Spécial Cybersécurité
La quête des équilibres

IT for Business

Le magazine des managers du numérique

« Notre autonomie stratégique doit se construire maintenant »

Emmanuel Sardet,
président du Cigref

N°2309 OCTOBRE 2025

TECH SHOW
PARIS

5 - 6 novembre 2025, Paris Expo Porte De Versailles

EXPLOREZ, NETWORKEZ ET INNOVEZ AU COEUR DE L'ÉCOSYSTÈME TECH

Tech Show Paris est le rendez-vous de référence pour les professionnels de la tech et de l'innovation digitale en France.
Il rassemble cinq événements majeurs: Cloud & AI Infrastructure, Cloud & Cyber Security Expo, DevOps Live, Data & AI Leaders Summit et Data Centre World.

+ 7 900 visiteurs | + 275 exposants I + 320 conférenciers

Scannez le QR code pour vous inscrire dès maintenant !

TECH SHOW PARIS
techshowparis.fr

REGROUPANT

CLOUD & AI INFRASTRUCTURE | DEVOPS LIVE | CLOUD & CYBER SECURITY EXPO | BIG DATA & AI WORLD | DATA CENTRE WORLD

L'ÉVÈNEMENT DÉDIÉ AUX PROFESSIONNELS DE LA TECH EN FRANCE

ORGANISÉ PAR

CloserStill

Une manche à rien ?

François Jeanne
Rédacteur en chef

C'est l'histoire drôle, résumée ici, d'une ribambelle d'intermédiaires qui achètent et revendent successivement un lot de chemises avec une seule manche, de plus en plus cher à chaque transaction. Jusqu'à ce que le dernier d'entre eux s'étonne et questionne : «*Mais pourquoi voulez-vous que j'achète ces chemises immettables ?*» Ce à quoi le dernier revendeur lui rétorque : «*Pourquoi t'inquiètes-tu ? L'important, c'est de trouver un nouvel acheteur !*»

La même parabole vaut pour les joueurs de football, qui s'échangent à prix d'or, de plus en plus élevés. Les journalistes sportifs ont beau s'étrangler devant ces montants, sans rapport avec leurs qualités sportives, l'important est de pouvoir les revendre la saison suivante, encore plus cher dans la plupart des cas.

Et pour les sommes actuellement engagées par les OpenAI, les Nvidia et consorts ? On parle désormais en centaines de Md$. Et même si les prévisions de ventes, au moins pour les GPU, sont impressionnantes, il est hautement probable qu'une bonne partie des sommes misées ne trouvent pas un ROI. Sauf à faire payer sur le long terme les clients, sous forme d'abonnements de plus en plus coûteux à des services qu'ils ne pourront pas trouver ailleurs. Les clients, ce sont les entreprises et leurs souscriptions à des services cloud ou des logiciels SaaS. Et dans une moindre mesure les particuliers, qui retrouveront des fonctionnalités ++++ sur un smartphone de plus en plus onéreux.

«*Quand on pense qu'il suffirait que les gens n'achètent pas pour que cela ne se vende pas*», disait déjà Coluche il y a 40 ans. Mais cela reste-t-il possible ? Nous n'imaginons plus pouvoir nous passer de ces fonctionnalités. Et nous sommes écrasés sous ces chiffres, paralysés par l'idée que nous n'aurons jamais les moyens de rivaliser.

Sauf que des clubs à petits budgets parviennent encore à gagner des titres au football. Et des joueurs de tennis issus des qualifications à se hisser jusqu'en finale de tournois du Grand Chelem. À condition que les règles du jeu ne soient pas toujours édictées par les plus puissants, il n'y a pas de raison que cela ne continue pas. Mais il faut pour cela que l'Europe, en jouant collectif, se fasse respecter. Nous n'aurons certes pas les centaines de milliards des entreprises de technologie américaines à mettre sur la table, mais il y a du talent de ce côté de l'Atlantique, des valeurs et un sens du doute – c'est-à-dire une capacité à la remise en question des évidences ou de la force brute – qui peut nous faire regagner du temps sur la concurrence. Prêts pour la seconde manche ? ■

sommaire

tendances

l'entretien

talents

opinions

parole de DSI

IT for Business

Président & directeur de la publication, éditeur
Frédéric Ktorza

Directeur de la rédaction
Thierry Derouet
tderouet@itforbusiness.fr
06 22 12 09 24

RÉDACTION

Rédacteur en chef
François Jeanne
fjeanne@itforbusiness.fr

Rédacteur
Alessandro Ciolek
aciolek@itforbusiness.fr

Ont participé à ce numéro
Xavier Biseul, Alain Clapaud, Laurent Delattre, Patricia Dreidemy, Pierre Fontaine, Aude Leroy, Charlotte Mauger, Stéphane Miekisiak, Frédéric Simottel

RÉDACTION TECHNIQUE

Direction artistique
Bertrand Grousset

ÉVÉNEMENTS

Responsable éditorial événements et programmes
Thomas Pagbe
tpagbe@itforbusiness.fr

Responsable Partenariats Groupe et Média
Verena Holder
vholder@choyou.fr
06 03 87 45 78

PUBLICITÉ, OFFRES COMMERCIALES

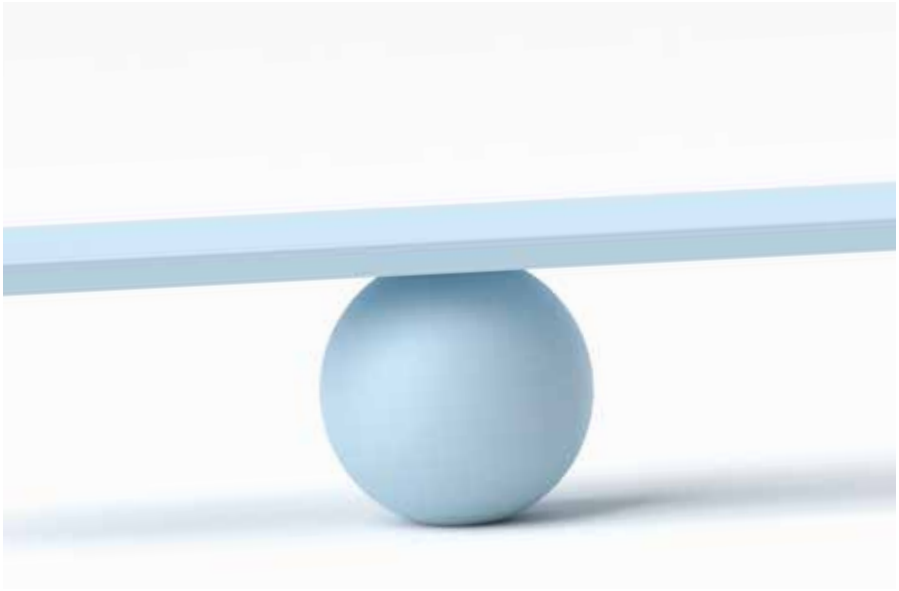
Romain Duran
rduran@choyou.fr
06 03 25 37 27

Karim Baqlou
kbaqlou@choyou.fr
01 53 05 93 79
06 09 91 20 08

DOSSIER SPÉCIAL

Cybersécurité

La quête des équilibres



« Il faut cultiver la lucidité des collaborateurs, pas leurs peurs »

ABONNEMENTS

France métropolitaine
1 an (11 nos) : 200 € HT
soit 204,20 TTC (TVA 2,10 %)

Étudiants (sur justificatif)
1 an (11 nos) : 100 € HT
soit 102,10 TTC (TVA 2,10 %)

Outre-mer / Étranger
Nous consulter

Service Abonnement
6, rue de Lisbonne
75008 Paris
COURRIEL *contact@itforbusinessabonnement.fr*
TÉL. 01 53 05 93 83
WEB *www.itforbusiness.fr/abonnes*

Vente au numéro
(France métropolitaine)
25 € HT (TVA 2,10 %)

IT FOR BUSINESS
est édité par IT for Business,
6, rue de Lisbonne
75008 Paris
RCS Paris 440 363 679

Dépôt légal à parution
N° de commission paritaire
0326 T 85172
ISSN 2258-5117
Code APE 5814Z

Photo de couverture
Maÿlis Devaux

Imprimé en France
par Imprimerie de Champagne,
Rue de l'Étoile-de-Langres,
ZI Les Franchises
52200 Langres

Origine du papier Italie.
Taux de fibres recyclées 0 %.
Certification PEFC 100 %.
Eutrophisation PTot 0,036 kg/t.

CENTRE DE RECHERCHE JÜLICH / KURT STEINHAUSEN.

L'Europe inaugure Jupiter pour affirmer une souveraineté… encore fragile

Une belle brochette d'officiels, allemands ou scandinaves, ont fêté début septembre le lancement de Jupiter, le premier supercalculateur « exascale » (un trillion d'opérations par seconde) du Vieux Continent, destiné en particulier à supporter le développement de modèles d'IA. D'une surface d'un demi-terrain de football et avec ses 24 000 processeurs, pour un coût total estimé à 500 M€, il est effectivement assez impressionnant. Mais si la volonté européenne de réduire l'écart avec les États-Unis et la Chine dans le domaine de l'intelligence artificielle (IA) n'est pas discutable, il reste que les processeurs en question sont d'origine américaine (Nvidia), faute d'alternative domestique. Et au passage, on notera qu'alors que la « bête » en question a été conçue et fabriquée par la filiale d'Atos Eviden, aucun représentant de cette firme pourtant bien européenne n'est sur la photo. Encore un effort pour jouer en équipe messieurs les Allemands ?

PRIVACY

72 %

des Européens

font confiance aux acteurs du Continent pour protéger leur vie privée. Ce chiffre tombe à 8 % pour les fournisseurs chinois de produits et services numériques, et à 20 % pour les Américains.

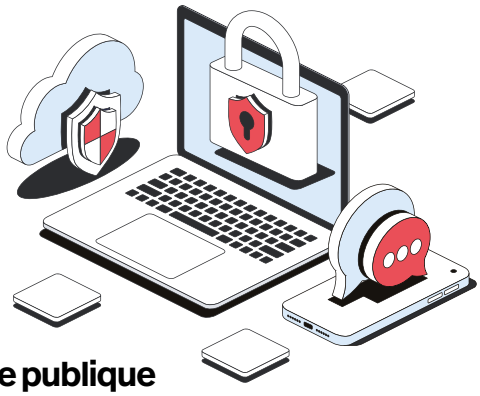
GIM POUR SCHWARZ DIGITS

L'IA gagne l'or en code, mais pas la confiance

Après sa médaille d'or aux Olympiades internationales de mathématiques, Gemini 2.5 Deep Think, modèle avancé de Google DeepMind, a remporté l'or à l'ICPC 2025, une compétition de programmation universitaire. Il a résolu dix des douze problèmes proposés en cinq heures, surpassant la majorité des 139 équipes humaines. Et il été le seul à résoudre un problème d'optimisation complexe (le « Problème C »), mobilisant théorie des jeux et programmation dynamique. La performance, qui marque au passage le rattrapage réussi de OpenAI par Google/Deepmind, ravive le débat sur les capacités d'abstraction des IA. Il y a d'un côté les enthousiastes qui voient là une performance digne de Deep Blue ou AlphaGo. Et de l'autre ceux qui, malgré une intégration progressive de l'IA dans leurs pratiques de développement, ne lui font toujours pas confiance, à l'instar de 60 % des développeurs qui dénoncent des bugs, une sécurité douteuse et une lisibilité insuffisante, selon une enquête récente de Stack Overflow. L'enjeu pour les DSI reste donc entier : intégrer ces IA dans des chaînes de valeur fiables, auditables et gouvernées.

Le secteur public accélère sur le cloud, mais pas sur SecNumCloud

Selon les données fournies par l'UGAP, qui commercialise en partie les offres de cloud public accessibles au secteur public justement, la croissance des commandes ne se dément pas en 2025, avec une augmentation des marchés passés attendue entre 30 et 40 %. Cette dynamique profite surtout aux acteurs européens, au détriment de leurs concurrents hors-Union (essentiellement américains), considérés comme tels même s'ils disposent de datacenters en Europe. Autres victimes, les offres SecNumCloud, qui ne parviennent pas à séduire. La faute à un contexte réglementaire encore mal consolidé ? OVH, l'un de ses acteurs de pointe, s'en tire néanmoins avec les honneurs, avec plus de 40 % des ventes en 2024 (23,4 M€). Il est vrai que le fournisseur français dispose aussi d'une offre commerciale non adossée à la qualification de l'ANSSI.



L'adoption du cloud dans la sphère publique bénéficie aux fournisseurs européens

Année	Marketplace (achats complémentaires)	Offre commerciale SecNumCloud	Offre commerciale UE	Offre commerciale non-UE	Total
2021		1	3	8	**12 M€**
2022		4	7	10	**20 M€**
2023		12	10	13	**34 M€**
2024		20	18	14	**52 M€**
2025 *(fin août)*	1	12	23	13	**48 M€**

SOURCE NUMERIQUE.GOUV.FR

OpenAI–Oracle : un méga-contrat qui inquiète les clients d'OCI

Le contrat d'environ 300 Md$ sur cinq ans passé par OpenAI auprès d'Oracle, pour accéder à la puissance de ses datacenters à partir de 2027, fait trembler l'écosystème… surtout côté clients d'Oracle Cloud (OCI). En cause : le risque de priorisation des capacités (GPU, énergie, réseaux) au bénéfice d'OpenAI, une pression à la hausse sur les prix, et des SLA fragilisés si l'afflux de charges IA déborde. Des analystes pointent aussi un risque d'exécution inédit à cette échelle, dont l'impact se mesurerait d'abord chez les clients existants. En clair : le GPU d'OpenAI passera toujours avant votre ERP – même si vos SLA, eux, restent bien au tarif premium.

ENVIRONNEMENT

57 %

des dirigeants mondiaux

estiment qu'en matière de défense de l'environnement, l'IA générative apporte des bénéfices qui dépassent son coût. Ils étaient 67 % l'année dernière.

SOURCE CAPGEMINI RESEARCH INSTITUTE

SAP jure que la souveraineté «n'est plus optionnelle»

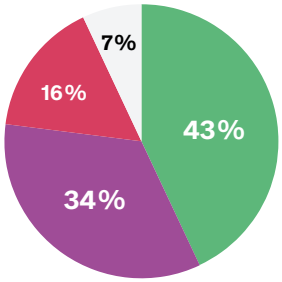
Pour Thomas Saueressig, membre du directoire de SAP chargé du product engineering, *«la souveraineté n'est plus optionnelle, elle conditionne liberté, prospérité et démocratie»*. L'éditeur promet donc notamment d'investir 20 Md€ sur dix ans pour proposer trois offres: une opérée dans ses propres datacenters en Europe, une autre chez les clients, on-premise, et enfin une dernière dans le cadre d'un partenariat avec Delos Cloud pour le secteur public allemand. Ambition : couvrir les volets données, opérationnel, technique et juridique. Les utilisateurs saluent cette orientation mais, comme le rappelle Gianmaria Perancin (USF), il faudra juger de la maturité réelle et de l'alignement avec les référentiels de sécurité européens. Et il reste une ombre au tableau : cette souveraineté «made in SAP» demeure étroitement arrimée à Microsoft et Nvidia.

Le mainframe résiste à tout ou presque

Bien qu'intéressée, l'étude annuelle de Kyndryl, spécialiste des services sur les infrastructures et les mainframes notamment, est toujours… intéressante. À la fois parce qu'elle mesure bien, année après année, l'importance de ces serveurs et plus généralement du legacy dans les entreprises du monde entier. Et parce qu'elle capte aussi les évolutions en cours, qui ne sont pas anodines quand on sait le temps et les investissements que réclament des migrations partielles ou totales depuis ces mainframes vers d'autres infrastructures, en particulier cloud.

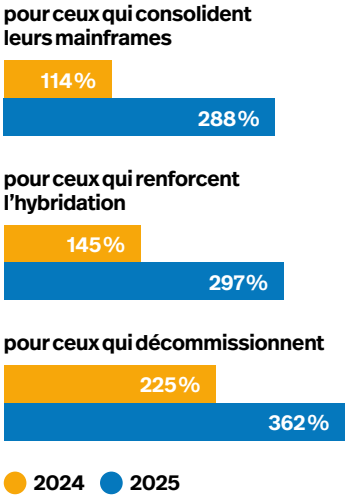
On retiendra de cette édition que 2024 a été marquée par des ruptures importantes pour les stratégies des DSI, avec des choix très divergents. Et s'ils affirment dans 11% des cas que le mainframe devient moins important dans ces stratégies, ils sont encore 56% à en augmenter l'usage. Le recours à l'IA qui se généralise leur permet en tout cas de revisiter leurs scenarios de migration ou de MCO, ce qui n'a pas manqué de susciter moult changements de pied. Bref, et malgré les funestes oracles qui se répètent depuis bientôt 40 ans, la bête n'est pas encore morte !

80% des entreprises ont changé de stratégie de modernisation pour leurs mainframes en 2024



- choisissent de moderniser plus encore leur mainframe
- d'accentuer l'interopérabilité avec le cloud
- accélèrent la bascule d'applications hors du mainframe
- NSP

Avec des ROI qui augmentent dans tous les cas



SOURCE : KYNDRYL'S 2025 STATE OF MAINFRAME MODERNIZATION SURVEY REPORT

Microsoft contraint de séparer Teams d'Office 365 : un signal fort de Bruxelles

La Commission européenne impose à Microsoft de découpler Teams de sa suite Office/Microsoft 365 dans l'UE. L'éditeur doit proposer une version sans Teams, à un tarif réduit, et publier des interfaces pour faciliter l'interopérabilité et la portabilité des données. L'objectif est de mettre fin au «liage forcé» qui bridait la concurrence et enfermait les entreprises dans l'écosystème Microsoft. «*Les clients et les concurrents méritent une concurrence loyale et un réel choix*», a déclaré la commissaire Margrethe Vestager. Les flux collaboratifs devraient ainsi gagner en ouverture, même si l'attractivité des offres alternatives reste à prouver.

Mistral AI, pari réussi… à l'échelle de l'Europe

En deux ans, Mistral AI, fondée à Paris en 2023, sera devenue la start-up d'IA la plus valorisée d'Europe (11,7 Md€), grâce à sa dernière levée de fonds record de 1,7 Md€. Soutenue par des investisseurs majeurs et désormais par ASML – acteur clé des semi-conducteurs – Mistral est sur le toit du Continent et fait face aux géants américains de l'IA comme OpenAI ou Anthropic. L'entrée d'ASML notamment, qui devient son principal actionnaire, marque une alliance industrielle stratégique visant à intégrer l'IA dans la chaîne de production des puces et à renforcer l'autonomie technologique de l'Europe. Mais l'écart avec les leaders US reste important, encore plus depuis que Nvidia a décidé de sortir son portefeuille (voir page suivante).

Le Tribunal de l'UE déboute Philippe Latombe sur le Data Privacy Framework

Le Tribunal de l'UE a rejeté le recours du député français Philippe Latombe contre la décision d'adéquation de 2023 instaurant le Data Privacy Framework (DPF) entre l'UE et les États-Unis. L'élu contestait l'indépendance du Data Protection Review Court (DPRC), créé par décret présidentiel aux USA, ainsi que l'absence d'autorisation préalable par une autorité indépendante avant toute collecte de données par les agences américaines. Les juges ont estimé que le DPRC disposait de garanties suffisantes et qu'un contrôle a posteriori respectait la jurisprudence Schrems II. Max Schrems a réagi en estimant que «*le DPF est presque identique aux accords déjà annulés*» et qu'un nouveau recours reste inévitable.

CBC CYBER SECURITY Business Convention

Le salon PRO de la Sécurité Numérique

L'ESSENTIEL DE LA CYBERSÉCURITÉ, EN UN SALON

MERCREDI 26 & JEUDI 27 NOVEMBRE 2025

TOULOUSE - MEETT

220 exposants & partenaires

3 500 visiteurs attendus

+80 prises de paroles

2 JOURS POUR EXPLORER L'UNIVERS DE LA CYERSÉCURITÉ

Un salon unique qui rassemble fournisseurs de solutions et décideurs autour de rencontres privilégiées sur les stands et lors de rendez-vous d'affaires ciblés.

- **Des rencontres avec les experts du secteur** : conférences prospectives, ateliers techniques et démonstrations.
- **Des expériences immersives** : simulations de cellule de crise & challenge Capture the Flag* pour savoir anticiper et réagir aux attaques *(*Capture le drapeau)*
- **Les grandes thématiques 2025** : régulations européennes, chaînes industrielles & cybersécurité, cybersécurité spatiale, IA dans les collectivités.

PLONGEZ DANS L'UNVERS DU CBC

www.cbc-convention.com

Suivez-nous @CBC - Cybersecurity Business Convention

Ouverture des inscriptions visiteurs début septembre

Organisé par : Sponsor gold : Sponsor silver : Sponsor bronze : Partenaires :

Partenaires média :

Nvidia – OpenAI : l'accord à 100 Md$ qui propulse l'IA dans une nouvelle dimension

Cent milliards injectés dans Open AI sur dix ans. Et 5 Md$ dans Intel, immédiatement. Alors que la Chine venait d'interdire à ses entreprises d'acquérir des puces Nvidia, le fabricant américain a repris l'offensive avec éclat. De quoi bouleverser les équilibres sur les marchés de l'IA et des semi-conducteurs.

Décidément, Nvidia ne fait pas dans la demi-mesure. Quelques jours après avoir annoncé le 19 septembre son entrée au capital d'Intel pour 5 Md$ (voir encadré), le leader des puces pour l'IA a de nouveau affolé les compteurs, cette fois en signant avec OpenAI un deal à 100 Md$ pour créer la plus puissante infrastructure mondiale d'intelligence artificielle et verrouiller la concurrence. Cette infrastructure d'apprentissage et inférence de l'IA d'au moins 10 gigawatts reposera sur les technologies de Nvidia, et plus précisément sur la prochaine génération de superchips « Vera Rubin ».

Le standard de performance se déplace vers des niveaux qui seront très difficiles à atteindre

Malgré des termes de l'accord qui restent flous – combien et quand exactement – la somme a de quoi donner le vertige. Une habitude quand on parle d'OpenAI depuis maintenant trois ans, mais tout de même ! *« C'est le plus grand projet d'infrastructure dédié à l'intelligence artificielle de toute l'histoire »*, s'est d'ailleurs enthousiasmé Jensen Huang, fondateur et PDG de Nvidia, pendant que le CEO d'OpenAI Sam Altman affirmait que *« aucun autre partenaire que Nvidia n'est capable de réaliser cela à une telle échelle et avec une telle rapidité. »*

Il faut rapprocher cette annonce du deal conclu entre OpenAI et Oracle d'un montant annoncé de 300 Md$ sur cinq ans autour de l'hébergement et l'exploitation des charges de calcul de l'IA sur l'infrastructure cloud d'Oracle (voir page 7). Bien qu'annoncés séparément, ces deux accords sont liés et forment l'ossature du fameux projet Stargate annoncé en début d'année.

Avec ces deux annonces, OpenAI cherche en réalité à sécuriser la fourniture des équipements et les investissements financiers qui seront essentiels à la création et l'hébergement de ses futurs modèles IA. Ces accords permettent à OpenAI à la fois de s'assurer la fourniture de la prochaine génération de puces Nvidia en millions d'exemplaires dans un marché sous très haute tension et de disposer de la capacité d'hébergement et de mise en réseau à grande échelle sur les infrastructures d'Oracle Cloud.

Une course hors de portée de l'Europe ?

Cette montée en puissance vise à lever l'un des principaux verrous de l'IA actuelle : l'accès à des ressources de calcul massives pour entraîner et faire fonctionner des modèles avancés, capables de raisonnement complexe, d'orchestration multi-agentique, de traitement multimodal et de gestion de contextes étendus. L'accord a surtout de quoi inquiéter la concurrence. Les rivaux d'OpenAI, qu'ils soient éditeurs de modèles ou fournisseurs d'infrastructures, voient le standard de performance se déplacer vers des niveaux qui seront très difficiles à atteindre sans alliances de même envergure. AMD, Google DeepMind, Microsoft, Meta, Anthropic devront accélérer leurs investissements pour rester dans la course. Quant à l'Europe et pour Mistral AI, le défi commence à prendre vraiment mauvaise tournure. Comment ne pas se laisser distancer trop rapidement à la vitesse où s'enchaînent les innovations et où coulent les milliards de dollars outre-Atlantique ?

LAURENT DELATTRE

Nvidia et Intel, des chemins qui se croisent

Destins contraires, entre Intel sur la pente descendante (-60 % en bourse l'année dernière), obligé de faire appel au gouvernement américain via le Chips Act pour une prise de participation salvatrice de 9,9 % dans son capital, et Nvidia qui a vu son cours d'action grimper de 171 % depuis 2024. De quoi pouvoir tendre la main à un compatriote en difficulté, en lui injectant 5 Md$ et en prenant 4 % environ de son capital ? Business is business. C'est donc surtout la perspective d'un co-développement de processeurs IA mêlant CPU x86 et GPU NVLink pour contrer notamment AMD qui semble avoir guidé Nvidia. La perspective de renforcer ses positions en Occident également, au lendemain de l'annonce de la Chine d'une interdiction faite à ses entreprises d'acquérir les GPU de l'américain, invoquant des risques d'espionnage, les restrictions américaines et sa volonté d'indépendance technologique. En développant une plateforme IA intégrée, soutenue par les fonds publics américains, Nvidia construit une « forteresse technologique », face à cette même Chine – qui affirme que ses propres solutions sont compétitives, notamment chez Huawei –, bien sûr, mais aussi pour confirmer sa domination en Europe.

Un événement **IT for Business** avec le concours du Cigref, French Women CIO et Atout DSI

Les DSI de l'année 2025

27e Édition

Directions des Systèmes d'information et du Numérique de l'Année

Le rendez-vous incontournable des managers du numérique

27e édition

ET SI C'ÉTAIT VOUS ?

6 Trophées pour récompenser les meilleures oeuvres de la DSI durant l'année 2025

+ le Grand Prix du DSI de l'année

Rendez-vous sur dsidelannee.fr pour découvrir les catégories récompensées et candidater.

L'open source en Europe, une adhésion sans direction

L'Europe exploite l'open source à grande échelle, mais trop souvent en simple consommatrice. Faute de stratégie et de contributions solides, elle prend le risque de perdre son leadership technologique et sa souveraineté numérique selon la Linux Foundation qui vient de publier son rapport 2025 pour l'Europe.

La Linux Foundation a entrepris depuis 2022 de dresser annuellement, avec le rapport *World of Open Source Europe*, un panorama des pratiques open source de ce côté de l'Atlantique. L'édition 2025 confirme d'abord que les organisations du continent utilisent massivement ces technologies. Les niveaux d'adoption sont très élevés en Europe. Plus de 90 % des organisations ont déclaré que la valeur tirée de l'open source s'était maintenue ou accrue ces douze derniers mois. Le rapport souligne aussi une forte pénétration dans des domaines critiques tels que les systèmes d'exploitation notamment côté serveurs (64 % des organisations), les technologies cloud et conteneurs (55 %), et le développement applicatif (54 %).

▼ Le Top 10 des domaines d'utilisation de l'OSS en Europe
(% d'entreprises utilisatrices)

1	SYSTÈMES D'EXPLOITATION	64 %
2	CLOUD ET CONTENEURISATION	55 %
3	DÉVELOPPEMENT WEB ET APPS	54 %
4	Bases de données et administration	53 %
5	CI/CD et DevOps	52 %
6	CI/CD et DevOps	51 %
7	IA / machine learning	41 %
8	Cybersécurité	36 %
9	Analytics et data science	33 %
10	Stockage	26 %

SOURCE LINUX FOUNDATION EUROPE, 2025

Moins de la moitié des entreprises utilisatrices contribuent aux projets open source

Sauf que cette adoption généralisée reste trop passive et sans véritable stratégie définie au plus haut niveau. En effet, seulement 34 % des organisations européennes disposent d'une stratégie formelle en matière de logiciel open source (OSS), et à peine 22 % ont mis en place un bureau dédié à l'open source (OSPO). Et les directions interrogées restent à distance du sujet : si 86 % des employés reconnaissent la valeur de l'OSS, ce chiffre tombe à 62 % chez les cadres dirigeants. Résultat, 30 % des entreprises européennes se contentent de consommer du logiciel open source sans y contribuer en retour. Seulement 42 % des organisations contribuent activement aux projets dont elles dépendent. Et seulement 28 % emploient des mainteneurs ou contributeurs à temps plein. Pourtant, le contexte géopolitique actuel contribue activement à transformer l'open source en un levier stratégique pour la souveraineté numérique européenne. Il est même perçu comme essentiel pour reprendre le contrôle des piles technologiques. Mais la fondation dénonce un sous-investissement structurel de l'Europe, en particulier dans la maintenance et la sécurité des briques critiques : trop peu d'organisations financent des mainteneurs ou leurs dépendances amont de façon durable, et les mécanismes publics restent épars, à court terme et de taille insuffisante par rapport aux besoins.
Et si l'association salue l'initiative allemande « Sovereign Tech Agency (STA) » et y voit un modèle de financement public à suivre, elle considère que l'initiative est « *de plusieurs ordres de grandeur trop petit* » et appelle à un dispositif plus ambitieux à l'échelle de l'UE et à des lignes budgétaires dédiées dans un cadre financier pluriannuel. Des politiques trop « localistes » risquent de fragmenter un écosystème par nature transnational. L'Europe doit coordonner financements, marchés publics et politiques d'ouverture pour transformer l'avantage théorique de l'open source en avance concrète. Faute de quoi, elle risque de rapidement décrocher, s'enfermant dans des statu quo qui renforcent ses dépendances vis-à-vis de fournisseurs extra-européens et fragilisent sa compétitivité.

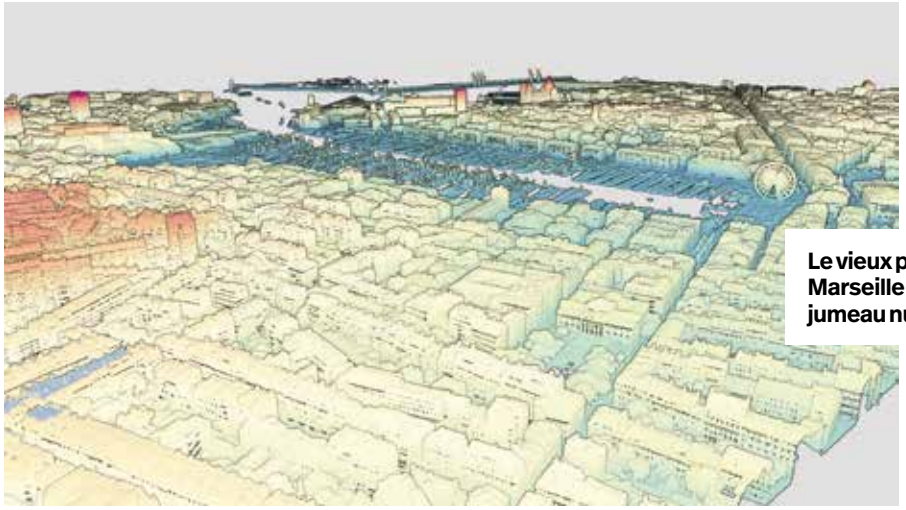
LAURENT DELATTRE

Gabriele Columbro, DG, Linux Foundation Europe

« L'open source est à un tournant en Europe. Notre rapport 2025 montre un large consensus, public comme privé : l'open source est à la fois moteur d'innovation, garantie d'indépendance vis-à-vis des fournisseurs et socle de souveraineté numérique. Mais sans investissements stratégiques, sans sponsorship des comités de direction et sans un environnement pro-entrepreneurs, l'Europe laissera filer l'avantage. Les communs numériques sont notre meilleur levier pour l'autonomie et la compétitivité mondiale. »

Le jumeau numérique de la France en construction

L'Université de la Transition Numérique des Territoires, qui s'est tenue à Dijon, a fait le point sur les avancées de l'infrastructure-socle qui accueillera à terme l'ensemble des jumeaux produits en France, publics ou privés. À condition que les financements suivent.



SOURCE IGN

Le vieux port de Marseille a déjà son jumeau numérique.

Réplique dynamique d'un territoire, le jumeau numérique, qui croise les données de terrain provenant de multiples sources, suscite aujourd'hui un vif intérêt tant chez les acteurs publics que privés. Il représente en effet un outil précieux pour orienter les décisions en matière de politiques publiques, notamment dans l'anticipation des défis environnementaux. Ces enjeux stratégiques ont été débattus lors de l'Université de la Transition Numérique des Territoires de la Fédération InfraNum, mi-septembre. D'autant que, sous l'impulsion du Secrétariat Général pour l'Investissement (SGPI), qui pilote France 2030, un projet d'infrastructure-socle visant à interconnecter toutes les initiatives de jumeaux numériques en France et à mutualiser les ressources, a été lancé par l'IGN, le Cerema et l'INRIA. «*Initié voilà deux ans, ce projet va permettre à des acteurs – aussi bien publics que privés – ayant déjà développé leur jumeau numérique de venir s'appairer à cette infrastructure-socle. Aux acteurs qui n'ont pas encore engagé cette démarche, il évitera de repartir à zéro puisqu'il leur offrira la possibilité de s'emparer de données open data et de technologies open source comme la visualisation en 3D, mais également des premières briques de simulation disponibles*, a rappelé Rudy Cambier, chef du département Innovation et Partenariats industriels France/Europe à l'IGN. *Car l'enjeu même des jumeaux numériques réside dans leur capacité à simuler des scénarii comme l'impact du dérèglement climatique sur des zones géographiques, des infrastructures, des bâtiments ou encore des zones agricoles ou forestières.*» Le projet bénéficie par ailleurs du soutien du BRGM (Bureau de Recherches Géologiques et Minières) et du CNES, ainsi que de plusieurs entreprises qui vont participer à l'élaboration de l'infrastructure-socle, parmi lesquelles 1Spatial, IGO, LuxCarta et Siradel.

Une politique de commun numérique

Afin de cartographier l'écosystème des jumeaux numériques en France et de prioriser un certain nombre de cas d'usage, ces trois partenaires ont lancé un appel à communs en mai 2024 lors du salon VivaTech. Son objectif était également d'adresser les collectivités moins en capacité d'investir massivement et de prendre en compte la diversité géographique et géologique du territoire français : zones urbaines, périurbaines, rurales, forestières, littorales et montagneuses. «*La plupart du temps, ces zones sont quelque peu oubliées et mises de côté*, souligne Rudy Cambier. *Alors que la continuité territoriale doit être assurée avec les jumeaux numériques.*»

Le projet a pour vocation de développer un modèle économique hybride public-privé, qui ira au-delà du financement de France 2030. «*Le SGPI ne subventionne pas, il investit dans l'économie d'avenir. Un des enjeux du projet est notre capacité à le développer avec une gouvernance "public-privé-recherche" dans laquelle des industriels comme des acteurs publics et de la recherche auront intérêt à travailler avec nous et à investir pour pérenniser l'infrastructure.*»

La construction de l'infrastructure-socle devrait démarrer au cours du premier trimestre 2026 et se poursuivre sur trois ans. Parallèlement, les premiers cas d'usage seront développés progressivement sur la macro-architecture déjà en place, sur laquelle les partenaires travaillent depuis deux ans. Pour cela, il faudra que les financements suivent, or les incertitudes politiques du moment bloquent pour le moment les prises de décisions.

La Commission européenne a de son côté déjà mis en place une boîte à outils numérique locale, la Local Digital Twin (LDT), fondée sur l'interopérabilité, l'ouverture et l'évolutivité. Elle est destinée à aider les territoires souhaitant créer leur propre jumeau numérique. Quant à l'Union européenne, elle porte un projet encore plus ambitieux : un jumeau numérique de la Terre, Destination Earth (DestinE), dont la version initiale a été lancée en juin 2024.

PATRICIA DREIDEMY

Emmanuel Sardet

Président du Cigref

Un an après son élection à la présidence du club, Emmanuel Sardet dresse un premier bilan. Entre dépendances numériques, surabondance réglementaire, initiatives européennes, il appelle les grandes entreprises et administrations à développer leur autonomie stratégique et à jouer un rôle dans l'émergence d'un écosystème numérique européen crédible, au bénéfice de la croissance et de l'innovation.

Propos recueillis par **THIERRY DEROUET** *Photos* **MAŸLIS DEVAUX**

« Notre autonomie stratégique *doit se construire maintenant* »

LE RISQUE, C'EST D'EMPILER LES TEXTES COMME DES POUPÉES GIGOGNES, SANS LOGIQUE D'ENSEMBLE

Comment conciliez-vous votre rôle de président du Cigref (Club informatique des grandes entreprises françaises) avec vos responsabilités professionnelles au Crédit Agricole ? Qu'est-ce que cela vous apporte ?

Les deux rôles sont très synergiques. Certes, cela prend plus de temps que si je me consacrais uniquement à mon métier, mais la richesse est réelle : l'intelligence collective, le contact avec l'écosystème, les travaux d'influence, les réflexions communes... C'est d'ailleurs pour cela que le Crédit Agricole est adhérent du Cigref : cela complète et nourrit mon action au sein du Groupe.

Le rôle de président et celui que chacun exerce dans son entreprise ou son administration constituent un voyage commun. Un voyage qui enrichit, qui fait grandir, et qui donne plus de sens à nos responsabilités respectives.

L'étude du Cigref sur les dépendances numériques a suscité le débat, mais elle les a surtout chiffrées : 264 Md€ de coûts pour l'Europe. Quelle était la finalité de ce travail et quelles suites en tirez-vous ?

Cette étude n'était bien sûr pas là pour apprendre à nos adhérents qu'ils étaient dépendants : chaque DSI en a une conscience intime au moment de reconduire un budget ou d'intégrer une innovation. L'objectif était de prendre conscience collectivement de cette situation et de proposer pour la première fois un cadre de mesure. C'est assez frappant : il n'existe pas d'outil pour évaluer ces flux, qui échappent aux balances commerciales.

Certes, la méthode a ses biais et ses approximations, mais elle tend la main aux décideurs publics, aux fournisseurs et aux consommateurs que nous sommes : si l'on veut que ce cadre normatif soit utile, il faut l'améliorer ensemble.

Surtout, c'est un appel à l'action concrète, opérationnelle : comment mieux orchestrer notre autonomie stratégique ? Cela veut dire réduire les risques, planifier, quantifier la dépendance, se donner des marges de manœuvre et explorer les alternatives. Certains évoquent 10, 15 ou 20 % d'achats européens. Le vrai enjeu, c'est de transformer cette intuition quotidienne en stratégie de résilience et d'autonomie.

Quel distinguo faites-vous entre autonomie stratégique et souveraineté européenne ?

L'autonomie stratégique, c'est le traitement concret des risques de dépendance, qui nous font perdre nos marges de manœuvre, favorisent les positions dominantes et freinent l'innovation. C'est le vrai sujet pour les entreprises et les administrations. La souveraineté, elle, est attachée à un territoire et à un État, ou à une délégation d'autorité au niveau européen. Beaucoup d'acteurs ont donc un agenda de souveraineté, car nous opérons sur un territoire, en France, en Europe, avec nos collaborateurs et nos ressources locales. Mais tout ne passe pas par un écosystème souverain.

Être un fournisseur européen ne fait pas toujours de vous un modèle. Demandez aux DSI industriels confrontés aux éditeurs de progiciels

supply chain : leurs pratiques ne sont pas toujours plus vertueuses que celles des grands acteurs américains du cloud. Mais le Cigref en est convaincu, c'est avec une alternative crédible, européenne plutôt que nationale, que nous créerons de la valeur et réduirons les risques de dépendance.

Vous avez mis en garde contre la multiplication des réglementations et l'inflation de charges administratives qui en découle. Comment éviter que les entreprises soient étouffées par NIS 2, DORA, CRA et autres textes européens ?

Le risque, c'est d'empiler les textes comme des poupées gigognes, sans logique d'ensemble. Aujourd'hui, le SecNumCloud en France, l'EUCS au niveau européen... On additionne ou on juxtapose des cadres, chacun avec ses spécificités. Et pour les grandes entreprises qui opèrent dans plusieurs pays, c'est vite infernal.

Notre priorité, depuis un an, c'est de travailler au niveau européen avec nos associations sœurs – Beltug en Belgique, Voice en Allemagne, CIO Platform Nederland. Nous ne sommes que quatre, alors qu'il pourrait y en avoir vingt-sept, mais cette union est essentielle (*). Nous voulons pousser une voie unifiée, pour éviter une fragmentation réglementaire coûteuse et inefficace.

Un autre combat, c'est de repousser la charge de la conformité vers les fournisseurs. Il n'est pas acceptable qu'ils accèdent au marché européen sans intégrer ces règles by design. Aujourd'hui encore, quand on demande à un fournisseur : *« Quelle est votre offre pour une banque en Europe soumise à DORA ? »*, il répond : *« Voici mon produit, et ensuite on verra comment vous vous mettez en conformité. »* Même chose avec le CRA (Cyber Resilience Act). S'il n'est pas appliqué correctement, il risque d'augmenter la charge des DSI au lieu de les soulager de certains risques.

Il faut que la conformité devienne un argument commercial : les acteurs qui intégreront ces exigences dès la conception gagneront en attractivité. Et en parallèle, nous travaillons avec les régulateurs pour simplifier : réduire la complexité, harmoniser au niveau européen, éviter qu'il y ait vingt-sept implémentations différentes. Les États-Unis le font pour eux, la Chine le fait pour elle. L'Europe doit en être capable aussi.

Après l'acquisition de VMware par Broadcom, vous avez alerté la Commission européenne sur les risques de pratiques anticoncurrentielles. Comment anticiper et se prémunir de ce type de dépendances critiques ?

L'histoire Broadcom était à la fois inacceptable, prévisible et attendue. Non pas que ce soit dans l'ordre des choses, mais parce que la stratégie de Broadcom était limpide dès son annonce du rachat de VMware en mai 2022. Elle a été exécutée point par point : hausse brutale des prix, suppression d'offres ou de produits, clients placés devant le fait accompli.

Ce n'est pas illégal à ce stade. Nous avons saisi la Commission européenne avec nos homologues européennes dès 2022, mais pour Bruxelles, *« même si un fournisseur fait x5000 sur ses tarifs, ce n'est pas une preuve de position dominante »*. Le vrai sujet n'est pas seulement le prix, c'est l'ensemble des leviers employés pour verrouiller le marché.

Comment s'en prémunir ? Certaines grandes entreprises, comme le Crédit Agricole, ont les moyens de décider une sortie de produits, même

PARCOURS

Depuis octobre 2024 : président du Cigref

Depuis 2023 : DSI adjoint du groupe Crédit Agricole et group CTO.

2019 – 2023 : pour le groupe Crédit Agricole, directeur général de CA-GIP, l'entreprise technologique du groupe.

2001 – 2018 : partner chez Accenture, en charge d'activités de stratégie et de transformation IT, de conseil en technologie et d'infogérance pour les grands clients de l'industrie financière.

1996 - 2000 : directeur chez GE Capital Consumer Finance, en charge de programmes de transformation mêlant métiers et informatique.

1993 – 1996 : débuts au sein du groupe Paribas : stratégie, contrôle interne, développement commercial.

FORMATION

Ingénieur diplômé de Télécom ParisTech, spécialité IA (1993)

si cela fait très mal. Mais si l'entreprise est petite ou moyenne, elle subit beaucoup plus. Il faut donc préparer en amont des alternatives, y compris des ruptures brutales.

C'est une culture que nous n'avons pas encore en Europe : nous aimons les relations de long terme, de confiance avec nos fournisseurs. Mais il va falloir apprendre à faire différemment. Exiger la portabilité, inscrire dans les contrats l'absence de frais de sortie. Et s'appuyer sur des socles réglementaires comme le Data Act (adopté en 2023, qui impose la portabilité des données et encadre l'accès aux données industrielles) pour rééquilibrer les rapports de force.

Le vrai risque, c'est que le succès boursier de Broadcom inspire d'autres fournisseurs dans l'IA, la data ou le cloud. Il faut donc panser nos blessures, mais surtout se préparer à éviter d'autres «cas Broadcom» dans les cinq ans qui viennent.

Vous avez soutenu Eurostack et la Suite numérique, portés par la Dinum, en tant qu'alternatives européennes. Quels rôles peuvent-elles jouer pour les DSI et avec quelles limites ?

Ces initiatives, toutes imparfaites qu'elles soient, sont à saluer. Leur objectif, c'est de faciliter l'apparition d'un cadre qui permette aux DSI de gagner du temps. Elles peuvent choisir une solution en sachant qu'elles n'auront pas à le regretter plus tard en termes de conformité ou de protection.

Certains voudraient que ce soit un supermarché idéal, bien organisé et garanti par l'État. Ce n'est pas le vrai monde. La réalité, c'est que vous ouvrez le supermarché, et vous découvrez que la grande allée est surtout remplie de produits américains... Ce sont eux qui sponsorisent la logistique. Cela ne veut pas dire que l'idée est mauvaise. Au contraire, il faut se dire : prenons-nous en main. Les grandes entreprises et administrations ont la capacité de se fédérer, d'adopter des comportements qui favorisent l'émergence d'acteurs européens crédibles, sans attendre uniquement des initiatives publiques. Regardez GAIA-X : cela donne un cadre normatif, bien construit, pour que des entreprises et acteurs publics partagent en confiance, et cela a permis l'éclosion d'un écosystème d'acteurs de solutions et services. C'est vertueux.

Mais il y a un travers typiquement européen – et français – qui consiste à subventionner l'incertitude du marché et à espérer que les champions soient désignés à l'avance. Le rôle de l'action publique, c'est plutôt d'être exemplaire : appliquer elle-même les solutions qu'elle promeut et éviter de morceler l'écosystème. Nous avons besoin de consolidation, pas de dispersion. Un acteur uniquement français ou allemand ne nous sert à rien. Il en faut qui soient capables d'entrer en compétition au niveau européen, avec des écosystèmes solides, crédibles, et soutenus par des comportements d'achat cohérents des grandes entreprises.

L'apparition de nouvelles régulations européennes suppose des compétences accrues. Comment le Cigref peut-il aider les DSI et leurs équipes à s'y préparer ?

C'est un sujet central. Chaque année, nous travaillons avec près de 4000 collaborateurs des entreprises et administrations qui participent à nos ateliers à produire des guides opérationnels : comme récemment, sur la mise en œuvre de l'AI Act.

Nous avons aussi lancé un nouveau cycle sur

la manière de comprendre et d'intégrer les règlementations européennes. La Commission européenne publie énormément d'appels à contribution. Or les entreprises y répondent en ordre dispersé, pensant que les associations professionnelles verticales le feront plus globalement pour elles. C'est une erreur car pendant ce temps, les lobbyistes sont très structurés.

Il nous faut donc contribuer plus directement, mais encore faut-il savoir comment. Est-ce le rôle des affaires publiques ? Des informaticiens ? Des juristes ? Des acheteurs ? Des risk managers ? On voit une grande hétérogénéité d'organisation selon les entreprises. Notre mission est de faire gagner du temps par la pédagogie notamment : partager des retours d'expérience, produire des publications utiles à nos membres, mais aussi aux plus petites entreprises. Le guide de l'audit des SI est devenu une référence au-delà du Cigref ; et celui des métiers du numérique est utilisé par beaucoup de DRH. Imposer ces références nous permet aussi de peser auprès des fournisseurs, pour les inciter à aligner leurs offres sur nos exigences.

Reste un chantier immense : influencer en amont la création des compétences, depuis l'université jusqu'à l'entreprise. En France, le décalage reste criant entre la formation académique et les besoins réels des entreprises. Les jeunes diplômés arrivent avec des savoirs qui ne correspondent pas toujours aux métiers créés. Cet écart à l'entrée est très compliqué à réduire.

Quels seront les grands enjeux pour l'année à venir ?

Trois priorités ressortent clairement. D'abord, renforcer encore le lien avec nos 160 membres. Le Cigref grandit, et nous devons être en prise directe avec leurs besoins réels. Nos adhérents ne veulent pas seulement que nous débattions du DMA ou de l'AI Act avec Bruxelles : ils attendent que nous transformions ces textes en outils pratiques qui leur permettent de se développer.

Ensuite, il y a un agenda européen. Nous travaillons main dans la main avec nos associations sœurs en Belgique, en Allemagne et aux Pays-Bas. L'objectif est clair : éviter une fragmentation réglementaire et peser collectivement pour simplifier et harmoniser les cadres, au bénéfice de toutes les entreprises.

Enfin, il y a la transformation de l'écosystème des fournisseurs numériques. Nous devons aider les DSI à reprendre la main sur l'adoption de l'innovation, à choisir quand et comment elle crée de la valeur, et à réduire la part des dépendances.

À titre professionnel, au Crédit Agricole, je vis cela de manière très concrète : le Groupe est ancré dans les territoires, face à des défis majeurs, mais avec une capacité unique à accompagner la rupture numérique au bénéfice de nos clients, de nos marchés et de nos pays. C'est passionnant de transformer ces défis en opportunités. Et à titre plus personnel ? Ce qui me fait courir, ce n'est pas de voir la capitalisation boursière d'un fournisseur s'envoler. C'est de constater que le numérique, lorsqu'il est bien pensé, bénéficie aux citoyens, aux entreprises et aux territoires. C'est là que réside l'aspect vertueux de notre action. ■

(*) Les secondes rencontres numériques de Strasbourg, organisées en avril dernier avec Numeum, ont accueilli pour la première fois ces trois associations « sœurs » du Cigref.

Retrouvez l'intervention d'Emmanuel Sardet dans la matinale d'*IT for Business*, le 18 septembre 2025.

apidays PARIS

APIdays Paris | 9–11 déc.
× Les Rencontres de la DSI | 9 déc.

3 jours pour accélérer. 1 jour pour décider.

APIdays Paris est le rendez-vous européen des APIs, de l'IA et des architectures cloud-native.
Au sein de APIdays Paris, Le 9 décembre, "Les Rencontres de la DSI" offrent des ateliers confidentiels entre DSI, CTO et RSSI pour transformer les enjeux en plans d'action — sécurité proactive, data/IA utile, maîtrise des coûts, expérience employé & client.

À la clé : Frameworks, KPIs, contacts.

À court terme : AP quick wins.

À 12 mois : AP

Pour s'inscrire :

https://dsidelannee.fr/rencontresdsi.html

Coupon discount 50% exclusif
pour les lecteurs d'IT For Business Magazine

ITFORBUSINESS50

talents

Comment resouder le binôme RH-IT

PAGE 24

LES MOUVEMENTS DU MOIS

Erwan Rolland

Commissaire au Numérique de Défense

Il débute sa carrière comme officier de transmissions et voit ses responsabilités s'élargir progressivement. Il est notamment à la DGIC à partir de 2006 puis directeur central adjoint de la Dirisi (2023) et enfin directeur central (2024). À la tête du CND qui rassemble depuis août l'ensemble des forces numériques de la Défense nationale à l'exception de ce qui relève de l'État-major, le général de corps d'armée Erwan Rolland est diplômé de l'Académie Militaire de Saint-Cyr Coëtquidan (1993).

Victor Kerr

DSI de Storengy

Après des débuts comme ingénieur réseau et sécurité chez Devensys puis SCC, il devient consultant chez Wavestone à partir de 2016. En 2020, il avait rejoint le groupe Engie, maison mère de Storengy, en tant que responsable gouvernance, risques et compliance cybersécurité, avant d'accéder au poste de responsable de la transformation cyber en 2023. Victor Kerr est détenteur d'un master en ingénierie informatique de Supinfo (2014).

Dimitri Chevtchenko

DSI Belambra

D'abord ingénieur systèmes et réseaux chez Neurones puis Euris, il entre à l'Inrap à partir de 2010. En 2014, il arrive chez le spécialiste de la formation en ligne Skill and You, comme responsable infrastructures. Il en devient CDIO à partir de 2021. En 2023, il rejoint Chateauform en tant que DSI. Dimitri Chevtchenko est diplômé de l'AFTI (CFA de Thales, Orange et Alcatel notamment) en 2006 et du Cnam.

Raphaël Viard

CDIO Forvia (Fusion Faurecia-Hella)

Après des débuts de chef de projet au ministère de l'Intérieur, il rejoint Alstom en 2005 comme responsable sécurité IT et télécom. Il y évolue et sera notamment CIO/VP de sa BU ITSC en 2015. CTO pour la SNCF (2016) et responsable de la transformation à partir de 2018, on le retrouve en 2019 chez Saint-Gobain HPS comme CDIO. Il avait rejoint Bouygues Construction comme CDO fin 2024. Raphaël Viard est diplômé de l'Epita (2002) et titulaire d'un mastère de Télécom Paris (2002).

Xavier Le Bleu, DSI depuis 1998

« C'est en codant que je suis devenu… ce que je suis »

Piqué au vif ou presque. Pour avoir été en contact avec des enfants qui montraient, contrairement à lui à cette époque, une grande aisance dans la programmation des ordinateurs comme le TO7/MO5 de Thomson dans les années 80, Xavier Le Bleu s'est pris au jeu. *«J'ai trouvé un livre expliquant le langage Basic et je m'y suis mis»*, se rappelle-t-il aujourd'hui. Et d'en sourire : *«Je n'ai donc pas eu la vocation à l'âge où on veut devenir pompier à 10 ans, mais au moins, à partir de cette période, j'ai su ce que je voulais faire.»*

Une Miage obtenue en 1989, un premier séjour en entreprise et des expériences de déploiement sur le terrain d'un logiciel pour les concessions automobiles plus tard, le voici au moment de la première Guerre du Golfe à la croisée des chemins. *«J'ai alors monté une SSII, me suis battu pendant deux ans, avant d'arriver à la conclusion qu'il valait mieux retourner chez mon employeur précédent.»* Surtout que c'est l'époque des réseaux Novell et qu'il en met beaucoup en place : *«C'était une technologie remarquable par sa fiabilité. Dommage qu'elle n'ait pas eu par la suite tout le succès mérité.»*

Au tournant du siècle, il est d'abord responsable informatique dans une PME industrielle, avant de devenir DSI d'un groupe belge qui se développe en France notamment, mais aussi beaucoup à l'international. Il y restera 19 ans au total, construisant une équipe qui va compter plus de 60 personnes, et déployant les solutions sur de nombreux sites, y compris à l'étranger.

Le syndrome de la cinquantaine le rattrape et après une période sabbatique appréciée, il décide que c'est vraiment le rôle de DSI auquel il tient le plus. Ce sera d'abord au travers de missions de transition, avec à chaque fois la satisfaction d'intervenir en «urgentiste», dans des situations où le temps presse et où la tech apporte des solutions souvent pertinentes à la crise. Ses missions lui permettent aussi de prendre du recul, comme lors de cet audit qu'il réalise chez Tunstall-Vitaris, N°1 de la téléassistance senior, qui lui proposera ensuite un poste de DSI internalisé. Cette mission, achevée aujourd'hui, lui a une nouvelle fois permis de vérifier son goût pour le bel ouvrage technique, mais aussi l'intérêt de suivre les projets sur le long terme, un luxe généralement inaccessible pour le manager de transition qui repart une fois le SI relancé. Dans cet univers varié et mouvant de la tech, savoir où l'on veut aller est assurément une force.

FRANÇOIS JEANNE

PARCOURS

Depuis 2023 : auditeur (indépendant) puis DSI de Tunstall-Vitaris

2022 – 2023 : coordinateur DSI au LFB (Laboratoire Français du Fractionnement et des Biotechnologies)

2019 – 2022 : DSI de Dalloyau

2018 – 2019 : DSI de transition chez Airfoils Advanced Solutions (JV Safran/Air France)

1998 – 2017 : DSI de Sibelco France

1996 – 1998 : RSI chez Tissus Techniques de Trévoux

1994 – 1995 : superviseur de migration pour Datafirst (éditeur)

1992 – 1994 : gérant et fondateur de la SSII Netland

FORMATION

C.I.G. (MIAGE), Informatique de gestion (CCI de Besançon, 1989)

La place de la technologie dans votre parcours ?

Essentielle, depuis le début. Je me suis toujours attaché à maîtriser la machine, les langages et les systèmes associés, c'est un sentiment grisant. Par ailleurs, lorsque l'on doit gérer des équipes IT, être passé par la technique rend le discours beaucoup plus crédible et légitime, car on connaît les difficultés.

Votre vision du rôle de DSI ?

J'y ai beaucoup réfléchi, en profitant d'un moment sabbatique il y a une dizaine d'années. Ce mélange de projets à mener, d'animation d'équipes, de stratégie et d'optimisation budgétaire, me plaît vraiment. Surtout si, comme c'est généralement le cas, la dimension technique reste omniprésente et prépondérante.

Fervent du management de transition ?

Le positionnement est intéressant pour celui qui apprécie les missions commandos, avec souvent une forte composante techno. L'autre versant, c'est que cela impose mobilité et disponibilité immédiate, même si avec le télétravail on peut aujourd'hui réduire un peu cette contrainte.

Un livre qui vous a marqué récemment ?

Cela va vous faire sourire. Je suis un grand lecteur d'ouvrages techniques. Récemment, j'en ai étudié un qui m'a permis d'apprendre à bien coder en Python pour programmer les Raspberry Pi.

CONDUITE DU CHANGEMENT

Face à l'IA, les salariés se sentent insuffisamment accompagnés

Près de trois ans après l'arrivée de ChatGPT, où en est l'adoption de l'IA générative en entreprise ? D'après une étude menée par ChooseMyCompany, en partenariat avec Rennes School of Business et Crédit Mutuel Arkéa, les 13 000 salariés français interrogés lui réservent un bon accueil pour peu que son déploiement soit accompagné d'une vraie politique de conduite du changement.

69 % des collaborateurs utilisent déjà l'IA dans leur quotidien professionnel, et 64 % estiment qu'elle aura un impact positif sur leur métier. Pour autant, alors que l'IA bouleverse les codes du travail, ils sont dans une proportion sensiblement similaire (63 %) à ne pas se sentir suffisamment accompagnés dans cette transition.

Ce constat diffère selon le secteur d'activité. Le niveau d'engagement bondit dans les entreprises des services, de l'audit ou du digital où l'IA est bien intégrée. À l'inverse, les acteurs de la fonction publique, de la santé ou de la logistique accusent, selon l'étude, un retard, qui, *« quand il n'est pas lié à la nature du poste, est souvent dû à des restrictions d'accès ou des freins culturels »*.

Cette frustration est de nature à nourrir la « shadow AI ». Selon une autre enquête, conduite cette fois par Ipsos pour Greenworking, seuls 32 % des utilisateurs emploient systématiquement les outils d'IA générative homologués par leur entreprise. Une dérive d'autant plus préoccupante que nombre d'entre eux n'informent ni leurs managers (seulement 55 %), ni leurs clients (43 %) lorsqu'ils utilisent l'IAGen dans le cadre professionnel.

FORMATION

Paris School of AI forme les experts en IA de demain

La Paris School of AI a fait sa première rentrée des classes le 1er septembre dernier. Ce nouvel établissement de l'université Paris Sciences et Lettres (PSL) a pour ambition de former *« des experts en IA de haut niveau et des profils interdisciplinaires »* afin de *« répondre aux enjeux de demain et penser les nouveaux usages »*.

Le programme couvre, de fait, un large spectre de disciplines allant des mathématiques aux sciences humaines en passant par l'informatique, les sciences cognitives, l'économie ou encore le droit et l'éthique. La Paris School of AI propose une offre complète en formation initiale – licence, master, doctorat – et continue. La première promotion compte 30 étudiants avec, pour objectif, de monter à 150 dans les prochaines années.

LIVRE

Quel droit pour nos identités virtuelles ?

À la fois philosophe, psychanalyste et essayiste, Elsa Godart apporte un éclairage original sur l'impact des technologies numériques sur nos modes de vie, nos interactions sociales et professionnelles. ***« L'intelligence artificielle ne se limite pas à automatiser des tâches, elle façonne des comportements originaux, influence les décisions et redéfinit les rapports de pouvoir »*****, estime cette chercheuse qui a cofondé avec Pierre-Antoine Chardel, l'Institut de recherche en éthique du sujet numérique (IRESN). Est-ce que l'individu est réduit à l'état de données parmi d'autres ou bien reste-t-il un acteur capable de se définir et de se projeter librement ? Face à ces mutations profondes, Elsa Godart propose d'ériger une déclaration universelle des droits et des devoirs du citoyen numérique.**

Éditions Hermann*, 314 pages*

Face au renouvellement accéléré des technologies, les RH se sentent légitimement dépassés par la complexité des métiers de la tech. Ce décrochage a des conséquences négatives sur le recrutement et les parcours de carrière des collaborateurs de la DSI. Adrien Nortain, CTO de Zenika, appelle donc à revoir le contrat passé entre la DRH et la DSI.

Comment resouder le binôme RH-IT

Il y a vingt ans, les relations entre la DSI et la DRH étaient simples. La première demandait à la seconde de recruter des «développeurs» aux contours de poste bien bordés. Depuis, le renouvellement accéléré des technologies a changé la donne, avec une hyperspécialisation des métiers. «*Aujourd'hui, il faut savoir distinguer un SRE d'un DevSecOps, un architecte cloud d'un ingénieur MLOps, un product owner d'un engineering manager*», avance Adrien Nortain, CTO de l'ESN Zenika.

La nomenclature du Cigref version 2024 compte ainsi 52 descriptions de profils métiers dont chacun peut jouer plusieurs rôles distincts. «*Le poste d'expert DevOps revêt, par exemple, différentes réalités*, illustre Adrien Nortain. *Il peut intervenir sur l'automatisation des processus ou la modernisation de l'architecture technique. Et selon le stade dans le cycle de vie d'un projet, une organisation aura besoin d'un ingénieur ou d'un architecte DevOps.*»

Dépassés par ces subtilités et la complexification des métiers de la tech, «*les DRH ont progressivement délégué aux DSI la sélection des profils, voire la rédaction des fiches de poste*». Un désengagement lourd de conséquences selon le CTO. Les profils tech ne sont plus évalués selon une culture RH basée sur les compétences comportementales comme l'adaptabilité, le leadership, le sens du collaboratif. Par ailleurs, «*les managers techniques se retrouvent à piloter seuls des recrutements sans accompagnement structuré*».

S'il ne leur demande pas de savoir coder, «*les RH ne peuvent plus se permettre de ne pas comprendre les métiers pour lesquels ils recrutent*». Ne pas savoir distinguer un développeur front d'un ingénieur cloud, ou ce qui relève de l'effet de mode – blockchain – d'une tendance lourde – cloud, IA, cybersécurité – constitue, à ses yeux, un angle mort dangereux.

Adrien Nortain, CTO de Zenika : «*Les RH ne peuvent plus se permettre de ne pas comprendre les métiers pour lesquels ils recrutent.*»

Au recrutement volumique et industrialisé, réalisé par des recruteurs RH généralistes, il oppose un modèle qualitatif, plus lent et coûteux, mobilisant des recruteurs acculturés aux métiers de l'IT voire issus de la tech. Il voit d'ailleurs émerger dans certaines DSI des «tech talent partners», des «HR business partners» ou des binômes RH/lead tech sur les postes critiques.

Ce serait d'autant plus profitable que ce manque de vision RH ne s'arrête pas au recrutement. Le parcours d'intégration, puis les programmes de gestion des talents, par trop génériques, en souffrent aussi. À la question «*quelle est la prochaine étape de mon évolution professionnelle ?*», on renvoie souvent l'informaticien à la fameuse «échelle de carrière», basée sur des étapes de progression hiérarchique. C'est une nouvelle fois oublier les spécificités des métiers de l'IT et la valorisation de la voie de l'expertise. «*Il ne faut pas s'arrêter aux trajectoires types, mais adapter les évolutions de carrière au profil du professionnel, à ses performances et ses aspirations*», estime Adrien Nortain.

Là-encore, le binôme DSI-DRH permet selon lui d'offrir davantage d'agilité organisationnelle. La DSI fixe des enjeux de montée en compétences par rapport à ses priorités technologiques, puis la DRH travaille sur la définition des postures et des soft skills associées. Le CTO de Zenika prône également la culture du partage et de la veille technologique. Ce modèle d'organisation apprenante doit notamment permettre aux profils exécutants, gérant le legacy et donc peu confrontés aux innovations technologiques, de briser le plafond de verre qui les enferme.

XAVIER BISEUL

Abonnez-vous

IT for Business

Le média des managers du numérique

Offre Full Digital

- Le magazine en ligne
- Nos archives numériques en PDF
- Contenus réservés à la communauté
- La newsletter hebdo

1 an 160 € HT

Offre Full Digital & Print

- Le magazine en ligne
- Nos archives numériques en PDF
- Contenus réservés à la communauté
- La newsletter hebdo

\+ 11 numéros/an d'IT for Business

1 an 200 € HT
2 ans 360 € HT

OUI, je m'abonne

- ☐ Abonnement **Full Digital 1 an** | 163,36 € TTC *
- ☐ Abonnement **Full Digital & Print 1 an** | 204,20 € TTC *
- ☐ Abonnement **Full Digital & Print 2 ans** | 367,56 € TTC *

Je règle:

- ☐ À réception de facture
- ☐ Par chèque bancaire à l'ordre d'IT for Business
- ☐ Par CB, prélèvement SEPA ou Apple Pay (flashez le QR Code ci-contre)
  www.itforbusiness.fr/abonnes
- ☐ Je souhaite recevoir une facture acquittée

Bulletin d'abonnement à adresser à
IT for Business – Service Abonnements
6, rue de Lisbonne, 75008 Paris
01 53 05 93 83 | contact@itforbusinessabonnement.fr

DATE ET SIGNATURE OBLIGATOIRE

☐ Madame ☐ Monsieur

NOM

PRÉNOM

E-MAIL (obligatoire pour bénéficier de nos services en ligne)

SOCIÉTÉ

FONCTION

CP **VILLE**

TÉL.

Si l'adresse de facturation est différente de celle de la livraison, merci de nous le préciser.

- ☐ J'accepte de recevoir par mail des offres promotionnelles de la part d'IT for Business
- ☐ J'accepte de recevoir par mail des offres promotionnelles de la part des partenaires d'IT for Business

* TVA 2,10%. Offre valable jusqu'au 31/12/2025 pour les nouveaux abonnés en France métropolitaine uniquement. L'éditeur s'engage à livrer votre magazine sous un délai maximum de 5 semaines. Les informations sont nécessaires à IT for Business pour traiter votre commande et les services qui y sont associés. Ces informations sont enregistrées dans notre fichier clients et peuvent donner lieu à l'exercice du droit d'accès, de rectification et de suppression auprès du service Abonnements au moyen d'un e-mail adressé à : contact@itforbusinessabonnement.fr conformément à la loi « informatique et libertés » du 6 janvier 1978 telle que modifiée en 2004. L'Éditeur se réserve le droit de modifier le contenu, le titre ou le format de la publication objet du présent abonnement, dans le respect de son actuelle ligne éditoriale. Conformément à l'article L 121-20-2, 5° du Code de la consommation, vous ne bénéficiez pas d'un droit de rétractation. Les demandes de résiliation anticipée et de remboursement ne seront prises en compte que dans le seul cas d'un motif légitime dûment justifié. Les demandes sont à adresser exclusivement par simple courrier à l'attention du service Abonnements à l'adresse suivante : IT for Business – Service Abonnements – 6, rue de Lisbonne, 75008 Paris.

Les DSI de l'année

27e Édition

Rendez-vous à **l'Hôtel de Ville de Paris,** le 12 mars 2026

Le rendez-vous incontournable des managers du numérique

27e édition

La cérémonie des DSI de l'Année se tiendra le 12 mars 2026 dans le cadre prestigieux de l'Hôtel de Ville de Paris. Un lieu emblématique pour célébrer celles et ceux qui incarnent une DSI visionnaire, résiliente et engagée face aux grands défis de notre époque.

dsidelannee.fr

Inscrivez-vous pour une soirée inoubliable, où l'innovation technologique rencontre le patrimoine national :
dsidelannee.fr

Un évènement IT for Business avec le concours du Cigref, French Women CIO et AtoutDSI

DOSSIER SPÉCIAL

IT for Business

CYBER

SÉCURITÉ

LA QUÊTE DES ÉQUILIBRES

Dossier spécial réalisé par **XAVIER BISEUL, ALAIN CLAPAUD, LAURENT DELATTRE, THIERRY DEROUET, PIERRE FONTAINE, FRANÇOIS JEANNE, AUDE LEROY** *et* **CHARLOTTE MAUGER**

Des attaques qui se multiplient, des surfaces d'exposition qui s'élargissent, et une IA qui renforce l'arsenal des hackers… Ils pourraient baisser les bras, mais les RSSI ne lâchent rien. C'est en utilisant la pression réglementaire comme un catalyseur, en diffusant la culture cyber dans l'entreprise et en rebâtissant inlassablement de nouvelles défenses, qu'ils espèrent et peuvent reprendre la main.

Anticiper et innover pour ne plus subir, *le Graal de la cybersécurité*

L'été sera chaud, disait le chanteur. L'année prochaine, sûrement. Mais dès cette année, et comme la précédente, elle fut déjà brûlante sur le front des attaques cyber. Impossible de dresser ici la liste de toutes les entreprises qui ont subi des vols de données, d'autant qu'il y a fort à parier qu'elles ne les ont pas toutes déclarés à la CNIL. De quoi décourager les Comex, qui ont pourtant fini ces dernières années par accepter le coût de la sécurité des systèmes d'information, et souvent accueilli les RSSI en leur sein ? Sans doute et heureusement pas. Car même si certaines organisations, comme France Travail ou Auchan, ont dû reconnaître de nouvelles attaques réussies, quelques mois après une première intrusion, *« cela ne signifie pas que leurs RSSI n'ont pas travaillé depuis le premier événement,* analyse Emmanuel Cheriet, DG d'Intelcia ITS. *C'est juste que la surface d'attaque à protéger n'en finit plus de s'élargir devant eux. »*

Les réponses techniques des RSSI et des DSI, leurs alliés naturels dans l'entreprise, se sont étoffées

Pas de tout repos

Pas au point de baisser les bras tout de même. Mais la lecture de notre dossier confirme à l'envi que les professionnels de la cybersécurité n'ont pas une vie de tout repos. Les menaces arrivent de toutes parts, en particulier au travers des supply chain et des API, ou encore via des briques open source de plus en plus souvent présentes au sein des systèmes d'information ; sans oublier les failles ouvertes par des utilisateurs négligents et/ou mal informés. Elles changent aussi de nature ou, pour être plus précis, d'intensité, à cause de l'irruption de l'intelligence artificielle dans l'arsenal des hackers.

Face à cela, les réponses techniques des RSSI et des DSI, leurs alliés naturels dans l'entreprise – le rapprochement est récent ! – se sont également étoffées. Les XDR, la plateformisation des solutions ou encore le recours à l'IA pour analyser les codes suspects et prévoir des comportements agressifs leur permettent de faire bonne figure, à défaut de pouvoir se dire totalement sereins.

À la recherche des facteurs X

La situation semblerait presque figée, avec un jeu d'attaque/défense, une lutte éternelle entre les gendarmes et les voleurs, les bons et les méchants. Heureusement, des éléments nouveaux laissent espérer des évolutions en profondeur. À commencer par les progrès de la règlementation (si si !), qui dessine des chemins certes de plus en plus exigeants, mais aussi de plus en plus clairs pour les responsables des entreprises. Difficile désormais pour un Comex de refuser à un RSSI les moyens de se mettre en conformité si la sanction pécuniaire prévue devient élevée, ou pire, si comme c'est le cas avec Dora par exemple, le non-respect d'un règlement peut entraîner une inscription de l'entreprise en liste noire, avec une interdiction d'opérer sur les marchés.

Autre tendance, encore ténue mais majeure, la religion du

business first est enfin remise en question. Elle a conduit ces dernières années à des mises en place de solutions trop rapidement, voire à l'émergence d'une shadow IT bien difficile à contrôler. Il était alors compliqué pour un RSSI ou un DSI de s'opposer aux demandes et aux initiatives des métiers, systématiquement privilégiés en Comex. «*Mais l'ambiance est en passe de changer,* estime Emmanuel Cheriet. *Les nouveaux business à lancer font aujourd'hui l'objet d'analyse des risques cyber associés, à la fois en termes de coûts mais aussi d'image. Et j'ai même vu des directions métiers qui se faisaient taper sur les doigts pour leur imprudence.*»

De là à voir le RSSI comme une star écoutée des dirigeants, et la cybersécurité qu'il incarne comme une science exacte et respectée comme telle ? Sans doute pas, surtout tant que des attaques réussies et des vols de données feront régulièrement la une des journaux. Emmanuel Cheriet trouve le procès injuste, lui qui propose avec Intelcia ITS des solutions pour protéger, détecter, anticiper certes, mais pas de schémas directeurs : «*On est encore essentiellement en réaction dans les entreprises, pas encore dans la diffusion d'une culture de la cybersécurité qui permettrait de combattre les risques au plus tôt de leur origine.*» Un peu comme des pompiers qui n'ont pas forcément le temps d'inspecter les lieux sous leurs responsabilités en amont des incendies, et se «contentent» de les éteindre, alors que ces sinistres sont pourtant prévisibles...

Anticiper bien sûr, et aussi innover

Pourtant, et comme le rappellent les experts, il y aurait beaucoup à faire par anticipation. En identifiant les risques, notamment les failles qui sont restées non traitées dans le SI. Puis en établissant des priorités de traitement, en fonction de leurs coûts mais aussi du rapport entre ces coûts et les améliorations attendues. Il ne faudrait pas non plus oublier de préparer la réaction, car comme le dit l'adage désormais bien intégré, ce n'est pas la question du si qu'il faut poser, mais celle du quand.

Pour toutes ces démarches, il existe des méthodes et des appuis, à chercher du côté de l'ANSSI, des normes, voire sur les guides d'audit associés aux nouvelles réglementations. Les RSSI sont au travail bien entendu, et à leurs côtés, les DSI sont conscients que c'est en renforçant leurs pratiques en amont du développement, avec DevSecOps notamment, que les nouvelles failles pourront être limitées.

Limitées mais certainement pas éliminées totalement. «*La sécurité à 100% n'existera jamais*», rappelle Emmanuel Cheriet. Un constat qui ne doit pas empêcher de traiter le sujet, à commencer par la prise en compte du principal risque, à savoir le comportement des utilisateurs, «*responsables de 70% des failles. Mais il ne faut pas les braquer, ni les directions métiers*». Pour cela, Thierry Happe et son Predictive Cyberlab misent sur une approche innovante, avec un story telling qui doit impliquer différemment les collaborateurs et leur faire prendre conscience que la cyber n'est pas une affaire de techniciens exclusivement *(voir entretien ci-après)*.

D'autres vont beaucoup plus loin et méritent l'attention de ceux pour qui le positionnement du RSSI est intenable, notamment psychologiquement. À ceux-là, qui cherchent une issue à cette énième représentation du mythe de Sisyphe, suggérons la lecture de l'ouvrage *Anti-fragile, les bienfaits du désordre* de l'essayiste et scientifique Nassim Nicholas Taleb, qui revisite le mythe de l'Hydre de Lerne pour explorer les capacités de résilience et d'amélioration de systèmes – d'information – soumis au stress. Un auteur dont un précédent ouvrage traitait des «cygnes noirs». N'est-ce pas un signe effectivement ?

FRANÇOIS JEANNE

LES COMMANDEMENTS DU RSSI EN 2025

- **Protéger en particulier l'organisation contre les nouvelles menaces basées sur l'IA**
- **Sécuriser aussi l'IA, au niveau des usages mais aussi face aux menaces spécifiques qui la concernent**
- **Maintenir l'excellence opérationnelle des processus de cybersécurité déjà en place**
- **Agir sans nuire à l'agilité de l'entreprise et à ses prises d'initiatives business**
- **Auditer et sécuriser la chaîne d'approvisionnement en logiciels tiers et open source**
- **Tenir compte des réglementations en cours de déploiement, et de celles à venir**
- **Se protéger personnellement sur le plan juridique, par exemple au travers d'une assurance responsabilité civile des administrateurs et des dirigeants**
- **Obtenir les ressources adaptées aux besoins du moment, qu'il s'agisse de compétences ou de budget**
- **Défendre au plus haut niveau la place et le statut de la sécurité dans l'entreprise, donc celle du RSSI**
- **Ne rien lâcher sur le front de la sensibilisation et de la formation des utilisateurs**

Emmanuel Cheriet,
DG d'Intelcia ITS

«L'ambiance est en passe de changer dans les entreprises. Les nouveaux business à lancer font aujourd'hui l'objet d'analyse des risques cyber associés, à la fois en termes de coûts, mais aussi d'image.»

Thierry Happe

Président et fondateur du Predictive Cyberlab

« Il faut cultiver la lucidité des collaborateurs, *pas leurs peurs* »

Thierry Happe, à l'origine de l'Observatoire Netexplo, s'attaque cette fois à la cybersécurité avec son Predictive Cyberlab. Face à la complexification des cyberattaques, il prône un changement radical : faire de chaque collaborateur un acteur engagé, capable d'anticiper et de réagir aux menaces. Son approche remplace la culpabilisation pour susciter plutôt intérêt, compréhension et action, au bureau comme dans la vie personnelle.

Propos recueillis par **FRANÇOIS JEANNE** *Photos* **MAÏLIS DEVAUX**

IL FAUT DES COLLABORATEURS PLUS QUE SENSIBILISÉS, VÉRITABLEMENT MIS EN ACTION POUR DEVENIR DES « CYBER-ACTEURS »

Avec l'objectif de détecter les usages et les tendances émergentes autour du numérique, Thierry Happe a lancé puis dirigé pendant 15 ans l'Observatoire Netexplo en partenariat avec l'Unesco, 24 entreprises du CAC 40, et un réseau de 22 universités dans le monde. Après l'avoir cédé au groupe Les Echos en 2023, il crée Open C Future et lance fin 2024 le Predictive Cyberlab avec cette même philosophie, à savoir combattre les peurs autour de la technologie en suscitant au contraire de l'intérêt et des questionnements.

Comment votre Predictive Cyberlab entend-il de renouveler les approches autour de la cybersécurité ?

Il y a un écart grandissant entre les règles de sécurité prescrites dans les grands groupes et les pratiques réelles. Les RSSI ont plutôt bien fait leur travail sur la partie technique et la protection des SI, même si les attaques toujours plus sophistiquées ne permettent aucun relâchement. Mais aujourd'hui, 70% des cyberattaques reposent sur l'ingénierie sociale, c'est-à-dire la manipulation des comportements.

Pour couvrir cette autre dimension, il faut des collaborateurs plus que sensibilisés, véritablement mis en action pour devenir des «cyber-acteurs». Il leur faut comprendre et identifier les risques, être capables d'apporter des réponses, individuellement ou collectivement, par anticipation ou par réaction, pour créer une véritable résilience. Cela s'appelle la cybermaturité. Nous n'avons pas inventé le terme ; il a été développé, notamment au MIT, il y a quelques années. Et la cybermaturité, cela ne s'improvise pas : il faut la travailler et la développer.

Il faut donc des outils différents. Que proposez-vous ?

Concrètement, nous avons trois familles de livrables. La première, ce sont des séances dites de narrative design – c'est-à-dire une forme de design thinking centrée sur le récit – auxquelles les collaborateurs sont conviés. Le récit permet de faire bouger les gens. Si vous voulez une mise en action, il faut qu'ils puissent intégrer ces sujets dans leur manière de fonctionner et se les approprier. Aujourd'hui, ce n'est pas le cas : la «cyber» est vécue comme une contrainte, la cyber-fatigue est réelle. Et les campagnes de phishing avec leur logique culpabilisante ne sont pas forcément le meilleur outil pour faire évoluer les comportements. Nous avons donc choisi d'utiliser un film de fiction comme catalyseur, pour que les spectateurs imaginent à leur tour des scénarios, et se disent *«voilà ce qui pourrait arriver chez nous»*.

Le visionnage de ce film, par groupes d'environ 25 personnes, débouche sur la création d'un réseau de cyber-ambassadeurs ou de cyber-influenceurs, c'est aux entreprises de choisir le terme, qui ne seront surtout pas seulement des profils IT/cyber. Au contraire, tous les métiers sont représentés, sur tous les sites, en France et à l'étranger. Ces personnes vont jouer un rôle de relais. Nous les infor-

mons en priorité. Certaines ont déjà de l'appétence, d'autres découvrent le sujet et s'y intéressent progressivement.

Ce sont eux que nous avons invités à notre journée en présentiel en juin, où sont intervenus des experts, des entreprises, des représentants de la société civile, des hackers, pour explorer tous ces enjeux de la cybermaturité. Environ 400 personnes sont venues, majoritairement des cyber-ambassadeurs, dont certains confrontés pour la première fois à ces sujets, et notamment au rôle accélérateur des technologies. Les retours ont été très positifs parce que nous avons parlé un autre langage que celui des spécialistes. Le langage «cyber» n'est pas fait pour les non-initiés : si vous ne savez pas ce qu'est la MFA, si la terminologie vous paraît barbare, vous n'adhérez pas. Et si vous jouez sur l'angoisse et la culpabilité, vous n'embarquez personne.

Et le troisième livrable ?

Cet événement a marqué le début d'une communauté d'action pour anticiper collectivement les menaces et faire émerger des comportements plus efficaces face aux risques numériques. Car le dernier livrable, c'est un programme en ligne. Il n'est pas conçu comme une formation classique, mais à partir d'un film de fiction – toujours celui qui a servi d'introduction aux séances. Ce film vise à embarquer totalement, nous avons mis les moyens dans ce but : des scénaristes réputés, notamment Thomas Bidegain et Yannick Muller, et les apports de notre conseil scientifique pluridisciplinaire. Nous sommes allés assez loin dans la démarche : les acteurs jouent même dans une sorte de making-of pour expliquer comment ils se sont fait piéger. Ils prolongent leurs rôles. Et il y a des «hackers», en fait des acteurs également, qui expliquent comment ils ont piégé les gens. Le film appelle des questions de personnes qui ne se les posaient pas forcément. Il est suivi de documentaires, puis d'une validation des acquis en conclusion qui débouche sur la certification Predictive Cyber Engagement.

Qui fait partie de ce conseil scientifique ?

Vous y trouvez des personnalités comme Guillaume Poupard. Quand il a quitté l'ANSSI, il m'avait confié que ce qui avait joué le plus positivement dans le développement de l'agence, n'était pas venu de l'ANSSI elle-même, mais de la diffusion par Canal+ de la série *Le bureau des légendes*, qui a permis à de jeunes talents de se projeter en «agents» de la tech, et qui se sont dits qu'ils avaient envie de passer par l'agence.

C'est l'imaginaire qui a joué dans cet exemple. Jusqu'alors, le sujet cyber avait été traité comme un sujet de management, par des techniciens RSSI ou des DRH. Personne n'avait porté un récit différent. L'image du type à capuche dans sa cave qui tape sur un clavier persiste depuis des années. La réalité est que cela touche tout le monde et que c'est bien plus sophistiqué. Il ne s'agit pas de dire que rien n'a été fait d'utile – au contraire – mais de sortir d'une approche anxiogène et culpabilisante pour aller vers un message impliquant, ancré dans la vie perso et pro. Le récit tisse nos vies : il donne du sens, capte l'attention, crée de l'émotion, offre des leçons et guide l'action.

Il y a d'autres profils étonnants dans ce conseil, comme des représentants des sciences humaines et sociales ?

PARCOURS

Depuis 2024 : président Open C Future
Depuis 2024 : membre fondateur de l'association Predictive Cyber for Society
Depuis 2024 : président fondateur de Predictive Cyberlab
2007 – 2023 : président fondateur Netexplo Observatory
2004 – 2006 : président fondateur HappeningCo
1994 – 1999 : pour Havas Group, président Euro RSCG Futurs puis président des agences
1988 – 1994 : cofondateur et CEO de l'agence Darjeeling

MON OBJECTIF EST DE SOUTENIR LES PLUS VULNÉRABLES AUJOURD'HUI : HÔPITAUX, COLLECTIVITÉS TERRITORIALES…

Oui, par exemple, Francesca Musiani, directrice de recherche au CNRS, qui travaille spécifiquement sur la cybersécurité ; ou bien Serge Tisseron, psychiatre-psychologue, qui a beaucoup étudié l'empathie numérique, le harcèlement et les biais cognitifs. Il nous apporte son expertise à impliquer les gens par la vraie vie, pas uniquement via des consignes de management.

Nos partenaires du CNRS, de l'X, de Télécom Paris nous aident également pour travailler le scénario du film, le rendre crédible y compris pour un RSSI. Sinon, nous serions seulement vus comme des professionnels de la communication. Avec eux, nous validons aussi les dimensions ergonomiques du programme en ligne, et nous le traduisons en dix langues. Nous travaillons déjà avec Airbus, Crédit Agricole, Renault, des entreprises qui ont des sites dans plusieurs pays. Il est indispensable d'embarquer les collaborateurs dans toutes ces configurations, en tenant compte des nuances culturelles.

Avez-vous de nouveaux KPI pour mesurer le succès de cette démarche inédite ?

Tout à fait. Nous sommes obsédés par la mesure. Or celles qui existent sont insatisfaisantes. Il est certes facile de réaliser une campagne de phishing et de comptabiliser les personnes qui ont cliqué. Mais il y a des limites : au bout d'un moment, les gens se braquent. Quant aux QCM en ligne par exemple, ils sont loin de proposer une mise en situation réelle.

Nous travaillons donc actuellement sur d'autres approches, par exemple l'utilisation de l'IA générative pour des mises en situation de validation d'acquis, avec des interfaces vocales personnalisées par secteur et par métier. Nous avons identifié des start-up qui font des choses remarquables. Cela devrait permettre d'obtenir des KPI beaucoup plus précis. Nous n'en sommes qu'au début de l'histoire, mais à terme, nous devrions pouvoir délivrer des certificats moins « scolaires » que des QCM, et plus personnalisés par la mise en situation.

Vous avez proposé cette démarche gratuitement aux collectivités et aux hôpitaux. Pourquoi ce traitement de faveur ?

Ce n'est pas un traitement de faveur. J'ai eu la chance de créer plusieurs entreprises qui ont bien fonctionné et je suis reconnaissant à nos institutions. D'ailleurs, notre programme est placé sous le haut patronage du Sénat et le marrainage de la ministre chargée de l'IA et du Numérique.

Mon objectif est de soutenir les plus vulnérables aujourd'hui : hôpitaux, collectivités territoriales, certaines écoles. Aussi, à côté de l'entreprise qui pilote le Predictive Cyberlab [Open C Future, NDLR], nous avons créé l'association loi 1901 Predictive Cyber for Society, non profitable, pour mettre gratuitement à disposition ce que nous développons, via les régions et leurs partenaires. Nous avons aussi décidé de mettre gracieusement à disposition le programme aux sous-traitants des grands comptes qui le financent, par exemple chez Safran, via le GIFAS, pour les PME de l'aéronautique et du spatial, bien plus vulnérables que leurs donneurs d'ordres.

N'est-ce pas une erreur de laisser croire aux collaborateurs que tout est sous contrôle, au risque de réveils difficiles quand une cyberattaque survient. Ne faut-il pas rompre avec la croyance des dirigeants que la confiance fait le business ?

Je partage en partie votre constat. On a surjoué la technologie avec les bons firewalls, les bons systèmes, etc., alors que les deux tiers des attaques reposent sur l'ingénierie sociale. Il n'y a pas besoin de «*défoncer la porte*» ni de craquer le SI lorsque quelqu'un vous ouvre l'accès.

L'idée que les pros de l'IT vont tout gérer n'est d'ailleurs plus si répandue. Nous avons mené une enquête IFOP l'an dernier auprès d'un échantillon représentatif en entreprise de 2000 personnes. À la question : «*Selon vous, qui devrait être principalement responsable de la protection contre les cybermenaces ?*», ils ne sont plus que 31% à citer les professionnels (RSSI, responsables IT), mais 48% à estimer que la responsabilité est à partager entre les pros de la tech et chacun d'entre eux, et enfin 21% à penser que c'est à chacun de se protéger.

Sans doute que la forte médiatisation des risques pesant sur la sphère personnelle a contribué à une prise de conscience collective. Il faut en tirer parti pour transformer chaque collaborateur en un véritable acteur de la cybersécurité : capable d'identifier les menaces, de connaître les premières mesures à adopter, et surtout, d'avoir le réflexe d'alerter – même en cas d'erreur. Car en cybersécurité, comme dans le mythe de Sisyphe, l'effort est sans fin : il n'y a jamais de «sécurité totale», jamais de moment où tout serait définitivement «under control».

Nous assistons à un véritable changement de paradigme : nous passons d'un modèle centré uniquement sur la technologie à une approche qui reconnaît enfin le rôle clé de l'humain – non pas comme une faiblesse, mais comme une partie de la solution. Les individus commencent à se sentir concernés dès lors que leur vie personnelle est touchée : usurpation d'identité, vol de données bancaires, arnaques en ligne... Pour les mobiliser, il faut leur donner des repères simples et les aider à comprendre les techniques utilisées par les attaquants. La situation est déjà complexe, et elle le sera encore plus avec l'évolution de l'IA. C'est pourquoi il est essentiel de préparer chacun à devenir un cyber-acteur – car, au fond, chacun a un intérêt direct à se protéger.

Face au risque, deux attitudes extrêmes coexistent : la paranoïa ou l'insouciance. La plupart des gens, cependant, cherchent un équilibre. Votre démarche permet surtout de les responsabiliser sans les angoisser...

Oui, nous en faisons des acteurs positifs. Il faut sortir de la peur et de la culpabilité, montrer l'intérêt personnel et professionnel de comprendre le sujet. Il faut faire de la cybersécurité un sujet de vie, pas d'angoisse. Les outils comme l'IA générative ne sont ni bons ni mauvais, tout dépend de ce qu'on en fait. Mais de comprendre les attaques possibles aide à se préparer. Le but n'est pas de faire peur, mais de rendre les gens lucides. ■

« L'EFFORT EST SANS FIN : IL N'Y A JAMAIS DE MOMENT OÙ TOUT SERAIT DÉFINITIVEMENT « UNDER CONTROL »

La cybersécurité reste un domaine encore extrêmement dynamique de l'IT, avec l'apparition toujours très rapide de nouvelles solutions et de nouvelles catégories d'outils à intégrer. L'essor du cloud marque un point d'inflexion : de nombreuses technologies migrent désormais vers le web, et des plateformes cyber émergent avec la promesse d'apporter rationalité et simplicité.

Move to cloud et essor de l'IA : *la plateformisation de la cyber s'accélère*

Comme pour tout secteur qui gagne en maturité, nous assistons aujourd'hui à une concentration du marché de la cybersécurité. Après le feuilleton de l'acquisition par Google de Wiz, spécialiste de la sécurité cloud, pour 32 Md$, Palo Alto Networks a avalé cet été CyberArk, un autre spécialiste israélien, cette fois dans le domaine de la gestion des identités, pour 25 Md$. Cette vague de consolidation permet aux géants de la cyber de tenir leurs objectifs de croissance, mais vise aussi à leur permettre de constituer des plateformes cloud intégrant un maximum de briques de protection.

Ce mouvement de plateformisation est à l'œuvre depuis quelques années et s'est renforcé ces derniers mois. Eric Antibi, directeur technique de Palo Alto Networks, raconte : «*Bien que la situation économique ne soit pas très favorable, de plus en plus de nos clients accélèrent leurs projets de plateformisation. Cela va dans le sens d'une simplification des architectures de sécurité, et évite d'avoir à déployer des dizaines de solutions qu'il est ensuite extrêmement difficile d'administrer et qui imposent de maintenir des compétences multiples.*» Le responsable reconnaît que le moteur n°1 de ces projets chez ses clients est une recherche d'économies d'échelle. «*Quand on remplace six à dix solutions en place par une plateforme et quelques options, l'économie est évidente. En outre, nous sommes capables de créer une trajectoire de migration sur trois à cinq ans pour que le client n'ait pas à payer des contrats redondants.*» Le second moteur, c'est la recherche d'efficacité opérationnelle. La présence d'un data lake unique rend cette approche par la plateforme beaucoup plus efficace.

La montée en puissance du modèle SASE (Secure Access Service Edge) dans l'accès témoigne de cet essor. Ces plateformes cloud allient des solutions de passerelle web SWG, une gestion des accès réseaux ZTNA, des briques CASB et DLP. Elles sont amenées à connaître une croissance supérieure à 27% par an entre 2025 et 2030, pour atteindre des ventes de l'ordre de 17 Md$, selon Grand View Research.

Comme les CISO pourraient être réticents à mettre la majeure partie de leur sécurité dans les mains d'un seul et même éditeur, ces plateformes doivent être ouvertes au reste de l'écosystème cyber. C'est ce que l'on appelle chez Check Point Software la stratégie «open garden» que pré-

L'évolution de la protection des postes de travail, depuis les antivirus classiques jusqu'aux services managés appuyés sur des solutions EDR/XDR.
SOURCE CISCO

sente Adrien Merveille, son directeur technique France : *« Chaque entreprise a son propre écosystème de solutions. À travers des intégrations et des partenariats, nous allons chercher à faciliter la sécurité entre ces différentes couches d'infrastructure. Ainsi, dans l'écosystème Azure, nous avons la capacité de nous intégrer aux services délivrés par Microsoft pour appliquer les règles de sécurité sans que nos clients aient à déployer eux-mêmes un firewall. »* L'éditeur a ainsi multiplié les partenariats technologiques, il en compterait actuellement près de 250 et fait aujourd'hui évoluer son approche afin d'automatiser la réponse à incident et d'augmenter la posture de sécurité.

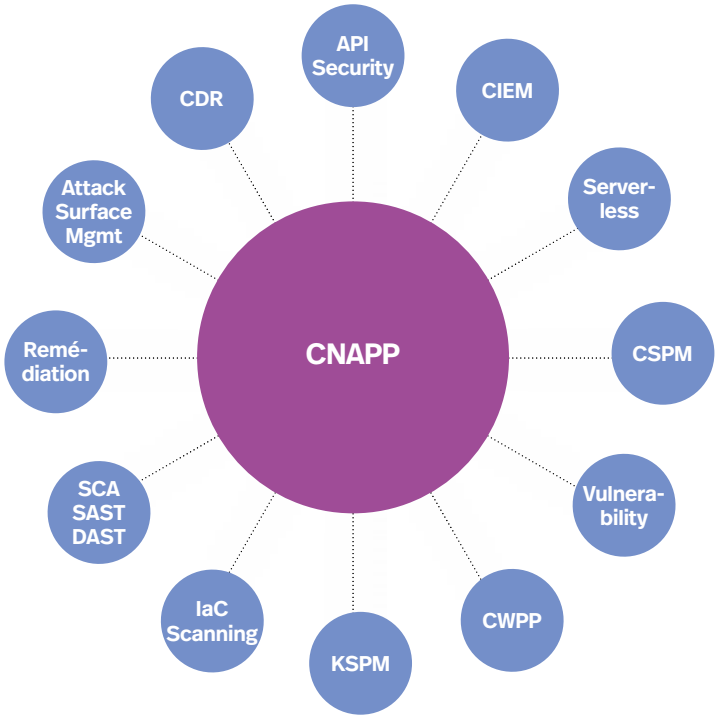
Cette plateformisation participe aussi à la démocratisation des offres les plus pointues. Ainsi, l'analyse de flux réseaux avec les NDR est maintenant à la portée des PME. Pascal Le Digol, country manager France chez WatchGuard, explique pourquoi : *« Le NDR était jusqu'alors très peu arrivé sur ce marché de la PME. Comme d'habitude, les nouvelles technologies cyber pénètrent d'abord les grands comptes, puis redescendent progressivement auprès des petites structures. »* L'américain, qui s'est fait une spécialité de la démocratisation de ces technologies, a réalisé l'acquisition de CyGlass il y a deux ans, avec pour objectif d'intégrer son NDR dans un package cyber global et proposé sous forme de simple option payante.

L'IA infuse dans l'ensemble des briques de sécurité

Cette meilleure intégration des outils ouvre la voie à une plus grande automatisation des SOC (Security Operations Center), ces véritables tours de contrôle qui veillent à la sécurité des systèmes d'information. Les solutions SOAR (Security Orchestration, Automation, and Response/ Orchestration, automatisation et réponse en matière de sécurité) ont montré la voie, avec la capacité pour les analystes de créer des automatisations pour la collecte et l'enrichissement des données relatives à un incident et pour appliquer des mesures de remédiation. Cette première étape avait déjà permis à la productivité des équipes de progresser, mais l'IA va occasionner une rupture encore plus nette dans les pratiques et l'organisation des SOC.

L'une des clés de l'efficacité opérationnelle évoquée par Eric Antibi réside justement dans la mise en œuvre de ces technologies pour exploiter ces données, tant pour améliorer la détection que l'analyse des incidents. L'IA a fait ses preuves dans la protection des endpoints (postes de travail et serveurs) avec la montée en puissance des EDR qui ont permis de contrer la vague de ransomwares. Le machine learning a notamment donné de bons résultats là où l'antivirus traditionnel et sa base de signatures échouait à détecter des malwares sans cesse

L'IA va occasionner une rupture encore plus nette dans les pratiques et l'organisation des SOC



Le CNAPP (Cloud-Native Application Protection Platform) regroupe une myriade de solutions, toutes destinées à sécuriser les différents aspects du cloud.
SOURCE FORTINET

renouvelés. «*En 2025, nous avons vu une multiplication du nombre de solutions qui embarquent des IA*, explique Pierre Haikal, SOC manager France chez Nomios. *Les éditeurs ont commencé à les intégrer à plusieurs endroits, notamment dans les interfaces à destination des analystes SOC. On a vu naître des chats ou des copilotes auxquels on peut poser des questions avec un LLM qui répond avec le contexte de la plateforme. Ce n'est toutefois que la genèse de ce que va permettre l'IA dans l'univers de la cyber.*»

Singularity de SentinelOne est l'exemple type de la stratégie plateforme défendue par les grands éditeurs : de multiples briques de sécurité dont les données convergent vers une plateforme unique et qui viennent alimenter une IA.

C'est que le «move to cloud» des plateformes cyber a repoussé les limites en termes de capacités de stockage des gestionnaires événements (SIEM). Eric Brégand, vice president produit et R&D chez Tehtris, le souligne : «*L'IA vient aider les analystes en désignant les alertes sur lesquelles ils doivent concentrer leur attention, et enrichir les incidents de toutes les données pertinentes à la compréhension.*» La nouvelle version du XDR développé par l'éditeur français adopte une approche métier, pilotée par l'IA. «*Lorsque l'analyste du SOC de l'entreprise ou du MSSP se connecte à la plateforme, l'IA a déjà analysé la situation et lui présente la liste des alertes sur lesquelles il doit se pencher. La landing page de l'application lui présente les trois alertes les plus importantes à traiter et leur impact potentiel sur le SI. L'idée est de gagner en productivité, mais aussi de contrer le phénomène de fatigue qui fait que l'analyste pourrait laisser passer un incident important du fait de la masse de travail à traiter.*»

Aller vers des SOC sans analyses de niveau 1 est une autre tendance forte, comme nous l'explique Éric Vedel, directeur cybersecurity products specialists chez Cisco : «*L'analyste de niveau 1, dont la mission était de faire du tri de manière très répétitive et fastidieuse, va pouvoir être reconverti en niveau 2 grâce à l'action des IA. Il pourra effectuer des tâches à plus haute valeur ajoutée et c'est très bien pour lui du point de vue développement personnel.*» Le spécialiste précise aussi que si les IA apportent une assistance dans la détection et la réponse aux incidents, l'humain reste décisionnaire dans la chaîne : «*L'IA peut recommander de couper l'accès réseau d'un poste car il est infecté, mais seul l'humain sait si le poste en question joue un rôle critique dans un process industriel et ne doit pas être arrêté sans prendre des précautions.*»

La sécurité du cloud et des IA en question

Le cloud et les IA apportent de nouvelles solutions aux problèmes existants, mais présentent aussi leur lot de vulnérabilités. L'accroissement de la surface d'attaque induit par la mise en œuvre d'architectures hybrides ou 100 % cloud implique de revoir la sécurité des ressources placées dans ces infrastructures ouvertes. L'exemple connu des buckets AWS en accès public dans lequel les utilisateurs stockent des données confidentielles est sans doute caricatural, mais pas aussi rare qu'il n'y paraît. Ainsi, les données d'accès aux bases de données de Ford et de Netflix ont fuité dans la nature du fait d'un bucket S3 laissé libre d'accès par l'éditeur de logiciel Attunity (Qlik).

Toute une série de nouvelles solutions cyber conçues pour le cloud sont donc apparues au catalogue de start-up spécialisées, puis dans celui des grands éditeurs. La gestion de la posture de sécurité ou CSP vise ici à s'assurer que la configuration de toutes les ressources cloud de l'entreprise est bien maîtrisée et conforme aux règles établies par le RSSI. Regroupées dans la catégorie valise CNAPP (pour Cloud-Native Application Protection Platform), ces nouvelles solutions ont pour noms WAAP (Web Application and API Protection), un firewall conçu pour le cloud, CSPM (Cloud

Security Posture Management) et CIEM (Cloud Infrastructure Entitlement Management) qui visent à la conformité et la configuration des ressources cloud, DSPM (Data Security Posture Management) et CWPP (Cloud Workload Protection Platform) pour la détection des comportements anormaux en production.

Le potentiel de développement de ces solutions est considérable. «*Notre mission est de sécuriser tout ce que les clients conçoivent et déploient dans le cloud, de façon claire, simple et intuitive*», résume Geoffrey de Seroux, regional vice president pour la France du spécialiste du CNAPP Wiz, dont Google s'est donc emparé en mars dernier. La plateforme Wiz se compose de trois modules : Wiz Cloud, l'offre «historique» de la start-up qui apporte la visibilité sur l'ensemble des ressources cloud (le CSPM), Wiz Code pour les développeurs d'applications dans une optique shift-left de la sécurité vers les développeurs, et Wiz Defend, son CWPP. «*Depuis cinq ans, nous accompagnons des entreprises de toutes tailles, de tout secteur d'activité, et ce qui est frappant, c'est que nous suivons des clients qui présentent tous les stades de maturité dans le cloud.*»

La protection cloud est le terrain de jeu de nombreux acteurs. C'est le cas de Netskope, avec un focus sur la donnée. Ray Canzanese, directeur des threat labs de l'éditeur, en résume la stratégie : «*Nous délivrons une plateforme pour sécuriser les données, les ressources web, cloud, IA. L'entreprise fait passer par nous l'ensemble de son trafic et nous assurons le monitoring de ses flux afin de repérer toute fuite de données, les menaces. Nous surveillons l'ensemble des données stockées, que celles-ci soient dans le cloud et même on-premise.*» Sa plateforme repère tout usage inhabituel, par exemple un utilisateur qui commence à télécharger de gros volumes de données en dehors de l'entreprise. «*La plateforme voit toutes les données où qu'elles se situent et repère ces menaces intérieures et externes, et tout ce qui peut faire peser un risque sur les données.*»

TÉMOIN **Eric Antibi,** directeur technique de Palo Alto Networks

« La sécurité des IA va être un sujet clé pour nous »

« La protection des intelligences artificielles va devenir un sujet prédominant pour les entreprises. Les usages de la GenAI explosent et les entreprises vont devoir réfléchir à faire de la sécurité by design sur ces infrastructures. Pour l'instant, le mode de gouvernance n'est pas encore très clair : est-ce que le CISO doit être responsable de la sécurité des IA ou faut-il un AI/GenAI officer qui sera responsable des IA, de leur comportement et qui s'appuiera sur le CISO pour le volet cyber pur ? Tout reste à inventer. »

L'IA : un nouveau workload avec des risques très spécifiques

Les nouveaux risques arrivent aussi avec l'IA. Les infrastructures des LLM sont bien souvent à base de conteneurs logiciels et d'appels à des API externes et doivent être sécurisées en tant que telles, mais les modèles eux-mêmes présentent des vulnérabilités très spécifiques. Bernard Montel, directeur technique EMEA de Tenable, s'en inquiète : «*Notre dernière étude Cloud Risk Report montre que si les projets d'IA vont très très vite, la sécurité ne suit pas. 70% des services d'IA qui tournent chez nos clients présentent des vulnérabilités critiques, contre 50% en moyenne pour les applications "classiques". Nous travaillons sur ces nouveaux risques d'exposition amenés par l'IA car nos chercheurs comme nos clients pointent le besoin de solutions pour adresser ce problème.*» Un modèle peut notamment être utilisé par un attaquant pour organiser une fuite de données, peut être manipulé pour nuire à l'entreprise par une prompt injection, l'attaque contre les IA sans doute la plus connue. Les chercheurs ont déjà créé de multiples outils open source pour tester leurs créations, et les éditeurs s'intéressent de près à ce nouveau marché. Palo Alto a tiré le premier avec Prisma AIRS, une plateforme totalement dédiée à tous les aspects de la sécurité des IA. Nul doute que tous les autres majors de la cyber vont rapidement lui emboîter le pas.

ALAIN CLAPAUD

TÉMOIN **Pierre de Neve,** responsable des ventes secteur public et leader de la sécurité du cloud hybride chez Trend Micro

Le CNAPP vérifie la mise en œuvre des meilleures pratiques définies par l'OWASP Foundation

« Le CNAPP (Cloud-Native Application Protection Platform) propose une solution globale pour la protection du cloud. Il s'agit de sécuriser les conteneurs, la consommation de services et de micro-services, avec lesquels on ne maîtrise pas la plateforme sous-jacente. L'approche peut être assez traditionnelle, avec une protection des workloads assurée via les intégrations avec AWS, Azure, GCP et Alibaba. Ou passer par le CSPM (Cloud Security Posture Management) qui s'attache à donner de la visibilité sur les ressources cloud. Il s'agit alors de s'assurer de la bonne configuration de tous les services mis en œuvre dans l'architecture par rapport aux meilleures pratiques définies par l'OWASP Foundation. »

Big data et IA accélèrent la convergence des réseaux IT, ceux de l'informatique de gestion, et OT, ceux des objets industriels. Ce mouvement de fond impose plus de collaboration entre les directions industrielles et les DSI sur la cyber. Une démarche indispensable avant de penser à des SOC communs IT et OT.

La convergence IT/OT *bute à la porte du SOC*

Le modèle d'une informatique industrielle totalement isolée a vécu. La démarche Industrie 4.0 impose au contraire de plus en plus d'échanges de données avec l'extérieur. Une telle transformation s'accompagne d'une montée en flèche du risque d'attaque : en 2024, le spécialiste de la sécurité dans le cloud Zscaler a bloqué 45% de plus de malwares visant l'IoT qu'un an auparavant.

Le rapport 2024 de l'observatoire de la convergence IT-OT NXO et Cisco dressait aussi un constat plutôt alarmant : 75% des décideurs déclaraient que leur niveau de connaissance sur ce sujet était partielle ou très faible, et 34% seulement estimaient que leurs réseaux industriels OT étaient bien définis dans leur organisation. Franck Bonnard chez NXO a toutefois noté une amélioration ces derniers mois : *«Nous avons observé une accélération de la prise en compte des problématiques cyber de l'OT par les DSI. Ceux-ci s'emparent du sujet car les métiers ont besoin de données pour mesurer et améliorer les performances de leurs processus et mettre en œuvre les IA.»*

Dans un tel contexte, quelle organisation cyber adopter ? Pour Sabri Khemissa, cofondateur de Fortress Cybersecurity, il y a trois grandes catégories d'organisations. *«Il y a celles où la DSI va progressivement prendre en charge la cybersécurité des installations. Une autre approche est d'étendre le périmètre d'action du RSSI. Sa position est un peu ambivalente, car il doit protéger des ressources qui ne sont pas sous la responsabilité de la DSI, tout en lui reportant parfois... Enfin, il y a des cas où la direction industrielle se saisit elle-même du sujet cyber.»* Vincent Nicaise, responsable des partenaires industriels et de l'écosystème chez Stormshield, confirme : *«Dans certains contextes, les usines restent maîtresses de la cybersécurité, car elle fait partie de la sûreté de fonctionnement qui est de leur ressort. C'est un vrai enjeu, car elles ont les budgets.»*

Si les acteurs montent en compétence sur l'OT, la convergence des SOC IT et OT n'est pas encore à l'ordre du jour : *«Ils sont de natures très différentes»*, explique Khalil Bajnati, SOC/CSIRT leader chez Serma Safety & Security, filiale du groupe industriel Serma, qui développe des offres de SOC OT mises en œuvre sur les entités industrielles du groupe, avant de les proposer à des tiers. L'intégration IT/OT va donc devoir faire entrer des experts avec des compétences industrielles dans les SOC. Comment savoir en effet que sur tel ou tel système SCADA, modifier un simple paramètre de vitesse de rotation ou de déplacement peut avoir des conséquences graves et endommager une machine ? L'IA pourrait assez rapidement apporter des éléments de réponse à ce type de questionnement. Mais la convergence des SOC prendra plus de temps.

ALAIN CLAPAUD

TÉMOIN **Franck Bonnard,** consultant connectivité et cybersécurité des environnements convergés IT-OT chez NXO

Mettre la cybersécurité à hauteur d'atelier

«La priorité est de mettre la cybersécurité à hauteur d'atelier. Les DSI doivent faire l'effort d'amener des solutions simples et opérables par les métiers avec un certain degré d'autonomie. Le contre-exemple, c'est la mise en œuvre d'un bastion qui reste compliquée et ne peut se faire sans la DSI. Or la solution doit être exploitable directement par les métiers. Il ne faut pas devoir appeler un administrateur réseau pour créer un accès un dimanche soir à 23h pour l'intervenant qui doit dépanner une machine et reprendre la production !»

Abonnez-vous en ligne

IT for Business

Le média des managers du numérique

Offre Full Digital

- Le magazine en ligne
- Nos archives numériques en PDF
- Contenus réservés à la communauté
- La newsletter hebdo

1 an 160 € HT

Offre Full Digital & Print

- Le magazine en ligne
- Nos archives numériques en PDF
- Contenus réservés à la communauté
- La newsletter hebdo

\+ 11 numéros/an d'IT for Business

1 an 200 € HT
2 ans 360 € HT

OUI, je m'abonne
en flashant le QR code ci-dessous

CHAQUE MOIS
le magazine
et sa version digitale

CHAQUE SEMAINE
les infos clés du marché

CHAQUE JOUR
une base de plus de 10 000 articles
+ les archives du magazine

* TVA 2,10%. Offre valable jusqu'au 31/12/2025 pour les nouveaux abonnés en France métropolitaine uniquement. L'éditeur s'engage à livrer votre magazine sous un délai maximum de 5 semaines. Les informations sont nécessaires à IT for Business pour traiter votre commande et les services qui y sont associés. Ces informations sont enregistrées dans notre fichier clients et peuvent donner lieu à l'exercice du droit d'accès, de rectification et de suppression auprès du service Abonnements au moyen d'un e-mail adressé à : contact@itforbusinessabonnement.fr conformément à la loi « informatique et libertés » du 6 janvier 1978 telle que modifiée en 2004. L'Éditeur se réserve le droit de modifier le contenu, le titre ou le format de la publication objet du présent abonnement, dans le respect de son actuelle ligne éditoriale. Conformément à l'article L 121-20-2, 5° du Code de la consommation, vous ne bénéficiez pas d'un droit de rétractation. Les demandes de résiliation anticipée et de remboursement ne seront prises en compte que dans le seul cas d'un motif légitime dûment justifié. Les demandes sont à adresser exclusivement par simple courrier à l'attention du service Abonnements à l'adresse suivante : IT for Business – Service Abonnements – 6, rue de Lisbonne, 75008 Paris.

Ce sera sans nul doute la grande affaire pour des dizaines de milliers de RSSI à travers toute l'Europe. Les pays transposent progressivement le texte européen en droit national. Et même si l'ANSSI a promis un sursis de trois ans avant les premières sanctions, le travail de mise en conformité s'annonce immense et doit débuter rapidement.

NIS 2, *le chantier n°1 des RSSI pour 2026*

À l'heure où paraissent ces lignes, le texte de transposition de NIS 2 (Network and Information System) dans la loi française n'est toujours pas voté et l'instabilité politique actuelle de la France laisse planer la menace d'un nouveau report. C'est dans ce contexte que les DSI et les RSSI doivent néanmoins préparer leur budget 2026 en tenant compte de la mise en conformité à NIS 2. Pas simple quand on ne connaît pas avec certitude les entreprises et les collectivités locales auxquelles s'appliquera finalement le texte.

L'ANSSI livre néanmoins, sur le site MonEspaceNIS2, les grandes lignes du futur texte, et surtout les critères d'éligibilité des EE (Entités Essentielles) et EI (Entités Importantes). Tous les domaines d'activité sont listés et des milliers de collectivités locales, d'administrations publiques, d'entreprises moyennes et plus grandes dans 18 secteurs seront concernées. Laurent Gelu, cybersecurity & resilience leader chez Kyndryl France, calibre le chantier NIS 2 selon les typologies d'entreprises : *« Pour les grandes, NIS 2 n'apportera pas de grande nouveauté : elles sont déjà dans une approche SMSI (Système de management de la sécurité de l'information), ont fait l'effort d'aller vers l'ISO 27001 et sont engagées dans un processus d'amélioration continue. »* Par contre, pour les plus petites organisations, NIS 2 va représenter un travail beaucoup plus conséquent. *« L'objectif de NIS 2 est justement d'élever le niveau de sécurité général de toutes les organisations en Europe, car toutes peuvent être potentiellement la cible d'une attaque. Or le niveau d'investissement en cyber d'une grande banque ou d'une entreprise du SBF 120 n'a rien à voir avec ce qu'une PME peut consacrer à sa sécurité. »* Pour tenir compte de ce dernier point, NIS 2 introduit la notion de proportionnalité : une entreprise de taille moyenne n'aura pas à se doter d'une cyber du niveau d'un géant de la Défense, mais elle devra s'aligner sur les dix grands principes du texte.

Des mesures évidentes, d'autres plus structurantes

Certaines mesures de NIS 2 peuvent sembler évidentes, comme avoir une gestion des accès ou disposer d'un PRA pour assurer la continuité des activités critiques. D'autres demanderont beaucoup plus d'efforts. C'est notamment le cas de la gestion des incidents. Le délai de signalement d'un incident de sécurité majeur va rester de 72 heures auprès de la CNIL, mais sera de 24 heures seulement auprès du CSIRT local ou de l'ANSSI. Cela laisse peu de temps pour enquêter à son sujet, ce qui veut dire que l'entreprise doit pouvoir s'appuyer sur un SOC pour analyser rapidement l'incident remonté par les

TÉMOIN **Fabrice Bru,** président du CESIN (Club des Experts de la Sécurité de l'Information et du Numérique)

Une opportunité de faire monter le niveau de sécurité

« NIS 2 est une très belle opportunité pour tout l'écosystème de faire monter le niveau de sécurité de l'ensemble des entreprises et des organisations à l'échelle européenne et française. Les JO 2024 ont montré que si on s'en donne les moyens, le risque cyber, même très élevé, peut être maîtrisé. Le CESIN œuvre pour aboutir à un texte voté rapidement. Nous sommes en bonne voie. Avec d'autres organisations professionnelles, nous avons été entendus par le groupe parlementaire de l'Assemblée nationale au mois de juin et nous avons pu faire part de nos interrogations sur le texte et les points qui devaient encore être précisés. »

LES DIX POINTS CLÉS À TRAITER SELON NIS 2

- **Politiques d'analyse des risques et de sécurité des SI.**
- **Gestion des incidents.**
- **Continuité des activités.**
- **Sécurité de la chaîne d'approvisionnement.**
- **Sécurité de l'acquisition, du développement et de la maintenance des réseaux et des SI.**
- **Évaluation de l'efficacité des mesures de gestion des risques cyber.**
- **Pratiques de base en matière d'hygiène de sécurité et de formation.**
- **Utilisation de la cryptographie et, le cas échéant, du chiffrement.**
- **Sécurité des ressources humaines, des politiques de contrôle d'accès et la gestion des actifs.**
- **Utilisation de solutions d'authentification à plusieurs facteurs ou d'authentification continue, de communications vocales, vidéo et textuelles sécurisées, et de systèmes sécurisés de communication d'urgence.**

SOURCE MONESPACENIS2.CYBER.GOUV.FR

outils de détection afin d'éliminer un éventuel faux positif, et le qualifier afin de décider si celui-ci doit faire l'objet d'un signalement officiel. Que le SOC soit internalisé, mutualisé auprès d'un MSSP ou, pour les plus petites organisations, qu'il repose sur une offre MicroSOC d'un opérateur télécom, impossible désormais de laisser passer le week-end avant d'investiguer.

L'autre point de NIS 2 qui suscite sans doute le plus de discussions entre les professionnels porte sur la sécurité de la supply chain. Les grands comptes étant plutôt bien protégés, les attaquants visent leurs fournisseurs afin de rebondir vers leur cible principale. Avec NIS 2, le donneur d'ordres doit pouvoir s'assurer que l'ensemble de ses sous-traitants ont mis en place un minimum de protections autour de leur SI. Les outils pour y parvenir sont connus : questionnaires à remplir, clauses contractuelles ou encore recours aux systèmes de notation, ces mesures n'excluant pas des audits ciblés pour s'assurer que ce qui est déclaré correspond à la réalité…

Une portée transnationale qui pose question(s)

Enfin, la portée transnationale de NIS 2 crée de nouvelles problématiques pour les entreprises. Chaque pays légifère selon sa propre lecture du texte, or pour le DOSI d'un grand groupe, le diable se niche dans les détails. Il faudra gérer les différences d'interprétation. Autre question, une conformité NIS 2 reconnue dans le pays du siège va-t-elle couvrir l'ensemble des filiales ? Et où faudra-t-il déclarer un incident de sécurité si celui-ci a eu lieu dans une filiale danoise ou grecque ?

On le voit, beaucoup de points doivent encore être précisés pour que NIS 2 devienne une réalité sur l'ensemble du continent. «*L'ENISA* [NDLR : Agence européenne de Cybersécurité] *a publié au début de l'été un guide d'application de NIS 2 qui reprend 80% de l'ISO 27002, mais l'encre n'est pas encore sèche et des réponses doivent encore être trouvées à des questions importantes*», prévoit Laurent Gelu.

Pour autant, faut-il attendre que tout le dispositif soit prêt pour se lancer dans la mise en conformité ? Vincent Strubel, le directeur de l'ANSSI, a certes promis trois années de sursis avant l'application de sanctions, mais il ne cesse par ailleurs d'alarmer la communauté cyber sur la charge que va représenter la mise en conformité dans les prochaines années. Les compétences disponibles sont rares et vont s'arracher à prix d'or… Pierre Jacob, directeur général adjoint de Magellan Sécurité, estime donc que les entreprises doivent rapidement évaluer leurs chances d'être soumises au texte «*Si l'on est concerné, il ne faut pas attendre pour lancer la démarche de mise en conformité. La trajectoire de certains pays, dont la Belgique, est de se rapprocher de l'ISO 27001. Ça ne veut pas dire pour autant que si on est conforme ISO, on le sera avec NIS 2, mais c'est un socle qu'il est important de maîtriser.*» Pour le consultant, les gains en termes de sécurité opérationnelle peuvent déjà légitimer la démarche de conformité auprès des directions générales : «*NIS 2 va représenter un certain nombre de thématiques cyber et de chantiers à mener. Quoi qu'il arrive, l'entreprise va gagner en résilience et en protection de ses ressources.*»

ALAIN CLAPAUD

De la fraude hyper-personnalisée aux malwares polymorphes et aux agents autonomes, l'intelligence artificielle redéfinit en profondeur le paysage des menaces. Mais face à ces attaques industrialisées, la défense se réinvente aussi avec copilotes SOC, automatisation et prédiction. Tout en sécurisant ses propres modèles pour éviter un nouveau point de rupture.

IA en cybersécurité : *qui mène vraiment le jeu ?*

La cybersécurité repose sur un déséquilibre fondamental : d'un côté, des attaquants qui frappent quand ils veulent, comme ils veulent, là où ils veulent ; de l'autre, des défenseurs qui doivent tout protéger, partout, tout le temps, alors même que la surface d'attaque s'étend inexorablement avec le SI et sa complexité. Si l'IA a longtemps été perçue comme un moyen de rééquilibrer les forces, l'arrivée de l'IA générative a relancé le jeu du chat et de la souris.

Emanuela Zaccone,
AI and cybersecurity product strategist chez Sysdig

« D'ici un an, je pense que les équipes de sécurité commenceront à interagir avec leurs plateformes principalement par le biais d'assistants IA. »

Certes, les avis divergent sur l'état actuel des forces. *« En 2025, l'augmentation exponentielle des fraudes optimisées par l'IA a été à l'avantage des attaquants »*, estime David Girard, head of AI security & alliances chez Trend Micro. D'autres, comme David Grout, CTO EMEA de Google Cloud Security, tempèrent en affirmant que *« sur les douze derniers mois, l'avantage est à la défense, car de nombreuses innovations sur tous les fronts ont permis d'améliorer les processus de détection et la vitesse de réaction. »* Emanuela Zaccone, stratège chez Sysdig, considère de son côté que *« l'enjeu n'est pas de savoir qui profite le plus de l'IA, mais qui l'utilise le plus efficacement. Or, contrairement aux défenseurs, les cyberattaquants ne sont soumis à aucune restriction, aucune directive éthique et aucune exigence de conformité. »*

IA Générative : un changement d'échelle, de vitesse et de réalisme

L'IA générative ne crée pas tant de nouvelles catégories d'attaques qu'elle ne perfectionne et n'industrialise les vecteurs existants à un niveau alarmant : elle a fondamentalement altéré la nature, l'échelle et la vitesse des cybermenaces. En pratique, la bascule se manifeste par trois ruptures majeures.

D'abord, l'hyper-personnalisation et l'ingénierie sociale à l'échelle industrielle : *« Le véritable bouleversement réside dans le réalisme des attaques à grande échelle »*, avertit Adrien Porcheron, DG France de Cato Networks, pour qui cette sophistication rend *« indispensable une inspection IA-native* [qui scrute l'intention et le contexte plutôt que le code seul, NDLR] ». Les attaques d'ingénierie sociale, autrefois artisanales et chronophages, sont désormais produites en masse. Les LLM rédigent des courriels crédibles, contextuellement pertinents et grammaticalement parfaits, s'adaptant au style d'une entreprise ou aux intérêts d'une cible. *« L'ingénierie sociale devient presque indiscernable d'une interaction authentique. »*

« L'IA élimine les signaux d'alerte habituels (grammaire, localisation, urgence). L'attaque a contourné ainsi trois vérifications humaines avant sa détection par l'analyse comportementale. » précise Samy Reguieg, GM France et Afrique

Top 10 des risques de sécurité pour les applications IA/LLM

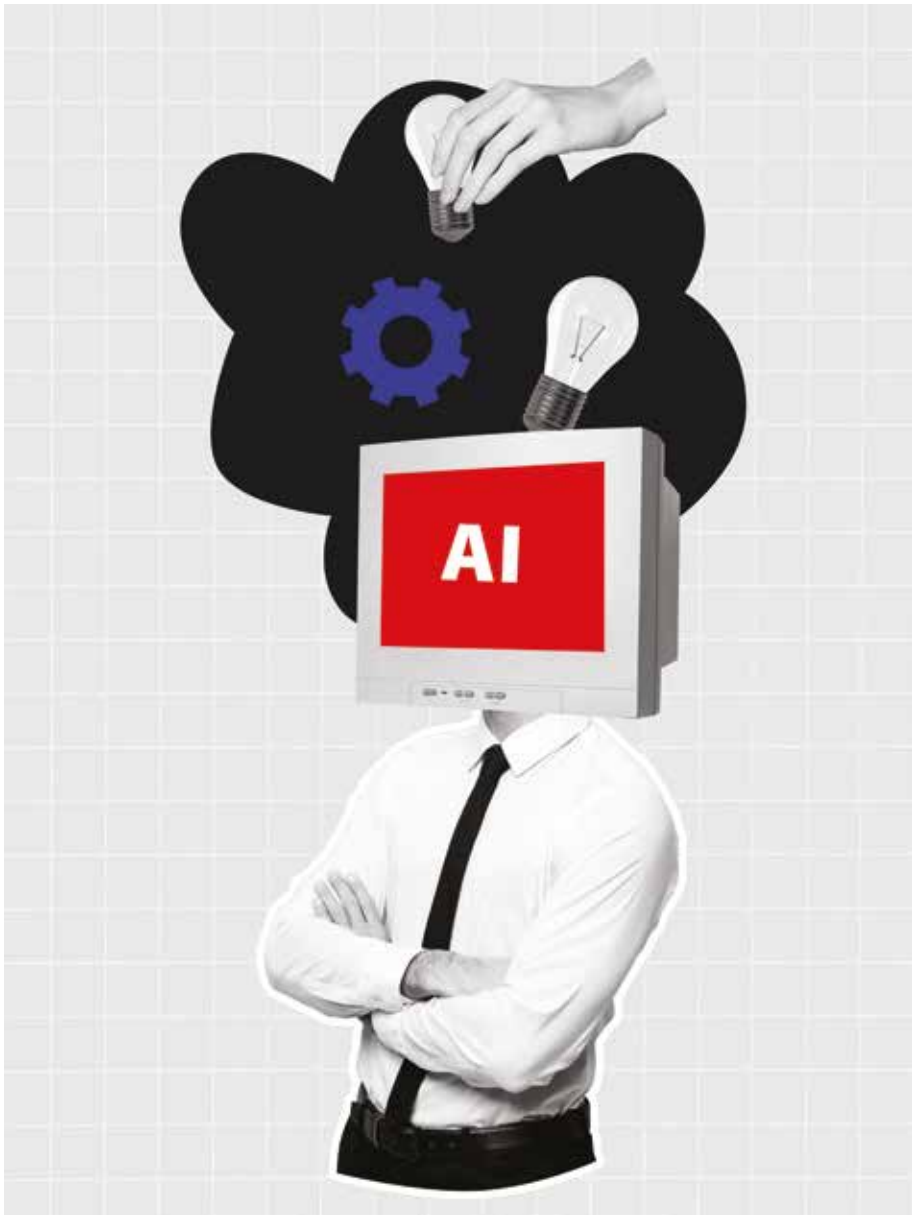
	RISQUE	PARADE
1	**Injection de prompts : manipulation des instructions via des entrées malveillantes pour contourner des contrôles ou provoquer des actions non autorisées.**	Séparer strictement instructions/ données, listes de permissions, filtres d'entrée/sortie, validations, supervision humaine pour actions critiques.
2	**Gestion non sécurisée des sorties : utilisation des réponses du modèle comme « fiables » (exemple : exécuter du code généré) sans validation.**	Traiter les sorties comme non fiables : validation systématique, assainissement, sandbox en aval.
3	**Empoisonnement des données d'entraînement : contamination du dataset pour biaiser le modèle, introduire des backdoors.**	Vérifier provenance et intégrité, filtrer/désinfecter les sources, contrôles d'accès aux jeux d'entraînement.
4	**Déni de service du modèle : saturation par requêtes coûteuses/volumineuses (ou prompts adversariaux) entraînant dégradation et surcoûts.**	Rate limiting, quotas par utilisateur, budgets de tokens, surveillance d'usage et coupures automatiques sur pics anormaux.
5	**Vulnérabilités de la chaîne d'approvisionnement : modèles/données/ composants tiers compromis.**	Auditer dépendances, privilégier sources fiables, SBOM/MLSBOM, mises à jour contrôlées, signatures et vérifications.
6	**Divulgation d'informations sensibles : fuite de données d'entraînement ou de contexte dans les réponses.**	Masquage/filtrage des sorties, politiques de données minimales, durcissement/ affinage du modèle, tests d'exfiltration.
7	**Conception non sécurisée des plugins/outils : contrôles d'accès insuffisants, permissions excessives.**	Authentification forte, moindre privilège, validation des entrées, sandbox des connecteurs.
8	**Agentivité excessive : trop d'autonomie/ permissions → dommages en cascade si détournement.**	Permissions minimales, garde-fous, validation humaine pour actions à fort impact, circuit breaker/kill switch.
9	**Sur-confiance (overreliance) : accepter sans vérification les sorties du modèle.**	Supervision humaine, politiques de double contrôle, formation des utilisateurs, métriques de qualité.
10	**Vol de modèle : extraction/vol d'un modèle propriétaire (perte IP/coûts).**	Accès strictement contrôlé, chiffrement au repos/en transit, monitoring d'extraction, watermarking/provenance si applicable.

SOURCE OWASP

d'Acronis. Dans le même temps, *« la baisse du niveau de compétence requis pour les attaquants »* est, pour David Girard, le changement le plus important engendré par l'IA générative. *« Les auteurs de menaces n'ont plus autant besoin d'expertise underground pour mener des attaques convaincantes. »* Surtout que la menace va désormais bien au-delà du texte : les deepfakes audio et vidéo servent à des usurpations d'identité d'un réalisme troublant, comme l'illustre l'exemple d'un employé de Hong Kong ayant transféré 25 M$ à la suite d'une visioconférence avec un « directeur financier », entièrement généré par IA.

Des malwares polymorphes

Ensuite le renforcement des malwares polymorphes, qui rendent l'adversaire invisible et en constante mutation. Ces logiciels malveillants qui modifient leur propre code à chaque exécution pour déjouer les détections, ne sont pas nouveaux, mais l'IA les a fait changer d'échelle. *« 70 % des compromissions d'entreprise en 2025 ont impliqué des malwares polymorphes »*, affirme Richard de la Torre, technical product manager chez Bitdefender. La seule manière de contrer ces menaces est de concentrer la détection sur leur comportement : privilégier l'observation de *« ce que fait »* l'attaque plutôt que *« ce qu'elle est »*. Mais les détections comportementales vont devoir se réinventer. La découverte récente du malware Promptlock l'illustre crûment : ce rançongiciel expérimental s'appuie sur un LLM local (le modèle open source gpt-oss-20b d'OpenAI via Ollama) pour générer à la volée des scripts Lua malveillants et multiplateformes (Windows, Linux, macOS). Cette technique introduit une part de



non-déterminisme qui complique les détections. Promptlock est la preuve que des outils IA rendent économiquement viable une polymorphie de plus en plus «comportementale» et non uniquement une polymorphie du code généré.

L'accélération via les agents

Enfin l'agentisation accélère tout : déjà en développement, la prochaine génération de menaces repose sur l'IA agentique, avec des systèmes autonomes capables de planifier et d'exécuter des chaînes d'attaques complexes avec peu d'intervention humaine. Cette autonomie réduit les cycles d'attaques de plusieurs jours à quelques minutes, créant un décalage de vitesse insurmontable pour les équipes de sécurité humaines. Selon Aziz Si Mohammed, senior manager solutions engineering chez Okta France, «*des cas récents ont montré que des cybercriminels utilisaient déjà des IA avancées comme Claude pour automatiser des étapes entières d'attaques : collecte d'informations, intrusions, rédaction de messages d'ingénierie sociale ou encore exigences de rançon*». Mais Richard de la Torre nuance : «*À ce stade, les attaques agentiques relèvent davantage de la fiction que d'une réalité imminente.*» Selon lui, les groupes cybercriminels hésiteraient à automatiser toute une attaque «*en utilisant des systèmes sujets aux hallucinations qui les mettraient en danger*» et «*trouvent pour l'instant bien plus de valeur dans les LLM pour l'ingénierie sociale*».

La riposte : le SOC augmenté

Face à cette IA offensive, il faut une IA défensive plus rapide, plus intelligente et mieux intégrée. La riposte s'organise autour d'un triptyque : plateformes AI-native, copilotes SOC et automatisation de bout en bout. D'abord avec des XDR/SIEM : ces plateformes de nouvelle génération, intégrant nativement l'IA, ingèrent et corrèlent en temps réel d'immenses volumes de données (terminaux, cloud, réseaux, identités) pour offrir une vue unifiée et contextuelle de la posture de sécurité. Car l'IA excelle à faire émerger du signal utile dans le brouhaha massif de données de logs, à contextualiser et à hiérarchiser. En réduisant drastiquement les faux positifs qui épuisent les analystes et en priorisant les alertes selon leur criticité, l'IA améliore le retour sur investissement des outils de sécurité et l'efficacité des équipes. Intégrée à ces outils, elle peut également agir et lancer des remédiations automatisées. Mais pour l'instant, «*cette automatisation est pertinente lorsqu'il s'agit de flux de travail répétitifs et à faible risque. En revanche, pour des actions à forte criticité, comme la désactivation de comptes utilisateurs ou l'arrêt brutal de processus métier, l'intervention humaine reste indispensable*», tempère Adrien Porcheron. Encore faudra-t-il organiser le changement des pratiques dans les équipes, un vrai sujet de gouvernance et de RH.

Au-delà de la détection, la cyberdéfense s'oriente vers l'anticipation grâce à la predictive threat intelligence. Cette discipline mobilise IA et machine learning pour analyser les tendances d'attaque (TTP) des acteurs malveillants et les vulnérabilités émergentes, afin de prévoir où et comment la prochaine attaque est susceptible de se produire. Les équipes renforcent ainsi

les défenses proactivement, corrigent les bonnes vulnérabilités et ajustent les contrôles avant l'exploitation. *«Les renseignements et l'anticipation, que ce soit dans une guerre traditionnelle/cinétique ou cyber, ont toujours été les clés»*, rappelle Lucas Guiglionia, customer success management manager de Filigran.

Enfin, l'agentique devrait devenir un allié de plus en plus précieux des équipes SOC, pour résumer un incident en langage naturel, suggérer des requêtes et des investigations, produire des IOC, rédiger un plan de remédiation, générer un playbook SOAR... Des assistants comme Microsoft Security Copilot ou Google Security AI Workbench automatisent déjà les tâches répétitives et à faible valeur ajoutée, libérant les experts pour les investigations complexes, la chasse aux menaces et la décision stratégique. La collaboration Homme-IA devient une compétence clé de ces experts : l'IA excelle sur l'analyse à grande échelle et la reconnaissance de schémas à vitesse machine, mais l'humain garde l'avantage en pensée critique, intuition, compréhension du contexte métier et arbitrage face à l'inédit. *«L'avenir ne se situe pas dans une défense 100% autonome, mais dans un modèle hybride où l'IA agit comme copilote auprès des analystes SOC. Cette combinaison garantit une réponse rapide tout en préservant le discernement humain nécessaire dans les décisions à fort impact»*, insiste Adrien Porcheron. La performance d'un SOC moderne dépendra de sa capacité à faire collaborer efficacement ces deux formes d'intelligence.

Sécuriser l'IA : nouveau front de la cyberdéfense

Reste que, alors que la course à l'armement entre IA offensive et défensive fait rage, un second front, tout aussi critique, s'est ouvert : la sécurisation des systèmes d'IA eux-mêmes. L'IA n'est plus seulement un outil de défense ou d'attaque, elle devient une nouvelle surface d'attaque au sein de l'entreprise !

Conscient de ce péril, l'OWASP (Open Worldwide Application Security Project) a publié un Top 10 spécifiquement dédié aux risques des applications LLM (voir ci-dessus). Ces risques ne sont pas théoriques : ils ont déjà été exploités dans des scénarios réels, soulignant l'urgence de développer une discipline de sécurité dédiée.

Au-delà de ces risques techniques, *«le danger le plus largement sous-estimé est celui de la shadow AI*, constate Adrien Porcheron. *La première étape de toute stratégie de sécurité IA doit être la découverte et la surveillance de l'ensemble des usages, qu'ils soient officiels ou non.»* Bernard Montel, EMEA technical director & security strategist de Tenable, voit plutôt le principal risque du côté des modèles et de leurs données : *«Un adversaire peut empoisonner l'entraînement, créer des angles morts et pousser un système défensif à agir contre son objectif – un risque "méta" potentiellement catastrophique.»*

Pour contrer ces menaces spécifiques, une discipline émerge : le MLSecOps (Machine Learning Security Operations) qui vise à intégrer la sécurité tout au long du cycle de vie du machine learning, de la collecte des données au déploiement et à la surveillance continue du modèle. Il étend les pratiques DevSecOps à des composants propres aux systèmes d'IA : jeux de données d'entraînement, modèles et pipelines d'inférence.

Partant du principe que les intelligences artifcielles sont amenées à prendre de plus en plus de décisions autonomes à impact métier (approbation de crédit, diagnostic médical, maintenance prédictive, etc.), l'intégrité des modèles devient un enjeu critique qui conditionne l'intégrité des opérations. Mais pour Emanuela Zaccone, il ne faut pas envisager *«la sécurité de l'IA uniquement en termes de précision des modèles ou de données d'entraînement. Le véritable enjeu réside dans l'exécution : comment l'IA se comporte-t-elle lorsqu'elle interagit avec des personnes, des données et des systèmes ? Il est impossible de vérifier à l'avance chaque décision qu'elle prend. C'est pourquoi nous avons besoin d'un modèle d'exécution à privilèges minimaux pour l'IA, dans lequel chaque entrée est traitée par défaut comme non fiable et chaque sortie est conforme à la politique. Sans ce changement, les organisations risquent d'intégrer l'IA dans des processus critiques sans les contrôles nécessaires.»*

La mise en place d'un cadre MLSecOps ne sera pas une tâche pour la seule équipe de sécurité : c'est une question de gouvernance d'entreprise qui requiert une collaboration transverse entre métiers, équipes data, IT et direction. Mais le RSSI doit en être le catalyseur, pour garantir que l'IA – nouveau moteur de la valeur – est déployée de façon fiable, éthique et sécurisée.

LAURENT DELATTRE

Un modèle IA de sécurité en open source

Cybertron est un modèle de langage open source conçu par Trend Micro pour répondre aux défis spécifiques de la cybersécurité. Contrairement aux IA généralistes, il s'appuie sur des jeux de données spécialisés, réunis au sein d'un dataset ouvert dénommé Primus, et sur une architecture optimisée pour analyser, détecter et contrer les menaces complexes.

Notamment disponible sous forme de micro-services Nvidia NIM, Cybertron peut être déployé partout, offrant aux entreprises un contrôle total et une approche «zero-trust» de l'IA. En rendant publics ses modèles et ses données, Trend Micro espère favoriser la transparence, la vérifiabilité et l'innovation collaborative autour de l'IA dédiée à la cybersécurité.

Richard de la Torre,
technical product marketing manager, enterprise solutions chez Bitdefender

«Des tâches auparavant manuelles et chronophages, telles que la collecte de données et l'exploration de réseaux à la recherche de vulnérabilités exploitables, sont désormais effectuées par l'IA générative.»

Face aux cybermenaces, la détection des vulnérabilités devient stratégique. En combinant les outils spécialisés, et le recours aux services des experts en découverte de failles, les organisations renforcent leur posture de sécurité.

Des outils et des services *pour détecter les failles avant les hackers*

Selon les prévisions de Gartner en matière de sécurité de l'information en 2024, le marché mondial des services de cybersécurité devrait croître de 15,6% en 2025. Celui de la découverte de vulnérabilités est en phase avec ce mouvement général d'externalisation. Car au-delà des failles identifiées par les éditeurs ou via les programmes de bug bounty (voir encadré), les organisations restent exposées à d'autres risques concrets : mauvaises configurations par rapport aux référentiels de sécurité, vulnérabilités zero-day ou encore composants non inventoriés – un phénomène accentué par le développement de la Shadow IT. «*La découverte de failles est un sujet extrêmement vaste, il y a de nombreuses façons de faire pour une approche de bout en bout*», explique Christophe Menant, directeur de l'offre cybersécurité chez Capgemini. Le recours à des solutions automatisées et à des prestataires spécialisés se généralise donc. De nombreux acteurs sont présents aujourd'hui sur le marché, avec des approches diverses selon les besoins (applications, infrastructures, cloud, IoT). Pour les DSI et les RSSI, un des défis consiste à se repérer dans ce paysage complexe et à choisir les partenaires ou solutions les mieux adaptés à leur contexte.

Christophe Menant,
directeur de l'offre cybersécurité chez Capgemini

« La découverte de failles est un sujet extrêmement vaste, il y a de nombreuses façons de faire pour une approche de bout en bout. »

Agir le plus tôt possible dans la chaîne du développement

Le premier terrain sur lequel une organisation peut agir est celui du développement logiciel. Les démarches de type DevSecOps visent précisément à intégrer la sécurité dès les premières étapes du cycle de développement logiciel (SDLC). Les solutions de type SAST, pour Static Application Security Testing, sont conçues pour analyser automatiquement le code source afin d'identifier en quasi temps réel les failles avant que l'application ne soit déployée. Leur intégration directe dans les chaînes CI/CD permet d'éviter des coûts élevés de correction en phase de post-production, puisque les anomalies sont corrigées au fil de l'eau, lors du développement. «*Plus tôt on détecte la vulnérabilité et moins cela coûte cher à l'organisation*», rappelle Christophe Menant. Les solutions proposées par GitLab CI/CD, Checkmarx ou Black Duck s'inscrivent dans cette logique, certaines intégrant aujourd'hui des modules d'intelligence artificielle capables non seulement de détecter les failles, mais aussi de suggérer des pistes de correction.

Pour les applications en production, le SAST atteint en revanche ses limites. Cette méthode nécessite en effet un accès direct au code source et ne teste pas l'application dans son environnement opérationnel, avec ses intégrations, ses dépendances et ses comportements réels. De ce fait, ce sont ici les approches dynamiques qui sont privilégiées, à travers des solutions dites DAST (Dynamic Application Security Testing). «*La détection de failles se découpe en deux grandes catégories. D'une part, la découverte par rapport à une base de données de failles déjà connues, ce qui est plus facilement automatisable. D'autre part, le recours à des spécialistes avec des compétences en découverte de failles*», précise Christophe Menant. Ces deux approches se complètent dans une stratégie de détection cohérente.

Des approches qui se complètent

Des solutions comme IBM QRadar ou CybelAngel permettent par exemple de cartographier et de surveiller la surface d'attaque externe, en identifiant en continu les actifs connectés à Internet et en vérifiant leur niveau de sécurité. Elles s'appuient sur des bases de vulnérabilités connues et mettent à jour leurs modèles au fur et à mesure de l'émergence de nouvelles menaces. Leur pertinence réside dans leur capacité à automatiser une grande

partie de la détection, mais elles se heurtent à un problème bien connu : la surcharge d'alertes et l'impossibilité pratique de traiter toutes les vulnérabilités détectées. *«Il faut réussir à identifier celles qui doivent être traitées en priorité»*, insiste Christophe Menant. Or, la criticité est liée au contexte propre à l'organisation, notamment à l'exposition de l'actif concerné, au scénario d'exploitation envisageable et à l'impact potentiel sur les métiers. L'expertise humaine complète ce socle automatisé. Les cabinets de conseil, les ESN et les start-up spécialisées viennent renforcer les dispositifs existants en simulant des attaques réelles. Certaines structures ont une expertise ciblée sur des pans précis de la détection de vulnérabilités. C'est le cas de FuzzingLabs avec, comme son nom l'indique, le fuzzing : *«Cette méthode consiste à envoyer des données aléatoires ou pseudo-aléatoires sur une application-cible afin de voir si on peut lui faire faire des choses anormales»*, détaille son fondateur et CEO Patrick Ventuzelo. Cette technique, qui génère des milliers d'exécutions par seconde, met en évidence des comportements inattendus, dont certains peuvent être exploités par un attaquant pour obtenir des privilèges ou détourner un processus. *«Nous développons généralement un fuzzer pour le client, celui-ci va générer des millions de données intelligentes et spécifiques au contexte de l'application ciblée. Ensuite, nous formons les équipes du client pour leur apprendre à maintenir ces fuzzers sur le long-terme et leur donner les moyens de continuer la recherche de vulnérabilités de leur futur code»*, poursuit Patrick Ventuzelo.

Tester régulièrement

D'autres acteurs, comme Synacktiv, privilégient une approche offensive plus large, en proposant à la fois du pentest et du red teaming. *«Dans le pentest, nous venons tester un des systèmes de l'entreprise, généralement un site web. Le but peut être de réussir à devenir administrateur de tous les postes, ou à accéder à des informations sensibles en identifiant et en exploitant des failles»*, explique Kévin Tellier, expert sécurité chez Synacktiv. Cette approche vise à identifier un maximum de failles sur le système testé. *«Pour une entreprise qui n'a jamais fait de pentest sur son réseau interne, nous réussissons dans 95% des cas à compromettre son réseau en trois jours.»*

Le red teaming procède d'un autre objectif, en exploitant tous les moyens possibles (même les failles humaines grâce à des e-mails de phishing ou en s'introduisant sur site) jusqu'à atteindre des trophées (compromettre un environnement, accéder à une boîte mail, etc.), mais sans chercher à lister toutes les failles. *«Cette méthode intéresse de plus en plus le marché, et nous voyons le nombre de commandes bondir»*, ajoute-t-il.

Au-delà du résultat immédiat, ces exercices ont également une valeur stratégique : ils contribuent à mettre en lumière des vulnérabilités systémiques et multifactorielles, renforçant ainsi les arguments pour l'obtention de budgets cybersécurité accrus. Mais dans tous les cas, les tests devront être réguliers. **CHARLOTTE MAUGER**

Pentest, bug bounty ou red teaming

BUG BOUNTY : programme participatif mis en place par une entreprise visant à récompenser toutes personnes qui identifient et signalent des vulnérabilités sur un site ou un logiciel.
PENTEST : mission ponctuelle confiée à un prestataire pour tester la sécurité d'un système-cible en simulant des attaques. Cet exercice vise à établir la liste la plus exhaustive possible des vulnérabilités de ce système.
RED TEAMING : Un exercice global où un prestataire simule une attaque réaliste jusqu'à un objet précis, en utilisant tous les moyens à sa disposition. Le rapport produit ne liste pas les vulnérabilités des systèmes, mais les failles exploitées étape par étape jusqu'au trophée.

D'ici 2029, les certificats TLS (Transport Layer Security) ne vivront plus que 47 jours. Une décision portée par Google, Microsoft, Apple et validée par le CA/Browser Forum. Pour les RSSI, il faudra tourner la page des fichiers Excel et accepter une évidence : la gestion des certificats doit devenir industrielle, automatisée et gouvernée.

Certificats TLS plus courts : *industrialiser pour survivre*

Le cadenas de votre navigateur lors d'une connexion HTTPS ? Un symbole, celui de la présence du certificat numérique qui joue le rôle d'une carte d'identité pour le serveur auquel vous vous connectez et atteste de l'utilisation d'une clé de cryptage protégeant vos échanges. Ces certificats, émis au format X.509 par une autorité de certification (AC), comportent notamment deux champs, NotBefore et NotAfter, qui fixent leur période de validité. Tant qu'ils sont dans cette fenêtre, ils sont acceptés par le navigateur et permettent d'établir une connexion HTTPS chiffrée. En cas de compromission ou de dépassement des délais, les règles du CA/Browser Forum imposent une révocation sous 24 heures. Mais les mécanismes de révocation – qu'il s'agisse des CRL (listes de certificats révoqués) ou de l'OCSP (protocole de vérification en ligne) – sont souvent mal implémentés ou ignorés, si bien qu'un certificat compromis peut continuer à être utilisé, lors de communications mal sécurisées donc.

Romain Quinat,
chief marketing officer du groupe Nomios
« Nous aidons nos clients à industrialiser leur gestion. L'idée n'est pas de multiplier les certificats, mais d'éviter que leur complexité devienne un point de fragilité. »

Sans certificat valide, pas de confiance

La durée de vie des certificats (délai entre le NotBefore et le NotAfter) n'a cessé de raccourcir. De cinq puis trois ans, on est passé en 2018, à 825 jours (deux ans et trois mois). Au 1er septembre 2020, Apple a officiellement limité à 398 jours la durée de validité sur iOS et macOS, rapidement suivi par Chrome, Firefox et Edge. En avril 2025, le CA/Browser Forum a voté un plan encore plus drastique : 200 jours dès mars 2026, 100 jours en 2027, et seulement 47 jours à partir de mars 2029. *« Certains évoquent même dix jours à terme »*, souligne Romain Quinat, chief marketing officer du groupe Nomios, intégrateur œuvrant dans le domaine de la cybersécurité. Google, de son côté, avait déjà ouvert le débat en mars 2023 dans son document Moving Forward Together, plaidant pour une durée maximale de 90 jours.

Une logique sécuritaire, l'autre opérationnelle

Deux logiques expliquent cette accélération. La première est sécuritaire. Plus un certificat reste en circulation longtemps, plus sa clé privée est exposée. Et demain, l'ordinateur quantique pourrait accélérer la capacité de casser des clés cryptographiques aujourd'hui jugées robustes. *« Le raccourcissement des durées vise surtout à anticiper la fragilisation des algorithmes asymétriques (RSA, ECC) à l'ère post-quantique. »* La seconde raison est opérationnelle. Il s'agit, en rendant quasiment impossible une gestion « manuelle » de certificats à renouveler plus souvent, de forcer les organisations à automatiser ces renouvellements, ainsi que la vérification de la validité des certificats en usage.

Une usine à mettre en place

Pour une PME dotée d'un simple site vitrine, la contrainte reste supportable : il suffit de s'appuyer sur un acteur comme Let's Encrypt, qui renouvelle automatiquement les certificats tous les 90 jours. Mais à l'échelle d'un grand groupe, le décor change radicalement. Sa DSI doit veiller sur des milliers de

DIX GESTES BARRIÈRE CONTRE L'EXPIRATION

- **Cartographier :** recenser tous les certificats, y compris internes, oubliés dans des API ou sur des VPN. L'oubli d'un seul certificat peut bloquer une chaîne métier.
- **Classifier :** distinguer les certificats vitaux (paiements, messageries sécurisées) des secondaires.
- **Centraliser :** créer un registre unique, dynamique, qui remplace Excel. Comme pour l'adressage IP, il faut passer de la feuille statique à l'IPAM (IP Address Management) dynamique.
- **Superviser :** mettre en place un monitoring actif, avec alertes avant expiration.
- **Automatiser :** adopter ACME ou les API des autorités de certification.
- **Industrialiser :** intégrer cette logique dans les pipelines CI/CD. Dans une entreprise DevOps, chaque déploiement applicatif doit inclure ses certificats.
- **Sécuriser :** protéger les clés privées dans des coffres-forts numériques.
- **Former :** sensibiliser les équipes techniques. Le RSSI ne peut pas tout porter seul : les DevOps, les exploitants et les métiers doivent comprendre l'enjeu.
- **Aligner :** inscrire la gestion des certificats dans les politiques NIS 2, DORA, ISO 27001, SecNumCloud.
- **Prévoir un plan B :** définir une procédure d'urgence manuelle pour les cas extrêmes.

certificats disséminés dans le SI : sites internes, applications métiers, API, messagerie, VPN… La moindre négligence peut se transformer en incident majeur.

Des exemples ? En 2021, un certificat oublié a suffi à plonger Facebook dans le noir pendant plusieurs heures, entraînant une panne mondiale. En février 2021, c'est Google Voice qui est resté hors service plus de quatre heures à cause d'un certificat TLS expiré, conséquence d'un renouvellement manqué. Même scénario en février 2020 pour Microsoft Teams, tombé en panne durant trois heures, privant ses millions d'utilisateurs d'accès à la messagerie et aux appels, là encore pour un certificat d'authentification périmé. Ces incidents rappellent qu'un simple oubli peut suffire à créer une interruption massive de service – et jusqu'à 15 M$ de pertes pour une grande entreprise, selon certaines estimations.

Impossible de continuer avec un simple tableur

Longtemps, la gestion des certificats s'est faite à la main. Un fichier Excel, quelques colonnes, un rappel Outlook… *« Tant qu'il y avait un renouvellement annuel, ça passait. Mais à 100 jours, et a fortiori à 47, c'est terminé »*, tranche Romain Quinat. Deux chantiers s'ouvrent donc pour les RSSI. Le premier, assez simple, consiste à automatiser la demande et la réception d'un certificat auprès des autorités de certification avec le protocole ACME (Automatic Certificate Management Environment), standard largement adopté dans l'écosystème. *« C'est la partie la plus simple, parce que c'est standardisé. Mais attention, encore faut-il que toutes les applications soient compatibles ACME. Dans les environnements legacy, c'est loin d'être toujours le cas. »* Le second chantier est autrement plus délicat : installer automatiquement le certificat renouvelé dans les applications, serveurs, répartiteurs de charge (load balancers), voire dans Outlook pour les certificats personnels utilisés en messagerie chiffrée.

« C'est là que la vraie complexité apparaît », insiste Romain Quinat. L'obstacle n'est pas seulement technique. C'est aussi une question de responsabilité. Dans de nombreuses organisations, c'est le RSSI qui gère la relation avec l'autorité de certification, mais ce sont les responsables applicatifs qui installent les certificats. Et lorsque l'un oublie sa mission, l'autre accuse. *« Avec des cycles à 47 jours, on ne pourra plus se renvoyer la balle. »*

Une coopération entre RSSI et responsables applicatifs

Surtout, le RSSI n'a plus vocation à vérifier chaque date de péremption. *« Le renouvellement en soi n'a aucun intérêt pour lui*, affirme Romain Quinat. *Son rôle, c'est la vigilance : révoquer un certificat compromis, gérer les cas de clés volées, garantir la gouvernance et la conformité. »* Les organisations les plus matures, déjà engagées dans des pratiques DevOps, pourront intégrer la gestion des certificats dans leurs pipelines CI/CD (Continuous Integration/Continuous Delivery). Les autres, encore organisées en silos, devront avancer domaine par domaine.

Ce basculement s'inscrit dans un contexte réglementaire plus large. Les textes européens comme NIS 2 (Network and Information Security Directive) ou DORA (Digital Operational Resilience Act) n'évoquent pas directement les certificats, mais imposent continuité, traçabilité et résilience. *« La réduction des durées va dans ce sens*, observe Romain Quinat. *Les normes ne disent pas "vous devez gérer vos certificats", mais elles fixent un cap. Les RSSI n'ont plus le choix. »*

THIERRY DEROUET

Officiellement, la cybersécurité européenne existe depuis la création en 2004 de l'Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA). Depuis, d'autres initiatives ont vu le jour comme le Centre européen de lutte contre la cybercriminalité (EC3), le réseau CyCLONe ou encore des normes de cybersécurité de l'Union européenne, sans oublier le règlement européen sur la cyber-résilience de 2024. Mais sur le terrain, la réalité est plus floue.

L'Europe, *géant réglementaire aux pieds d'argile*

L'Europe dispose d'une large palette de textes en matière de cybersécurité. Cette année encore, la Commission européenne a lancé de nouvelles initiatives pour promouvoir notamment la cyberrésilience, avec la première législation de l'UE traduite en exigences de protection. Le 4 février a aussi marqué l'entrée en vigueur de la loi européenne sur la cybersolidarité (Cyber Solidarity Act). Le bouclier européen se construit donc, au moins réglementairement.

Pourtant, *«l'Europe est la seule à croire au libéralisme appliqué à la lettre. Elle est un peu la "naïve du village libéral", elle est plus royaliste que le roi»*, affirme Thomas Kerjean, PDG de Mailinblack. Après avoir vécu en Chine et aux États-Unis, il observe que ces pays n'hésitent pas à adopter des stratégies protectionnistes et souveraines pour leurs industries. Cette différence d'état d'esprit se remarque particulièrement en France, selon le député Philippe Latombe, auteur d'un rapport sur la souveraineté numérique en 2021 : *«Nous avons un problème de mentalité et de culture. Les fournisseurs ne collaborent pas suffisamment, contrairement au modèle allemand du "chasser en meute". Il rappelle aussi que le marché des capitaux mobilisables à l'échelle européenne est très étroit : cela rend les introductions en bourse difficiles et entraîne un manque de liquidité, donc moins d'investissements, contrairement à Israël»*.

Malgré tout, le député croit en l'émergence d'une cybersécurité européenne, qu'il juge presque inexistante aujourd'hui (voir ci-après). Il propose la création d'une *«BITC, une base industrielle et technologique de cybersécurité, sur le modèle de la BITD dans la défense. Nous en avons un embryon en France, mais pas en Europe. À part la réglementation NIS 2, il n'y a pas grand-chose d'autre. Or il faut une structure de ce genre pour donner un élan suffisant et participer à la souveraineté numérique.»* Cette initiative doit selon lui se faire à l'échelle européenne.

La sophistication croissante des menaces pousse à une approche collaborative des acteurs

Plaidoyer pour un BTIC

En attendant, le constat est sans appel : la cybersécurité européenne est très fragmentée. *«Les règlements comme le RGPD ou NIS 2 existent, mais il n'y a pas d'intention unifiée»*, insiste Thomas Kerjean. *«Ces normes créent un cadre commun, mais l'écosystème ne vit pas à l'échelle de l'Union, chaque pays agissant dans son propre intérêt»*, ajoute Benoît Grünemwald, directeur des affaires publiques chez ESET. Pour lui, la cybersécurité européenne est toutefois en construction : *«Elle s'appuie sur des habitudes d'échanges et de coopération entre pays et s'élabore sur un marché jeune, ce qui facilite sa mise en œuvre.»* Le numérique favorise l'interopérabilité plus que les secteurs traditionnels, grâce à des outils souvent standardisés, facilitant les ajustements techniques. Et l'Europe légifère activement sur ces normes et plateformes communes.

La sophistication croissante des menaces pousse aussi à une approche collaborative des acteurs, intégrant leurs solutions pour protéger efficacement les clients. *«Si l'antivirus était la panacée au début, aujourd'hui ce n'est qu'une brique parmi d'autres. Pour être efficaces, toutes ces briques doivent communiquer et se reconnaître»*, explique Benoît

Grünemwald. «*Reste à vérifier si les entreprises européennes privilégieront la coopération ou la concurrence pure*», poursuit-il.

Sur le volet commercial justement, la complexité des marchés publics, leurs processus fastidieux, limitent l'expansion transfrontalière des sociétés. Leur diffusion européenne reste incertaine. D'autant qu'elles doivent faire face à la concurrence venue d'autres continents, notamment d'acteurs israéliens performants et américains, alimentant le débat sur la souveraineté numérique. «*70% du marché est détenu par des sociétés américaines, notamment pour la sauvegarde et les outils*», note Tibaud Estienne, expert en régulations chez SPAC Alliance (Smart Physical Access Control Alliance, organisation européenne rassemblant les acteurs de la sécurité physique et logique). Il reste néanmoins optimiste : «*On va petit à petit avoir un cadre européen efficace, adapté et durable*». Il espère voir la cybersécurité européenne évoluer favorablement d'ici 2028-2029, le temps que les grandes régulations structurantes produisent leurs effets. Cet optimisme s'appuie aussi sur une philosophie européenne de la cybersécurité, moins brutale que l'approche américaine illustrée par le Cloud Act. «*Techniquement, la France et l'Europe ont les solutions pour supporter cette approche*», affirme Tibaud Estienne, évoquant aussi le «Digital Decade Policy Program 2030», qui vise à créer un écosystème complet incluant IA et prémices de l'ère quantique, avec une capacité autonome de protection, redémarrage et innovation. Une vraie chance de rebattre les cartes dans l'avenir.

AUDE LEROY

3 QUESTIONS À **Philippe Latombe,** député de Vendée (85)

Pourquoi la France est-t-elle si forte en cybersécurité ?

La France dispose d'écoles d'ingénieurs de très bon niveau et a rapidement identifié la cybersécurité comme un enjeu stratégique. Des entreprises s'y sont impliquées très tôt, et l'ANSSI joue depuis plusieurs années un rôle clé dans la structuration de l'écosystème, notamment via d'anciens membres ayant fondé des start-up désormais bien établies.

Elle pèse cependant peu au niveau international, pourquoi ?

Notre écosystème reste principalement constitué de sociétés en phase d'amorçage. Il manque des entreprises ayant atteint une taille critique. Plusieurs cas l'illustrent : Wallix, introduite en bourse en 2015, peine

encore à se développer ; Vade, mal préparée à son expansion aux États-Unis, a été laminée par Proofpoint, puis contrainte de s'associer à l'allemand Hornetsecurity… lui-même racheté par Proofpoint en mai dernier. Les acteurs américains disposent d'une capacité de levée de fonds qui leur permet des acquisitions prédatrices, alors qu'en France, peu d'entreprises ont atteint un niveau de maturité suffisant pour devenir elles-mêmes acquéreuses. Résultat : nous avons de grosses PME, mais pas d'acteurs de stature internationale. Il existe sans doute un problème d'éducation et de management : en France, on observe une tendance aux sorties de capital («exits») sans réinvestissement systématique, contrairement à la culture israélienne où un exit génère immédiatement la création de nouvelles start-up. Autre difficulté : le manque de coopération entre acteurs. Faute de confiance, même lorsque 90 à 95 % des activités ne sont pas concurrentes, les entreprises hésitent à s'associer, notamment pour répondre à des appels d'offres. Cette méfiance freine les synergies et la dynamique collective.

Quelles seraient les solutions d'émergence d'une cybersécurité européenne ?

D'abord, il faut un véritable marché des capitaux à l'échelle européenne, pour disposer de liquidités et permettre aux entreprises de passer à l'échelle, investir massivement et se développer à l'international – un processus coûteux nécessitant des fonds mobilisables. Ensuite, il est essentiel que la commande publique, et même privée, privilégie les entreprises européennes. Ce point progresse actuellement, notamment face à l'hégémonie croissante des acteurs américains (par exemple sur les systèmes d'exploitation), qui finit par soulever des enjeux de souveraineté. **AL**

Devant la hausse exponentielle de cyberattaques, l'État a mis en place de nombreux outils pour les différents publics, allant de la TPE aux plus grandes entreprises. Au risque de provoquer une certaine confusion.

Appuis publics à la cybersécurité des entreprises, *une cartographie complexe*

Historiquement, l'État français a commencé à organiser la lutte contre les cybermenaces dès 2004 pour les sites gouvernementaux, les institutions, les opérateurs d'importance vitale (OIV). Ces derniers ont pour interlocuteur l'Agence nationale de la sécurité des systèmes d'information (ANSSI), sous la houlette du SGDSN. En cas d'incident de sécurité, un formulaire dédié est à remplir et à envoyer en ligne.

L'évolution des menaces, leur nombre toujours plus grand, leur sophistication ont conduit à la définition d'une politique spécifique de cybersécurité par la Revue stratégique de cyberdéfense de 2018. Elle s'est alors accompagnée de l'entrée en vigueur de la directive européenne NIS 1 de 2016. Trois autres textes, NIS 2, REC et DORA, qui devaient être adoptés cet automne, mais restent largement soumis aux aléas de la situation politique du pays, vont élargir le champ des organismes soumis à des obligations de gestion des risques et d'informations en cybersécurité, en fonction de leur criticité, de leur secteur et de leur taille – on passe de 500 à 15 000 entités concernées.

Au sujet des sinistres à proprement parler, depuis 2017, le GIP cybermalveillance.gouv.fr aide en cas d'escroquerie ou de cyberattaque l'ensemble du spectre français : grand public, entreprises privées (ETI, PME, TPE), administrations, organismes publics, collectivités territoriales non régulées. En 2023, la plateforme a été visitée par plus de 3,7 millions de personnes et a analysé plus de 280 000 demandes d'assistance.

L'offre publique fourmille, apportant souvent beaucoup de confusion

Abondance de biens ne nuit pas ?

La prise de conscience de l'impérieuse sécurisation des collectivités publiques, des PME et TPE s'est accompagnée d'une prolifération de services d'accompagnement et autres outils, parfois difficilement lisibles. Parmi eux, MonAideCyber (MAC) permet des diagnostics rapides et gratuits des systèmes d'information. Cet outil est une déclinaison et une extension de celui de la Gendarmerie nationale, DIAGONAL (DIAGnostic Opérationnel NationaL Cyber). Sur le même thème, la Direction générale des entreprises (DGE) a conçu en 2023 le dispositif CyberPME. D'autres mécanismes sont en cours d'installation comme le filtre anti-arnaque destiné aux professionnels assujettis à l'obligation de mise en œuvre du filtre national de cybersécurité au bénéfice de la DGE.

Parallèlement, des formations sont accessibles, soit directement proposées par l'ANSSI – son Centre de formation pour la sécurité des systèmes d'information (CFSSI) en propose aujourd'hui 29, gratuites, pour les agents publics, les personnels de OIV et OSE –, soit via son label SecNumdu (65 formations valides aujourd'hui).

L'offre publique fourmille donc, apportant souvent de la confusion. Ce que la Cour des comptes, dans la conclusion intermédiaire de son rapport du 16 juin 2025, n'a pas manqué de souligner : *«Il apparaît nécessaire de fixer des objectifs clairs aux dirigeants d'administration, dans leur lettre de mission, concernant l'homologation des systèmes d'information, pour garantir la vigilance nécessaire en la matière [...] Quant à l'accompagnement de l'écosystème, il a été concrétisé par des "outils" emblématiques comme le Campus cyber, efficients comme le GIP Acyma, mais sans définir précisément leurs missions ni leur financement pérenne. Il convient désormais d'élaborer leur modèle économique, en phase avec les besoins du secteur. Par ailleurs, des dispositifs de soutien aux entités les plus fragiles ont été créés par accumulation. Il apparaît nécessaire de les articuler pour les rendre plus lisibles.»* Encore un effort pour notre cybersécurité à tous...

AUDE LEROY

Officiellement hors du champ régalien, la Santé n'échappe pourtant pas aux enjeux de sécurité nationale. Face aux cyberattaques croissantes, parlementaires et experts dénoncent l'inaction de l'État, les failles budgétaires et l'absence de cadre clair de responsabilité.

Cybersécurité de nos hôpitaux, *une mission de l'État ?*

Si officiellement la Santé n'est pas l'une des quatre fonctions régaliennes de l'État, la pandémie de Covid-19 en a certainement modifié la perception chez les citoyens, en ce sens qu'elle a eu des effets sur leur sentiment de sécurité, dont le maintien relève pour le coup de ces missions régaliennes. Ceci explique peut-être que dans son rapport du 6 janvier 2025, sur «La sécurité informatique des établissements de santé», la Cour des comptes étrille le faible investissement de l'État dans la protection de leurs systèmes d'information (1,7% du budget d'exploitation en moyenne contre 9% dans la banque et 2% dans l'industrie des biens de consommation). Un constat partagé par des parlementaires qui pointent un manque d'intérêt des directions, sans risque de sanctions.

Olivier Cadic, sénateur représentant les Français établis hors de France (UC), n'y va pas par quatre chemins : *«Une attaque cyber à l'encontre des hôpitaux relève d'un acte criminel s'il provient d'un gang organisé pour collecter de l'argent. Si c'est une attaque d'un État étranger, cela relève du sabotage. Mettre hors d'usage un établissement de soins peut entraîner des conséquences fatales. La question fondamentale est : à quel moment analyse-t-on que c'est un acte de guerre ? À quel moment l'État considère-t-il qu'il doit être en première ligne ?»*

Pas de responsables

Dénonçant une asymétrie problématique de responsabilité entre hôpitaux publics et privés, le sénateur déplore qu'il *«n'existe aucun cadre clair établi pour déterminer quand et comment la responsabilité de l'État s'applique, particulièrement lorsque le secteur privé ne peut pas se défendre contre des attaques de niveau étatique»*. Le parlementaire se dit choqué du manque de prises de responsabilités de l'État, lors des cyberattaques d'établissements de soins. Au lendemain de l'attaque informatique de l'hôpital de Corbeil-Essonnes en août 2022, Olivier Cadic avait posé la question au SGDSN : *«Vers qui la victime se retourne-t-elle ? Contre celui qui dirige le service informatique de l'hôpital, contre le patron, contre l'agence sanitaire ? Personne ne savait me répondre.»* Pour lui, le rôle de l'État est de protéger le citoyen dans les domaines régaliens, *«et là, on y est !»*

Philippe Latombe, député de Vendée (Renaissance), n'est pas plus tendre et trouve inadmissible qu'un patron de centre hospitalier départemental ne soit jamais sanctionné si une fuite de données survient alors que le système informatique n'a pas été sécurisé : *«Les directeurs d'hôpitaux et les Agences régionales de Santé (ARS) sont complètement indépendants, c'est un califat dans le califat. C'est hallucinant, j'ai rarement vu ça. Ils ont une autonomie de gestion telle que ça en devient scandaleux. Un directeur d'hôpital fait ce qu'il veut. L'ARS, si elle n'a pas envie, elle ne fait pas. Quant au ministre de la Santé, il n'a pas la main sur l'ARS, il n'a pas la main sur les directeurs d'hôpitaux, ou alors quand vraiment il y a eu des grosses bêtises.»*

L'Agence du Numérique en Santé du ministère a pourtant mis en place un plan de protection cyber des hôpitaux 2023-2027, avec un budget fléché pour la cybersécurité et envoyé à toutes les ARS. Philippe Latombe précise : *«Seules trois ARS, comme celle de Bretagne ou celle des Pays de la Loire, ont consommé le budget alloué au niveau national. Les autres n'y ont absolument pas touché. Cela crée des inégalités de protection entre les régions. En réalité, tout dépend de l'intérêt des dirigeants locaux pour le sujet.»*

Les deux parlementaires en concluent que privilégier des investissements dans les RH et l'équipement médical (scanners, robots chirurgicaux...) au détriment de la cybersécurité est un non-sens. Cette approche est coûteuse, à long terme et l'État a selon eux bel et bien un rôle à jouer dans ce domaine, régalien ou pas.

AUDE LEROY

Face à une cyberadversité qui ne désarme pas, bien au contraire, le tandem DSI-RSSI se réinvente. Désormais complices plus que rivaux, ces deux rôles essentiels naviguent entre enjeux de gouvernance, pressions budgétaires et impératifs de sécurité. Un équilibre délicat à tenir, mais vital pour piloter la transformation numérique en toute confiance.

DSI et RSSI *ont appris à jouer en équipe*

L'année 2025 aura été celle de la *«montée en puissance du cyber adversaire audacieux»*, selon l'éditeur Crowdstrike dans son rapport annuel. Face à cet ennemi de plus en plus protéiforme, se dresse un duo aux missions et intérêts divergents, en apparence tout au moins, le tandem DSI et RSSI. Et de fait, bon enfant, Alain Bouillé, directeur général du CESIN (Club des Experts de la Sécurité de l'Information et du Numérique), qui a fait toute sa carrière dans l'IT et souvent sous la houlette d'un DSI, résume ainsi la relation entre ces deux postes : *«Je t'aime, moi non plus.»* La formule donne à entendre la difficulté d'un équilibre à trouver entre les deux fonctions, et toute la complexité d'une relation soumise à de multiples pressions. Une relation qui évolue au rythme des transformations de l'entreprise, d'un *«système d'information qui n'est plus entre quatre murs»*, et d'un projet en constante réinvention, celui de la cybersécurité.

Alain Bouillé,
directeur général du CESIN
« Le pire que puisse dire un RSSI à un DSI, c'est : je te l'avais bien dit. Même lors d'un plantage, on assume à deux ; sinon, on perd la crédibilité et la confiance. »

Deux modèles de gouvernance

Le RSSI a longtemps été rattaché à la DSI, faisant de lui juste un collaborateur, voire un subalterne, *«le forçant à batailler pour faire entendre sa voix, et faire respecter ses prérogatives auprès de la direction»*. Surtout, cette situation le privait d'un budget propre. Une spécificité française ? *«Quand on est CISO outre-Atlantique, on est chef* [chief, NDLR], *on est donc rattaché au board, tandis que quand on est RSSI, on est juste responsable»*, explique en tout cas Sébastien Drouin, président du XV DSI, qui a commencé dans l'IT au Canada, avant de passer côté cybersécurité au cours d'un séjour de dix ans en Australie.

Si cette distribution des rôles perdure dans les petites et moyennes structures, ce n'est plus le cas dans les grands groupes depuis *«2017, et les premières grandes cyberattaques qui ont paralysé des géants comme Renault ou Saint-Gobain»*, se rappelle Alain Bouillé. Ces coups de tonnerre répétés ont bousculé la vision de la cybersécurité et de sa représentation dans l'entreprise.

L'accès au Comex et au budget, la clé de tout

Alors que *«le RSSI était vu comme un empêcheur de transformer en rond»*, selon Alain Bouillé, ces attaques ont aussi modifié en profondeur cette relation. Des organismes comme l'AMF recommandent désormais de *«placer le RSSI du côté risque de l'organisation, sans lien hiérarchique et au même niveau si possible qu'un DSI dans l'organigramme*, explique-t-il : *C'est le cas pour un bon tiers des RSSI du CESIN.»*

Dès lors, le couple DSI et RSSI est plus équilibré. Tandis que le DSI continue de porter le cœur du projet numérique de l'entreprise, le *«RSSI a son budget en propre, gagne en autonomie,* continue le directeur général du CESIN. *Si on regarde les entreprises du CAC 40 et du SBF 120, il est assez rare de trouver un RSSI en dessous du niveau N-2 au Comex.»*

Ces RSSI ont donc bien plus de facilités à obtenir des budgets et à acheter des outils coûteux, comme les EDR. Même si, précise Alain Bouillé, quand les crises sont passées, on observe toujours un tassement des financements et le retour des tensions sur la dépense. *«Qui voudrait payer quand tout va bien ?»*, s'amuse d'ailleurs Sébastien Drouin.

Cette situation dans les grandes entreprises est loin d'être la norme dans les sociétés plus petites ou dans d'autres secteurs, notamment hospitaliers. D'une part, parce que les experts n'y sont pas assez nombreux, même si des efforts sont faits. D'autre part, parce que *«toutes les structures n'ont pas les moyens ou la maturité pour aborder la cybersécurité telle qu'elle devrait l'être aujourd'hui»*,

nous explique Christian Sarazin, responsable du système d'information du Centre hospitalier de Martigues, et ancien RSSI. Dans son poste actuel, lui-même est à la fois DSI et RSSI, et applique une politique centralisée.

Un duo, mieux un trio

Pour être encore plus forts, la solution universelle consiste à transformer le duo en trio, en impliquant les métiers au cœur de la relation, par exemple pour lutter contre la Shadow IT, ou sa dernière évolution, la Shadow IA. Le RSSI se doit d'échanger avec ces directions et leur apporter des solutions. *«Il n'a pas à être dans une position dogmatique de refus. Il est là pour comprendre les enjeux du métier et l'accompagner à petits pas»*, affirme Sébastien Drouin. Ce que confirme par l'exemple Christian Sarazin : *«Utiliser WhatsApp dans le milieu professionnel répond à un besoin réel. C'est à nous de l'entendre et de proposer une alternative plus sécurisée»*, notamment pour les données médicales des utilisateurs. Si le RSSI travaille bien, jugent nos trois interlocuteurs, son rôle de contrôleur deviendra un rôle de vigie, qui permettra de voir émerger les usages à risques avant même que le DSI soit informé. *«J'ai souvent vu des DSI venir aux nouvelles dans mon service»*, explique ainsi Alain Bouillé. De «gêneur», le RSSI devient ainsi un allié.

Un couple qui regarde dans la même direction

Dans cette relation mieux équilibrée, *«le mauvais, c'est celui qui ignore l'autre»*, tranche Christian Sarazin pour souligner que le DSI et le RSSI se doivent de collaborer. *«Un peu comme dans un couple qui se dispute parfois, mais doit faire front devant les enfants»*, illustre Sébastien Drouin. Un couple où le RSSI doit faire preuve de pédagogie, de compréhension et toujours affiner l'équilibre entre une sécurité parfaite inaccessible et une souplesse fonctionnelle primordiale. Un couple où il peut aussi y avoir des dissensions, mais jamais devant les métiers, et jamais en cas de crise. *«Le pire que puisse dire un RSSI à un DSI, c'est : je te l'avais bien dit,* prévient Alain Bouillé. *Même lors d'un plantage, on assume à deux ; sinon, on perd la crédibilité et la confiance.»*

Cette complémentarité est vitale dans bien des situations, par exemple pour réaliser des simulations d'attaques pertinentes et efficaces, qui permettront d'éviter le pire, notamment dans les hôpitaux. Vitale aussi lorsque la DSI doit déployer ses solutions en tenant compte des réglementations, mais sans sombrer dans une vision de *«la sécurité check the box»*, indique Alain Bouillé. Cette manière d'agir vise à satisfaire les régulateurs, mais sans prendre en compte le réel, les failles nouvelles, les besoins... Autant d'évolutions qui exigent que la DSI travaille au contraire main dans la main avec le RSSI.

Et c'est encore mieux bien sûr *«si le RSSI est intégré dans les projets IT dès le départ, en mode sécurité by design»*, assure Sébastien Drouin. À ses yeux, les régulations, comme NIS 2, représentent une carte à jouer pour les RSSI, pas tant pour gagner en pouvoir que pour participer plus activement à la modélisation du progrès numérique en entreprise. *«La cybersécurité n'est plus une lubie du RSSI, mais une obligation»*, insiste-t-il. D'ailleurs, cela fait longtemps que les obligations liées au RGPD, et l'apparition de nouveaux postes, comme ceux de DPO, en complexifiant la partition numérique, donnent plus de poids au RSSI, qui *«joue un rôle central dans la mise en place de la stratégie de protection des données personnelles»*.

Le poste évolue donc, vers celui de «risk manager», selon Sébastien Drouin. Il prend en charge la *«sécurité au sens large»*, devenant un *«super gendarme de la sécurité et de la réputation de l'entreprise»*. À la DSI d'initier et de diriger le projet numérique, tandis que le RSSI l'accompagne et l'amende, en «bon technicien et fin stratège». Un pas de deux dont l'art est de maintenir l'unité alors que tout change, y compris l'équilibre entre risques et besoins. Un duo où chacun tient son rôle, avec ses outils et en fonction de ses obligations, pour que l'entreprise fonctionne et se transforme. Seuls d'accord, mais à deux, face aux adversaires. Et audacieux, eux aussi.

PIERRE FONTAINE

Confrontés à un déficit structurel de ressources, les acteurs de la cybersécurité ont beaucoup à gagner à attirer davantage de jeunes diplômés, de femmes, d'experts seniors, de professionnels en voie de reconversion ou de profils neuro-atypiques.

La cyber *doit élargir son vivier de compétences*

Intervenue courant 2024, la détente du marché de l'emploi IT ne profite qu'à la marge aux acteurs de la cybersécurité. Comme pour celui des experts de l'IA et du cloud, le recrutement des spécialistes cyber est toujours aussi difficile. Pourtant, le contexte géopolitique actuel conjugué à la prolifération et la sophistication des menaces permises par l'IA ne font qu'inciter les organisations à étoffer leurs équipes d'analystes SOC ou de pentesters.

Selon l'OPIIEC, l'Observatoire paritaire des métiers du numérique, 25 000 postes devraient être créés d'ici 2028 pour répondre aux besoins des entreprises. De 45 000 professionnels en 2004, l'effectif du secteur de la cybersécurité s'élèverait ainsi à 70 000 en 2028, soit un taux de croissance annuel de plus ou moins 10 % selon les spécialités.

Tous les métiers sont concernés, du pilotage de la politique de la sécurité, conduite par le RSSI et ses adjoints, à la détection et la gestion des incidents en passant par la conception et le maintien en conditions opérationnelles d'un SI sécurisé et conforme aux exigences réglementaires (NIS 2, DORA, Cyber Resilience Act).

Si l'expertise technique règne en maître dans le monde cyber, le rapport de l'OPIIEC insiste aussi sur l'importance des « soft skills » qui *« s'avèrent également essentielles »*. Il cite la compréhension fine des activités de l'entreprise, la communication efficace sur les enjeux cyber ou la capacité à gérer les situations de crise.

Une offre de formation « perfectible »

La pénurie de compétences entraîne mécaniquement une forte demande en formations initiales et continues. Malgré plus de 900 formations identifiées, l'offre est jugée « perfectible » par l'OPIIEC. L'Observatoire préconise d'intégrer la cybersécurité dans l'ensemble des cursus IT côté étudiants et de favoriser les parcours de reconversion professionnelle vers la cyber pour les employés en poste.

À condition de donner leur chance aux futurs experts. *« Avec la baisse des aides gouvernementales, les étudiants éprouvent des difficultés à trouver une entreprise pour leur alternance*, déplore par exemple Manon Pellat, cofonda-

Les neuro-atypiques font d'excellents analystes

En novembre 2022, le PEC (Pôle d'Excellence Cyber) publiait un *Manifeste pour plus de diversité & d'inclusion* où il encourage les entreprises du secteur à accueillir des profils neuro-atypiques. À savoir des personnes atteintes d'un trouble du spectre autistique, comme le syndrome Asperger. Pour favoriser leur intégration professionnelle, le pôle travaille avec les sociétés de services spécialisées Avencod et Audiconsult, les associations Atype-Friendly (ex-Aspie-Friendly) et AFG Autisme ou l'Institut Marie-Thérèse Solacroup en Bretagne. Parmi ses membres, Airbus et Capgemini sont particulièrement engagés sur le sujet. *« Les profils neuro-atypiques ont des compétences particulières à valoriser*, plaide le vice-amiral d'escadre Arnaud Coustillière, président du PEC. *Ce sont des professionnels particulièrement fiables et respectueux des consignes. Des capacités précieuses pour le métier d'analyste. »* Et de faire valoir pour convaincre une surreprésentation de personnes atteintes d'un trouble autistique à la tête des géants du numérique. Elon Musk, Bill Gates, Steve Jobs et Mark Zuckerberg compteraient parmi les « aspies » célèbres.

Ces experts cyber que l'on s'arrache

LES CINQ MÉTIERS CYBERSÉCURITÉ LES PLUS RECHERCHÉS

- Ingénieur cybersécurité
- Hacker éthique
- Analyste SOC
- RSSI
- Cryptologue

LES CINQ MÉTIERS QUI PROGRESSENT LE PLUS EN 2025

- Osint (open source intelligence) analyst
- Consultant GRC (gouvernance, risque, conformité)
- Expert DevSecOps
- Analyste forensic
- Fraud analyst

SOURCE GUARDIA CYBERSECURITY SCHOOL

trice de Cybersup, nouvel établissement d'enseignement supérieur qui a ouvert ses portes à la rentrée 2024. *Des recruteurs se plaignent de pénurie, mais n'embauchent que des professionnels justifiant de cinq à dix ans d'expérience.*»

Fruit d'un partenariat entre l'école de code La Plateforme et Frojal, la holding familiale du groupe d'édition Lefebvre Sarrut, Cybersup présente l'originalité d'ouvrir ses cursus aux sujets de gouvernance, de conformité réglementaire ou de géopolitique et de former aux softs skills. «*La cyber ce n'est pas que de la technique, c'est beaucoup de communication et de management de projet*», rappelle Manon Pellat.

S'écarter du stéréotype du hacker au sweat à capuche

La dirigeante insiste aussi sur la passion qui doit animer les futurs experts. Elle conseille aux recruteurs de s'assurer que les candidats participent sur leur temps libre à des concours de type CTF (capture the flag), se défient sur la plateforme Hack the Box ou se retrouvent physiquement au salon leHACK.

Fondateur d'Ideuzo At_Work, agence de communication RH, Olivier Letort aide les DSI à développer leur marque employeur. Il leur conseille d'adopter une démarche disruptive et d'aller chasser sur Twitch ou TikTok et pas seulement sur les sites d'emploi. Plus généralement, il leur propose de s'écarter du profil-type. «*Trouver un expert cyber qui coche toutes les cases, c'est mission impossible. Les organisations doivent accepter de recruter un candidat qui répond à 70 ou 80 % des exigences, puis de le former en interne.*»

Par ailleurs, les employeurs gagneraient, selon lui, à élargir leur champ de prospection aux jeunes diplômés, aux femmes, aux profils seniors, aux professionnels en voie de reconversion. Sur ces différentes populations, c'est la sous-féminisation qui est la mieux documentée. Selon l'ANSSI, 11% seulement des actifs de la profession étaient des femmes en 2021.

Pour faire bouger les lignes, des associations comme le Cercle des femmes de la cybersécurité (CEFCYS) ou Women4Cyber France font la promotion des métiers de la cybersécurité auprès des lycéennes ou des étudiantes en faisant l'éloge de «rôle models». Le Pôle d'Excellence Cyber (PEC) propose, lui, depuis 2021, le programme des «Cadettes de la Cyber». Entre dix et quinze étudiantes en Master 1 ou 2 se voient tous les ans accompagnées par un parrain ou une marraine dans leur cursus et la définition de leur projet professionnel. En contrepartie, ces cadettes viennent témoigner dans les classes de 5e et de 1ère.

De son côté, né en 2014 à l'initiative du ministère des Armées et du Conseil régional de Bretagne, le PEC réunit des industriels comme Thales, Airbus, Capgemini, Orange ou Sopra Steria, des acteurs académiques, des laboratoires de recherche, des collectivités et des start-up au profit des métiers de la cyber. À travers son projet phare baptisé CyberSkills4All, lancé cet été et doté d'un budget de 23M€, le PEC vise, entre autres, à convertir aux métiers de la cyber quelque 15000 non spécialistes issus des sciences, de la santé, du droit ou de l'économie, et à sensibiliser 80000 lycéens, le tout en Bretagne et sur une période de cinq ans. Rendez-vous en 2030 ? **XAVIER BISEUL**

Tous les recruteurs le disent, recruter un expert cyber reste un défi. Pénurie de talents, mais aussi fort turnover, le secteur peine à trouver des bras. Cette situation persistante pousse les entreprises à externaliser leur cyber auprès de MSSP et à miser sur l'IA pour assurer les tâches les plus basiques.

Les MSSP, *une solution pour pallier la pénurie de talents cyber*

Avec des budgets en hausse de 10% par an entre 2024 et 2027, la cybersécurité va connaître son âge d'or en France. Et pour faire face au besoin, malgré la création prévue par l'OPIIEC de 25000 postes d'ici 2028 en France, les écoles et les centres de formation auront bien du mal à répondre... faute de vocations. Ce manque de ressources humaines pousse les entreprises à recourir de plus en plus aux services externalisés de sécurité.

TÉMOIN **Pierre Haïkal,**
SOC Manager France chez Nomios

90% des alertes arrivant sur notre SOAR sont traitées automatiquement

« Opérer un SOC sans analystes de niveau 1, c'est déjà une réalité chez Nomios. Nous avons aujourd'hui un taux d'automatisation de 90% de l'ensemble des alertes qui arrivent sur notre SOAR. Cette automatisation est réalisée par une équipe outillage qui développe toute l'ingénierie nécessaire sur le SOAR et travaille avec le concours des analystes de niveau 2 et 3 à réaliser ces automatisations. »

La montée en puissance du modèle MSSP

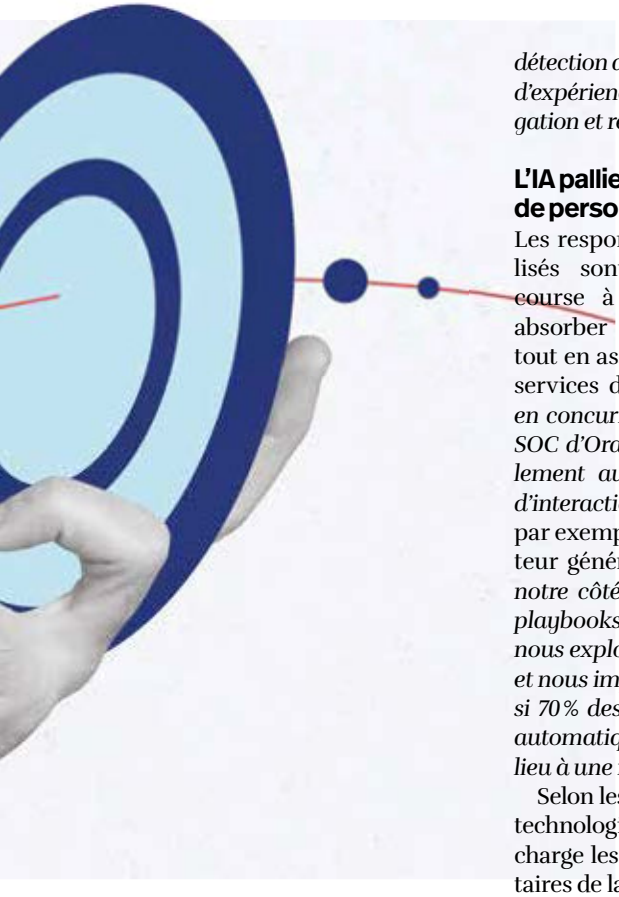
Selon Markess, le taux de croissance du marché des services de sécurité va s'élever en France à 12,5% par an jusqu'en 2027 où il pourrait atteindre 5,6 Md€. Parmi les moteurs de cette croissance, les MSSP, ces prestataires de service spécialisés qui délivrent des services cyber gérés en externe. On assiste ainsi à la montée en flèche des MDR (Managed Detection and Response), des services où les éditeurs et leurs intégrateurs assurent la supervision des EDR/XDR déployés dans les entreprises. De même, l'externalisation est de mise pour les SOC (Security Operations Center), en particulier auprès de grands acteurs comme les opérateurs de télécom, les ESN et les MSSP (Managed Security Service Provider) qui ont donné accès à ces solutions avancées à un plus grand nombre d'entreprises.

Pour certains services de cybersécurité offensive comme le bug bounty ou encore le red teaming, l'externalisation est même le modèle dominant. Enfin, les RSSI en temps partagé permettent clairement de mutualiser des ressources humaines rares et coûteuses. Directeur de l'organisme de formation cyber Sysdream, Ylan Elkeslassy souligne : *« Peu de PME ont la capacité de créer un poste à temps complet. Elles font donc appel à un expert en temps partagé. C'est un moyen pour elles d'avoir quelqu'un qui soit garant de la sécurité du SI, qui puisse sensibiliser le personnel et jouer le rôle de pendant au DSI. »*

Une externalisation synonyme d'automatisation à outrance

De nombreux MSP et ESN s'intéressent aujourd'hui au marché cyber et montent des activités MSSP. Fanny Sicard, ingénieur avant-vente en charge de l'offre MSP chez Hermitage Solutions, précise : *« Pour un intégrateur ou une ESN, devenir MSSP implique d'une part de mettre en œuvre de nouveaux outils, mais aussi de standardiser ses processus et structurer son offre. Cela passe par des outils de RMM (Remote Monitoring and Management), de PSA (Professional Services Automation) et par la documentation des processus, l'idée étant de réduire le plus possible les coûts d'exploitation pour améliorer sa rentabilité. »*

L'automatisation est la règle dans les SOC managés et ce sont les analystes de niveau 1, dédiés au tri des

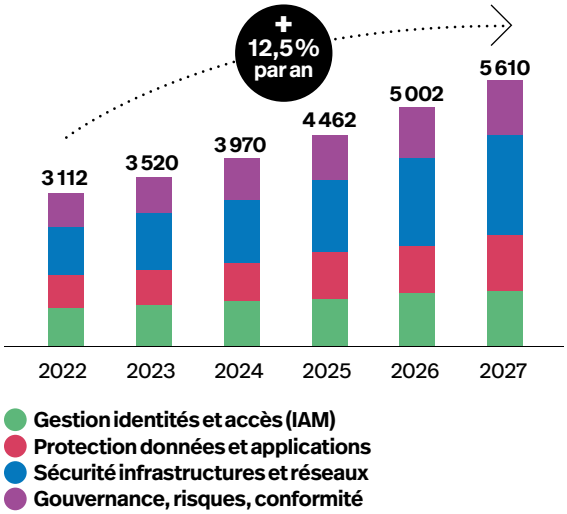


milliers d'alertes, qui sont remplacés par des process portés par les SOAR (Security Orchestration, Automation and Response). À chaque faux positif qui se répète, un script va éliminer l'alerte et soulager d'autant les équipes de permanence. Certains ont poussé le concept très loin en éliminant ce niveau 1 : aujourd'hui les MSSP revendiquent des taux d'automatisation de 90% des alertes. Pour y parvenir, ils ont modifié leur organisation interne. Auparavant, les analystes de niveau 2 et 3 étaient chargés de développer leurs automatisations en plus de leurs tâches d'investigation et de remédiation. Désormais, une équipe dédiée vient les aider dans cette tâche. *«Le fonctionnement est hybride : il est très important que les N2 et N3 soient toujours capables d'automatiser, de manière à ce qu'ils continuent de comprendre ce que fait l'équipe dédiée»*, continue Fanny Sicard. L'autre conséquence est une élévation du niveau d'expérience des nouvelles recrues : *«De fait, en 2025, nous avons recruté des analystes N2 et N3 et aucun analyste N1. Les N3 sont des experts en détection avec une dizaine d'années d'expérience, des experts en investigation et réponse à incident.»*

L'IA pallie déjà le manque de personnel dans les SOC

Les responsables de SOC mutualisés sont dans une véritable course à l'automatisation pour absorber de nouveaux clients tout en assurant la rentabilité des services délivrés. *«Nous sommes en concurrence avec l'offre Micro-SOC d'Orange Cyberdefense, totalement automatisée et avec peu d'interactions humaines*, explique par exemple Franck Burtin, directeur général de SNS Security. *De notre côté, nous développons des playbooks, des automatisations, nous exploitons des sources de CTI et nous implémentons de l'IA. Mais si 70% des alertes sont traitées en automatique, 30% donnent encore lieu à une intervention humaine.»*

Selon les éditeurs, la solution est technologique : l'IA va prendre en charge les tâches les plus élémentaires de la cybersécurité et consacrer les maigres moyens humains aux tâches les plus nobles. *«Sur une étude que nous avons menée auprès de 8000 RSSI, dont 300 en France, 89% des répondants expliquent qu'ils utilisent l'IA pour détecter les menaces, y répondre et remonter les systèmes*, résume Éric Vedel, directeur des activités et conseils en cybersécurité de Cisco. *Ces outils font aujourd'hui consensus dans les SOC afin d'atteindre une efficacité optimale. C'est une réalité et nous fournissons une intelligence augmentée avec tous nos outils XDR et SOAR au travers d'assistants conversationnels qui vont aider les analystes.»*



L'étude Cybersécurité – Données de marché (en M€) et perspectives d'évolution 2022-2027 de Markess by Exaegis montre la croissance rapide de la demande de services en cybersécurité auprès des entreprises françaises.

Les copilotes et autres assistants IA assurent l'enrichissement des données relatives aux alertes, effectuent les premières corrélations afin de prémâcher le travail des humains. Pour autant, la remédiation automatique reste encore très limitée : *«L'IA permet de simplifier la prise de décision des analystes, et d'automatiser le traitement de certains cas simples : si on détecte un fichier malicieux déjà bien identifié par plusieurs sources CTI, alors on peut le bloquer automatiquement. L'IA peut déjà réduire ce que l'on appelle l'alerte-fatigue chez nos analystes.»* En gommant les aspects les plus rébarbatifs du métier, peut-être ces outils vont-ils aussi contribuer à redorer le blason de la cyber et convaincre enfin les populations les moins représentées – jeunes, femmes – à s'y intéresser enfin. **ALAIN CLAPAUD**

TÉMOIN **Franck Burtin,** directeur général de SNS Security

«Les PME et les ETI n'ont pas les compétences pour internaliser un SOC. La technologie et les menaces évoluent trop vite. Nous leur mettons à disposition trois SOC, deux en France et un troisième au Vietnam afin de suivre les incidents de sécurité en H24. Pour proposer un tel service aux PME, la recette est de mutualiser le backend, avec le même XDR Sequoia pour tous nos clients. Mais si nous proposons l'EDR de SentinelOne en priorité à nos nouveaux clients, nous restons capables d'opérer tous les XDR du marché.»

Toujours en alerte, confrontés à des menaces qui se renouvellent sans cesse et à une avalanche de contraintes réglementaires, les RSSI vivent dans un état de tension permanente. Faut-il s'en inquiéter, ou au contraire voir dans ce stress un moteur de vigilance ? Leurs témoignages racontent en tout cas une profession sur le fil.

Le stress des RSSI, *une réalité avec laquelle composer*

La menace est omniprésente», rappelait encore l'Agence nationale de la sécurité des systèmes d'information (ANSSI) dans son panorama 2024. Et le 10e baromètre du CESIN paru en début d'année confirme que près d'une organisation sur deux a subi au moins une attaque réussie l'an dernier. Mais loin de provoquer la panique, cette constance a forgé une sorte de réflexe : les RSSI savent qu'ils ne peuvent jamais baisser la garde. Comme le souligne Alain Bouillé, délégué général du CESIN, «*la stabilité du nombre d'attaques traduit une maturité croissante des défenses*».

Un paradoxe subsiste pourtant : à force de vivre en état d'alerte, certains finissent par négliger certains signaux pourtant connus. L'Agence européenne de cybersécurité (ENISA) observe une recrudescence d'assauts sur la disponibilité – attaques DDoS, compromissions logiques – souvent préludes à des campagnes plus insidieuses. «*Ce n'est plus un sprint, c'est une course de fond*», résume un RSSI interrogé au détour d'un échange. Le stress entretient certes la vigilance, mais il l'érode aussi peu à peu.

Alors, faut-il voir dans cette tension un moteur ou un poison ? Les attaques évoluent plus vite que les budgets. Les ransomwares reculent grâce aux sauvegardes et aux EDR, mais les fraudes hybrides prospèrent : «arnaque au président» enrichie par des deepfakes, compromission via un fournisseur mal protégé, exploitation des failles cloud. À ce terrain technique s'ajoute un deuxième front : celui de la loi. NIS 2, DORA, RGPD… Autant de textes qui renforcent l'exigence documentaire. «*Ce que demandent les régulateurs, ce sont des capacités vérifiables*», insiste encore l'ANSSI. Logs, preuves, plans de continuité, notifications en 24 heures : l'exact contraire de l'improvisation.

Ne pas se tromper sur la mission du RSSI

Mais pour Franck Rouxel, vice-président de la Fédération Française de la Cybersécurité, expert SSI & ancien RSSI du ministère des Armées, l'essentiel est ailleurs. «*L'impuissance est un facteur de stress majeur. Beaucoup de RSSI restent subordonnés à une DSI dont les priorités sont d'abord business. Ils ont l'impression d'être inaudibles, de n'avoir aucune prise.* Et d'ajouter : *Un RSSI n'est responsable de rien, c'est la direction générale qui l'est. Son rôle, c'est d'alerter et de conseiller. Mais si on transforme son RSSI en fusible, il se condamne à l'épuisement.*»

Pour lui, les textes comme NIS 2 pourraient être vus comme une chance : «*Si votre approche, c'est la conformité, vous vous épuisez. Mais mon objectif n'est pas d'être conforme à NIS 2 ; en revanche, elle va m'aider dans mon travail, parce que je suis dans une vraie logique de gestion des risques.*» En bref, utilisée comme appui, la réglementation devient une arme pour légitimer la démarche du RSSI auprès du Comex. Utilisée comme checklist, elle se transforme en usine à gaz anxiogène.

Comment, dès lors, tenir mentalement ? En changeant de posture, répond Frank Rouxel. «*Vouloir*

Le stress des RSSI en chiffres

50 %
des organisations ont subi au moins une attaque réussie en 2023
SOURCE BAROMÈTRE CESIN 2024

76 %
des CISO estiment probable une attaque matérielle dans les douze mois
SOURCE PROOFPOINT, ÉTÉ 2024

87
sanctions prononcées par la CNIL en 2024, dont plusieurs pour défaut de sécurité

100 %
des RSSI jugent leur métier « stressant »
CYBERSECURITYTRIBE, 2024

- **88 %** évoquent un stress modéré à extrême
- **48 %** notent un impact direct sur leur santé mentale
- **40 %** sur leur entourage familial
- **31 %** sur leur efficacité professionnelle

qu'il n'y ait jamais d'attaque, c'est impossible. Le système est forcément troué. La mission du RSSI est de conseiller sur les risques, pas de garantir l'impossible.» Accepter cette asymétrie permet déjà de reprendre de la distance. Mais il faut aussi apprendre à déléguer : *«Sur une vraie compromission, avec une prod à plat, c'est du 24 heures sur 24. Si vous ne lâchez pas, vous explosez. Beaucoup de RSSI ne savent pas déléguer. Or, c'est vital.»*

Prévoir la crise et sa gestion

L'hygiène compte autant que la technique : savoir couper, respirer, se ménager des espaces de décompression, mobiliser des prestataires de gestion de crise si nécessaire. Frank Rouxel cite en exemple la SNCF : *«Leurs équipes sont staffées pré-crise, avec une maturité impressionnante. Recruter des profils rompus à la gestion de ces crises, ça rassure et ça réduit le stress.* Mais il prévient : *Lorsqu'elles se produisent, certains savent garder la tête froide, d'autres se figent comme un lapin dans les phares. Connaître ses limites et préparer un recours à des prestataires spécialisés : c'est aussi cela, l'hygiène de vie du RSSI.»*

La dimension émotionnelle est aussi trop souvent sous-estimée. Un incident, c'est traumatisant. On le porte longtemps en soi. Cinq ans après la cyberattaque qui a plongé Marseille dans le chaos numérique, tout a été certes reconstruit et les procédures sont désormais rodées, mais les cicatrices demeurent : *«Une telle épreuve ne s'efface jamais totalement, ni des systèmes, ni des mémoires»*, a témoigné il y a de cela quelques mois Jérôme Poggi, responsable de la sécurité des systèmes d'information de la Ville de Marseille, devant les équipes de Jérôme Notin et de cybermalveillance.gouv.fr.

Gemma Garcia Godall, coach en leadership et zone partner chez The Zone Global, le rappelle : *«Mettre des mots sur la peur apaise l'amygdale»*, cette zone cérébrale qui déclenche la réaction de fuite ou de combat. Dans une culture où exprimer ses émotions est encore perçu comme une faiblesse, surtout pour les hommes, ce non-dit aggrave l'anxiété chronique. D'où l'importance de parler, de partager, de transformer la peur en levier collectif. *«Tout comme un ordinateur a besoin d'électricité pour fonctionner, nous avons besoin des émotions pour nous donner de l'énergie. Elles nous poussent à agir, elles mobilisent les équipes et elles peuvent déplacer le monde»*, ajoute-t-elle.

Le pire travail de la Terre ?

D'autres témoignages viennent compléter ce tableau. *«Être CISO me détruisait à petit feu : les longues heures, la peur permanente d'avoir raté un détail. Passer au rôle de vCISO* [virtual CISO, externalisé donc, NDLR] *m'a rendu ma vie»*, confie Olivia Rose, fondatrice du Rose CISO Group et ancienne chief information security officer, dans le documentaire *CISO : The Worst Job I Ever Wanted* diffusé par CyberScoop en 2025. D'après l'enquête CybersecurityTribe, 100% des CISO jugent leur métier stressant ; 48% déclarent un impact direct sur leur santé mentale, 40% sur leur entourage familial, 31% sur leur efficacité professionnelle. La bascule se fait quand le stress cesse d'être aigu – moteur – pour devenir chronique et destructeur.

Le stress n'est pas un ennemi, conclut Franck Rouxel. C'est un signal d'alerte, un sismographe. Aigu, il garde en éveil. Chronique, il use. *«Le RSSI n'a pas vocation à porter seul la sécurité de l'entreprise. Son rôle est de mettre en garde et d'équiper le Comex pour décider. C'est là que le stress devient utile – quand il se transforme en énergie collective plutôt qu'en angoisse individuelle.»*

THIERRY DEROUET

À côté de la dette technique, préoccupation de toujours dans les DSI, la dette de sécurité informatique s'impose également dans les esprits depuis quelques années. Un déficit à mesurer d'abord, avant de l'attaquer pour réduire les risques.

Dette de sécurité logicielle : *un risque croissant à l'ère de l'IA*

Cela fait plus de dix ans que certains éditeurs alertent sur la présence et l'augmentation d'une dette de sécurité logicielle dans les entreprises. Non sans arrière-pensées, puisqu'ils proposent des outils pour y remédier, de façon automatisée par exemple au niveau des tests. Et non sans offrir le flanc à la critique concernant leur chiffrage du phénomène : ainsi le Software Security Report de Veracode prend comme repère les failles connues, sévères ou mineures, et non corrigées au bout d'un an, délai qui interroge forcément. C'est en tout cas à cette aune que l'éditeur a mesuré dans sa dernière étude parue début 2025 que 50 % des entreprises présentent des défauts persistants de grande gravité, qualifiés de dette critique.

Veracode attribue notamment cette progression à l'inflation des codes générés par l'IA, qui vient contrebalancer, dans le mauvais sens, les progrès réalisés par ailleurs en mettant en place des méthodes de production plus sécurisées comme DevSecOps par exemple. Or, «*le code généré par l'IA contient un taux de failles similaire à celui produit par les humains*», explique Chris Eng, chief research officer chez Veracode. Autrement dit, l'IA accélère autant le développement que l'apparition de nouvelles vulnérabilités, car la quête de rapidité favorise l'accumulation de failles non corrigées, augmentant ainsi la dette. Autre risque bien identifié, le recours à des logiciels open source ou de tierce partie en général. Preuve nous en a encore été fournie cet été avec le vol de données intervenu chez France Travail, à cause d'un logiciel tiers chez un sous-traitant.

L'IA et l'open source au banc des accusés… du moment

Comme souvent avec ce genre d'études, c'est l'évolution des indicateurs qui est la plus instructive (voir encadré). Mais si elles ont le mérite d'éveiller les consciences, c'est peu dire qu'elles ne font pas le tour de la question de cette dette. Pour une vision plus globale, mieux vaut se référer aux experts comme le chercheur en sécurité Krishna Chintalapudi, qui propose sur LinkedIn un panorama plus large du sujet : «*À l'instar de la dette technique, la dette de cybersécurité s'accroît lorsque les solutions à court terme, les mises à niveau différées et les traitements des risques tardifs s'accumulent au profit de la rapidité, de la commodité ou des contraintes budgétaires. Alors que les entreprises se précipitent pour innover, la sécurité reste souvent à la traîne, créant des failles qui deviennent de plus en plus coûteuses et dangereuses au fil du temps.*» Et de dresser la liste des problématiques, à commencer par «*les systèmes hérités qui ne sont plus corrigés mais restent critiques, les constatations non traitées issues des évaluations des risques et des audits, la mise en œuvre retardée des contrôles d'identité et d'accès, des programmes de formation ou de sensibilisation à la sécurité sous-financés ou encore les plans de réponse aux incidents incomplets.*»

Le business first creuse la dette

Jean-Christophe Vitu, directeur avant-vente et services professionnels France pour le spécialiste de la gestion des identités CyberArk, rejoint l'expert indien sur l'analyse des causes du creusement de la dette : «*La priorité au business conduit à des mises en place trop rapides de solutions applicatives, sans les contrôles adaptés qui permettraient la visibilité, le monitoring.*» Et le phénomène concerne même les entreprises a priori les plus averties sur le sujet : Microsoft mobilise par exemple en ce moment pas moins de 34000 ingénieurs sur sa Secure Future Initiative, censée réduire le nombre

Vericode cartographie… la dette de sécurité

% DES ENTREPRISES AVEC DES DETTES DE SÉCURITÉ À « HAUT RISQUE »

Il y a 1 an **46 %** → en 2025 **50 %**

DÉLAI MOYEN DE RÉPARATION DES FAILLES (EN JOURS)

Il y a 5 ans **171** → en 2025 **252**

% DES APPLICATIONS AVEC DES FAILLES SÉVÈRES

Il y a 10 ans **34 %** → en 2025 **20 %**

Comparaison entreprises plus performantes / moins performantes

EXISTENCE DE FAILLES SÉVÈRES

Entreprises plus performantes	Entreprises moins performantes
43 %	86 %

VITESSE DE CORRECTION DE LA MOITIÉ DES FAILLES

Entreprises plus performantes	Entreprises moins performantes
5 semaines	Plus d'un an

DETTE CRITIQUE LIÉE AUX LOGICIELS LIBRES

Entreprises plus performantes	Entreprises moins performantes
< 15 %	100 %

ÉTUDE PARUE DÉBUT 2025, BASÉE SUR LES DONNÉES RECUEILLIES PAR L'ÉDITEUR LORS DE RÉCENTS TESTS SAST, DAST ET SCA SUR 1,3 MILLION D'APPLICATIONS.

et la criticité des failles dans ses applicatifs. Avec un succès jugé mitigé pour l'instant.

« La question de la dette est plus claire dans la tête du DSI que dans celle du RSSI, constate Franck Rouxel, vice-président de la Fédération Française de la Cybersécurité, expert SSI & ancien RSSI du ministère des Armées. *Le premier a l'habitude de composer avec le legacy, quand le second y voit surtout un îlot de stabilité… jusqu'à ce qu'on l'ouvre pour en exploiter les data dans le cadre d'un passage au cloud. »*

Mais si tous deux s'accordent sur le besoin de traiter ce passif avec méthode, ils ne situent pas forcément la responsabilité au même endroit. Jean-Christophe Vitu est plutôt positif : *« Les RSSI ont des méthodes pour cartographier l'existant comme Ebios, la norme ISO 27001 pour l'amélioration continue et des réglementations comme DORA, NIS 2, etc., qui vont leur fournir des guidelines et l'occasion en même temps que l'obligation de procéder à des audits. »* Son confrère Franck Rouxel est moins optimiste : *« L'existence de cette cartographie tient encore du Graal. Pourtant, elle devrait déjà être en place, sous l'égide de la DSI, ne serait-ce que pour traiter correctement des PCA. »*

De la méthode comme vœu pieux

Il est sans doute encore loin le temps où les organisations considèreront *« la dette de sécurité informatique comme un risque stratégique »*, même si Krishna Chintalapudi a du mal à imaginer qu'on ne prenne pas le problème par ce – bon – bout. En attendant ce jour béni, il en est réduit à rappeler des mesures de bon sens, à commencer par la réalisation d'un audit de la dette (contrôles en retard, projets reportés, lacunes connues) qui débouche sur une priorisation des mesures correctives en fonction des risques.

Bien sûr, il faudrait également *« intégrer la sécurité à un niveau adéquat, à toutes les initiatives de transformation numérique dès le premier jour, pour ne pas avoir à la réadapter ultérieurement »*, donner aux RSSI l'autorité et la visibilité nécessaires pour plaider en faveur d'une action rapide. Et tant que nous y sommes, *« faire de la sécurité une responsabilité partagée entre toutes les fonctions de l'entreprise, pas seulement une préoccupation technologique ».*

Des vœux pieux sans doute car, comme le reconnaît Jean-Christophe Vitu, *« on compose avec la dette, plus qu'on ne la traite exhaustivement. Et d'autres risques émergent en permanence, par exemple autour de la multiplication des identités non humaines qui interviennent dans le SI. »* Le refrain est bien connu des DSI : chaque jour, on creuse cette dette. Et ce n'est pas près de s'arrêter. Ne serait-ce, comme le souligne Franck Rouxel, qu'en continuant les opérations de fusions et d'acquisitions de sociétés, sans jamais ou presque se préoccuper des composants plus ou moins « propres » qu'il va falloir alors intégrer dans le SI de l'entreprise. Preuve s'il en fallait une autre que l'acculturation des dirigeants aux questions de cyber est encore un long combat.

FRANÇOIS JEANNE

Alors que les formations traditionnelles ont montré leurs limites, des plateformes spécialisées jouent sur les mécanismes du jeu vidéo et de la mise en situation afin de favoriser la rétention des messages et l'engagement des salariés.

Réinventer la sensibilisation *des collaborateurs à la cyber*

Le chiffre est connu mais il est bon de le rappeler. Selon les études, de 80 à 95% des failles de sécurité trouvent leur origine dans une erreur humaine et non pas via des vulnérabilités techniques. Clic sur un lien suspect, recours à des mots de passe faibles, divulgation de données personnelles sur les réseaux sociaux… l'utilisateur est souvent présenté comme le maillon faible des politiques de cybersécurité.

La sensibilisation des salariés aux risques cyber est d'autant plus incontournable que l'IA générative professionnalise les techniques d'ingénierie sociale (voir également l'interview de Thierry Happe en début de dossier). Fini les messages d'hameçonnage à l'orthographe et à la mise en forme approximatives, les cybercriminels recourent à ChatGPT et consorts pour concevoir des campagnes de phishing ultra-personnalisées, sans parler des deepfakes vocaux et vidéos.

Xavier Paquin,
CEO de Kamae
« La gamification donne à l'utilisateur l'envie de progresser et de se challenger avec ses collègues. »

L'augmentation et la sophistication des attaques conduisent à revoir les programmes de sensibilisation. Les formations traditionnelles – dispensées en salle ou en ligne – ont montré leurs limites. Anxiogènes, elles peuvent même se révéler contreproductives. Coûteuses, elles manquent, par ailleurs, de récurrence alors qu'une stratégie de vaccination aux risques cyber doit s'inscrire sur la durée, en multipliant les piqûres de rappel.

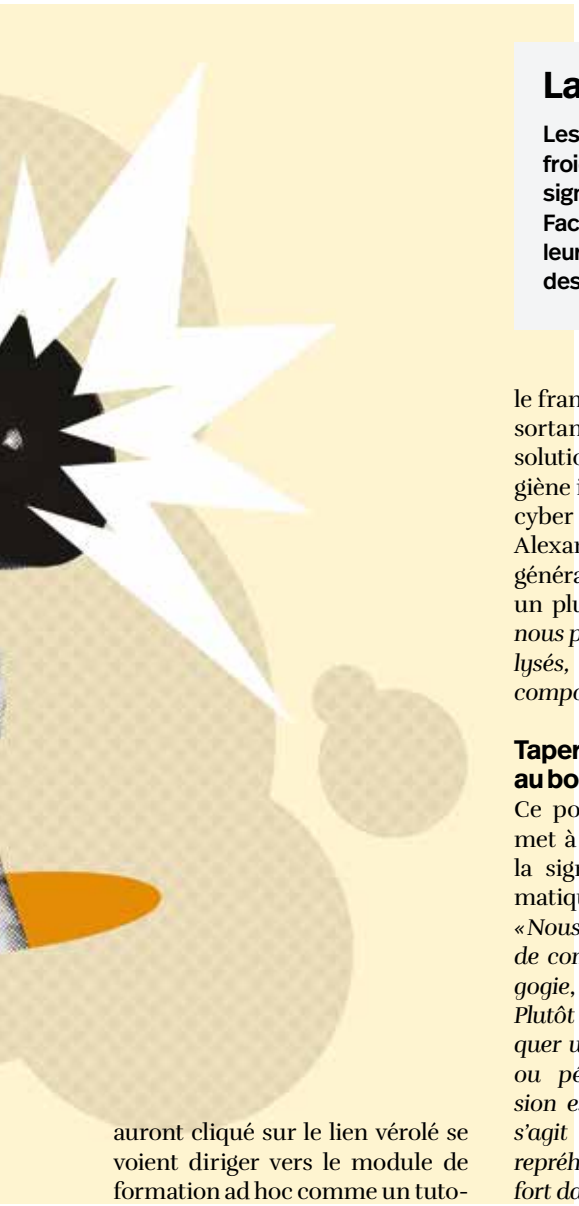
« Former ses équipes ne signifie pas simplement leur rappeler les règles élémentaires de sécurité, juge Olivier Arous, CEO d'OGO Security, dans une tribune libre. *Cela implique de créer une culture de vigilance numérique, d'organiser des simulations réalistes, d'adapter le discours à chaque métier, et de maintenir l'attention dans la durée. »*

Se challenger entre collègues

Depuis près d'une quinzaine d'années, l'offre de formation a, de fait, évolué, bousculant les codes en vigueur. Les éditeurs spécialisés proposent désormais des bibliothèques de contenus prêts à l'emploi, de quiz interactifs et de chatbots. Elles font la part belle aux modules de micro-learning. De courte durée, ces « capsules » facilitent la rétention du message tout en s'insérant aisément dans les agendas professionnels.

Le recours à des mécanismes de ludification – système de points et de récompenses, défis et classements entre services… – améliore par ailleurs l'engagement des collaborateurs. *« Cette gamification donne à l'utilisateur l'envie de progresser en débloquant des niveaux, mais aussi de se challenger avec ses collègues*, avance Xavier Paquin, CEO de Kamae. *Les capitaines d'équipes peuvent également servir au RSSI de relais terrain dans les directions métiers. »*

Ces programmes sont systématiquement associés à des campagnes de simulation qui consistent à envoyer à intervalles réguliers de faux courriels d'hameçonnage. Les employés qui



La cybersécurité, ce n'est pas mon affaire

Les résultats de la dernière étude de Cohesity risquent de donner des sueurs froides aux RSSI. Près d'un cinquième des salariés français (18,5%) ne signaleraient pas un incident cyber, estimant que *« ce n'est pas leur problème »*. Face à une cyberattaque, ils s'en remettent majoritairement à l'IT (60,5%), suivi de leur manager (51,2%) puis de l'équipe de cybersécurité (48,3%). Par ailleurs, 55% des employés français disent n'avoir jamais reçu de formation en cybersécurité.

auront cliqué sur le lien vérolé se voient diriger vers le module de formation ad hoc comme un tutoriel vidéo. Xavier Paquin fait le parallèle avec le judo. *« Au dojo, on répète les techniques, on apprend de nouvelles prises puis on passe au combat avec la simulation de phishing. »*

Ce système de mise en situation permet à une organisation d'évaluer son degré de maturité cyber, puis de voir les progrès réalisés au fil des campagnes en adaptant son programme et en le concentrant sur certaines populations cibles. La plateforme de Kamae propose pour cela un socle commun, puis des contenus avancés pour les employés à risques que sont les administrateurs réseaux, les commerciaux itinérants ou les dirigeants au statut VIP.

Connu pour être un spécialiste de la sécurisation des accès web, le français Olfeo s'est diversifié en sortant, en novembre 2023, une solution de sensibilisation à l'hygiène informatique et aux risques cyber (Olfeo Awareness). Pour Alexandre Souillé, son directeur général, cette double casquette est un plus. *« Notre activité de proxy nous permet, à partir des flux analysés, de mieux comprendre les comportements des utilisateurs. »*

Taper sur les doigts au bon moment

Ce positionnement original permet à Olfeo d'imposer au salarié la signature de la charte informatique avant de pouvoir surfer. *« Nous utilisons tous les moments de contact pour faire de la pédagogie*, poursuit Alexandre Souillé. *Plutôt que de se contenter de bloquer un site illégal de jeu en ligne ou pédopornographique, l'occasion est donnée de rappeler qu'il s'agit d'un acte juridiquement répréhensible. L'impact est plus fort dans le contexte. »*

Pionnier du secteur (création en 2007), Conscio Technologies travaille de son côté sur les vecteurs de persuasion et d'engagement avec le laboratoire de psychologie de l'université d'Aix-Marseille. Douze techniques ont été identifiées comme le bon usage de la peur, l'humeur positive ou l'identification sociale. *« Quand on parle du bon usage de la peur, il ne s'agit pas de choquer les utilisateurs, mais de leur apprendre à gérer le risque en leur expliquant qu'il existe des solutions »*, tempère Audrey Boussicaud, responsable pédagogique e-learning.

Depuis trois ans, Conscio Technologies a initié une approche sectorielle en proposant des parcours spécifiques à un domaine d'activité, comme celui de la santé. L'éditeur breton travaille, pour la suite, à une approche par métier ainsi qu'à une segmentation de ses contenus en trois niveaux d'expertise : débutant, intermédiaire, avancé.

80 à 95% des failles de sécurité trouvent leur origine dans une erreur humaine

En attendant, il a commercialisé en mars dernier un programme de sensibilisation à l'usage de l'IA dans un contexte professionnel. *« Il s'agit de traiter le sujet à 360° en rappelant les bonnes pratiques cyber, les risques liés à la conformité au RGPD ainsi que les enjeux éthiques ou les impacts environnementaux »*, complète Audrey Boussicaud.

Directrice commerciale chez Conscio Technologies, Morgane Sroka note qu'en dépit des contraintes économiques, *« le budget dédié à la sensibilisation des collaborateurs est préservé, même si les délais de prise de décision sont plus longs. »* Pour aider le RSSI à justifier cet investissement auprès du CoDir, l'éditeur remonte un nouvel indicateur, en plus des taux de participation ou de complétion : l'impact comportemental des campagnes. C'est-à-dire en quoi les actions de sensibilisation ont changé les comportements des salariés. *« Cette évaluation permet aussi à une organisation de se benchmarker avec d'autres structures comparables »*, conclut Morgane Sroka.

XAVIER BISEUL

Morgane Sroka,
directrice commerciale chez Conscio Technologies

« Le budget dédié à la sensibilisation des collaborateurs est préservé, même si les délais de prise de décision sont plus longs. »

GreenTech Forum

4 & 5 NOVEMBRE 2025

Palais des Congrès de Paris

LE RENDEZ-VOUS PROFESSIONNEL
NUMÉRIQUE RESPONSABLE

+ 70 conférences, keynotes, cartes blanches et ateliers
+ 100 exposants
+ 180 intervenant(e)s

#GreenTechForum

SOUS LE HAUT PATRONAGE DE Planet Tech'Care

UN ÉVÉNEMENT Formule Magique

Les 8 et 9 octobre
Lyon (69), Centre des Congrès
Convention USF

L'événement annuel du club des utilisateurs francophones de SAP célébrera ses « *35 ans d'intelligence collective et de passion* ». Ces noces de rubis, pierre associée à l'ardeur et au courage, donneront aux participants une nouvelle occasion de partager les expériences, les idées et les connaissances, de réfléchir aux problématiques technologiques et organisationnelles, d'étudier les solutions SAP et d'influencer l'écosystème, largement présent sur le congrès.

convention-usf.fr

Du 8 au 11 octobre
Monaco, Grimaldi Forum
Les Assises de la Cybersécurité

La prochaine édition sera placée sous le signe de la synergie CISO/métier avec comme fil rouge « FuturS, la cybersécurité au service des métiers et de la création de valeur. » Ses quatre déclinaisons ? Accompagner le business, innover chaque jour, rester pragmatique et faire émerger les talents. Autant de sujets d'échanges avec les acteurs de l'écosystème toujours plus nombreux sur les Assises.

lesassisesdelacybersecurite.com

Le 15 octobre en live
Collaboration et productivité dans un monde hybride : réinventer le travail

L'arrivée de solutions cloud native répond aux besoins d'agilité des entreprises, soucieuses de pouvoir adapter leurs environnements de travail à leur nombre de salariés, à leurs lieux de travail, sans compromettre leur sécurité. En les intégrant dans des architectures hybrides, elles peuvent en tirer parti sans altérer les performances des SI en place.

itforbusinesslesmatinales.fr

Les 4 et 5 novembre
Paris, Palais des Congrès
Green Tech Forum

Cinquième édition pour le rendez-vous professionnel dédié au numérique responsable. Alors que près de 2 500 participants s'y pressent chaque année, il y sera sans aucun doute question de la conjoncture actuelle nettement moins favorable aux politiques RSE et aux décisions de transformation à visée environnementale. Rappelons que le salon est placé sous le patronage de Planet Tech'Care, une initiative de Numeum.

greentech-forum.com

Les 5 et 6 novembre
Paris, Porte de Versailles (15e)
Tech Show Paris

Désormais bien installé dans le calendrier automnal, Tech Show Paris revient avec une formule qui a fait ses preuves et ses cinq événements : Cloud Expo Europe, DevOps Live, Cloud & Cyber Security Expo, Data & AI Leaders Summit, et Data Centre World. À noter la reconduction de la plateforme Connect @ Tech Show Paris, qui intègre des fonctionnalités de networking, de planification de rendez-vous et de gestion d'événements.

techshowparis.fr

Le 19 novembre en live
Quelle infrastructure cloud pour une organisation plus performante ?

Les DSI peuvent aujourd'hui s'appuyer sur différentes configurations de cloud – public, privé ou hybride – pour répondre à leurs exigences de flexibilité et de résilience, avec la dimension souveraine qui s'est imposée récemment en sus. Dans tous les cas, la question de la sécurité reste au cœur des priorités, notamment face à l'évolution des menaces et des contraintes réglementaires. Le choix de la bonne infrastructure n'en est que plus important.

itforbusinesslesmatinales.fr

Les 26 et 27 Novembre
Aussonne (31), MEETT – Parc des expositions
CBC Toulouse

La Cyber Security Business Convention continue de développer son riche programme : cette année, des zooms sont prévus sur l'Europe et la cyberdéfense, les nouvelles réglementations appliquées aux chaînes industrielles, mais aussi le hacking éthique ou encore la cryptographie et le quantique. Sont également programmées des mises en situation pédagogiques (cellules de crise cyber, serious game et Challenge Capture The Flag).

cbc-convention.com

Et aussi…

AI on us 2025
Biarritz, Hôtel du Palais & Casino, du 14 au 17 octobre
ai-on-us.com

Salon des maires et des collectivités locales
Paris, Porte de Versailles, du 18 au 20 novembre
salondesmaires.com

Apidays
Paris, Cnit Forest La Défense, du 9 au 11 décembre
apidays.global/events/paris

Les dérives éthiques des IA et l'excès de confiance dans leurs réponses, créent des risques bien réels pour nos sociétés, ce dont vous vous émouvez sur les réseaux. Heureusement, pendant qu'une partie de l'humanité s'enfonce dans ces ténèbres, une autre choisit d'exercer la sienne avec des initiatives solidaires. Comme quoi la technologie bien pensée peut aussi servir l'inclusion et le bien commun.

Lou Welgryn, coprésidente de Data for Good, *LinkedIn*

Meta AI a le droit «*d'engager un enfant dans des conversations romantiques ou sensuelles*» ou d'affirmer que les Noirs sont «*plus bêtes que les Blancs*». C'est ce que révèle une enquête de Reuters (…). Ils ont eu accès aux documents internes qui définissent le fonctionnement du chatbot. (…) Exemple de règle : Meta AI ne doit pas répondre des propos haineux. Cependant, une exception permet au bot «*de créer des déclarations qui dénigrent les personnes sur la base de leurs caractéristiques protégées*».

Meta AI peut aussi créer du contenu faux tant qu'il est explicitement reconnu que ce contenu est faux. Par exemple, il peut produire un article affirmant qu'un membre vivant de la famille royale britannique est atteint d'une IST comme la chlamydia – à condition d'ajouter une clause de non-responsabilité indiquant que l'information est fausse… (Depuis que le document a fuité, ils ont dit vouloir revenir sur certains éléments de leur politique…)

re: **James Martin,** Content & communication expert

Le plus choquant : ils ont attendu d'être démasqués pour faire leur mea culpa et ils ne sont revenus que sur «certaines» guidelines (ex. sur les enfants), mais pas toutes (ex. sur les personnes de couleur). Effarant…

Julien Briault, ingénieur réseaux senior chez Deezer, fondateur du Cloud du cœur, *LinkedIn*

Les Restos du Cœur reçoivent des ordinateurs donnés. Le seul «problème» : la plupart ne sont pas compatibles avec Windows 11, faute de support matériel (Cc la puce TPMv2). Plutôt que de les laisser dormir ou partir au recyclage, nous avons choisi une autre voie : créer une distribution Linux adaptée aux besoins des bénéficiaires et des bénévoles.

Les objectifs de Linux du Cœur sont simples : prolonger la vie des ordinateurs donnés en les rendant rapides et sécurisés, offrir un environnement simple, accessible et familier, sans barrière technique, promouvoir l'inclusion numérique en donnant à chacun les outils pour apprendre, travailler, communiquer.
(…) Si vous avez, dans vos entreprises, des ordinateurs portables inutilisés, des tablettes ou des Tiny PC qui prennent la poussière, n'hésitez pas à (nous) contacter.

Cyrille Chaudoit, cofondateur de Talenco, *LinkedIn*

Cet été, plus de 100 randonneurs ont trouvé la mort dans les Alpes italiennes. (…) Pas uniquement à cause du climat (fonte des glaces, etc.), de l'âge (tantôt ados, tantôt seniors++), du manque d'expérience ou de l'excès de confiance… Ou plutôt si : à cause de l'excès de confiance de + en + de randonneurs dans l'IA et notamment ChatGPT pour préparer leurs sorties !

Résultat : sentiers interdits recommandés comme «*belle balade*», via ferrata suggérée sans mentionner casque ni harnais, ou encore sortie en baskets proposée pour gravir un 3 000 m.
Le tout «*écrit avec assurance*» comme en a l'habitude l'IA, alors qu'évidemment elle ne sait rien et ne produit que des réponses «*plausibles*», pas les indications fiables d'un guide avisé.
Et le plausible en montagne, ça ne suffit pas.

re: **Julien De Sanctis,** philosophe, Consultant Santé mentale, *LinkedIn*

Certains diront que ce n'est pas l'IA en elle-même le problème, mais «*la façon dont on s'en sert*». Oui, sauf que non, pas que. Bien sûr que les usages comptent pour beaucoup. (…) Mais ce n'est pas là (et de loin) le fin mot de l'histoire, car les IA, comme toute autre techno, s'insèrent de leur conception à leur utilisation dans des cadres culturels et normatifs qui orientent ces usages. Autrement dit : le sujet utilisateur n'est jamais seul avec sa «volonté» face à un artefact. Par exemple, dans un contexte mondial de désinformation massive, la parole humaine, surtout dans sa dimension factuelle et scientifique, perd peu à peu sa valeur. Dès lors, n'est-il pas tentant de se fier aveuglément aux «résultats» d'une IA perçus, à tort, comme purement objectifs ? L'évidence du bon sens – mettre des chaussures de marche pour gravir 3 000m – est court-circuitée par une apparente objectivité prescriptrice face à laquelle nous devenons purement passifs.

Un événement **IT for Business** avec le concours du Cigref, French Women CIO et Atout DSI

Les DSIN de l'année 2025

27e Édition

Directions des Systèmes d'information et du Numérique de l'Année

Le rendez-vous incontournable des managers du numérique

27e édition

DEVENEZ PARTENAIRE

Réservez dès maintenant la date du
12 Mars 2026 pour la 27ème du DSIN !

Vous souhaitez devenir partenaire de cette soirée ?
Contactez nos équipes ou rendez-vous sur dsidelannee.fr

Frédéric Ktorza
fktorza@choyou.fr
06 12 81 30 70

Romain Duran
rduran@choyou.fr
06 03 25 37 27

Karim Baqlou
kbaqlou@choyou.fr
01 53 05 93 79

Antoine Gourévitch & Gildas Bouteiller
Directeurs associés, BCG

Le Cloud sous tension : coûts, souveraineté, gouvernance

Le Cloud demeure un enjeu aussi stratégique que complexe pour les entreprises. Les DSI doivent composer avec un environnement mouvant, marqué par l'incertitude. Elles doivent aujourd'hui faire face à trois types de pressions : une évolution incessante des politiques tarifaires, un impératif de rationalisation des coûts et, désormais, un défi réglementaire et géopolitique inédit.

En toile de fond d'abord, il y a cette bataille tarifaire mondiale qui ne faiblit pas. L'analyse pour les six premiers mois de 2025 du Nimbus Pricing Index, un indice permettant de comparer le prix des offres des trois principaux fournisseurs, révèle de nouveaux positionnements : stabilité des prix chez AWS, baisses ciblées d'Azure pour Microsoft en Asie-Pacifique, hausses modérées mais continues de Google.

Si les considérations de coûts ont toujours pesé lourd dans les choix des entreprises, un mouvement de fond rebat les cartes : la montée en puissance de la souveraineté numérique. D'ici 2028 en effet, 65% des pays auront adopté un plan dédié (*). La souveraineté numérique n'est donc plus une question politique abstraite. C'est un tournant de l'usage du Cloud pour toutes les entreprises. En quelques années, le sujet s'est imposé aux gouvernements de tous les pays et la tendance est encore accentuée par les tensions géopolitiques.

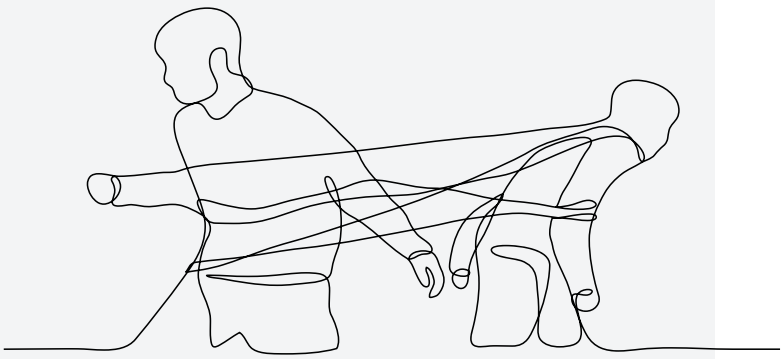
Les États du monde entier structurent leur régulation à un rythme soutenu, imposant une gouvernance locale des données. Mais dans de nombreux cas, le régulateur va plus loin. La souveraineté nationale ou régionale s'étend à la souveraineté opérationnelle et technologique. Seuls les citoyens de la juridiction peuvent alors accéder aux systèmes réglementés et les ordinateurs, réseaux, flux de données et sauvegardes doivent se trouver à l'intérieur d'une zone géographique. Les règles ne cessent de se durcir. Les sanctions risquent, elles aussi, de s'alourdir.

Concrètement, les entreprises doivent choisir. Investir dans des data centers locaux ou s'appuyer sur les offres de Cloud souverain proposées par les fournisseurs. Cette solution offre tous les avantages des services du Cloud tout en aidant l'entreprise à respecter les exigences de souveraineté numérique. Les fournisseurs se structurent pour répondre aux exigences réglementaires et opérationnelles croissantes des clients. Dans la plupart des cas, les modèles de Cloud souverain intègrent différents niveaux de réponses au cadre réglementaire. Il revient alors aux organisations d'arbitrer en fonction de leurs besoins, de leur activité et de leurs moyens. Car les tarifs des clouds souverains sont de 10 à 30% plus élevés que ceux du cloud public. Les analystes estiment que les dépenses dans ces infrastructures atteindront 169 Md$ en 2028 contre 37 Md$ en 2023.

Le concept de Cloud souverain est encore nouveau, son déploiement en cours. Mais les entreprises ne peuvent ignorer son émergence. Et les surcoûts, ajouté aux investissements déjà massifs réalisés, imposent un changement de méthode. Si la révolution Cloud a rempli ses promesses, il reste largement sous-optimisé. Son adoption à grande échelle génère aujourd'hui un gaspillage estimé à 30% des dépenses qui lui sont consacrées, du fait d'une mauvaise maîtrise des coûts et d'une utilisation qui demeure perfectible. Cette situation est devenue critique au regard des sommes mobilisées qui représentent aujourd'hui jusqu'à 17% des budgets informatiques. D'autant que 80% des entreprises s'attendent à voir grandir ce ratio dans les prochaines années.

Pour entrer dans la nouvelle ère de souveraineté numérique, les entreprises devront donc non seulement absorber des surcoûts, mais surtout revoir leur manière de gérer le Cloud : structurer les usages, renforcer la gouvernance, négocier différemment avec les fournisseurs. En assainissant leurs pratiques et en anticipant les nouvelles règles, elles transformeront cette contrainte en avantage stratégique. Dans un marché où l'incertitude devient la norme, la robustesse d'une stratégie Cloud ne se mesurera plus seulement en termes de performance technique, mais aussi de résilience réglementaire. ■

(*) Cloud Cover: Price Swings, Sovereignty Demands, and Wasted Resources (BCG, juillet 2025).



La souveraineté numérique n'est plus une question politique abstraite. C'est un tournant de l'usage du Cloud

Thomas Chejfec
Directeur des systèmes d'information
@ThomasChejfec

L'innovation, victime de l'urgence

Dans l'entreprise, le temps court est roi. Les métiers vivent au rythme du chiffre d'affaires quotidien, de la satisfaction client immédiate, des opérations qui ne peuvent souffrir d'aucune rupture. La logistique, la finance, la production : chacun a le nez collé sur l'urgence. Et quand la pression monte, l'IT est sommée de répondre vite, parfois dans l'instant.

C'est légitime. Sans temps court, pas de résultat. Sans résultat, pas d'entreprise. Mais ce temps court a un défaut : il ne laisse aucune place… au temps long. Or c'est ici que se pensent l'innovation, la transformation, et que se prépare l'avenir.

L'innovation est souvent la première victime de l'urgence. Quand les agendas sont saturés par l'opérationnel, elle devient suspecte. On la regarde comme un luxe, un terrain de jeu pour consultants, ou pire : comme une perte de temps. *«Il y a des clients à livrer, pas des POC à tester.»* Ce réflexe a tué bien des idées qui auraient, quelques mois plus tard, sauvé du temps ou de l'argent. La vérité, c'est que l'absence d'innovation fabrique de la dette… mais bon, tant qu'on fait tourner l'Excel du jour, tout va bien, n'est-ce pas ?

Pourtant et contrairement aux idées reçues, l'innovation n'est pas ce luxe qui nous détourne de nos priorités. Elle est l'alliée du temps court. Chaque automatisation réduit la pression du quotidien. Chaque refonte applicative supprime des irritants et rend le travail plus fluide. Chaque usage de la data ou de l'IA accélère la prise de décision et fiabilise le pilotage. Autrement dit, l'innovation ne ralentit pas l'entreprise : elle accélère son quotidien. Encore faut-il accepter de lever les yeux pour voir qu'elle est là – exercice parfois aussi difficile qu'un clic droit pour certains.

L'innovation n'est pas un gadget pour séminaire. Elle est un multiplicateur d'efficacité. Elle permet aux métiers de respirer quand la pression devient étouffante, d'anticiper plutôt que de subir, d'agir avant que la crise n'éclate. Mais pour que ce rôle soit reconnu, encore faut-il la rendre légitime. Trois leviers sont essentiels.

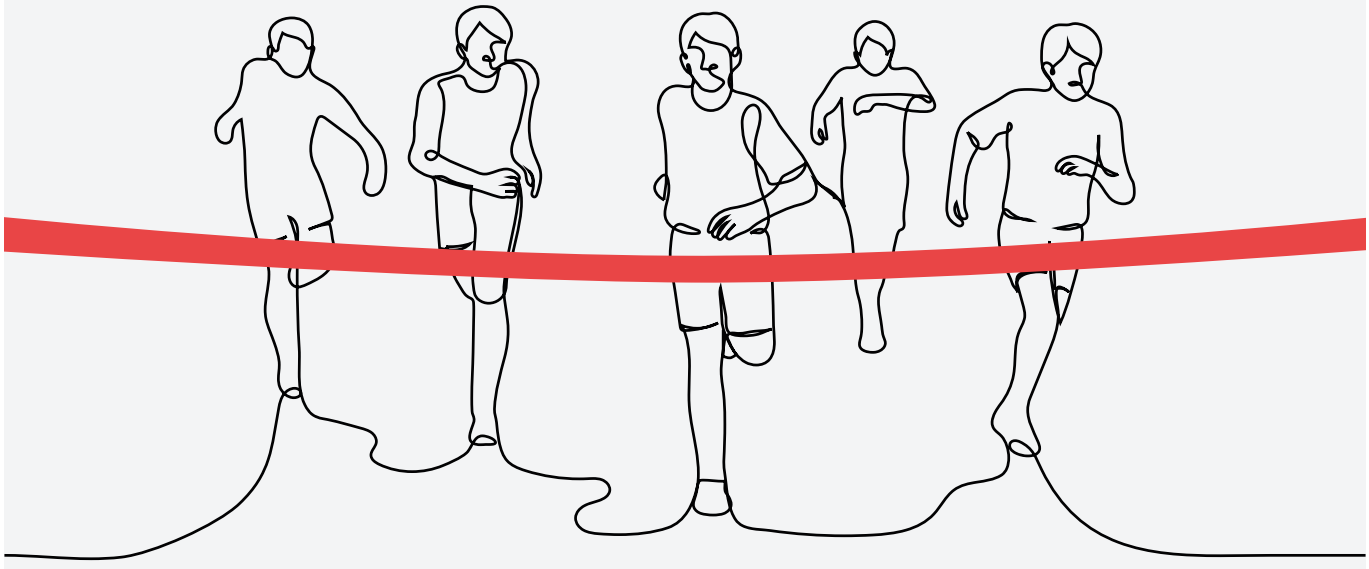
D'abord mesurer : pas de slogans, des faits. Même un petit gain – une heure économisée, un taux d'erreur réduit de 5%, une décision prise deux fois plus vite – suffit à prouver la valeur.

Ensuite acculturer : le temps long n'est pas une lubie de DSI, mais une assurance pour les métiers. Leur montrer que l'effort d'aujourd'hui allège la fatigue de demain, installe une vision partagée.

Enfin sanctuariser : l'innovation doit avoir ses espaces protégés, en temps, en budget et en gouvernance. Sinon, elle sera toujours sacrifiée aux urgences.

Ce triptyque – mesurer, acculturer, sanctuariser – garantit le contrat qui transforme l'innovation en investissement accepté, et non en luxe contesté.

Au fond, l'équilibre est là : il ne s'agit pas d'opposer temps court et temps long. Le premier permet de vivre aujourd'hui, le second garantit qu'on vivra demain. L'entreprise qui réussit est celle qui sait conjuguer les deux : traiter les urgences tout en construisant l'avenir. Une heure d'innovation aujourd'hui, ce sont dix heures de crises évitées demain. La vraie articulation des temps ? Une stratégie lucide qui relie l'immédiat au durable. ■



Frédéric Simottel
BFM Business
@simottel

« Fantastic Larry »

81 ans et toujours sur le podium des personnalités les plus riches de la planète. Grâce aux juteux contrats passés avec OpenAI, à sa proximité avec l'administration Trump (dont il est supporter depuis le début), le voici au cœur de la bataille sur l'intelligence artificielle. Il devrait aussi faire partie du conglomérat repreneur de TikTok US. Larry Ellison, fondateur d'Oracle, a toujours su bien choisir son camp. À 22 ans, il finance ses premiers logiciels spécialisés sur les bases de données grâce à des contrats passés avec l'Armée américaine. Il les adapte ensuite aux entreprises et cofonde alors Oracle en 1977. Il devient en quelques années l'un des hommes les plus puissants de l'informatique mondiale, défiant IBM et Bill Gates, son ennemi juré. Ce monument de l'informatique, proche de Steve Jobs même dans la tempête, a aussi racheté une icône de la Silicon Valley, Sun Microsystems. Passionné de voile, il a remporté l'America's Cup à deux reprises, sans regarder à la dépense (*« Budget ? What budget ?... No budget for sailing »*, me dira-t-il lors d'un interview dans les années 90). Il figure même au générique d'*Iron Man*, son personnage inoxydable ayant inspiré en partie le héros du film. Mais il a aussi su déléguer, à ses fidèles lieutenants qui ont repris les rênes de l'entreprise en 2004. Car si Ellison aime être à la barre, il a toujours su aussi s'entourer d'officiers capables de maintenir le cap.

La Hollande, l'autre pays de l'IA

Pour le coup, personne n'avait vu venir la prise de participation du néerlandais ASML auprès de Mistral AI : 1,3 Md€, sur les 1,7 levés. Ancienne spin-off de Philips, le leader mondial des machines de lithogravures est le seul industriel au monde à savoir graver les processeurs les plus fins. Désormais valorisé plus de 11 Md€ (une décacorne !), Mistral AI va apporter son expertise IA à ces machines, pour les rendre encore plus précises et performantes. Joli coup également pour un trio français inattendu : Arthur Mensch, brillant cofondateur de Mistral AI, Christophe Fouquet DG d'ASML et… Bruno Lemaire, conseiller stratégique de la firme hollandaise.

Retrouvez Frédéric Simottel dans l'émission
Tech & Co Business, le magazine de l'accélération numérique
Le samedi à 15h30 et le dimanche à 17h

Tiers de défiance

La vulnérabilité d'un tiers (sous-traitant, partenaire, éditeur de logiciel) figure parmi les risques majeurs identifiés par la plupart des CISO. Confirmation de leurs craintes ces derniers jours avec plusieurs aéroports européens bloqués, obligés d'annuler des vols. La faute à une cyberattaque sur Muse, un logiciel d'enregistrement des passagers fourni par Collins Aerospace. *« Malgré nos multiples couches de sécurité, nos process sans cesse mis à l'épreuve, nous ne sommes pas à l'abri de la défaillance d'un maillon de la chaîne de valeur »*, me confiait récemment le CISO d'un grand industriel français. Et de conclure : *« En pareil cas, la communication en temps réel est cruciale, ce sont les points sur lesquels il faut travailler. »*

Il faut sauver le soldat Intel

L'administration Trump n'y va pas par quatre chemins pour mener les débats dans l'univers des semi-conducteurs. Après avoir transformé ses aides auprès d'Intel en capital investi – l'État américain en est désormais le principal actionnaire –, le voici qui tord le bras de Nvidia pour que le leader mondial des puces IA investisse 5 Md$ chez Intel. On aura beau chercher toutes les justifications technologiques du monde à cet accord – entraide, co-partenariat et autres partages de valeur –, le but du gouvernement américain est bien de remettre Intel en selle pour maîtriser la chaîne logistique et surtout la fabrication des précieux semi-conducteurs. Si notre puissance publique pouvait s'en inspirer au lieu de se perdre dans ses méandres politiques…

LaMatinale

Un événement IT for Business

Les DSI qui ont pris la parole dans notre émission

Richard Bury
Directeur des Systèmes d'Information et de Management, EDF

Marie-Odile Lhomme
DSI, Audencia Business School

Bernard Giry
DSI, Directeur général adjoint région Île-de-France

Vous souhaitez partager votre expérience et votre expertise ? Contactez notre responsable éditorial événements et programmes, **Thomas Pagbe** *(tpagbe@itforbusiness.fr)*

INFOS ET INSCRIPTIONS

itforbusinesslesmatinales.fr

Vous êtes fournisseur IT et souhaitez-vous adresser directement aux DSI ?
Devenez partenaire !

Toutes les informations

Prochaines matinales 2026

11 février
CYBERSÉCURITÉ & RÉSILIENCE
Comment l'IA transforme votre cybersécurité ?

18 mars
CLOUD & INFRASTRUCTURES
Cloud souverain : quel niveau de confiance choisir ?

15 avril
DATA, IA & GOUVERNANCE
Quelle gouvernance de la donnée à l'ère de l'IA ?

27 mai
TRANSFORMATION & RÉGULATION
IA, cloud : comment garantir la bonne gestion de son budget IT ?

11 juin
CYBERSÉCURITÉ & RÉSILIENCE
NIS2, DORA : Comment préparer vos équipes à la résilience ?

1er juillet
DATA, IA & GOUVERNANCE
IA, ML : comment vos métiers s'en emparent ?

16 septembre
TRANSFORMATION & RÉGULATION
DSI, CMO :Comment répondre aux défis de la personnalisation de la relation client ?

14 octobre
CYBERSÉCURITÉ & RÉSILIENCE
DSI : Comment vous aider à devenir le copilote de votre stratégie business ?

18 novembre
STRATÉGIE & FUTUR DE LA DSI
Digital Workplace : vers un espace de travail hybride et sécurisé

9 décembre
TRANSFORMATION & RÉGULATION
Open Source : la (future) clef de voûte de votre stratégie IT ?

Envie d'en savoir plus ? Contactez notre équipe :

Romain Duran
rduran@choyou.fr
06 03 25 37 27

Karim Baqlou
kbaqlou@choyou.fr
01 53 05 93 79

KONICA MINOLTA

EXPERT CYBER
LABEL SÉCURITÉ NUMÉRIQUE
Cybermalveillance.gouv.fr
RÉPUBLIQUE FRANÇAISE

UN EXPERT IT À VOS CÔTÉS, AU QUOTIDIEN

POUR UNE GESTION SIMPLIFIÉE ET SECURISÉE.

Guichet unique : audit, accompagnement, assistance et maintenance

Gestion préventive & curative 24/7

Gestion de la sécurité 24/7

CONFIEZ VOTRE INFORMATIQUE À UN EXPERT CYBER CERTIFIÉ.

Giving Shape to Ideas*

Konica Minolta Business Solutions France
365-367 route de Saint-Germain 78424 Carrières-sur-Seine Cedex
S.A.S au capital de 46.290.375 € - RCS Versailles B302 695 614

*Donnez vie à vos idées

SCANNEZ POUR DEMANDER UN AUDIT

serein IT