



édito



Kamel Amroune
CEO

Chères lectrices, chers lecteurs,

Le 23 juillet 2025, le Luxembourg a découvert, à ses dépens, la brutalité d'une cyberattaque sophistiquée. En exploitant une vulnérabilité logicielle, des assaillants - non identifiés à ce jour - ont paralysé des services essentiels, rappelant une vérité implacable : aucune organisation, publique ou privée, grande ou petite, n'est à l'abri des conséquences d'une opération malveillante.

Cette réalité se confirme dans les chiffres : selon Check Point Software Technologies, le Grand-Duché a enregistré, lors du deuxième trimestre 2025, une hausse des cyberattaques de l'ordre de 59 % en comparaison avec la période correspondante en 2024. En moyenne, c'est à 1.862 attaques que les institutions et sociétés luxembourgeoises sont confrontées chaque semaine. Ces menaces, souvent invisibles mais omniprésentes, frappent sans distinction et fragilisent la confiance qui sous-tend nos sociétés numériques.

Au-delà des dégâts visibles - fuites de données, arrêts de production, rançons -, c'est la confiance dans l'intégrité de l'information et la préservation de nos vies privées qui vacille.

Quand les données sont altérées ou que les systèmes s'arrêtent, c'est la continuité des soins, la sécurité des transactions, la crédibilité des institutions qui sont en jeu.

Face à cette situation, la réponse ne peut se limiter à la technologie. Elle doit être stratégique, collective, et culturelle. Elle passe par la mise en place d'une gouvernance forte, par une vigilance partagée au sein de chaque organisation et par l'adoption de stratégies de protection multidimensionnelles.

C'est à cette réflexion que se consacre ce 11^e numéro de The Dots Magazine : comprendre comment les nouvelles vagues de menaces redessinent le risque, pourquoi la cybersécurité est plus que jamais l'affaire de tous et comment les entreprises peuvent bâtir une résilience accrue en s'appuyant sur la proactivité, la responsabilité et la confiance.

Parce que dans un monde hyperconnecté, protéger les données, c'est protéger l'avenir.

Bonne lecture.

Sommaire

#11

the
Dots.
MAGAZINE



[6] Le Grand Portrait

Pascal Bughin

La Mondiale Europartner

[10]

Faire de la cybersécurité
l'affaire de tous

[14]

Econocom

Sécurité dans le cloud privé :
Une approche ascendante
pour mieux protéger les
données

[16]

Business Elements Reply

The Frontier Firm: Redefining
Work in The Age of AI

[18]

NSI Luxembourg

Repenser le recrutement IT
L'approche 360° de NSI
Luxembourg

[20]

Oracle

Intelligence Artificielle :
Pourquoi 100 micro-projets
valent mieux qu'un unique
projet "moonshot"

[22]

When Truth Gets Corrupted:
Protecting Data Integrity in the
Age of Misinformation and
Breaches

[24]

Trustteam Luxembourg

Avec la solution Yogosha,
Trustteam Luxembourg
enrichit son portefeuille
cybersécurité

[26]

Ransomware on the Rise:
How Digital Extortion is
Crippling Economies



[28]

L'entretien

Daniel Mathieu

CFL

[32]

NEOFACTO x Aricoma

Une année de synergies
au service de la sécurité
numérique

[34]

Proximus NXT Luxembourg

La cybersécurité n'est pas
qu'une affaire de technologie

[36]

cegecom

Entre cyberscore, partenariats
et accompagnement, la
nouvelle stratégie de cegecom
pour sécuriser les entreprises

[38]

Vos données, vos droits
Protéger la vie privée dans un
monde sans oubli

[42]

delaware

From RPA to Real Autonomy:
Choosing the Right Automation
and Proving Its Value

[44]

Why No One is Safe from the
New Wave of Cyber Threats

[46]

AG2R La Mondiale

Cybersécurité et IA :
AG2R LA MONDIALE
adapte sa gouvernance
et ses pratiques

[48]

AI, Blockchain, and Beyond:
The Tech That's Reinventing
Cybersecurity

[50]

ESET

Appareils personnels et
risques d'entreprise :
L'avenir de la sécurité BYOD
selon ESET

[52]

Orange

Orange Flexy, un forfait mobile
pensé pour la résilience
numérique des entreprises

[54]

Programmation 2025

[56]

**Nexus Luxembourg
& Garden Party**

AWARENESS

is your best defense



With **Cyberone**, we protect your business and train your people to be the first line of defense :


Custom security rules

Advanced monitoring

Phishing campaigns

User training



A portrait of Pascal Bughin, a middle-aged man with dark hair, glasses, and a goatee, smiling. He is wearing a dark blazer over a light-colored button-down shirt. The background is a soft, out-of-focus indoor setting. The entire image is overlaid with a semi-transparent purple filter.

« Si l'on devait le définir,
Pascal Bughin se décrirait
comme un profil 'T-Shaped' »



AG2R LA MONDIALE

Le Grand Portrait

« - J'ai le sentiment que toute ma vie dépend de cet instant précis. Si je le rate...
- Moi je pense le contraire. Si on rate ce moment, on essaie celui d'après, et si on échoue, on recommence l'instant suivant. On a toute la vie pour réussir. »

Boris Vian



Pascal Bughin

Directeur Transformation, IT et Digital
La Mondiale Europartner

— Propos recueillis par Nostassia Houx

« Son objectif ?
Transformer les défis
technologiques en opportunités
humaines, en alliant innovation
et pragmatisme. »

Si l'on devait le définir, Pascal Bughin se décrirait comme un profil « *T-Shaped* » : transversal, multi-compétences et motivé par la diversité des défis, des savoirs et du genre humain, toujours dans le but de progresser. Dès ses études en sciences économiques, il a cherché à explorer un large spectre : mathématiques, économie, droit, langues, IT, psychosociologie,... « *Cette curiosité insatiable a tracé le fil rouge de ma carrière* », explique-t-il, ce qui l'a conduit de l'audit à l'IT, puis vers l'assurance, un secteur où il a pu exprimer sa capacité à naviguer entre les métiers et à créer des ponts entre les expertises, notamment opérationnelles et technologiques.

Avec plus de 25 ans d'expérience dans l'assurance, Pascal Bughin a endossé des rôles variés (COO, CEO, CRO, CIO), toujours animé par la même conviction : la qualité de service, qu'elle soit destinée aux clients, partenaires ou équipes internes, naît de la collaboration et de la complémentarité des talents.

« *Seul on va plus vite, ensemble on va plus loin* » : une philosophie popularisée par Nelson Mandela, qui résume parfaitement sa vision du leadership.

Aujourd'hui, en tant que Directeur Transformation, IT et Digital, il met cette approche au service de la modernisation des organisations. Son objectif ? Transformer les défis technologiques en opportunités humaines, en alliant innovation et pragmatisme. « *Au-delà des outils et processus, ce qui compte, ce sont les histoires que nous construisons ensemble : celles qui rendent le numérique plus humain et l'avenir plus accessible et prometteur* », affirme-t-il.



Interview

4 questions à Pascal Bughin

Directeur Transformation, IT et Digital chez La Mondiale Europartner

« La tech a un pouvoir fascinant : elle peut paraître presque ‘magique’, en apportant des solutions à des problèmes du quotidien encore non résolus. »
Pascal Bughin

Q1. Si vous deviez expliquer votre métier à un enfant, que diriez-vous ?

J'utiliserais la métaphore du restaurateur qui a un objectif avec son équipe : offrir la meilleure expérience culinaire à ses clients.

Mon restaurant, c'est la direction Transformation, IT et Digitale de LMEP. Mon équipe, ce sont des experts de la direction : certains conçoivent les plats – les outils digitaux –, d'autres les présentent aux clients – la promotion de l'outil – et d'autres encore veillent à l'hygiène – la sécurité informatique –.

En amont, il y a eu, bien sûr, des réflexions sur le thème du restaurant, c'est-à-dire la stratégie digitale. Moi, je m'assure que tout s'accorde comme un menu équilibré, afin que nos clients vivent une expérience si fluide et satisfaisante qu'ils ont envie de la poursuivre.

Q2. Dans une autre vie, quel métier auriez-vous exercé ?

Clairement, j'aurais choisi d'être écrivain. J'aime m'immerger dans des atmosphères diverses, saisir l'essence d'un lieu ou d'une situation, et écouter les récits du quotidien. Ces instants simples et extraordinaires – hors de mon ordinaire – sont des fragments du genre humain, uniques et porteurs de sens.

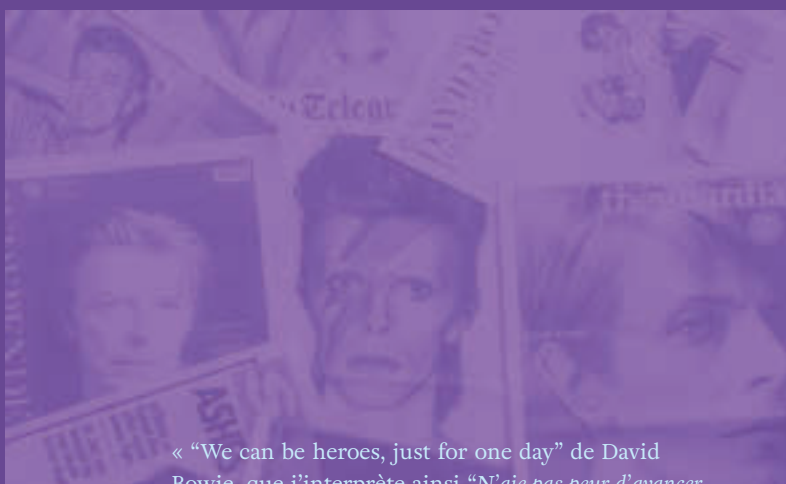
Mon enjeu aurait été de collecter ces témoignages, ces traces de vie et de les transformer en récits, quêtes, aventures ou réflexions, dans lesquels chacun pourrait trouver une réponse, une inspiration ou simplement un moment d'évasion pour avancer sur son propre chemin.

L'écriture aurait été un autre levier de transformation, une manière de coder l'avenir autrement.

Q3. Quelle personnalité emblématique vous a inspiré et quelle question lui poseriez-vous ?

D'un côté, je m'assiérais auprès de Galilée ou d'Isaac Newton. Par leurs recherches, ils ont offert une manière inédite de voir le monde, une vision qui dépasse les évidences. Je leur demanderais quelle émotion les a dominés au moment où tout a basculé, quand l'évidence les a frappés : était-ce l'euphorie d'un nouvel horizon ou la peur de voir s'effondrer les certitudes d'hier ?

De l'autre, je choiserais David Bowie, cet alchimiste de la réinvention. Je lui poserais cette question : comment avez-vous osé et trouvé l'énergie pour briser les codes et vous réinventer année après année ? Était-ce une nécessité artistique ou un rappel que, comme la technologie, la créativité est une frontière sans limite ?



« “We can be heroes, just for one day” de David Bowie, que j’interprète ainsi “N’aie pas peur d’avancer, un jour tu connaîtras ton succès” »

David Bowie

Quel conseil auriez-vous à donner à ceux qui débutent dans la tech ?

La tech a un pouvoir fascinant : elle peut paraître presque « magique », en apportant des solutions à des problèmes du quotidien encore non résolus. Mais attention, la technologie seule ne suffit pas !

Mon conseil ? Devenez un pont entre la maîtrise technique et son application sur le terrain. Posez-vous toujours trois questions simples :

1. Quels sont les enjeux de votre entreprise ?
2. Qui sont les utilisateurs : quelles sont leurs habitudes, leurs craintes, leurs envies ?
3. Comment le management perçoit-il la technologie ?

Quand une technologie est comprise, désirée et alignée avec les objectifs, elle cesse d’être un simple outil pour devenir un véritable levier de transformation et d’impact.

Anecdotes marquantes

Une désillusion marquante :

Il y a quelques années, lors d’un voyage entre le Sénégal et le Mali, un villageois m’a raconté son voyage à Paris : une expérience aussi déstabilisante pour lui que l’était pour moi la vie dans la brousse.

Lui avait été submergé par la modernité et le rythme effréné de la ville ; moi, j’étais inquiet de l’absence de repères technologiques dans cette nature riche, mais pleine de dangers.

Nous avons beaucoup ri de nos peurs respectives et j’ai compris, ce jour-là, l’importance de se questionner sur l’existence, observée d’un point de vue différent.

Q4.

Février 2003

Marque la fin, un peu brutale, de mon aventure chez Euresa-Life. Ce qui aurait pu ressembler à une chute s’est en réalité révélé être un tremplin : l’occasion de mettre à profit la diversité de mes compétences et d’orienter mon expertise là où elle pouvait créer le plus de valeurs. En saisissant cette opportunité, j’ai pu construire le parcours professionnel qui est le mien aujourd’hui.

18 juillet 2020

En plein COVID, nous donnions avec mon équipe le GO pour une migration d’outils et suivions les étapes en direct, mais chacun depuis chez soi. Ce week-end de 2020, nous avons non seulement réussi une étape clé, mais surtout lancé un nouveau mode de fonctionnement au sein de LMEP et insufflé une énergie nouvelle.


Dates
& chiffres clés



FAIRE DE LA CYBERSÉCURITÉ L'AFFAIRE DE TOUS


— Par Michaël Renotte

En mars 2024, la ville de Lille a subi une cyberattaque qui a paralysé ses services pendant plusieurs semaines. Les enquêteurs ont finalement découvert que, pour parvenir à leurs fins, les assaillants avaient utilisé un mot de passe dérobé à un employé municipal. Cet incident rappelle que, même avec les meilleurs outils techniques de protection, une simple défaillance humaine peut suffire pour compromettre la sécurité de toute une organisation.

 Malgré des investissements massifs dans les équipements de sécurité, le chiffrement et l'intelligence artificielle, l'humain reste à la fois le plus grand atout et la plus grande vulnérabilité en matière de cybersécurité. Le vrai défi pour les organisations est donc de transformer la cybersécurité d'une simple obligation réglementaire en un réflexe organisationnel aussi naturel que la bonne gestion financière, la conformité fiscale ou la sécurité au travail.

Le rôle prévalant du facteur humain

Le Verizon 2024 Data Breach Investigations Report (DBIR) a révélé que le facteur humain - hameçonnage, vol d'identifiants, erreurs, etc. - avait joué un rôle significatif dans la majorité des incidents étudiés. Dans son Threat Landscape 2024, L'ENISA - l'Agence de l'Union européenne pour la cybersécurité - confirme ce constat et souligne que l'ingénierie sociale reste une tactique privilégiée par les attaquants parce qu'elle permet de contourner de nombreuses protections techniques.

La seule mise en œuvre de politiques de sécurité ne permet pas de modifier les comportements susceptibles de mettre en péril l'intégrité des systèmes et d'ouvrir la porte aux cyberattaques. Il est essentiel de changer la culture même des entreprises en matière de protection des actifs numériques : les collaborateurs ont besoin à la fois des connaissances et de la motivation nécessaires pour agir de manière sécurisée, même si cette voie semble moins pratique ou plus contraignante. 

Former, impliquer, inspirer

Pour développer une culture de la cybersécurité, le meilleur exemple à donner est celui qui vient d'en haut. Lorsque les dirigeants montrent qu'ils accordent de l'importance à la sécurité, en participant aux sessions de sensibilisation, en posant des questions lors des réunions et en agissant eux-mêmes de manière responsable, l'ensemble de l'organisation s'en inspire.

S'il est important de donner un caractère obligatoire à la formation à la cybersécurité, celle-ci doit être pertinente, engageante et continue. Les campagnes de simulation de phishing, les modules de formation adaptés au rôle de chacun et les ateliers basés sur des scénarios concrets créent une dynamique d'apprentissage continu, bien plus pertinente qu'une procédure réduite à une liste de cases à cocher une fois par an. En France, l'Agence nationale de la sécurité des systèmes d'information (ANSSI) recommande de combiner ces initiatives de sensibilisation à des tests réguliers pour mesurer les changements réels de comportement.

Intégrer la sécurité au quotidien

La culture de la sécurité se développe d'autant mieux dans l'organisation que le comportement le plus sûr est aussi le plus simple à adopter. Cela implique de concevoir des systèmes et des processus qui réduisent les frictions : authentification forte avec connexion unique (SSO), mises à jour automatiques de sécurité et intégration de paramètres sécurisés par défaut dans les outils de tous les jours.

Les politiques doivent aussi être pragmatiques. Plutôt que d'interdire totalement l'usage d'appareils personnels (une interdiction bien souvent contournée), il est plus efficace de déployer des solutions de gestion des appareils mobiles (MDM) permettant un usage sécurisé tout en protégeant les données de l'entreprise.

Mesures et retours du terrain

Mesurer l'état de la culture de la sécurité est difficile, mais indispensable. Suivre attentivement les résultats des simulations de phishing, les taux de signalement d'incidents et le respect des politiques dans le temps permet de savoir si les initiatives portent leurs fruits. Rendre publics les progrès et valoriser les équipes qui adoptent de bonnes pratiques de sécurité renforce le message que la cybersécurité est reconnue et valorisée.

Les retours du terrain comptent également pour beaucoup dans le succès de ces initiatives : les collaborateurs doivent pouvoir signaler sans crainte les erreurs ou les activités suspectes. Cette ouverture améliore non seulement la détection des menaces, mais renforce aussi la confiance entre le personnel et les équipes de sécurité.

Un défi humain et organisationnel

Pour les organisations qui veulent passer d'une simple logique de conformité réglementaire à une véritable culture de cybersécurité, les priorités sont claires : définir ce que signifie un bon comportement de sécurité pour chaque rôle, du personnel de terrain à la direction générale ; fournir la formation, les outils et le soutien



« Plus de 90 % des employés interrogés par Gartner admettent avoir pris des initiatives dont ils savent qu'elles augmentent le niveau de risque cyber de leur entreprise »


Gartner Top Eight Cybersecurity Predictions for 2023-2024

« La cybersécurité n'est pas un problème purement technique ; c'est un défi humain et organisationnel »

ENISA Threat Landscape 2024

nécessaires pour en faire la norme ; donner l'exemple ; reconnaître et récompenser les comportements positifs ; intégrer la sécurité dans chaque décision, qu'il s'agisse de choisir un fournisseur, de lancer une campagne marketing ou de mettre à jour une ligne de produits. Comme le souligne encore l'ENISA, « la cybersécurité n'est pas un problème purement technique ; c'est un défi humain et organisationnel ».

Faire de la cybersécurité une responsabilité partagée

Passer de l'observance des règlements à une véritable culture de la sécurité est la dernière étape à franchir pour bâtir une cyber résilience durable. Cette mutation transforme la cybersécurité d'un exercice de conformité en une responsabilité partagée, inscrite dans les routines et les décisions quotidiennes. Dans un contexte où les attaquants exploitent la voie de moindre résistance, les organisations qui font de la sécurité un réflexe naturel non seulement survivront, mais prospéreront. 

NIS 2:

New Measures To Strengthen Corporate Cybersecurity

The European NIS 2 directive, which addresses corporate cybersecurity, now targets a broader range of companies and sectors, and holds company management accountable for cybersecurity. Here is an overview of the new requirements and the steps to take.



In response to the growing cyber threat and the ongoing digitalisation of services, the European NIS 2 directive (Network and Information Security) aims to harmonise and strengthen cybersecurity requirements, in order to better protect businesses and, through them, the citizens affected.

"NIS 2 was adopted in 2022 but will be implemented this year following its transposition into national law. It follows the 2016 NIS 1 directive, expanding its scope and objectives to provide even greater protection," explains Sheila Becker, Head of Network and Information Systems Security (NISS) at the Luxembourg Institute of Regulation (ILR).

Expansion of the sectors covered

More specific and more ambitious, this new directive introduces a number of key changes.

The first? A significantly broader range of companies are now affected. All entities are by default classified under two new categories: essential entities -- mainly businesses operating in highly critical sectors -- employing at least 250 people, or generating an annual turnover exceeding €50 million, or with an annual balance sheet total over €43 million; and important entities, employing at least

50 people or with a turnover or balance sheet total of at least €10 million.

This new classification comes with a significant expansion of the sectors covered: *"The space sector, manufacturing, online marketplaces, and food production, among others, are now included. The full list is available on our website ilr.lu, where you'll also find a detailed FAQ. Companies are welcome to send their questions via our dedicated email address: nis2@ilr.lu,"* notes Sheila Becker.

Registration and Incident reporting to the ILR

All affected companies must take the initiative to register themselves with their competent authority, namely the Luxembourg Institute of Regulation (ILR) or the Commission de Surveillance du Secteur Financier (CSSF) for companies in the financial sector.

Once registered, they are required to report any incident that could significantly impact cybersecurity within 24 hours.

"This could be an attack, a mishandling,

human error, a malicious act, a small explosion in the server room, or even a truck hitting an electronic communications distribution cabinet... In short, anything that could compromise IT systems and the data processed by the company," explains the Head of Network and Information Systems' Security.

Responsibility of management bodies

Another key change under NIS 2 is the accountability of company management. Cybersecurity is no longer solely the responsibility of the IT department. Executives are now expected to stay informed, undergo training, and ensure their staff are also trained on cybersecurity matters. They must understand the stakes and implement a risk analysis and IT system security policy.

It's important to note that failure to comply with the directive may result in penalties ranging from a formal warning to fines of up to €10 million or 2% of the company's total global turnover.

ILR

INSTITUT LUXEMBOURGEOIS
DE RÉGULATION

The full list is available on our website ilr.lu,
where you will also find a detailed FAQ.
Companies can also send us their questions
via our dedicated email address: nis2@ilr.lu

econocom

Sécurité dans le cloud privé : Une approche ascendante pour mieux protéger les données

— Par Badr Chimi

Face à l'essor des cybermenaces, la question de la sécurité du cloud privé est plus stratégique que jamais. Econocom PSF SA défend une approche ascendante : commencer par protéger la donnée, avant de bâtir couche par couche un environnement résilient. Alain Dekyvere et Michaël Devillet, tous deux Technical Architects chez Econocom PSF SA, nous présentent cette vision et expliquent son application concrète.

Le cloud privé, le choix de la maîtrise

Dans un paysage où les entreprises adoptent de plus en plus des architectures hybrides, le cloud privé conserve un attrait particulier. Dédié à une seule organisation, il permet de garantir un haut niveau de contrôle et d'isolation. « Le cloud privé séduit les acteurs les plus exigeants, notamment dans la finance, la santé ou le secteur public », rappelle Alain Dekyvere. « Avec notre solution Econocloud, nous leur offrons un environnement dédié, sécurisé et maîtrisé de bout en bout. »

Cette maîtrise constitue un avantage indéniable. Mais elle exige aussi une discipline constante : une mauvaise configuration ou un plan de sécurité incomplet peut transformer un atout en vulnérabilité. « C'est un paradoxe que nous rencontrons souvent : des clients choisissent le cloud privé pour sa sécurité, mais n'adoptent pas toujours les bonnes pratiques pour en tirer tout le potentiel », constate-t-il.

Repartir de la base : la donnée

L'erreur la plus fréquente, selon Michaël Devillet, consiste à se concentrer sur les couches visibles, comme les protections réseau ou applicatives, en négligeant la base même de la sécurité : la donnée. « Beaucoup d'entreprises pensent être protégées parce qu'elles ont installé un pare-feu, un antivirus ou une solution d'authentification renforcée. Mais si les données ne sont pas classifiées et protégées à la source, tout cela peut se révéler insuffisant », prévient-il.

La première étape consiste donc à identifier et classer les informations. « Nous encourageons nos clients à dresser une cartographie de leurs données, pour distinguer celles qui sont vitales et doivent bénéficier du plus haut niveau de protection », dit-il. « À partir de là, nous construisons l'infrastructure adaptée. »

Le stockage doit être conçu avec une redondance physique des composants pour résister aux pannes, un chiffrement systématique en transit comme au repos, et une isolation stricte des différents

trafics — qu'il s'agisse de la gestion, des données ou du stockage interne. « La résilience passe aussi par des sauvegardes fiables et diversifiées », poursuit Michaël Devillet. « Nous insistons sur l'importance des snapshots immuables et de l'isolement des copies critiques dans un coffre-fort numérique ou via une solution air gap. Mais surtout, nous recommandons de tester régulièrement la restauration complète. Une sauvegarde n'a de valeur que si elle peut être utilisée en cas de crise. »

La sécurité ne s'arrête pourtant pas à la technologie : « Nous alertons toujours sur la nécessité de mettre à jour ses équipements et de suivre attentivement les correctifs de sécurité publiés par les fournisseurs. Dans ce domaine, nous proposons à nos clients des services managés ou des audits réguliers que nous appelons Health Check. C'est un travail de fond, parfois invisible, mais qui fait toute la différence. »

Du stockage au réseau : un continuum de sécurité

Une fois la donnée protégée, la réflexion doit remonter vers le réseau, colonne vertébrale du cloud privé. « Le réseau transporte l'essentiel des données critiques. Il doit donc être capable non seulement de les acheminer, mais aussi de détecter et de bloquer les attaques en temps réel », pointe Alain Dekyvere.

L'installation de pare-feu dans le cloud est un premier pas, mais elle ne suffit pas. Alain Dekyvere insiste sur la nécessité de recourir à la virtualisation et à la segmentation : « Segmenter le réseau, c'est comme compartimenter un navire. Si une brèche survient dans un compartiment, les autres restent intacts. En cas d'attaque, cela permet de circonscrire l'incident et de faciliter le travail de remédiation. »

Les systèmes de détection d'intrusion complètent ce dispositif. Installés au niveau des serveurs ou sur des points stratégiques, ils surveillent en permanence fichiers, applications et flux pour repérer tout comportement suspect. Enfin, des technologies comme le SD-WAN ou les VPN sécurisent les communications étendues et chiffrent les échanges sur Internet.

Alain Dekyvere et Michaël Devillet
Technical Architects chez Econocom PSF SA

Zero Trust, le standard à adopter

Cependant, sécuriser la donnée et le réseau ne suffit pas. Le modèle de référence aujourd'hui est le Zero Trust, qui repose sur une idée simple : ne jamais accorder de confiance par défaut. « *Dans ce modèle, rien n'est acquis* », nous dit Michaël Devillet. « *Chaque utilisateur, chaque machine, chaque application doit prouver en permanence sa légitimité pour accéder à une ressource.* »

Concrètement, cela signifie que l'authentification multifactor devient obligatoire, qu'une gestion rigoureuse des accès à privilèges s'impose, et que les activités des serveurs et terminaux doivent être surveillées en continu par des solutions EDR capables de détecter les comportements anormaux. « *Le Zero Trust* », poursuit-il, « *c'est aussi cartographier et corriger les vulnérabilités grâce à des audits réguliers, et centraliser toutes les traces dans un SIEM pour pouvoir comprendre rapidement l'origine d'un incident.* »

Cette couche technologique doit être accompagnée d'une gouvernance claire : « *Nous travaillons avec nos clients sur la mise en place d'une GRC, c'est-à-dire une gouvernance qui associe analyse des risques, définition de politiques précises et plans de mitigation. Nous validons régulièrement ces dispositifs par des tests d'intrusion et des simulations de cyberattaques.* »

L'utilisateur, premier maillon de la défense

Aussi sophistiquées soient-elles, les technologies ne couvrent pas tout. Alain Dekyvere insiste : « *Le maillon décisif, c'est l'utilisateur. Chaque jour, des campagnes de phishing ou des demandes suspectes mettent à l'épreuve sa vigilance. Si l'utilisateur doute, s'il prend le temps de vérifier, il peut bloquer l'attaque dès le départ.* »

Econocom PSF SA intègre donc dans son accompagnement des sessions de sensibilisation et des mises en situation : « *Nous mettons les collaborateurs en face de scénarios réalistes. C'est en s'exerçant qu'ils acquièrent les bons réflexes. La cybersécurité est avant tout une culture* », constate-t-il.

Une sécurité en perpétuelle adaptation

La cybersécurité dans le cloud privé n'est pas un chantier ponctuel ; c'est une adaptation permanente. L'émergence de l'intelligence artificielle, qui manipule des volumes massifs de données, renforce encore l'exigence de confidentialité et d'intégrité. « *Nous devons en permanence ajuster nos pratiques pour rester au niveau des menaces. C'est un défi quotidien, mais aussi un moteur d'innovation* », souligne Michaël Devillet.

À travers sa solution Econocloud, Econocom PSF SA revendique une expertise éprouvée, qui associe technologies avancées, correctifs rapides, plans de réponse aux incidents et certifications conformes aux standards internationaux. Pour Alain Dekyvere, les certifications sont essentielles : « *Elles rassurent les clients et prouvent que nos solutions résistent aux audits internes comme externes. Elles garantissent aussi que nous respectons la législation en vigueur.* »

Il n'existe pas de sécurité absolue. Mais il existe des environnements où la confiance est construite et entretenue. « *Le cloud privé, lorsqu'il est pensé de manière ascendante, en commençant par la donnée, puis en consolidant le réseau, en appliquant les principes du Zero Trust et en formant les utilisateurs, peut offrir un très haut niveau de résilience* », résume Michaël Devillet. x



**Scannez le QR-Code
pour nous contacter.**

« Le cloud privé séduit les acteurs les plus exigeants, notamment dans la finance, la santé ou le secteur public. Avec notre solution Econocloud, nous leur offrons un environnement dédié, sécurisé et maîtrisé de bout en bout. »



The Frontier Firm: Redefining Work in The Age of AI

— By Estelle Fremaux, Associate Partner, Business Elements Reply



Estelle Fremaux
Associate Partner, Business Elements Reply

Artificial intelligence is reshaping the foundations of modern business. The Frontier Firm, a model envisioned by Microsoft, represents a decisive shift. This model envisions companies that don't merely use AI tools but rebuild themselves around them. By blending the strengths of human judgment and autonomous agents, the Frontier Firm creates a new operating system for business, one that amplifies human creativity and scales innovation. With the right partners, organizations can embrace this transformation smoothly and securely by creating and using AI agents capable of reasoning, planning, and acting into every layer of business operation.

Structural Change to Address The Capacity Gap

The pace of work has become unsustainable. Knowledge workers face hundreds of daily interruptions, while leaders demand ever-faster delivery. This mismatch between capacity and expectations creates what Microsoft calls the capacity gap. AI provides a way out. By embedding agents into business processes, organizations can reduce coordination overhead, streamline workflows, and redirect human energy toward strategic and creative tasks.

Enterprise AI adoption has already reached critical mass. According to McKinsey, 65% of businesses now regularly use generative AI tools. Microsoft reports that 81% of executives expect AI agents to be fully integrated into their strategic initiatives within the next 12 to 18 months. Those who act now will lead the frontier.

“The Frontier Firm is where human creativity meets the power of intelligent agents. This transformation is setting the stage for a new era of work, defined by adaptability, resilience, and boundless possibility.”

Human + Agent Teams: A New Operating Model

At the heart of the Frontier Firm lies human-agent teaming. Employees evolve from executors of tasks to orchestrators of systems. Rather than handling every detail, they manage AI agents that carry out workflows — in sales, IT support, or supply chain management. New roles are emerging: AI Product Owners oversee the design of agent workflows, Agent Managers supervise performance, and Governance Officers ensure compliance.

This redefinition of roles marks a cultural transformation as much as a technological one. Employees must learn to think in systems, adapt to continuous change, and collaborate with agents as true teammates. A key metric in this transformation is the human-agent ratio, a new KPI that measures how effectively human effort is being amplified by autonomous agents. By monitoring this ratio, organizations can track the balance between human oversight and agent autonomy, ensuring that collaboration remains efficient, scalable, and aligned with business outcomes.

Building The Right Foundations With Microsoft Technologies

Technology is the backbone of the Frontier Firm. Microsoft's ecosystem provides the layers needed to scale intelligence responsibly: natural language interfaces like Microsoft Copilot, reasoning engines capable of planning and orchestrating tasks, business skills integrations such as CRM and ERP, and governance frameworks that secure and regulate all activity.

To make this transformation seamless, organizations need both efficient tools and a clear strategy. Becoming a frontier firm requires a workforce that can design, manage, and improve AI systems. Business Elements Reply supports firms in translating Microsoft's vision into operational reality, identifying high-value workflows, setting up governance frameworks, and ensuring adoption happens smoothly and securely.


Increasingly, organizations are also turning to hackathons that provide employees with a collaborative, engaging, and secure environment to experiment with AI. These initiatives accelerate learning, encourage cross-functional teamwork, and make the adoption of AI both practical and accessible across the enterprise.

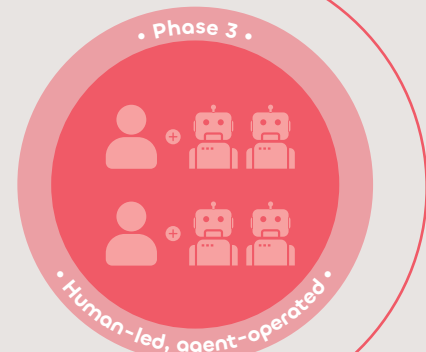
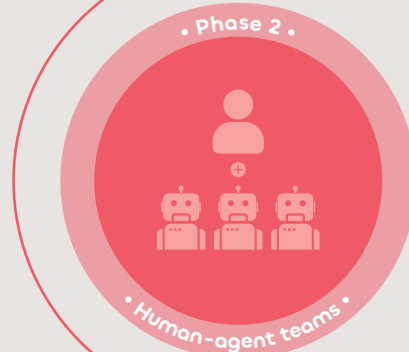
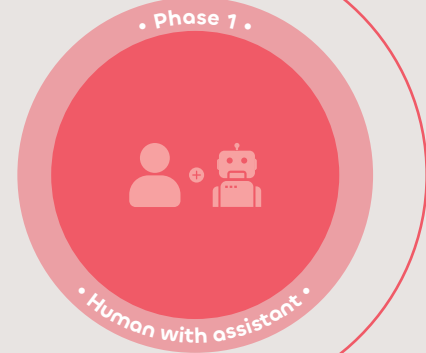
The Road Ahead: From Pilot to Scale

Transforming into a Frontier Firm is a journey that unfolds in stages. Within the first 90 days, organizations can establish an AI Transformation Office, identify pilot workflows, and launch the first agent. By the halfway point, multiple agents can operate across domains under defined human-agent ratios, with governance controls in place. After one year, companies can transition entire workflows to agent-led operations, supported by dashboards and trained managers.

Autonomous agents introduce complex challenges in compliance, data security, and ethical use. Frontier firms address these challenges by implementing role-based data access, designing policy-aware agents, and enforcing human-in-the-loop oversight for sensitive decisions. Continuous monitoring and testing, including red-teaming against adversarial scenarios, helps identify and mitigate risks early on. With the right strategy and support, organizations can evolve within a year, gaining measurable efficiency and resilience along the way.

Leading at The Frontier

The Frontier Firm is the next operating model for business. Companies that embrace this shift will achieve exponential productivity and unlock new forms of value creation. By combining Microsoft's technologies with the expertise of partners like Business Elements Reply, organizations can navigate this frontier, transforming AI into a core driver of competitive advantage. The winners of the next decade will be those who master this human-agent collaboration and redefine what it means to work, innovate, and lead. 





Repenser le recrutement IT : L'approche 360° de NSI Luxembourg

— Par NSI Luxembourg

Sur un marché du travail IT de plus en plus tendu, les entreprises luxembourgeoises doivent faire face à une problématique désormais structurelle : attirer et fidéliser les bons profils. Christophe Nicolas, Directeur de la Business Unit Talent Solutions chez NSI Luxembourg, partage son retour d'expérience sur les leviers activés en interne pour s'adapter à un environnement en constante mutation et répondre aux besoins des clients.

Une pénurie devenue chronique

La pénurie de talents IT n'est pas nouvelle, mais elle s'aggrave avec la montée en puissance de compétences pointues dans la cybersécurité, le cloud computing ou l'intelligence artificielle. Pour Christophe Nicolas, il ne s'agit plus seulement de recruter, mais de bâtir un écosystème complet autour de l'attraction, du développement et de la fidélisation des talents : « *Nous devons aller au-delà du recrutement classique. Nos BTMS – Business Talent Management Specialists – ne sont pas seulement des recruteurs, mais de véritables partenaires de carrière pour nos collaborateurs et des interlocuteurs clés pour nos clients.* »

Une organisation repensée

Depuis sa prise de fonction, Christophe Nicolas a fait évoluer le fonctionnement de la BU Talent Solutions. À la suite de plusieurs acquisitions, il a mis en place une organisation intégrée autour de huit BTMS qui accompagnent aujourd'hui près de 250 consultants, dont 180 en CDI et 70 freelances. Cette organisation hybride permet à NSI de répondre rapidement aux besoins des clients tout en offrant un cadre structurant aux talents : « *Chaque BTMS est impliqué dans le recrutement, le suivi de mission, le développement de compétences... C'est une approche à 360° qui donne du sens au travail de chacun.* »

Miser sur la montée en compétences

Dans un secteur en perpétuelle évolution, maintenir à jour les compétences est un impératif. NSI a donc investi dans une stratégie claire de développement continu via la NSI Academy, qui propose des formations internes, des certifications reconnues et un accompagnement personnalisé. « *La technologie évolue vite et nous ne pouvons pas nous permettre qu'un consultant soit dépassé. Nous anticipons leurs besoins de formation et les accompagnons dans la valorisation de leur parcours,* » témoigne Christophe Nicolas.



Christophe Nicolas
Directeur de la Business Unit Talent Solutions
chez NSI Luxembourg

Recruter autrement

Face à la concurrence des grandes métropoles comme Paris ou Bruxelles, qui peuvent offrir des packages attractifs et un télétravail quasi intégral, NSI mise sur un autre levier : sa culture d'entreprise. « *Nous mettons en avant notre proximité managériale, la diversité des missions, notre capacité d'écoute... Ce sont souvent ces éléments humains qui font la différence. Nous ne vendons pas seulement une mission, mais une trajectoire* »

NSI a également renforcé ses partenariats avec plusieurs écoles et universités pour identifier et former de jeunes talents dès la fin de leurs études. Par ailleurs, 10 à 15 % des recrutements proviennent de l'international (Maghreb, Inde, Portugal), un vivier qui nécessite un accompagnement spécifique, notamment sur les plans culturel, linguistique et administratif.

Une réussite collective

Interrogé sur sa plus grande réussite, Christophe Nicolas met plutôt en avant l'intégration réussie de son équipe après la fusion entre NSI et CTG : « *Il n'y a pas une seule réussite à mettre en avant, mais une dynamique d'ensemble. Nous avons réussi à créer une vraie cohésion malgré des parcours différents. Chacun a trouvé sa place, avec une volonté commune de faire avancer la BU Talent Solutions. La vraie victoire, c'est l'émulation et la complémentarité que nous avons mises au service de nos clients et de nos consultants.* »

TNT SYMPOSIUM

FAKE NEWS
DEEPFAKES
GENERATIVE AI
GEOPOLITICAL CHAOS

404_

REALITY NOT FOUND

→ DATE : DECEMBER 2ND, 2025

→ LIEU : GRIDX, WICKRANGE

>> BLIND MODE ACTIVATED <<
× × ×

GRIDX
LATITUDE : 49.5625 | LONGITUDE : 6.00889

FAKE MODE ON // 484...1010...0...1...235
23...1011...1...00 10 10

ORACLE



Intelligence Artificielle : Pourquoi 100 micro-projets valent mieux qu'un unique projet "moonshot"

— Par Oracle

Malgré un intérêt croissant pour l'intelligence artificielle (IA), de nombreuses organisations peinent encore à dépasser le stade des projets pilotes. Pourquoi et comment y remédier ? Sébastien Hans, Country Leader d'Oracle Luxembourg, nous livre son analyse : et si l'enjeu n'était pas de viser des projets "moonshot" — aussi ambitieux que difficiles à concrétiser — mais plutôt d'adopter une approche de micro-IA, génératrice de valeur rapide et tangible ?

« La stratégie la plus puissante est celle qui vous met en mouvement
dès aujourd'hui »

Comment expliquer l'écart entre le discours sur l'IA et sa mise en production effective dans les entreprises ?

Sébastien Hans (SH) : « Notre expérience au niveau mondial, tant auprès de nos clients qu'à travers notre propre transformation, nous a appris que tout repose avant tout sur l'approche adoptée en matière d'adoption et de transformation. Trop souvent, les organisations se lancent dans des projets "moonshot", qui, encore aujourd'hui, atteignent rarement la phase de production : selon McKinsey, 90 % des projets pilotes en IA ne passent jamais à l'étape de mise à l'échelle.

C'est également vrai au Luxembourg : malgré des ambitions fortes, nombre d'initiatives restent bloquées dans des "proof of concept" sans fin, sans lien clair avec les résultats métier ni avec une véritable gouvernance. On désigne parfois cette situation comme le purgatoire des projets pilotes — là où de bonnes idées meurent, non pas faute de potentiel, mais faute de résultats mesurables. »

Quelle est l'alternative ? Comment les organisations luxembourgeoises peuvent-elles tirer une réelle valeur de l'IA ?

SH : « Moins peut être plus. Les entreprises qui réussissent le mieux sont celles qui adoptent une approche de micro-IA. Il s'agit le plus souvent de petites fonctionnalités d'IA prêtes à l'emploi, déjà intégrées dans les applications utilisées au quotidien.

Il suffit alors aux équipes métier de les activer pour obtenir rapidement des résultats mesurables, avec un minimum d'efforts et de risques. Cette démarche a aussi un avantage stratégique : elle crée une base solide et crédible auprès du business, ce qui facilite l'acceptation de projets plus ambitieux par la suite. »

Un exemple concret ?

SH : « Imaginez que vous disposiez, aux côtés de vos équipes, de 100 stagiaires effectuant chacun une petite tâche individuelle. Chaque tâche, prise isolément, ne représente qu'une faible part de la charge de travail. Mais combinées, toutes ces petites tâches finissent par générer des gains significatifs.

Par exemple, au Royaume-Uni, The Very Group utilise nos solutions Oracle Fusion Cloud HCM pour ses 2 500 employés. L'entreprise a rapidement transformé ses processus de définition des objectifs et de revue de performance grâce à l'activation de l'IA, en un simple clic — et sans coût supplémentaire.

Imaginez maintenant ce type de bénéfices appliqué au secteur financier luxembourgeois, voire aux services publics. »

Quels pièges éviter ?

SH : « Première erreur : attendre d'avoir une stratégie IA "parfaite" avant d'agir. Autre erreur fréquente : croire que l'IA exige forcément de lourds investissements ou des projets IT complexes.


En réalité, les entreprises luxembourgeoises sont particulièrement bien placées pour tirer parti de la micro-IA, à condition de cibler des cas d'usage simples et pragmatiques.

Mais l'inverse est tout aussi risqué : se disperser ou multiplier les projets en silos sans feuille de route commune.

D'où l'importance d'un plan clair, avec une gouvernance solide, pour suivre et évaluer les déploiements ainsi que les gains. L'objectif est de détecter rapidement les problèmes, de les documenter et d'ajuster les approches en conséquence. »

Quel message clé pour les dirigeants luxembourgeois ?

SH : « Ne vous laissez pas hypnotiser par les projets "moonshot". Le succès de l'IA ne repose pas sur une percée spectaculaire, mais sur une succession de petites étapes bien ciblées qui améliorent le quotidien. Ces gains incrémentaux, une fois cumulés, génèrent un impact majeur et ouvrent la voie à des projets plus ambitieux.

La stratégie la plus puissante n'est pas celle qui promet de déplacer des montagnes, mais celle qui vous met en mouvement dès aujourd'hui. » 

90 %

Trop souvent, les organisations se lancent dans des projets "moonshot", qui, encore aujourd'hui, atteignent rarement la phase de production : selon McKinsey, 90 % des projets pilotes en IA ne passent jamais à l'étape de mise à l'échelle.

When Truth Gets Corrupted: Protecting Data Integrity in the Age of Misinformation and Breaches

— By Michaël Renotte

In October 2023, a cyberattack on a French hospital's IT system didn't just freeze access to patient records, it altered some of them. Blood type entries, medication dosages, and diagnostic notes were tampered with, forcing clinicians to halt certain treatments until data could be verified. While ransomware often dominates headlines, the less visible threat of data integrity breaches is emerging as one of the most dangerous risks in the digital economy.

[t]he challenge is simple but profound: when you can no longer trust the accuracy, completeness, or timeliness of your data, every decision – operational, financial, or medical – becomes suspect.

Data Integrity as a Core Business Risk

According to the EU Agency for Cybersecurity (ENISA), data integrity is "*the assurance that information is trustworthy and accurate*" and its loss can lead to cascading failures across systems and processes. Unlike data breaches, which focus on confidentiality, integrity attacks aim to manipulate or corrupt data – often subtly – to cause operational chaos, financial loss, or reputational damage.

Critical sectors such as healthcare, finance, energy, and manufacturing are particularly vulnerable. A 2024 NIST report warned that data integrity incidents in industrial control systems could trigger unsafe operations, supply chain disruptions, or environmental harm.

From Breaches to "Data Poisoning"

Integrity attacks take many forms. In the context of artificial intelligence, "*data poisoning*" – where attackers feed malicious or false data into training sets – can bias models, degrade accuracy, or introduce exploitable vulnerabilities. In operational systems, attackers may alter sensor readings to mislead control systems, or modify transaction logs to cover fraud.

A growing concern is the blending of integrity attacks with misinformation campaigns. An adversary might alter legitimate databases and then amplify those changes via social media to erode public trust in institutions, a tactic observed in hybrid cyber-information operations documented by CCDCOE (NATO's multinational and interdisciplinary hub of cyber defence expertise) researchers.

The High Cost of Compromised Integrity

The business impacts go well beyond technical recovery. If financial statements are corrupted, auditors may withdraw opinions, triggering regulatory scrutiny and market penalties. In healthcare, altered patient data can delay care or cause direct harm. In industrial settings, compromised operational data can result in production shutdowns, safety incidents, or product recalls.

“In the context of AI, “data poisoning” can bias models, degrade accuracy, or introduce exploitable vulnerabilities”

In some jurisdictions, integrity breaches also carry legal obligations. Under NIS2 and GDPR, significant incidents affecting the availability, authenticity, integrity, or confidentiality of data may require mandatory reporting to authorities and affected stakeholders.

Building Integrity into Cyber Resilience

Protecting data integrity starts with visibility and verification. Organizations should maintain cryptographic checksums or digital signatures for critical data sets and implement WORM storage for logs and records that must remain tamper-proof. Secure logging - ideally with blockchain-based or immutable ledger technologies - can help detect and prove changes to data.

Continuous integrity monitoring, including automated comparison of real-time data to known-good baselines, is essential for early detection. For high-impact systems, this should be combined with regular offline integrity audits to catch changes that automated tools might miss.

In AI and data analytics environments, dataset provenance - i.e. documenting and verifying the source and transformation history of data - is critical to prevent silent corruption. The EU AI Act, adopted in 2024, emphasizes data quality and integrity requirements for high-risk AI systems.

The Human and Process Dimensions

Technology alone cannot guarantee data integrity. Insider threats, whether malicious or accidental, remain a significant vector. Enforcing strict role-based access controls, separation of duties, and “four-eyes” validation for critical data changes reduces the risk of unauthorized alterations.

Training is also key. Staff must understand that modifying records, even for convenience, can have cascading effects. This cultural shift mirrors the broader push toward security-by-design: integrity is not an afterthought but a core design and operational principle.


A Leadership Imperative

Protecting data integrity is not just about avoiding tampering; it is about safeguarding decision-making itself.

Executive teams should begin by identifying and classifying the data whose integrity is mission-critical, then invest in preventive controls such as cryptographic protection, WORM storage, and secure logging. These measures should be complemented by continuous monitoring and regular offline integrity audits, ensuring



that any alterations are detected promptly. Integrity checks must also be embedded into incident response playbooks so that recovery processes address not only system availability but also the trustworthiness of the information restored. Finally, policies should be aligned with NIS2, GDPR, and any sector-specific regulations that govern the handling of sensitive or operationally critical data.

In an era of advanced cyber threats and pervasive misinformation, data integrity is the new battleground. Leaders must recognize that without trustworthy data, business continuity, safety, and reputation all stand on shaky ground. By combining robust technical controls with disciplined processes and a culture of vigilance, organizations can ensure that the data driving their decisions remains accurate, authentic, and uncorrupted - even under attack. 

Trustteam 

Avec la solution Yogosha, Trustteam Luxembourg enrichit son portefeuille cybersécurité

— Par Trustteam Luxembourg

Dans un environnement numérique de plus en plus menaçant, Trustteam Luxembourg renforce sa position de leader IT en intégrant Yogosha, plateforme de Sécurité Offensive française innovante, à son catalogue de solutions en cybersécurité. Cette intégration exclusive marque une nouvelle étape dans la capacité de Trustteam à offrir une stratégie de défense proactive, complète et sur-mesure à ses clients luxembourgeois.

Une offre cybersécurité déjà robuste... et désormais renforcée

Trustteam propose déjà une palette étendue de services cybersécurité, articulée autour de 4 piliers essentiels : "Governance, Risk & Compliance", "Training & Awareness", "Offensive Cyber Operations", et "Managed Security Services".

L'intégration de Yogosha viendra enrichir ce dispositif en y ajoutant une dimension de sécurité offensive reconnue, reposant sur une communauté de chercheurs en sécurité hautement qualifiés et spécialisés par type d'assets pour détecter des vulnérabilités exploitables, avec des programmes comme le Bug Bounty privé, le Pentest as a Service (PtaaS) et les VDP (Vulnerability Disclosure Program).

Un portefeuille renforcé, pensé pour le marché luxembourgeois

« En intégrant Yogosha à notre offre cybersécurité, nous proposons dorénavant une protection offensive haut de gamme, localement accessible, répondant aux besoins des entreprises luxembourgeoises — qu'il s'agisse des institutions financières, du secteur public ou des entreprises technologiques », commente Thierry Bousefsaf, Sales Director de Trustteam Luxembourg.

Cette nouvelle alliance permet à Trustteam d'adresser de façon cohérente les enjeux européens, notamment les exigences croissantes liées aux réglementations NIS2 (entrée en vigueur en octobre 2024) et DORA (d'application dès janvier 2025 pour le secteur financier), qui imposent des standards élevés en matière de résilience numérique et de réactions à incidents rapides.



Thierry Bousefsaf
Sales Director chez Trustteam Luxembourg


Une complémentarité unique : offensive, humaine et adaptée au Luxembourg

Ce partenariat traduit aussi une volonté stratégique de renforcer la souveraineté numérique : Trustteam reste le point de contact unique pour ses clients, tout en leur offrant une expertise européenne de pointe.

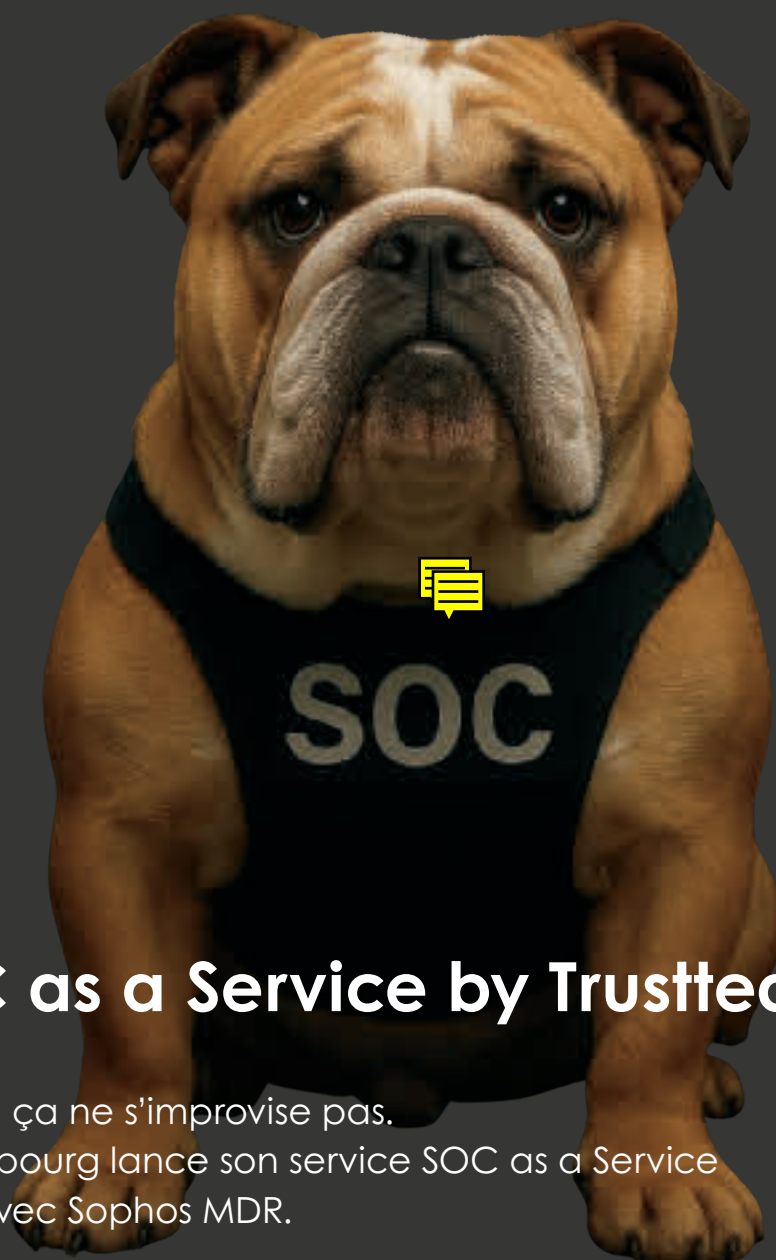
- **Offensive** : mise en œuvre proactive de détection des vulnérabilités via Yogosha.
- **Humaine** : accompagnement personnalisé au quotidien, avec des équipes ancrées localement à Capellen.
- **Adaptée** : offre conforme aux spécificités réglementaires et aux enjeux de résilience nationale.

Priorisés par Trustteam, le standard ISO 27001, les certifications PSF pour le secteur financier et la gouvernance sécurisée viennent légitimer une offre avancée, cohérente avec les besoins des organisations luxembourgeoises.

Vers une sécurité offensive de nouvelle génération

« Ce partenariat avec Yogosha représente plus qu'une simple extension d'offre », ajoute Thierry Bousefsaf. « C'est une transformation culturelle vers une cybersécurité proactive. Les clients de Trustteam disposent désormais d'un arsenal complet pour sécuriser leur environnement numérique, en détectant et anticipant les vulnérabilités — avant même qu'elles ne soient exploitées ». 

Même pas peur !



SOC as a Service by Trustteam

La cybersécurité, ça ne s'improvise pas.
Trustteam Luxembourg lance son service SOC as a Service
en partenariat avec Sophos MDR.

La protection robuste et fiable dont vos systèmes ont besoin.

✓ Surveillance 24/7 ✓ Réponse proactive aux menaces ✓ Piloté par des experts

Ransomware on the Rise: How Digital Extortion is Crippling Economies

— By Michaël Renotte

The playbook is painfully familiar: criminals gain a foothold, silently map the network, exfiltrate sensitive data, and then encrypt the most business-critical systems.

The countdown begins. For enterprises, ransomware has matured from an IT nuisance into an operational and financial crisis that hits supply chains, reputations, and balance sheets.

[r]ansom payments shattered records in 2023, exceeding \$1 billion according to the 2024 Ransomware Report by Chainalysis, a company specializing in tracing cryptocurrency transactions - a surge driven in part by mass-exploitation campaigns such as the MOVEit file-transfer attacks that swept across global supply chains.

What's Changed About Ransomware?


The scale and speed of attacks have shifted dramatically. ENISA's Threat Landscape 2024 underscores ransomware as a prime threat in Europe, with campaigns that are more automated, opportunistic, and professionalized. Threat actors now pair classic phishing and credential theft with rapid exploitation of freshly disclosed vulnerabilities and weaknesses in supplier ecosystems.

Tactics have evolved to maximize pressure. According to the EU Agency for Cybersecurity, double and triple extortion are now the norm: criminals steal data before encrypting it, threaten to disclose it, and increasingly invoke regulatory fines under laws such as the GDPR to increase pressure on victims.

The supply chain impact is particularly severe. A single exploited component or managed service can freeze hundreds of organizations simultaneously. Europol's Internet Organised Crime Threat Assessment (IOCTA) 2024 describes ransomware's central role in EU cybercrime and details how law enforcement is targeting affiliates, access brokers, and laundering networks that sustain the business model.

Ransomware's True Cost

At its core, ransomware is about business interruption. Even when a ransom isn't paid, downtime, recovery labor, and contractual penalties can exceed the ransom demand itself. The Chainalysis report shows that, while 2023 set a record for total ransom payments, early 2024 data suggested a shift: total payments fell



by roughly 35% year-over-year as more victims refused to pay, even as the number of attacks remained high. That decline in payouts is encouraging, but it has also driven attackers to escalate tactics to restore their leverage.

For EU leaders, the lesson is stark: their ability to operate - to fulfill orders, bill customers, ship goods, or provide patient care - is the real target. Cyber risk is enterprise risk.

Decisions That Change Ransomware Odds

Reducing ransomware exposure and impact starts with identity security. Stolen credentials and phishing remain the most common entry points, making phishing-resistant multi-factor authentication, minimization of standing privileges, and continuous monitoring for anomalous sign-ins non-negotiable.

Rapid patching of internet-facing services and widely deployed components is critical. Attackers now weaponize new vulnerabilities within days, often before organizations can respond. An exploit-driven patch management process with strict service-level agreements is essential.

As underlined by ENISA, resilience comes from segmentation, immutable backups, and rehearsed recovery. Network and identity segmentation limit the blast radius of a compromise, while offline, tamper-proof backups - tested regularly - ensure that an extortion demand is not the only path to restoration. Crisis playbooks should be tested through both tabletop exercises and live "pull-the-plug" recovery drills to shorten downtime.

Leaders must also understand their "crown jewels" - the systems that generate revenue and ensure safety, and the data whose exposure could cause regulatory, contractual, or reputational harm. Mapping these assets supports faster, prioritized recovery and targeted protection. This extends to the supply chain: contracts

"The Chainalysis report shows that, while 2023 set a record for total ransom payments, early 2024 data suggested a shift: total payments fell by roughly 35% year-over-year as more victims refused to pay, even as the number of attacks remained high."

with high-impact suppliers should mandate baseline security controls, defined patch timelines, logging, and incident-notification obligations, with verification through attestations or audits, as laid out in the NIS2 Directive supply chain provisions.

Should You Ever Pay?

European authorities and most incident-response experts discourage paying ransoms. Payment does not guarantee decryption or deletion of stolen data, it fuels the criminal economy, and it may create additional legal and ethical exposure. The recent decline in total ransom payments shows that resilience - i.e. segmentation, backups, and prepared communications - enables more organizations to resist paying.

However, this attitude only holds if the organization has invested in the right controls beforehand. Boards should define decision criteria, approval processes, and legal guardrails for ransom considerations before an incident, ensuring that in a crisis, leadership can act decisively rather than reactively.


Law Enforcement Pressure Is Growing

The EU and its international partners are increasingly coordinating takedowns, arrests, and infrastructure seizures that disrupt ransomware operations. Europol's IOCTA 2024 documents sustained pressure on the ransomware "as-a-service" economy, but warns that groups splinter and rebrand quickly. Organizations should engage with national CSIRTs and law enforcement early in an incident to benefit from intelligence, decryption tools, and investigative momentum.

Bending The Curve

Ransomware is no longer a niche IT concern; it is a leadership discipline. The organizations that achieve the best results are not necessarily those with the most advanced tools, but those that make a handful of strategic decisions early and rehearse them relentlessly.

Securing identities, patching quickly, segmenting networks, and maintaining tested offline backups are the technical foundations. Understanding business-critical assets, hardening supply chain security, and aligning with NIS2 and GDPR obligations round out the governance side.

The numbers tell a clear story: 2023 proved how lucrative ransomware can be for criminals, while 2024 showed that refusing to pay and building resilience can start to bend the curve. The challenge for 2025 is to keep bending it. 



« Chez CFL, le "I" d'AI
désigne l'innovation »

Chief Information Officer de la Société Nationale
des Chemins de Fer Luxembourgeois (CFL)

L'entretien

Daniel Mathieu : « Garder la complexité sous contrôle »

— Propos recueillis par Michaël Renotte

Les CFL ne se résument pas à l'image des trains qui sillonnent inlassablement le pays. Comptant plus de 5.000 collaborateurs et comportant de nombreuses filiales, l'entreprise publique luxembourgeoise couvre un large spectre d'activités. Au cœur de cet écosystème au service de la mobilité et de la logistique, l'IT joue un rôle de colonne vertébrale. Son CIO, Daniel Mathieu, raconte comment son équipe conjugue sécurité, qualité et innovation pour assurer la cohérence et la continuité d'un système complexe.

Les trois métiers d'un acteur stratégique


Lorsqu'on évoque les CFL, l'image qui vient spontanément à l'esprit est celle des trains sillonnant le pays. Pourtant, réduire l'entreprise à son parc ferroviaire serait une vision bien trop réductrice. La mission de la société va bien au-delà.

Les CFL s'organisent autour de trois grands métiers. Le premier est le **transport de voyageurs** au Luxembourg et dans la Grande Région. Il ne s'agit pas seulement d'acheminer des passagers d'une gare à l'autre, mais de leur offrir une expérience de mobilité complète. « *Notre objectif est d'accompagner l'utilisateur de bout en bout, de son point de départ jusqu'à sa destination finale* », explique Daniel Mathieu.

Concrètement, cela signifie que l'offre des CFL inclut non seulement le train, mais aussi les bus, les vélos, les voitures partagées CFL Flex, le funiculaire reliant Pfaffenthal et Kirchberg ainsi que l'ensemble des parkings connectés au réseau. L'ambition est claire : proposer une expérience de mobilité véritablement intégrée, qui va au-delà du simple voyage en train. « *L'utilisateur doit pouvoir planifier son déplacement du point A au point B, en choisissant la meilleure combinaison de modes de transport, et*

obtenir des informations pratiques comme la disponibilité d'un parking dans une heure ou le taux d'occupation de chaque voiture dans un train. » C'est dans cette logique d'intermodalité que l'IT joue un rôle déterminant. Elle permet de connecter les services, d'orchestrer les flux et de fournir à l'utilisateur une information utile en temps réel.

La deuxième activité de l'entreprise est la **gestion de l'infrastructure ferroviaire** nationale : gares, voies, centres de triage, centres de contrôle, systèmes de signalisation et de communication. Tout ce qui permet à des centaines de convois de circuler chaque jour en toute sécurité relève de ce périmètre.

Le troisième métier des CFL est le **fret**, qui dépasse les frontières du Luxembourg pour s'étendre à l'ensemble de l'Europe. Les trains CFL transportent des marchandises de toute nature, souvent dans une logique multimodale qui combine rail et route. « *L'idée est de réduire la part du camion sur les longues distances en utilisant le feroutage : les remorques sont chargées sur les trains pour parcourir 600 ou 1 000 kilomètres, avant d'être reprises par des poids lourds pour les derniers kilomètres* », illustre Daniel Mathieu. « *Le fret englobe aussi la logistique et l'entrepôtage.* Les CFL 

« Le service informatique se positionne clairement comme un partenaire des métiers »

gèrent par exemple des entrepôts capables de stocker des marchandises à -38 °C pour le surgelé, ou à 70 °C pour certains composants qui doivent être maintenus à température avant d'être transformés en produits finis. Cela peut paraître extrême, mais c'est essentiel pour nos clients industriels », précise-t-il.

« Les CFL constituent une infrastructure critique pour le pays », rappelle Daniel Mathieu. « Cela implique une obligation absolue de sécurité, de qualité et de continuité de service. Nous devons fonctionner 24 heures sur 24 et 7 jours sur 7, aussi bien pour les voyageurs que pour les marchandises. » L'enjeu est donc double : garantir la sécurité et délivrer le meilleur service au coût le plus juste, dans une logique d'efficacité qui, au-delà de la notion de performance, implique la nécessité d'une gestion durable et responsable des ressources.

Alignement dynamique avec les métiers

Le Service Informatique des CFL compte plus de 200 collaborateurs hautement qualifiés, renforcés par des partenaires externes sur certains volets spécialisés. Sa composition reflète la diversité des métiers à couvrir, du transport de voyageurs à la logistique internationale en passant par l'immobilier. « Peu d'entreprises luxembourgeoises cumulent un spectre d'activités aussi vaste », souligne Daniel Mathieu. « Nous devons répondre à des besoins très variés, parfois classiques, parfois industriels, toujours stratégiques. »

Pour structurer cette complexité, le Service Informatique s'est organisé en six divisions. La première est dédiée à la **cybersécurité** et à l'**architecture**. Elle définit l'urbanisme global du système d'information et s'emploie à garantir les meilleures exigences de sécurité. La deuxième gère les **opérations** : systèmes, réseaux, serveurs, maintenance, service desk et IT service management. La troisième est consacrée à l'**informatique industrielle** et à l'**IoT**, un domaine essentiel compte tenu de l'utilisation massive de capteurs et d'automates dans le réseau ferroviaire. La quatrième s'occupe de la **donnée** et de l'**analytique** : reporting, exploitation des données, machine learning. La cinquième développe les **applications** pour tous les métiers hors fret, avec une équipe d'environ 80 personnes. La sixième est spécifiquement dédiée aux besoins du fret, notamment pour les applications **B2B** intégrées avec les clients logistiques.

Le Service Informatique se positionne clairement comme un partenaire des métiers. « Nous ne nous considérons pas comme un fournisseur interne, mais bien comme un service à valeur ajoutée au bénéfice de l'entreprise », insiste Daniel Mathieu. « L'alignement doit être dynamique. Ce qui est vrai aujourd'hui est susceptible d'être revu demain, dans une logique d'amélioration continue de la réponse aux besoins des métiers. »

Pour fluidifier ce dialogue et améliorer le service client, les CFL ont mis en place un dispositif original : le binôme IT Business Partner (ITBP) et Digital Transformation Manager (DTM). L'ITBP est un collaborateur du Service Informatique qui maîtrise les rouages d'un métier donné. Le DTM est son homologue côté métier. Ensemble, ils traduisent les besoins, arbitrent les priorités et conçoivent les solutions. « Ce binôme permet d'éviter les incompréhensions et de maximiser la valeur créée. Il facilite la transformation digitale en rapprochant l'IT et le métier. »

Quatre axes de développement

La feuille de route de l'IT des CFL repose sur quatre axes stratégiques majeurs. Le premier est la **sécurité**, indissociable de la qualité de service. « La sécurité, qu'il s'agisse des personnes, du matériel, des infrastructures, des données ou des relations entre les parties prenantes, est au cœur de tout ce que nous faisons », assure Daniel Mathieu.

Le CIO parle de cybersécurité avec prudence : l'entreprise pratique un monitoring avancé, mène des tests et des exercices réguliers, et intègre de la redondance dans ses systèmes. « Nous restons humbles. En cette matière, il y a toujours beaucoup à apprendre et à améliorer. Nous devons nous mettre à jour quotidiennement », confie-t-il, « car notre responsabilité, c'est d'assurer la continuité de service, quoi qu'il arrive. »

Le deuxième pôle est l'orientation **service client**. « La digitalisation est partout au sein du groupe et le périmètre est très vaste. L'IT doit répondre de manière globale aux divers besoins des parties prenantes internes, des partenaires externes et des usagers. Dans ce contexte particulièrement exigeant, les équipes font preuve d'une expertise et d'un professionnalisme jamais mis en défaut », affirme-t-il.

Le troisième pan concerne l'architecture hybride. Le **Cloud** est utilisé là où il a du sens, en complément de solutions on-premise. « Le Cloud n'est pas une mode ou une tendance. Nous l'adoptons lorsqu'il apporte une efficacité réelle, en tenant compte des contraintes de sécurité, de performance et de service », dit-il encore.

Alignement dynamique avec les métiers

« Nous devons répondre à des besoins très variés, parfois classiques, parfois industriels, toujours stratégiques »

Le quatrième axe est ce que Daniel Mathieu désigne sous le terme **d'Artificial Innovation**. L'expression traduit une volonté de dépasser les effets de mode liés à l'intelligence artificielle pour se concentrer sur l'automatisation utile. « *Nous ne faisons pas de l'IA pour le buzz. Nous l'utilisons pour créer de la valeur, simplifier les processus, fiabiliser l'existant et anticiper les problèmes* », explique-t-il.

En matière d'Artificial Innovation, plusieurs cas d'usage sont à l'étude : la maintenance conditionnelle des trains, l'anticipation de l'usure des aiguillages grâce aux capteurs et aux modèles prédictifs, ou encore la surveillance du réseau par drones, qui offrent un contrôle rapide de l'état des infrastructures et la détection d'éventuels obstacles. L'entreprise explore également les technologies de Computer Vision et de BIM pour enrichir ses services, dans le respect de règles strictes de protection des données personnelles.


Ces innovations ne sont pas uniquement destinées à un usage interne. Elles débouchent aussi sur des services concrets pour l'utilisateur. Les CFL prévoient par exemple d'afficher prochainement le taux de charge de chaque voiture afin que les voyageurs puissent mieux se répartir le long du quai. A plus long terme, l'application à disposition des usagers gérant les parkings P+R affichera non seulement la disponibilité des places de stationnement en temps réel, mais aussi une prévision en fonction des événements, de la météo ou des perturbations régionales.

Gouvernance : rationaliser et éviter la prolifération technologique

L'un des défis majeurs d'un service informatique comme celui des CFL est de gérer la complexité. Pour Daniel Mathieu, la clé réside dans une bonne gouvernance

technologique : « *Notre intention n'est pas de multiplier les outils, mais de les rationaliser. Nous privilégions les solutions intégrées plutôt que d'empiler des briques disparates et nous cherchons à réutiliser les processus et technologies déjà adoptés plutôt que d'en introduire de nouveaux à chaque fois.* » Cette cohérence favorise l'efficacité et libère du temps pour l'innovation.

Il insiste sur le rôle stratégique de l'IT au sein des CFL : « *Notre vocation est d'incarner un partenaire de confiance pour les métiers et d'être un garant de la qualité de l'expérience vécue par les usagers et les clients. En gardant sous contrôle la complexité inhérente au large spectre d'activités de l'entreprise, nous assurons la continuité des services des CFL.* »

Dans un groupe aux multiples métiers, l'IT n'est pas un service de support qui fonctionne en retrait, mais la colonne vertébrale qui donne à l'ensemble opérabilité, flexibilité et sécurité. Qu'il s'agisse de l'acheminement de voyageurs au quotidien, du transport de marchandises d'un bout à l'autre de l'Europe, de la gestion d'infrastructures critiques ou du développement de nouveaux services numériques, le Service Informatique joue un rôle central. Et comme le résume Daniel Mathieu, « *c'est une mission exigeante, mais passionnante que tous nos agents réalisent au quotidien* ». 

Biographie

Physicien de formation, et après s'être consacré pendant quelques années au domaine de l'optique non-linéaire, Daniel Mathieu s'est réorienté vers la recherche industrielle avant de basculer vers la gestion des systèmes d'information. Pendant près de 25 ans, il a occupé au sein du groupe agroalimentaire Ferrero divers postes successifs de direction IT. Depuis deux ans, Daniel Mathieu est le Chief Information Officer de la Société Nationale des Chemins de Fer Luxembourgeois, CFL.



x ARICOMA

NEOFACTO & Aricoma

Une année de synergies au service de la sécurité numérique

— Par NEOFACTO

À l'heure où les cyberattaques se multiplient, intégrer la sécurité dès la conception des projets numériques n'est plus une option mais une nécessité. C'est tout l'enjeu du partenariat entre NEOFACTO, spécialiste luxembourgeois du développement digital sur mesure, et Aricoma, acteur européen de la transformation numérique et des services IT, reconnu pour son expertise en cybersécurité.

La sécurité, fondement de tout projet digital

« Tout projet sérieux intègre désormais l'aspect sécurité dès le départ », souligne Florian Sey, CTO de NEOFACTO. « Le périmètre s'élargit pour englober non seulement les mesures de protection classiques, mais aussi la vie privée, la conformité réglementaire et les enjeux éthiques liés à l'usage des technologies. Il ne s'agit plus seulement de sécuriser l'application, mais aussi la chaîne complète d'intégration et de livraison du logiciel, afin de garantir l'intégrité et la traçabilité des livrables ».

Une expertise issue de secteurs sensibles

Forte de plus de 25 ans d'expérience dans des environnements à haut niveau d'exigence — notamment la banque et les services publics —, NEOFACTO développe des solutions sur mesure respectant des standards stricts de qualité et de conformité. L'entreprise ne se positionne pas comme un pur acteur de la cybersécurité, mais ses équipes travaillent quotidiennement dans des contextes où la sécurité est omniprésente.


Une alliance stratégique

La complémentarité entre NEOFACTO et Aricoma prend toute sa valeur dans des domaines comme l'intelligence artificielle, l'analytique ou la gouvernance des données. Les deux partenaires partagent une même approche basée sur la structuration rigoureuse des

données, la conception de systèmes résilients selon le principe du security by design et la coordination étroite entre développeurs et experts en cybersécurité.

Avec plus de 2 000 collaborateurs et une offre couvrant l'ensemble du cycle de vie de la sécurité informatique — SOCs, audits, threat intelligence, services managés, ... —, Aricoma apporte un socle solide d'expertise.

Vers une nouvelle culture de projet

Au-delà de l'aspect technique, la volonté commune aux deux entreprises est de transformer en profondeur la manière dont les projets numériques sont menés. « *Ce que nous construisons* », explique Lukáš Texl, vice-président d'Aricoma en charge du développement international, « *c'est une nouvelle façon de collaborer : aligner les équipes de développement et de cybersécurité dès le départ, pour livrer des solutions plus fiables et plus résilientes* ». 

« La complémentarité entre NEOFACTO et Aricoma prend toute sa valeur dans des domaines comme l'intelligence artificielle, l'analytique ou la gouvernance des données. »



powered by **technoport®**

SAVE THE DATE

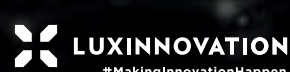
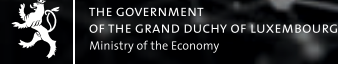
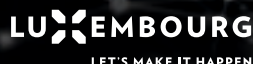
Next Summit
17-18 September 2026

Stay tuned 
www.deeptechventures.lu

Thanks to our Senior Partners



And 2024 edition Sponsors



BE PART OF IT
INFO@DEEPTECHVENTURES.LU

The Proximus logo, featuring the word "proximus" in a lowercase, sans-serif font. The "x" is stylized with a blue and purple geometric design.

LA CYBERSÉCURITÉ N'EST PAS QU'UNE AFFAIRE DE TECHNOLOGIE

— Par Proximus NXT Luxembourg

Interview avec Yvon Boutry, Security tribe leader chez Proximus NXT Luxembourg.

Les cyberattaques se multiplient, les données deviennent des cibles de choix, et la confiance est mise à rude épreuve. Dans ce contexte, nous avons rencontré Yvon Boutry, Security Infrastructure Department Manager chez Proximus NXT Luxembourg, pour comprendre comment les organisations peuvent protéger leurs informations sensibles et rester résilientes face à des menaces toujours plus sophistiquées.

Les cyberattaques n'ont jamais été aussi nombreuses. Qu'est-ce qui change aujourd'hui dans le paysage des menaces ?

Yvon Boutry : « On assiste à une professionnalisation impressionnante de la cybercriminalité. Les ransomwares restent très présents, mais ils évoluent. Les attaquants ne se contentent plus de bloquer l'accès aux données, ils les volent et menacent de les publier. Même une entreprise équipée de sauvegardes n'est donc plus à l'abri.

En parallèle, l'intelligence artificielle est devenue une arme à double tranchant. Elle aide les équipes de défense à détecter plus vite les anomalies, mais elle est aussi utilisée pour créer de faux emails, de faux profils ou des deepfakes extrêmement convaincants. Une voix clonée peut suffire à tromper un collaborateur. Cela montre bien que la frontière entre technique et humain est plus poreuse que jamais. »

L'intégrité des données est au cœur du thème de ce numéro. Pourquoi est-ce devenu un enjeu stratégique pour les organisations ?

Y.B. : « L'intégrité des données, ce n'est pas seulement s'assurer qu'elles ne soient pas altérées : c'est préserver leur valeur et la confiance qu'elles inspirent. Quand vous confiez vos informations médicales à un hôpital ou vos données bancaires à une institution, vous attendez qu'elles soient protégées.

Aujourd'hui, les réglementations comme le RGPD, NIS2 ou DORA poussent les entreprises à se mettre au niveau, mais au-delà de l'obligation légale, c'est une question de réputation et de relation avec les clients. Une fuite de données, ce n'est pas seulement une perte de fichiers, c'est une perte de confiance qui peut mettre des années à se reconstruire. »

Concrètement, comment Proximus NXT accompagne-t-elle les entreprises dans ce défi ?

Y.B. : « Notre rôle, c'est de bâtir une cybersécurité pragmatique et adaptée au contexte de chaque organisation. Nous travaillons sur plusieurs axes :

- La détection et la réponse : avec nos équipes SOC, renforcées par l'automatisation et l'IA, nous aidons à repérer les incidents en temps réel et à limiter l'impact.
- Le Zero Trust : ne jamais présumer qu'un utilisateur ou un appareil est fiable, mais vérifier en continu les identités et les accès.
- Le chiffrement et le cloud souverain : parce que nos clients veulent savoir où leurs données sont stockées et qui peut y accéder.
- La sensibilisation des équipes : car la technologie ne suffit pas. Dans plus de 70% des cas, l'attaque exploite une erreur humaine. Former, responsabiliser et donner des réflexes de sécurité reste essentiel. »



Yvon Boutry
Security tribe leader chez Proximus NXT Luxembourg

Finalement, la cybersécurité est-elle encore perçue comme une contrainte ?

Y.B. : « C'était vrai il y a quelques années : on voyait la cybersécurité comme une dépense, un frein à l'innovation. Aujourd'hui, les choses changent. La cybersécurité devient un argument de confiance et un facteur de compétitivité.

Une entreprise capable de prouver qu'elle protège ses données attire plus facilement des partenaires, rassure ses clients et peut aborder les innovations, IA, cloud, IoT, avec plus de sérénité.

Notre mission chez Proximus NXT, c'est d'aider nos clients à passer de la réaction à la résilience proactive. En clair : ne pas seulement éteindre les incendies, mais construire un environnement où la donnée est protégée, et où la confiance numérique devient un atout. »

EN SAVOIR PLUS

Envie d'aller plus loin ? Retrouvez Yvon Boutry et d'autres experts Proximus NXT dans le podcast NXT Talk.

Des discussions accessibles, concrètes et inspirantes pour comprendre les grands enjeux de l'IT.

Disponible sur Spotify et YouTube.



Pour en savoir plus sur nos services Cybersécurité et découvrir comment nous pourrions accompagner votre entreprise, contactez un de nos experts sur proximusnxt.lu.



Entre cyberscore, partenariats et accompagnement, la nouvelle stratégie de cegecom pour sécuriser les entreprises

— Propos recueillis par Badr Chimi et Nastassia Haux

Depuis 25 ans, cegecom s'est imposée comme le premier opérateur B2B alternatif au Luxembourg. Une longévité qui s'explique par une conviction : rester en mouvement et évoluer en permanence. Aujourd'hui, l'entreprise franchit une nouvelle étape avec l'ambition de devenir un fournisseur ICT 100 % made in Luxembourg. Cybersécurité et mise en conformité avec la directive européenne NIS2 figurent désormais au cœur de sa stratégie. Mais la priorité reste inchangée : répondre avant tout aux besoins de ses clients. Dans cet entretien, Serge Eiffes, Managing Director de cegecom, dévoile sa vision pour cette nouvelle ère.

Quelle est la mission de cegecom et quelle vision guide aujourd'hui votre développement au Luxembourg ?

« Nous sommes le premier opérateur alternatif pour le B2B au Luxembourg, avec 25 ans d'expertise. Nous sommes 100% made in Luxembourg et fournissons des offres sur mesure en connectivité, téléphonie, cloud IP sous toutes ses formes, internet haut débit, cybersécurité et data centers.

Notre vision est d'évoluer d'un simple opérateur télécom vers un ICT service provider, en construisant un écosystème de partenaires. Notre mission est de connecter les personnes et les entreprises avec des solutions digitales modernes, basées sur la confiance, l'expertise, la sécurité et l'innovation ».

Comment cegecom perçoit-elle les enjeux actuels en matière de cybersécurité, en particulier pour les PME ?

« Les enjeux en la matière sont énormes, mais beaucoup de PME les sous-estiment encore. Aujourd'hui, il n'est plus possible de les ignorer. Avec la réglementation NIS2, la cybersécurité devient un point crucial. Les dirigeants sont personnellement responsables et doivent prendre les bonnes initiatives, tout en étant capables de démontrer qu'ils ont fait le nécessaire pour protéger leur entreprise et leurs clients ».

« Notre vision est d'évoluer d'un simple opérateur télécom vers un ICT service provider, en construisant un écosystème de partenaires. »

En quoi votre approche de la cybersécurité se distingue-t-elle de celle des autres acteurs du marché ?

« Notre approche repose sur un écosystème de partenaires spécialisés, chacun expert dans son domaine. Cela permet d'aller en profondeur et d'apporter une valeur ajoutée réelle, plutôt que d'essayer de tout faire seuls. Par exemple, nous avons lancé un partenariat avec Luxcontrol, également 100 % luxembourgeois. Ensemble, nous proposons un audit de maturité qui délivre un cyberscore, à la manière du nutri-score ou de l'énergie-score. Ce système permet aux entreprises de situer leur niveau de protection et de définir un plan d'amélioration clair.

Nous nous distinguons donc par cet écosystème, par une approche one-stop-shop - un seul point de contact pour le client - et par notre rapidité de mise en place des solutions. Chaque client bénéficie également d'un interlocuteur unique, un chef de projet dédié qui coordonne l'ensemble du processus. Cette organisation évite toute complexité et garantit une mise en œuvre rapide et sur mesure ».



Serge Eiffes
Managing Director de cegecom

Quelles actions concrètes recommanderiez-vous aux entreprises pour renforcer leur résilience numérique face aux menaces ?

« La première étape consiste à réaliser un cyberscore ou un audit de maturité afin d'évaluer précisément la situation de l'entreprise. Cet audit permet de définir un plan d'action clair et de se conformer aux bonnes pratiques. Les entreprises peuvent également profiter des packages d'accompagnement déjà proposés, notamment par la House of Entrepreneurship, qui couvrent différents volets de la cybersécurité.

Sur cette base, cegecom peut accompagner ses clients avec des solutions adaptées. Cela inclut des connectivités hautement sécurisées et totalement indépendantes d'Internet, ainsi que des solutions multi-opérateurs intégrant un système de backup fixe et mobile. À cela s'ajoutent des solutions complémentaires comme les VPN, la protection DDoS sur toutes les lignes, les firewalls managés et des packages personnalisés. Enfin, grâce à notre partenariat avec Luxcontrol, les entreprises peuvent bénéficier d'une expertise de consultance supplémentaire si l'audit met en lumière des points à renforcer ».

Comment anticipez-vous l'évolution des menaces numériques dans les prochaines années et comment cegecom s'y prépare-t-elle ?

« Nous continuerons à investir massivement dans notre propre sécurité, au Luxembourg ainsi qu'en Allemagne via notre second opérateur, VSE Net. Comme tous, nous devons nous conformer aux réglementations de NIS2, ce qui implique de réaliser des audits réguliers et de mettre en œuvre les recommandations.

Nous avons également élargi notre écosystème de partenaires, notamment autour de l'intelligence artificielle. Dans le contexte de la cybersécurité, l'IA permettra d'automatiser certaines détections, de générer des pré-alertes et de réagir plus rapidement face aux menaces.

Nous allons rajouter d'autres partenaires à l'écosystème. Notre objectif est de proposer une solution 360°, comprenant un Security Operation Center, la business continuity, le disaster recovery et la résilience. Le tout avec une approche qui supprime la complexité pour les clients, afin qu'ils puissent se concentrer sur leur cœur de métier ».

100% made in Luxembourg

Nous fournissons des offres sur mesure en connectivité, téléphonie, cloud IP sous toutes ses formes, internet haut débit, cybersécurité et data centers.

Solution 360°

Notre objectif est de proposer une solution 360°, comprenant un Security Operation Center, la business continuity, le disaster recovery et la résilience.



Vos données, vos droits Protéger la vie privée dans un monde sans oubli

— Par Michaël Renotte

« Le respect de la vie privée n'est pas seulement une obligation légale, mais un facteur clé pour garantir la confiance sur laquelle reposent nos sociétés »
CEPD, Rapport annuel 2024

En janvier 2024, l'Autorité néerlandaise de protection des données (Autoriteit Persoonsgegevens) a infligé à l'Administration fiscale et douanière une amende de 3,7 millions d'euros pour avoir traité illégalement des données personnelles dans un système de détection des fraudes. La base de données conservait des informations pendant bien plus longtemps que nécessaire et contenait des données sensibles sans base juridique adéquate, en violation des principes du Règlement général sur la protection des données (RGPD).

[C]ette affaire illustre une vérité fondamentale à l'ère du digital : la capacité d'une organisation à collecter, stocker et traiter des données s'accompagne d'obligations, non seulement vis-à-vis des régulateurs, mais aussi envers les personnes dont la vie est reflétée par ces données. Dans un monde où chaque clic, chaque transaction et chaque mouvement laissent une trace numérique, la protection de la vie privée met à rude épreuve la gouvernance d'entreprise.

La permanence de l'empreinte numérique

Contrairement aux archives papier, les données numériques peuvent être dupliquées facilement, stockées indéfiniment et partagées à grande échelle. Cette permanence amplifie le risque d'utilisation abusive ou de divulgation non autorisée. Dans son dernier rapport annuel, le Contrôleur européen de la protection des données (CEPD) met en garde : la collecte massive de données, combinée à des techniques d'analyse avancées, peut permettre un profilage intrusif, des décisions automatisées et un traçage inter-contextes dont les individus n'imaginent pas la portée.

Dans le secteur privé, les données clients alimentent la personnalisation, le marketing ciblé et le développement de produits. Dans le secteur public, les données des citoyens soutiennent les services numériques. Mais sans garanties solides, ces deux contextes peuvent éroder la confiance. Et celle-ci une fois perdue, elle est coûteuse à rétablir.

L'ossature juridique : le RGPD et au-delà

En vigueur depuis mai 2018, le RGPD européen reste la législation sur la protection de la vie privée la plus complète au monde. Il accorde aux individus le droit d'accéder à leurs données, de corriger les inexactitudes, de demander leur suppression ("droit à l'oubli") et de s'opposer à certains traitements. Pour les organisations, il impose des principes stricts de minimisation des données, de limitation des finalités ainsi que de la durée de conservation, assortis d'amendes pouvant atteindre 20 millions d'euros ou 4 % du chiffre d'affaires annuel mondial.

En 2024, le Digital Services Act (DSA) et le Digital Markets Act (DMA) ont introduit des obligations complémentaires pour les plateformes en ligne, axées sur la transparence, le contrôle par l'utilisateur et une concurrence loyale. Parallèlement, le Data Act de l'UE - applicable en septembre 2025 - encadrera l'accès et l'utilisation des données générées par les objets connectés, remodelant encore le paysage de la protection des données.

La technologie, levier de protection de la vie privée

Si la réglementation fixe les règles, la technologie permet de les appliquer. Le chiffrement de bout en bout protège les communications contre l'interception ; les techniques de confidentialité différentielle permettent de générer des statistiques sans révéler l'identité des individus ; l'anonymisation et la pseudonymisation réduisent les risques de réidentification lors du partage de données.

Dans les environnements cloud et hybrides, les technologies de renforcement de la vie privée (privacy-enhancing technologies, PETs) gagnent du terrain. L'ENISA, qui donne des orientations sur ces technologies, souligne leur rôle dans la réduction des risques de confidentialité dans l'IA, le big data et les flux de données transfrontaliers.

Le rôle stratégique du management

Protéger la vie privée n'est plus seulement une fonction de conformité ; c'est aujourd'hui un différenciateur stratégique. Une entreprise perçue comme respectueuse des droits des utilisateurs et gérant les données de manière responsable dégage un avantage concurrentiel, tandis qu'une organisation impliquée dans un manquement à la confidentialité risque de perdre clients, partenaires et investisseurs.

Pour les dirigeants, ce constat implique d'intégrer la protection de la vie privée dans la gouvernance de l'entreprise. Cela commence par la cartographie des données : savoir quelles données personnelles sont collectées, où elles sont stockées, qui y a accès et pourquoi elles sont traitées. Les analyses d'impact sur la vie privée (PIA) doivent être menées pour toute activité de traitement à haut risque, avec des mesures de réduction des risques intégrées dès la conception. Les politiques et la formation doivent toucher non seulement le service juridique, mais aussi chaque employé manipulant des données personnelles.

Bâtir une culture de protection des données

La protection de la vie privée ne peut reposer uniquement sur des clauses juridiques et des outils informatiques. Elle nécessite de promouvoir une culture où chaque employé comprend que les données personnelles ne sont pas un actif abstrait, mais la représentation de personnes réelles. Ce changement culturel s'inscrit dans le principe de "protection de la vie privée dès la conception et par défaut", consacré par l'article 25 du RGPD, où les systèmes et processus sont conçus pour minimiser la collecte de données et maximiser leur protection dès le départ.

Des formations régulières, des circuits clairs pour l'escalade en cas de violation suspectée et un engagement visible de la direction sont essentiels pour intégrer la protection de la vie privée dans la pratique quotidienne.


« En vigueur depuis mai 2018, le RGPD européen reste la législation sur la protection de la vie privée la plus complète au monde. Il accorde aux individus le droit d'accéder à leurs données, de corriger les inexactitudes, de demander leur suppression ("droit à l'oubli") et de s'opposer à certains traitements. »

« La protection de la vie privée est aujourd'hui un différenciateur stratégique. »

Transformer la confidentialité en un atout durable

En résumé, les dirigeants soucieux de faire de la protection de la vie privée un différenciateur stratégique pour leur organisation doivent prendre une série de mesures visant à intégrer la confidentialité dans la gouvernance, les processus et la culture d'entreprise en :

- maintenant une cartographie à jour de toutes les activités de traitement de données personnelles,
- réalisant régulièrement des PIA et agir sur leurs conclusions,
- adoptant et surveillant l'utilisation de technologies de protection de la vie privée,
- s'assurant que les contrats avec les fournisseurs et partenaires incluent des obligations strictes en matière de confidentialité,
- et en donnant l'exemple par la promotion d'une culture où la vie privée est prioritaire.

Dans un monde qui n'oublie rien, la vie privée est à la fois un droit et une responsabilité. Les organisations qui l'abordent comme une valeur centrale de l'entreprise - et non comme un simple obstacle réglementaire - seront mieux placées pour maintenir la confiance, se conformer aux lois en constante évolution et exploiter la valeur des données sans compromettre les individus qu'elles représentent. 

Cybersecurity starts
with the right talent.
We **find it**
or we **build it.**



Experis[®]
ManpowerGroup



Discover how to secure your projects with us:
Cybersecurity **recruitment** & **training** by **Experis IT**



From RPA to Real Autonomy: Choosing the Right Automation and Proving Its Value

— By delaware

Not all automation is created equal, and choosing the right approach can mean the difference between transformational success and a costly misfire. At delaware, we help organizations navigate this complexity by identifying the right level of automation and tying it to measurable impact. Here's how.

The 3 levels of automation, and where they shine

1. Traditional automation (RPA)

Think digital assembly lines. RPA excels at stable, rule-based tasks — like automating journal entries — delivering speed and auditability. But it's brittle: exceptions or changes in logic require constant maintenance.

2. AI-Assisted automation (Copilots)

AI drafts, analyzes, and suggests, while humans stay in control. Copilots slot easily into existing workflows — like drafting customer emails — and boost productivity with minimal disruption. But their effectiveness remains bounded by human-in-the-loop throughput.

3. Agentic AI (Autonomous agents)

This is where automation becomes truly transformative. Goal-driven agents work end-to-end, coordinating across systems, making decisions, and continuously learning. Deployed right, they can cut claims handling costs by 40% and lift NPS by 15 points. But they also bring new challenges.

The 3 big challenges, and how to turn them into value

1. Data quality: The fuel for autonomy

Agentic AI is only as good as the data or information it uses. Bad or siloed data leads to bad decisions, compliance risks, and eroded trust.

What to do:

- Audit key data sources early
- Fix the top five issues pre-launch
- Enable real-time access via APIs or streams

Value link: Clean data raises task success rates, reduces human overrides, and speeds up ROI.

2. Monitoring & AgentOps: From "Deploy & Pray" to continuous control and improvement

Agent deployment isn't a one-off event. Without visibility, you can't detect drift, explain decisions, or prove compliance.

What to do:

- Define goal-outcome metrics (e.g. success rate, override frequency)
- Instrument every decision, and alerting solutions
- Build dashboards for execs and ops teams

Value link: Monitoring builds trust and mitigates risk, enabling confident scaling.

3. Change Management: Winning hearts and minds

Agentic AI changes not just processes, but roles. Employees move from doing to supervising, and without support, resistance can derail adoption.

What to do:

- Communicate the "why" from day one, and include the stakeholders in designs
- Start with copilots to build trust, then graduate to autonomy
- Offer training and feedback loops

Value link: Engaged teams accelerate adoption, reduce errors, and foster innovation.

"With the right balance of ambition and control, agentic AI becomes a sustainable driver of transformation."



“Not all automation is created equal, and choosing the right approach can mean the difference between transformational success and a costly misfire.”

A modular roadmap for agentic success

At Delaware, we guide organizations through a four-stage journey, modular, flexible, and value-driven:

1. Strategy & Readiness

Align on outcomes, set governance structures, and select use cases with reliable data and clear KPIs. Engage stakeholders early and anchor decisions in both operational and financial impact.

2. Pilot & Prove

Start small. Develop resilient agents with guardrails, test thoroughly, and launch in human-in-the-loop mode to manage risk.

3. Scale & Integrate

Redesign SOPs to include agentic capabilities, support evolving employee roles, and expand AI coverage across adjacent processes.

4. Optimize & Transform

Gradually increase autonomy where safe, enable multi-agent orchestration, and embed AI KPIs in business reviews. Keep compliance close.

What makes the Delaware approach work?

Data first, visibly. We dedicate a fast “Phase 0” to fix the minimum viable data set, avoiding endless prep cycles.

AgentOps from day one. We track real-time metrics like success rate and override frequency to ensure transparency.

People in the loop. We co-design pilots with frontline teams, start in copilot mode, and scale only where it makes sense.

How to start (or accelerate) your agentic AI journey, a 90day plan

1. Plan

To bring this approach to life, Delaware proposes a 12-week AI agent implementation roadmap. It begins with framing the value (Weeks 1–2), followed by making data agent-ready (Weeks 3–5). Next comes building the agent in copilot mode and gradually


transitioning toward autonomy (Weeks 6–8). In Weeks 9–10, a “prove & publish” phase helps validate impact by launching a value dashboard tracking success rate, override percentage, cycle time, and euros saved. Finally, Weeks 11–12 are dedicated to scaling: capturing lessons learned, updating SOPs, and confirming compliance sign-off. This structured yet agile framework enables fast, controlled deployment while ensuring quality, governance, and measurable business impact from day one.

2. Cost transparency beats precision

Costs vary by scope, but the key is visibility. By tracking Total Cost of Ownership, Time to Value, and Payback Period, leaders can align financial stewardship with business impact.

3. Build Momentum, Then Scale

Identify high-impact use cases, form cross-functional AI squads, and iterate quickly with agile pilots. Invest in upskilling and celebrate wins visibly. Don’t wait for perfection: use real-world metrics to scale with confidence.

As adoption grows, revisit governance and expand monitoring to include technical, user, and business KPIs. With the right balance of ambition and control, agentic AI becomes a sustainable driver of transformation. 

Keep raising the bar for autonomy, measurement, and engagement, and you will accelerate both the value and the trust in your agentic AI journey.



Want to know more?
A full article with more insight can be found on our website:
www.delaware.pro

Why No One is Safe from the New Wave of Cyber Threats

— By Michaël Renotte

In April 2025, the British retail giant Marks & Spencer (M&S) was struck by a devastating ransomware attack that brought its online store, click-and-collect service, and contactless payments to a standstill, forcing the shutdown of in-store operations for nearly four months. The estimated cost of the incident is around €350 million, and while the company has begun restoring services, the disruption has left lasting financial and operational scars. That story is no longer exceptional. From public services to manufacturers, from healthcare to logistics, cyberattacks hit organizations of every size — and every boardroom.

The Expanding Threat Landscape

Today's campaigns are highly automated, opportunistic, and increasingly professionalized. The EU Agency for Cybersecurity (ENISA) tracks the evolution of threats across Europe and notes that ransomware, phishing, and data-related threats remain dominant and continue to adapt.

SMEs are a persistent target because attackers look for reachable weaknesses at scale. ENISA's analyses over recent cycles highlight the disproportionate impact on smaller organizations and essential or important service providers in the EU.

From Technical Breach to Strategic Threat

A breach is no longer "*some stolen files*". It can halt operations, trigger contractual penalties, and erode trust, sometimes for months. Incidents in logistics and transport illustrate the cascade effects on dependent businesses; when a node is down, the network stalls. ENISA's reporting underscores how ransomware downtime and data exfiltration drive the business impact. For company leaders, the takeaway is simple: cybersecurity is a strategic risk alongside financial, legal, and operational exposures.

Leadership's Role in Cyber Resilience

Cybersecurity can't be relegated to IT, it belongs at the heart of corporate governance. Boards should integrate cyber risk into enterprise risk management, treating potential cyber incidents like any other material threat, with a clearly defined risk appetite and tolerances, as outlined in the NIS2 governance requirements for essential and important entities.

Strategic budget allocation must reflect the organization's digital exposure and regulatory obligations, whether under NIS2 or the General Data Protection Regulation (GDPR). Regular resilience testing is equally critical, not just through technical penetration tests or red teaming, but also via business continuity exercises

such as tabletop simulations to validate recovery capabilities. Finally, leaders must ensure there is a clear and actionable communication plan for cyber incidents. Transparent and timely disclosure not only preserves trust but also ensures compliance with mandatory notification duties set out in European regulations.

A European Context With Global Implications

Europe's regulatory posture is comparatively strong. Under NIS2, essential and important entities face stricter measures and administrative fines up to €10 million or 2% of total worldwide annual turnover (whichever is higher), depending on the infringement and entity category.

But supply chains are global. A breach at a non-EU vendor can still cascade into the EU. Leaders should apply consistent security baselines and contractual requirements across all partners, regardless of jurisdiction.

The Human Factor, Still the Weakest Link

According to the Verizon 2024 Data Breach Investigations Report (DBIR), the human element (including phishing, use of stolen credentials, and misconfiguration) was implicated in a majority of breaches analyzed. The report also shows phishing and credential abuse as persistent top pathways.

European authorities echo this. National agencies such as ANSSI in France regularly highlight phishing, weak authentication, and social engineering as leading initial access vectors – and stress the need for training and multi-factor authentication.


Action Points for Leaders

For executives, the path to cyber resilience starts with visibility. Conducting a comprehensive audit of the organization's digital footprint (mapping critical systems, third-party connections, identities, and sensitive data) provides the foundation for informed decision-making.

This visibility must be matched by a readiness to act: establishing breach playbooks, coordinating legal and public relations responses, and ensuring 24/7 escalation capabilities are essential to reducing downtime and confusion during an incident.

Technical defenses should follow a layered approach, combining phishing-resistant multi-factor authentication, strict privileged access controls, network segmentation, and continuous monitoring in line with ENISA and NIS2 expectations.

Finally, no technical measure can succeed without the human factor: ongoing security awareness programs, realistic phishing simulations, clear policies, and leadership accountability help build the culture that turns every employee into a frontline defender.

In 2025, every C-level executive is a cybersecurity leader. The organizations that endure aren't the ones that never face attacks. They're the ones that prepare, respond, and recover while maintaining trust with customers and regulators. Europe's frameworks (NIS2, GDPR) provide a helpful backbone; leadership turns those obligations into resilience. 

3rd Edition

AI Horizon

Conference **2025**

Build the Intelligent Future

Agentic AI · Security & Sovereignty
Frontier Firm · Human Transformation

Closing Remarks by

Hanna Engel

Microsoft Most Valuable
Professional & AI Lead @Azelis

AI-driven tech consulting

November 13TH, 2025 | From 5:30 pm
Location: Tero River House Luxembourg



AG2R LA MONDIALE

Cybersécurité et IA : AG2R LA MONDIALE adapte sa gouvernance et ses pratiques

— Propos recueillis par Badr Chimi

Phishing automatisé, deepfakes, attaques sur les modèles internes : face à l'essor des menaces liées à l'intelligence artificielle, AG2R La Mondiale renforce sa gouvernance et ses dispositifs de protection, en France comme au Luxembourg. Xavier Migaud, Directeur Cybersécurité Groupe & RSSI, et Éric Persiali, Responsable Infra LMEP, détaillent les enjeux, les réponses mises en place et la manière dont le Groupe anticipe les nouvelles réglementations européennes.

Avec la montée des menaces liées à l'IA, comment AG2R La Mondiale adapte-t-elle sa gouvernance cyber à l'échelle du Groupe, et quelles implications cela a-t-il au niveau européen ?

Xavier Migaud (XM) : « Avec l'IA, les menaces s'intensifient : le phishing automatisé permet désormais des campagnes massives, ciblées et générées par intelligence artificielle. Les deepfakes ouvrent la voie à une usurpation d'identité visuelle ou vocale, qui peut tromper nos collaborateurs ou nos clients, à l'image d'une fraude au président réinventée. De la même manière, les malwares générés par IA deviennent plus adaptatifs et donc plus difficiles à détecter. Enfin, nos propres modèles d'IA internes peuvent être la cible d'attaques, qu'il s'agisse de data poisoning, d'injections de prompts ou encore d'exfiltration de données.

Face à cette réalité, nous avons renforcé notre stratégie et notre gouvernance cyber. Nous avons d'abord actualisé notre cadre de gouvernance en intégrant les risques liés à l'IA dans notre cartographie des menaces émergentes et opérationnelles. Un comité cyber assure le suivi régulier de ces évolutions. Nous avons également musclé notre dispositif GRC avec des indicateurs spécifiques pour mieux piloter ces risques, tout en intensifiant la sensibilisation de nos collaborateurs aux scénarios d'attaques par IA et en renforçant l'expertise de notre CERT, notamment en matière de forensics.

Sur le plan opérationnel, nous avons consolidé la détection grâce à une amélioration continue de nos cas d'usage au sein du SOC et du CERT. Nous déployons plus systématiquement l'authentification forte sur nos applications critiques et intensifions le partage d'informations avec nos homologues, notamment via l'InterCERT. En parallèle, un pôle de notre département cyber est

dédié au développement de nouvelles capacités, avec une mission de veille technologique sur la cybersécurité et l'IA.

Les réglementations européennes jouent également un rôle déterminant. Une équipe dédiée au suivi de la gouvernance cyber nous permet d'anticiper une conformité toujours plus exigeante, tant au Luxembourg qu'en France. Le règlement européen DORA impose une identification et une évaluation accrues des risques cyber, tout en encourageant le partage d'informations liées aux détections de menaces. Il nous oblige aussi à notifier les autorités en cas d'attaque, avec des seuils désormais très précis. La directive NIS2, de son côté, renforce les obligations de gouvernance en matière de cybersécurité. Enfin, l'AI Act, adopté en 2024, définit un cadre pour la gestion des risques liés à l'IA. Il nous impose d'évaluer la robustesse et les risques de nos systèmes intégrant de l'intelligence artificielle. C'est pourquoi nous avons instauré une gouvernance interne dédiée, avec un collège d'experts – DPO, cybersécurité, IT – qui examine chaque projet IA et statue sur sa conformité à l'AI Act, au RGPD et aux principes de security by design ».

Les environnements collaboratifs comme Microsoft 365 et Teams sont devenus essentiels mais aussi plus exposés. Comment le Groupe et ses entités locales coordonnent-ils la détection, la prévention et la réponse aux attaques ciblant ces plateformes ?

XM : « Microsoft 365 et Teams sont des cibles privilégiées, qu'il s'agisse d'attaques pilotées par l'IA ou non. L'essentiel est d'assurer une détection, une prévention et une réponse adaptées. Un point clé est la bonne intégration de notre SIEM dans cet écosystème : nous devons nous assurer que les logs M365 sont bien collectés et exploités par le SOC et le CERT.



Eric Persiali
Responsable Infra LMEP

Nous utilisons également des outils de type UEBA et DLP, qui permettent d'identifier des comportements anormaux, comme une connexion inhabituelle ou un transfert massif de fichiers. La surveillance du darkweb complète ce dispositif, en nous aidant à anticiper d'éventuelles fuites d'informations concernant nos prestataires. Enfin, l'authentification multifacteur et une segmentation rigoureuse du réseau restent des leviers essentiels pour réduire la probabilité d'attaque et limiter notre surface d'exposition ».

Eric Persiali (EP) : « Chez LMEP, La Mondiale Europartner, nous utilisons uniquement Teams et Azure AD. Le périmètre de fonctionnalités – et donc de risques – reste limité, mais nous maintenons une surveillance active grâce à des outils d'audit qui détectent les comportements ou tentatives de connexions anormaux. Nous avons également mis en place un geofencing interdisant toute connexion depuis des pays jugés à risque, comme la Russie ou la Chine. Cela réduit de manière significative notre surface d'attaque ».

Des projets locaux récents ont-ils représenté des défis à surmonter en matière de cybersécurité ?

EP : « Pour LMEP, le projet majeur est la migration de nos solutions et données on-premise vers une instance Microsoft 365 dédiée et en ligne. Notre premier défi est de réussir le transfert des données et la migration des services. Le second, tout aussi important, est d'assurer la sécurisation de l'instance M365, de l'ensemble des données, des accès et des fonctionnalités.

Ces deux volets doivent avancer conjointement, l'un ne pouvant se réaliser sans l'autre. Pour relever ce défi, LMEP investit dans des outils de sécurité spécifiques – DLP, chiffrement avec clés propriétaires, SOC et SIEM –, dans la montée en compétences de ses équipes à travers formations et expertises CERT, et dans une surveillance continue grâce aux tests de vulnérabilité et aux pentests ».

Avec la mise en place d'Almia, votre plateforme interne d'IA générative, et vos déploiements dans le Cloud, comment protégez-vous vos systèmes face aux risques ?

XM : « Les déploiements cloud – IaaS, PaaS, SaaS – offrent agilité et scalabilité, mais accroissent aussi notre exposition aux risques cyber. La protection repose sur un triptyque : gouvernance, contrôles techniques et conformité réglementaire. Notre gouvernance IA, associée à notre méthodologie d'analyse des risques cyber dans les projets, nous permet de bâtir un socle de contrôle solide. Nous disposons également de compétences internes nous permettant de mener nos propres tests d'intrusion et d'organiser régulièrement des exercices de red teaming.

Le chiffrement des données sensibles reste notre meilleur atout contre les pertes de confidentialité en cas d'attaque. Par ailleurs, nous avons fait le choix d'un Cloud en cours de qualification SecNumCloud. AG2R La Mondiale est l'une des premières entreprises à avoir retenu S3NS, la coentreprise de Google et Thales. Le service de chiffrement externe proposé par Thales et hébergé sur S3NS protège désormais nos données stockées sur GCP ».

EP : « Les objectifs d'innovation IA pour LMEP s'alignent avec la solution Almia développée au niveau du groupe. Pour répondre à la réglementation du Commissariat aux Assurances et aux contraintes liées aux données sensibles au Luxembourg, une instance Almia spécifique à LMEP sera déployée. Hébergée et sécurisée par les services GCP et S3NS, elle sera opérée directement par nos équipes locales, conciliant ainsi expertise, sécurité et conformité réglementaire. »



Xavier Migaud
Directeur Cybersécurité Groupe & RSSI

AI, Blockchain, and Beyond: The Tech That's Reinventing Cybersecurity

— By Michaël Renotte

“Advanced technologies like AI, blockchain, and zero trust are reshaping the cybersecurity landscape.”

In late 2024, researchers demonstrated that AI-driven detection models can spot ransomware activity hours before file encryption begins, not through constant human monitoring, but by flagging abnormal patterns in user behavior and system activity. This is the promise of next-generation cybersecurity: tools that are not just reactive, but predictive.

[a]s cyberattacks grow more complex and automated, defenders are increasingly turning to advanced technologies - artificial intelligence, blockchain, and zero-trust architectures - to level the playing field. The question for leadership is no longer whether to invest in these tools, but how to integrate them strategically into a broader security posture.

AI as the New Threat Hunter

AI and machine learning (ML) are transforming threat detection and response. By analyzing vast volumes of network traffic, endpoint logs, and behavioral data, AI systems can spot anomalies that may indicate an intrusion, even if the specific attack signature has never been seen before.

In its report Artificial Intelligence Cybersecurity Challenges ENISA, the EU Agency for Cybersecurity, highlights AI's role in shortening "dwell time" - the period attackers spend undetected inside a network - and in enabling automated containment of compromised systems.

However, AI in cybersecurity is not without risks. Adversarial attacks, in which threat actors manipulate AI models or feed them misleading data, can blind detection systems. This means organizations must pair AI-driven tools with robust validation, human oversight, and continuous retraining of models to avoid "model drift" and false confidence.

Blockchain for Integrity and Transparency

Beyond cryptocurrencies, blockchain technology is finding its place in cybersecurity for its ability to create immutable, verifiable records. Distributed ledger systems can be used to secure logs, verify software integrity, and ensure that data has not been altered without authorization.

For example, in the European Commission-funded SPARTA cybersecurity research program, blockchain-based logging is being tested to improve the forensic reliability of audit trails and ensure regulatory compliance in sectors such as finance and healthcare. In supply chain security, blockchain can provide traceability of hardware and software components, reducing the risk of tampering and counterfeit insertion - a concern highlighted in the NIS2 Directive's supply chain provisions.

Zero Trust: The Architecture for a Borderless World

Traditional network security models assumed a "trusted" internal network and an "untrusted" outside world. That assumption has been dismantled by cloud adoption, hybrid work, and the proliferation of connected devices.

Zero trust architectures (ZTA) operate on the principle of "never trust, always verify." Every request, whether from inside or outside the corporate network, is authenticated, authorized, and encrypted. ENISA and NIST both promote zero trust as a key approach for modern enterprises, emphasizing identity-based access controls, micro segmentation, and continuous verification.



Implementing zero trust requires more than technology; it demands organizational change. Asset classification, identity management, and rigorous policy enforcement become daily disciplines, not occasional projects.

Opportunities and Risks

Emerging cybersecurity technologies present both strategic opportunities and governance challenges. AI can deliver faster detection and response, blockchain can enhance trust and compliance, and zero trust architectures can close gaps created by modern working patterns.

However, these technologies are not silver bullets. They require skilled teams, integration with existing systems, and an understanding of both their limitations and regulatory implications. For example, AI systems processing personal data must comply with the GDPR, and the EU AI Act - entered into force on August 1, 2024 - will impose additional transparency and risk management requirements for high-risk use cases.


From Pilot to Production

Adoption should start with pilot projects targeting high-value use cases - for example, deploying AI-driven detection in critical network segments, or using blockchain to secure audit logs for compliance-sensitive applications. Pilots should have clear metrics for success, such as reduced detection time, improved accuracy, or audit pass rates.

Once validated, these technologies can be scaled and integrated into a layered defense strategy that combines prevention, detection, response, and recovery.

Security Strategy Accelerators

Advanced technologies like AI, blockchain, and zero trust are reshaping the cybersecurity landscape. But their value depends on leadership's ability to deploy them wisely. They should be viewed not as stand-alone solutions, but as accelerators of a mature, risk-based security strategy.

The competitive advantage will belong to organizations that can adopt these innovations early, integrate them seamlessly, and manage their risks responsibly, proving that, in cybersecurity, the best defense is not only strong, but smart. 

SPARTA

In the European Commission-funded SPARTA cybersecurity research program, blockchain-based logging is being tested to improve the forensic reliability of audit trails and ensure regulatory compliance in sectors such as finance and healthcare.

ZTA

Zero trust architectures (ZTA) operate on the principle of "never trust, always verify." Every request, whether from inside or outside the corporate network, is authenticated, authorized, and encrypted.



Appareils personnels et risques d'entreprise L'avenir de la sécurité BYOD selon ESET

— Par ESET

Aujourd'hui, le lieu de travail est plus mobile, plus connecté et plus personnel que jamais. D'une politique marginale, la tendance du BYOD (Bring Your Own Device) est devenue une pratique courante. L'une des principales préoccupations en matière de sécurité liées au BYOD est l'absence de protection standardisée des appareils personnels. Cette lacune a pour conséquence d'élargir la surface d'attaque que les entreprises et leurs équipes de sécurité doivent impérativement protéger.

[n] e bénéficiant pas des fonctionnalités de cybersécurité et des restrictions imposées par l'entreprise, les appareils personnels peuvent être exposés aux cybermenaces via des applis malveillantes ou des liens d'hameçonnage si les utilisateurs manquent de formation en cybersécurité. Ces appareils peuvent être utilisés par des personnes étrangères au personnel de l'entreprise ou être connectés à des réseaux publics non sécurisés, ce qui en fait des cibles privilégiées pour les attaques.

L'ombre de la Shadow IT

La "Shadow IT" est un autre problème important. Trop souvent, des employés installent des applications non autorisées ou utilisent des services cloud non contrôlés à des fins professionnelles, pensant ainsi améliorer leur productivité. Il peut s'avérer complexe de s'assurer que ces appareils respectent des normes réglementaires strictes, comme celles décrites dans le RGPD en Europe ou dans les lois HIPAA et CCPA aux États-Unis. Les organisations doivent donc adopter une approche plus proactive et plus structurée pour sécuriser les environnements BYOD.

Des politiques de sécurité claires et contraignantes

La visibilité est à la base d'une sécurité BYOD efficace. Dans ce cadre, il est essentiel pour les entreprises d'inventorier chaque appareil personnel accédant aux ressources de l'entreprise — serveurs de messagerie, plateformes internes, disques partagés et applications cloud.

Elles doivent ensuite appliquer des normes de sécurité minimales et imposer une configuration optimale. Il peut s'agir de chiffrement obligatoire, de mots de passe robustes, de l'authentification à deux facteurs ou de la protection des terminaux. Tout cela doit être clairement défini dans une politique BYOD officielle à laquelle les employés adhèrent avant de connecter leurs appareils aux réseaux de l'entreprise.

Pour atténuer les risques liés à la "Shadow IT", les organisations seraient bien avisées d'implémenter des politiques de contrôle des applications, telles que la mise sur liste noire des applications à risque ou sur liste blanche des outils approuvés.

La gestion des mises à jour, un défi partagé

Corriger les vulnérabilités connues et mettre à jour rapidement les appareils sont parmi les moyens les plus efficaces de prévenir les violations. Mais dans des environnements BYOD, la responsabilité de maintenir les logiciels à jour incombe souvent à l'employé, ce qui peut constituer un autre problème.

C'est ici que les solutions de gestion des appareils mobiles (Mobile Device Management, MDM) prennent toute leur valeur. Elles permettent aux équipes informatiques d'assurer le suivi, la protection et la conformité des terminaux personnels utilisés dans l'entreprise.

Lorsque leur déploiement n'est pas envisageable, les administrateurs doivent a minima mettre en place des mesures alternatives :

« Alors que les modèles de travail évoluent continuellement, le BYOD restera un pilier des stratégies de mobilité des entreprises. »
ESET

- rappeler régulièrement aux utilisateurs d'installer les mises à jour,
- fournir des instructions claires pour faciliter l'application des correctifs,
- suivre l'état d'avancement de ces mises à jour pour garantir une résolution rapide des failles de sécurité,
- prévoir l'effacement des données en cas de perte ou de vol d'un appareil,
- veiller au respect des politiques de l'entreprise.

Ces actions doivent être menées avec un juste équilibre : renforcer la sécurité sans empiéter inutilement sur l'espace numérique personnel des employés.

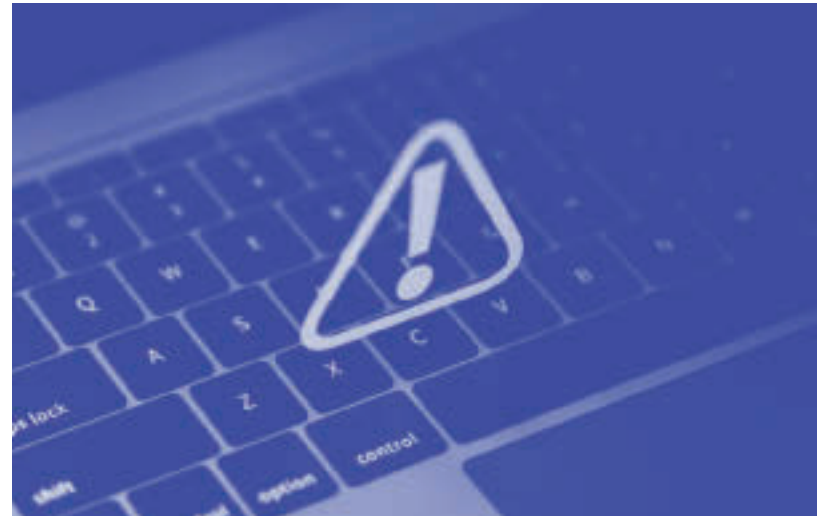
Le télétravail et l'enjeu du réseau

En matière de télétravail, que les employés travaillent chez eux ou dans un lieu public, l'utilisation de réseaux Wi-Fi publics ou non sécurisés présente un risque important. Le déploiement d'un réseau privé virtuel (VPN) correctement configuré est indispensable. Les VPN créent des tunnels cryptés, protégeant les données en transit et réduisant le risque d'attaques.

Les organisations doivent en outre s'assurer que l'accès au protocole RDP (Remote Desktop Protocol) est configuré de manière sécurisée pour protéger l'accès à distance. Les RDP mal configurés étant souvent un vecteur de cyberattaques, les entreprises doivent traiter la configuration avec la même rigueur que les autres systèmes.

La protection des données sensibles

Stocker des données sensibles de l'entreprise sur des appareils personnels augmente le risque d'exposition en cas de perte, de vol ou d'accès par un autre membre de la famille. Pour y remédier, il faut établir des règles imposant la protection par mot de passe, le verrouillage automatique et le chiffrement des appareils. Les données classées comme confidentielles ou critiques doivent être chiffrées au repos et en transit. L'authentification multifactorielle



(AMF) est obligatoire pour tout accès aux systèmes hébergeant des données sensibles.

Former et responsabiliser les employés

La force d'une politique BYOD dépend de son utilisateur le plus vulnérable. Les organisations doivent donc prévoir des logiciels de sécurité multicouches spécifiques à chaque appareil, avec protection anti-malware et chiffrement sophistiqués, ainsi que des fonctions d'effacement à distance.

Des sauvegardes régulières et des formations régulières à la sécurité sont essentielles. Les employés doivent comprendre les risques liés à l'utilisation d'appareils personnels à des fins professionnelles et les mesures à prendre pour protéger leurs informations et celles de l'entreprise.

La confiance comme condition de réussite

Les entreprises doivent être transparentes à propos des données auxquelles elles auront accès et à la manière de respecter la confidentialité des données personnelles des employés. Les solutions MDM prenant en charge les architectures privilégiant la confidentialité - en séparant les données professionnelles des données personnelles - peuvent aider à combler ce fossé. Créer la confiance entre les équipes informatiques et les employés est essentiel à la réussite de toute initiative BYOD.

Vers un futur hybride et sécurisé

Alors que les modèles de travail évoluent continuellement, le BYOD restera un pilier des stratégies de mobilité des entreprises. Dès lors, entreprises et employés doivent accepter que les appareils ne soient plus "personnels" lorsqu'ils accèdent aux systèmes et données critiques de l'entreprise.

L'avenir appartient aux organisations capables d'être flexibles tout en maintenant de solides bases de cybersécurité. Le recours au BYOD est pratique et apporte des avantages certains, mais il introduit aussi un risque. Les responsables informatiques doivent donc implémenter des mesures de protection stratégiques pour protéger à la fois leurs collaborateurs et leurs données. x



Orange Flexy, un forfait mobile pensé pour la résilience numérique des entreprises

La connectivité est devenue un pilier de l'activité des entreprises, qu'il s'agisse de maintenir la disponibilité des équipes en déplacement, d'assurer la réactivité des services d'urgence ou encore de soutenir le télétravail. Dans ce contexte, Orange Luxembourg propose Orange Flexy, une offre mobile qui combine flexibilité tarifaire et continuité de service.

Garantir la disponibilité en toutes circonstances

La dépendance aux réseaux mobiles s'est accrue avec l'accélération de la transformation numérique et l'adoption massive d'outils collaboratifs. Une interruption de service peut rapidement impacter la productivité et, dans certains cas, compromettre la capacité d'intervention d'une organisation.


C'est précisément sur ce terrain qu'Orange positionne Flexy : offrir des lignes de secours prêtes à l'emploi, sous forme de SIM physique ou d'eSIM, accessibles y compris aux entreprises qui ne sont pas clientes de l'opérateur. Cette approche permet, par exemple, à un service informatique de maintenir la connectivité de ses collaborateurs en toutes circonstances, ou à une équipe commerciale de rester joignable en déplacement malgré un incident imprévu.

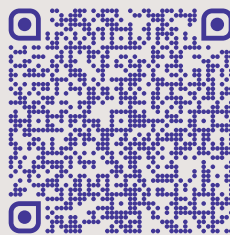
Une facturation adaptée à l'usage réel

Le modèle économique d'Orange Flexy repose sur la souplesse : lorsqu'une ligne n'est pas activement utilisée, son coût se limite à deux euros par mois. Dès qu'un usage est détecté – appel, SMS ou connexion internet – le forfait s'ajuste automatiquement. Cette logique vise à optimiser les coûts tout en assurant une disponibilité immédiate.

Dans la pratique, un tel système peut s'avérer utile pour des flottes de mobiles d'astreinte, destinés à être mobilisés seulement en cas de besoin. Les organisations disposent ainsi d'un outil de résilience sans supporter le coût d'un forfait complet permanent.

Flexibilité, maîtrise des coûts et continuité de service

Orange Flexy illustre une tendance plus large dans le secteur des télécommunications : l'évolution des offres vers des modèles centrés sur la flexibilité et la maîtrise des coûts. Pour Jean-Sébastien Berneyron, Head of BtoB Sales chez Orange Luxembourg, cette solution constitue « un atout pour garantir la performance et la réactivité des entreprises aujourd'hui », en conjuguant adaptabilité et continuité de service. 



Contactez dès aujourd'hui les experts d'Orange Luxembourg en flashant ce QR code.



ENJOY

TIMELESS TASTE



Traiteur d'exception *pour tous vos événements*

+352 47 47 47 1
catering@kaempff-kohler.lu
40 rue Gabriel Lippmann
L-6947 Niederanven



PROGRAM- MATION 2025

TNTRIP

From October 1st to October 3rd, 2025

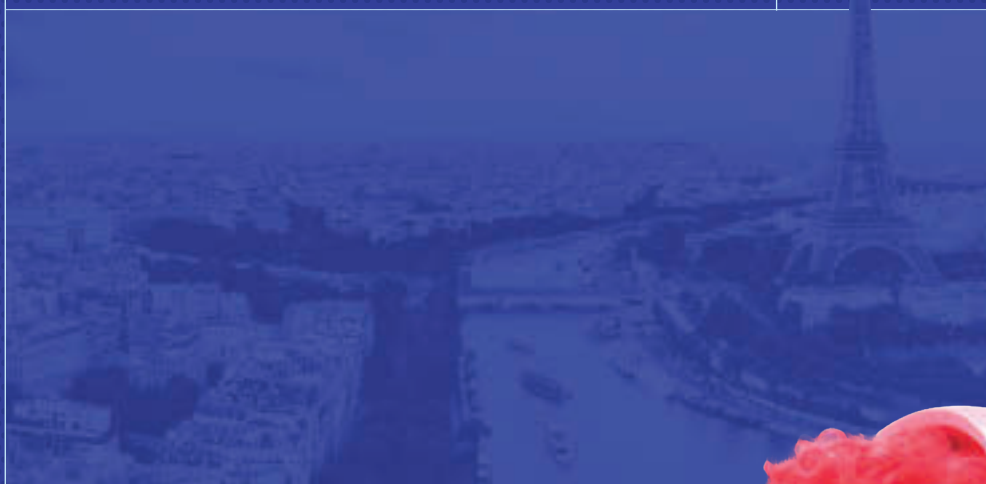
Paris

Embark on an unforgettable journey with fellow CIOs and tech leaders to one of Europe's most iconic destinations: Paris. A city where culture, leadership, and innovation converge.

Amid global conversations on AI and digital transformation, our program is designed to inspire and connect. Join immersive workshops, share insights with pioneers, and explore the future of technology together.

Highlights include an exclusive Jules Verne-inspired performance in a historic château, where you'll step right into the story.

TNTRIP 2025 is more than an event—it's a voyage of innovation, connections, and unique Parisian moments.



November 13th — 2025

PWC

The **TechSense Summit** gathers CIOs and tech decision makers to offer them the opportunity to connect and exchange about different topics as AI & Data, Cybersecurity, Cloud, Green IT, ESG etc.

This event features roundtable, client stories, workshops on the topics of the event and networking.





From November 24th to 28th

Discover concrete solutions with Distributed Ledger Technology (DLT), Digital Assets, Decentralised Finance, Web3 and more.

Stay up to date with the latest developments and applications of DLT across industries. Since April 2021, Luxembourg Blockchain Week has established itself as Europe's main event for institutional Digital Assets.

Alongside the core Finance event, it also hosts diverse satellite events, open to a wider audience, offering insights into DLT through various places, speakers and topics.

TNT SYMPOSIUM

December 2nd — 2025

GRIDX

At the end of November, TNT Symposium will gather Technology, Innovation and Digital decision-makers for an explosive evening! More than a Gala, it promises you: ideas to share and learn, networking opportunities, a convivial atmosphere, new business leads, and pride for the award winners. The program includes a conference, cocktail and dinner.

Mark your calendars!

The Dots podcasts: Discover our unique formats!

- **Kamel Sans Filtre** : Join an open conversation with Kamel Amroune, where sensitive topics around tech will be discussed without beating around the bush.

- **90 Secondes Outside** : The challenge? Introduce yourself and answer professional questions in record time. A short, impactful, and efficient immersion!

Ready to try the experience? Come record in our brand new studio. Customizable formats according to your needs.

Contact us to know more!

D. +352 20 60 29 410



Tuesday - Wednesday

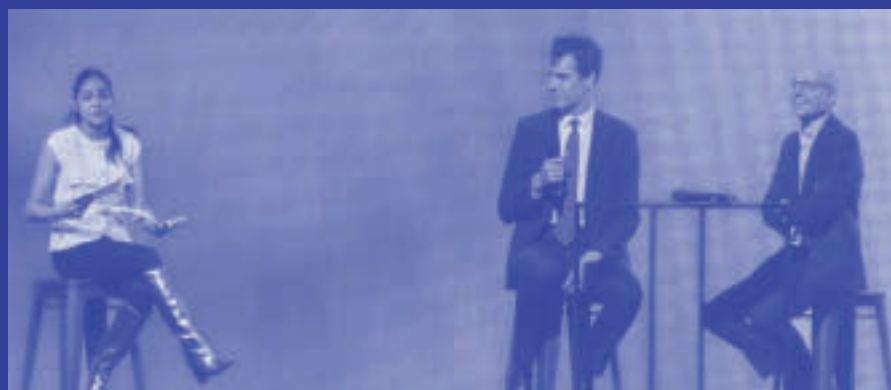
June 10th - 11th — 2026

Luxembourg City

Nexus Luxembourg, the new annual tech event, presents three days of discovery, inspiration, and learning, as well as opportunities for encounters, networking, and matchmaking.

Nexus Luxembourg is an international hub for stakeholders combining ecological and digital transitions, aiming to leverage technology for the benefit of governments, organisations and businesses to achieve their net-zero strategies by 2050. It's about using technology to advance human progress, considering both productivity gains and addressing pressing ethical issues.

Nexus Luxembourg is also a showcase of Luxembourg's tech and innovation ecosystem and will feature numerous public and private initiatives.





the
Dots.

MANAGING EDITOR

Kamel Amroune

CEO

kamel.amroune@thedots.lu

ADVERTISING CONTACT

Aurélié Paini

Head of Sales & Operations

aurelie.paini@thedots.lu

+352 691 339 918

Ludivine Barthel

Project Manager

Sales, Marketing & Event Officer

ludivine.barthel@thedots.lu

+352 691 181 057

EDITORIAL TEAM

Michaël Renotte

Editor-in-Chief

michael.renotte@thedots.lu

Nastassia Haux

Editorial Contributor

Marketing Manager

nastassia.haux@thedots.lu

Badr Chimi

Editorial & Content Assistant

badr.chimi@thedots.lu

PHOTOGRAPHER

Jordan Koenig

Digital Content Officer

jordan.koenig@thedots.lu

DESIGN

Nicolas Bœuf

Art Director

nicolas.boeuf@thedots.lu

DISTRIBUTION

Post Luxembourg

PRINTING

BDZ Luxembourg

Print 1000 exemplaires

EDITOR

The Dots

281, Route d'Arlon

L-8011 Strassen

+352 20 60 29 410



the
Dots. #12
MAGAZINE

À retrouver dès
le mois de février

