moment, et comprend Dora, CRA, et NIS 2. Comment OUTSCALE peut aider ses clients, ses partenaires, à la fois pour la Conformité et la Cybersécurité par rapport aux exigences ?*

DC : Effectivement il y a tout cet ensemble de Réglementation et de Directives, ainsi que la loi SREN (Sécurisation de l'Espace Numérique) également qui va être déclinée sous forme de différents décrets de mises en application. Ce qui, à mon sens, est important et qui nous a toujours animés, c'est d'être en totale transparence et dans les règles de l'art vis-à-vis de nos clients. Nous adressons des clients qui ont une sensibilité sur la Cybersécurité, sur la responsabilité d'être un Opérateur de Services Cloud. Et à travers notre relation commerciale avec nos clients, nous sommes à livre ouvert avec eux, avec des contrats qui expliquent les différentes responsabilités. Souvent, la Cybersécurité est une responsabilité qui est quelque part partagée. Nous avons une responsabilité sur les couches basses des niveaux de service et le client apporte sa responsabilité sur sa propre gestion du service qu'il opère. Ce partage de responsabilités est extrêmement clair. Cela nous permet d'avoir cette relation de confiance dans cette transparence qui nous permet d'opérer des clients qui ont des activités extrêmement sensibles, qui sont considérées dans ces nouvelles réglementations, et de façon qu'il puisse y avoir cette transparence mutuelle qui est essentielle. L'autre partie aussi importante à mon sens, c'est qu'au niveau d'OUTSCALE, tous les services que nous opérons incluent le support 24-7 qui n'est pas une option, mais est intégré à nos tarifs. Et pourtant, nos prix de vente sont alignés avec ceux d'AWS.

En conclusion, faire un choix souverain chez OUTSCALE ne coûte pas plus cher que d'aller chez le leader mondial. Cet alignement nous permet d'avoir l'industrialisation. Nous sommes Dassault Systèmes, le côté industriel de ce que nous mettons en œuvre nous caractérise toujours. Et ce Support 24 -7 est « follow the Sun » c'est-à-dire qu'il suit la course du soleil.

GS MAG : *Quels seraient vos messages clés à nos lectrices et lecteurs ?*

DC : Le message clé est que OUTSCALE est le partenaire pour votre transformation numérique dans un acte de pérennité, d'excellence, et de sérénité, puisque nous avons les plus hauts standards de Cybersécurité, avec notamment la qualification SecNumCloud de l'ANSSI, mais également dans le design même de nos services, typiquement avec OKS, qui est déployé de façon managée, sécurisée et souveraine, et dans l'excellence, puisque c'est notre ADN, en tant que Dassault Systèmes, de proposer des services qui sont toujours à l 'état de l'art et parfaitement opérationnels. ■

LA SOUVERAINETÉ AU COEUR DE NOTRE ADN

LLMaaS

Mistral AI

OUTSCALE KUBERNETES AS A SERVICE

Cloud Public SecNumCloud 3.2

VISA DE SÉCURITÉ ANSSI

outscale.com

OUTSCALE

NICOLAS
LIARD

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

LE SOC AUGMENTÉ :
QUAND L'IA DEVIENT LE NERF DE LA RÉSILIENCE CYBER

Alors que les cybermenaces prennent la forme d'entités furtives, adaptatives et parfois propulsées par l'intelligence artificielle elle-même, les centres opérationnels de sécurité (SOC) font face à un défi structurel : évoluer vers un modèle plus intelligent ou sombrer dans l'inefficacité. Les SOC ne peuvent plus se contenter d'une détection réactive, d'une surveillance linéaire ou d'une centralisation technique désincarnée.

Il leur faut embrasser une approche systémique et adaptative, où l'intelligence artificielle devient un levier d'anticipation, de contextualisation et de gouvernance.

L'émergence du SOC augmenté marque ainsi un tournant dans la stratégie cyber des organisations. Plus qu'une mise à jour technique, il s'agit d'une métamorphose conceptuelle et opérationnelle.

SOC CLASSIQUE : LES LIMITES D'UNE DÉFENSE FIGÉE

Durant près de deux décennies, le SOC s'est imposé comme une forteresse centralisée, reposant sur des SIEM, des corrélations statiques, et des analystes opérant dans l'urgence. Pourtant, dans un monde où les volumes de logs explosent, où les environnements deviennent hybrides et où les cybercriminels exploitent l'IA pour se camoufler ou automatiser leurs attaques, ce modèle se montre dépassé.

■ LES SOC TRADITIONNELS SOUFFRENT DE TROIS CARENCES MAJEURES :

- Une surcharge informationnelle : l'avalanche de données rend l'analyse humaine inefficace.
- Un déficit contextuel : les signaux faibles passent inaperçus, noyés dans des alertes techniques décontextualisées.
- Un déficit de réactivité : les analystes sont englués dans des workflows répétitifs et manuels.

Dans ce paysage fragmenté, où les cyberattaques opèrent en essaims, en flux continus ou en tâches furtives, la vigilance humaine seule ne suffit plus. Le SOC classique devient un poste d'observation à la fois saturé et aveugle.

DU SIEM PASSIF AU SIEM INTELLIGENT : UNE ÉVOLUTION NÉCESSAIRE

Historiquement conçu pour collecter, centraliser et corréler des logs, le SIEM a longtemps été présenté comme la tour de contrôle du SOC. Mais cette promesse s'est diluée dans des réalités techniques complexes, entre faux positifs, difficultés d'investigation et lourdeur des règles statiques.

La transformation du SIEM s'impose comme une condition sine qua non du SOC augmenté.

■ LES NOUVEAUX PARADIGMES S'IMPOSENT :

- Analyse comportementale (UEBA) : détection des anomlies à partir de modèles d'usage avec une pondérance forte pour les événements les plus rares, même en l'absence d'Indicateur de compromissions.
- Orchestration automatisée (SOAR) : réponse adaptative, documentation dynamique, intégration à des playbooks contextuels.
- Priorisation orientée risque : intégration des données métier, de la criticité des actifs et des intentions adverses.

En devenant proactif, contextualisé, et décisionnel, le SIEM moderne cesse d'être un simple agrégateur de logs : il devient le cerveau opérationnel du SOC, articulé avec les autres composantes de sécurité.

>>> LE SOC COMME TOUR DE CONTRÔLE : DE LA SUPERVISION À L'ORCHESTRATION

Le SOC augmenté s'affirme comme une tour de contrôle interconnectée, capable de lire l'environnement numérique dans sa globalité. Là où l'ancien SOC voyait des alertes isolées, le SOC augmenté détecte des chaînes d'attaque, contextualise les signaux faibles, et enclenche des réponses proactives.

■ CETTE NOUVELLE POSTURE REPOSE SUR TROIS PILIERS :

1_ L'interopérabilité des outils : XDR, DLP, IAM, SASE ne sont plus des silos mais des acteurs synchronisés.

2_ La convergence IT/business : les signaux techniques sont enrichis par les données RH, CRM, CMDB

3_ L'automatisation intelligente : les réponses sont déclenchées de manière contextuelle, selon des modèles d'intention malveillante.

Le SOC cesse d'être un centre d'alerte pour devenir un centre de décision, stratégique, adaptatif et résilient.

L'IA AGENTIQUE : UNE NOUVELLE FAÇON DE PENSER LA CYBERDÉFENSE

L'introduction de l'IA agentique (Agentic AI) dans le SOC change radicalement la donne. Contrairement à l'IA conventionnelle, centrée sur la détection ou la corrélation, l'IA agentique opère en autonomie, dans un cadre contextuel, avec des objectifs métier alignés.

■ LES AGENTS INTELLIGENTS S'INCARNENT SOUS PLUSIEURS FORMES :

- Agent de surveillance comportementale : modélise les habitudes et détecte les écarts subtils.
- Agent de triage : priorise et enrichit les alertes selon des critères métiers.
- Agent de remédiation : exécute des actions adaptées à la criticité du contexte.
- Agent de simulation (purple teaming) : teste la résilience des défenses.
- Agent conversationnel : facilite l'investigation via le langage naturel.

En systématisant l'usage de ces entités autonomes, le SOC gagne en agilité, en rapidité et en compréhension située.

Le SOC augmenté est plus qu'un bouclier. Il devient une boussole dans un cyberespace déroutant.

MENACE INTERNE : L'ÉPREUVE DU FEU POUR LE SOC AUGMENTÉ

Le cas de la menace interne illustre parfaitement les apports du SOC augmenté. Trop souvent ignorée ou détectée trop tard, elle exige une détection comportementale, une corrélation contextuelle et une réaction adaptative.

■ **SCÉNARIO : UN EMPLOYÉ DU SERVICE R&D, SUR LE DÉPART, TENTE DE SUBTILISER DES DONNÉES STRATÉGIQUES.**

- Le SOC traditionnel ne détecte rien : les accès sont légitimes, les actions fragmentées.
- Le SOC augmenté corrèle préavis RH, accès anormaux, transferts suspects.
- Un agent alerte l'analyste avec un résumé clair : risque de fuite imminent.
- La réponse est enclenchée en quelques minutes : restriction d'accès, surveillance, notification RH.

Le SOC devient alors un organe immunitaire, capable d'identifier, d'interpréter et de neutraliser une menace avant qu'elle n'impacte l'organisation.

L'IA COMME SURFACE D'ATTAQUE : MAÎTRISER L'ADVERSAIRE INTÉRIEUR

L'IA, si elle est un atout pour le SOC, peut aussi devenir sa faille. Deepfakes, phishing vocal, injections de prompts, empoisonnement de modèles : le SOC doit protéger ses propres briques d'IA.

■ **LES CONTRE-MESURES S'IMPOSENT :**

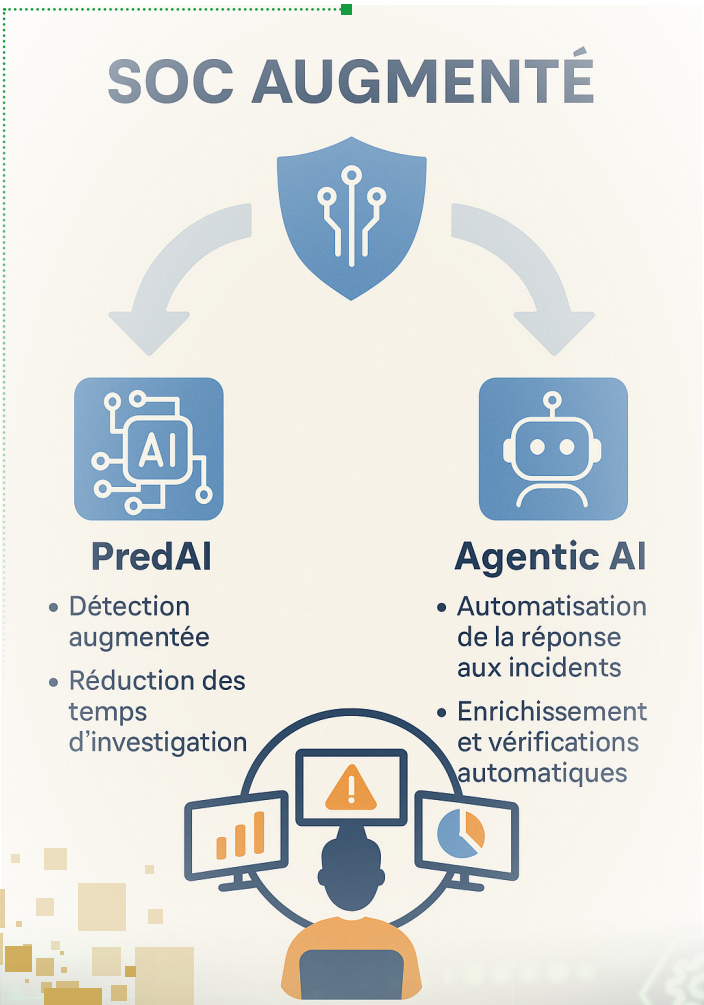
- Audit continu des modèles
- Isolation des environnements d'inference
- Chiffrement des modèles et des prompts
- Supervision humaine avec explication des décisions algorithmiques

C'est en s'armant contre les dérives de l'IA que le SOC augmenté pourra construire une résilience durable.

VERS UN CYBERESPACE MAÎTRISÉ

Le SOC augmenté n'est pas un simple centre d'alerte dopé à l'IA. Il est la manifestation d'une gouvernance cybernétique consciente. Il orchestre des agents intelligents, contextualise les signaux techniques, intègre les données métiers et positionne l'analyste comme stratège, non comme simple opérateur. Il ne s'agit plus de réagir, mais d'anticiper. Il ne s'agit plus de surveiller, mais de comprendre. Il ne s'agit plus de protéger, mais de gouverner.

"Le SOC augmenté est plus qu'un bouclier. Il devient une boussole dans un cyberespace déroutant." ■



MARINE DU MESNIL & PAUL MOLIN

Head of Cybersecurity Tribe, Theodo

Group CISO, Theodo

LIVRE CYBER : *IL ETAIT UNE FAILLE* Histoires marquantes de cybersécurité pour frissonner et s'en protéger

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

MD/PM : Tout a commencé avec une newsletter interne chez Theodo. Nous voulions sensibiliser les développeurs à la cybersécurité grâce à des récits d'attaques réelles.
Les retours ont tout de suite été très positifs. Des développeurs nous ont par exemple raconté qu'ils venaient de corriger une faille dans leur application juste après avoir lu une de nos histoires. Grâce à cette approche narrative, les failles sont devenues plus compréhensibles, car illustrées par des exemples concrets.

C'est ainsi qu'est née l'idée d'Il était une faille.
Le livre reprend et enrichit une partie de nos meilleures histoires. À chaque fois, nous expliquons comment certaines erreurs ont conduit à des incidents majeurs et, surtout, les bonnes pratiques pour les éviter. Cela permet de donner aux équipes des clefs concrètes pour repérer et corriger les vulnérabilités avant qu'elles ne soient exploitées. Nous avons voulu aider les développeurs à se créer des modèles mentaux et à savoir reconnaître les situations dangereuses.

Nous nous sommes basés sur les standards du marché pour choisir les histoires les plus pertinentes. C'est pour cela que chacun des premiers chapitres reprend une des catégories du top 10 de l'OWASP.
Les derniers chapitres abordent des points clefs qui ne sont pas présents dans cette catégorisation.

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

MD/PM : D'abord, c'est un outil de formation concret à mettre entre les mains de leurs équipes : il permet de faire monter en compétence sur la sécurité applicative, de manière claire et stimulante. Ensuite, il montre que raconter des histoires, ça fonctionne. Parce que ça donne des exemples concrets, faciles à retenir, et que ça crée des émotions chez le lecteur — ce qui rend l'apprentissage beaucoup plus efficace. Il peut ainsi se reconnaître dans les situations décrites et se poser les bonnes questions. Enfin, c'est une première base d'histoires à réutiliser : en réunion, en formation interne, ou même pour animer une présentation. Et le gain peut alors dépasser les simples objectifs de formation, en faisant passer des messages clefs qui permettent de mieux prioriser les sujets de sécurité.

GS MAG : *Quels sont vos messages pour nos lectrices et lecteurs ?*

PM : Si on veut bien se protéger, il faut commencer par comprendre comment les attaquants s'y prennent. C'est pour ça qu'on croit autant aux histoires : elles montrent que les failles, ce ne sont pas des concepts abstraits — ce sont des choses qui arrivent, dans la vraie vie, à des vraies équipes.

Aux développeurs, on a envie de dire : vous avez un vrai rôle à jouer. Vous êtes celles et ceux qui connaissent le mieux le fonctionnement du produit, ses subtilités, ses zones grises. Nous recommandons aux RSSI et aux experts sécu de demander aux développeurs comment ils attaqueraient leur application. De notre côté, nous avons parfois des réponses surprenantes, et souvent très ingénieuses. Pour que ça fonctionne, il faut cependant que les développeurs soient formés. Racontez-leur des histoires, aidez-les à se construire des modèles mentaux.

Enfin, il est facile d'introduire des vulnérabilités partout, dans chaque brique d'un système. Un seul individu ne peut pas tout maîtriser. Mais si chacun sécurise ce qu'il construit, si chaque membre de l'équipe est un peu plus alerte, alors on réduit massivement les risques.

Nous espérons que ce livre aidera nos lecteurs à voir la cybersécurité sous un nouvel angle, plus accessible et engageant. Nous écrivons toujours des newsletters qui sortent toutes les trois semaines, il est possible de les recevoir en s'inscrivant sur le site de Theodo. ■

HS2
Hervé Schauer Sécurité

Formation cybersécurité technique

DÉTECTION ET RÉPONSE • INFORENSIQUE • SÉCURITÉ OFFENSIVE

PROGRAMME

Détection et réponse aux incidents

OSINT
Formation OSINT
SECUBLUE1
Surveillance, détection et réponse aux incidents de sécurité
SECUBLUE2
Surveillance, détection et réponse avancée aux incidents de sécurité
SECUSOC
Surveillance, analyse et corrélation
SPLUNK
Formation SPLUNK
ISO27035
Formation Gestion des incidents de sécurité

Inforensique

FORENSIC1
Analyse inforensique Windows
FORENSIC2
Analyse Inforensique avancée
REVERSE1
Rétroingénierie de logiciels malfaisants
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

www.hs2.fr

formation@hs2.fr

MOUNTAHA NDIAYE

EMEA Director Ecosystem Sales and Programs Hyland

SELON VOUS, L'IA

IA EST L'ARBRE QUI CACHE LA FORÊT DE LA QUATRIÈME RÉVOLUTION INDUSTRIELLE

L'intelligence artificielle (IA) est sans doute l'innovation technologique qui suscite le plus de débats et de projections aujourd'hui. Selon Nick Bostrom, philosophe et futurologue suédois, l'IA atteindra bientôt un niveau d'intelligence surpassant celui des humains, ce qui pourrait transformer radicalement notre civilisation. Ce concept, appelé singularité, pose une question cruciale : l'IA va-t-elle rendre le travail humain obsolète ?

Face à une inquiétude croissante chez les travailleurs - en 2022, 60 % des Français redoutaient l'impact de l'IA et de l'automatisation sur leur emploi - il est essentiel d'aborder ce sujet de manière pragmatique. Plutôt que de redouter un futur dystopique, analysons comment l'IA transforme les modèles économiques, le marché du travail et la création de valeur.

UNE RÉVOLUTION INÉVITABLE

L'histoire économique est marquée par des ruptures technologiques majeures :

1. **Révolution industrielle 1.0 (fin XVIII^e siècle) :** la machine à vapeur et les chemins de fer bouleversent l'industrie et les transports.
2. **Révolution industrielle 2.0 (fin XIX^e siècle) :** l'électricité, le moteur à combustion et les télécommunications accélèrent la production et la connectivité.
3. **Révolution industrielle 3.0 (années 1960) :** l'ère du numérique transforme la gestion de l'information et l'automatisation des processus.
4. **Aujourd'hui, la Révolution industrielle 4.0 s'articule autour de l'IA,** de la robotique avancée et de l'automatisation intelligente.

Mais cette fois, la rupture est différente. Contrairement aux précédentes révolutions, qui nécessitaient encore un rôle clé de l'humain, l'IA progresse vers une autonomie croissante.

Les agents autonomes et les intelligences génératives commencent déjà à se substituer à l'humain dans des domaines complexes, et cette tendance est irréversible.

Ce n'est pas une simple transition technologique, c'est une refonte totale de la place de l'être humain dans l'économie et la société.

L'IA DÉPASSE DÉJÀ L'HUMAIN : CAS D'USAGE CONCRETS

Loin d'être une simple assistance, l'IA surpasse déjà l'humain dans plusieurs secteurs, signant le début d'une ère où l'automatisation remplace progressivement le travail humain :

- **Médecine :** Les IA de diagnostic comme celles développées par DeepMind ou IBM Watson détectent des cancers avec une précision supérieure aux radiologues humains.
- **Finance :** Les algorithmes d'IA anticipent les tendances des marchés et gèrent des portefeuilles avec une rapidité et une efficacité inégalées, rendant obsolètes certaines fonctions analytiques humaines.
- **Secteur public :** L'IA optimise la gestion des infrastructures, prédit les besoins en services publics et automatise les tâches administratives complexes, remplaçant progressivement les agents administratifs.
- **Énergie :** Des IA comme celles utilisées par Google DeepMind réduisent la consommation énergétique des data centers de 40 %, surpassant les ingénieurs humains en optimisation.

>>>

>>> • **Transport :** Tesla et Waymo développent des véhicules autonomes capables de réagir plus vite qu'un conducteur humain en situation d'urgence.

- **Commerce :** Les plateformes d'e-commerce utilisent des IA pour personnaliser l'expérience utilisateur, anticiper la demande et optimiser les stocks, réduisant le besoin en personnel de gestion.
- **Éducation :** Des assistants virtuels et des plateformes adaptatives comme Coursera et Duolingo ajustent les parcours d'apprentissage en fonction du niveau et du rythme des étudiants.
- **Pharmacie :** L'IA accélère la découverte de nouveaux médicaments, comme l'a démontré AlphaFold en prédisant la structure des protéines avec une précision inédite, supplantant les chercheurs humains dans certaines tâches de R&D.

UN CHANGEMENT GÉOPOLITIQUE ET SOCIAL MAJEUR

L'émergence des agents autonomes ne bouleverse pas seulement le monde du travail, elle redéfinit également les dynamiques géopolitiques et sociales :

- **Un accès universel au savoir :** Avec l'IA capable de traiter et d'expliquer instantanément n'importe quelle information, l'accès à la connaissance sera démocratisé. Les pays en développement pourront rivaliser avec les grandes puissances en matière d'expertise et d'innovation.
- **La crise des cols blancs :** Les métiers intellectuels sont désormais en première ligne. La montée en puissance des agents autonomes annonce la disparition progressive des experts, des analystes et des professions de conseil.
- **La fin des cabinets de conseil :** Jusqu'ici indispensables aux grandes entreprises et aux gouvernements, ces structures seront rendues obsolètes par des IA capables d'analyser, de prédire et de recommander des stratégies plus efficacement que n'importe quel consultant humain.
- **Une redéfinition des interactions sociales :** Avec la généralisation des agents autonomes et des intelligences sociales, chacun pourra créer son propre avatar IA pour interagir dans des mondes virtuels ou physiques, modifiant radicalement notre manière de communiquer et de collaborer.
- **Les pays riches en matières premières en position de force :** Les ressources naturelles essentielles aux infrastructures IA (puces électroniques, data centers, électricité) deviendront stratégiques. Les nations possédant ces matières premières auront un avantage décisif dans la course à la domination technologique.

LA FIN DU TRAVAIL TEL QUE NOUS LE CONNAISSONS

L'un des débats majeurs autour de l'IA concerne son effet sur l'emploi. Mais au-delà des inquiétudes classiques sur l'automatisation, il faut comprendre que nous entrons dans une phase où des agents autonomes IA, capables de prendre des décisions complexes et de s'adapter en temps réel, vont remplacer une partie croissante des travailleurs humains.

Une étude de McKinsey estime que 14 % des emplois actuels sont hautement automatisables et que 5 % pourraient disparaître d'ici 2030. Mais cette estimation pourrait s'avérer conservatrice face aux progrès fulgurants de l'IA générative et des modèles autonomes. Des métiers entiers, notamment dans les services, la gestion de l'information et la logistique, sont menacés d'une automatisation totale. ■

CONCLUSION

La première révolution universelle

Les révolutions ne naissent pas du progrès seul, elles sont nourries par les luttes de pouvoir et attisées par les désirs inavoués de domination et de contrôle. L'intelligence artificielle n'échappe pas à cette règle. Elle marque une transformation radicale du travail, de l'économie et de la société. Nous sommes au début d'un basculement où les agents autonomes IA ne seront plus de simples assistants, mais les véritables moteurs des entreprises et des institutions. Cette révolution est inévitable.

Les nations qui possèdent les ressources clés – l'énergie, les matières premières essentielles aux infrastructures IA, et la capacité d'innover rapidement – prendront l'ascendant sur le reste du monde. La hiérarchie économique et géopolitique sera redéfinie, non plus par le nombre de travailleurs ou la main-d'œuvre qualifiée, mais par la capacité à déployer et entretenir ces intelligences autonomes. Ceux qui n'auront ni la capacité ni la vision stratégique pour s'adapter risquent de voir leur influence décliner rapidement.

Les organisations qui intégreront l'IA comme pilier central de leur stratégie survivront. Les autres, figées dans des modèles où l'humain reste indispensable, risquent de disparaître. La question n'est plus de savoir si l'IA remplacera l'humain, mais si nous saurions nous adapter à ce nouveau monde où la connaissance serait instantanée, les décisions automatisées, et où l'intelligence artificielle deviendra à la fois le moteur et l'architecte d'une nouvelle ère. La révolution est en marche, nourrie par les ambitions, les inégalités et l'inévitable quête de domination technologique.

HS2
Hervé Schauer Sécurité

Formation
Continuité et résilience
Protection des données
Droit de la cybersécurité

Shutterstock

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

www.hs2.fr

formation@hs2.fr

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

INTELLIGENCE ARTIFICIELLE ET RESPONSABILITÉ : UNE QUESTION (ENCORE) DE SOUVERAINETÉ

L'intelligence artificielle ne date pas d'hier, pourtant elle n'a jamais fait autant parler d'elle qu'aujourd'hui.

C'est la démocratisation de son usage, et non pas l'innovation en tant que telle, qui a poussé le législateur européen à rédiger - et modifier de nombreuses fois, le règlement UE 2024/1689 dit « IA Act »1.

Ce texte a finalement été publié au JOUE le 12 juillet 2024, et on ne le présente plus. Il tente d'imposer la vision et les valeurs européennes, avec une approche par les risques, en interdisant les IA jugés comme dangereuses pour nos droits et libertés, et en imposant des obligations proportionnées aux risques estimées (élevés ou faibles) pour les fournisseurs et les distributeurs de systèmes d'IA.

Ce dont on a beaucoup moins parlé, c'est la mise en application en pratique de ces dispositions, et les questions de responsabilité en matière d'IA. Concrètement, en cas de dommages causés par un « fournisseur » ou un « déployeur » d'un système d'IA, qui est responsable ? Quels sont les outils offerts aux citoyens pour obtenir dédommagement ?

En l'absence de réponse dans le règlement IA Act, un projet de Directive n°2022/0303 devait instaurer un régime de responsabilité civile extracontractuelle propre à ce domaine, mais ce projet a été abandonné.

PROPOSITION DE DIRECTIVE SUR LA RESPONSABILITÉ EN MATIÈRE D'IA – CONTEXTE ET MESURES PHARES

Ce projet de directive sur la responsabilité en matière d'IA s'appuyait notamment sur le Livre blanc sur l'IA de 2020 du Comité Européen Social et Economique (CESE)2, document dont s'inspire également le règlement IA Act. Le principe est que « l'humain doit rester au commande ». En matière de responsabilité, ce Livre blanc plaide pour que les régimes de responsabilité existants s'appliquent en matière d'IA, mais que des mesures supplémentaires soient adoptées « lorsqu'il est difficile de déterminer l'opérateur économique effectivement responsable ».

Le projet de directive précité fait le même constat, dans son premier considérant, et estime que compte tenu de la complexité et l'opacité des systèmes d'IA, il peut être « difficile ou excessivement coûteux » pour les victimes d'identifier la personne responsable et apporter la preuve des « conditions requises pour obtenir gain de cause ».

Pour pallier cette difficulté, ce projet de directive proposait des règles de responsabilité civile uniformes dans tous les pays de l'UE, en se plaçant en faveur des victimes (européennes) des dommages causés par un système d'IA.

L'une des mesures les plus marquantes était le renversement de la charge de la preuve, qui devait peser sur les fabricants de systèmes d'IA, et qui impliquait l'existence d'un lien de causalité présumé entre le dommage et les prestations du système d'IA.

L'autre mesure phare était la possibilité donnée au juge d'ordonner la divulgation des éléments de preuve pertinents concernant des systèmes d'IA à haut risque spécifiques, soupçonnés d'avoir causé un dommage.

En février 2025, ce projet de réglementation a cependant était abandonné. La raison ? Au numéro 32 de l'annexe IV du programme de travail de la Commission pour 2025, ce retrait est justifié par le fait qu'« aucun accord ne soit prévisible »3. Dans les couloirs (et dans les médias), il se murmure surtout que l'Europe a peur de « sur-réglementer » et d' « étouffer » l'innovation.

SANS RÈGLEMENTATION EUROPÉENNE : COMMENT GÉRER LA RESPONSABILITÉ EN MATIÈRE D'IA ?

Pourtant, la question de responsabilité n'est pas qu'une question juridique, c'est aussi notre **souveraineté numérique qui est impactée en l'absence de règles communes.** Les fournisseurs et distributeurs de systèmes d'IA sont en grande majorité de prestataires étrangers, pour la plupart etats-uniens, qu'il est souvent difficile d'atteindre.

En l'absence de mesures fortes, et communes au niveau UE, il est fort à parier que les géants de la tech verront leur responsabilité contractuelle ET extracontractuelle quasi-exclue.

Concernant la responsabilité contractuelle de ces plateformes tout d'abord, ce sont les Conditions Générales que nous acceptons en échange de l'utilisation « gratuite » du service qui dictent les règles du jeu. Ces contrats d'adhésion non négociés excluent quasi-systématiquement la responsabilité des plateformes dans le cadre de l'utilisation de leurs services. De plus, et quand bien même leur responsabilité serait engagée, encore faut-il pouvoir les atteindre, leur CGU désignant la plupart du temps les compétences d'un juge américain en cas de litige, et l'application de la loi américaine4.

Concernant la responsabilité extracontractuelle, il existe tout de même quelques fondements pour agir en cas de préjudice subi du fait d'un système d'IA. L'entraînement des systèmes d'IA générative à partir de masse critique de données « scrappées » sur internet et les résultats qu'elles produisent sont notamment susceptibles de contrevenir à des droits de propriété intellectuelle (droits d'auteur, brevet, marques, droit sui generis du producteur de bases de données), au secret des affaires, à la vie privée ou encore au RGPD. Les systèmes d'IA générative sont également à même de créer des contenus diffamatoires, injurieux ou dénigrants, qu'il serait donc possible de sanctionner sur le fondement du droit de la presse ou du Code civil pour le dénigrement.

En l'absence de Directive européenne sur ces sujets, ce seront les régimes de responsabilité de chaque Etat membres qui s'appliqueront, avec des risques de divergences, mais surtout une réelle difficulté pour le citoyen lésé d'apporter des preuves tangibles de son dommage.

Le règlement européen n°2016/679 sur la protection des données, dit « RGPD », avait quant à lui bien compris cette problématique. Son article 82 prévoit en effet une responsabilité partagée entre responsable de traitement et sous-traitant, permettant à la personne physique

concernée de se retourner selon son choix contre l'un ou l'autre, et lui permettant ainsi d'obtenir réparation de manière effective.

En conclusion, rédiger des réglementations spécifiques à chaque innovation, et y intégrer nos valeurs est une chose. Les faire appliquer en est une autre. Aucune Loi ne peut survivre sans un écosystème qui lui est favorable : une volonté politique tout d'abord, avec l'assignation de budgets à la hauteur des enjeux ; des juges compétents et à même de comprendre la complexité de ces nouvelles innovations… et un système de responsabilité adapté. Notre souveraineté numérique sera protégée le jour où le Législateur, le Juge et le Politique travailleront main dans la main. ■

[1] Règlement (UE) 2024/1689 du Parlement européen et du Conseil du 13 juin 2024 établissant des règles harmonisées concernant l'intelligence artificielle et modifiant les règlements (CE) n° 300/2008, (UE) n° 167/2013, (UE) n° 168/2013, (UE) 2018/858, (UE) 2018/1139 et (UE) 2019/2144 et les directives 2014/90/UE, (UE) 2016/797 et (UE) 2020/1828 (règlement sur l'intelligence artificielle)

[2] Livre blanc sur l'intelligence artificielle – Une approche européenne axée sur l'excellence et la confiance [COM(2020) 65 final]

[3] ANNEXES to the COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS Commission work programme 2025

[4] Comme c'est le cas par exemple pour le service d'OpenAi, qui désigne dans ses CGU les « tribunaux fédéraux ou d'État de San Francisco, en Californie » et le « droit californien » comme loi applicable en cas de litige.

FRANCK ROUXEL

Point de vue du CISO
Cofondateur
AGORA RSSI CISO
Vice-Président FFCYBER

DE LA DÉFENSE PÉRIMÉTRIQUE À L'ANTIFRAGILITÉ :
LA MÉTAMORPHOSE DE LA CYBERSÉCURITÉ

*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.*

L'ESSENCE DE LA DÉFENSE NUMÉRIQUE

Il fut un temps où les pare-feu et VPN constituaient l'essence même de la défense numérique. Aujourd'hui, ces bastions d'une époque révolue laissent place à des systèmes plus nuancés, où l'intelligence artificielle, le XDR, le Zero Trust, le SASE et le SOAR redéfinissent progressivement le paysage de la cybersécurité. Plutôt que de s'enorgueillir d'un passé glorieux, il convient de reconnaître que l'évolution de la sécurité informatique repose sur une combinaison subtile d'innovation et de pragmatisme. L'analyse des premières solutions, simples et parfois naïves, révèle que les fondations posées jadis ont préparé le terrain à des mécanismes de défense bien plus complexes et adaptatifs.

Ces innovations, si elles promettent une détection des menaces affinée et une réponse automatisée à la hauteur des défis actuels, présentent néanmoins des difficultés notables lors de leur intégration dans les systèmes d'information existants. Les organisations se heurtent souvent à l'enchevêtrement d'outils sophistiqués – EDR, XDR, SOAR – qui, mal orchestrés, risquent de transformer leur environnement en un labyrinthe complexe. À cette équa-

tion s'ajoute la lourdeur persistante des systèmes legacy, héritages d'une ère moins numérique, qui continuent d'entraver l'harmonisation des processus. Ce cocktail – un savant mélange d'innovations de pointe et de technologies d'un autre temps – illustre avec une pointe d'ironie que le progrès ne s'improvise pas et que la coordination minutieuse reste indispensable pour éviter que l'excès de technologie ne se mue en un casse-tête insurmontable.

LA DÉPENDANCE CROISSANTE AUX INFRASTRUCTURES CLOUD ET LES ALÉAS GÉOPOLITIQUES

Au-delà de ces enjeux d'intégration, une dimension souvent négligée dans l'évaluation des solutions de cybersécurité modernes réside dans leur dépendance croissante aux infrastructures cloud. Les XDR, SOAR et autres plateformes avancées s'appuient massivement sur des architectures distribuées, hébergées chez les grands fournisseurs cloud internationaux. Cette évolution, si elle apporte agilité et puissance analytique, introduit également une vulnérabilité systémique dans un contexte géopolitique de plus en plus tendu. Les récentes tensions internationales révèlent la fragilité de ces équilibres. Un cas emblématique est celui du cadre juridique des transferts de données transatlantiques, actuellement mis à l'épreuve par des bouleversements politiques aux États-Unis. La remise en question des organes de contrôle indépendants comme le Privacy and Civil Liberties Oversight Board (PCLOB) ou le Data Protection Review Court (DPRC) illustre parfaitement comment des changements politiques peuvent, en quelques semaines, fragiliser des accords internationaux considérés comme stables.

> il convient de reconnaître que l'évolution de la sécurité informatique repose sur une combinaison subtile d'innovation et de pragmatisme.

Face à ces incertitudes, les organisations doivent désormais intégrer à leur analyse de risques la possibilité de perturbations majeures dans l'accès à leurs solutions de sécurité : que se passerait-il si, suite à des tensions diplomatiques, un fournisseur cloud étranger se voyait contraint de suspendre ses services ? Comment garantir la continuité de la détection et de la réponse aux incidents si les flux de données analytiques étaient soudainement interrompus par une décision réglementaire ou politique ? Cette problématique exige une évaluation minutieuse des architectures sous-jacentes aux solutions de cybersécurité déployées. Le choix d'un fournisseur XDR ou SOAR ne peut plus se limiter à ses capacités techniques, mais doit intégrer la résilience de son infrastructure face aux aléas géopolitiques et sa conformité durable aux exigences réglementaires comme le RGPD ou la NIS2.

L'ARRIVÉE IMMINENTE DE L'INFORMATIQUE QUANTIQUE ET SES RÉPERCUSSIONS

Parallèlement à ces préoccupations immédiates, l'horizon technologique s'assombrit avec l'arrivée imminente de l'informatique quantique. Les algorithmes de cryptographie traditionnels – RSA, ECC – voient leur robustesse mise en question par la promesse d'une puissance de calcul inédite. Le redouté scénario du « stocker maintenant, décrypter plus tard » n'est plus à exclure : des données précieuses, interceptées aujourd'hui, pourraient être déchiffrées demain par des machines quantiques.

Pour répondre à ce défi, la communauté internationale s'active autour de la normalisation des algorithmes post-quantiques, avec des initiatives menées par le NIST, l'ANSSI et d'autres acteurs de premier plan. Cependant, l'expérience de la transition TLS 1.1 vers TLS 1.2 nous enseigne que de telles migrations cryptographiques à l'échelle mondiale peuvent prendre bien plus longtemps que prévu – près d'une décennie pour TLS 1.2, malgré une standardisation dès 2008. La transition vers la cryptographie post-quantique s'annonce encore plus complexe, car elle implique non seulement des changements de protocoles, mais une refonte fondamentale des primitives cryptographiques sous-jacentes.

Les obstacles structurels observés lors de la migration TLS sont susceptibles de se reproduire, mais avec une ampleur accrue : inertie des systèmes legacy, retard d'adoption dans certains secteurs (comme l'éducation et l'administration publique qui accusaient encore 40% de retard en 2020 pour TLS 1.2), et difficulté à coordonner une transition homogène à travers des écosystèmes hétérogènes. Si la migration TLS 1.2 a nécessité des annonces coordonnées des grands navigateurs et l'appui de réglementations sectorielles comme PCI-DSS, la transition post-quantique exigera une stratégie encore plus globale et concertée.

De plus, contrairement à TLS 1.2 qui apportait des améliorations incrémentales, les algorithmes post-quantiques présentent des caractéristiques radicalement différentes (signatures et clés plus volumineuses, nouvelles propriétés

>>>

>>> mathématiques) qui pourraient affecter la performance et nécessiter des adaptations matérielles. La transition post-quantique devra donc naviguer entre l'urgence sécuritaire et les contraintes pratiques de déploiement, tout en évitant la fragmentation qui pourrait résulter de l'adoption de solutions temporaires divergentes. Dans ce contexte, les approches hybrides combinant cryptographie classique et post-quantique semblent incontournables pour assurer une transition en douceur, à l'image de la coexistence prolongée de TLS 1.0/1.1 avec TLS 1.2 qui a permis la continuité des services pendant la période de migration.

LA CYBERSÉCURITÉ DANS UN PAYSAGE EN CONSTANTE ÉVOLUTION

Dans ce paysage en constante évolution, la cybersécurité ne saurait se réduire à une question purement technique. L'évolution des menaces impose une révision des modes de gouvernance, où le rôle du RSSI, désormais CISO, se mue en véritable levier stratégique. Ce dernier, qui n'est plus cantonné aux opérations techniques, doit aujourd'hui traduire les risques en enjeux économiques et culturels, et guider l'ensemble de l'organisation vers une posture résiliente. Dans ce contexte, la notion d'antifragilité – la capacité non seulement à résister aux chocs mais à s'en enrichir – émerge comme un concept déterminant. Cette philosophie, adoptée par des entreprises avant-gardistes, ouvre la voie à une mutation du CISO vers le rôle de Chief Resilience Officer, une fonction qui transcende la sécurité pure pour englober la gestion globale des risques, qu'ils soient cyber ou organisationnels. La gouvernance moderne, soutenue par une approche agile et collaborative, se doit ainsi d'intégrer cette dimension antifragile, favorisant une adaptation constante et une anticipation des imprévus, sans pour autant renoncer à la rigueur nécessaire pour répondre aux exigences réglementaires et aux défis géopolitiques.

Les incertitudes géopolitiques actuelles viennent renforcer cette nécessité d'évolution, soulignant l'importance d'une approche prudente en matière de délégation de services critiques. Les organisations doivent réexaminer leurs dépendances technologiques à l'aune de scénarios de crise jusqu'alors considérés comme improbables : suspension soudaine d'accords internationaux sur les transferts de données, rupture d'approvisionnement en services cloud, ou restrictions d'accès aux mises à jour de sécurité. Cette nouvelle réalité appelle au développement de stratégies de souveraineté numérique, où les considérations de continuité opérationnelle s'étendent bien au-delà des traditionnels plans de reprise d'activité. Il s'agit désormais d'anticiper les conséquences de décisions politiques prises à des milliers de kilomètres, susceptibles d'affecter en quelques heures la disponibilité de services jugés essentiels. La diversification des fournisseurs, l'évaluation systématique des risques géopolitiques dans la chaîne d'approvisionnement technologique, et le développement de compétences internes critiques deviennent ainsi des composantes essentielles d'une stratégie de cybersécurité mature.

En définitive, l'avenir de la cybersécurité réside dans l'équilibre subtil entre l'innovation technologique et la transformation des mentalités. Les organisations, pour demeurer pertinentes dans un environnement en perpétuelle mutation, doivent non seulement investir dans des outils de pointe, mais aussi repenser leur structure, intégrer les vestiges du passé sans s'y enliser, et adopter des méthodes collaboratives qui embrassent l'antifragilité comme moteur de résilience. Il ne s'agit pas ici de glorifier la technologie ou de fustiger le legacy, mais de reconnaître que la véritable avancée se trouve dans la capacité à se réinventer continuellement, en gardant toujours à l'esprit que la force d'une organisation réside autant dans son agilité que dans sa solidité. C'est cette approche mesurée et pragmatique qui, en définitive, permettra de transformer les défis d'un monde numérique incertain en opportunités de progrès durable, en cultivant une résilience qui dépasse la simple robustesse pour atteindre une véritable antifragilité organisationnelle. ■

les organisations doivent désormais intégrer à leur analyse de risques la possibilité de perturbations majeures dans l'accès à leurs solutions de sécurité

Future of IT

#FutureOfIT

JEUDI
19
JUIN
2025

LE RDV INCONTOURNABLE DU MONDE DE L'IT

QUI RÉUNIT **PLUS DE 300 ACTEURS CLÉS** DE LA PROFESSION

3ÈME ÉDITION

THÉMATIQUE

QUELLES OPPORTUNITÉS POUR L'EUROPE DANS LE NUMÉRIQUE DE DEMAIN ?
IA GÉNÉRATIVE, RÉGLEMENTATION, CYBERSÉCURITÉ ET RSE

2 TEMPS FORTS

JOURNÉE WORKSHOPS & NETWORKING

Au Cercle d'Aumale
de 8h45 à 16h45

GALA FUTURE OF IT

Au pavillon Vendôme
de 18h00 à 23h45

S'INSCRIRE
SCANNEZ ICI

A L'INITIATIVE DE

AGORA CLUB Chief Data Officer
AGORA CLUB DSI et CIO
AGORA CLUB RSSI et CISO

UN ÉVÉNEMENT

AGORA MANAGERS MEETING & EVENT

JEANNE MAZELIER

Consultante Cybersécurité, Advens

BENJAMIN LEROUX

Chief Marketing Officer, Advens
Membre du CA Clusif
Membre CESIN

INTERVIEW CROISÉE

GS MAG : *Bonjour Jeanne, bonjour Benjamin, pouvez-vous vous présenter et nous dire comment vos parcours professionnels vous ont amené.e.s à vos rôles actuels chez Advens ?*

JM : J'ai suivi un master en relations internationales à Sciences Po Bordeaux, au sein duquel j'ai rapidement fait le choix d'intégrer des cours liés aux enjeux du numérique.

Cette appétence s'est concrétisée dans le cadre de la rédaction de mon mémoire sur les enjeux de cybercriminalité – un sujet à la fois transversal et stratégique, qui m'a permis d'explorer les zones grises entre sécurité, droit international et nouvelles technologies.

J'ai ensuite voulu confronter ma vision théorique à la réalité du terrain. C'est dans cette dynamique que j'ai décidé de me rendre au Forum International de la Cybersécurité (FIC), afin de rencontrer des professionnels du secteur, échanger avec eux sur leurs quotidiens et parcours variés.

La toute première assise où je me suis rendue était celle d'Advens. C'était un peu par hasard, mais c'est aussi ce moment qui a marqué un tournant dans ma trajectoire : j'y ai trouvé une équipe ouverte, passionnée, et disponible, ce qui m'a confortée dans l'idée que ce milieu, souvent perçu comme très technique et fermé, pouvait être accessible, humain.

BL : Par rapport à Jeanne, je suis un … vétéran de la Cyber ! J'évolue dans ce milieu depuis 20 ans, après une formation d'ingénieur. J'ai été consultant, chez Accenture notamment, ainsi que RSSI dans les services financiers… puis à nouveau consultant chez Advens.

À l'époque chez Advens, nous n'étions que quelques dizaines, à Lille et Paris. J'ai mené différentes missions de conseil et d'accompagnement de RSSI.

J'ai toujours été passionné par la « vision » de la cybersécurité que l'on souhaitait partager sur le marché et surtout auprès de nos clients. J'ai travaillé sur ces éléments et cela m'a mené à faire d'autres activités que des missions, comme des prises de parole lors d'évènements Cyber ou des contributions sur des livres blancs. A cela s'est ajouté un certain temps d'avant-vente… et, si on peut dire, d'avant-avant-vente, etc.

En remontant le fil, je me suis mis au Marketing. La société était en train de se structurer. J'avais une appétence pour ces sujets et je souhaitais contribuer autrement que par les missions de Conseil. C'est comme ça que je suis devenu directeur marketing, par la porte « métier » et non par la porte académique du marketing

GS MAG : *Le contexte géopolitique semble avoir des répercussions sur les Nouvelles Technologies et la Cybersécurité. Quelles répercussions dans votre métier de Consultante chez Advens ? Quelles répercussions dans votre métier de CMO chez Advens ?*

JM : L'accélération des tensions, les cyberattaques étatiques ou paraétatiques, les enjeux de souveraineté numérique ont redéfini les priorités de l'ensemble des acteurs de la cybersécurité. On observe une plus grande attention portée aux solutions utilisées (locales ou extra-européennes), et aux logiques de cloisonnement, d'interopérabilité ou de contrôle de la donnée.

Le contexte géopolitique pousse les organisations à revoir leurs architectures de sécurité, à se préparer à des scénarios plus extrêmes, et à faire des choix technologiques qui ne sont plus seulement techniques, mais aussi politiques.

On nous sollicite davantage pour construire des plans de continuité d'activité ou intégrer des scénarios étatiques dans les analyses de risque. L'anticipation devient centrale, avec des attentes plus fortes sur la résilience et la réactivité face à des attaques sophistiquées, parfois orchestrées dans des contextes de tension internationale.

BL : Comme tous les métiers, ou presque, le Marketing a ses outils et ses stacks technos : Hubspot, Salesforce, et j'en passe. Ces outils, largement répandus dans le Marketing, et pas que dans le Marketing pour la Cyber, sont plutôt américains : la question de la souveraineté et de la dépendance technologique se pose, comme dans la Cyber.

Au-delà des outils, pour le Marketing Cyber, je trouve que ces sujets « chauds » et à connotation politique ne sont pas les plus simples à manier. Faut-il communiquer et commenter ces sujets, qui évoluent très vite ?
Faut-il prendre parti ? Cela rejoint un peu la question de l'attribution des attaques. Qui doit s'en charger et que faut-il en faire dans une démarche de communication et de valorisation d'expertise Cyber ?

Il faut un bon équilibre entre l'opportunité que représente un sujet d'actualité et un message de fond, qui sert une démarche Marketing. Et j'aurais tendance à m'abstenir si je n'ai pas le message de fond !

JEANNE Benjamin

JM : Marketing & Cybersécurité… je t'aime moi non plus ? Est-ce un rôle facile à exercer ?

Il faut avouer que dans un domaine aussi technique, les profils Marketing n'ont pas toujours bonne presse ! Ils sont plutôt déconsidérés par les experts, qui associent le Marketing à tout un tas de qualificatif que je ne répéterai pas ici. Dans mon cas, avoir été consultant ou RSSI change la donne. Je pense (enfin j'espère) que je comprends de quoi on parle ! C'est aussi un challenge car j'ai une pratique non-académique du marketing, ce qui peut être positif quand les intuitions donnent des résultats… mais à double-tranchant si l'on rate certaines figures imposées.

Finalement, si on se préoccupe de la valeur qu'on apporte au marché et aux clients, faire du marketing dans la Cyber est passionnant. Des sujets nouveaux tous les jours ou presque, un domaine qui évolue à 100 à l'heure, des hommes et des femmes passionnées. Un contexte très agréable et très inspirant.

JM : Cybersécurité & Engagement : Advens met en avant l'engagement de ses équipes, comment le vis-tu au quotidien ?

C'est vrai que nous sommes tous engagés, soit dans l'atteinte des objectifs de nos clients, soit dans des projets sociétaux, qui dépassent le strict cadre de la Cyber. De mon côté, je suis fortement engagé dans le développement d'Advens… et aussi dans la Cybersécurité au sens large. Je le fais via le monde associatif en étant impliqué dans le conseil d'administration du CLUSIF. C'est une façon pour moi de contribuer à promouvoir la Cyber au sens large – et quelque part une façon de redistribué ce que ce domaine m'a offert. Je suis aussi impliqué sur les volets humains de ce domaine, via les travaux menés avec le CESIN sur le stress des responsables Cyber.

JM : Pour en revenir à la technologique, quel est ton rapport à la technologie ? A-t-il changé au fil du temps ?

La techno est une des réponses au risque Cyber. C'est indéniable. Il faut s'appuyer sur la technologie pour avoir une démarche de sécurité équilibrée. Cependant, avec le temps, on peut se sentir un peu blasé… Encore une nouvelle solution magique ? Encore un acronyme qui va faire l'objet d'un cadran magique ? Encore une réponse toute prête pour être conforme à un nouveau référentiel ? Il faut prendre du recul, bien sûr. Mais il faut savoir s'émerveiller devant les progrès. L'IA est un bon exemple : ça va changer la donne… à condition d'en dompter le potentiel.

C'est un peu comme la Sensibilisation, qui est presque l'opposé du sujet technologique. On peut perdre espoir après des années de campagne de sensibilisation. Mais l'Humain doit toujours faire l'objet de toutes les attentions et doit être accompagné dans ses usages numériques.
A nous de nous réinventer !

BENJAMIN Jeanne

BL : Pourquoi la Cyber ?

La question du cyberespace, longtemps traitée comme un sujet technique à part, est aujourd'hui au cœur des enjeux de souveraineté, de sécurité nationale, de protection des données et même de démocratie. J'ai très vite compris que si je voulais travailler sur des problématiques actuelles, concrètes et à fort impact, c'était vers ce domaine qu'il fallait me tourner.

Par ailleurs, travailler dans la cybersécurité oblige à rester curieux, à se former en continu, et à collaborer avec des profils très différents – juridiques, techniques, stratégiques. Mon passage chez InterCERT m'a d'ailleurs permis d'en prendre pleinement conscience : au-delà de la technique, il y a un véritable enjeu de coordination et de mise en réseau des acteurs, dans une logique d'intelligence collective face aux cybermenaces.

Mais, par-dessus tout, ce qui me plait c'est qu'on a le sentiment d'être utile. Derrière chaque action, chaque projet, il y a une finalité concrète : sécuriser des systèmes essentiels, protéger des entreprises, prévenir des attaques, garantir des droits.

BL : Quels ont pu être les freins pour entrer en Cyber ? Ou au contraire quels facilitateurs ?

Dans mon cas, deux facteurs sont intervenus : tout d'abord la méconnaissance de la diversité des métiers liés à la cybersécurité au moment des choix d'orientation, notamment en début de parcours universitaire. Le domaine est parfois perçu comme réservé à des profils déjà très techniciens ou expérimentés, ce qui peut être intimidant pour des personnes n'ayant pas eu d'exposition préalable à ces notions.

A cela s'ajoutent les stéréotypes de genre qui associent encore trop souvent les compétences techniques à des profils masculins. Ces représentations peuvent générer une forme d'auto-censure, freinant l'ambition ou la confiance des jeunes femmes à s'engager dans ce secteur. Je sais que cela a été mon cas.

BL : La place de la technologie dans la Cyber et en particulier dans une carrière dans la Cybersécurité : faut-il être technophile ? Geek : un peu, beaucoup, passionnément… ou pas du tout ?

C'est un sujet épineux. C'est un univers exigeant, très technique, où les compétences informatiques sont très valorisées – et c'est tout à fait légitime.

Mais dans ce contexte, lorsqu'on vient d'un autre horizon, c'est parfois difficile de trouver sa place, de faire entendre sa vision. En tant que profil "non technique", on peut avoir le sentiment de devoir constamment prouver sa légitimité, alors même que l'on aborde les problématiques sous un angle complémentaire, souvent plus transversal mais tout aussi nécessaire.

D'après moi, la cybersécurité ne se limite pas à la maîtrise des outils ou des protocoles : elle touche à des enjeux de gouvernance, de conformité, de communication, de géopolitique, etc.

Autant de dimensions qui nécessitent des profils venus du droit, des sciences sociales, des relations internationales. Ces apports sont essentiels pour penser la cybersécurité dans toute sa complexité, et pas uniquement sous l'angle technique.

Selon moi, ce qui compte avant tout, c'est d'accepter de ne pas tout savoir faire (et ce pour tout type de profil) et de ne pas hésiter à solliciter le point de vue d'autres acteurs. C'est justement cet apprentissage continu, cette capacité à faire le lien entre les disciplines, qui permet d'apporter de la valeur.

Si je devais donner un conseil à un profil similaire au mien ce serait donc de ne pas se formaliser des quelques interactions déstabilisantes qui peuvent venir réveiller cette impression de "pas assez" et de se concentrer sur ce que l'on est capable d'apporter professionnellement. Et souvent, une fois la porte passée, on se rend compte que l'on a beaucoup plus à apporter que ce que l'on imaginait.

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 (ISC2 Official Training Partner)

CISM / CISA / CRISK (ISACA Accredited Partner)

+ 33 974 774 390

www.hs2.fr

formation@hs2.fr

exabeam™

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

tealenium

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

Our People. Your Platform. Managed.

contact@tealenium.com