N°221 — Novembre 2023

www.linformaticien.com

L'INFORMATICIEN

RH/formation
AFNIC contre le cybersquatting

Étude
Le Cigref se projette dans le futur

DOSSIER STOCKAGE

LE BRAS ARMÉ DE LA RÉSILIENCE

Hardware
Lenovo : l'IA dans votre poche

Retex
Pierre Fabre met en place un data mesh

L 14614 - 221 - F: 8,50 € - RD

Innovation
RAILwAI optimise les infrastructures ferroviaires

Construire des applications métiers solides, performantes et durables !

- Audit de code
- Création d'API
- Développement sur-mesure
- DevOps
- Écoconception
- Maintenance
- Expertise web et mobile
- Optimisation des performances

AXOPEN

AXOPEN c'est une équipe de 50 profils techniques spécialisée dans le développement et la maintenance d'applications métiers sur-mesure.

axopen.com

www.linformaticien.com

L'INFORMATICIEN

RÉDACTION

15, avenue de la Grande Armée, 75116 Paris, France.
Tél. : +33 (0)1 74 70 16 30 — *contact@linformaticien.com*

RÉDACTION : Bertrand Garé (rédacteur en chef)
et Guillaume Périssat (chef de rubrique)
avec : Olivier Bellin, Pierre Berlemont, Patrick Brebion, Jérôme Cartegini, Michel Chotard, Alain Clapaud, François Cointe, Victor Miget et Thierry Thaureaux.

SECRÉTAIRE DE RÉDACTION : Boutheïna Saddi

MAQUETTE ET RÉALISATION : Franck Soulier (chef de studio)

PUBLICITÉ
Tél. : +33 (0)1 74 70 16 30 — *pub@linformaticien.com*

VENTE AU NUMÉRO

France métropolitaine 8,50 € TTC (TVA 5,5 %)

ABONNEMENTS

France métropolitaine 72 € TTC (TVA 5,5 %)
magazine + numérique

Toutes les offres :
www.linformaticien.com/abonnement

Pour toute commande d'abonnement d'entreprise ou d'administration avec règlement par mandat administratif, adressez votre bon de commande à :

L'Informaticien, service abonnements,
5, avenue de la Grande Armée, 75116 Paris, France.
ou à abonnements@linformaticien.com

IMPRESSION

Imprimé en France par Imprimerie Chirat (42)
Dépôt légal : 4ème trimestre 2023

Toute reproduction intégrale, ou partielle, faite sans le consentement de l'auteur ou de ses ayants droit ou ayants cause, est illicite (article L122-4 du Code de la propriété intellectuelle). Toute copie doit avoir l'accord du Centre français du droit de copie (CFC), 20 rue des Grands-Augustins 75006 Paris. Cette publication peut être exploitée dans le cadre de la formation permanente. Toute utilisation à des fins commerciales de notre contenu éditorial fera l'objet d'une demande préalable auprès du directeur de la publication.

L'INFORMATICIEN est publié par PC PRESSE, S. A. S.
au capital de 130 000 euros.
Siège social : 15, avenue de la Grande Armée, 75116 Paris, France.

ISSN 1637-5491

Une publication PCpresse,

GROUPE FICADE

PRÉSIDENT, DIRECTEUR DE LA PUBLICATION :
Gaël Chervet

Le mot de l'année

Face à un contexte incertain et souvent dangereux, Résilience a certainement été le mot de l'année 2023. Il devrait encore tenir son rang en 2024. Pour parvenir à cet état de résilience, une pratique est souvent oubliée, ou peu mise en avant : le stockage. C'est notre dossier du mois. Face aux attaques, à l'augmentation explosive du volume des données, celui-ci s'adapte et suit les dernières tendances technologiques comme l'Intelligence Artificielle, les améliorations continues sur les disques flash ou non, les mémoires, le Cloud. Si les cas d'usages sont souvent différents entre blocs, fichiers et objet, les offreurs abondent dans le sens d'une unification ou l'utilisateur peut selon ses besoins choisir l'un ou l'autre. Lorsque le stockage devient trip complexe ou difficile à gérer, le « storage as a service » supplée le manque de ressources, de moyens, de compétences. Le stockage est à la fois la première ligne et le dernier bastion de la résilience de l'entreprise et redevient une infrastructure stratégique pour les entreprises pour préserver le premier actif de celles-ci : les données.

Autre moment important, le Palmarès de *L'Informaticien* va rendre ses verdicts dans sa troisième édition. Nous reviendrons largement dessus dans notre prochain numéro avec, je l'espère, de nombreux gagnants à nos côtés lors de la remise des prix qui se tiendra le 20 novembre prochain dans les Salons Hoche.

Toujours sur le terrain, *L'Informaticien* vous rendra compte des principales conférences qui se sont tenues récemment aux USA ou en Europe. Vous retrouverez bien sûr vos rubriques habituelles et notre insert spécial cyber avec *L'InfoCR*. □

Bertrand Garé
Rédacteur en Chef

Votre réussite,
Notre engagement.

SQORUS
People and Solutions that matter

CONSEIL • IMPLEMENTATION • PILOTAGE •
DATA MANAGEMENT • BUSINESS INTELLIGENCE •
DEVOPS & INFRA • AMELIORATION CONTINUE

Un partenaire de confiance pour la modernisation des fonctions RH, Finance et IT.

- Une capacité à imaginer des solutions sur mesure et innovantes
- Un partenariat durable et créateur de valeurs
- Une expertise Métier et Technique

SQORUS est un cabinet de conseil spécialisé dans la transformation digitale des fonctions RH, Finance et IT. Avec une équipe de 300 consultants, experts métier et technique depuis plus de 30 ans, nous proposons aux ETI et grandes entreprises les talents et les solutions au service d'une excellence opérationnelle et d'une croissance continue.

www.sqorus.com

25 rue de Maubeuge 75009 Paris - Tél. +33 (0)1 44 54 26 36 - contact@sqorus.com

blue.

EN CYBERSÉCURITÉ, LES SUPER-POUVOIRS NE SONT PAS SUFFISANTS.

FAITES APPEL À NOS EXPERTS

www.bt-blue.com

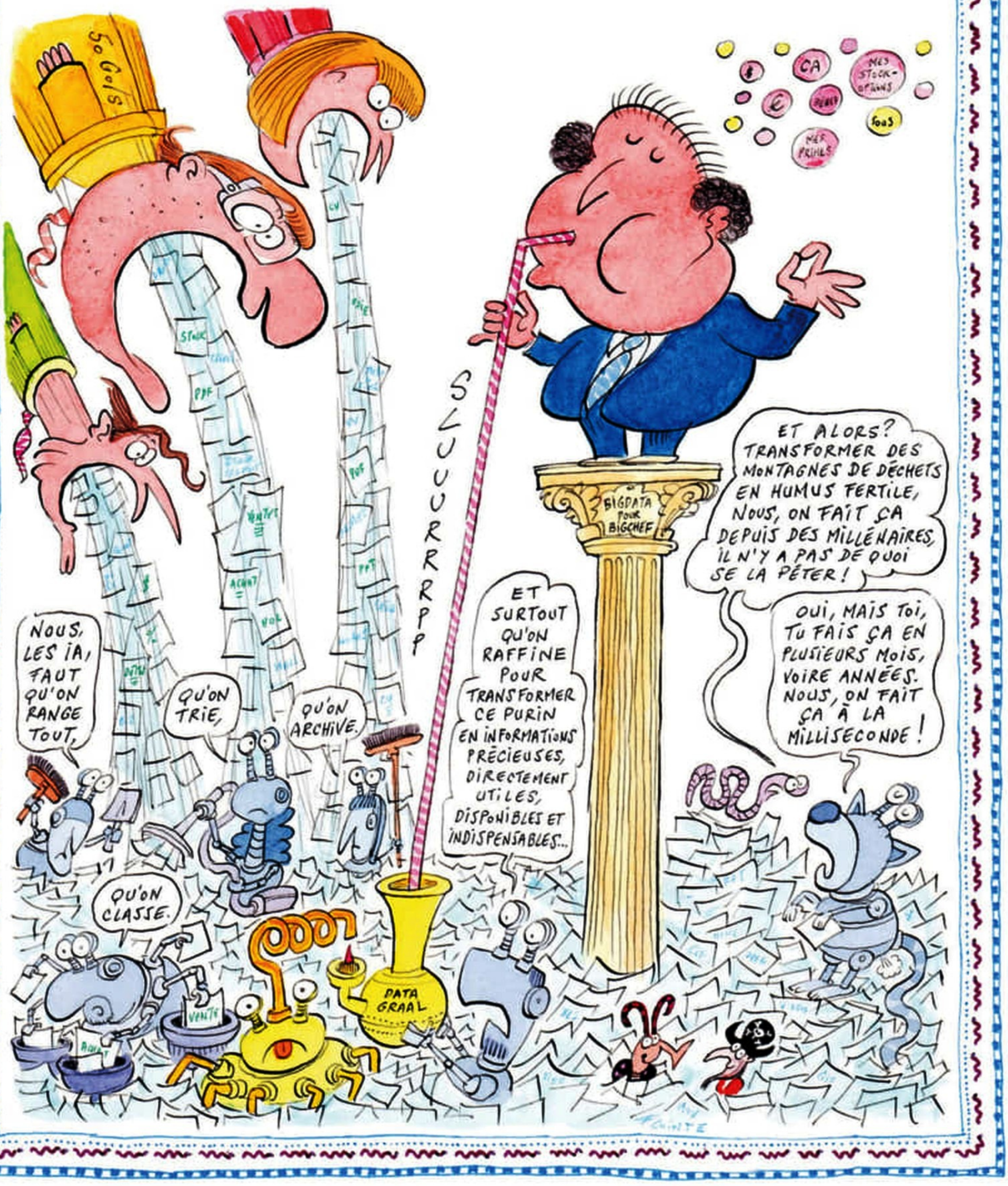
En partenariat :

vmware CLOUD VERIFIED

SentinelOne

IBM

LES AS DU STOCKAGE INTELLIGENT



FOCUS

Le **chahut continue** chez **Atos**

Valse des dirigeants et des administrateurs, projets de vente et de scission repoussés ou avortés, cours en bourse qui joue au yoyo... retour sur près de deux ans de rebondissements.

Tout commence en juin 2022, lorsque l'ESN révèle son plan : Atos sera séparé en deux entités, d'un côté Tech Foundations, qui regroupe le cœur historique des activités de la société, soit l'infogérance, le Digital Workspace et les services professionnels, de l'autre Eviden, Evidian à l'époque ou encore SpinCo, avec les activités les plus rentables du groupe : big data, transformation numérique et cybersécurité, soit l'essentiel de la branche BDS d'Atos. Alors que Thales attendait au tournant, prêt à s'emparer d'Eviden, l'ESN fait le choix d'Airbus, rejetant sèchement au passage une offre de Onepoint et du fonds d'investissements anglo-saxon ICG à 4,2 milliards. En février 2023, Atos annonce *« avoir reçu une offre indicative d'Airbus pour conclure un accord stratégique et technologique de long terme et acquérir une participation minoritaire de 29,9 % dans Evidian »*. Pourtant, dans les semaines qui suivent, on apprend par voie de presse que les discussions avec l'avionneur capotent. Fin mars, le couperet tombe, Airbus estimant que *« l'acquisition potentielle d'une part minoritaire de 29,9 % d'Evidian ne correspond pas aux objectifs de l'entreprise »*. Il semblerait bien que le géant de l'avion ait considéré la valorisation d'Eviden surévaluée, pour des résultats qui n'étaient pas à la hauteur des attentes. Pendant ce temps, l'ESN se sépare d'un certain nombre de branches, à l'instar de ses activités en Italie ou encore d'EcoAct à Schneider, tandis que la grogne monte chez les actionnaires, certains d'entre eux demandant, en juin, le départ du président du groupe, Bertrand Meunier, et la nomination de Léo Apotheker, ancien patron de HP et de SAP.

Daniel Kretínsky à la reprise

Soudain, le 1er août, nouveau rebondissement. Dans un communiqué, le Conseil d'administration d'Atos annonce avoir *« décidé d'entrer en négociations exclusives avec EP Equity Investment (EPEI) pour le projet de cession de 100 % de Tech Foundations, avec un impact positif net sur la trésorerie de 0,1 milliard d'euros et le transfert de 1,9 milliard d'euros d'engagements au bilan »*. EPEI est le bras armé du milliardaire tchèque Daniel Křetínský. Ni une, ni deux, les boucliers se lèvent. D'autant que René Proglio, administrateur et président du comité des comptes d'Atos était opposé à ce projet. Mais, au moment de la réunion du conseil d'administration le 31 juillet, il était en déplacement, révèle BFM Business. Les fonds Alix AM et CIAM, des actionnaires d'Atos, portent plainte devant le Parquet National Financier (PNF), le premier pour *« corruption active et passive »*, le second pour *« diffusion d'informations fausses ou trompeuses »*. Le monde politique et numérique est lui aussi en émoi, nombreux étant ceux s'inquiétant du projet de cession et des habilitations secret défense qui tomberaient dans les mains du milliardaire. Atos se rebiffe, reproche à ses actionnaires leurs sorties dans les médias. Et la valse commence. Fin septembre, Jean-Philippe Poirault, CEO de BDS, est remercié par Bertrand Meunier. Philippe Oliva, co-CEO en charge des activités devant constituer Eviden, le remplace au pied levé. Avant d'annoncer son départ d'Atos le 4 octobre, Yves Bernaert, ex-patron d'Accenture Technology Europe, lui succède en tant que directeur général d'Atos. Caroline Ruellan, administratrice indépendante depuis juillet 2022, démissionne elle aussi.

Enfin, lundi 16 octobre, le groupe annonce la démission de son président, Bertrand Meunier. Un départ demandé par certains des petits actionnaires du groupe. On apprend par la même occasion que René Proglio serait lui aussi sur le départ. Le conseil d'administration nomme alors *« avec effet immédiat »* Jean-Pierre Mustier, ancien banquier de la Société Générale, en tant que Président non-exécutif et de Laurent Collet-Billon, ex-DGA en tant que Vice-Président non-exécutif. Tous deux étaient administrateurs depuis mai dernier. Ces changements de gouvernance donnent quelques couleurs à Atos en bourse. Mais, quand bien même Jean-Pierre Mustier annonçait sa volonté de poursuivre la restructuration de l'ESN, décision a été prise de reporter la scission d'Atos et la vente à EPEI à, au moins, le deuxième trimestre 2024. Ni une ni deux, face aux incertitudes quant à l'opération et à son calendrier, l'action est repartie à la baisse. Et le feuilleton de continuer, au moins jusqu'au deuxième trimestre 2024.

Nvidia visité par l'Autorité de la concurrence

Nvidia a reçu une visite surprise des autorités. *« Les services d'instruction de l'Autorité de la concurrence ont procédé hier, après autorisation d'un juge des libertés et de la détention, à une opération de visite et saisie inopinée auprès d'une entreprise suspectée d'avoir mis en œuvre des pratiques anticoncurrentielles dans le secteur des cartes graphiques »*, a déclaré l'Autorité à la concurrence dans son communiqué, sans préciser que l'entreprise en question était Nvidia. *« L'Autorité de la concurrence ne fera aucun autre commentaire ni sur l'identité de l'entreprise visitée ni sur les pratiques visées »*. Peu de temps après, le magazine Challenges a révélé qu'il s'agissait du constructeur américain de cartes graphiques devenu le principal fournisseur de puces d'intelligence artificielle au monde. L'Autorité n'a pas non plus précisé sur quelle pratique elle enquêtait concernant Nvidia. Son enquête porte néanmoins plus globalement sur les sociétés de cloud computing et vise à déterminer si les plus gros fournisseurs n'utilisent par leurs accès privilégiés à une importante puissance de calcul pour entraver le développement de plus petits concurrents. Et Nvidia dans tout ça ? Avec l'avènement des systèmes d'IA générative, la demande de puces du fabricant a explosé, le propulsant comme leader incontesté avec 90 % des parts de marché dans le domaine des puces d'IA selon l'entreprise financière Citi. Ce qui a eu pour effet de placer les fournisseurs de Cloud dans une situation de dépendance vis-à-vis de Nvidia.

L'iPhone 12 rayonne et sa mise à jour tarde

La commercialisation de l'Phone 12 est suspendue en France depuis le 12 septembre 2023, dans l'attente de mesures correctives afin de réduire les émissions d'ondes de l'appareil pour donner suite à une étude de l'Agence nationale des fréquences (ANFR). En Europe, la réglementation exige qu'un smartphone tenu en main et dans la poche d'un pantalon (DAS membres), ou dans une poche de veste ou un sac (DAS tronc), respecte des valeurs limites de 4 W/kg pour le DAS « membre » et 2 W/kg pour le DAS « tronc ». Dans le cas de l'IPhone 12, l'ANFR a établi que la valeur de DAS « membre » dépassait la limite et atteignait 5,74 W/kg. Apple a profité de sa récente annonce pour donner une explication sur les écarts entre les résultats des calculs réalisés par l'ANFR et

ceux d'autres pays. La firme a indiqué que depuis plus de 10 ans, ses iPhones incluent des capteurs qui permettent au téléphone de détecter quand il se trouve à proximité du corps d'un utilisateur afin de maintenir une puissance de transmission à des niveaux inférieurs. Lorsque le téléphone n'est pas à proximité d'un corps, la puissance de transmission augmente légèrement. D'après la marque à la pomme, le protocole de test de l'ANFR ne prenait pas en compte cette fonctionnalité. La mise à jour, qui sera mise en ligne dans le courant du mois d'octobre, désactivera cet outil afin que les niveaux de puissance de transmission restent inférieurs à tout moment. Et d'ici là ? La firme a assuré que ses iPhone 12 peuvent être utilisés en toute sécurité, même sans la mise à jour logicielle. *« L'iPhone 12 a été certifié conforme aux réglementations et normes mondiales applicables en matière de transmission d'énergie lors de sa première expédition en 2020 et aucun changement n'a été apporté depuis lors. »*

Cloud : la CMA britannique enquête sur AWS et Azure

L'Autorité de la concurrence britannique (CMA) a lancé une enquête sur le marché local du cloud computing afin de déterminer si la domination d'Amazon et de Microsoft entraîne des risques pour la concurrence. Tous deux représentent 70 à 80 % du secteur du Cloud au Royaume-Uni selon l'Ofcom, l'organisme de surveillance des médias au Royaume-Uni. Un état de fait qui n'a pas manqué d'attirer l'attention de la CMA, qui a ouvert une enquête afin de déterminer s'il existe des problèmes de concurrence et, *« le cas échéant, quelles interventions peuvent améliorer l'offre de ces services importants »*, décrit-elle dans un communiqué. Dans son étude de marché, l'Ofcom a identifié certaines difficultés pour les clients à changer de fournisseur cloud, ou à en utiliser plusieurs. L'organisme s'inquiète notamment des frais de sortie pour les clients qui doivent payer pour le déplacement de leurs données vers d'autres emplacements. Ce sont aussi les remises qui incitent les clients à n'utiliser qu'un seul fournisseur, ou encore les obstacles techniques mis en place par les fournisseurs de cloud qui sont pointés. L'Autorité va chercher à déterminer si la concurrence sur ce marché fonctionne correctement ou si des mesures doivent être prises pour le réguler. Les conclusions de l'enquête sont attendues à horizon avril 2025.

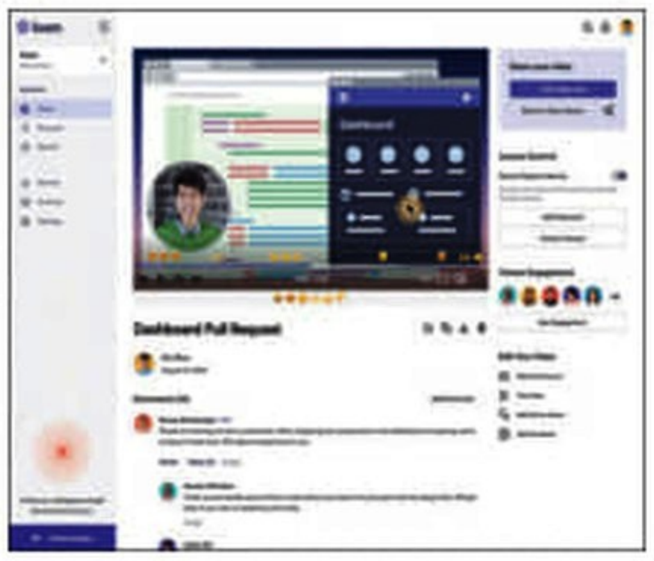
RACHATS

Qui pour **racheter** la cyber de **Risk&Co** ?

Risk&Co pourrait bien être démantelé. Depuis quelques années, l'Entreprise de Services de Sûreté et de Défense (ESSD), fondée et longtemps dirigé par un ancien du secrétariat général de la défense et de la sécurité nationale (SGDSN), Bruno Delamotte, est en proie aux difficultés financières. Elle a été contrainte, il y a plusieurs années, de se séparer de certaines activités et avait finalement été reprise par LGT Capital Partners en 2019. À l'époque, le fonds avait d'ailleurs damé le pion à Amarante, une autre ESSD, fondée quant à elle par deux anciens de la DGSE. Malgré le soutien de LGT, Risk&Co a été placé le 30 août 2023 en redressement judiciaire par le tribunal de Nanterre. Selon les Echos et la Lettre A, plusieurs entreprises sont sur les rangs pour s'emparer des activités en cybersécurité de ce groupe spécialisé dans la sûreté et l'intelligence économique. Si sa branche cyber ne pèse que quelques millions d'euros, ce sont surtout les contrats existants avec les services de l'Etat ou des grands comptes qui intéressent les potentiels repreneurs, en tête desquels on retrouve Orange CyberDefense. Foliateam, HeadMind Partners et ChapsVision font également partie des prétendants.

Atlassian s'offre **Loom**

Né en 2016, Loom est une plateforme de messagerie vidéo professionnelle, entendre par là qu'elle s'adresse avant tout aux entreprises et surtout celles ayant des bureaux sur différents fuseaux horaires. Sa spécialité, la vidéo asynchrone, soit la possibilité d'enregistrer un message vidéo qui sera visionné plus tard par le destinataire. Atlassian, éditeur de Jira, Trello, Confluence ou encore BitBucket, vient d'annoncer débourser 975 millions de dollars pour s'offrir la jeune pousse. 880 millions en cash, le reste en actions. La transaction devrait être finalisée au troisième trimestre de l'exercice 2024 d'Atlassian, sous réserve évidemment des conditions de clôture habituelles et de l'approbation réglementaire requise. Le géant du collaboratif est un client de longue date de Loom et explique utiliser sa solution comme *« outil de communication de référence »*. Intégrée aux différents logiciels d'Atlassian, la plateforme de messagerie vidéo *« améliorera encore l'expérience de collaboration des équipes »* : *« bientôt, les ingénieurs pourront enregistrer visuellement les problèmes dans Jira ; les dirigeants peuvent utiliser des vidéos pour communiquer avec les employés à grande échelle ; les équipes commerciales peuvent envoyer des mises à jour vidéo personnalisées aux clients et les équipes RH peuvent intégrer les nouveaux employés avec des vidéos de bienvenue personnalisées »* écrit Atlassian.



Owlint rejoint **ChapsVision**

À peine une semaine après avoir annoncé une levée de 90 millions d'euros, ChapsVision effectue un nouveau rachat. L'entreprise s'empare d'Owlint dont elle annonce le rachat, pour un montant non divulgué. Cette startup fondée en 2018 a tranquillement fait son nid dans le domaine de l'évaluation de l'exposition aux risques cyber, procédant principalement par des analyses en sources ouvertes, OSINT pour les intimes. Or, l'OSINT doit devenir l'une des cordes à l'arc de ChapsVision, à en croire son communiqué. *« ChapsVision souhaite devenir un acteur important dans ce domaine. Depuis deux ans, le groupe avait d'ailleurs progressivement déjà enrichi son portefeuille d'offres avec les solutions d'intelligence économique et stratégique telles qu'AMI EI, Qwam et Geotrend »* écrit la société.

AMD fait ses emplettes **dans l'IA**

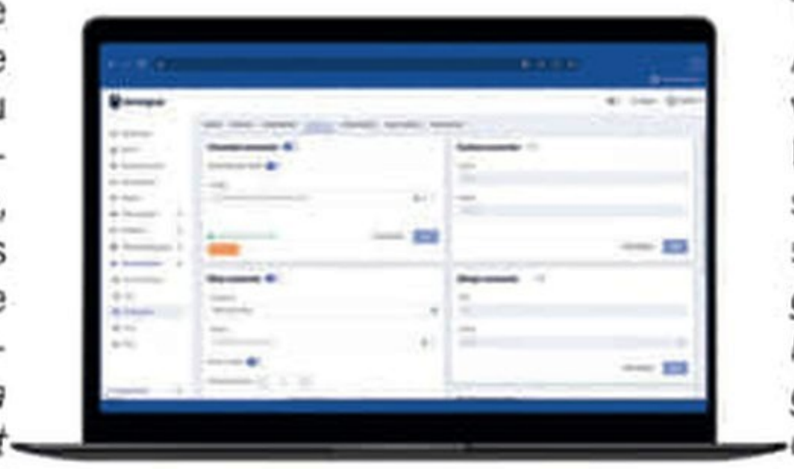
Le fabricant de semi-conducteurs, AMD, a annoncé, mardi 10 octobre, l'acquisition de Nod.ai, une startup spécialisée dans les logiciels d'IA open source et l'optimisation des modèles d'IA. *« L'acquisition de Nod.ai devrait améliorer considérablement notre capacité à fournir aux clients de l'IA un logiciel ouvert leur permettant de déployer facilement des modèles d'IA hautement performants adaptés au matériel AMD »*, a déclaré Vamsi Boppana, vice-président senior du groupe d'intelligence artificielle chez AMD, cité dans un communiqué. L'acquisition s'inscrit dans la logique de croissance d'AMD centrée, en matière d'IA, sur un écosystème logiciel ouvert qui doit abaisser les barrières à l'entrée pour les clients en fournissant des outils de développement et des bibliothèques de modèles. Nod.ai a déjà développé une technologie logicielle qui accélère le déploiement de solutions d'IA optimisées pour les accélérateurs de centres de données AMD Instinct, les processeurs Ryzen AI, les processeurs EPYC, les SoC Versal et les GPU Radeon. AMD espère boucler l'acquisition dès ce trimestre.

NANO Corp remet le couvert

NANO Corp est née en 2019 à Paris, fondée par d'anciens du ministère des Armées. Positionnée dans le NDR, la startup a développé sa propre sonde réseau et a breveté la technologie sous-jacente. En 2021, elle levait 1,6 million d'euros auprès du fonds Elaia Partners. NANO Corp a annoncé remettre le couvert. Cette fois-ci, c'est le fonds allemand G+D Ventures qui est à la manœuvre, rejoint par Cyber K1 et d'Inovia Capital Precede Fund I. Elaia Partners a lui aussi remis au pot. Levant lors de ce tour en seed 4,2 millions d'euros, la jeune pousse de 16 personnes entend étendre la commercialisation de sa solution NDR en Europe. *« Cette levée de fonds représente plus qu'un simple capital. Elle valide la vision de NANO Corp et le potentiel de notre technologie à révolutionner la sécurité numérique à l'échelle mondiale »* ajoute Fanch Francis, CEO de la société. *« Alors que nous visons des horizons plus larges que la France, nous sommes profondément reconnaissants à nos investisseurs d'avoir compris le potentiel de transformation de NANO Corp »*.

25 millions d'euros pour HarfangLab

L'EDR tricolore HarfangLab annonce une levée de fonds de Série A, menée par Crédit Mutuel Innovation, au terme de laquelle elle encaisse 25 millions d'euros. L'investisseur historique, Elaia, a lui aussi mis au pot, deux ans après avoir mené la première levée de fonds de la jeune pousse, de 5 millions d'euros en 2021. *« À l'époque, la levée avait permis d'investir surtout dans la recherche et le développement de l'EDR »* explique HarfangLab dans son communiqué. Depuis, l'entreprise a bien grandi : avec plus de 250 clients et 800 000 postes de travail et serveurs protégés, elle affiche 250 % de croissance de ses revenus sur l'année 2022 et vise les 10 millions d'euros de chiffre d'affaires. Avec cet argent frais, la jeune société veut accélérer son développement en Europe et continuer d'investir dans sa R&D, en se concentrant sur trois secteurs porteurs que sont *« l'intelligence artificielle, l'automatisation de la détection et la cyber threat intelligence »*. En outre, *« HarfangLab va également accélérer les recrutements et les investissements pour développer son réseau de partenaires, décupler sa force de vente et diversifier ses compétences et activités »*.



Data4 emprunte 2,2 milliards d'euros

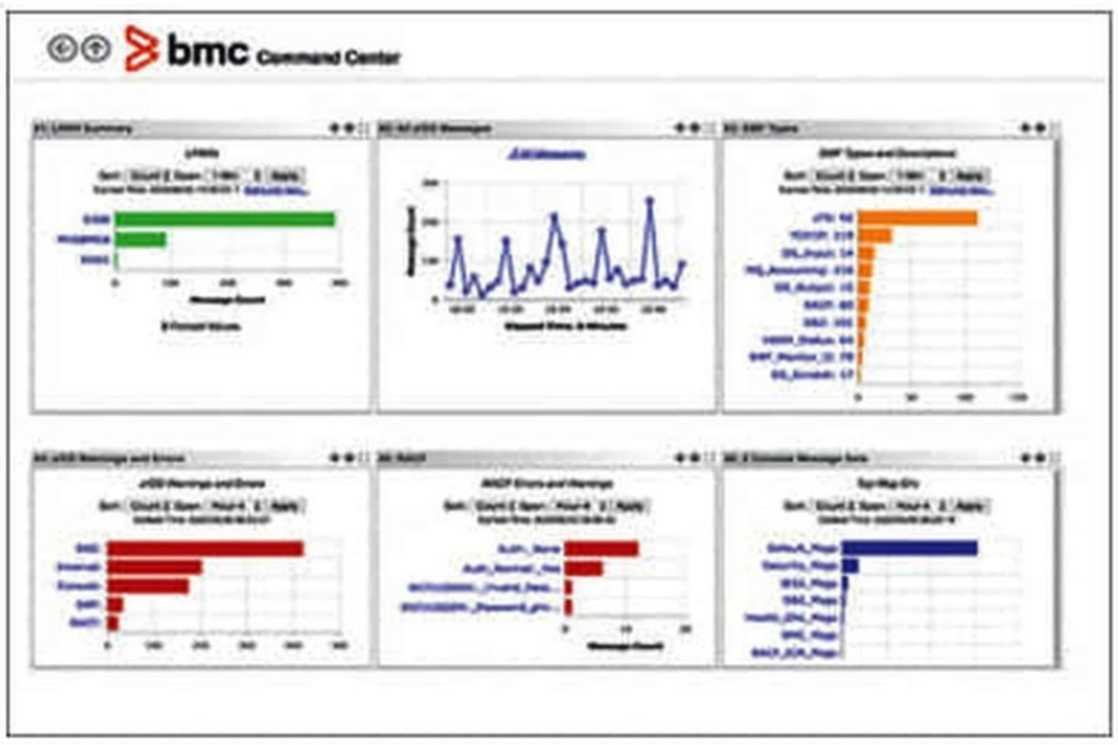
Le Français Data4, récemment tombé dans le giron du Canadien Brookfield Infrastructure, poursuit sa stratégie d'investissement. D'ici à fin 2029, l'opérateur compte allouer 2 milliards d'euros à ses campus en France, un milliard d'euros en Allemagne, un milliard en Italie et plus de 500 millions en Espagne ainsi qu'en Pologne. En 2021, Data4 empruntait de 620 millions d'euros auprès de trois banques, Deutsche Bank, Société Générale et Sumitomo Mitsui Banking Corp. Le groupe visait désormais un chiffre d'affaires doublé d'ici à 2024, soit 200 millions d'euros. Désormais, la société voit plus grand, annonçant un nouvel emprunt, à hauteur de 2,2 milliards d'euros, extensible jusqu'à 3,2 milliards, auprès de BNP Paribas, Natixis, ABN AMRO et Deutsche Bank. 1,2 milliard d'euros vont au refinancement de la dette existante, quant au milliard restant, il sera dédié à l'acquisition de nouveaux sites et à la construction de futurs datacenters. L'entreprise a annoncé ces derniers mois l'acquisition du site de Grossauheim en Allemagne et du siège de Nokia, situé dans l'Essonne, lequel accueillera à terme 8 datacenters.

Keysight et Synopsys collaborent sur la sécurité de l'IoT

Les deux éditeurs deviennent partenaires pour fournir aux fabricants d'appareils de l'Internet des objets (IoT) une solution complète d'évaluation de la cybersécurité.

Dans le cadre de cet accord, l'outil de fuzzing Defensics de Synopsys sera intégré en option dans la solution d'évaluation de la sécurité de l'IoT de Keysight. Avec l'ajout de Defensics à l'évaluation de la sécurité de l'IoT de Keysight, les utilisateurs disposent désormais d'une solution qui combine des évaluations de vulnérabilités connues avec un fuzzer polyvalent capable d'analyser plus de 300 protocoles technologiques différents utilisés dans divers secteurs d'activité pour tester rapidement les vulnérabilités et les faiblesses inconnues. En plus de signaler les failles de sécurité découvertes grâce au fuzzing, la solution détecte les exploits potentiels résultant d'une authentification et d'un chiffrement faibles, de certificats expirés, de vulnérabilités Android et d'expositions à Android Debug Bridge (ADB), de vulnérabilités et d'expositions communes (CVE) connues et de failles intégrées dans les piles de protocoles, telles que les attaques Bluetooth Low Energy comme SweynTooth et BrakTooth.

De plus, la solution Keysight IoT Security Assessment permet aux fabricants de tester facilement et à moindre coût les appareils IoT dès maintenant et d'obtenir la nouvelle certification White House Cyber Trust Mark lorsqu'elle sera lancée. Cette plateforme de certification de cybersécurité clé en main permet une validation automatisée via une interface de type pointer-cliquer, ce qui permet aux fabricants d'appareils de mettre rapidement sur le marché de nouveaux produits IoT.



Infotel collabore avec BMC

Les deux entreprises se rapprochent afin de combiner leurs expertises et proposer des solutions logicielles et de sécurité mainframe. Dans le cadre de l'accord de revente récemment signé, Infotel améliorera son offre en intégrant les produits BMC AMI Security aux côtés de ses solutions logicielles et de services mainframe.

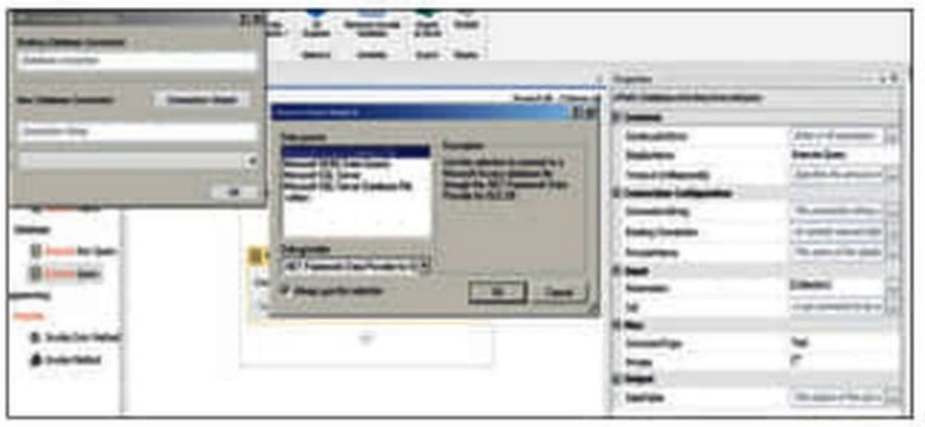
OVHcloud et Console Connect partenaires au niveau mondial

Le fournisseur de services en nuage se rapproche de Console Connect, un fournisseur de services réseau, pour ses solutions de connectivité.

Cette collaboration a pour but de proposer des solutions de connectivité plus flexibles et sécurisées pour accéder à OVHcloud. Les entreprises auront la possibilité de provisionner elles-mêmes des connexions privées vers et entre les centres de données d'OVHcloud dans le monde entier via un portail de gestion ou via une API. Contrairement à d'autres plateformes NaaS, Console Connect fournit une connectivité de niveau 2 et de niveau 3 à OVHcloud en utilisant un réseau privé à hautes performances, qui comprend un réseau Tier 1 de câbles sous-marins redondant et résilient.
La plateforme permet d'interconnecter directement sur les sites distants (Immeubles et bureau en intégrant la boucle locale dans 10 pays). Également disponible directement dans plus de 950 centres de données répartis dans 60 pays. Grâce à la nouvelle solution Edge SIM de Console Connect, les entreprises peuvent également sécuriser le trafic entre les appareils de l'Internet of Things (IoT) et OVHcloud sans utiliser l'Internet public. Le réseau sous-jacent de Console Connect offre également des SLA stricts et peut aider les entreprises à améliorer la résilience et la redondance de leur architecture réseau. En utilisant CloudRouter, la solution de connectivité multicloud de Console Connect, les entreprises peuvent en outre se connecter de manière transparente entre OVHcloud et d'autres partenaires cloud de premier plan, dont AWS, Google Cloud, IBM Cloud, Microsoft Azure, Oracle Cloud, StackPath, Vultr ou bien se connecter entre plusieurs régions d'OVHcloud.
La plateforme Console est entièrement intégrée à OVHcloud et offre aujourd'hui des interconnexions vers le centre de données d'OVHcloud en France. Dans les semaines à venir, d'autres centres de données d'OVHcloud seront ajoutés à la plateforme, notamment des sites en Allemagne, au Royaume-Uni, au Canada, aux États-Unis et à Singapour.
L'étendue du réseau de la plateforme Console Connect soutiendra le déploiement mondial d'OVHcloud, le fournisseur de cloud devant ouvrir 15 nouveaux centres de données d'ici 2024.

UiPath et Teradata s'associent

Le fournisseur de solutions d'automatisation et l'éditeur de solutions analytiques nouent un partenariat pour aider les entreprises à automatiser en toute transparence et en toute sécurité des applications de données complexes directement à la source — des tableaux de bord à l'IA générative en passant par les grands modèles de langage (LLM).



Les deux entreprises voient une opportunité du fait de leur positionnement respectif pour générer un impact positif en aidant leurs clients à concrétiser leurs ambitions ESG grâce à une meilleure harmonisation des données à l'échelle de l'entreprise. Les clients d'UiPath pourront ainsi bénéficier de l'expertise de Teradata pour permettre à leur entreprise d'activer et d'exploiter leurs données et les analyses qui en découlent. UiPath fournira aux entreprises une plateforme complète dédiée à la mise en œuvre et à l'exploitation des processus d'automatisation alimentés par l'IA. L'intégration des données présentes dans Teradata dans un workflow automatisé grâce à UiPath Database Activities, permet d'utiliser les données Teradata dans des processus multi-systèmes. Les activités fonctionnent par « glisser-déposer » et ne nécessitent pas l'écriture d'un code complexe ; cela signifie que tout utilisateur peut désormais lancer le processus d'automatisation dans le cadre de la maintenance des données, des tests continus et des activités liées à l'administration.

Après la collecte des données dans les différents systèmes, il est ensuite possible de traiter les données structurées et non structurées puis de les stocker dans la plateforme de Teradata. La solution est immédiatement disponible.

Naitways et Scality partenaires

Le fournisseur de services cloud et l'éditeur de solutions de stockage objet se rapprochent pour proposer une offre à destination des PME et ETI.

L'opérateur français propose désormais à ses clients et prospects de bénéficier de la solution RING 9 pour leurs besoins en matière de stockage objet. Par un hébergement en France, réparti sur 3 centres de données à Paris et à Lyon, cette offre répond aux structures désireuses de plus de résilience, de voir leurs données stockées sur le territoire et de bénéficier d'un accompagnement personnalisé et sur-mesure. Déjà partenaire VEEAM, Naitways, en ajoutant RING à son catalogue d'offres, propose désormais à ses clients et prospects un éventail de possibilités de stockage répondant à tout type de besoins et d'environnements de SI. En outre, les experts de Naitways leur offrent également l'opportunité d'assurer la résilience de leur entreprise, en cas de panne ou d'incident, en élaborant un plan de sauvegarde et de reprise d'activité (PRA).

Colt étend sa présence en France

En partenariat avec Eurofiber, le fournisseur de services de connectivité va ajouter de nouveaux réseaux métropolitains (MAN) à Bordeaux, à Lille et à Toulouse, ainsi que d'étendre le réseau métropolitain de Colt aux Pays-Bas et en Belgique.

Reposant sur la solution Hybrid on Net de Colt, qui permet de bénéficier des avantages d'une connexion en fibre optique dédiée, sans avoir à supporter les coûts et la complexité liés à la mise en œuvre de l'infrastructure réseau, le fournisseur de solutions réseau va exploiter la fibre noire passive de fournisseurs de réseaux métropolitains. Ce nouveau partenariat formalise et étend la relation existante entre les deux entreprises, qui a débuté en 2010.

AGENDA

VMware Explore
6-9 novembre 2023
Fira Gran Via, Barcelone, Espagne

Web summit
13-16 novembre 2023
Altice Arena & Fil, Lisbonne, Portugal

Microsoft Ignite
14-17 novembre 2023
Seattle Convention Center, Seattle, USA

Big Data Paris
15-16 novembre 2023
Palais des Expositions, Porte de Versailles, Paris

Tech Show
15-16 novembre 2023
Palais des Expositions, Porte de Versailles, Paris

AWS re:Invent
27 novembre - 1er décembre 2023
Venetian Resort Hotels, Las Vegas, Nevada USA

SIDO Paris
6-7 décembre 2023
Palais des Congrès, Porte Maillot, Paris

CES
9-12 janvier 2024
Multiples localisations, Las Vegas USA

BACK UP AND KEEP CALM

Operate

Secure

Protect

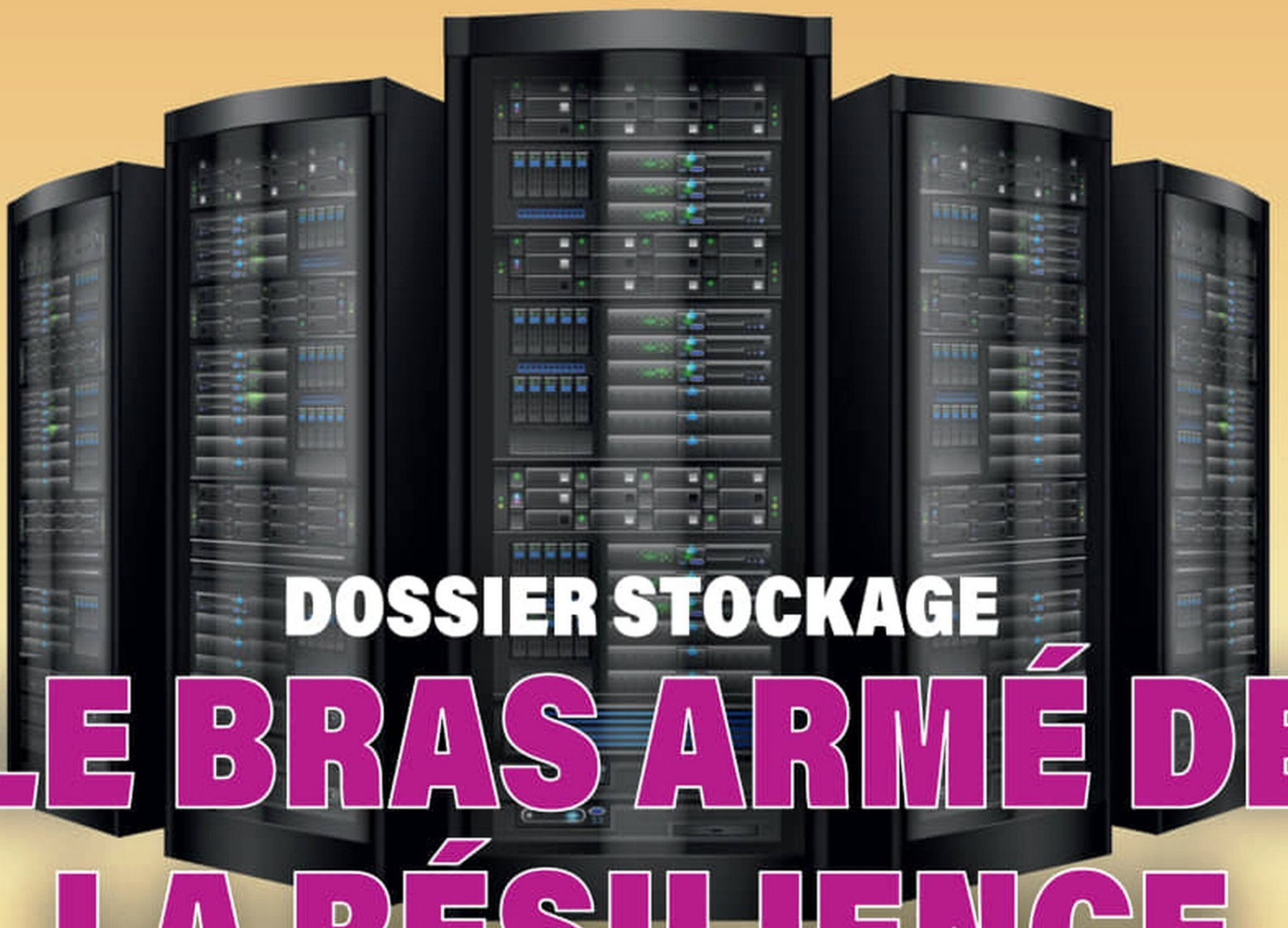
Leader français de la protection des données

ANTEMETA

AntemetA accompagne les directions dans la sanctuarisation et l'évolution de leur Système d'Information.

AntemetA, tiers de confiance, assure le plan de reprise d'activité en cas de cyberattaque par la mise en œuvre en amont de solutions d'infrastructure, la fourniture de services Cloud et une expertise des services managés.

Contact
www.antemeta.fr
+33 1 85 40 03 36



DOSSIER STOCKAGE

LE BRAS ARMÉ DE LA RÉSILIENCE

Face à un contexte incertain et mouvant, les entreprises se doivent de se doter des outils pour faire face à de nombreux défis : attaques, croissance du volume des données, etc. Souvent noyé dans l'infrastructure, le stockage retrouve son lustre pour devenir un élément stratégique dans le but de passer tous les caps et assurer la résilience de l'activité de l'entreprise. Afin de faire face, le domaine innove beaucoup et rapidement. Avec un marché estimé à 16, 8 Mds $ par le cabinet Gartner, le stockage primaire reste un poste important dans les entreprises. Les prix sont soutenus par l'innovation qu'embarquent les équipements de stockage : disques flash de dernière génération, nouveautés logicielles avec l'introduction de l'intelligence artificielle. Du côté des vendeurs, les offres se déclinent de plus en plus sous forme de services et s'appuient sur le Cloud.

Dans ce dossier, nous ferons un aparté sur les outils de stockage plus personnels qui peuvent s'avérer utiles dans un contexte professionnel, comme les disques externes ou les clés USB. Ensuite, nous explorerons les pistes pour un stockage du futur et les alternatives au stockage des données tel qu'on le connaît aujourd'hui.

Dossier réalisé par Bertrand Garé

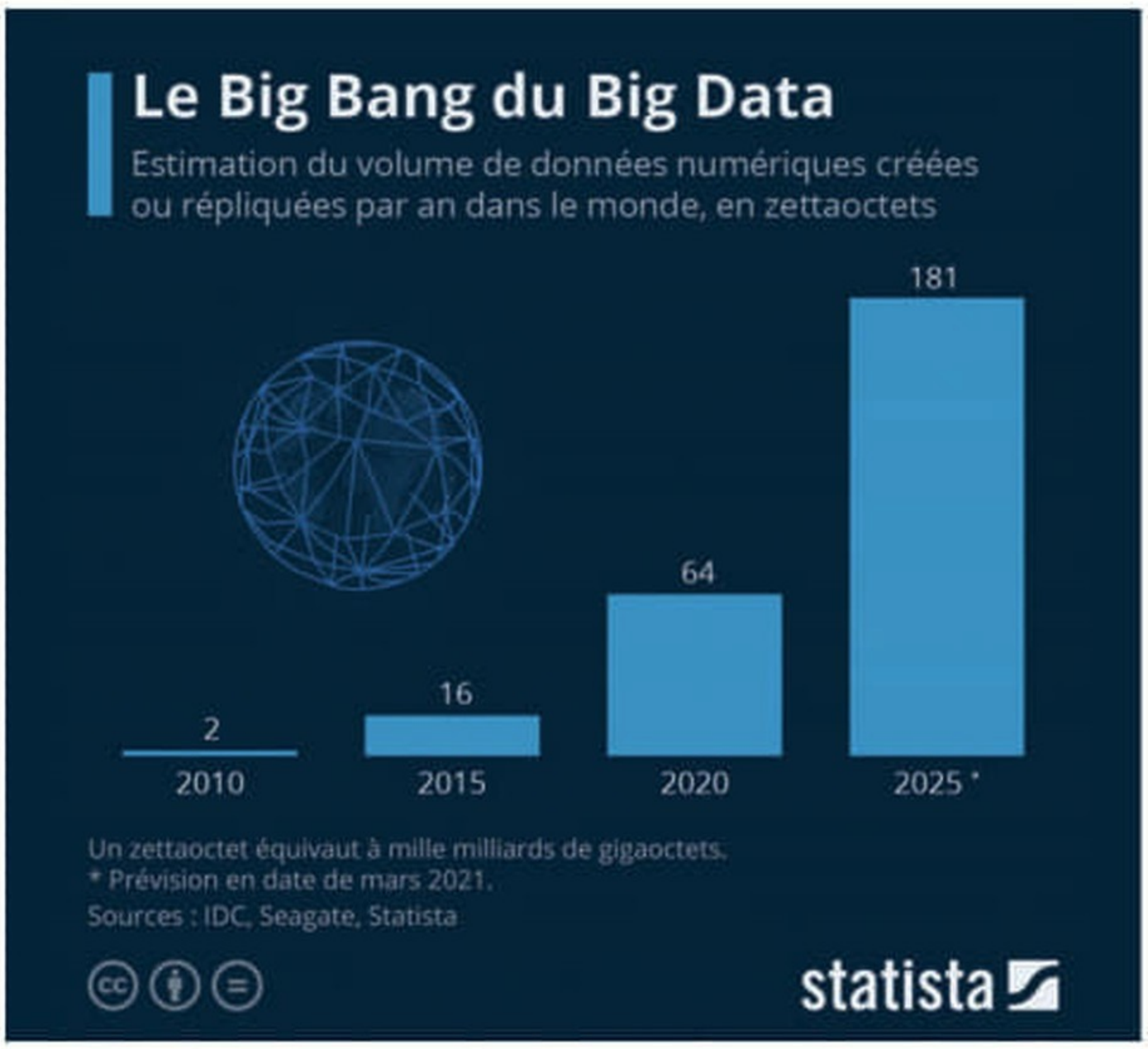
Une évolution **vers le service**

Le marché du stockage primaire innove et évolue rapidement vers un type de stockage en tant que service proposant un modèle de facturation à la consommation effective afin d'aligner les coûts et les besoins des entreprises.

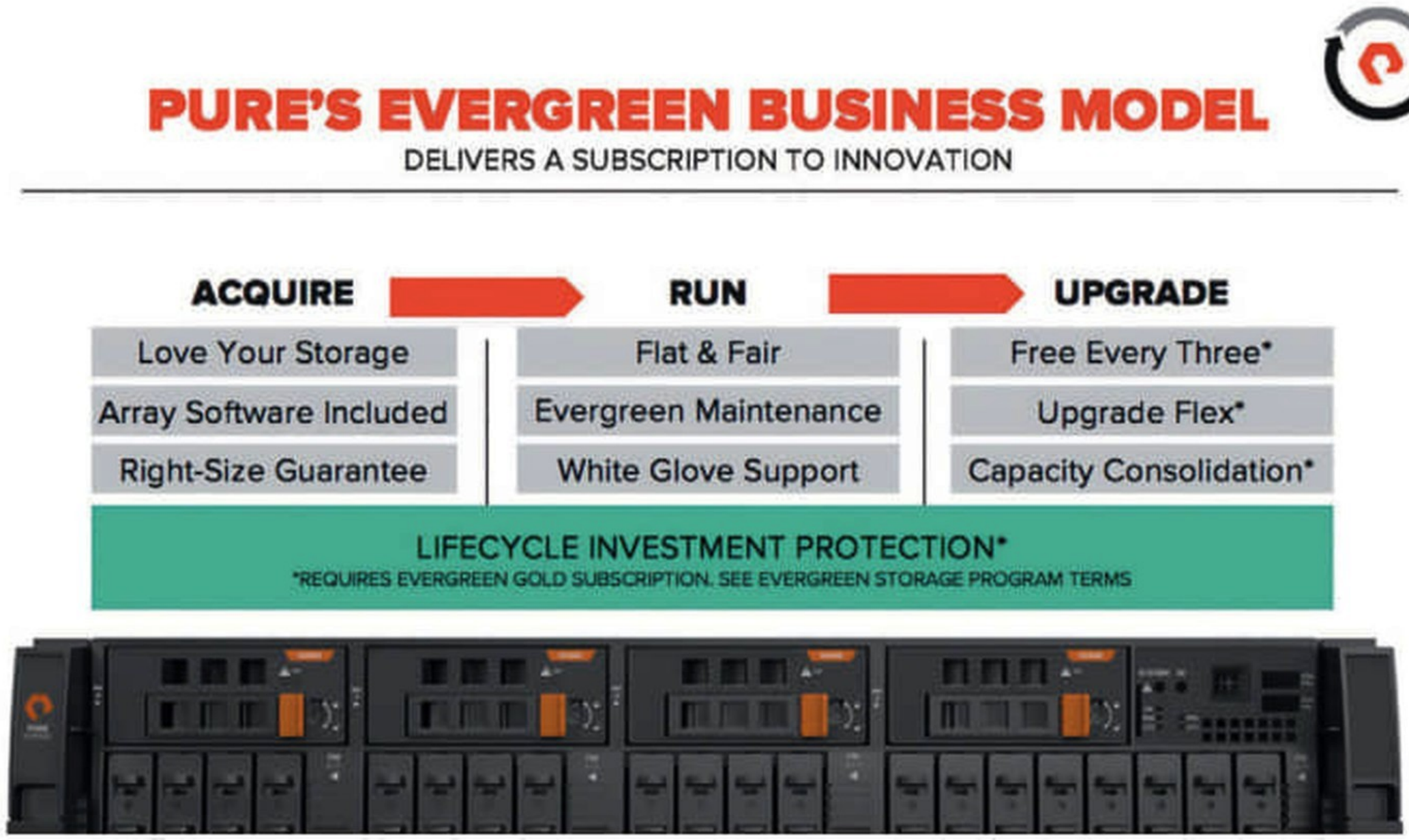
Avec un marché évalué à 16,8 Mds de dollars en 2022, le stockage reste un pan important dans les infrastructures des entreprises. Le cabinet Gartner définit ce marché comme l'ensemble des offreurs proposant des produits dédiés ou des services qui regroupent des capacités de stockage pour présenter des LUN (Logical Unit Number) à des applications par des protocoles d'interfaces blocs comme Fibre Channel ou iSCSI (Internet Small Computer System Interface). Cela se complète par des fonctions de haute disponibilité et de protection des données.

Des besoins de performance

Le stockage primaire est principalement dédié au support d'applications critiques et aux larges bases de données. Il est aussi en appui d'environnements de postes de travail virtualisés ou la persistance d'environnements de containers... Pour y parvenir, le stockage doit répondre à différents enjeux autour de la performance et de la tenue à l'échelle. Le volume des données dans les entreprises croît rapidement. Selon Statista, le volume des données générées dans le monde devrait dépasser 180 zettaoctets à l'horizon 2025, une augmentation de 40 % en moins d'un lustre. Il est communément admis que le volume des données en entreprise double tous les 2 ans. Les baies du moment répondent donc à la fois à la nécessité d'ingérer et de restituer les données rapidement en cas de sinistre avec des capacités de plus en plus grandes. Les dernières évolutions FlashArray//X et FlashArray//C R4 de Pure Storage sont un exemple de ces évolutions. Ces nouveaux modèles délivrent des performances jusqu'à 40 % plus élevées, accélèrent les capacités de mémoire de plus de 80 % pour mieux consolider les charges de travail et offrent une compression en ligne de 30 % pour étendre davantage la capacité de stockage. Optimisés par la technologie PCIe Gen4, par le dernier chipset Intel Xeon et par une mémoire DRAM DDR5, les modèles FlashArray//X et FlashArray//C offrent, de plus, la puissance pour prendre en charge de plus grandes charges de travail avec jusqu'à 74 % d'économies sur leur coût total de possession. Pour la capacité, les FlashArray//C intégreront la prochaine version de modules QLC DirectFlash de 75 To avec RAM non volatile intégrée (DFMD). La version FlashArray//X sera, quant à elle, équipée de DFMD TLC de 36 To. Ces DFMD offrent 1,5 Po pour 3 unités de rack, soit une amélioration de 106 % en termes de densité par unité de stockage. Les DFMD, introduits pour la première fois avec FlashArray//XL, réduisent l'espace de stockage nécessaire et permettent d'augmenter encore en capacité, tout en supportant de meilleurs débits de NVRAM. La technologie DirectFlash offre une



Croissance du volume des données selon Statista.



Le business model d'Evergreen de Pure Storage.

fiabilité 20 fois supérieure et un rendement énergétique plus de 4 fois supérieur à celui des baies 100 % flash à base de SSD. D'autres acteurs comme NetApp développent des matériels similaires avec une nouvelle famille de baies Flash ASA.

Pour sa part, Dell a amélioré les performances de sa solution Powerstore à destination du middle market jusqu'à 58 % pour gérer les charges de travail en constante augmentation. Infinidat a été distingué pour sa solution InfiniBox par le cabinet GigaOm en privilégiant la capacité avec sa solution rack-scale pouvant monter à 17 Po de capacité de stockage effective en un seul rack et une très faible latence de 35 microsecondes, avec InfiniBox SSA II.

Pour sa part, Arcitecta combine sa solution Scale ZFS avec Mediaflux pour autoriser une mise à l'échelle rapide de la performance et de la capacité de stockage. Cette intégration de ZFS contourne le principal problème de mise à l'échelle des traditionnelles solutions scale-up sur ZFS et permet une réduction des coûts.

Une poussée vers le StaaS

Devant les défis qui attendent les entreprises avec leur stockage, quasiment tous les offreurs proposent la possibilité de se tourner vers un modèle de service et une facturation à la consommation. Ainsi, le Gartner prévoit qu'en 2026, les plateformes avec un paiement à la consommation et des niveaux de services garantis vont remplacer la moitié des modes de stockage traditionnels sur site, alors qu'actuellement, le taux est de 10 %. Le même cabinet estime que les dépenses en infrastructure de stockage sur site seront à moins de 30 % dans les entreprises connaissant une décroissance spectaculaire des 85 % actuels. En 2028, le STaaS se substituera à 35 % aux dépenses en capital en plus que triplant sa place actuelle (10 %). En optant pour des solutions STaaS, les entreprises cherchent à obtenir des résultats basés sur les accords sur les niveaux de service (SLA) qui optimisent non seulement les budgets et les dépenses informatiques, mais aussi le travail tout en favorisant la réalisation des objectifs de sécurité, de développement durable et d'agilité.

Pure Storage s'est lancé très tôt sur ce créneau avec son offre Evergreen en 2015. Récemment, Pure Storage a étendu son offre de services en proposant une technologie efficace du point de vue énergétique sur le marché, et en aidant ses clients à réduire leur consommation énergétique et leurs émissions de carbone jusqu'à 85 %, ainsi que leur espace rack jusqu'à 95 % par rapport aux offres de la concurrence.

Une étude réalisée pour le compte de Stordata et NetApp indique que 91 % des décideurs IT français sont convaincus qu'une meilleure gestion du stockage des données est susceptible d'avoir un impact important sur la réduction des émissions carbone. 86 % sont conscients que le stockage excessif de données contribue à accroître de manière significative l'empreinte carbone de leur entreprise et 39 % soulignent un besoin d'investissement dans une infrastructure informatique plus efficace et durable.

Pour être complet, le recours au Cloud s'accélère et les dépenses dans ce type de stockage dépassent maintenant celles sur site. Cela s'explique principalement par un recours au SaaS de plus en plus fréquent et la volonté des entreprises d'accélérer dans leur transformation numérique qui s'appuie sur les offres d'infrastructure des hyperscalers, et en particulier leur service de stockage en ligne. □

Des **tendances technologiques** qui s'affirment

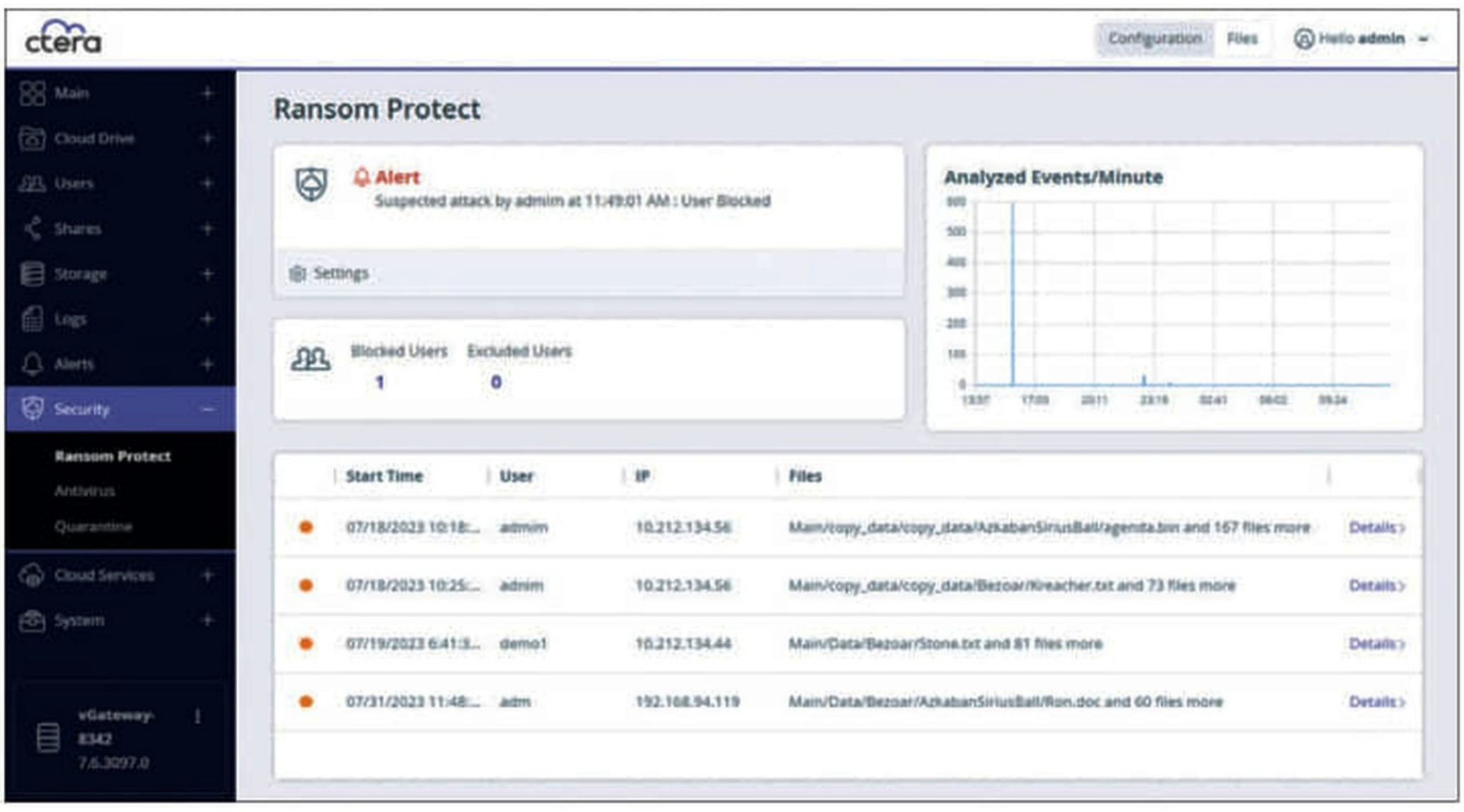
Avec la transformation numérique, les besoins des entreprises changent. Les besoins en faible latence, performance à l'échelle et consistance des environnements de stockage sont au centre des demandes. Un autre axe émerge, particulièrement dans notre pays, avec la recherche de solutions de stockage plus durables.

Premier axe technologique remarquable dans le secteur du stockage, les disques flash se généralisent. Si Pure Storage assure que les disques classiques ne seront plus vendus ou achetés vers 2028, il n'en reste pas moins que les disques durs classiques font de la résistance et augmentent en capacité.

Pour des raisons de coûts, les principaux constructeurs se rallient aux disques QLC. Si le prix de ceux-ci est encore supérieur à celui des HDD, il devra devenir quasiment équivalent dès 2026, soit 15 $/ To selon une prévision de Wikibon. Après HPE, NetApp et Pure Storage, c'est DDN qui s'est converti en mai dernier aux disques QLC pour des baies hybrides qui combinent le système de fichier parallèle de DDN avec une nouvelle solution de compression côté client. Selon les constructeurs, la solution augmente la performance d'un facteur 10, la capacité effective d'un facteur 15 et réduit l'empreinte dans le centre de données de moitié. Le tout dans un format 2U pour une capacité effective de 4,7 Po à 11,7 Po avec un taux de compression (conservateur) de 2. Ces baies ont été disponibles au cours du 3ème trimestre.

Une convergence avec la sécurité

Pour renforcer la résilience, les solutions de stockage embarquent de plus en plus des fonctions qui étaient auparavant dévolues à la sécurité pour la protection des données.



Un écran de la solution de protection contre les ransomwares de CTera.

La baie DDN-AI400X2
qui s'appuie sur des disques QLC.

Ainsi, CTERA a dévoilé CTERA Ransom Protect, un nouveau moteur de cyber protection à base d'IA intégrée en natif dans le système de fichiers global de CTERA. Des capteurs d'activité intégrés au système de fichiers alimentent un algorithme d'apprentissage automatique avancé, formé sur un vaste ensemble de données de flux d'attaques. Grâce à ces capteurs, CTERA Ransom Protect est capable de détecter et de bloquer les attaques en quelques secondes, et fournit des outils pour une atténuation immédiate et une récupération instantanée. Pour sa part, NetApp offre désormais une garantie permettant aux entreprises de se rétablir après des attaques ransomware. La garantie de récupération ransomware NetApp tire parti de la combinaison unique et exclusive de NetApp ONTAP de fonctions de sécurité intégrées et de protection contre les ransomwares. Rappelons qu'ONTAP peut bloquer automatiquement les types de fichiers malveillants connus, bloquer les administrateurs indésirables et les utilisateurs mal intentionnés grâce à la vérification multi-administrateurs. Il peut également fournir des snapshots inviolables qui ne peuvent pas être supprimés, même par l'administrateur de stockage.

Dans sa version 10, Zerto surveille et analyse les flux de données entrantes, détecte toute activité anormale en quelques minutes et édite des rapports. Sa puissante capacité de diagnostic est capable d'alerter sur une potentielle attaque ransomware à son stade le plus précoce et de déterminer à quel moment exactement cette dernière a été lancée. Les données pourront ainsi être recouvrées à un point de contrôle de récupération quelques secondes avant la livraison de la charge utile par le cybercriminel. Ajoutant une couche de sécurité additionnelle au système d'alerting temps réel, le nouvel environnement isolé Zerto Cyber Resilience Vault offre aux entreprises la capacité de concevoir et de personnaliser un coffre-fort de récupération de données éprouvé.

Fujitsu a lancé en avril dernier une nouvelle architecture de référence CS800 RA dédiée aux PME qui souhaitent se prémunir des attaques de ransomwares grâce à la réplication de données, au chiffrement et aux snapshots sécurisés. Ces fonctions sont associées à de puissantes capacités de déduplication qui permettent de réduire les besoins de stockage jusqu'à 95 %.

L'architecture de référence Fujitsu CS800 RA a été pensée pour que son approche multicouche intègre la protection des données dès la conception. Les sauvegardes étant aujourd'hui l'une des cibles privilégiées pour les cybercriminels, cette nouvelle architecture de référence fait désormais partie des solutions complètes de Fujitsu pour la sauvegarde et l'archivage des données, pour les bases de données stockées dans le cloud et sur support, mais aussi pour la reprise des activités après sinistre.

Dell est dans la même mouvance avec l'introduction de la réplication synchrone native sur PowerStore qui offre des opérations actives/actives sans interruption, éliminant ainsi le risque de perte de données en cas de panne de site ou de catastrophe naturelle. Un service de témoin agit comme une entité impartiale, vérifiant de manière autonome l'état de deux sites sur un réseau métropolitain et utilise son intelligence pour déclencher une bascule automatique vers la baie survivante en cas de défaillance.

L'IA s'installe dans les baies

Si les constructeurs et éditeurs de solutions de stockage utilisaient depuis déjà un certain temps des fonctions d'apprentissage machine et d'intelligence artificielle, celle-ci se fait actuellement une place plus marquante. Dans les baies PowerMax de dernière génération, des fonctions AiOps de CloudIQ apportent de nouvelles optimisations opérationnelles, énergétiques et de sécurité pour fournir des prévisions, des notifications, des recommandations et des actions correctives aux utilisateurs concernant la capacité prédictive, les performances, la configuration et bien sûr la sécurité.

Des enjeux RSE

Que ce soit pour leurs clients ou pour eux-mêmes, les constructeurs et éditeurs se préoccupent fortement des émanations carbone des solutions proposées. Une étude réalisée pour le compte de Stordata et NetApp indique que 91 % des décideurs IT (et 70 % des salariés) estiment qu'une meilleure gestion du stockage des données peut avoir un impact sur la réduction des émissions carbone et 36 % attendent une amélioration de la planification de la capacité de stockage alors que, en moyenne, 17 % des données stockées sont inutilisées, inutiles… voire indésirables. L'ensemble du secteur vise à améliorer leur performance avec comme repère la consommation en Watt par Teraoctet. □

Le **stockage** peut être aussi **personnel**

Si les « drives » ont largement fait leur place dans l'outillage des salariés, il existe d'autres moyens de stocker les données, ce qui peut toujours être utile en cas de problème, en particulier si vous travaillez à distance.

Selon une étude réalisée pour le compte de Seagate, la plupart des organisations qui doivent gérer des jeux de données larges (définis comme dépassant 10 To) rencontrent régulièrement des problèmes pour transférer ces données. Dans de nombreux cas, suite à un incident ou une erreur humaine, les travailleurs isolés ou distants peuvent avoir un problème avec leurs données. S'il est rare que les entreprises autorisent ce type de sauvegarde, il est somme toute préférable d'avoir, en respectant les règles de l'entreprise, une copie des données à disposition. Disques externes, voire clés USB ont désormais des capacités assez importantes. Ainsi, PNY propose le SSD portable PNY Elite X-Pro. Ce SSD est ultra pratique pour emporter ses fichiers partout en toute sécurité. Il offre des vitesses de transfert exceptionnelles allant jusqu'à 1600 Mo/s en lecture et 1 500 Mo/s en écriture et est disponible dans des capacités allant jusqu'à 4 To pour répondre aux besoins de stockage les plus exigeants. Du côté USB, le constructeur a mis récemment sur le marché la clé USB Duo Link 3.2 Type C qui ne nécessite pas de connexion WiFi. Elle permet d'accéder à ses documents facilement et partout. La Duo Link est adaptée à une grande variété d'utilisateurs, qu'ils soient photographes, vidéographes, influenceurs, créateurs de contenus… mais aussi à toute personne disposant d'un appareil Android, rendant possible un transfert rapide de contenus entre un mobile et un PC sans devoir passer par des services Cloud. Ils pourront ainsi profiter de possibilités presque illimitées quant à la gestion de leurs données afin de ne jamais rater un instant par manque d'espace. La clé USB Duo Link 3.2 Type C offre des capacités de stockage allant de 64 GB à 256 GB.

Le SSD portable PNY Elite X-Pro.

Des capacités au-delà du To

Western Digital a annoncé une gamme de nouvelles solutions sous sa marque SanDisk, conçues pour répondre aux besoins des utilisateurs en matière de stockage, tant à domicile qu'en déplacement. Pour les appareils Android, les Chromebook et les ordinateurs Windows, les nouvelles cartes microSD de 1,5 To offrent un espace de stockage massif avec des vitesses de transfert allant jusqu'à 150 Mo/s en lecture lorsqu'elle est associée à un lecteur de carte microSD SanDisk MobileMate USB 3.0. Les nouvelles cartes de 1,5 To sont disponibles dès maintenant au prix conseillé de 175,99 € en France et bénéficient d'une garantie limitée de 10 ans. □

LE STOCKAGE À FROID

Au début de cette année, Western Digital a discerné 5 grandes tendances dans le stockage dont celle de l'archivage sur le long terme ou stockage à froid. Il s'agit de l'archivage sur le long terme de données non utilisées sitôt produites et traitées uniquement en cas de besoin. Cela concerne notamment des informations non structurées telles que les enregistrements de vidéosurveillance et les données ou images issues de capteurs, qui présentent un immense potentiel pour de futures applications autour de l'IA ou de l'analyse. Le stockage à froid est une approche peu coûteuse et de plus en plus populaire pour stocker des données. À l'horizon 2025, près de 80 % des données numériques pourraient être conservées dans des archives.

Le stockage **du futur**

La tendance de l'accroissement des données n'est pas près de s'arrêter et à un certain niveau, il va donc falloir penser à d'autres solutions pour conserver les volumes sur le long terme. Différentes solutions commencent à sortir des laboratoires.

Le stockage sur ADN est une piste intéressante pour conserver un large volume de données sur une longue période.

De nouvelles solutions et des innovations sont nécessaires pour pouvoir archiver des données numériques sur des périodes dépassant les 100 ans. Le stockage sur ADN, plus précisément sur la structure moléculaire de l'ADN, est particulièrement prometteur. Si elle semble relever de la science-fiction, la mise en œuvre de cette technologie est parfaitement possible aujourd'hui, et pourrait même révolutionner l'avenir du stockage de données. L'utilisation de molécules d'ADN pour transporter des données présente de gros avantages : une densité de stockage très élevée et des coûts de maintenance faibles. Des avancées majeures en matière d'ingénierie génétique et de séquençage toujours en phase de développement, ainsi que la baisse des coûts de synthèse de l'ADN, pourraient rapidement favoriser l'arrivée sur le marché du stockage sur ADN.

Le stockage en cube !

Sur le même modèle que les QR Codes qui encodent et stockent des informations sur des surfaces pixelisées, des chercheurs américains et chinois développent actuellement un système pour encoder les données, cette fois-ci au sein de patterns de couleur disposés sur un cube en hydrogel. L'avantage est de profiter de la surface cubique et de ses trois dimensions pour étendre la capacité de stockage. Le principe est de déplacer les patterns de couleurs à volonté pour encoder de nouvelles données. Pour vous donner un chiffre, les chercheurs estiment qu'il existe environ 43 multipliés par 10 puissances 18 configurations de couleurs possibles.

Retour vers le futur

Autre piste à suivre, la combinaison entre stockage flash et la bonne vieille bande magnétique avec la technologie FLAPE (Flash and Tape). Les données les plus accédées sont stockées sur des disques Flash mais toutes les données sont placées sur des bandes autorisant le stockage de larges capacités à moindre coût. Une déclinaison FLAPE Plus ajoute un NAS RAID pour apporter plus de vitesse à ce type de solutions. Selon IDC, 80 % des données sont actuellement placées sur des bandes magnétiques dans les centres de données.

Encore un petit verre !

Une équipe de l'Université de Southampton développe un support de stockage miniaturisé qui se compose d'une nanostructure en verre à 5 dimensions. Lorsque cette solution sera mature, il sera possible de stocker 360 To à température ambiante pour des milliards d'années et résistera à de fortes pressions et des températures allant jusqu'à 1000 degrés Celsius.

Le stockage holographique

Il s'agit d'une méthode utilisant l'holographie afin de stocker de grandes quantités de données dans des cristaux ou des polymères photosensibles. Il est possible d'y inscrire des données sous différents angles *via* un faisceau enregistreur, et donc, d'entasser d'importantes quantités de données dans un espace extrêmement restreint. Il ne s'agit pour l'instant que d'une étude dans les laboratoires de Microsoft, mais cela reste une piste intéressante même si le principe n'est pas nouveau. □

bouygues TELECOM ENTREPRISES

Device as a Service

Une solution clé en main pour louer, déployer et piloter votre flotte de smartphones et tablettes d'entreprise :

Simplicité
Profitez de services tout inclus dans un abonnement mensuel unique

Sérénité
Bénéficiez d'un remplacement de vos terminaux sous 24h en cas de panne

Performance
Préservez votre trésorerie tout en utilisant une flotte mobile de dernière génération

Écoresponsabilité
Restituez vos équipements pour les reconditionner / recycler aux normes DEEE*

3100 3100 Service & appel gratuits | **bouyguestelecom-entreprises.fr**

Offre soumise à conditions. En savoir plus sur bouyguestelecom-entreprises.fr. * DEEE : Déchets d'Équipements Électriques et Électroniques.

Bletchley Park

par Bertrand Garé

C'est tout un symbole. L'Union européenne, les États-Unis et la Chine viennent de signer une déclaration pour un développement "sûr" de l'intelligence artificielle (IA), lors du premier sommet international consacré à la sécurité autour de cette technologie. Le symbole tient dans le lieu de la signature de la déclaration, là où des chercheurs étaient regroupés pour déchiffrer les codes des armées allemandes lors de la Seconde Guerre mondiale. Cela deviendra plus tard le GCHQ, le Government Communications Headquarters, le service gouvernemental du Royaume-Uni responsable du renseignement d'origine électromagnétique et de la sécurité des systèmes d'information.

Un premier pas

Cette déclaration propose, pour la première fois, un accord sans précédent entre 28 pays, énonçant une compréhension commune des opportunités et des risques posés par l'intelligence artificielle (IA). Ce texte met en évidence l'urgence de gérer collectivement les risques potentiels liés à cette technologie révolutionnaire, dans le but de garantir un développement sûr et responsable de l'IA, au bénéfice de la communauté mondiale, et souligne que la coopération internationale est la meilleure approche pour faire face à ces risques. Les signataires se sont engagés à collaborer sur la sécurité et la recherche en matière d'IA, en favorisant une plus grande collaboration scientifique. La République de Corée a accepté de coorganiser un sommet virtuel sur l'IA au cours des six prochains mois, tandis que la France accueillera le prochain sommet en personne dans un an.

Quels risques ?

Beaucoup mettent en avant des conséquences catastrophiques pour l'humanité comme la prise de contrôle du système financier ou la rébellion de l'IA contre les humains. Hélas, sur le long terme, rien ne permet d'exclure ces risques. D'autant que certains experts indiquent que l'IA pourrait atteindre le niveau d'intelligence humaine globale en 2028, soit demain ! Quand on constate comment cette intelligence humaine se conduit dans les affaires internationales, on peut évidemment prévoir de gros risques ! Ils ont même classé ces risques au niveau d'une pandémie ou d'un conflit nucléaire. Pour d'autres, il va falloir de larges améliorations des modèles actuels pour parvenir à ce stade et mettent en doute la réalisation des risques ultimes. En fait, ces risques mis en avant masquent le principal problème du moment : la désinformation et les progrès des « deepfakes ». La désinformation est déjà bien présente dans nos sociétés. Elle provient à la fois d'un changement des usages de consommation des médias par la population, une vision purement financière des médias, privilégiant de plus en plus les intérêts de leurs propriétaires plutôt que l'information. Cela s'accompagne d'une baisse de confiance dans les gouvernements et des attaques de plus en plus sévères contre les régimes démocratiques tel que nous les connaissons. De la dictature à « l'illibéralisme », toutes ces tendances vivent et exploitent la désinformation pour mieux asseoir leur pouvoir. Le danger provient de l'efficacité de l'intelligence artificielle dans la création de ces fausses annonces, de ces fausses déclarations vidéos, audios qui renforcent encore la confusion dans les esprits. Aidan Gomez indique : *« ces modèles d'IA peuvent créer*

des médias extrêmement convaincants, il est pratiquement impossible de les distinguer du texte, des images, ou des médias créés par l'homme, c'est donc un problème auquel nous devons nous attaquer en toute urgence ».

La question est cependant centrale et inquiète au plus haut niveau les états. Le président des USA, Joe Biden, a donc dévoilé des règles et principes censés assurer que l'Amérique *« montre la voie »* dans la régulation de cette technologie. Un décret impose notamment aux entreprises du secteur de transmettre au gouvernement fédéral les résultats de leurs tests de sécurité, quand leurs projets posent *« un risque sérieux en termes de sécurité nationale, de sécurité économique nationale, ou de santé publique »*. Les critères de ces tests de sécurité seront fixés au niveau fédéral et rendus publics. Le texte donne également des orientations en matière d'équité (pour éviter les biais discriminatoires de l'IA), lance des recherches sur l'impact de l'intelligence artificielle sur le marché du travail et recommande le développement d'outils pour identifier facilement les contenus produits avec de l'IA.

Un front d'opposition

Vu la situation institutionnelle et la nécessité de passer devant le Congrès américain, les bonnes dispositions de Joe Biden risquent d'être rapidement battues en brèche. C'est surtout le débat autour de la technologie elle-même qui alimente un front contre la régulation de l'intelligence artificielle. Ainsi, dans une interview remarquée et reprise par l'Usine Digitale Andrew Ng, s'il n'est pas contre une utilisation responsable, considère que surréguler la technologie aboutit à une colossale stupidité, car cela s'appuie sur deux arguments qui vont freiner l'innovation : le sentiment que l'IA pourrait conduire à l'extinction de l'humanité et la volonté d'instaurer un système de licence, considéré comme un bon moyen pour rendre l'IA plus sûre. Et de dénoncer les grandes entreprises du secteur qui viseraient à conserver leur prééminence dans le domaine au détriment de l'open source et de nouveaux acteurs.

Si libérer l'innovation est encore d'aller plus vite pour fournir les moyens à l'IA de devenir encore plus dangereuses pour nos sociétés, les bons sentiments d'Andrew Ng ne vont pas bien loin. Par ailleurs, dans tous ces débats, les conséquences sociales de la technologie ne sont pas encore réellement perçues. Une étude réalisée par une banque indique que l'IA peut automatiser 300 millions d'emplois. Et de nous refaire le discours sur les destructions créatrices inspirées de Schumpeter avec la disparition d'emplois, mais la création d'autres. Au passage, il faut remarquer que ces créations sont moindres que les emplois détruits, demandent des niveaux de compétences bien plus élevés...

Autre facteur social souvent négligé, la discrimination. Les algorithmes d'intelligence artificielle figent des stéréotypes racistes ou sexistes. Un exemple frappant est celui de l'algorithme de recrutement qui était utilisé par Amazon il y a quelques années. En octobre 2018, les analystes se sont rendu compte que leur programme, basé sur un système de notation automatisé, pénalisait les candidatures où figurait une référence aux femmes. Nous ne développerons pas les problèmes liés aux données personnelles ou à la propriété intellectuelle.

Espérons juste que le symbole de Bletchey Park soit suivi d'effet avec l'instauration de véritables règles autour de l'utilisation de l'IA qui s'imposeront à tous et pas aux seuls signataires de la déclaration, qui semblent plus d'intention que d'une volonté réelle. □

Conseil, pilotage et développement IT

meritis

Meritis, célèbre cette année son **16ème anniversaire** et affiche une **croissance de plus de 40% par an depuis sa création et compte près de 900 collaborateurs !**
Et comme chaque projet est avant tout une aventure humaine, nous recherchons de nouveaux consultants qui partagent nos valeurs : **bienveillance, proximité, exigence et humilité.**

Best Workplaces™ De 250 à 1 000 salariés Great Place To Work. FRANCE 2020

TOP 3

Nos expertises : **Software Engineering, Cloud & Infra, Data, Finance et Projects / Program / Products.**

Meritis, société de conseil en Transformation des Systèmes d'Information et Organisations, **est régulièrement certifiée Great Place to Work depuis 10 ans.**
En 2020 Meritis rejoint le **Top 3 des GPTW** de 250 à 1000 salariés.

Nous recherchons de nombreux consultants à **Paris** et partout en France : **Développeurs, Développeurs Java, C++, Experts DevOps, Ingénieurs Test QA, data Engineers et bien d'autres !**

Nous recherchons de nombreux profils !
Venez nous rencontrer.

Paris
75008
36 Avenue Pierre 1er de Serbie

Sophia Antipolis Cedex
06901, Les Algorithmes
Aristote B, 200 Route des Lucioles

Aix-en-Provence
13290
240 Rue Paul Langevin

Montpellier
34000, Parc Club du Millénaire
Bâtiment 2, 1025 rue Henri Becquerel

Nantes
44000
1 rue Eugène Varlin

Processeurs

Puces d'IA : une course lancée sur un terrain accidenté

Les avancées telles que ChatGPT, et la déferlante d'IA générative qui en a découlé, ont fait exploser les besoins de calcul matriciel et donc la demande de semi-conducteurs.

Les entreprises investissent des milliards dans ces modèles d'IA, si bien que la pénurie de puces dédiées à ces applications d'IA est à craindre. Une situation qui amène l'industrie à remettre en question la conception même de ces modèles, tout en offrant une opportunité unique de marché aux challengers qui souhaiteraient rivaliser avec Nvidia, leader encore incontesté du secteur.

Nvidia est un acteur plutôt connu des amateurs de jeux vidéo. L'entreprise est avant tout reconnue pour ses cartes graphiques bien établies. En forme, la multinationale a pourtant saisi l'opportunité de se réinventer un peu par hasard. Avec l'avènement des IA génératives, illustré par l'arrivée de ChatGPT (Open AI) dont la première version a été présentée en novembre 2022, et plus tard de Bard (Google), les GPU (Graphics Processing Unit ou unité de traitement graphique) de la multinationale se sont avérés particulièrement précieux. *« L'industrie s'est rendu compte que des processeurs, initialement fabriqués pour la 3D, étaient également utiles pour le calcul matriciel en matière de deep learning et donc essentiels pour entraîner les modèles d'IA »*, explique Stéphane Roder, président d'AI Builders, un cabinet de conseil spécialisé dans la transformation des données IA des entreprises.

Un besoin en calcul qui explose

Et ce besoin en calcul a littéralement explosé avec l'arrivée des IA génératives. Reposant sur des technologies de traitement automatique du langage (NLP) et des grands modèles de langage (LLM), elles sont entraînées sur des centaines de milliards de paramètres pour les plus performantes d'entre elles, comme ChatGPT4.

Stéphane Roder, président du cabinet de conseils AI Builders.

« Un juriste n'aura besoin que d'un outil qui comprenne l'analyse juridique, un analyste financier, d'un LLM capable de traiter des données financières. »

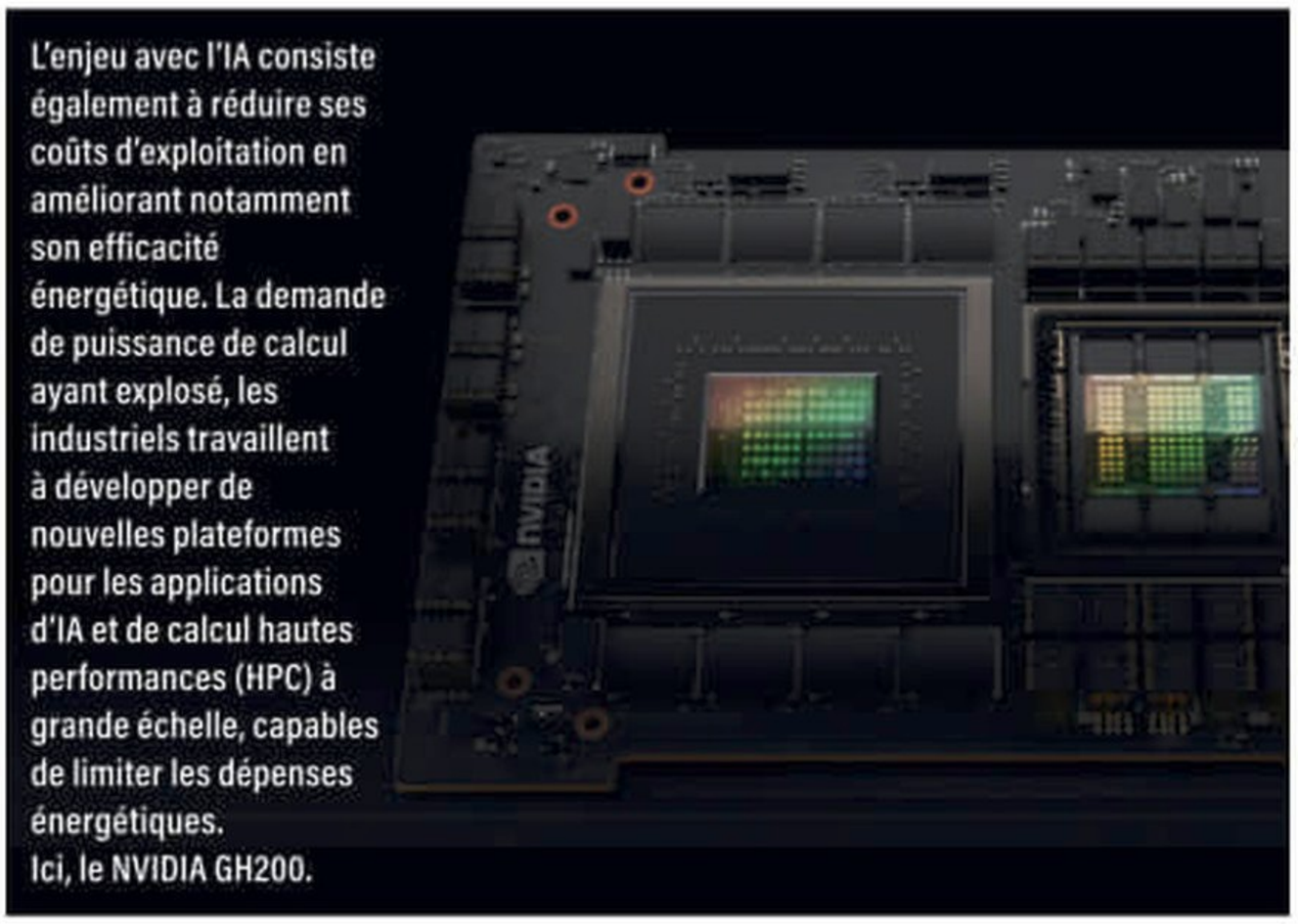
À titre de comparaison, GPT3 n'en compte « que » 175 milliards. Sans même parler de l'avalanche des IA génératives, comme Bard (Google), qui ont vu le jour pour tenter de concurrencer le bébé d'Open AI. Toutes, sans exception, sont gourmandes en calcul.

D'autant qu'avec les promesses de ces technologies, toutes les entreprises s'y mettent, ou y songent fortement. Un rapport d'IDC (International Data Corporation) avance, par exemple, que les entreprises investiront, pour la seule année 2023, près de 16 milliards de dollars dans le monde dans les modèles d'IA générative, d'infrastructure, ainsi que dans les services informatiques associés. Investissements qui devraient grimper à 143 milliards sur la période 2023-2027, avec un taux de croissance annuel de 73%. Autre rapport, celui du bureau d'étude Gartner qui estime que 80% des entreprises auront adopté des API d'IA génératives (GenAI) ou déployé leurs propres modèles d'ici 2026.

Le processeur Intelligence Processing Unit (IPU) de Graphcore, l'IPU Bow, utilise la technologie d'empilement 3D Wafer-on-Wafer (WoW). IPU Bow offre jusqu'à 350 téraFLOPS de calcul IA.

Circuler, il n'y a plus de GPU

« Plus il y a de paramètres, plus le calcul matriciel est important. Nous sommes à un moment de l'histoire de l'IA où ces calculateurs matriciels sont extrêmement demandés, et c'est ce qui a propulsé des acteurs comme Nvidia », explique Stéphane Roder. Tant mieux pour Nvidia. Mais face à cette demande exponentielle, le marché, lui, est confronté à ses limites. Les délais de livraison des GPU H100 et A100 de Nvidia ont explosé, et le carnet de commandes est plein jusqu'à fin 2024. La chaîne d'approvisionnement en est largement perturbée, et le risque d'une nouvelle pénurie de GPU est bien réel, puisque Nvidia fournit entre 80 et 90 % de ceux qui sont spécifiquement adaptés aux applications d'IA.



L'enjeu avec l'IA consiste également à réduire ses coûts d'exploitation en améliorant notamment son efficacité énergétique. La demande de puissance de calcul ayant explosé, les industriels travaillent à développer de nouvelles plateformes pour les applications d'IA et de calcul hautes performances (HPC) à grande échelle, capables de limiter les dépenses énergétiques.
Ici, le NVIDIA GH200.

Miser sur la frugalité

Pas le choix, pour ne pas stagner, l'industrie de la GenAI va devoir évoluer. Pour éviter la pénurie, la solution consisterait, selon Stéphane Roder, à créer des modèles qui utilisent tout simplement moins de ressources à performance égale. Autrement dit, développer des modèles ultraspécialisés : conçus pour réaliser une tâche bien définie, ils seraient ainsi moins exigeants en paramètres et donc plus frugaux en processeurs. *« Les ChatGPT et autres Bard sont de merveilleux démonstrateurs, mais dans la vie d'une entreprise, un juriste n'aura besoin que d'un outil qui comprenne l'analyse juridique, un analyste financier, un LLM capable de traiter des données financières »*, fait remarquer Stéphane Roder.

En réalité, ce mouvement est déjà engagé. Bloomberg, par exemple, l'a fait avec son modèle d'apprentissage automatique BloombergGPT, en s'associant avec Nvidia et Amazon Web Services. Présenté comme un outil de recherche et d'analyse financière, il applique le type de techniques d'IA de GPT à des ensembles exclusifs de données financières. Citons aussi les industriels qui développent des composants de moindre puissance. Ainsi, AMD a récemment annoncé le GPU Instinct MI300X, pour alimenter des modèles de langage de 40 à 80 milliards de paramètres.

La chasse aux parts de marché

Cette tension sur le marché des GPU laisse entrevoir également une opportunité à la concurrence, comme ARM, Intel, ou encore Graphcore. *« La situation est un atout pour celle-ci ; elle va pouvoir faire évoluer les architectures et en proposer de nouvelles »*, souligne Stéphane Roder. Tenstorrent, entreprise spécialisée dans les processeurs d'IA et la fourniture de licences pour l'architecture RISC-V IP, travaille avec Samsung Foundry pour commercialiser sa prochaine génération de chipsets d'IA. Ils fourniront une puissance évolutive du milliwatt au mégawatt et doivent *« repousser les limites du calcul dans plusieurs secteurs, tels que les centres de données, l'automobile et la robotique »*, indiquait la société dans un communiqué. Pour Jim Keller, son PDG, l'objectif est clair : *« développer des calculs hautes performances »* et *« fournir ces solutions à des clients du monde entier »*. Graphcore développe, quant à lui, son processeur Intelligence Processing Unit (IPU), qui constituera, selon lui, la norme mondiale en matière de calcul d'intelligence artificielle. Pour le moment, Nvidia a encore de beaux jours devant lui, mais il devrait quand même regarder par-dessus son épaule. □

V.M

LES GPU PLUS STRATÉGIQUES QUE LES ARMES

Même les géants font face à des difficultés. Depuis quelques mois, Nvidia et les autres doivent conjuguer avec un contexte géopolitique tendu entre la Chine et les États-Unis. Sur fond de guerre technologique et commerciale, Washington accuse Pékin d'avoir volé des technologies sensibles à des entreprises américaines par le biais d'espionnage industriel ou de projets de coentreprises. Les États-Unis cherchent également à priver la Chine des technologies essentielles à son industrie militaire et à ses projets liés à l'intelligence artificielle. L'administration Biden a ainsi limité, en octobre 2022, la puissance de calcul des puces destinées à être exportées en Chine sans licence préalable et a introduit des restrictions à l'exportation de technologies nécessaires à la fabrication de semi-conducteurs. Nvidia, comme d'autres fabricants, a bien tenté de les contourner en développant des puces de moindre puissance pour le marché chinois — par exemple, les H800 et A800. Mais le département du commerce américain envisage de renforcer encore un peu plus ces restrictions.

Espace de travail

JobsTable : une table ultra high-tech pour les télétravailleurs

Comme son nom l'indique, la JobsTable est une table modulable de travail développée pour répondre aux besoins spécifiques des télétravailleurs ayant peu d'espace. Créée par Omar Seck, un ingénieur informatique français, cette innovation a été primée au concours Lépine 2021. Gros plan sur un produit pour le moins atypique.

Après plusieurs années de développement et une présentation couronnée de succès par la plus haute distinction du concours Lépine 2021, la JobsTable est disponible à la vente depuis le 22 septembre dernier sur le site : [https://fr.jobstableproject.com/]. Grâce à une ingénieuse architecture modulaire et trois puissants vérins, ce meuble deux-en-un prend la forme d'une table basse ou d'un bureau multimédia complet en seulement quelques secondes. Basée sur un châssis en aluminium à structure déformante, la table est totalement ajustable à la position voulue par l'utilisateur. Habilement dissimulées dans la structure en bois, quatre roulettes peuvent également être déployées pour déplacer facilement l'ensemble.

Un bureau futuriste modulable

Destinée aux télétravailleurs qui ont peu d'espace, la JobsTable se transforme à la demande en une plateforme multimédia comprenant un écran central de 27 pouces ainsi qu'un clavier et un trackpad pouvant être intégrés en option dans une vitre de commande tactile. La table dissimule également une caméra HD 1080p, quatre haut-parleurs à 360° en option (deux à l'avant et deux à l'arrière), et un micro de qualité studio pour les visioconférences et autres appels vidéo. Différents boutons de commandes sont disponibles sur le pupitre pour actionner les mécanismes, gérer le volume, ou encore la luminosité de l'écran. Ne cherchez pas d'ordinateur, il n'y en a pas. Pour que son produit ne devienne pas obsolète au bout de deux ou trois ans, son concepteur a préféré intégrer tous les connecteurs nécessaires pour que les utilisateurs puissent brancher en un clin d'œil leur propre ordinateur Mac ou PC. La JobsTable intègre ainsi des ports HDMI, USB-A, USB-C, une prise de courant 220 volts, un module sans-fil Bluetooth, et même un câble USB-C (compatible Thunderbolt 3 et 4) permettant de brancher et recharger rapidement différents terminaux. Sans oublier une niche équipée de ports USB-C de type 3.1 Gen 2 pour loger et brancher un ordinateur portable au système. Le plateau de gauche dissimule un chargeur à induction (norme Qi) permettant de recharger tous les appareils compatibles. Véritable bureau multifonctionnel, la JobsTable dispose également de différents espaces de rangement que cela soit pour le clavier, la souris, le trackpad, les câbles, les chargeurs, ou même les télécommandes du salon. Mention spéciale pour le coffre à disques durs externes (en option) équipé de connecteurs USB-C et USB-A afin de pouvoir les relier directement à l'ordinateur utilisé avec la table ! Qui a dit ingénieux ? Il existe quatre différentes versions qui se distinguent essentiellement par leur équipement multimédia. Les tarifs varient de 5 500 à 6 900 euros pour la version Pro la plus haut de gamme. □

Jérôme Cartegini

CARACTÉRISTIQUES DE LA JOBSTABLE

- **Écran LED 27 pouces :** résolution QHD (2 560 × 1 440 pixels)
- **Caméra** HD 1080 p
- **Audio :** 4 haut-parleurs coaxiaux 210 W
- **Connectivité sans fil :** Bluetooth 5.0
- **Microphone :** micro qualité studio
- **Connectique :** 1 x USB-C (connexion ordinateur), 1 x USB-A, 2 x USB-C type USB 3.1 Gen 2, 1 prise 220 V, 1 port HDMI
- **Clavier** AZERTY Bluetooth
- **Trackpad** multi-touch Bluetooth
- **Dimensions** position table basse (H x L x P) : 47 × 126 x 70 cm
- **Poids :** 80 kg • **Prix :** à partir de 5 500 €

Lenovo Tech World 2023

L'IA de votre poche au Cloud

Lors de sa conférence mondiale qui s'est tenu à Austin au Texas, le constructeur a présenté sa vision pour l'intégration de l'intelligence artificielle dans l'ensemble de ses lignes de produits : des téléphones en passant par les PC et ses lignes de serveur.

Les CEO de Lenovo et de NVidia sur scène pour l'extension de leur partenariat.

Après l'annonce de son investissement d'un milliard de dollars dans l'intelligence artificielle (IA), Lenovo a présenté lors de la neuvième édition de sa conférence et la première de visu depuis 2019 la concrétisation de sa feuille de route avec l'intelligence artificielle. Le constructeur propose une approche dynamique d'une IA hybride qui s'appuie sur les Foundation Models que ce soit pour une utilisation publique (ouverte à tous), privée (qui ne s'adresse qu'à un groupe ou sur les données internes de l'entreprise) ou personnelle (sur les données et les matériels d'une seule personne). Dans ce dernier cas, Lenovo ajoute des fonctions de gestion des données et un proxy pour protéger le caractère privé des données. Celui-ci peut masquer et démasquer les données ou réarranger les données pour apporter une réponse conforme. Les modèles pour entreprise ou personnels ne fonctionnent pour l'instant que sur un matériel ou serveur sur site en assurant qu'aucune donnée ne sera partagée ou ne sera utilisée dans un modèle public.

Quel que soit le type de modèle, il apprend des données du propriétaire des celles-ci pour s'initier selon le système de valeur des humains sur un large volume de données (entre 100 et 200 milliards de paramètres) s'adaptant à de nombreux cas d'usages métiers ou autres. Ces Foundation Models sont un matériau brut avec lequel il est possible d'interagir par de multiples moyens. Ainsi, les modèles pour entreprise peuvent bénéficier d'entraînements additionnels. En combinant une configuration fine et une base de données vectorielle pour découvrir et coupler les différentes structures puis estimer leur importance ou criticité (comme un RAG, retrieval-augmented generation), il est possible d'allouer plus ou moins de bits avec l'intégration avec les sous-systèmes afin d'obtenir une tâche spécifique à l'entreprise de bout en bout. Il est possible d'agir sur la taille du modèle et de le compresser pour le porter sur un smartphone, un PC/laptop ou tout autre matériel apte à le recevoir.

Un jumeau de vos données

Pour les entreprises et les simples utilisateurs, Lenovo veut encore aller plus loin en créant un véritable jumeau de vos données numériques avec l'IA. Les applications d'intelligence artificielle, avec les données provenant des matériels, de la périphérie ou du cloud privé, détiennent le savoir des entreprises et le conservent de manière

sécurisée. Ce jumeau intelligent peut être ainsi utilisé pour de multiples usages ; réserver par exemple des déplacements, tout en respectant les règles internes de l'entreprise et les préférences de l'utilisateur, ou encore pour des équipes s'occupant de la chaîne d'approvisionnement pour anticiper une rupture du fait de phénomènes météo provenant d'une intelligence artificielle publique pour anticiper une rupture de livraison, ou encore prendre la décision de déplacer la source d'un approvisionnement. Il en est de même pour le Personal AI Twin qu'a présenté le constructeur.

Une vue du nouveau concept de téléphone flexible de Motorola avec l'IA de Lenovo

À l'analyse, Lenovo va donc largement renforcer ses matériels pour fournir ce type de possibilité avec l'intelligence artificielle. Cela devrait combiner des configurations plus puissantes que ce soit pour le stockage, les serveurs ou les PC et smartphones. Le constructeur va certainement combiner dans ces configurations musclées des processeurs dédiés comme des GPU, des DPU, des NPU. Cela devrait donc avoir des conséquences sur le prix de ces matériels. À savoir si les bénéfices apportés par l'IA vont pouvoir convaincre les acheteurs potentiels de payer un prix élevé pour leur configuration.

Une avalanche de partenariats

Sans surprise, la session plénière a été aussi l'occasion de présenter de nombreux partenariats, nouveaux ou étendus. Le plus significatif a été celui avec l'inévitable Nvidia. Les deux entreprises étendent leur partenariat existant avec de nouvelles solutions hybrides et des liens autour de l'engineering de ces solutions. Par une proche collaboration, les deux entreprises vont développer des solutions de computing, spécifiquement conçues pour l'IA de la périphérie au Cloud. Elles s'appuieront sur les services professionnels de Lenovo pour déployer une approche hybride avec le service Cloud de Nvidia (AI Foundations) afin de le porter sur les systèmes sur le site de Lenovo, intégrant les matériels et logiciels de Nvidia conçus pour l'IA générative. Par le moyen de Nvidia NeMo, inclut dans Nvidia AI Enterprise, les organisations ont la possibilité de personnaliser des LLM présents dans AI Foundation en s'appuyant sur une configuration fine et un modèle RAG pour générer des applications d'IA pour les données internes de l'entreprise de manière optimisée sur les solutions hybrides de Lenovo. Les principaux matériels de Lenovo impliqués dans ce partenariat sont les serveurs ThinkSystem SR675 V3 et les stations de travail ThinkStation PX optimisés pour Nvidia AI Entreprise. The ThinkSystem SR675V3 va embarquer le GPU NVIDIA L40S, les DPUs NVIDIA BlueField-3 et la connectivité NVIDIA Spectrum-X. La ThinkStation PX va apporter de nouvelles capacités d'IA et des performances de centres de données au poste de travail avec jusqu'à 4 GPUs NVIDIA RTX 6000 Ada. Les autres partenariats annoncés ou étendus sont ceux avec Microsoft autour d'LIA, de Qualcomm et d'AMD autour des chipsets et processeurs.

L'IA dans votre poche

La conférence a été aussi l'occasion de présenter différentes innovations dont un smartphone qui ne contient plus de coques solides, mais un support flexible qui permet de faire prendre au téléphone plusieurs positions comme de le porter en bracelet pour un usage main libre ou de le plier pour le faire tenir seul sans nécessiter un support spécifique. Ce nouveau type de téléphone utilise un écran FHD+ POLED qui peut être plié. Ce concept peut s'adapter à un téléphone Android avec un écran 6.9 pour retrouver une expérience plus classique. Par l'intelligence artificielle, l'utilisateur peut personnaliser son téléphone en créant par exemple un fond d'écran avec les motifs de ses vêtements par une simple photo. De plus, Lenovo a développé un assistant personnel qui apprend en permanence par un Foundation Model qui est personnalisé pour son seul utilisateur et donc protégeant sa vie privée. MotoAI, le doux nom du modèle, traite les données, réalise des tâches localement et bénéficie d'une base de connaissance qui stocke les préférences et les habitudes de l'utilisateur. L'assistant peut répondre à des questions, proposer des rédactions de messages, planifier des tâches...

Les autres innovations présentées sont une amélioration du scanner de document pour une meilleure qualité des scans, des fonctions de résumés de documents longs qui sont restitués sous forme de messages sur les points clés pour une compréhension rapide du document. Pour le respect de la vie privée, l'IA identifie et floute les zones contenant les photos de profils ou les noms dans un billet sur les réseaux sociaux si l'utilisateur le souhaite. □

B.G

adista

Pour un Système d'Information agile, durable et sécurisé

La synergie des services Connectivité, Cloud et Cybersécurité

TOPTECH
GREEN IT Économie circulaire | 2023

adista.fr
contact@adista.fr - 03 57 54 54 00

Étude « Grand Angle ESN & ICT »

La filière performe

Pour la cinquième fois, Numeum a publié son étude du marché des ESN et des ICT, réalisée cette année avec KPMG. Pas de grande surprise du côté du classement, ni des stratégies mises en œuvre par les sociétés de la filière.

Le marché des ESN ne connaît pas la crise. Tel est le constat que l'on peut dresser à la lecture de l'étude *« Grand Angle ESN & ICT »* réalisée par Numeum et KPMG. Désormais, l'ensemble des sociétés du Top 10 font au moins un milliard d'euros de chiffre, pour un total dépassant les 20 milliards de dollars. Soit une progression de 17 % sur un an. Comme à chaque édition, ce groupe de tête tire l'ensemble du secteur : les cent premières sociétés de services informatiques cumulent 36 milliards d'euros de revenus, en hausse de 23 % comparé à l'année précédente. On comprend alors aisément que 98 % des entreprises sont confiantes ou très confiantes dans leurs objectifs de croissance à 3 ans, 3 points de plus que l'année précédente. *« Malgré une conjoncture mondiale incertaine, l'écosystème numérique apparaît comme peu impacté par les crises. Agiles et résilients, la plupart des acteurs de la filière ont enregistré une croissance à deux chiffres »* écrit Numeum.

Conseil et cloud

Cette croissance est, à en croire l'étude, portée par une stratégie des ESN tournée pour 80 % d'entre elles vers le développement d'offres à très haute valeur ajoutée et innovantes, suivie de la mise en place de plans de recrutement (74 %) et du positionnement sur des secteurs porteurs (62 %) à l'instar des services financiers, de l'industrie et de l'énergie. À noter que, pour un quart des ESN, le conseil en transformation digitale a pris le pas sur le cloud (21 %) comme activité la plus dynamique. La conception et le développement de solutions technologiques arrivent en troisième position (16 %). La R&D attire d'ailleurs en moyenne 7 % du chiffre d'affaires des ESN et mobilise 13 % des effectifs à temps plein, soit une hausse de 8 % d'une année sur l'autre.

Orange Business fait son entrée dans le Top 10 des ESN lors de cette édition 2023, avec un chiffre d'affaires de près de 1,5 milliard d'euros, contre 884 millions l'année précédente.

Rang	ESN & ICT	Chiffres d'affaires en France *(en milliers d'euros)*
1	CAPGEMINI	4276000
2	SCC FRANCE	2616753
3	ACCENTURE	2387398
4	SOPRA STERIA	2039000
5	ATOS	1960000
6	IBM FRANCE	1740000
7	ORANGE BUSINESS	1494664
8	ECONOCOM	1457000
9	CGI France	1286705
10	ALTEN	1178171
11	INETUM	998403
12	COMPUTACENTER France	879000
13	DOCAPOSTE	836000
14	AKKODIS	756510
15	NEURONES	665400
16	THALES SERVICES NUMERIQUES	515200
17	SPIE ICS	515000
18	AXIANS COMMUNICATION & CLOUD	470000
19	DEVOTEAM	469000
20	TESSI	466600
21	SII GROUP	434070
22	WAVESTONE	425211
23	SOLUTIONS30	425162
24	OVHCLOUD	389000

Sans grande surprise, le cloud représente la majorité (18 %) de ces investissements dans l'innovation. Conception de solutions technologiques, conseil en transformation digitale et IA occupent ex-æquo (14 %) la deuxième marche du podium. La cybersécurité, avec 12 % des investissements, ferme la marche. On remarquera en outre que 31 % des projets en innovation s'achèvent par une mise sur le marché.

Selon Numeum, *« ce dynamisme est le fruit de la mobilisation de tout un écosystème, puisque 49 % des ESN et ICT déclarent faire appel à des acteurs externes pour mener à bien des projets d'innovation »* : fournisseurs (52 %), universités, chaires ou établissements d'enseignement supérieur et laboratoires publics (48 %), instituts technologiques, centres de recherche, laboratoires privés et pôles de compétitivité (43 %), start-up et scale-up (38 %), clients (24 %) et freelances (24 %). Ce recours à des acteurs externes peut également s'expliquer par les

Rang	ESN & ICT	Chiffres d'affaires en France *(en milliers d'euros)*
25	OPEN	381000
26	SCALIAN	346430
27	DAVIDSON CONSULTING	305000
28	TALAN	300322
29	MAGELLAN PARTNERS	300000
30	ASTEK	293000
31	INFOTEL	270659
32	EXPERIS FRANCE	233326
33	INHERENT	218000
34	APSIDE	214000
35	FUJITSU	183353
36	HELPLINE	183076
37	NEOSOFT	176000
38	VISIATIV	166100
39	KEYRUS	159000
40	GROUPE TIBCO	151000
41	ITS GROUP	150000
42	CONSORT GROUP	143142
43	SYNCHRONE	139000
44	GROUPE SMILE	138000
45	HARDIS GROUPE	137100
46	MC2I	136000
47	SQLI	130700
48	AFD. TECH	125000
49	NIJI	113534
50	KLEE GROUP	112000

Les incertitudes autour du projet de restructuration d'Atos se ressentent sur ses performances, notamment financières. L'ESN recule de deux places au classement, laissant la 3ème marche du podium à Accenture.

difficultés de recrutement des ESN et ICT. Les externes représentent désormais 11,7 % des effectifs en 2022 contre 10,1 % en 2021. Ainsi, 81 % des entreprises ont confiance dans leur capacité à remplir leurs objectifs en termes de recrutement à 3 ans. Soit 8 points de moins que lors de la précédente étude.

Le recrutement, nerf de la guerre ou talon d'achille

Pour autant, le secteur affiche des objectifs particulièrement ambitieux pour l'année 2023 et engage des dépenses conséquentes dans la formation et la fidélisation. 58 % des entreprises misent ainsi sur l'augmentation des salaires pour garder leurs talents et 85 % proposent deux à trois jours de télétravail par semaine. Autre signe des temps qui courent, les ESN accentuent leurs efforts en matière de RSE. 63 % d'entre elles ont d'ailleurs rattaché la fonction RSE/ESG à la direction générale. Objectif prioritaire : la réduction de l'empreinte environnementale du numérique (31 %). 78 % des entreprises se sont équipées d'un outil de mesure et de pilotage de leurs actions, un bond de 16 % par rapport à 2022. Arrivent ensuite la création d'emplois et le développement de nouvelles compétences (28 %) et le développement de solutions et services innovants à finalité ESG (19 %).

Outre l'étude, le classement lui-même est révélateur de l'état du marché des ESN et des ICT. Ainsi, on ne s'étonnera pas du recul d'Atos. En pleine incertitude quant à son projet de scission et de vente de ses activités historiques, l'ESN, malgré une légère croissance de son chiffre d'affaires, quitte le Top 3 et chute à la cinquième place, tandis qu'Accenture monte sur la troisième marche du podium. On notera également la belle performance d'Orange Business, passant de la onzième à la septième place. Capgemini, avec plus de 4 milliards d'euros de chiffre d'affaires, continue de dominer le classement, toujours suivi de SCC France. Sopra Steria reste à la quatrième place et IBM France à la sixième. □

Guillaume Périssat

Cybersécurité

Kyndryl veut s'imposer dans le service managé

La branche Cybersécurité est actuellement l'une des plus dynamiques chez Kyndryl. À sa tête, Kris Lovejoy (ci-contre) tire profit d'une longue expérience du marché des MSSP pour y imposer l'ESN.

L'Informaticien : Comment définissez-vous la cyber-résilience ?

Kris Lovejoy : C'est un terme évolutif. Nous considérons la cyber-résilience comme étant l'intersection entre la cybersécurité, la continuité des activités et la reprise après sinistre. Dans une sorte de description plus large, le risque pour les entreprises numériques se manifeste sous de nombreuses formes. Il peut s'agir de pannes matérielles, de pannes logicielles, de perturbations de la chaîne d'approvisionnement, de pannes de centres de données, de pannes de réseau et de problèmes de cybersécurité. Souvent, la cause première d'une panne ou d'un problème particulier n'est pas bien connue. Ce que je veux dire, c'est qu'il existe un problème de cyber-risque et que de nombreux facteurs différents peuvent avoir un impact sur le numérique. Le marché appelle aujourd'hui à une simplification de l'approche de gestion du cyber-risque. Ainsi, la description de la cyber-résilience serait la capacité d'anticiper, de se protéger, de résister, c'est-à-dire de détecter et de répondre, ainsi que de se remettre de tout événement lié à la cybersécurité pouvant avoir un impact sur vos services numériques, y compris, mais sans s'y limiter, la cybersécurité.

Considérez-vous Kyndryl comme un MSSP ?

En effet, nous disposons de capacités MSSP, que je décrirais comme étant très atypiques. Nous essayons de disrupter le marché des MSSP avec nos services managés, car je pense que le marché des MSSP traditionnel est fondamentalement insoutenable.

Insoutenable ? C'est-à-dire ?

Le marché des MSSP — et je dois dire que je suis dans une large mesure coupable d'avoir participé à la structuration initiale alors que je dirigeais plusieurs des premières sociétés de services gérés — était en réalité un marché de startups. De très petites entreprises qui essayaient de fournir à des grands comptes des systèmes d'alerte à grande échelle. Or, nous n'avions pas suffisamment de personne pour effectuer la gestion et l'intégration de systèmes complexes. Donc, pour que nous puissions servir nos clients, nous devions créer une unique pile de technologies incluant un gestionnaire d'informations et d'événements de sécurité. Ce que nous disions au client, c'est que, sur un contrat de cinq ans, nous allions réorganiser leur infrastructure au cours des deux premières années, pour l'intégrer dans cette pile unique. Puis, lors des cinq années suivantes, nous allions nous asseoir au sommet de cette pile et nous allons fournir des services d'alerte à forte valeur ajoutée. Le problème est que les clients possédaient déjà leur propre équipement et ne pouvaient pas intégrer toutes leurs sources de données dans le gestionnaire d'événements. En outre, ils n'aimaient pas la rigidité du modèle. Eux, ont le contexte métier, nous non, et ils demandaient à inverser le modèle. Les clients veulent une flexibilité absolue, ils veulent choisir leur propre technologie, leur propre système de détection, leur système de *threat intelligence, etc*. De plus, ils voulaient aussi pouvoir choisir les technologies en fonction des pays, car vous pouvez avoir des restrictions à l'exportation, des exigences en matière de localisation des données...

En quoi votre approche est-elle différente ?

Nous nous sommes demandé comment pouvons-nous servir au mieux le client. Donc, nous avons mis au point le *« security operations as a platform »*, une data fabric avec une couche AI OPS qui nous permet d'intégrer, à condition qu'il soit standard, n'importe quel outil dans cet écosystème, de le gérer et de le déployer *via* un système de « pods », qui peuvent être différents selon si le client veut le déployer en France, en Chine ou aux États-Unis. Ce qui permet d'être flexible et de choisir qui gère les alertes : nous, un partenaire tiers ou le client. Kyndryl a six SOC, mais ceux-ci sont généralement utilisés pour le déploiement des pods. Leur gestion et la gestion des alertes sont souvent côté client.

Vous simplifiez donc la gestion de ces opérations ?

Vous savez, les écosystèmes de sécurité sont intrinsèquement complexes : il y a beaucoup d'outils, et tout le monde aime en avoir beaucoup. Or, nous constatons pour nos clients que la meilleure approche pour améliorer la sécurité et la résilience n'est pas d'acheter plus de sécurité mais de moderniser l'infrastructure sous-jacente. Ce que nous constatons, c'est que, en particulier après le COVID, la plupart des organisations avaient introduit de nouvelles technologies avec un contrôle de sécurité limité et ajoutaient plus de complexité dans un environnement qui était déjà saturé de nombreuses infrastructures legacy. Souvent, je dis aux clients que, à leur place, je ne dépenserais pas d'argent pour sécuriser cela, je le reconstruirais en gardant à l'esprit la sécurité et la résilience. Car, sinon, vous allez dépenser tout votre argent pour sécuriser une voiture vieille de 30 ans alors qu'il est probablement moins cher d'en acheter une neuve. C'est une façon très différente de penser la sécurité : notre travail n'est pas nécessairement de vendre des outils, mais de fournir la meilleure solution au client. Et cela peut impliquer de ne pas vendre de sécurité. □

G.P

ACCESSECURITY

SALON EUROMÉDITÉRRANÉEN
CYBERSÉCURITÉ & SÛRETÉ

06-07
MARS
2024

MARSEILLE
CHANOT

LE RDV BUSINESS & INNOVATION

Pour exposer, contactez-nous

accessecurity@safim.com

ACCESSECURITY.FR

#ACCESSECURITY

Écosystème

Le Cigref milite pour la sobriété numérique et la protection des données

Jean-Claude Laroche, le président du Cigref, a présenté le 11 octobre à Paris les grandes orientations et actions à venir de cette association de responsables des services informatiques (DSI) des grands groupes. Au programme de cette 53ème AG, la (re)valorisation des notions de progrès, de sobriété numérique et la législation en matière de protection des données.

Intervenant devant plusieurs centaines de représentants de grandes DSI, Jean-Claude Laroche a mis un accent particulier cette année sur l'impact environnemental du Numérique. Il considère la sobriété numérique comme le premier défi à relever par le Cigref. Il invite donc ses membres, et surtout leurs fournisseurs IT, à réaliser davantage de progrès dans ce domaine : *« le Cigref s'implique activement sur cette thématique depuis plus d'une décennie. Mais, il faut aller plus loin pour progresser en termes de sobriété numérique, en se concentrant sur un fait : les études montrent que la fabrication du matériel informatique représente 70 % de cette empreinte environnementale »*.

Jean-Claude Laroche, président du Cigref.

Jean-Claude Laroche met cette industrie au défi de changer les modes de fabrication de la couche matérielle de l'espace numérique : *« l'objectif doit être de réduire de manière décisive les activités extractives et les émissions de carbone générées par cette industrie »*. Il invite donc les gouvernements à *« mettre en place une régulation adaptée à l'industrie des équipements numériques afin de les rendre, de façon significative, plus durables, plus réparables et plus recyclables »*. Le président du Cigref a aussi rendu hommage appuyé au projet Planet Tech'Care porté par Numeum et initié par Véronique Torner, sa présidente, qui était d'ailleurs venue présenter leurs initiatives conjointes.

Une protection des données pragmatique

Le deuxième défi du Cigref concerne la gestion de l'effervescence en matière de protection des données sensibles des entreprises. Jean-Claude Laroche s'inquiète de voir, *« depuis quelques mois, de plus en plus de parlementaires, de tous horizons politiques, être déterminés à renforcer les obligations des entreprises en la matière »*.

Le Cigref n'y est bien sûr pas opposé, car il y voit un enjeu stratégique majeur : *« nous avons bien compris la nécessité de protéger nos données sensibles, mais aussi son corollaire, l'autonomie technologique européenne sur le marché du cloud, pour lequel l'Europe accumule des retards depuis plus d'une décennie »*.

Mais le président du Cigref a égratigné au passage les Gouvernements successifs quant au manque relatif de pragmatisme dans ce domaine et à la poursuite de chimères « souveraines » : *« pour légiférer sur ce sujet, il faut le faire de la bonne manière, au bon moment, et pour les bonnes raisons. En particulier, je caricature à peine, rien ne justifierait que soit imposé à nos membres d'héberger des systèmes d'information qui ne le justifient pas sur des infrastructures qui n'existent pas... »*.

Il intervenait après le discours de Jean-Noël Barrot, ministre délégué en charge de la Transition numérique et des Télécommunications, qui a promis aux membres du Cigref *« de les aider à se défaire de la dépendance dans le Cloud qu'ils ont créé avec les Gamma »*. Un projet de loi en ce sens devait être soumis au vote du Parlement le 17 octobre.

Enfin, Jean-Claude Laroche soutient la création d'un musée du numérique et de l'informatique porté par le Conservatoire national des arts et métiers, l'INRIA et la Société informatique de France : *« ce musée permettra aux jeunes générations de comprendre l'intérêt de nos métiers et les rouages de l'informatique, ses différents métiers et débouchés, et l'impact du domaine numérique sur la réalité »*. Le Cigref annonce aussi qu'il organisera les Rencontres numériques de Strasbourg du 20 au 22 mars 2024. Accessible sur invitation uniquement, cet événement est dédié aux décideurs de haut niveau de l'écosystème numérique. □

Olivier Bellin

Services

Linkt propose une connexion de bout en bout

L'opérateur ajoute un service managé de WiFi à son offre existante et étend ainsi sa couverture après son annonce autour du SD-WAN.

Proposée en complément de ses offres de connectivité WAN, l'offre LAN WifiLinkt permet aux entreprises de bénéficier de fonctionnalités, de technologies et de services cohérents sur l'ensemble de leurs sites. L'administration de leur LAN au travers d'une console centralisée offre une exploitation simple et efficace de leurs switchs et bornes Wifi. Linkt accompagne ses clients de bout en bout pour la conception et le déploiement de leur solution LAN ; de l'aide à la collecte à l'accompagnement à la prise en main de la console de management centralisée. Le co-management consiste à laisser aux entreprises le choix du niveau de management qu'elles veulent assurer elles-mêmes ou confier aux experts Linkt.

L'offre se décline en différentes possibilités. Une version Avantage permet d'avoir accès à des fonctionnalités prédéfinies et Premium, qui propose de choisir avec le conseil d'experts Linkt des fonctionnalités sur-mesure.

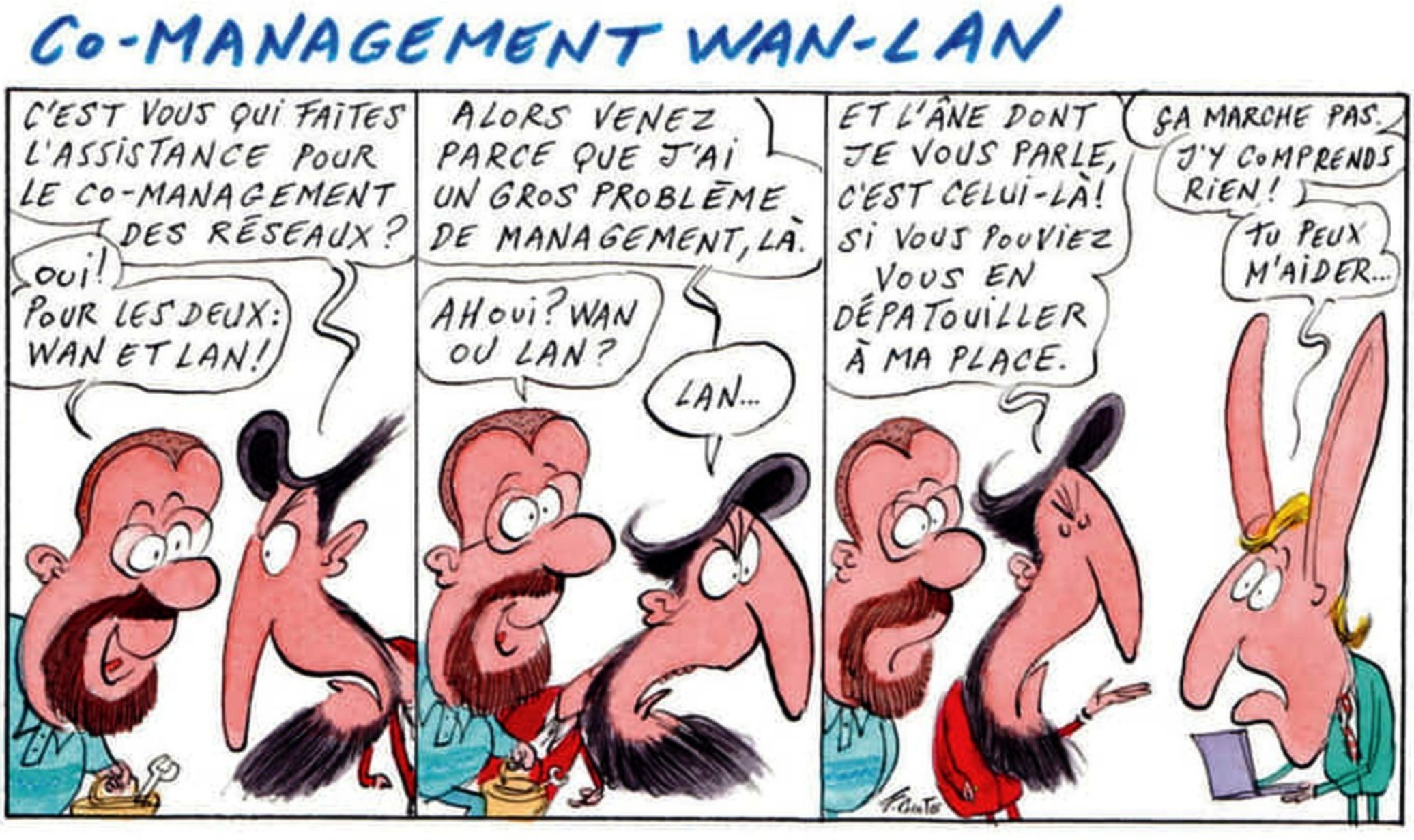
Un complément de l'offre SD-WAN

Cette offre WiFi suit de près l'annonce d'un service managé de SD-WAN appelé « Connectivité Augmentée », et ambitionne de réinventer le modèle d'interconnexion des différents sites d'une même entreprise. Accessible aux grandes entreprises comme aux ETI, l'offre apporte une connectivité performante, résiliente, et propose aux responsables SI et réseaux un pilotage personnalisé de leur réseau. L'offre Connectivité Augmentée de Linkt consiste tout d'abord à associer ces avantages du SD-WAN au modèle « agrégateur d'infrastructures » de Linkt, et ainsi, proposer ces services sur des liens (FFTO, FTTH, 4G/5G, xDSL) de dizaines d'opérateurs d'infrastructures avec lesquels Linkt est interconnecté.

Là encore, la solution se décline en différentes versions (Essentiel, Avantage, Premium) permettant aux entreprises de choisir à la fois le niveau fonctionnel le plus adapté à leurs besoins métiers, et les services managés les plus complémentaires à leur organisation.

Le principal bénéfice de l'offre est de gagner en consommation de bande Internet. Elle garantit, tout comme un VPN MPLS classique, des temps de latence identiques d'un site à l'autre. L'offre permet d'unifier l'intégralité des connexions au réseau : qu'elles soient fibre optique, ADSL, 4G ou encore 5G. Cet équipement intelligent va également répartir de façon optimale le trafic présent sur le réseau et ainsi, augmenter la productivité.

B.G



SecOps

Sécuriser les environnements industriels : la mission de TXOne

TXOne Networks est une entreprise filiale de Trend Micro qui travaille en collaboration avec les principaux fabricants et opérateurs d'infrastructures critiques afin de développer des approches pratiques en matière de cyberdéfense pour les équipements industriels.

Initialement, TXOne a été fondée sur le développement de semi-conducteurs. Puis, l'entreprise a développé une approche OT Zero Trust afin d'aller au-delà de la cyberdéfense traditionnelle pour rationaliser la gestion et protéger les environnements critiques industriels et ainsi réduire les frais de sécurité. TXOne Networks équipe aujourd'hui plus de 3600 entreprises dans le monde dans les secteurs suivants : automobile, santé & pharmacie, énergie, transports, électronique, aérospatial,...


Le Portable Inspector de TXOne.

Les systèmes d'encaissements, d'affichage et, de manière générale, l'ensemble des automates avec lesquels la population interagit quotidiennement sont des appareils susceptibles d'utiliser les technologies proposées par TXOne Networks.

Les fondements de toute usine intelligente reposent sur la collecte, le partage et l'analyse des données, qui sont souvent compliqués par l'inclusion d'actifs provenant d'un éventail divers de fabricants travaillant dans un large éventail de conditions et de situations. En utilisant l'approche OT Zero Trust, le principe de fonctionnement de TXOne est d'inspecter les actifs dès leur arrivée et segmenter le réseau afin de sécuriser le flux de données au niveau de l'atelier (données utilisées, données en transmission et données au repos). La technologie native OT aide les techniciens à gérer de manière centralisée la cyberdéfense d'un grand nombre d'actifs anciens et modernes fonctionnant côte à côte sans interrompre les opérations.

Les solutions TXOne fonctionnent sur 3 paliers distincts

Le premier consiste à inspecter les appareils, sans installation d'une application. Par exemple, il peut s'agir d'une clé USB contenant un jeu de diodes à 3 couleurs qui indiqueront une situation bonne, moyenne ou mauvaise. Comme le décrit Maxime Wiart, directeur Europe du Sud de TXOne : *« c'est un produit étonnant dans la mesure où il responsabilise les utilisateurs, et ce de manière très simple. Ces outils sont particulièrement utiles pour des machines-outils qui n'ont pas embarqué une dimension de cybersécurité lors de leur conception. »*

Le 2ème axe consiste à adresser des anciens PC fonctionnant sous Windows XP, voire des versions antérieures, équipés de ports série plutôt que de ports USB. TXOne intervient alors en mettant « sous cloche » ces environnements au travers d'un logiciel développé par l'entreprise.

La solution vise des matériels plus récents mais dans lesquels il est impossible d'installer des logiciels sous peine de faire sauter la garantie du constructeur. Dans ce cas, TXOne installe un boîtier externe qui analyse et filtre les informations qui vont et viennent de l'automate. Ce sont par exemple des machines-outils pilotées par des automates industriels pour lesquels il devient possible de remédier à une faille et ne pas uniquement alerter.

De manière plus générale, TXOne est un acteur silencieux de la sécurité des environnements industriels qui touchent les consommateurs finaux, ces derniers n'ayant aucune connaissance du rôle joué par un acteur tel que celui-là. □

S.L

www.linformaticien.com

ABONNEZ-VOUS À L'INFORMATICIEN

linformaticien.com/abonnement

MAGAZINE

Recevez chaque mois (10 numéros par an) le magazine «papier» et accédez également aux versions numériques.

1 AN FRANCE : 72 €
2 ANS FRANCE : 135 €
1 AN UE : 90 €
2 ANS UE : 171 €
1 AN HORS UE : 108 €
2 ANS HORS UE : 207 €

NUMÉRIQUE

Accédez chaque mois (10 numéros par an) à la version numérique du magazine et retrouvez également via votre compte en ligne les versions numériques des dernières publications.

1 AN : 49 €
2 ANS : 89 €

Une **offre triple** pour ne rien manquer des dernières tendances et innovations

ÉTUDIANT / ÉCOLE

Abonnez vos étudiants avec une formule dédiée à 60 % du prix normal de l'abonnement sous forme de PDF (10 numéros par an).
Possibilité abonnements groupés en contactant le service abonnements du magazine à abonnements@linformaticien.com.

ABONNEMENT 1 AN : 43, 20 €

Bonnes pratiques

Gen AI, un déploiement sous haute surveillance

Les entreprises désireuses d'implémenter les nouveaux outils d'intelligence artificielle générative (Gen AI) doivent s'inscrire dans une démarche d'apprentissage, d'expérimentation et d'appropriation. Un processus indispensable pour mieux maîtriser les coûts et les risques associés. Explications.

Toutes les sociétés d'études IT confirment l'engouement massif, mais prudent, des entreprises pour les nouveaux outils d'intelligence artificielle, générative (GenAI) notamment. Selon Gartner, environ 80 % des organisations l'auront utilisé d'ici 2026, sous forme d'interfaces de programmation d'applications (API) ou de modèles, et/ou déployé des applications basées dans des environnements de production..., contre moins de 5 % en 2023.

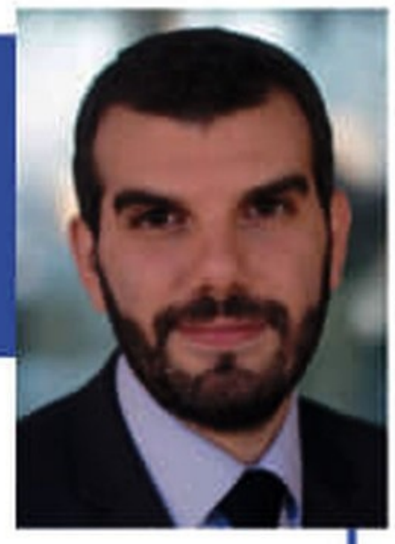
Le déploiement dans une entreprise d'une application de Gen AI est-il très différent de celle d'un progiciel, de type ERP ou CRM par exemple ? La réponse varie beaucoup en fonction de la qualité des données disponibles et de leur intégration dans des solutions BtoB déjà déployées.

Créer un responsable Gen AI ou une "AI Tower"

Avant même de choisir une application de Gen AI ou de la déployer, la société devra nommer un chef de projet, issu ou pas de la DSI, quand elle existe. Il ou elle rapportera aussi probablement à la direction générale, dont l'implication est nécessaire pour embarquer et responsabiliser les métiers. Sa mission : mener en amont du déploiement une étude — avec ou sans l'aide d'une ESN — sur leurs besoins, les moyens disponibles, les finalités, *etc.*

Le Cigref indique que des *« entreprises ont aussi mis en place un comité transverse et pluridisciplinaire aussi appelé "AI Tower", ou encore "Generative AI committee", pour suivre et valider les différents cas d'usage d'IA génératives et LLM dans l'entreprise, comme cela a été fait pour la data, et maintenir à jour les recommandations et réponses aux FAQ (questions fréquemment posées) »*.

Ce comité peut répertorier les besoins spécifiques de chacun des métiers et les aligner, de manière réaliste, face à des cas d'usage potentiels autour de la Gen AI. En effet, les fonctionnalités et résultats recherchés (génération de rapports, de messages marketing, de code, *etc.*), diffèrent entre les divisions marketing et commercial par exemple. Tout comme la nature des données à y entrer.



Chadi Hantouche, partenaire spécialisé en AI de la société de conseil Wavestone.

« Certaines entreprises ne vont pas généraliser l'accès de ces outils à tous leurs salariés. »

La qualité de vos données est-elle suffisante ?

Avant même d'envisager de connecter ces outils à leurs progiciels ou au CRM par exemple, un soin tout particulier doit donc être porté aux données qui alimenteront leurs outils d'intelligence artificielle afin de limiter les risques, déjà élevés, d'erreur ou d'hallucination dans les réponses. Si la DSI ne la possède pas encore, chaque département devra aussi fournir au chef de projet la liste, la qualité et le format des données disponibles à entrer dans l'outil en y ajoutant, si besoin, un classement en fonction de leur niveau de confidentialité.

Certaines sociétés réaliseront alors (enfin) que leurs bases de données existantes ne sont toujours pas assez qualifiées... Leurs données ne sont ni suffisamment bien structurées, ni même compatibles RGPD peut-être, pour alimenter correctement leur Gen AI, ou un projet de CRM ou de Big Data *a fortiori*.

Au nom du mantra *« shit in / shit out »* bien connu dans le secteur, il est préférable que les DSI reportent leurs projets afin de limiter les risques. Ils inviteront également les entreprises, avant tout déploiement, à amender, au moins *a minima*, leur plan de gouvernance des données, si elles en ont un, ou d'en créer un d'urgence sinon.

Chadi Hantouche, un partenaire spécialisé en AI de la société de conseil Wavestone, conseille aussi aux sociétés d'expérimenter à petite échelle ces Gen AI, pour des questions de coûts et de sécurité notamment. *« Certaines entreprises ne*

veulent pas forcément généraliser l'accès de ces outils à tous leurs salariés. Elles vont sélectionner certaines populations et leur donner des accès en fonction de leurs besoins ». Il est donc préférable de ne déployer ces Gen AI que sur certains cas d'usage bien bordés par le chef de projet avec les métiers, dans un nombre limité de départements, et sur un panel présélectionné en amont. La DSI peut ainsi identifier plus facilement leur potentiel, l'accueil que leur réservent les collaborateurs, mais aussi leurs limites.

Brider l'accès aux outils de Gen AI augmentera le « shadow IT »

Le choix de limiter l'accès à la Gen AI augmentera-t-il les risques, déjà élevés, d'utilisation « sauvage », dîtes « shadow IT » ? C'est possible selon Chadi Hantouche : *« l'outil amène un tel potentiel aux métiers que certains directeurs de divisions ont peut-être déjà décidé de passer outre la politique de la DSI pour tester ou déployer un ChatGPT Entreprise par exemple »*.

Henri d'Agrain, le délégué général du Cigref, estime qu'il est illusoire de croire que la DSI ou la DG pourront empêcher l'utilisation de ces Gen AI à des collaborateurs qui emploient déjà ChatGPT, ou l'un de ses concurrents, à titre personnel : *« les DSI du Cigref estiment qu'aucune digue ne pourra nous prémunir contre cette vague technologique, car les outils de Gen AI sont là pour longtemps. Au contraire, il faut mettre en œuvre des méthodes et démarches d'appropriation par les métiers et de leur fournir des outils performants permettant de limiter les risques ensemble, qui sont assez nombreux »*.

Acculturer les collaborateurs aux usages BtoB et sécurisés

Le Cigref conseille aux DSI, dans un rapport sur la Gen AI paru en 2023, *« d'évaluer la maturité de l'ensemble des équipes sur la data et les IA afin d'adapter au mieux la communication et la formation à mettre en œuvre »*. En effet, il est primordial d'acculturer et former les collaborateurs aux usages BtoB des outils d'IA générative, ne serait-ce que pour les informer et démystifier les applications farfelues ou

Guillaume Gérard, responsable des solutions de Gen IA en Europe du sud de l'ESN Capgemini.

« L'utilisation du langage naturel facilite déjà l'appropriation des Gen AI par les métiers. »

Henri d'Agrain, délégué général du Cigref, l'association des grandes DSI.

« Aucune digue ne pourra nous prémunir contre cette vague technologique. »

risquées qui traînent sur les réseaux sociaux. Le comité exécutif est la première cible.

Mais, la formation en profondeur des collaborateurs aux outils de Gen AI est-elle bien nécessaire, sachant que nombre d'entre eux les ont déjà testé à titre personnel ? Selon une enquête de Statista, réalisée en 2023 aux États-Unis, 29 % des répondants de la génération Z ont déjà utilisé ces outils, contre 28 % de la génération X, et 27 % pour les millennials.

La plupart des intervenants interrogés, dont François Familiari, responsable des ventes en Europe du sud de Zoom, estiment que *« la Gen AI ne nécessite pas de formation spécifique des utilisateurs, sauf sur la partie relations avec les utilisateurs »*. Guillaume Gérard, responsable des solutions de Gen IA en Europe du sud de Capgemini, encourage surtout les entreprises à développer *« une culture de l'accompagnement au changement, car l'utilisation du langage naturel facilite déjà l'appropriation des Gen AI par les métiers »*.

Qualifier les prompts et les POC

En revanche, il peut s'avérer utile de former les personnels à la définition de requêtes ou de prompts plus qualifiés et sécurisés, permettant ainsi à l'entreprise d'obtenir des réponses ou du code de meilleure qualité, et sans dévoiler ses données critiques à l'extérieur. *« Chez Databricks, nous organisons beaucoup de hackathon sur le code afin de montrer les cas usages et les meilleures pratiques avec la Gen AI »*, explique Nicolas Maillard, responsable avant-vente en Europe du sud de cet éditeur de logiciels.

Enfin, les équipes pluridisciplinaires devront plancher sur l'industrialisation des PoC en cas de succès. Le Cigref leur conseille de *« déterminer des indicateurs/critères pour en évaluer les réels bénéfices, que ce soit d'un point de vue quantitatif ou qualitatif, dans l'objectif de les pérenniser au niveau de l'organisation »*. Enfin, il invite les DSI à déployer un comité qui évalue l'éthique des projets, analyse les possibles biais ou résultats erronés et définit le contour et les fonctionnalités du produit qu'on veut créer, ainsi que le cadre juridique, voire son impact Responsabilité Sociétale des Entreprises. □

Olivier Bellin

Oracle CloudWorld 2023

L'IA et le Cloud au cœur des débats

La manifestation géante d'Oracle a débuté avec deux sessions générales notables, celle de Safra Catz, la CEO de l'éditeur, et celle de l'emblématique CTO, Larry Ellison. Ces interventions avaient en commun de mettre en avant les changements qu'induisaient les nouvelles technologies dont l'intelligence artificielle. Larry Ellison a ainsi dressé le tableau d'innovations dignes des meilleurs romans d'Isaac Asimov.

Dans sa session d'ouverture, Safra Catz a rendu hommage au courage de se lancer dans une transformation profonde pour une entreprise et les risques pris à ce moment-là. Elle a aussi insisté sur les bénéfices que peuvent en tirer les entreprises quand le projet est mené à bien. De nombreux clients d'importance comme Uber ou Aon ont ainsi détaillé comment ils ont profité des apports d'Oracle pour leurs affaires et comment ils se sont profondément transformés avec le Cloud et les outils applicatifs d'Oracle.


Larry Ellison lors de son keynote sur OCW 2023.

Une vision du futur

Larry Ellison, pour sa part, a donné la vision stratégique que va suivre l'éditeur dans ses produits. Celle-ci reposera désormais fondamentalement sur l'intelligence artificielle générative qui va être omniprésente dans la pile logicielle et l'infrastructure d'Oracle. Pour lui *« GenAI change tout »*. Il prévoit ainsi une course vers l'amélioration de cette technologie qui de balbutiante devient *« un bébé qui parle »* et qui va vite marcher pour se lancer sur le chemin de son futur qui apportera des possibilités extraordinaires dans la médecine, l'agriculture et bien d'autres secteurs. Ainsi, il prévoit que, rapidement, les voitures autonomes seront largement disponibles, que la découverte de nouveaux traitements antiviraux verront le jour en quelques jours et non plus des semaines, que des assistants digitaux vocaux vont permettre d'échanger entre médecin et patients sans avoir à traduire les différentes langues dans la conversation entre eux... Toutes ces innovations sont des projets développés par Oracle avec des clients partenaires. Ainsi, il a cité le projet déjà en place de Cerner Millennium qui vise transformer profondément le secteur de la santé avec l'apport de l'intelligence artificielle afin de fournir des diagnostics plus rapidement sur les cancers ou autres pathologies de ce type, de développer des traitements contre les virus et d'apporter une expérience de qualité tout au long de la chaîne, du patient au praticien en passant par le payeur pour simplifier ce processus complexe du parcours de soins.

Le plus spectaculaire a été certainement la présentation d'un projet de fermes hydroponiques très proches de ce que l'on peut voir dans les romans d'Isaac Asimov afin de créer des aliments plus sains. Cette start-up, Sensei, bénéficie du financement direct de Larry Ellison, L'idée est de faire pousser les végétaux dans de l'eau et non le sol avec des ajouts de nutriments pour renforcer la valeur nutritive des aliments. Des études américaines

démontrent que les aliments ont perdu 30 % de leur valeur nutritive depuis 1950. Du fait du changement climatique, des aliments comme le riz ou le blé pourraient perdre de 20 à 30 % de leurs protéines. Cette baisse n'est pas sans conséquence, et il est possible que certaines populations connaissent des carences en zinc et en fer.

Larry Ellison veut voir le côté positif de l'IA et de ce qu'elle peut apporter pour le meilleur. Il est évident que l'intelligence artificielle générative apporte un véritable tournant technologique et n'en est qu'à ses débuts. Comme toute technologie, elle deviendra ce que les humains voudront en faire.

L'IA générative et le Cloud comme cap

Lors de l'événement, Oracle a présenté l'ajout de fonctionnalités de recherche sémantique basées sur des vecteurs d'IA dans Oracle Database 23c, notamment AI Vector Search pour stocker et interroger des données non structurées sous forme de vecteurs, ainsi que la prise en charge de la génération augmentée de récupération (RAG) pour des réponses précises en langage naturel, sans exposer de données privées. De plus, de nouvelles instances Oracle Cloud Infrastructure (OCI) Compute avec des processeurs graphiques NVIDIA Tensor Core H100, L40S et des processeurs Ampere AmpereOneTM, offriront des performances améliorées pour une variété de workloads cloud, y compris l'IA et le transcodage vidéo.

Pour le cloud, Oracle élargit son offre de cloud distribué pour s'adapter aux besoins variés des entreprises et à la demande mondiale croissante de services Oracle Cloud Infrastructure (OCI), offrant des solutions telles qu'Oracle Database@ Azure et MySQL HeatWave Lakehouse sur AWS, tout en renforçant son partenariat avec Oracle Alloy pour une adoption accrue de sa stratégie de cloud distribué par des partenaires internationaux.

Une mise à jour d'Oracle Access Governance vise à améliorer la gestion des accès des utilisateurs aux applications et aux ressources techniques, offrant une visibilité détaillée et une réduction des risques en garantissant que seuls les utilisateurs autorisés peuvent interagir avec des ressources restreintes, y compris le code source, les brevets, les bases de données et les infrastructures cloud.

Des partenariats renforcés

Red Hat et Oracle élargissent leur alliance pour offrir à leurs clients davantage de choix lors du déploiement d'applications sur Oracle Cloud Infrastructure (OCI), avec la certification et la prise en charge de Red Hat OpenShift, la plateforme d'applications cloud hybrides basée sur Kubernetes. Cette collaboration renforcée permettra aux clients de bénéficier d'une solution de déploiement d'applications natives du cloud sur OCI.

Le partenariat avec Ampere va proposer des instances nouvelles offrant jusqu'à 44 % de rapport prix-performance comparé aux offres x86 et sont idéales pour l'inférence IA, les bases de données, les services web, les charges de travail de transcodage de supports et la prise en charge des langages de programmation, tels que GO et Java. Les deux entreprises ont également annoncé l'arrivée de nouveaux clients pour les services OCI basés sur Ampere, ainsi que l'adoption des solutions Ampere pour les applications Oracle Fusion Cloud. Les quelques centaines de services OCI fonctionneront désormais sur des processeurs Ampere. □

B.G

CLOUDWORLD ET FRENCHCLOUD

SuiteWorld

Moins d'efforts et plus d'efficacité

Pour son 25ème anniversaire, Oracle NetSuite a réuni ses clients et sa communauté à Las Vegas pour faire de nombreuses annonces. Comme souvent maintenant, l'intelligence artificielle était au cœur des nouvelles fonctionnalités présentées.

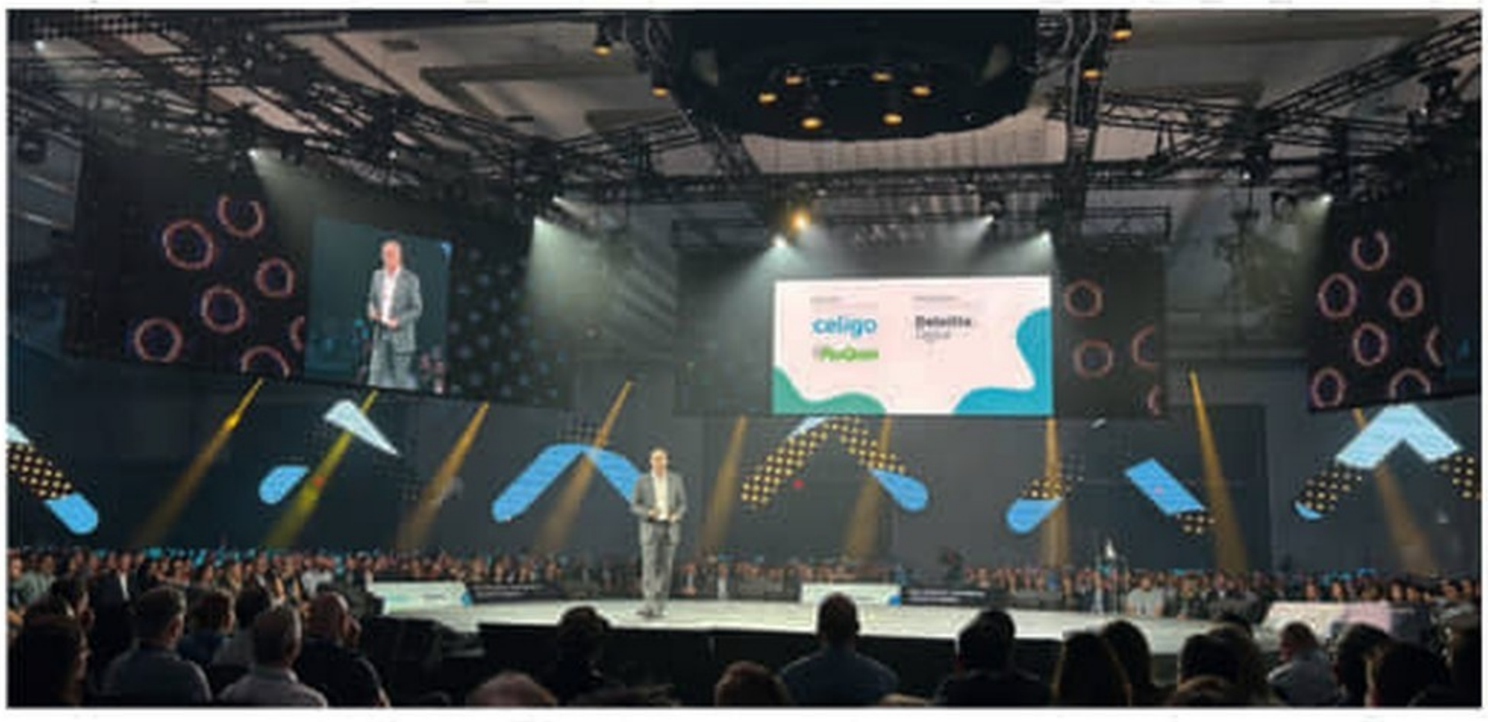
Dans les prochains mois, l'entreprise introduira NetSuite Text Enhance, basé sur l'intelligence artificielle générative. Grâce à quelques mots de départ, Text Enhance décrira les intentions d'un client et lui fournira une assistance pour la réalisation de tâches comme les rapports financiers ou pour la chaîne d'approvisionnement. De nombreuses autres fonctionnalités ont également été annoncées avec comme point commun la réduction des efforts pour une meilleure efficacité. Toutes ces annonces avaient pour point commun d'aider les clients à réduire les coûts tout en fonctionnant de manière plus simple et efficace. Plus de 6 500 personnes avaient fait le déplacement pour en savoir plus. Les dernières innovations comprennent des capacités alimentées par l'intelligence artificielle dans l'ensemble de NetSuite ainsi que de nouvelles solutions de gestion des services sur le terrain et de gestion des performances de l'entreprise (EPM). Ce n'est pas tout puisque les développeurs ont aussi apporté des améliorations pour les entreprises spécialisées dans la finance, la relation client et l'industrie. Comme le rappelle d'ailleurs Ham Patel, directeur opérationnel EMEA, la grande majorité des clients de l'éditeur est issue de la finance et des services. L'intelligence artificielle générative s'intègre encore plus dans la suite afin que les 37 000 clients d'Oracle NetSuite améliorent la planification et la budgétisation, éliminent la saisie manuelle des données et développent les perspectives commerciales de leur société.

Simplifier les tâches des utilisateurs

Dans un but de simplification et d'amélioration de la productivité, NetSuite a donc accru l'intégration de l'intelligence artificielle dans sa solution. Cela se traduit directement sur NetSuite Text Enhance qui, alimenté par l'intelligence artificielle générative avec Oracle Cloud Infrastructure (OCI) et les modèles de langage de Cohere, permet aux utilisateurs de créer un contenu contextuel et personnalisé pour n'importe quelle zone de texte dans NetSuite. Cette fonctionnalité est très intéressante puisqu'avec quelques mots de départ décrivant l'intention, NetSuite Text Enhance s'adresse directement à de nombreux départements d'une entreprise (finance, comptabilité, ressources humaines, chaîne d'approvisionnement, ventes et marketing). Pour en mesurer les avantages sur la chaîne d'approvisionnement, les équipes pourront, par exemple, générer des bons de commande et des lettres de demande, élaborer des courriers personnalisés pour les fournisseurs ou mettre à jour les calendriers de livraison et la création de descriptions de produits utilisés par les autres départements concernés. Quant au service support, NetSuite Text Enhance pourra générer des réponses suite aux commentaires des clients en ligne. Le but est d'augmenter la productivité des agents et offrir une meilleure expérience aux clients. *« Les nouvelles capacités de NetSuite Text Enhance ne sont qu'un début, et nous continuerons aussi à intégrer de puissantes capacités d'intelligence artificielle dans l'ensemble de NetSuite »*, a déclaré Evan Goldberg, cofondateur et vice-président exécutif d'Oracle NetSuite. D'abord disponible en anglais, cette fonctionnalité devrait intégrer de nouvelles langues.

De nombreuses nouvelles fonctionnalités

Outre la présentation de NetSuite Text Enhance, l'ensemble des fonctionnalités de NetSuite est boosté par l'intelligence artificielle. Il sera trop long d'en faire le détail complet, mais certaines fonctionnalités viennent



Evan Goldberg, cofondateur et vice-président exécutif d'Oracle NetSuite, a effectué seul un keynote durant lequel il a balayé l'ensemble des nouveautés de NetSuite. Il s'est longuement attardé sur NetSuite Text Enhance, l'une des principales annonces de SuiteWorld 2023.

De nombreux partenaires et clients d'Oracle NetSuite étaient réunis dans l'espace d'exposition de SuiteWorld 2023.

en soutien de l'amélioration des performances d'une entreprise comme c'est le cas avec NetSuite Enterprise Performance Management. Cet ensemble intégré de solutions financières relie la planification financière et opérationnelle, automatise le rapprochement des comptes, rationalise les processus de clôture et améliore les rapports fiscaux. Autre nouveauté : NetSuite Capital. Ce nouveau service a vocation à aider les utilisateurs à mieux gérer les flux de trésorerie et réduire les délais de recouvrement des créances. Comme l'a expliqué Evan Goldberg, un tel outil permettra aux entreprises d'accélérer les paiements et augmenter ainsi leur fonds de roulement, qui est le nerf de la guerre pour une société.

À cela, il faut aussi ajouter NetSuite Electronic Invoicing. Cette solution de facturation électronique aide les entreprises à optimiser les paiements et les encaissements, à réduire les coûts et à rationaliser la conformité de la facturation en fonction des règles comptables des différents pays. En restant dans le domaine de la facturation, NetSuite Bill Capture démontre tout l'intérêt de l'utilisation de l'intelligence artificielle par NetSuite. Avec ce logiciel, les clients peuvent éliminer la saisie manuelle des factures et augmenter la productivité des équipes comptables. *« Grâce à l'intelligence artificielle, NetSuite Bill Capture enregistre tous les détails de chaque facture et vient les reconnaître pour les classer directement »*, a précisé Evan Goldberg. On notera aussi que pour la partie EPM, la fonction Corporate Tax Reporting permettra aux entreprises d'automatiser les processus de déclaration fiscale et, pour celles qui ont des activités multinationales, de se conformer aux nouvelles obligations de déclaration des pays membres de l'OCDE.

Mieux comprendre un secteur d'activité

Toujours dans le but de simplifier le travail des entreprises et de favoriser l'accroissement de leur activité, NetSuite a créé le nouvel outil NetSuite Benchmark 360. Cette fonctionnalité permet aux clients d'analyser les informations opérationnelles et financières clés afin de mieux comprendre comment leurs structures se comportent par rapport à des organisations similaires dans leur secteur d'activité et leur région. Toutes les informations récoltées apparaissent dans un tableau de bord récapitulatif. *« Cela permet aux utilisateurs de comparer leurs performances par rapport à leurs homologues dans le même secteur industriel et dans leurs régions. Ainsi, ils reçoivent des recommandations générées automatiquement par l'intelligence »*, a commenté Evan Goldberg. Pour obtenir ces informations capitales pour le développement d'une entreprise, NetSuite Benchmark 360 vient agréger les données des clients de NetSuite, avec leur autorisation explicite bien entendu. *« Cela représente des milliers de données et cela permet aux clients d'apprendre grâce à l'expérience des autres clients »*, a complété Bec Vaughan, directrice des produits management de NetSuite.

Pour finir, NetSuite introduit également un nouveau modèle de licence qui permettra aux clients d'obtenir des licences spécifiques pour les employés qui n'ont pas besoin d'un accès complet au logiciel. L'exemple d'un employé travaillant dans un entrepôt est révélateur de l'utilité de ce modèle. En effet, ce dernier pourra uniquement se servir des modules NetSuite pour la réception des produits, l'entrée en stock, la préparation des commandes et l'expédition. Avec cela, les clients pourront dès lors réduire leurs coûts en utilisant seulement ce dont ils ont besoin. Dans un premier temps, ce nouveau mode de fonctionnement sera disponible pour NetSuite Warehouse Management. Pour le reste, la plupart des nouvelles fonctionnalités sont d'ores et déjà disponibles. NetSuite Text Enhance sera lancé dans les six prochains mois. □

Michel Chotard

SAP Une convention USF animée

La cuvée 2023 de l'association française des utilisateurs de SAP a été l'occasion pour des dizaines d'entreprises de présenter leurs projets vers S/4HANA et, pour l'éditeur, de présenter sa roadmap. Les relations avec ce dernier restent en demi-teinte. Dernier caillou dans la chaussure, les clients français de la version sur site ont reçu fin août un courrier leur imposant une hausse de 5 % sur la maintenance.

La dernière édition de la convention a vu passer environ 1850 visiteurs les 11 et 12 octobre dernier. Si la fréquentation était au rendez-vous, les relations avec l'éditeur allemand sont toujours en dents de scie. Dernier caillou dans la chaussure, les utilisateurs français d'ECC 6 vont devoir payer une augmentation de 5 % pour continuer à bénéficier de la maintenance. Inflation moindre oblige, le chiffre est un peu moins élevé en Suisse. Une majoration contractuelle, a souligné la direction de l'éditeur présente sur le salon. ECC ne sera mis à jour que pour suivre les évolutions réglementaires jusqu'à la fin annoncée de sa maintenance, 2027 ou 2030 en option. Une bonne partie des adhérents de l'USF continuent à utiliser cette version de l'ERP.

Olivier Nollent, PDG SAP France, Gianmaria Pérancin, Président de l'USF et du Sugen.

Côté S/4HANA, les déclarations en août de Christian Klein, PDG monde de l'éditeur, ont également suscité un certain émoi. Le dirigeant a déclaré que seules les versions cloud, public et privé, de S/4HANA bénéficieraient d'innovations comme Green Ledger, ce qui exclut la version sur site. Une manière peu amène de pousser toujours plus ses clients vers le cloud. L'USF n'a pas été la seule à réagir. Fin septembre, forte de ses quelques 30 000 membres, l'association allemande DSAG a demandé que toutes les innovations soient portées dans toutes les versions de S/4HANA. *« Une stratégie cloud-only n'est pas une option »*, a résumé son président. *« L'éditeur ne peut pas imposer sa roadmap »*, a assené de son côté Gianmaria Pérancin, président de l'USF et du Sugen[1], lors de la plénière de la convention.

Pour les entreprises qui en font le choix, le cloud suppose une autre contrainte. Si ce n'est pas une obligation, le passage à S/4HANA suppose de recourir à des fournisseurs certifiés par l'éditeur pour bénéficier de toutes les garanties. Sans surprise, les trois « hyperscalers » sont dans la liste à côté d'IBM et de quelques datacenters de l'éditeur. L'USF demande un élargissement de cette liste à des acteurs comme Bleu (Orange, Capgemini et MS Azure), à S3NS (Thales et Google Cloud) ou encore, à OVHcloud, *« des solutions qui pourraient répondre à la question du cloud de confiance »*, a souligné Gianmaria Perancin. De fait, OVHcloud propose déjà une offre SAP dans le cadre d'une solution de *« partenaire ordinaire »* pas certifiée. Comme pour les autres alternatives, certifier celle-ci pour le programme Rise, le programme d'accompagnement vers le cloud, serait un investissement important, considère l'éditeur, détaillant que, outre l'infrastructure, le code est inclus dans cette certification. Plus globalement, SAP avance que les coûts liés à la certification de chaque environnement sont trop onéreux et, pour les limiter, milite en faveur d'une norme européenne de cloud sécurisé, qui serait l'équivalent de SecNumCloud. *« Il ne faut pas oublier que SAP maintient huit versions de son ERP »*, a ajouté Olivier Nollent, PDG de la filiale française. Et pour enfoncer le clou, il a insisté : *« les innovations de rupture nécessitent le passage sur le cloud »*. Malgré ces freins, SAP avance qu'environ un tiers de sa base installée en France a initié un projet vers S/4HANA.

Autre point en suspens, l'IA, en particulier sa déclinaison générative, a fait l'objet d'annonces de SAP. Elle prendra la forme d'un assistant, baptisé Joule, accessible dans de nombreux applicatifs à partir d'un simple clic, pour *« optimiser »* les processus, comprendre et générer des devis par exemple. À titre personnel, Gianmaria Pérancin considère que cette technologie n'a pas fait la preuve de sa maturité. *« Elle peut inventer des sources »*, a-t-il illustré. Un groupe de travail de l'USF devrait prochainement être constitué pour se pencher sur le sujet. Dernier grand sujet d'actualité pour les entreprises comme pour l'éditeur, la *« durabilité ou sustainabilité »*, qui a fait l'objet de plusieurs réactions. Une préoccupation liée à la réglementation. Depuis cette année, les entreprises de plus de 500 salariés sont tenues de mesurer leurs émissions de gaz à effet de serre (GES) pour le scope 3. Ce dernier niveau recouvre les émissions indirectes, par exemple, celles liées à la production des matières premières achetées par l'entreprise, ou encore au transport des marchandises. Une sinécure pour les organisations, pas moins de 1100 critères sont à prendre en compte. La solution de SAP, Green Ledger, ne suffit pas. Bernard Cottinaud, vice-président stratégie de l'USF, a avancé : *« SAP a une belle carte à jouer parce que ses ERP voient passer toutes les données financières. »* Au final, toujours beaucoup de questions en suspens. □

Pbr

1 : Le Sugen — SAP User-Group Executive Network — regroupe 21 associations d'utilisateurs au niveau mondial. Elle ne compte ni l'Allemagne ni les États-Unis. Elle est également présidée par Gianmaria Perancin.

LE SALON ONE TO ONE MEETINGS DES RÉSEAUX, DU CLOUD, DE LA MOBILITÉ ET DE LA CYBERSÉCURITÉ

IT AND CYBERSECURITY

MEETINGS BY WEYOU GROUP

WWW.IT-AND-CYBERSECURITY-MEETINGS.COM

19, 20 & 21 MARS 2024

PALAIS DES FESTIVALS ET DES CONGRÈS DE CANNES

ILS SONT DÉJÀ INSCRITS

6cure, adista, AISI, allentis, alt/nativ, APIXIT, aqua, arcserve, ARMIS, BCS Solutions, betoobe, BeyondTrust, Bitdefender, BlackBerry Cybersecurity, BlueFiles, BlueTrusty, board of cyber, bso, CATO, cegedim, ClariLog, CLOUDFLARE, COHESITY, conecto, CROWDSTRIKE, CRYPTOBOX, cybereason, Cyberwatch, CYBLEX, DESCRYPTA, DATACORE, Delinea, DIGITAL REALITY, dust, EASYVISTA, EATON, efficient IP, EGERIE, EPOS, ERCOM, eset, EV Observe, exabeam, Tenable, EXCUBE, FILIGRAN, Forcepoint, FORTINET, GAT MALWARE, GitGuardian, CONVERGENCE, HarfangLab, HEXANET, HUMAN, iLex, INFINIGATE, IRON MOUNTAIN, ITS Telcom, Jabra, juniper, KADISKA, KDDI, Linkt, Lutessa, MAKE IT SAFE, ManageEngine, MANAGETAN, MITEL, MY, nameshield, NeoVAD, netskope, NOZOMI, OPEN DOOR OPEN, okta, ONE IDENTITY, opentext Cybersecurity, Orange Cyberdefense, OVERSOC, OWN, Patrowl, PENTERA, Ping, platform.sh, pradeo, PRIMX, proofpoint, PURE STORAGE, pythea, Qualys, radware, RingCentral, Riot, rubycat, SailPoint, sea tpi, SentinelOne, sewan, Skyhigh, SOPHOS, sosafe, STORMSHIELD, Suricate, synetis, TANIUM, TDF, TERREGOV, TELEHOUSE, Tenacy, TrustHQ, TrustBuilder, TYREX, UBIKA, vade, VARONIS, WAVESTONE, WITH, xmco, ZeroTrust, Zerto, zpe

by weyou group

Professional Exhibitions and One to One Meetings Exhibitions

Communauté

Une édition 2023 contrastée pour l'Open source Summit Europe

L'évènement de Linux s'est tenu à Bilbao entre les 19 et 21 septembre dernier. Derrière le dynamisme du monde open source, plusieurs gros nuages sont (re)apparus.

Le Summit s'est déroulé autour de plusieurs thématiques d'actualité comme l'IA, avec l'Open AI & Data Forum, le cloud, avec le CloudOpen et l'Emerging OS Forum. Sans surprise, les organisateurs avaient aussi prévu une conférence pour présenter les solutions technologiques susceptibles de décarboner l'économie. Côté pile, il a été l'occasion de souligner l'importance économique du domaine en Europe. Publié par The Linux Foundation Research, le rapport *« World of Open Source : Europe Spotlight 2022 »* a souligné l'importance croissante des logiciels open source en Europe. Ce secteur est considéré comme vital pour l'avenir de l'industrie par 91 % des personnes interrogées. Petit bémol, dans le secteur public, la valeur perçue tirée des logiciels open source semble avoir stagné depuis l'année dernière. 53 % des répondants indiquant qu'elle n'a pas évolué, contre seulement 25 % dans les autres secteurs. Sujet plus satisfaisant : le dynamisme des communautés de développeurs. Directeur principal, et chargé du développement de la communauté Mirko Boehm a illustré : *« certaines communautés au sein de la Fondation Linux comptent un nombre important de projets et de contributeurs. La Cloud Native Computing Foundation, par exemple, héberge 164 projets et 215 000 contributeurs venant de 190 pays, réunissant environ 14,4 millions de contributions. »* Parmi ces projets, et bien qu'il n'existe pas encore, à ce jour, de définition concrète « open source », l'intelligence artificielle a fait l'objet d'une attention particulière. *« Nous avons annoncé le lancement du Generative AI Commons, destiné à promouvoir les technologies d'IA générative open source, notamment les Large Language Models (LLM), grâce à une gouvernance neutre et de confiance et à une collaboration transparente »*, a décrit Mirko Boehm. L'événement a aussi été l'occasion pour Fujitsu de renforcer son positionnement sur ce domaine. Avec la Fondation Linux, le japonais a lancé deux projets d'IA, « SapientML » et « Intersectional Fairness », qui seront hébergés par la Fondation.

Un support des LTS de 6 à 2 ans

Plusieurs gros nuages ont assombri ce paysage. Selon Jonathan Corbett, développeur du noyau Linux et rédacteur en chef de Linux Weekly News, la durée du support des versions LTS de noyau va se réduire drastiquement :

RED HAT JOUE SA PROPRE PARTITION

Contributeur majeur de l'open source, Red Hat joue sans vraie surprise de plus en plus cavalier seul. Le « doublon » entre les OS serveurs RHEL (Red Hat Enterprise Linux) et sa version open source CentOS a récemment passablement surpris une partie des utilisateurs de cette distribution. *« 100 % du code de RHEL est disponible en licence open source, rappelle Hervé Lemaitre, RHEL Senior Product Marketing Manager chez Red Hat. Nous commercialisons le support. »* Red Hat propose un support étendu sur RHEL V7 d'une durée de 4 ans. Reste que l'abandon de CentOS Linux V8 en 2024 n'était pas vraiment attendu, le support prévisible devait s'étendre sur plusieurs années. Cette annonce, faite en juin 2023, laisse peu de temps aux entreprises pour migrer leurs applications critiques tournant sur cette plateforme. *« Red Hat était quasiment le seul contributeur sur cet OS. Environ la moitié des quelque 21 000 collaborateurs de Red Hat contribuent »*, défend Hervé Lemaitre. Red Hat propose désormais CentOS Stream, une version communautaire qui intègre les développements au fil de l'eau. Une version qui ne peut constituer un socle stable pour des applications. Des versions mineures de RHEL seront disponibles tous les six mois et intégreront toutes les nouveautés et patchs jugés pertinents déjà dans CentOS Stream.

Hervé Lemaitre, RHEL Senior Product Marketing Manager chez Red Hat.


Mirko Boehm, Directeur principal, développement de la communauté.

en passant de 6 à 2 ans. Au bout de cette période, la migration vers la dernière version du noyau stable s'imposera pour les applications d'entreprise. Si, bien sûr, le faible nombre d'utilisateurs sur les versions les plus anciennes du noyau ne justifie pas six années, c'est d'abord une certaine lassitude des développeurs prenant en charge la maintenance qui est responsable de cette réduction drastique. Le bât blesse côté mise à jour dans les six versions antérieures encore mises à jour. *« Les développeurs qui se chargent de la maintenance de ces versions de noyau, à savoir le contrôle de la qualité du code, s'épuisent »*, ont avancé plusieurs participants. La version LTS la plus ancienne du noyau datant de 2017 a nécessité 300 mises à jour. Serpent de mer, la rémunération de ces « mainteneurs » a été remise sur le tapis. Seule une partie d'entre eux le sont. Un constat quelque peu paradoxal s'impose. Alors que nombre d'entreprises, notamment parmi les plus grandes, communiquent autour de leur utilisation de l'open source, le noyau lui-même, manque de ressources et de financements. Souvent utilisatrices de versions anciennes, ces grandes entreprises auraient pourtant intérêt à prendre cette question à bras-le-corps !

Une résistance tenace contre Rust

Autre nuage : Rust, un langage doté de caractéristiques séduisantes. Il permet notamment d'éviter des classes entières d'erreurs, un risque lié au langage C très majoritairement utilisé dans le noyau. En 2021, Linus Torvalds avait annoncé la migration du noyau vers Rust. Première pierre d'achoppement pour une partie de la communauté qui se charge de la maintenance, il suppose pas mal d'adaptations pour fonctionner correctement sous Linux. Plus lourd, il implique pour ces développeurs spécialistes du C de réapprendre un langage complexe. Quelques-uns n'ont pas oublié de signaler que de larges parties du code C ne présentent pas de bogues. Pour l'instant, seules quelques implémentations avec Rust sont en cours.

Une épée au-dessus de la tête

Au-delà de ces questions, une nouvelle réglementation européenne a ému tous les acteurs du libre. Et, une fois n'est pas coutume, la quasi-totalité de ces derniers s'accordent sur le sujet. Le Cyber Resilience Act — CRA — rendrait les communautés de développeurs responsables de la mise en conformité, avec des obligations de reporting, de certification et de maintenance. Pour le CNLL[1], ce Règlement ne prend pas suffisamment en compte les modèles spécifiques des logiciels libres, et fait porter des exigences disproportionnées sur les petites entreprises et les projets non commerciaux qui n'ont pas les ressources, notamment financières, pour y répondre. Autre point, si la réglementation prévoit des exceptions, elle ne précise pas clairement les responsabilités d'une partie de la communauté. *« Le CRA aurait, dans sa forme actuelle, un effet négatif important sur le secteur de l'open source. Lors du Summit, une table ronde réunissant des représentants de la communauté du noyau Linux, de la Python Software Foundation, de Red Hat, de GitHub et d'Ericsson a appelé unanimement les législateurs de l'UE à modifier l'approche de cette loi »*, a insisté Mirko Boehm. La Linux Foundation Europe a également profité de l'évènement pour lancer la campagne #FixTheCRA qui vise à sensibiliser les développeurs, les communautés et les entreprises à la nécessité de réexaminer le CRA. En France, le CNLL a publié une étude sur une étude détaillée sur l'impact du CRA sur la filière du logiciel libre et pointe les éléments qui peuvent encore en limiter les conséquences négatives s'ils sont pris en compte. L'association demande à ce que le gouvernement français *« fasse tous les efforts nécessaires pour que soient clarifiées les questions de responsabilité pour les créateurs de logiciels et composants open source, afin d'éviter tout risques juridiques et de minimiser l'impact du CRA sur l'économie et la souveraineté numériques »*. □

PBr

1 : Le Conseil national du logiciel libre regroupe plus de 200 entreprises dont le modèle économique repose sur l'open source (start-ups, éditeurs de logiciels, sociétés de service et cabinets de conseil).

Alternative

pCloud : une décennie d'innovations !

L'expert en stockage cloud suisse pCloud fête cette année ses 10 ans d'existence. Depuis sa création en 2013, la jeune société a multiplié les innovations pour s'imposer comme une excellente alternative aux géants américains Google Drive, Dropbox ou One Drive.

En moins d'une décennie, pCloud a réussi à séduire plus de 19 millions d'utilisateurs particuliers et professionnels. Le jeune service suisse a réussi à s'imposer sur le marché ultra concurrentiel du stockage en ligne grâce notamment à sa politique de confidentialité et ses fonctionnalités avancées de protection des données. Pour faire face aux géants américains — Google Drive, Dropbox, Box, OneDrive, etc.-, pCloud a mis en place un stockage cloud sécurisé respectueux des lois suisses sur la vie privée et du RGPD, un cryptage AES 256 bits des serveurs de données, et une authentification à deux facteurs. Ce n'est pas tout, pCloud se distingue de tous ses concurrents en proposant des abonnements à vie en un seul et unique paiement, et l'outil payant Crypto qui permet de chiffrer ses données en local sur votre appareil avant de les enregistrer sur le cloud.

Une confidentialité zéro connaissance

Pour une sécurité optimale, le fournisseur conserve chaque fichier téléchargé dans au moins 3 serveurs localisés à différents endroits dans des espaces de stockage protégés. Les datacenters de la société sont localisés aux États-Unis et en Europe (Luxembourg). Les utilisateurs peuvent librement choisir la région de données qu'ils souhaitent lors de l'inscription ou par la suite, à condition de payer des frais de transfert. Comme la plupart de ses concurrents, pCloud utilise la norme de cryptage AES 256 bits pour sécuriser les fichiers durant leur transfert entre un terminal et ses serveurs. Une fois que les fichiers se trouvent sur le serveur de stockage, ils ne sont plus chiffrés. Cela signifie que toutes les personnes ayant un accès au service de stockage (personnel de pCloud, autorités gouvernementales...) peuvent accéder aux données. Pour remédier à ce problème et proposer un service sécurisé de bout en bout, pCloud a développé sa technologie « Crypto » qui permet de chiffrer tous ses fichiers sur le Cloud. C'est un chiffrement offrant une confidentialité « à connaissance nulle ». Cela signifie que les données sont chiffrées sur l'appareil et que seul le client détient les clés de chiffrement. Très confiant quant à la sécurité de son service et ses techniques de chiffrement sophistiquées, pCloud a lancé le concours « Encryption Challenge » avec une récompense de 100 000 $ à la clé afin de mettre au défi les meilleurs ingénieurs informatiques et autres hackers de la planète de parvenir à casser ses protections. À ce jour, personne n'y est arrivé. □ **J.C**

Tunio Zafer, CEO et fondateur de pCloud

Pour les dix ans de pCloud, nous avons rencontré Tunio Zafer, CEO et fondateur de pCloud. L'occasion de revenir sur les temps forts de son entreprise et de nous parler des projets en cours pour assurer l'avenir de l'entreprise.

pCloud qui fête ses dix ans cette année revendique plus de 19 millions d'utilisateurs. Est-ce que vous vous attendiez à rencontrer un tel succès ?
Absolument, nous nous attendions à ce niveau de succès, et c'est le résultat de notre engagement inébranlable envers nos utilisateurs et nos principes fondamentaux. Dès le départ, notre objectif a été de fournir un service de stockage en ligne qui réponde aux besoins spécifiques de nos utilisateurs. Nous voulions créer la plateforme de stockage cloud la plus intuitive, la plus innovante et la plus centrée sur l'utilisateur du secteur, et c'est exactement ce que nous avons fait. Si notre principal objectif a toujours été d'offrir une expérience utilisateur transparente, nous avons également fait de la sécurité des données notre priorité absolue. Nous savons que les utilisateurs nous confient leurs données importantes et qu'il est de notre responsabilité de les protéger. Cet engagement en faveur d'une conception centrée sur l'utilisateur et d'une sécurité solide a été essentiel à notre succès. Le fait que nous ayons atteint plus de 19 millions d'utilisateurs témoigne de la confiance qu'ils nous ont accordée, et nous prenons cette confiance très au sérieux. Nous continuerons à innover et à nous assurer que pCloud reste une solution fiable et sécurisée pour notre base d'utilisateurs en constante augmentation.

Qu'est-ce qui vous a motivé à lancer pCloud ? Comment l'entreprise a-t-elle évolué depuis son lancement en 2013 ?
La motivation derrière le lancement de pCloud est profondément ancrée dans la reconnaissance de l'importance croissante des données à l'ère numérique. Nous sommes convaincus que les données sont le « pétrole du futur » du 21e siècle et qu'il est de notre devoir de les protéger, tout comme une banque veille sur les actifs de ses clients. Notre vision était de devenir la banque suisse des clients pour leurs fichiers numériques, en leur offrant une solution de stockage sécurisée, confidentielle et facilement accessible. Depuis notre création en 2013, pCloud a considérablement évolué pour accomplir cette mission. Nous avons continué à perfectionner nos services et nos technologies, offrant aux utilisateurs non seulement un espace de stockage pour leurs données, mais aussi une solution complète pour le stockage, l'accès et la protection de leurs précieux fichiers. Nous avons étendu nos fonctionnalités, introduit des mesures de sécurité de pointe telles que le chiffrement côté client, et développé des outils de collaboration pour faciliter la gestion des données pour les entreprises comme pour les particuliers. Notre volonté constante d'innovation nous a poussés à améliorer l'expérience de l'utilisateur et à renforcer la sécurité des données.

Les entreprises bénéficient-elles d'options spécifiques ? Si oui, pouvez-vous nous dire lesquelles ?
Nous offrons une variété d'options spécifiques aux entreprises pour répondre à leurs besoins. Ces options sont conçues pour améliorer la productivité des équipes, la sécurité des données et la collaboration. Voici les principales fonctionnalités et offres destinées aux entreprises :

– **Gestion des équipes et des utilisateurs :** les forfaits Business de pCloud permettent aux organisations de gérer efficacement les utilisateurs et les équipes. Les administrateurs peuvent facilement ajouter ou supprimer des membres d'équipe, attribuer des ressources de stockage et contrôler les autorisations d'accès afin de s'assurer que les bonnes personnes ont accès aux données appropriées.

– **Registres d'activité :** les entreprises peuvent surveiller et suivre l'activité des utilisateurs grâce à des registres d'activité détaillés. Les administrateurs peuvent ainsi contrôler la manière dont les données sont consultées, partagées et modifiées au sein de l'entreprise, ce qui garantit la transparence et la responsabilité.

– **Collaboration avec chiffrement côté client :** les entreprises peuvent collaborer en toute sécurité dans l'environnement pCloud, en tirant parti des avantages du chiffrement côté client. Cela garantit que les données sensibles sont protégées même pendant la collaboration, faisant de pCloud une plateforme sécurisée pour les projets d'équipe et le partage de documents.

Nos plans Business sont flexibles et extensibles, ce qui les rend compatibles avec les entreprises de toutes tailles, des petites startups aux grandes entreprises. Ces plans sont conçus en tenant compte des besoins des entreprises en matière de sécurité et de collaboration, ce qui leur permet de profiter des fonctionnalités avancées de pCloud tout en conservant le contrôle et la protection des données.

Prévoyez-vous de lancer de nouvelles innovations ?
Nous nous concentrons constamment sur l'innovation afin d'améliorer notre service et d'apporter plus de valeur à nos utilisateurs. Nos projets actuels et futurs se concentrent sur plusieurs domaines clés : collaboration en ligne, la recherche et la facilité des accès, et de nouveaux produits de sécurité pour renforcer la protection des données. Notre engagement en faveur de l'innovation s'étend à tous les aspects de notre service, et nous sommes impatients de proposer ces nouveaux développements à nos utilisateurs. Ces efforts visent à offrir la solution de stockage en ligne la plus fiable, la plus conviviale et la plus riche en fonctionnalités qui soit. Restez à l'écoute des nouveautés que nous avons prévues pour l'avenir.

J.C

Zero Trust

Zscaler s'approche timidement de l'IA générative

Employant largement le machine learning dans ses outils existants et ceux à venir, le spécialiste du Zero Trust fait évoluer son offre.

La conférence de Zscaler à Berlin de juin dernier a démarré sur de mauvais auspices. Selon l'éditeur de sécurité sur le web, les attaques par ransomware ont augmenté de 40 % sur un an. Et désormais, la mode est au ransomwares as a service : *« ceux-ci ont contribué à la hausse continue d'attaques de plus en plus sophistiquées »*, estime Deepen Desai, DSI de Zscaler. Plusieurs To de données ont ainsi été chiffrés ou volés pour faire de l'extorsion de fonds auprès des entreprises. Lesquelles dépensent beaucoup d'argent pour leur sécurité : 220 Md$ en 2023. Mais pas toujours à bon escient : les logiciels sont mal intégrés, ont recours à tout un tas d'API, ce qui transforme leur administration en casse-tête. Pour Zscaler, la solution est le zero trust — c'est d'ailleurs sa spécialité. *« Pour simplifier, le zero trust consiste à se poser les questions suivantes : qui êtes-vous ? Sur quelles applications allez-vous ? Pour quoi faire ? »*, explique Kavitha Mariappan, VP exécutif chez Zscaler.

Visualiser les risques

Pour y répondre, Zscaler propose quatre outils. Le plus récent est Zscaler Risk 360. C'est un framework qui visualise et quantifie les risques. Il existe des logiciels équivalents sur le marché, mais qui ne traitent pas autant de données. Environ 300 milliards de transactions sont traitées quotidiennement par Zscaler, soit plus que le nombre de requêtes sur Google.

L'événement européen Zenith Live s'est tenu fin juin à Berlin.

Zscaler s'est associé à Equinix pour créer une appliance, Zero Trust Branch Connectivity, destinée à mettre en place une politique zero trust pour les succursales des grandes entreprises, de façon pratiquement plug&play. Avec, à la clé, une réduction des coûts. ZSLogin est un tableau de bord centralisant les personnes connectées et distribuant les jetons pour une authentification multifacteurs. Il assure une gestion des identités avec des solutions tierces. Enfin, Zscaler Identity Threat Detection and Response (ITDR) repère les mauvaises configurations ainsi que les usurpations d'identité, souvent obtenues par ingénierie sociale et difficiles à détecter.

L'IA est au cœur de la stratégie de Zscaler. À la fois pour épauler Zero Trust Exchange, sa plateforme de sécurité dans le cloud, mais aussi pour se protéger des applications faisant appel à l'IA. Sur ce dernier point, Zscaler prépare des applications, encore en bêta. AITotal est un système de gestion de risques évaluant les dangers d'une application en termes de vie privée, et conseille ou non de l'adopter. Data Protection for AI averti l'entreprise des risques de fuites de données dus à une application d'IA. AI Visibility and Access Control sont des applications web indiquant qui utilise une application d'IA et s'il en a l'autorisation.

Des RSSI méfiants

Dans le domaine de la sécurité, l'IA est employée depuis longtemps. Plus exactement le machine learning, sur lequel sont basés les antispams. Mais la grande nouveauté chez Zscaler est l'exploitation de l'IA générative. A priori, le rapport avec la sécurité n'est pas évident. Pourtant, il n'est pas le seul à y faire appel. Google Cloud Security AI Workbench and Microsoft Security Copilot sont des solutions s'appuyant sur l'IA générative. Reste que les RSSI restent méfiants face aux outils tels que ChatGPT. Certaines entreprises exploitent ChatGPT pour coder des scripts en Python. Mais elles veulent savoir à quelles données accède ChatGPT. Pas question par exemple de le laisser accéder à la formule d'une molécule pharmaceutique. □

Pierre Berlemont

IVAN ROGISSART, EN CHARGE DES INGÉNIEURS AVANT-VENTE POUR L'EUROPE DU SUD

« L'IA générative permet de prévoir une faille, de générer un scénario d'attaques et d'effectuer des recommandations. L'utilisateur prend une décision d'évaluer le risque en remarquant que des choses bizarres se passent et que c'est sérieux, car il a déjà vu ce type de comportement. Cette partie est basée sur l'algorithme de machine learning que nous avons développé. Puis, nous allons coacher le logiciel pour qu'il puisse automatiquement proposer très simplement de remédier à l'attaque. Il reconnaît une potentielle faille, et propose des moyens de remédiation. Autre exploitation de l'IA générative : l'utilisation de ChatGPT. Tous les utilisateurs savent que ChatGPT peut les aider dans leur tâche. Mais il faut pouvoir le contrôler. Il y a un équilibre à trouver entre les gains de productivité attendus et les risques d'utilisation. Pour cette raison, les RSSI doivent avoir de la visibilité sur ce que fait ChatGPT. »

CLUB DECISION DSI EUROPE

1er Club Français de décideurs informatiques & télécoms

Un réseau privé et indépendant où siègent 13 DSI et 1 RSSI 1500 Membres

Le Club accompagne les DSI à faire les bons choix technologiques en adéquation avec leurs projets.

FONDATEURS

Véronique Daval Présidente — Julien Daval Vice-Président

LES MEMBRES DU BUREAU ET AMBASSADEURS DU CLUB

Armand ASSOULINE
CIO & National Documentation Manager - MSC

Laurent BAYOL
DSI
LA COMPAGNIE

Nawal BENSASSI
CIO & Digital Officer
ESRI FRANCE

Gilles BERTHELOT
Directeur Sécurité Numériques
GROUPE SNCF

Christophe BOUTONNET
Directeur Adjoint du Numériques
Ministère écologie, énergie, territoires et mer

Benoit DECOCK
Business transformation numérique leader
AGFA

Christian DOGUET
CIO
CHAINE THERMALE DU SOLEIL

Alain GUEDE
CIO
GROUPE SARETEC

Christophe GUILLARME
RSSI
LAGARDèRE TRAVEL RETAIL

Philippe LAGRANGE
Directeur recherche et prospective
MUTUELLE GéNéRALE DE LA POLICE

Stéphane MALGRAND
DSI
LABORATOIRE NATIONAL MéTROLOGIE ET ESSAIS

Sandrine RACOUCHOT
DSI
INTER MUTUELLES hABITAT

Lionel ROBIN
DSI
THE SET hOTELS

Claude YAMEOGO
ARCHITECT SI
ALSTOM

COORDINATEUR

TRIEU hUyNh-ThIEN

CLUB DECISION DSI 33, Rue Galilée 75116 Paris • Tél +33 1 53 45 28 65
Contact : Véronique DAVAL - Présidente • veronique.daval@decisiondsi.com

www.clubdecisiondsi.fr

Alliance CIO

Cloud

Les laboratoires Pierre Fabre marient les approches Data Fabric et Data Mesh

Le castrais vient de mener le « Move to Cloud » de sa plateforme Data sur Azure avec pour objectif de proposer une plateforme Data performante à ses utilisateurs métiers. Présenté lors du salon Big Data & IA Paris, ce projet s'appuie sur la solution de virtualisation de données Denodo, une couche d'abstraction pour apporter une vue unifiée aux utilisateurs.

Avec un chiffre d'affaires de 2,5 milliards d'euros et 9 600 employés dans le monde, les laboratoires Pierre Fabre sont un poids lourd industriel de la région castraise. L'entreprise a longtemps privilégié un hébergement on-premise, dans son propre datacenter régional, mais a finalement lancé un programme « Move to Cloud » de sa plateforme de données. L'objectif est de moderniser la plateforme de données afin de transformer le groupe en entreprise « Data Driven » et véritablement pilotée par la Data. Le groupe a un historique de plus de 25 ans dans la donnée, avec la mise en place d'un premier Data Warehouse en 1998. La plateforme s'appuyait alors sur la base de données Oracle, sur les solutions de reporting et d'analyse de Cognos et SAS, puis de Business Objects et Tibco Spotfire, pour enfin aboutir à Tableau aujourd'hui. Un Data Lake est mis en place en 2015 en s'appuyant sur la distribution MapR d'Apache Hadoop déployée sur site. *« Avec la mise en œuvre de Tableau notamment, nous avons accentué la prise en main des Data par les métiers pour faire de l'analytique »* explique Wassim Bouaziz, directeur de l'intégration et Data à la DSI de Pierre Fabre.

Wassim Bouaziz, directeur de l'intégration et Data à la DSI de Pierre Fabre.

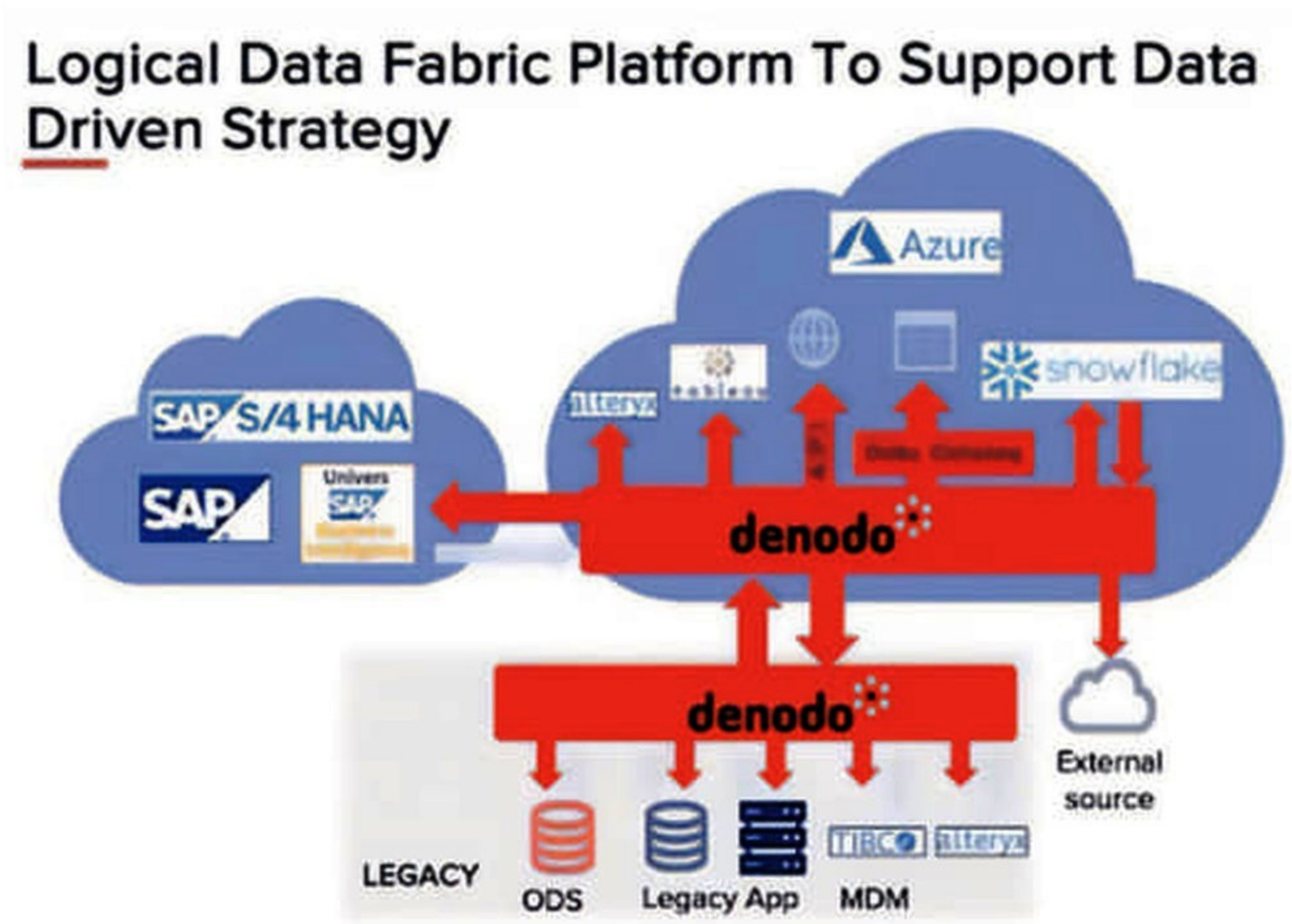
« Nous sommes partis d'un existant on-premise très siloté à une approche à la fois mieux gouvernée, mieux architecturée et qui s'appuie sur une architecture de type Data Fabric qui supporte l'ensemble du cycle de vie de la donnée. »

Un Data Office créé pour accélérer la stratégie Data

Suite de cet audit, un programme Data est mis en place avec pour principaux piliers : la mise en place d'une gouvernance de la donnée, le lancement d'initiatives d'acculturation des métiers à la donnée ainsi que la construction d'une nouvelle Cloud Data Platform. Dans cet élan, un Data Office devient chargé de l'animation de cet écosystème Data interne et doit aider les métiers de tous horizons à mener des analyses de données plus avancées. De son côté, la DSI a pour mission de mettre en place une nouvelle plateforme de données rassemblant toutes les technologies nécessaires pour couvrir l'ensemble des périmètres métiers de l'entreprise. Ce programme de transformation des infrastructures et des usages va alors impliquer une forte collaboration entre le Data Office et la DSI.

Les Laboratoires Pierre Fabre ont investi sur la donnée depuis plus de 25 ans maintenant. Le Data Warehouse Oracle a été complété par un Data Lake Hadoop en 2015, et vient d'opérer son Move to Cloud pour tirer profit des solutions de dernière génération.

Les études techniques vont conduire la DSI à mettre en place une architecture de type Data Fabric. *« Nous avons rapidement identifié les insuffisances de notre existant on-premise et les capacités du Cloud »*



La solution de virtualisation de données Denodo constitue la clef de voûte de l'architecture Data des Laboratoires Pierre Fabre où cohabitent des technologies de natures diverses.

Architecture key points for Denodo

- ➔ Denodo for hybrid architecture managing whole securtity
- ➔ Denodo to offload data in Snowflake and unify On Prem, SAP, Snowflake and Azure
- ➔ Denodo Data Catalog to fuel and manage Data Marketplace portal

détaille Wassim Bouaziz. *« Nous avons souhaité construire une architecture combinant les meilleures solutions et la transformation de l'existant. Il ne s'agissait pas seulement d'une migration. Nous avons commencé à revoir nos données maîtres afin de structurer nos données par domaines métiers. Nous avons associé à ce "Move to Cloud" une nouvelle analyse de l'existant afin de travailler sur de nouvelles capacités, de nouveaux cas d'usage, de nouveaux contextes. »*

De 2021 jusqu'au début de l'année 2022, les équipes se sont attelées à la création de la plateforme de données. Celle-ci reste encore fortement hybride. La base Oracle ODS, le MDM et Tibco Spotfire restent déployés en interne, mais la plateforme met en œuvre des briques Cloud plus modernes, à commencer par Snowflake, Azure, Tableau. Dans cette approche hybride, la solution Denodo joue un rôle pivot grâce à sa technologie de virtualisation de la donnée : *« Denodo est l'un des composants principaux de notre architecture hybride. La solution fait à la fois le lien entre notre architecture legacy et le Cloud. La solution assure aussi la gestion de la couche sémantique et le data cataloging des données et des produits data proposés aux métiers. »* Quels que soient les outils mis en œuvre et le profil des utilisateurs ou des applications, toutes les requêtes convergent vers Denodo, une centralisation des accès qui permet à la DSI d'avoir une vision à 360° de l'ensemble des accès aux données. *« Nous avons combiné l'approche Data Platform sur l'architecture technique et une approche Data Mesh, sans toutefois en reprendre tous les principes. Nous restons dans une organisation centralisée »* précise le responsable. Côté métier, cette couche sémantique permet aux utilisateurs de retrouver leurs objets métiers quel que soit l'outil ou son point d'accès à la donnée. À ce jour, plus de 300 sources de données ont été connectées à la Data Platform.

Un gros effort porté sur l'acculturation des utilisateurs

Si le volet technologique est la base d'une stratégie Data, l'adhésion des utilisateurs reste essentielle au succès de l'initiative. *« Beaucoup d'efforts et d'investissements ont été réalisés sur l'acculturation pour expliquer la stratégie de l'entreprise, plusieurs sessions de formation organisées à partir de 2021 sur l'usage de la Data Platform, démontrer l'accessibilité de la donnée afin de promouvoir les usages et susciter la création de nouveaux cas d'usage. »*

Plus de 1 500 personnes ont été formées et acculturées à la stratégie Data du laboratoire, soit 16 % de l'effectif total. Plus de 400 utilisateurs métiers ont été formés à la Data Marketplace, soit 5 % de l'effectif lors d'un bootcamp d'une semaine pour apprendre à exploiter la plateforme et créer de la valeur. *« Nous essayons de faire monter en maturité les usages de la Data et, d'ici la fin de l'année, notre objectif est d'aller plus loin, de capitaliser sur les cas d'usage métiers, pour l'optimisation des process métiers et la favorisation de nouvelles opportunités business. »* L'idée est désormais de pousser les utilisateurs pour aller vers plus d'autonomie. Wassim Bouaziz estime qu'il faut encore travailler sur les aspects gouvernance de la donnée et la responsabilisation des métiers pour aller dans ce sens.

La DSI a mis à disposition les technologies qui doivent soutendre la stratégie Data et doit maintenant promouvoir ces services auprès des métiers : *« nous devons passer d'une ère où l'on analyse le passé pour aller vers le prédictif et les analyses avancées et des cas d'usage purement métiers pour rechercher de la valeur ajoutée, créer des insights. Tous les services sont aujourd'hui en production sur la plateforme, et nous cherchons maintenant à capitaliser sur les cas d'usage. »* La transformation de l'approche Data de Pierre Fabre bat son plein et l'objectif de devenir une Data Driven Company n'a jamais été aussi proche. □

AC

Virtualisation du poste de travail

Les architectes passent sur Shadow

Depuis son rachat par Octave Klaba, Shadow s'est éloigné du gaming. Son sacerdoce désormais : convertir les entreprises au poste de travail dans le Cloud. Ses offres ont ainsi séduit plusieurs cabinets d'architectes et de design.

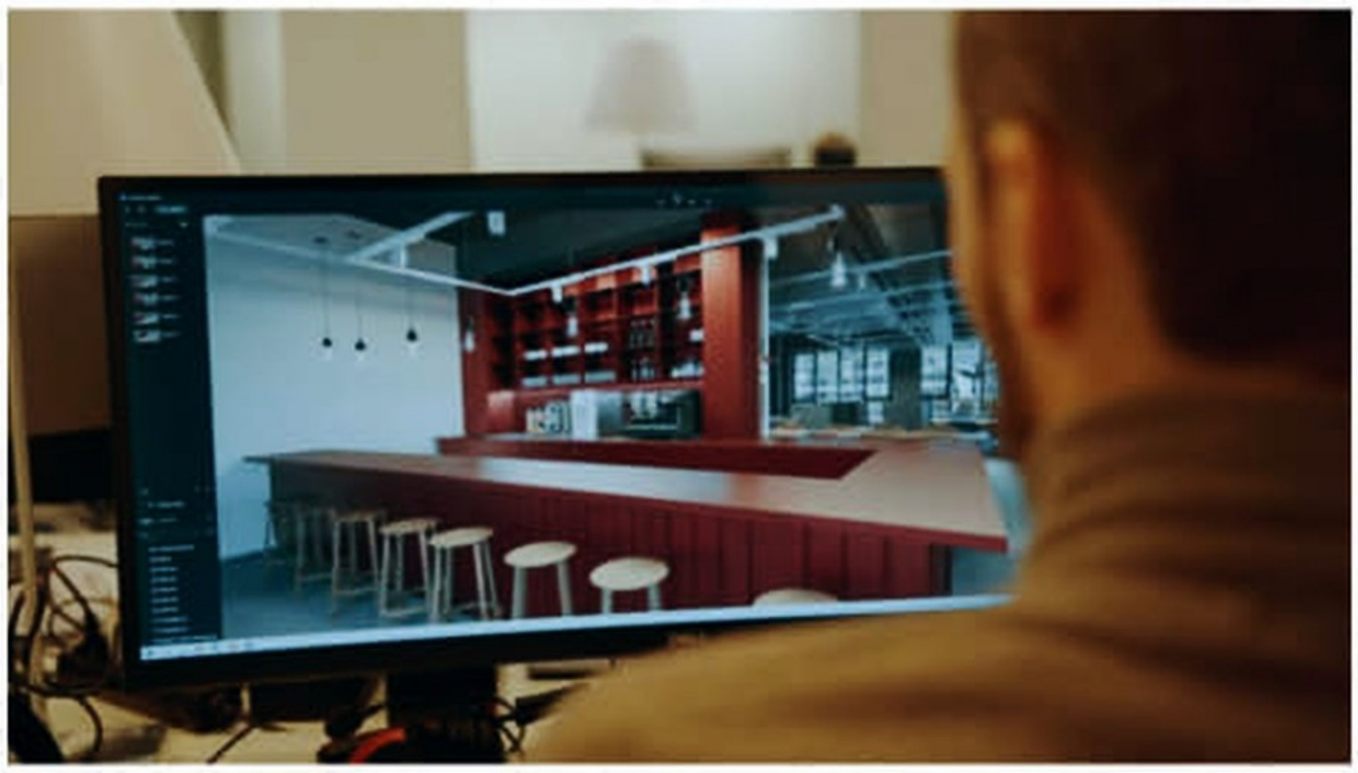
En 2021, dans la foulée de sa reprise par Octave Klaba, Shadow promettait de travailler sur son côté B2B. L'entreprise était en effet surtout connue pour ses offres de cloud gaming mais, comme nous l'expliquait alors son CEO, Éric Sèle, *« pendant les confinements, des architectes, des développeurs de jeux sont venus nous voir. À partir de là, nous avons commencé à avoir des discussions sur le sujet »*. Il détaillait : *« cette expérience utilisateur vraiment renforcée nous impose de repenser notre système d'information global pour, à terme, pouvoir continuer et valoriser la croissance de l'offre B2C mais également aller dans le B2B et ajouter des verticales »*. Deux ans, et une refonte de son offre plus tard, Shadow semble en passe de remporter son pari.

« Avec Shadow PC Pro, nous avons pour ambition de libérer les petites et moyennes entreprises de leurs contraintes technologiques en leur fournissant des outils innovants, intuitifs et puissants, conçus pour l'ère du travail à distance » indique Stéphane Héliot, directeur général adjoint de la société. Ce sont notamment les agences d'architectes que la solution séduit. En effet, Shadow PC Pro se décline en quatre gammes, allant d'une offre à moins de 40 euros comprenant une carte graphique Nvidia GTX 1080, un CPU Intel Xeon 8 cœurs et 12 Go de RAM à une autre à près de 75 euros avec une RTX 6000, un Xeon 12 cœurs et 41 Go de RAM. Bref, il y en a pour tous les goûts et tous les budgets. D'autant que la solution est compatible avec la majeure partie des outils les plus utilisés par les créatifs, à l'instar de Photoshop, After Effect, ArchiCAD, AutoCAD, Blender, Indesign, SketchUp, Solidworks, Unity ou encore Unreal Engine, pour ne citer qu'eux. Le tout sans avoir à s'encombrer d'une volumineuse station de travail.

Un gain de temps et d'argent

Ainsi, voilà un peu plus d'un an que PCA Stream virtualise ses postes de travail avec Shadow. Cette agence composée surtout d'architectes, mais aussi d'urbanistes et de chercheurs, compte une centaine de collaborateurs et

collaboratrices dans ces bureaux parisiens. Après avoir testé la solution de PC dans le cloud à une échelle réduite, la société a passé l'ensemble de son équipe chargée de la visualisation 3F sur Shadow. *« Nous utilisons encore nos PC physiques pour modéliser et designer et nous utilisons les PC Shadow pour le rendu »* explique Yan Roche, chef de projet chez PCA-Stream. *« Nous avons aussi étendu notre parc Shadow pour nos architectes et certains profils qui ont besoin de plus de puissance pour des tâches spécifiques. Au lieu d'acheter des ordinateurs coûteux et qui ne seraient pas utilisés quotidiennement, nous utilisons Shadow pour ces projets »*.



« Shadow nous permet de gagner beaucoup de temps car il faut plusieurs semaines ou mois pour acheter un ordinateur puissant quand un Shadow PC peut être activé en moins d'un jour » poursuit-il. Pour PCA Stream, c'est aussi une question de place. Les mètres carrés sont rares et chers à Paris, avoir recours à des machines virtuelles lui permet donc de gagner de l'espace dans ses locaux, en n'évitant d'avoir trop d'ordinateurs volumineux sur ou sous les bureaux. Satisfait de la solution, le cabinet songe désormais à étendre Shadow à d'autres équipes, pour le design en interne, la communication ou encore la réalisation de vidéos.

Accessible même sur un iPad

Du côté de Mon Concept Habitation, une agence spécialisée dans la rénovation intérieure, on utilise Shadow PC depuis deux ans et demi : *« ça m'a tout de suite séduit, ce concept de PC totalement accessible à distance, qui permet de s'affranchir de l'obsolescence programmée des ordinateurs, tout en étant assuré d'avoir toujours accès à un PC très puissant avec une très bonne carte graphique »*, précise Laurent Mudry, co-fondateur de Mon Concept Habitation. Il apprécie d'autant plus l'offre, étant flexible et s'adaptant à la croissance très rapide de la société. *« Nous sommes passés de zéro salarié à quinze en deux ans et demi. Je peux ouvrir de nouveaux comptes Shadow très facilement. Ça m'évite d'immobiliser 1500 ou 2 000 euros dans un ordinateur et ça permet d'étaler sur le temps en garantissant une performance optimale »*. Autre avantage, le télétravail. Car Shadow PC Pro permet aux salariés et salariées de se connecter à leur poste de travail depuis n'importe quel terminal. *« Chacun a son outil, certains sont sur Mac, d'autres sur PC, on arrive même à le faire marcher sur iPad si besoin »* souligne le co-fondateur de l'agence.

Enfin, l'agence White Red, basée à Londres, est spécialisée elle aussi dans l'architecture et le design. Son équipe compte une vingtaine de personnes. Son directeur, Dicky Lewis a découvert Shadow il y a plusieurs années alors qu'il recherchait des alternatives pour accéder à leurs appareils à distance tout en étant compatibles avec leurs logiciels graphiques. Il rejoint Laurent Mudry sur la flexibilité de l'offre : *« Shadow est la seule alternative du marché qui nous permet, via ses applications, de travailler à distance sur iPad par exemple »*. L'entreprise utilise Shadow depuis maintenant deux ans. Après un test, dans un premier temps, des différentes configurations pour s'assurer que le service était compatible avec les outils utilisés par les architectes, *« et surtout efficace pour tous nos usages »*, c'est toute l'agence qui a adopté la solution de PC dans le cloud. □

G.P

Framework

Blazor, la nouvelle révolution du développement Web made in Microsoft

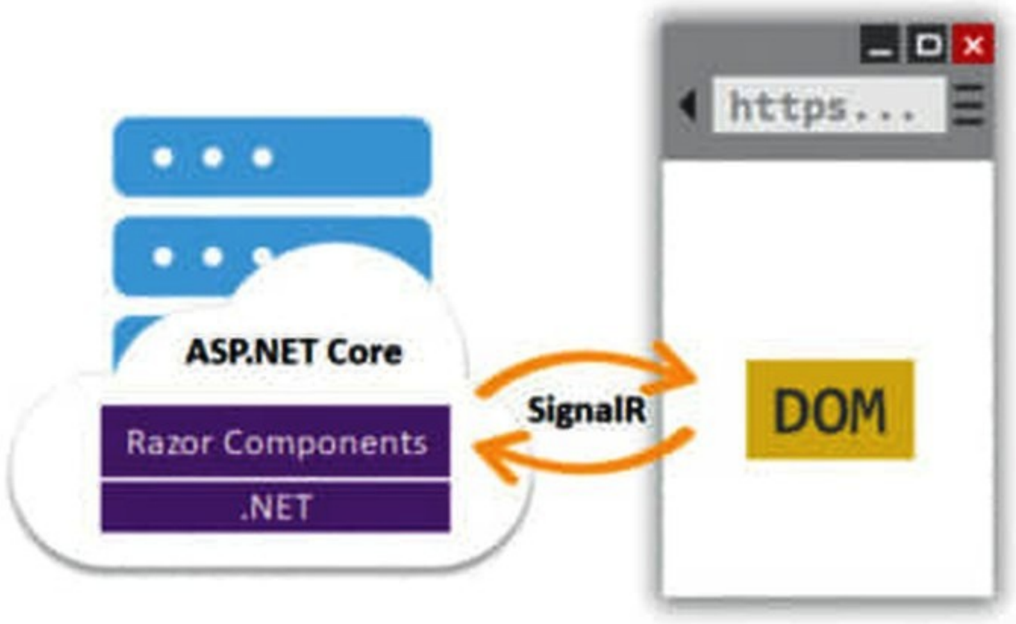
Blazor, le framework de Microsoft, a été créé pour concurrencer les plateformes leaders du développement Web telles que React ou Angular. Il offre aux développeurs la possibilité de concevoir des applications Web interactives uniquement avec du code C# et HTML. Les applications ainsi conçues sont exécutées par le runtime. NET.

Blazor est donc un banc de travail de génération d'interfaces utilisateur (IU) web interactives côté client avec. NET derrière pour partager la logique d'application aussi bien côté serveur que côté client. Il permet de décrire les éléments d'interface en langage HTML et CSS et de générer des applications de bureau et mobiles hybrides. L'utilisation de. NET dans le développement web offre de nombreux avantages, dont la possibilité d'écrire les 2 parties, serveur et métier, en C# et de bénéficier des performances, de la fiabilité et de la sécurité de. NET. Quel que soit le système d'exploitation cible, Windows, Linux ou macOS, et celui utilisé pour le développement, que vous fassiez ou non de la cross-compilation, vous pouvez utiliser Visual Studio ou Visual Studio Code disponibles pour toutes ces plateformes. L'intégration aux plateformes d'hébergement modernes telles que Docker est, elle aussi, amplement facilitée.

Composants

Les applications Blazor sont fondamentalement basées sur le principe des composants. Un composant Blazor est un élément d'IU tel qu'une page, un formulaire de saisie de données, une boîte de dialogue, une liste déroulante et autres choses du genre. Ces composants sont des classes C#. NET appartenant à des assemblys (packages. NET) et permettant de définir une logique de rendu flexible et de gérer les événements utilisateur. Ils peuvent être imbriqués, réutilisés, partagés et distribués sous la forme de bibliothèques de classes Razor ou de packages NuGet. La classe de composant est généralement écrite sous la forme d'une page de balises Razor. Le fichier source correspondant a comme extension de nom de fichier.razor. Les composants Blazor sont appelés officiellement des composants Razor, et officieusement des composants Blazor (et oui). De fait, Razor est une syntaxe combinant à la fois des balises HTML et du code C#. Il est ainsi possible de basculer entre des balises HTML et du C# dans le même fichier source. C'est un peu le même principe qu'avec Angular, mais avec un langage plus « sérieux », le C#, et ce, encore une fois, aussi bien côté client que côté serveur. Blazor utilise des balises HTML, tout ce qu'il y a de plus classique pour la composition de l'interface client. Voici un exemple de composant incrémentant un compteur lorsque l'utilisateur clique sur un bouton. Une partie d'une application est créée à partir d'un modèle de projet stocké dans un fichier nommé Counter.razor :

```
razor
@page "/counter »
<PageTitle>Counter</PageTitle>
<h1>Counter</h1>
<p role="status">Current count : @currentCount</p>
<button class="btn btn-primary » @onclick="IncrementCount">Click
me</button>
@code {
// partie code C#
private int currentCount = 0 ;
private void IncrementCount()
{
currentCount++;
}
}
```



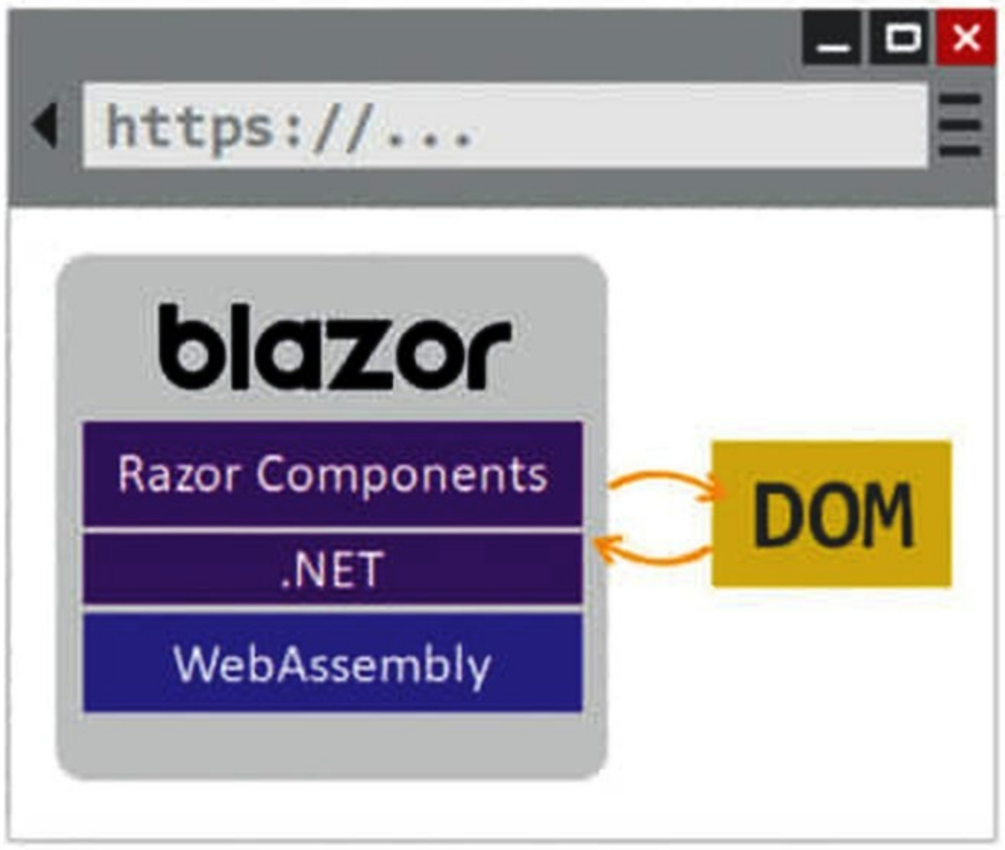
Blazor Server utilise une connexion SignalR pour assurer la communication entre le client et le serveur. C'est une couche « élaborée » au-dessus d'une connexion WebSocket.

Le composant Counter précédent définit sa « route » avec la directive @page sur la toute première ligne, ainsi que son titre de page et affiche la valeur courante du nombre actuel via la propriété @currentCount. currentCount est une variable entière définie dans le code C# du bloc @ code. Il affiche aussi un bouton pour déclencher la méthode IncrementCount, qui figure également dans le bloc @code et augmente la valeur de la variable currentCount. Les composants s'affichent dans une représentation en mémoire du modèle DOM (Document Object Model) du navigateur appelée également arborescence de rendu qui permet de mettre à jour l'IU de manière très flexible. Le code C# s'exécutant beaucoup plus rapidement que du JavaScript. Vous

pourrez profiter d'un backend avec des performances bien plus élevées qu'avec Angular ou React. Blazor apporte aussi une meilleure interopérabilité, de nombreuses applications utilisant déjà le langage C # pour le backend. Une API ASP. NET interagissant avec une interface React nécessite des modèles distincts pour le serveur et le client ainsi qu'un code distinct. S'ils utilisent le même langage, cela permettra de partager facilement du code et des bibliothèques entre client et serveur. C'est le principe suivi avec NodeJS côté serveur et JavaScript de l'autre côté. Avoir des applications créées dans un seul langage réduit considérablement le temps de développement et encore plus celui de la maintenance (correction, débogage, optimisation and co).

Blazor Server

La philosophie de Blazor Server consiste à prendre en charge l'hébergement de composants Razor sur le serveur dans une application ASP. NET Core. Les mises à jour de l'IU sont gérées via une connexion SignalR. Le runtime gère l'envoi des événements d'interface utilisateur du navigateur au serveur et applique les mises à jour de l'interface utilisateur renvoyées par le serveur dans le navigateur après avoir exécuté le code des composants.



Blazor WebAssembly appréhende le serveur dans sa globalité et l'exécute avec le runtime. NET au-dessus de WASM. Au lieu de parler au serveur via SignalR, il « parle » directement au DOM.

Le runtime reste côté serveur et gère les éléments suivants :

- L'exécution du code C# de l'application.
- L'envoi des événements d'interface utilisateur depuis le navigateur vers le serveur.
- L'application de mises à jour de l'IU à un composant affiché, qui sont renvoyées par le serveur.

Les applications Blazor Server affichent le contenu dans les applications ASP. NET Core à l'aide de vues ou de pages Razor. Les deux modèles utilisent le langage Razor pour décrire le contenu HTML, mais ils diffèrent considérablement en ce qui concerne le mode d'affichage des balises. Quand une page ou une vue Razor est affichée, chaque ligne de code Razor émet du code HTML sous forme de texte. Une fois le rendu effectué, le serveur supprime l'instance de page ou de vue ainsi que tout état produit. Quand une autre requête se produit pour la page, la totalité de celle-ci est régénérée au format HTML et envoyée au client. Blazor Server travaille différemment. Au contraire de Razor, il produit un graphique de composants qui s'affiche comme un DOM HTML ou XML. Le graphe de composants interprète les données d'état contenu dans les propriétés et les champs. Blazor évalue le graphe de composants nécessaire à la production d'une représentation binaire des balises. Ce dernier est envoyé au client pour le rendu final. Une fois la connexion établie entre le client et le serveur, les éléments statiques préaffichés du composant sont remplacés par des éléments interactifs. Le pré-rendu du contenu sur le serveur rend l'application plus réactive sur le client. Une fois que les

BLAZOR SERVER VERSUS BLAZOR WEBASSEMBLY

Blazor Server utilise une connexion SignalR pour assurer la communication entre le client et le serveur. Il s'agit tout simplement d'une couche « sophistiquée » au-dessus d'une connexion WebSocket pouvant éventuellement se rabattre sur d'autres connexions si cela s'avérait nécessaire. Cela permet de garder tout le traitement sur le serveur et de laisser le client sous la forme d'une vue simple. Blazor WebAssembly n'est pas un langage de programmation à proprement parler, mais plutôt une cible de compilation. Il fonctionne en fait comme le MSIL (Microsoft Intermediate Language). La différence essentielle est qu'il s'exécute à l'aide du runtime WebAssembly dans le navigateur et non avec celui de. NET. En pratique, le C# est compilé en MSIL qui est lui-même compilé en WebAssembly. Il faut aussi savoir que n'importe quel langage peut être compilé en WASM, même les langages de type client lourd (de bureau si vous préférez) entièrement natifs comme les langages C++ ou Rust, par exemple. Blazor WebAssembly prend le code serveur dans sa globalité ainsi que le runtime. NET et les exécute au-dessus de WASM. Ensuite, au lieu de parler au serveur via SignalR, il parle directement au DOM. Cela supprime le traitement côté serveur, ce qui est parfait pour certaines applications. Dans les deux cas, l'interopérabilité avec JavaScript est totale. Blazor peut aussi appeler des fonctions JavaScript à partir de code managé, comme ceci :

```
private async Task ConvertArray()
{
text = new(await JS. InvokeAsync<string>("convertArray", quoteArray)) ;
}
```

Et inversement :

```
DotNet.invokeMethodAsync('{ASSEMBLY NAME}', '{. NET METHOD ID}', {ARGUMENTS}) ;
```

composants sont interactifs côté client, les mises à jour de l'IU sont déclenchées par les interactions utilisateur et les événements d'application. Quand une mise à jour se produit, le graphe de composants est réaffiché et une différenciation de l'IU est alors calculée. Cette différenciation est le plus petit ensemble de modifications du modèle DOM nécessaire pour la mise à jour de l'IU du client. La différenciation évaluée est envoyée au client dans un format binaire et appliquée par le navigateur. Les composants stockés ne sont pas supprimés aussitôt mais seulement lorsqu'ils n'ont pas été utilisés pendant un certain temps.

Blazor WebAssembly

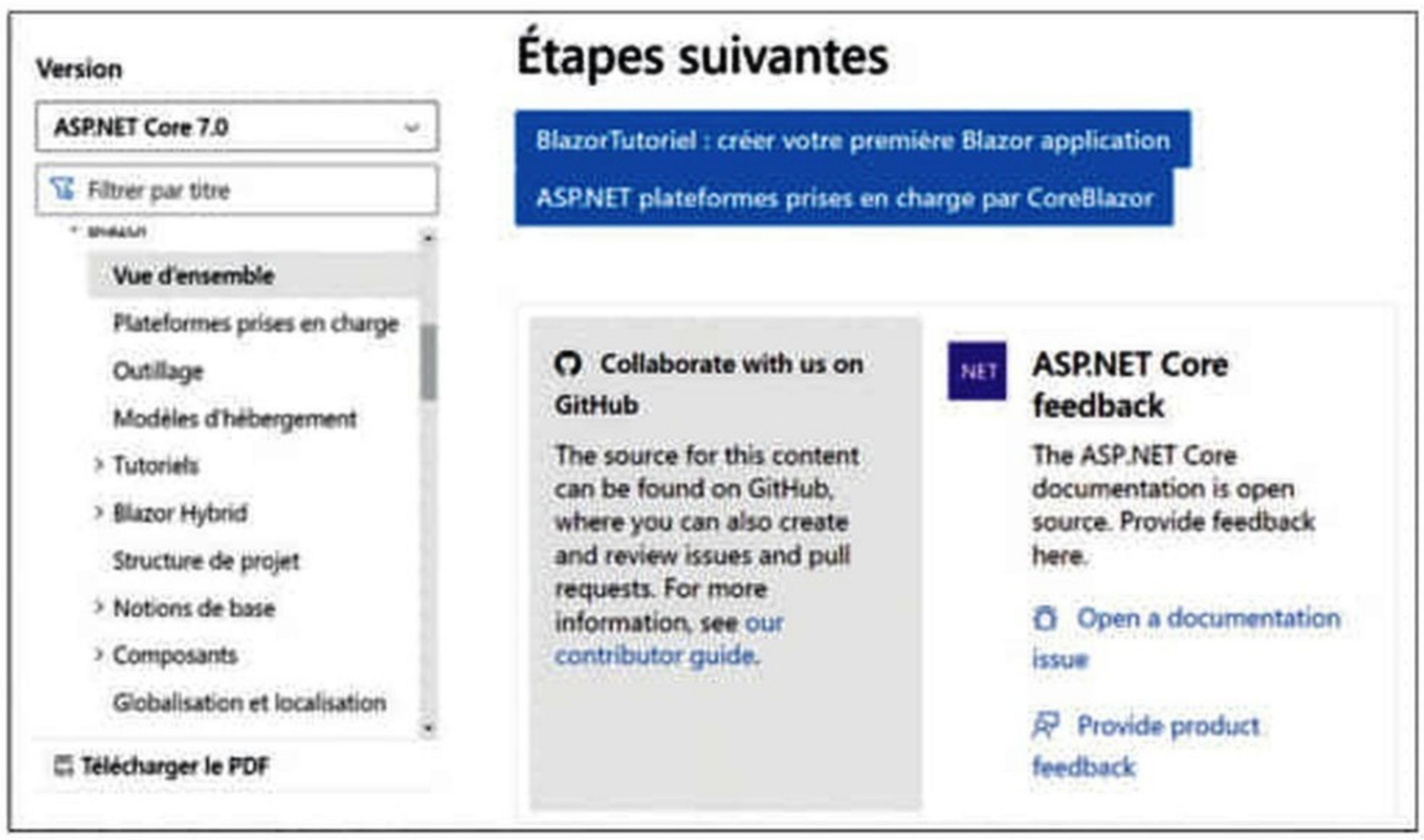
Blazor WebAssembly est un framework d'application monopage (SPA pour Single Page Application) pour la génération d'applications web interactives côté client avec. NET. L'exécution de code. NET dans les navigateurs web est rendue possible par WebAssembly (Wasm). WebAssembly est un format bytecode compact optimisé pour un téléchargement rapide et une vitesse d'exécution optimale. C'est un standard web ouvert pris en charge dans les navigateurs web depuis peu sans qu'aucun plug-in ne soit nécessaire. Blazor fonctionne dans tous les navigateurs web modernes, y compris les mobiles. Le code WebAssembly peut accéder à toutes les fonctionnalités du navigateur via leur moteur JavaScript. Cela s'appelle l'interopérabilité JavaScript, JavaScript interop ou bien encore JS interop. Le code. NET exécuté via WebAssembly dans le navigateur s'exécute dans le bac à sable JavaScript du navigateur avec les protections idoines contre toute tentative d'action malveillante sur l'ordinateur du client. Quand une application Blazor WebAssembly est créée et exécutée, voici ce qu'il se passe :

- Les fichiers de code C# et les fichiers Razor sont compilés en assemblys. NET.
- Les assemblys et le runtime. NET sont téléchargés dans le navigateur.
- Blazor WebAssembly démarre le runtime. NET et le configure pour charger les assemblys de l'application. Il a pour cela recours à l'interopérabilité avec JavaScript pour gérer la manipulation du modèle DOM et les appels d'API du navigateur.

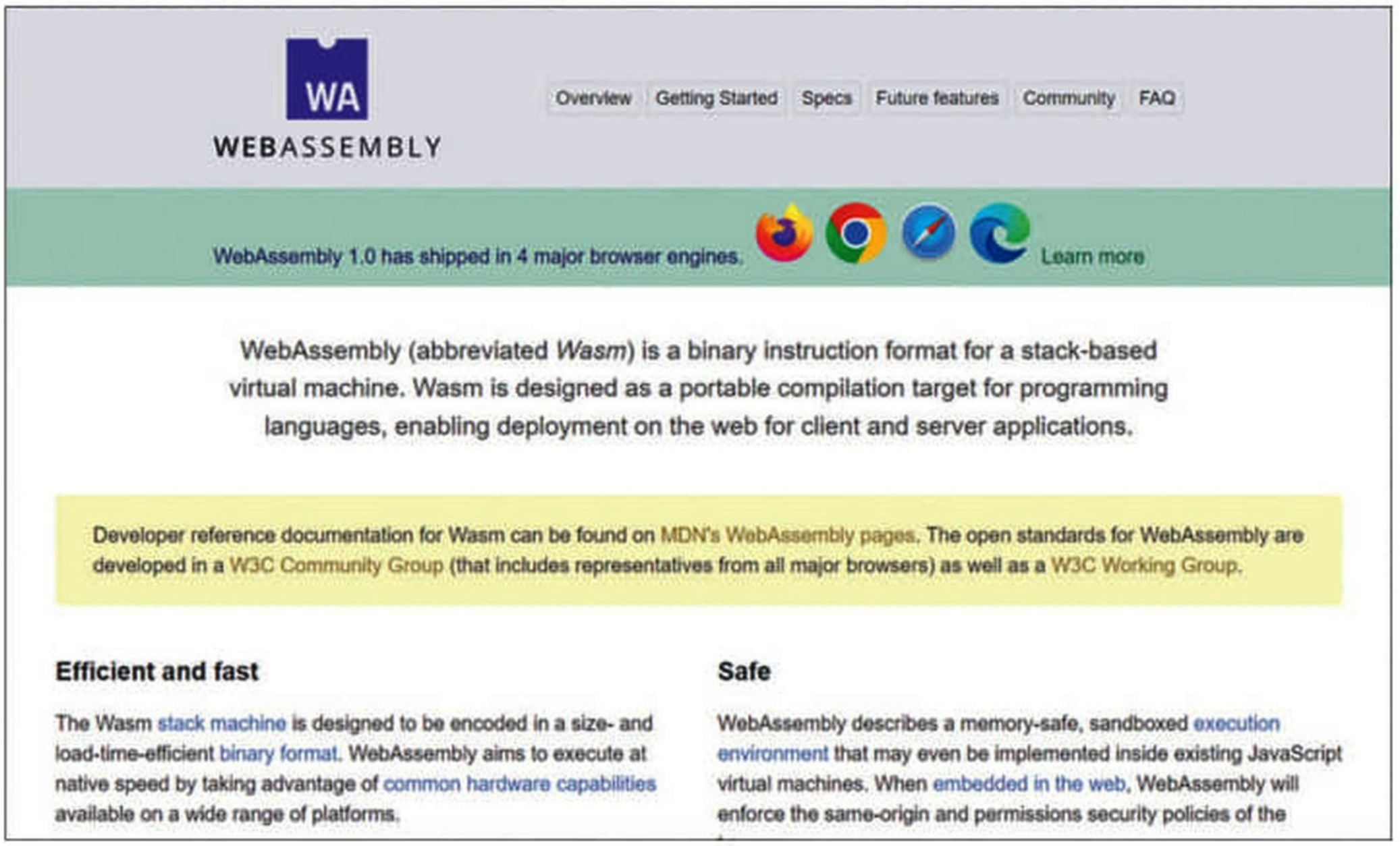
La taille de l'application publiée, c'est-à-dire sa taille de charge utile (ou payload dans la langue de Shakespeare), est un facteur de performance critique pour une application web. Le téléchargement d'une application volumineuse dans un navigateur peut prendre beaucoup de temps et nuire à l'expérience utilisateur. Blazor WebAssembly optimise la taille de cette charge utile afin de réduire les temps de téléchargement. Il a recours pour cela à plusieurs techniques. D'abord, le code inutilisé est retiré de l'application au moment de sa publication. Les réponses HTTP compressées et le runtime. NET, assemblys inclus, sont mis en cache dans le navigateur. Techniquement, vous pouvez utiliser tous les packages NPM existants avec Blazor, mais la configuration peut parfois s'avérer relativement complexe. Il est

PETITE HISTOIRE D'ASP. NET

Blazor ne représente qu'une petite partie de l'écosystème ASP. NET. La plateforme ASP. NET a presque 20 ans d'existence et s'est constamment améliorée au fil du temps. Au début, ASP. NET était utilisé pour créer toute sorte d'applications Web. ASP. NET MVC (Model-View-Controller) permettait de créer des pages Web basées sur les données. ASP. NET WebAPI était lui spécialisé dans les API backend. Ces outils n'ont pas réellement disparu. Ils ont récemment été fusionnés dans un package unifié intégré au nouveau noyau ASP. NET. Razor Pages (à ne pas confondre avec Blazor, même si leurs noms prêtent à confusion) a été publié il y a cinq ans pour simplifier la syntaxe très expressive de MVC. Razor permet de créer des pages ou des composants en intégrant le code directement sur la page. Néanmoins, les pages MVC/Razor traditionnelles utilisant ASP. NET ne sont pas assez efficaces et conduisent souvent à des conceptions brouillonnes. Blazor a justement été créé pour répondre à cette problématique. Son fonctionnement est assez similaire à celui de React ou d'Angular : les actions modifient l'état et les accessoires et déclenchent des mises à jour de l'application. Le framework se charge de mettre à jour le DOM en conséquence en fonction des composants concernés. Cela permet de concevoir des applications plus orientées temps réel où la page peut être mise à jour ou même complètement redessinée sans devoir pour autant la recharger.



Pour tout savoir sur Blazor et ASP. NET Core 7, rendez-vous sur le site de Microsoft dédié à ces technologies à l'adresse : https://learn.microsoft.com/fr-fr/aspnet/core/blazor/hosting-models?view=aspnetcore-7.0



WebAssembly (Wasm pour les intimes) a été conçu comme une cible de compilation portable pour les langages de programmation. Pour en savoir plus sur ce formidable outil, rendez vous sur le site de Mozilla à l'adresse https://developer.mozilla.org/fr/docs/WebAssembly/Concepts ou sur celui qui lui est dédié, https://webassembly.org

plus simple d'employer des packages NuGet. Microsoft prévoit d'aller encore plus loin avec Blazor Desktop. L'entreprise de Seattle a comme projet final de se débarrasser complètement de la dépendance à un navigateur et à JavaScript et d'exécuter directement un conteneur natif avec une vue Web. NET de bout en bout. Cette vue utiliserait un moteur Web tel que Safari, WebKitGTK ou WebView2, selon le système d'exploitation cible.

Blazor Hybrid

Les applications hybrides mélangent allégrement les technologies web et les natives. Une application Blazor Hybrid peut utiliser Blazor dans une application cliente native. Les composants Razor s'exécutent de manière native encore dans le processus. NET et affichent l'IU web dans un contrôle Web View intégré. WebAssembly, en revanche, n'est pas utilisé dans ce type d'applications (les hybrides). Ces applications englobent les technologies suivantes :

- .NET Multi-platform App UI (. NET MAUI), un framework multiplateforme pour la création d'applications mobiles et de bureau natives en C# et XAML.
- WPF (Windows Presentation Foundation), le bon vieux (mais pas tant que cela) framework d'IU indépendant de la résolution, pour concevoir aussi bien des applications de type client lourd que des applications Web.
- Windows Forms, le framework à base de composants graphiques destinés à créer des applications de bureau pour Windows.

JavaScript interop

Les applications nécessitant des bibliothèques JavaScript tierces et l'accès à des API de navigateur utilisent des composants qui interagissent avec JavaScript. Le code C# peut appeler du code JavaScript et, réciproquement, le code JavaScript peut appeler du code C#.

L'avenir de Blazor

Il existe plusieurs déclinaisons de Blazor, cinq en tout. Deux versions ont été publiées depuis un certain temps : Blazor Server, qui fonctionne comme React Server Side Rendering et permet de réaliser la majeure partie du traitement côté serveur, et Blazor WebAssembly qui donne elle la possibilité d'exécuter du code. NET dans un navigateur Web. Microsoft a également publié trois autres versions de Blazor plus récemment :

- Blazor PWA, conçue autour du concept de publication du site en tant qu'application Web progressive (Progressive Web Application) et installable.
- Blazor Desktop/Hybrid qui permet d'intégrer des applications Blazor dans des applications de bureau. Son fonctionnement est bien évidemment très proche de celui d'Electron qu'il concurrence ouvertement. Il a l'avantage d'offrir de bien meilleures performances.
- Blazor Native, enfin, qui remplace l'interface utilisateur Web par une interface native de la plateforme.

T.T

Alberto Pan,
Chief Technology Officer,
Denodo

ACCÉLÉRER LA CRÉATION DE VALEUR GRÂCE AU *DATA MESH* ET DENODO

Une approche de gestion décentralisée de la donnée selon le concept du Data Mesh permet d'accroître l'agilité des organisations data driven, garantir la qualité de la donnée et en démocratiser l'accès à tous les utilisateurs

POUR EN SAVOIR PLUS

denodo

Denodo est un leader en gestion des données. La solution primée Denodo Platform est la plateforme leader en matière d'intégration, de gestion et de livraison des données, grâce à une approche logique pour permettre la BI en libre-service, la data science, l'intégration des données hybride/multi-cloud et les services de données métiers.
Les clients de Denodo, des moyennes et grandes entreprises dans plus de 30 secteurs d'activité, ont obtenu un ROI de plus de 400 % et réalisé des millions de dollars de bénéfices en moins de 6 mois.

www.denodo.com/fr https://www.linkedin.com/company/denodo-technologies/

Chiffrement

20 énigmes ludiques pour se perfectionner en cryptographie

L'art du chiffrement et du secret date de plusieurs millénaires. L'ouvrage de Pascal Lafourcade et Cristina Onete vous lance différents défis autour de ce thème du chiffrement et permet de découvrir les concepts clés de cet art du secret. La difficulté de ces énigmes est progressive et permet d'avancer pas à pas pour se perfectionner.

Si vous avez du mal à découvrir les solutions, des indices émaillent l'ouvrage. À la fin du livre, une explication détaillée vous donnera la clé de chaque énigme.
En complément de ces 20 énigmes, de très nombreux encadrés vous présentent les techniques qui se cachent derrière les codes secrets les plus célèbres et les personnages historiques qui les ont créés ou les ont « cassés ».
Pour s'y retrouver dans un monde qui est aujourd'hui de plus en chiffré, la plupart des échanges actuels sur Internet utilisent le protocole HTTPS qui est la version chiffrée de http. Bonne chance à vous, car toutes les énigmes ne sont pas si simples !

Une démarche anonyme

Une montre connectée mesure l'activité réalisée par semaine en nombre de kilomètres parcourus à pied. Elle possède un mécanisme de récompenses, qui encourage les utilisateurs à avoir une vie plus saine.

Le fournisseur veut démontrer l'efficacité de cette montre. Avec l'accord de ses clients, il se propose de publier des données (anonymisées) de ses clients et des statistiques qui montrent l'impact positif de son produit sur leur santé. Pour chaque utilisateur, l'entreprise stocke son nom, mais aussi : une tranche d'âge, le sexe, le département de résidence, le revenu par an et le nombre de kilomètres parcourus par semaine dans les cinq premières semaines.

Pour anonymiser la base de données, il faut d'abord enlever les noms des clients, ce qui donne une base de données au format suivant :

Âge	Sexe	Département	Salaire	Nombre km/semaine
40-50	H	23	57 000	12, 13, 13, 15, 14
20-30	H	35	22 000	20, 20, 15, 25, 22
20-30	H	75	25 000	13, 15, 15, 18, 20
30-40	F	75	42 000	25, 28, 30, 30, 32

K-ANONYMAT

En 1998, Pierangela Samarati et Latanya Sweeney tentent de trouver une réponse à la question de recherche suivante : *dans le contexte d'une analyse sur des données sensibles de certains utilisateurs, est-il possible d'anonymiser l'ensemble des données traitées de telle façon que les utilisateurs restent anonymes, mais que l'analyse sur les données anonymisées reste utile ?*
Les deux chercheuses ont répondu à cette question par l'affirmative : elles ont avancé l'idée de trouver les attributs sensibles qui peuvent identifier un utilisateur, des plus identifiants (comme les nom, prénom ou numéro de Sécurité sociale) aux plus vagues (comme la religion, l'âge, le code postal, etc.) — et ensuite de s'assurer que, sur l'ensemble de données, chaque attribut apparaît au minimum *k* fois. Plus la valeur de *k* est élevée, plus l'anonymat est garanti par les données.

Est-ce que les données sont anonymisées ? Difficile à dire !

Par exemple si un attaquant connaît une femme qui utilise sa montre, alors avec les entrées de la base de données ci-dessus, il aura directement une information sensible

sur elle, notamment son revenu. Un attaquant qui connaît une personne dans le département 23 (Creuse) qui utilise cette montre pourra directement déduire son revenu.

Par conséquent, pour la publication des données, le fournisseur veut garantir le 3-anonymat (un cas particulier du *k*-anonymat) pour l'âge, le sexe et le département de résidence : chaque valeur de chacun de ces attributs devra apparaître au moins 3 fois.

Si les attributs identifiants des données sont l'âge, le département et le sexe, alors l'ensemble de données publiées devrait comporter au minimum *k* fois la même tranche d'âge, le même département et le même sexe. Les données de la figure 1 assurent le 3-anonymat, mais pas le 4-anonymat (car il n'y a que 3 occurrences de chaque département, par exemple).

Âge	Sexe	Département	Salaire	Nombre km/semaine
40-50	H	23	57 000	12, 13, 13, 15, 14
30-40	F	75	42 000	25, 28, 30, 30, 32
20-30	H	35	22 000	20, 20, 15, 25, 22
30-40	F	35	27 000	20, 22, 22, 25, 23
20-30	H	75	25 000	13, 15, 15, 18, 20
40-50	F	35	57 000	15, 14, 17, 0, 1
30-40	H	23	57 000	12, 13, 13, 15, 14
40-50	H	75	30 000	6, 6, 7, 6, 8
20-30	F	23	33 000	20, 24, 24, 30, 28

Figure 1 - Base de données 3-anonyme.

Le fournisseur de montres est satisfait de l'extrait de sa base de données. Elle a désormais au moins 3 participants dans chaque tranche d'âge, il y a au moins 3 participants de chaque sexe, et chacun des 3 départements apparaît 3 fois.

Énigme 2 : *Le fournisseur montre sa base de données à un ami cryptographe qui habite la Bretagne. Sa question : la base de données est-elle suffisamment anonymisée ? Son ami regarde... et déclare avoir directement reconnu une voisine, qui s'était cassé la jambe récemment et qui ne s'était toujours pas remise de son accident.*
Quel est le revenu de la voisine en question ?

Route 666

Un célèbre chanteur de rock qui habite aux États-Unis décide de publier son numéro de téléphone d'une façon cachée sur Internet. Comme tous les numéros aux États-Unis, le sien commence par le code national 001, qui est suivi par un code de zone (area code) à 3 chiffres, un préfixe à 3 chiffres, puis un numéro unique à 4 chiffres.

Il hache son numéro en utilisant la fonction de hachage SHA-256, il obtient ainsi :
9dd8646d336e4dc5b08b5f15e3fe6980e645f1f96e79862b54460e4d21287819.

Il publie le texte suivant sur Twitter :

Trouvez-moi si vous pouvez ! #Rock #SHA256 #9dd8646d336e4dc5b08b5f15e3fe6980e645f1f96e79862b54460e4d21287819 #USA #ZONE555 #PREFIXE666

Énigme 3 : *Quel est le nombre de valeurs à essayer, étant donné l'accès à la fonction de hachage SHA-256, pour trouver le numéro de téléphone du chanteur de rock par force brute ?*

En cryptographie, une attaque par force brute consiste à essayer toutes les solutions possibles pour retrouver une valeur particulière : un mot de passe, un code secret, la valeur d'une clé privée, etc.

En suivant le principe de Kerckhoffs — qui postule qu'aucun cryptosystème ne devrait se baser sur l'obfuscation de la méthode utilisée — la cryptographie moderne demande l'utilisation de certaines valeurs dites secrètes : des clés, certains nombres aléatoires, etc. Ces valeurs

LE DÉFI SNAKE #1

En mai 2023, un défi a été lancé par un trio de chercheurs français : Louis Béziaud, Tristan Allard et Sébastien Gambs. Ils ont ouvert une compétition sur des algorithmes qui génèrent des données anonymisées à partir d'un ensemble de données. Dans la vraie vie, ces données pourraient appartenir à un hôpital ou à une caisse d'assurances. Pour réaliser des statistiques sur ces données sensibles, il faut bien entendu les anonymiser avant de les utiliser.
Le défi Snake est de trouver des corrélations entre les données — c'est-à-dire des faiblesses dans les algorithmes d'anonymisation. Les participants ont accès à l'ensemble de données que l'algorithme a reçu en entrée, l'ensemble généré par l'algorithme, la paramétrisation des paramètres spécifiques à l'algorithme utilisé et un nombre de cibles. Le but est d'indiquer la probabilité que certaines cibles se trouvent dans l'ensemble de sortie de l'algorithme ou non.

La compétition se trouve en ligne :
www.codabench.org/competitions/879/

AUGUSTE KERCKHOFFS (1835-1903)

Auguste Kerckhoffs, né le 19 janvier 1835 à Nuth (Pays-Bas), décédé le 9 août 1903, était un grand linguiste et cryptographe. Son essai La cryptographie militaire, publié en 1883, est un ouvrage de référence dans le domaine. Il présente des principes sur lesquels les cryptosystèmes modernes devraient reposer pour être utilisés en toute sécurité dans des cas d'usages militaires. Parmi les 6 principes évoqués dans son texte, les trois suivants ont révolutionné la cryptographie moderne* :

► *« Le système doit être matériellement, sinon mathématiquement, indéchiffrable »* : ce principe indique l'utilité des primitives et des protocoles cryptographiques à sécurité computationnelle (l'attaquant ne réussit pas à les casser dans un temps raisonnable).

► *« Il faut qu'il n'exige pas le secret, et qu'il puisse sans inconvénient tomber entre les mains de l'ennemi »* : la sécurité d'un schéma cryptographique ne doit pas reposer sur le secret (de la part de l'attaquant) des algorithmes que le schéma utilise. Aujourd'hui la plupart des algorithmes cryptographiques existants sont publics, ce qui permet d'analyser leur sécurité.

► *« La clé doit pouvoir en être communiquée et retenue sans le secours de notes écrites et être changée ou modifiée au gré des correspondants »* : ce principe introduit la notion d'une clé facilement utilisable et renouvelée souvent.

**Toutes les citations sont extraites de La cryptographie mllitaire, travail publié dans le Journal des sciences militaires, volume IX, pages 5-38 (janvier 1883) et pages 161-191 (février 1883).*

sont typiquement tirées de façon aléatoire dans un ensemble qui est connu par l'attaquant. Ce dernier peut donc mener une attaque par force brute pour trouver le secret choisi. Pour se prémunir contre ce type d'attaque, plusieurs méthodes sont utilisées :

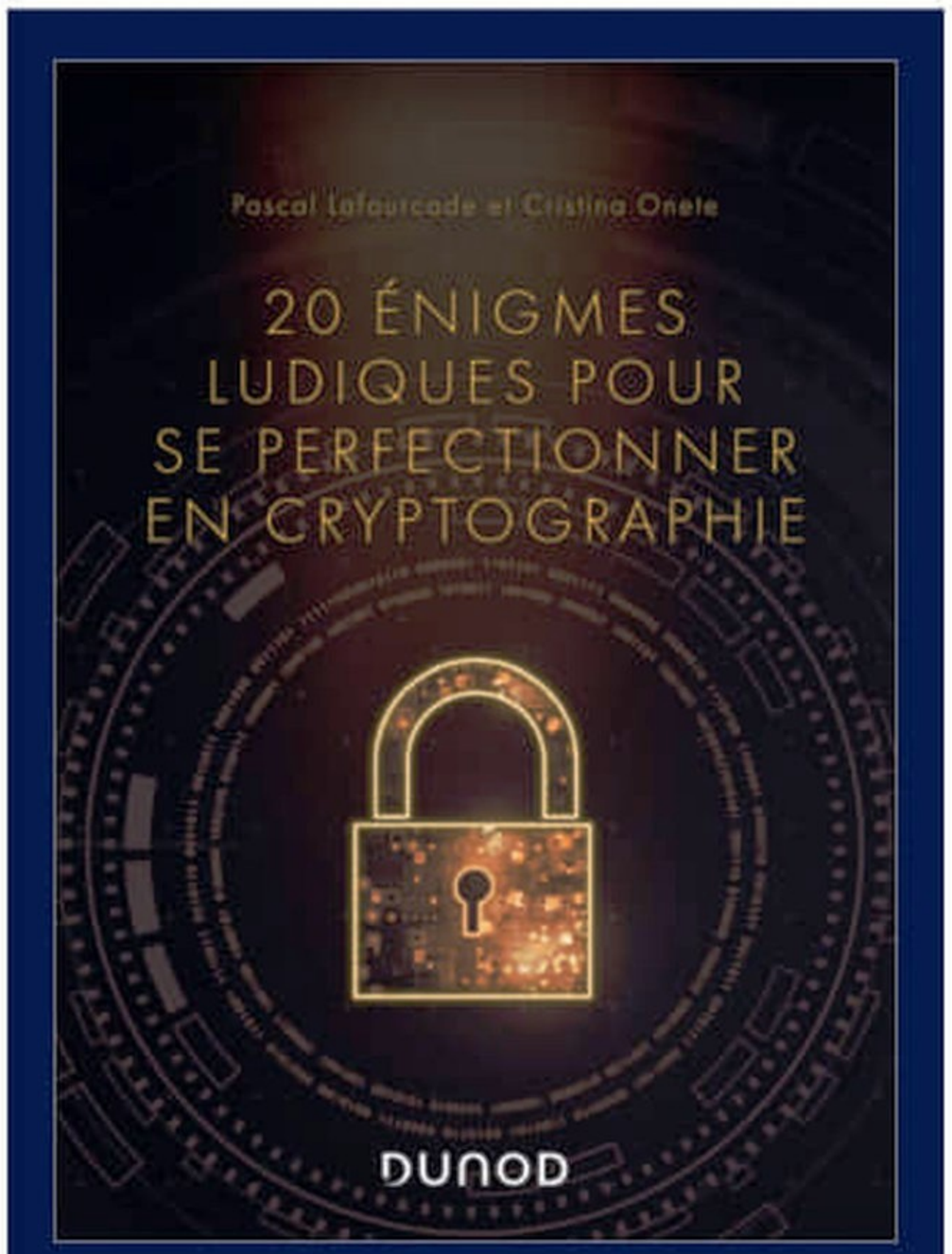
• Les clés sont choisies dans un ensemble de taille très large, rendant la tâche d'un attaquant plus difficile. Un attaquant cherchant à trouver une valeur secrète qui se compose de 128 bits aléatoires se confronte à un espace de $2^{128} \approx 10^{39}$ valeurs possibles. Si l'attaquant a besoin d'une nanoseconde (0,000000001 seconde) pour tester chaque valeur, il lui faudra plus de 32•1024 ans (32 milliards de milliards d'années) pour essayer toutes les possibilités.

• L'attaquant a un nombre limité d'essais avant que le secret change ou qu'une vérification ait lieu. Par exemple, chaque utilisateur a 3 essais consécutifs pour trouver le code de sa carte bancaire avant que le compte soit verrouillé.

• Utiliser une solution cryptographique moins efficace, mais avec une sécurité parfaite, comme le chiffrement à masque unique.

Cette méthode de chiffrement prévoit d'utiliser une clé unique et aléatoirement choisie à chaque chiffrement, ce qui cache un message d'une certaine taille parfaitement parmi tous les textes possibles de la même taille.

Comme la cryptographie moderne emploie souvent des clés suffisamment longues, l'enjeu des attaquants est de réduire l'espace de valeurs possibles avant de se lancer dans une attaque par force brute : soit par des méthodes mathématiques ou physiques, soit en utilisant d'autres sources d'information via l'ingénierie sociale, le hameçonnage, etc. □



224 pages
Collection
HORS COLLECTION
Dunod
Tout public
EAN9782100855117
EAN EBOOK : PDF 9782100863334

Optimisation

RAILwAI veut éviter la vie duraille !

RAILwAI est une startup française créée en octobre 2021 sise à Montpellier. Sa spécialité est de proposer une solution de maintenance préventive s'appuyant sur l'intelligence artificielle.

Les deux cofondateurs de l'entreprise sont partis d'un constat : il y a beaucoup de données dans le monde des transports, mais très peu de celles-ci sont utilisées, soit moins de 20 %. La plupart des sociétés du secteur réalisent d'ailleurs la maintenance de manière empirique. Elle est le plus souvent corrective, voire préventive dans le meilleur des cas. Le prédictif a encore tout son chemin à faire.

L'intelligence artificielle peut grandement aider les opérateurs sur la maintenace et la fiabilité de leur réseau pour lutter contre les retards.

Une situation dégradée

La demande de moyens de transports de plus en plus durables ajoute une contrainte sur les transports ferroviaires qui connaissent une forte tension. Le moindre incident crée des retards... et des mécontentements chez les usagers devenus clients des sociétés de transports. Ainsi, 10 % des trains sont en retard en Europe. La solution de l'éditeur vise à rendre l'infrastructure ferroviaire plus fiable et disponible pour ce moyen de transport considéré comme le plus propre. Les salariés de RAILwAI viennent à la fois du monde des transports et de la donnée et souhaitent apporter une réponse concrète aux problèmes du ferroviaire. Selon Bruno Dabilly, le directeur général de la société : *« nous avons constaté une baise des coûts de maintenance de 10 à 15 % chez nos clients et une hausse de 15 % de productivité »*. Ces chiffres sont en phase avec une autre étude réalisée par McKinsey sur la maintenance du secteur ferroviaire. La société a ouvert une filiale en Espagne, un marché qui recèle un important potentiel et l'expansion internationale est au programme avec des discussions et des prospects dans d'autres pays. La société regarde aussi des partenariats avec des grands groupes du transport qui ont déjà des implantations locales.

Une combinaison de modèles

La solution combine différents types d'intelligence artificielle et de modèles. Nos interlocuteurs ont pris bien soin de préciser qu'ils ne s'occupent pas du matériel roulant et ne fournissent pas de capteurs ou de matériels. La plateforme unifiée collecte, ingère. RAILwAI nettoie, enrichit et traite les données pour fournir des prédictions, des rapports ou des analyses. Sur le marché, la plupart des solutions ne fonctionnent que sur des dépassements de seuils. La solution va plus loin en donnant une contextualisation pour définir d'où vient le défaut. La plateforme est très ouverte et permet d'ingérer quasiment toutes les sources de données présentes sur le marché. Selon leur sensibilité, les données peuvent être traitées différemment. De plus, il est possible de prévoir ou d'anticiper ce qui pourrait entraîner des risques pour les voyageurs. La solution s'appuie sur Big Query et l'infrastructure de Google Cloud Platform. La solution est facturée au déploiement des différents modules de la plateforme et des frais de licences pour l'utilisation des modules. L'éditeur réfléchit à un modèle par abonnement plus flexible.

Pour tous les transports

Jusqu'à présent, la solution ne vise pas les opérateurs structurants comme les grands réseaux type SNCF ou Deutsche Bahn, mais elle est adaptée pour des réseaux urbains comme le métro, les tramways, les réseaux de transports portuaires... □

B.G

Bio-informatique

Une IA à base de cellules souches

Une petite société suisse s'est lancée depuis presque 10 ans dans la conception de « bio-processeurs », comprendre de vrais neurones issus de cellules souches. Si l'approche reste embryonnaire, le dispositif est aujourd'hui opérationnel pour de premières expérimentations.

Remplacer le silicium par de vrais neurones pour disposer d'applications d'IA ? Ce pourrait être la prochaine étape. C'est, en tout cas, le pari du suisse FinalSpark. *« Nous ne sommes qu'au stade embryonnaire de cette approche »*, insiste Fred Jordan, cofondateur de la société. Pourquoi aller dans cette voie qui pose de nombreuses questions éthiques ? Elle présente plusieurs avantages conséquents. Un cerveau humain composé de dizaines de milliards de neurones ne consomme que 20 watts. Son équivalent, en termes de nombres de « neurones » en silicium, consommerait au moins 10 mégawatts selon l'Université de Stanford. Constat similaire pour la scalabilité de cette approche, plus facile à mettre en œuvre avec l'ajout de « bio-processeurs ». Enfin, côté recyclage *« jeter au compost suffit »*, s'amuse Martin Kutter, l'autre cofondateur.

Fred Jordan et Martin Kutter, cofondateurs de FinalSpark.

Créée en 2014 par Fred Jordan et Martin Kutter, la start-up a mis au point un dispositif expérimental basé sur des neurones destinés à calculer ou à stocker de l'information. *« Une grande partie du travail a consisté, et consiste toujours, à bien "nourrir" ces neurones issus de cellules souches, une approche biologique avant tout »*, explique Martin Kutter. Les cellules souches, des cellules de base produites chez l'humain par la moelle osseuse ont été découvertes dans les années 60. En 2006, le futur prix Nobel de médecine Shinya Yamanaka trouve le moyen de les programmer dans une déclinaison dite pluripotente induite ou iPS par l'insertion de gènes. Traduction, ces cellules peuvent se spécialiser et, entre autres, peuvent évoluer en précurseurs neuronaux, puis en neurones. FinalSpark utilise celles-ci, regroupées en amas de quelques milliers d'unités baptisées « neuro-sphères ». *« Pour l'instant, leur durée de vie reste de l'ordre de trois mois. Nous cherchons à améliorer cette durée en particulier à travers la vascularisation de ces amas »*, détaille Martin Kutter. Ces neuro-sphères sont déposées à l'aide de pipettes sur des électrodes en platine, et y adhèrent naturellement. *« Ces électrodes servent à la fois à la lecture et à la stimulation des signaux électriques »*, ajoute ce dernier.

Premier constat, les neuro-sphères génèrent une activité électrique spontanée, *« à l'instar du cerveau par exemple pendant le sommeil »*, souligne Fred Jordan. Elles réagissent également aux stimulations électriques. *« Nous travaillons sur des patterns, en d'autres mots, nous cherchons à établir une répétabilité entre des types de stimulation et de réponse »*, explique Fred Jordan. La démarche consiste concrètement à envoyer des séquences de stimulations à partir des différentes électrodes et de *« récompenser »* les neuro-sphères en ajoutant dans la culture nourrissante de la dopamine. *« Tester ces modèles est très simple. Nous avons développé une interface permettant de les programmer en Python »*, souligne Fred Jordan.

Si très peu d'entreprises se sont lancées dans l'aventure à ce jour, quelques laboratoires académiques se penchent sur la question. *« Notre plateforme est ouverte, plusieurs labos, l'Institut Neuromod de l'Université Côte d'Azur entre autres, l'utilisent dans le cadre de leurs recherches »*, appuie Fred Jordan. □

PBr

FINALSPARK SURTOUT FINANCÉ PAR UNE AUTRE START-UP

Les deux créateurs de FinalSpark ont créé en 2001 une autre société, AlpVision, spécialisée dans la lutte contre la contrefaçon. La technologie qu'ils ont développée repose sur l'ajout de microstructures sur les emballages, blisters ou produits, invisibles à l'œil nu, et identifiables à travers une application embarquée dans un smartphone. Ce, même si une partie de l'emballage est abîmée. Cette technologie est compatible avec les outils dédiés à la fabrication des emballages sans nécessiter d'étape supplémentaire. *« La solution peut être utilisée dans de nombreux domaines, pour authentifier des médicaments, des lingots d'or... Notre plus gros marché est la pharmacie, celui pour lequel les conséquences de la contrefaçon sont les plus graves. Plus de 30 milliards de produits utilisent notre technologie »*, illustre Martin Kutter. Les deux hommes continuent à gérer AlpVision en parallèle de FinalSpark.

Prospective

Les impacts forts sur le secteur du numérique d'ici 2040

Jean-Claude Laroche, le président du Cigref, a présenté mi-octobre le rapport d'orientation stratégique de cette association composée de Directeurs des Services Informatiques (DSI) des grands groupes. Il évoque 10 hypothèses de ruptures économiques, technologiques ou sociétales pouvant impacter fortement le secteur du numérique d'ici 2030-2040.

Cette 53ème AG du Cigref était concentrée sur la (re)valorisation des notions de progrès et de sobriété numérique notamment. Des thèmes d'ailleurs traités dans son nouveau rapport d'orientation stratégique (ROS), qui contient 10 hypothèses de rupture pouvant impacter fortement le secteur du numérique d'ici 2030-2040.

Quatre d'entre elles méritent que l'on s'y attarde, dont la rupture 2 évoquée par le Cigref. Celle-ci postule que le déploiement des réseaux mobiles 5G, puis de la 6G, mais aussi l'introduction de concepts tels que l'Open RAN, accéléreraient la virtualisation, l'automatisation et la désagrégation des réseaux télécoms d'ici 2030.

Jean-Claude Laroche, président du Cigref.

Cette association de DSI de premier plan s'inquiète également de l'ouverture de ces réseaux télécoms à de nouveaux acteurs, issus de l'informatique notamment. Avec à la clef, la séparation des différentes fonctions d'accès *via* des briques interopérables, dotées d'interfaces ouvertes, telles que permises par ces nouvelles technologies réseau.

Selon le Cigref, *« cette évolution permettrait à des entreprises spécialisées dans la virtualisation et le cloud, telles que VMWare, RedHat et les géants américains du cloud, d'entrer sur le marché des services télécoms. En créant des tranches de réseaux cloisonnées (network slicing), ces nouveaux acteurs pourraient proposer des offres personnalisées avec un débit plus important, une gestion réseau plus souple et une moindre latence »*. Et quid alors de la création éventuelle d'un réseau Internet privé à plus haut débit garantie ?

Et d'en conclure que cette ouverture favoriserait ces acteurs américains du cloud, au détriment d'équipementiers européens traditionnels, tels que Ericsson et Nokia, qui ont jusque-là dominé le marché télécoms.

Une réglementation de l'UE impose à l'industrie numérique un recyclage à 100 %

La Rupture numéro 4 évoque un thème désormais important pour Jean-Claude Laroche : celui de l'impact environnemental du Numérique. Il considère la sobriété numérique comme le premier défi à relever par le Cigref. Il invite donc les DSI, et surtout leurs fournisseurs IT, à réaliser davantage de progrès dans ce domaine : *« le Cigref s'implique activement sur cette thématique depuis plus d'une décennie. Mais il faut aller plus loin pour progresser en termes de sobriété numérique, en se concentrant sur un fait : les études montrent que la fabrication du matériel informatique représente 70 % de cette empreinte environnementale »*.

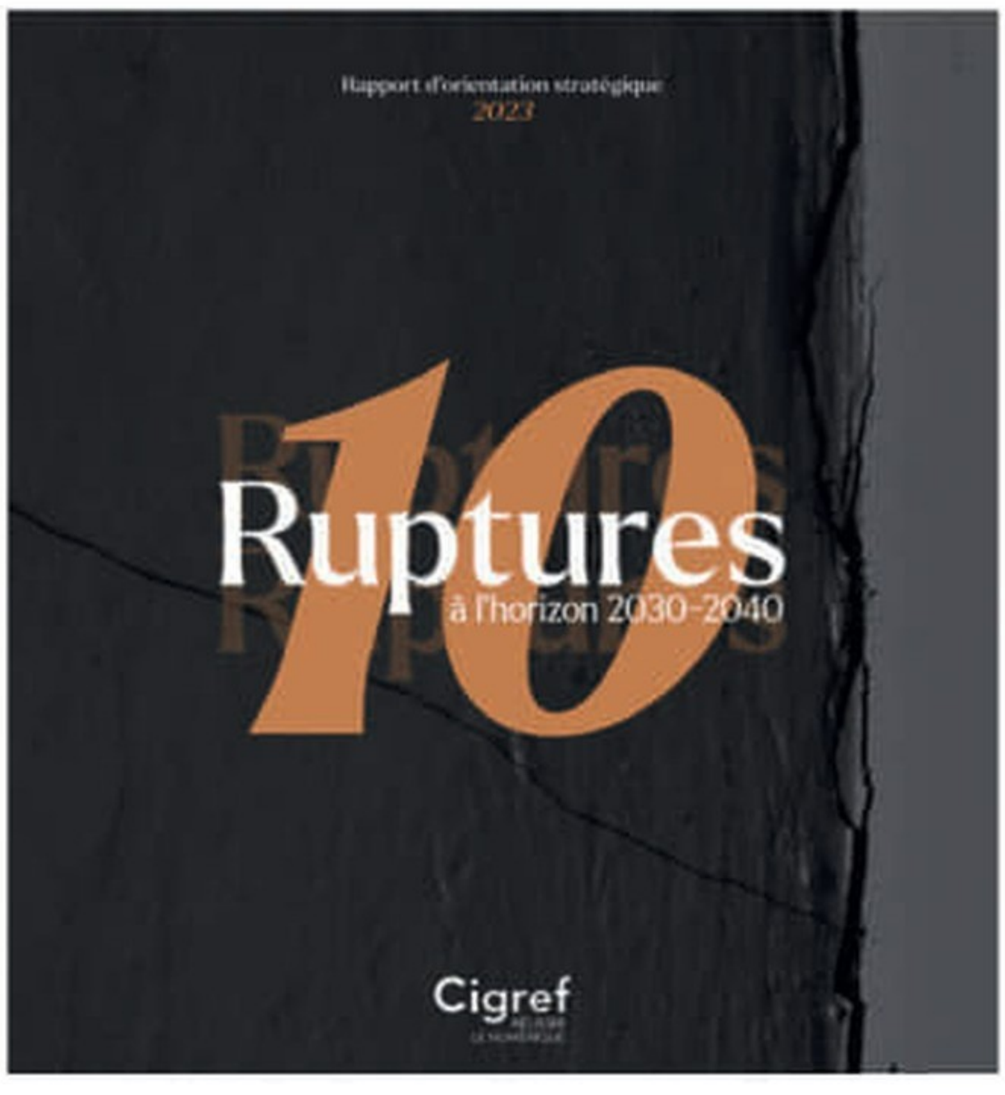
Dans ce cadre, le ROS du Cigref pose l'hypothèse selon laquelle l'Union européenne imposerait à l'industrie numérique le recyclage à 100 % de tous les composants et matériels informatiques à l'horizon 2040. *« Cette réglementation favoriserait la réduction des déchets électroniques et stimulerait la recherche et le développement de technologies de recyclage innovantes. Les fabricants devraient revoir leurs processus de conception pour garantir que les composants peuvent être facilement démontés et recyclés en fin de vie »*.

Et cette association de DSI d'en conclure que *« cette évolution créerait de nouvelles opportunités pour les entreprises du secteur, mais elle pourrait également entraîner des coûts d'achat plus élevés pour les entreprises et les consommateurs. L'objectif serait de diminuer l'empreinte environnementale du numérique et de favoriser une économie circulaire plus durable »*.

Jean-Claude Laroche met donc cette industrie au défi de changer dès que possible les modes de fabrication des matériels et équipements numériques : *« l'objectif doit être de réduire de manière décisive les activités extractives et les émissions de carbone générées par cette industrie »*. Au final, il invite les Gouvernements à *« mettre en place une régulation adaptée à l'industrie des équipements numériques afin de les rendre, de façon significative, plus durables, plus réparables et plus recyclables »*.

2040, Les GAMMA se sont effondrés

L'hypothèse envisagée par le Cigref à l'horizon 2040 est l'une des plus surprenantes parmi les 10 points traités dans son rapport. En effet, elle évoque un possible ralentissement plus marqué de la croissance des géants du numérique, dont celles des Gamma (Google, Amazon, Microsoft, *etc.*). Il s'accompagnerait alors d'un effondrement progressif de leur capitalisation boursière.



Cette rupture pourrait résulter de divers facteurs. Cette association de DSI cite par exemple l'incapacité de ces fournisseurs à s'adapter à des évolutions technologiques majeures ou à des changements profonds dans les usages numériques de leurs clients. N'est-ce pas un peu surprenant sachant que les technologies numériques inventées et commercialisées par les Gamma et les Batx, leurs homologues chinois, s'imposent souvent à nos usages et font office de mode ?

Le Cigref motive également cette perte de leadership des MAG par l'apparition d'exigences législatives accrues en matière de concurrence, ou d'événements extérieurs, telles que des décisions politiques restrictives ou des chocs géopolitiques, économiques ou environnementaux. Optimiste mais pragmatique, le Cigref estime au final que la disparition éventuelle de ces oligopoles américains du numérique pourrait favoriser l'émergence de nouveaux acteurs locaux, tout en compliquant cependant l'accès à certains de leurs produits et services numériques déjà installés. Dans leurs clouds notamment.

D'ici 2030, l'Intelligence Artificielle, modifiera radicalement l'organisation du travail

Une autre hypothèse de rupture envisagée par le Cigref, à l'horizon 2030, prédit que l'IA générative (Gen AI) soit largement adoptée et permette d'automatiser de nombreuses tâches en entreprise. Et cela grâce à une meilleure compréhension de ses capacités et à son intégration plus poussée dans les outils numériques BtoB utilisés. Certes, l'efficacité et la productivité des employés augmenteraient, mais cela pourrait également entraîner des pertes d'emplois et nécessiter des reconversions professionnelles.

Cependant, de nouveaux métiers liés au développement et à la supervision de l'IA générative pourraient émerger, créant ainsi de nouvelles opportunités selon le Cigref. Cette évolution pourrait également réduire le temps de travail des employés, impactant les équilibres entre vie privée et vie professionnelle. Jean-Claude Laroche considère donc que *« si ces avancées technologiques ont ouvert de nouvelles perspectives, elles ont également soulevé des questions éthiques et sociétales quant à l'impact de l'IA sur l'emploi, la formation, la vie privée et la confiance dans les systèmes automatisés. La technologie engage complètement notre responsabilité. Et de ce point de vue, je ne vois pas de raison de considérer l'intelligence artificielle d'une façon différente des autres technologies »*. □

Olivier Bellin

Facilitez les accès numériques de vos prestataires, en maintenant une cybersécurité maximale

Vos prestataires ont besoin de se connecter au SI de votre entreprise. Problème : ils sont très nombreux et changent régulièrement. Gérer et sécuriser leurs accès numériques est chronophage pour vos équipes IT et coûteux.

Avec SaaS Remote Access, la technologie SaaS de sécurisation des accès distants de WALLIX, les métiers enregistrent et paramètrent eux-mêmes les droits d'accès de leurs prestataires, pour un temps donné. Les mots de passe sont isolés de l'annuaire et gérés et sécurisés par SaaS Remote Access. Vous maitrisez ainsi les cycles de vie avec une visibilité complète des accès externes, tout en respectant les normes d'audit ISA et les recommandations de l'ANSSI.

WWW.WALLIX.COM

SaaS REMOTE ACCESS

WALLIX
CYBERSECURITY SIMPLIFIED

Cyberdéfense

Le COMCYBER s'allie avec l'EPITA et L'X pour une formation spécifique

Pour répondre à ses besoins en spécialiste en cyberdéfense, le COMCYBER lance en partenariat une formation au sein du Bachelor EPITA, avec la participation active de l'École Polytechnique à la rentrée 2024.

Dès la rentrée 2024, 120 bacheliers intégreront le Bachelor en Cybersécurité de l'EPITA en association avec l'École polytechnique. Opéré par l'EPITA depuis 2021, le programme bénéficiera de la collaboration nouée avec l'École polytechnique pour proposer un enseignement renouvelé. À la solide expérience de la formation professionnalisante proposée par l'EPITA, l'École polytechnique apportera des enseignements adossés à sa recherche scientifique d'excellence pour former en 3 ans de nouveaux talents.

Un vivier de talents

Le ministère des Armées participe activement à la constitution de ce nouveau vivier de talents sous l'impulsion du COMCYBER. Ainsi, parmi les 120 étudiants du programme, 30 auront été sélectionnés pour suivre un parcours « Cyberdéfense » et rejoindre le ministère des Armées à l'issue de leur formation. Le ministère prendra en charge leurs frais de scolarité à la condition qu'ils s'engagent dans la réserve opérationnelle pendant leurs études, qu'ils obtiennent leur diplôme, et qu'ils signent un contrat d'engagement comme officiers pour une période de 5 ans. Ces 30 élèves effectueront leur 3e année en alternance au sein des forces du ministère des Armées. L'ouverture d'une voie de recrutement Cyberdéfense au sein du Bachelor Cybersécurité de l'EPITA, qui s'associe à l'X, s'inscrit plus largement dans la volonté du ministère des Armées de faire de l'École polytechnique un centre d'excellence dans le domaine de la cybersécurité. Celui-ci reposera sur le Centre Interdisciplinaire d'Études pour la Défense et la Sécurité (CIEDS) développé en lien avec le ministère des Armées.

Un niveau licence

Assorti du grade de licence, le cursus a pour objectif de former en 3 ans des experts qui acquièrent les fondamentaux du numérique tout en se spécialisant en cybersécurité dès la première année de leur cursus. Le parcours pédagogique inclut de nombreux projets permettant aux étudiants d'acquérir des compétences à la fois techniques, humaines et professionnelles. La pédagogie est fondée sur une mise en situation concrète. Deux stages sont prévus en fin de première et deuxième année, et la troisième année s'effectue en apprentissage. La localisation de la formation, au cœur du Campus Cyber national situé à La Défense, permettra par ailleurs aux étudiants de bénéficier de la présence sur site de nombreux acteurs de la Cybersécurité : entreprises de renom, institutionnels (ANSSI, INRIA) et intervenants de haut niveau. À la fin de la formation, les étudiants peuvent se tourner vers différentes fonctions comme architecte sécurité, spécialiste en développement, opérateur analyste SOC, consultant en cybersécurité, pentester, reverse codeur, analyste de malwares...

Des étudiants de l'EPITA cyberdefense lors de l'exercice DEFNET 2022. Source EPITA.

L'EPITA réalise depuis plus de dix ans des actions en collaboration avec les services de l'État et plus particulièrement, depuis six ans, avec le ministère des Armées. Depuis 2019, l'EPITA est certifié partenaire de la Défense nationale et a signé une Charte d'engagement avec la Garde nationale. □

B.G

Noms en ligne

L'AFNIC lance une formation sur les abus en ligne

L'Association française pour le nommage Internet en coopération est l'office d'enregistrement désigné par l'État pour la gestion des noms de domaine en .fr et prend aussi en charge les extensions pour les territoires d'outre-mer. L'AFNIC vient de lancer une formation sur les abus en ligne à destination des publics concernés.

Engagée dans la lutte contre les abus liés aux noms de domaine, l'AFNIC a fait le constat que les professionnels qui accompagnent les victimes de ces abus à protéger leurs droits ne connaissent que faiblement les règles qui les encadrent. L'AFNIC a donc conçu une nouvelle formation intitulée *« Noms de domaine et abus en ligne »* avec l'objectif de permettre à ses futurs apprenants de maîtriser le cadre juridique des noms de domaine, et les solutions les plus adaptées pour identifier, prévenir et faire cesser ces abus.

Un exemple de typosquatting.

Un public large

Cette formation s'adresse à toutes personnes dont la profession implique de conseiller et accompagner leurs clients à protéger et défendre leurs droits en la matière : conseils en propriété industrielle, avocats, juristes de bureau d'enregistrement ou en propriété intellectuelle d'entreprise, *etc.* Le cursus permet de définir un abus dans le secteur des noms de domaine, d'identifier les catégories d'acteurs lors d'un abus, de qualifier un abus en apprenant à faire le lien entre des faits, une situation et la qualification juridique/technique de l'abus, de lister et expliquer les solutions pour se défendre face aux abus, et enfin de diagnostiquer les solutions pertinentes à son cas d'espèce (abus) en identifiant les stratégies pour faire cesser et maîtriser l'abus et ses conséquences.

Un cycle court

La formation, s'étendant sur deux jours, est dispensée en présentiel au Campus Cyber à La Défense. Elle est animée par Nathalie Boulvard, Juriste Senior & Déléguée à la protection des données à l'AFNIC et Marianne Georgelin, Directrice Juridique à l'AFNIC. L'évaluation se déroule en deux étapes avec une première évaluation formative sous forme de quiz, et une évaluation finale sous forme de cas pratique. Le prix de la formation est de 1400 HT par étudiant. Pour plusieurs personnes, l'AFNIC propose un devis. Pour rappel, l'AFNIC est un organisme certifié Qualiopi pour les actions de formation. □

B.G

UN PODCAST POUR SE RENSEIGNER

Depuis janvier dernier, l'AFNIC a aussi lancé un podcast sur le sujet hébergé sur la plateforme Ausha. Pour son lancement, l'association a proposé 6 épisodes à écouter gratuitement qui sont consacrés aux abus en ligne : cybersquatting, phishing, usurpation d'identité... Cette première collection, réalisée en collaboration avec Makheia et Nouvelles Voix, permet de comprendre les différents types d'abus sur les noms de domaine, les risques associés et les outils mis à disposition par le .fr, précise l'AFNIC. Les titres de ces 6 podcasts sont :

1. Interview : abus sur les noms de domaine, de quoi parle-t-on et comment agir ?
2. Interview : atteintes en ligne, quels recours ?
3. Qu'est-ce que le cybersquatting ?
4. Qu'est-ce que le phishing ?
5. Qu'est-ce qu'un registre de noms de domaine ?
6. Qu'est-ce que l'usurpation d'identité dans un nom de domaine et comment s'en prémunir ?

Intelligence artificielle

OpenClassrooms présente 3 formations gratuites

Fidèle à sa mission de rendre l'éducation et les métiers qui recrutent accessibles à tous, OpenClassrooms annonce aujourd'hui le lancement de son premier cycle de formations digitales 100 % dédié à l'Intelligence Artificielle.

Ce nouveau cycle de formations gratuites comporte trois volets : un premier dédié à ChatGPT, suivi d'une formation dédiée aux technologies émergentes et enfin, une formation d'initiation à l'IA. Le premier module intitulé *« Utilisez ChatGPT pour améliorer votre productivité »* est un cours accessible à tous, créé et enregistré par Mathieu Nebra, le cofondateur d'OpenClassrooms. Son objectif est de faire ses premiers pas avec ChatGPT et de savoir l'utiliser au quotidien, car sa maîtrise deviendra déjà une compétence requise sur le marché de l'emploi.

Un deuxième cours vise à montrer comment aborder les technologies émergentes afin de pouvoir prendre des décisions éclairées sur l'opportunité et la manière de les utiliser au mieux dans sa carrière. À l'issue de ce cours, chaque apprenant sera en mesure d'identifier les opportunités d'innovation par la cartographie de la chaîne de valeur, établir un cadre d'analyse pour examiner les technologies et enfin, élaborer des hypothèses pour mettre en œuvre les technologies émergentes. « Objectif IA » se veut plus qu'une simple formation, mais un réel mouvement qui — en partenariat avec l'Institut Montaigne — ambitionne de former au moins 1% de la population française (soit 670 000 personnes) aux fondamentaux de l'IA. Le programme a été conçu par des personnalités et de nombreux experts choisis et réunis par l'Institut Montaigne, OpenClassrooms et la Fondation Abeona, de façon à proposer les éléments les plus ludiques et intuitifs possibles. Ce cours s'adresse à tous ceux qui s'interrogent sur l'Intelligence Artificielle, souhaitent s'informer et s'instruire. Les cours sont librement ouverts et ne nécessitent aucun prérequis en termes de niveaux, ils sont en accès en ligne totalement libre. □

B.G

OPENCLASSROOMS EN BREF

OpenClassrooms est une entreprise à mission certifiée B Corp avec des bureaux à Paris, New York et Londres. L'école propose de nombreux cours en accès libres et gratuits, ainsi que des programmes certifiants pour les métiers qui recrutent (tech, IT, data et bien plus encore). Le tout 100 % en ligne. OpenClassrooms crée et produit l'intégralité de ses cours et contenus pédagogiques et s'appuie sur un modèle unique en son genre, axé sur la pratique à travers des projets professionnalisants et de l'accompagnement par des mentors experts du métier.

UN ASSISTANT IA POUR LES ÉTUDIANTS

Récemment, OpenClassrooms a lancé son propre assistant IA pour apporter un soutien en temps réel à ses étudiants. Ces derniers ont besoin de réponses plus rapides, surtout lorsqu'ils sont bloqués entre des sessions de tutorat. L'assistant IA est là pour combler ce fossé, en veillant à ce que les étudiants reçoivent le soutien dont ils ont besoin, 24h/24 et 7j/7. Ils peuvent poser des questions, déboguer du code, demander des conseils sur les détails d'un projet, ou même demander une assistance étape par étape.

RGPD : Sécurisez vos appareils, sécurisez vos données !

Après les menaces en ligne et la divulgation involontaire de données, les appareils mobiles et la perte physique constituent la plus importante source de violations de données.[1]

Tous les jours, en moyenne, plus de 5 millions d'enregistrements de données sont perdus ou volés[2], et plus d'1/3 des entreprises n'ont aucune politique de sécurité physique pour protéger les ordinateurs portables, les appareils mobiles et les autres biens électroniques.[3]

Pour y palier, Kensington propose une large gamme de solutions pour protéger les appareils contre le vol, même en l'absence d'encoche de sécurité.

En cas d'infraction, l'amende peut s'élever jusqu'à 4 % du chiffre d'affaires annuel ou 20 millions d'euros. Investir dans la sécurité physique n'a jamais été aussi judicieux !

MicroSaver® 2.0 & ClickSafe® 2.0
Pour les appareils avec encoche de sécurité Kensington standard

N17
Pour les appareils avec une encoche non-standard Wedge

Solutions pour Microsoft Surface™
Pour Surface™ Pro, Book, Studio et Surface Laptop

Station de sécurité
Pour les ordinateurs sans encoche de sécurité

Trouvez le bon câble de sécurité pour votre appareil : **kensington.com/securityselector**

1. 2016 Data Breaches - Privacy Rights Clearinghouse 2. Breach Level Index, Septembre 2017 3. Kensington IT Security & Laptop Theft Survey, Août 2016

Kensington®

The Professionals' Choice™

www.linfocr.com

L'INFO CYBER-RISQUES

L'INFORMATICIEN

Le RSSI au Comex !

Sommaire

Cette édition de *L'InfoCyberrisques* s'ouvre sur un titre un brin provoc'. Le RSSI au Comex... et pourquoi pas au conseil d'administration, tant qu'à faire ! Pourtant, à la faveur de la pandémie et de l'évolution de l'informatique d'entreprise, ces portes se sont ouvertes à ceux et celles qui, longtemps, n'ont été vus que comme des empêcheurs de tourner en rond. Mais encore faudrait-il qu'ils parlent le même langage que les dirigeants d'entreprise. La tendance devrait s'accentuer puisque la pression réglementaire n'est pas près de s'alléger. Rien que dans les pages qui suivent, nous traitons de DORA, de SREN et du RGPD qui fête ses cinq ans. Avec un directeur de l'ANSSI qui, aux Assises, expliquait vouloir simplifier et rendre plus abordables les outils de sécurité, gageons que les RSSI vont plus encore discuter avec leurs directions. Ils seront écoutés, mais seront-ils entendus...

La cybersécurité est-elle réellement le risque n°1 de l'entreprise ? Laissons les experts en débattre et préférons un consensus : les comités de direction et les conseils d'administration sont aujourd'hui plus conscients du risque cyber. Une connaissance qui s'accompagne d'effets positifs, notamment pour le RSSI qui est désormais bien plus audible. Pour autant, ce n'est pas demain qu'un ou une responsable de la sécurité du système d'information siégera au sein des instances dirigeantes.

Non, ce titre n'est pas la réalité. On voit peu, voire pas, de responsables de la sécurité informatique siéger au comité de leur direction de leur entreprise. On les voit encore moins dans les conseils d'administration. Il ne s'agit pas non plus d'un manifeste appelant à intégrer les RSSI aux CoDir… quoique. Non, il est surtout question dans les pages qui suivent du rapport que les dirigeants d'entreprise entretiennent avec la cybersécurité et celles et ceux qui l'incarnent, généralement les Responsables de la sécurité des systèmes d'information. D'étude en étude, on lit tout et son contraire au sujet du RSSI, mais on observe heureusement une constante : ça va un peu mieux dans les relations des RSSI avec leur direction générale. Il faut dire aussi que les cyberattaques font désormais la Une, aussi bien dans la presse quotidienne régionale qu'au journal télévisé. Soudain mise en lumière, la cybersécurité est sortie de l'ombre pour s'inviter à la table des ComEx et des conseils d'administration. S'y ajoutent une économie de plus en plus portée sur la donnée, une informatisation croissante de tous les secteurs, industrie comprise, et une migration vers le Cloud de bon nombre d'entreprises. Cette dernière stratégie n'est pas sans être problématique en matière de sécurité, puisque l'approche monolithique qu'on a longtemps connue ne tient plus, obligeant les RSSI à aller voir du côté de la sûreté ou encore du juridique.

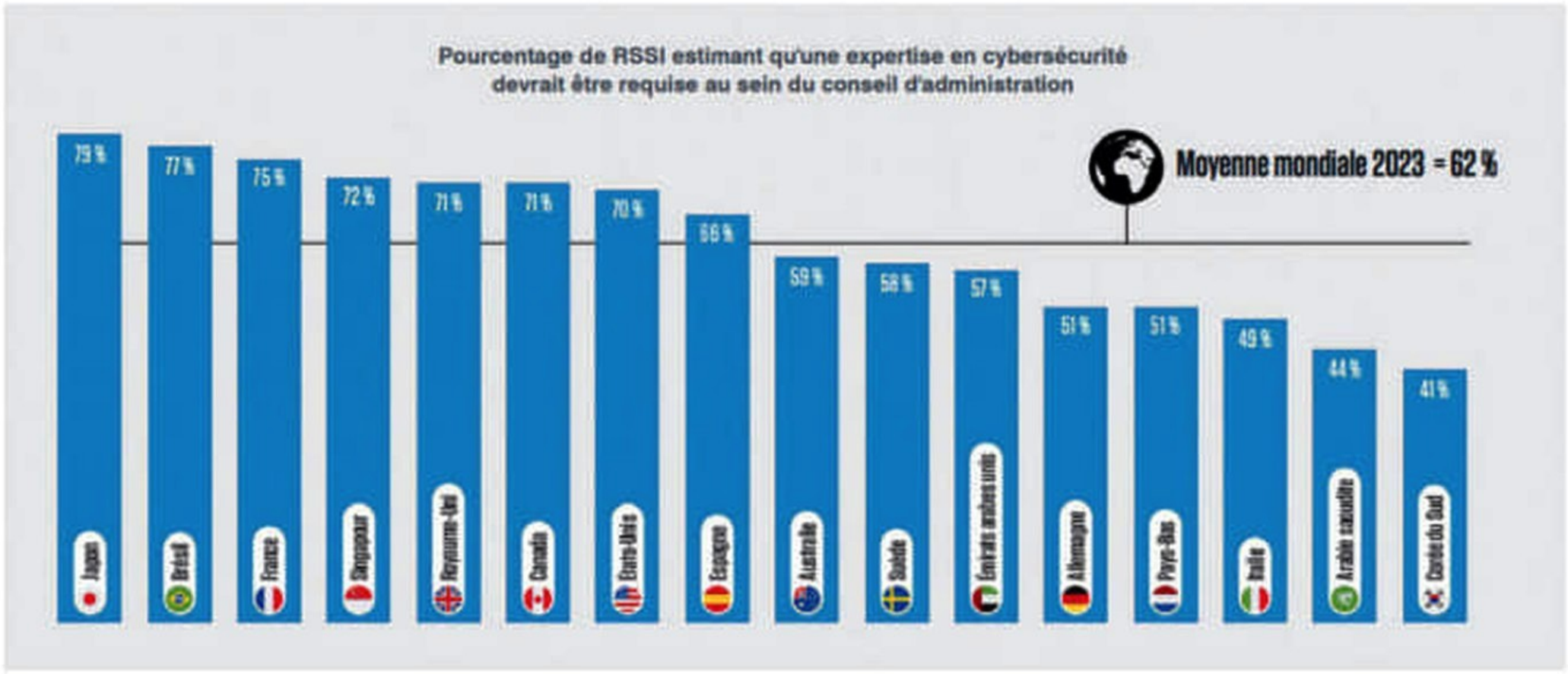
Un rôle qui change

Ainsi, leur rôle a grandement évolué ces dernières années, notamment son périmètre de responsabilité et l'attention qu'on lui accorde en entreprise. D'un empêcheur de tourner en rond, d'un obstacle au métier, le ou la RSSI est désormais un pourvoyeur d'assistance et de conseils sur l'un des principaux risques qui pèse sur l'entreprise. En effet, l'aspect cyber fait désormais partie de la cartographie des risques des comités exécutifs. La pandémie a aidé en cela, ouvrant la porte du conseil d'administration ou du ComEx aux experts en cybersécurité. Ce qui sous-tend une certaine proactivité désormais possible pour le RSSI, puisqu'il a pour mission de réduire le risque auquel sont exposés les métiers, que ce soit en gérant les vulnérabilités des systèmes qu'en définissant la stratégie cybersécurité de l'entreprise. Plus proches des autres composantes d'une entreprise toujours plus informatisée, toujours plus productrice et consommatrice de données, les responsables de la sécurité informatique doivent déterminer ce qui est vital de ce qui ne l'est pas. C'est pourquoi les interactions avec le conseil d'administration et le ComEx sont plus fréquentes.

Selon le *« State of Cybersecurity report »* de Wipro, 68 % des organisations signalent les cyber-risques au conseil d'administration au moins une fois par trimestre. Du côté de Salt Security, on y va aussi de son enquête, où la plupart des personnes interrogées indiquent que les membres de leur conseil d'administration reconnaissent le cyber-risque comme un problème commercial majeur. Plus de la moitié des RSSI (57 %) sont déjà présents au conseil d'administration sur l'atténuation des cyber-risques au moins tous les six mois, et un peu plus d'un quart (26 %) sont présents au moins une fois par trimestre. Au total, 83 % des RSSI se présentent au conseil d'administration tous les six mois ou plus souvent. Et les relations s'améliorent. Le *« Voice of the CISO »* de Proofpoint note que 62 % des RSSI estiment s'entendre avec leur conseil d'administration au sujet des problèmes de cybersécurité, contre 59 % en 2021 et 51 % en 2022. On pourrait en conclure que la baisse observée l'an dernier était due au contexte post-pandémie immédiat et aux incertitudes quant à la situation géopolitique. Les membres des conseils d'administration sont encore plus positifs, puisque 69 % d'entre eux partagent cet avis. Selon cette même étude du spécialiste de la protection des messageries, le niveau de connaissances des membres du Conseil d'administration sur les questions de cybersécurité va lui aussi en s'améliorant, du moins au goût des RSSI. La grande majorité des responsables cyber (96 %) déclarent que le conseil d'administration de leur organisation connaît bien la cybersécurité, 63 % d'entre eux indiquant que le conseil d'administration est *« très compétent »* sur le sujet.

« Le RSSI n'est pas aujourd'hui un décideur. »

Benoît Fuzeau,
président du Clusif.



L'expertise cyber n'est pas encore entrée dans les conseils d'administration

Ce chiffre doit toutefois être nuancé puisqu'on découvre peu après dans *« Voice of the CISO »* que, en France, 75 % des RSSI estiment qu'une expertise en cybersécurité devrait être requise au sein du conseil d'administration. Au niveau mondial, ils sont 62 %, ce qui sous-entend que la majeure partie des RSSI considère que les membres des conseils d'administration manquent de connaissances techniques. Au niveau sectoriel, les répondants des secteurs de la vente au détail (73 %), de l'informatique, des technologies et des télécommunications (69 %) et de l'enseignement (67 %) sont les plus nombreux à être d'accord avec cette affirmation, tandis que ceux de la santé (50 %) et des transports (44 %) sont les moins nombreux. *« Une plus grande expertise en cybersécurité au sein du conseil d'administration profite à l'ensemble des parties prenantes. Si aucun membre existant du conseil d'administration ne peut endosser ce rôle, cela peut offrir des perspectives de carrière aux professionnels de la sécurité qui en sont capables »* explique Proofpoint. Mais est-ce seulement possible ?

Outre-Atlantique, IANS Research, un institut spécialisé dans les enjeux relatifs aux CISO, s'est penché sur la capacité des RSSI à intégrer un ComEx. Son étude, *« CISOs as Board Directors — CISO Board Readiness Analysis »*, évalue ainsi les compétences des décideurs cyber des 1000 premières entreprises américaines cotées en bourse, le Russell 1000. Les résultats ne sont guère reluisants, puisque 14 % des RSSI de l'indice R1000 sont candidats idéaux pour des postes au sein de conseils d'administration ou de ComEx. L'enquête se fonde sur cinq compétences : l'ancienneté dans la cybersécurité, l'expérience, de la capacité à faire face à la complexité organisationnelle, les diplômes et la diversité du background. *« Les nouvelles modifications apportées aux règles de la SEC obligeront les sociétés cotées à divulguer l'expertise en matière de cybersécurité des membres du conseil d'administration, ainsi que les pratiques de gouvernance en matière de surveillance du risque de cybersécurité. Dans la plupart des conseils d'administration, la compréhension de la cybersécurité est insuffisante, des recherches récentes révélant que la plupart des entreprises ne disposent même pas d'un seul administrateur possédant une expertise en cybersécurité »* écrit l'institut. Ces 14 % de CISO parfaits ou presque, réunissent au moins quatre de ces caractéristiques. Un tiers sont des candidats solides, avec trois sur cinq, mais plus de la moitié des responsables cyber des mille premières entreprises américaines n'ont qu'une ou deux caractéristiques correspondantes. On notera d'ailleurs que, selon *« CISOs as Board Directors — CISO Board Readiness Analysis »*, la moitié des conseils d'administration du Russel 1000 n'a aucune expérience en matière de cybersécurité. *« L'expertise en technologie et en cybersécurité à elle seule ne suffit pas pour siéger à des conseils d'administration. Il s'ensuit que les RSSI qui souhaitent siéger à des conseils d'administration devraient apporter davantage en termes d'expériences ou de diversité non liées à la cybersécurité, ainsi que de sens financier et de présence de la direction »* explique Brian Walker, CEO de The CAP Group.

Un écart de perception

En d'autres termes, les conseils d'administration manquent de compétences en matière de cybersécurité et, à l'inverse, les RSSI n'ont pas les qualités requises pour y siéger. Et si les directions et les responsables cyber se comprennent de mieux en mieux, tout n'est pas rose. La dernière étude en date de Delinea sur le sujet est particulièrement sombre. Menée à l'échelle internationale, il en ressort que 61 % des RSSI interrogés estiment que les dirigeants négligent l'importance de la cybersécurité. Seuls 37 % des répondants français pensent que leur direction ou conseil d'administration comprennent bien son rôle. D'ailleurs, pour un tiers des RSSI, la cybersécurité n'est vraiment prise en compte que dans le but de respecter la réglementation. En France, un tiers des RSSI considère que cette conception de la cybersécurité comme une liste de cases à cocher pour être en conformité, a pour corollaire l'augmentation du nombre de cyberattaques faisant mouche. Un tiers également y voit la raison pour laquelle les investissements tardent à se concrétiser. C'est également l'avis de Salt Security, pour qui 82 % des RSSI déclarent disposer d'un budget de sécurité plus important qu'il y a deux ans, mais en tenant compte de l'augmentation des revenus de leurs entreprises et de l'inflation, leur pouvoir d'achat effectif a diminué. En outre, un tiers

des personnes interrogées dans cette étude citent la justification des dépenses et presque autant le manque de budget comme principaux défis de sécurité. Ces deux résultats suggèrent que les RSSI manquent toujours du financement dont ils ont besoin pour répondre aux nouvelles exigences de sécurité créées par la transformation numérique.
Ce décalage peut s'expliquer par, là encore, une différence de perception. Du côté de Delinea, les RSSI citent comme premier indicateur pour mesurer l'efficacité de la cybersécurité le nombre d'attaques évitées. L'étude de Proofpoint observe un écart similaire : les RSSI pensent que les principales préoccupations de leur conseil d'administration sont l'atteinte à la réputation (36%), l'impact sur la valeur de l'entreprise (36%) et la perte de clients actuels (36%) quand, pour eux, les principales conséquences réelles des fuites de données sont le temps d'arrêt et de récupération des données (38%), les pertes financières (33%) et les sanctions réglementaires (33%). Les chiffres de Wipro ne sont guère mieux, puisqu'il ressort de son *« State of Cybersecurity report »* que, si 85% des conseils d'administration ont mis en place une forme de supervision de la cybersécurité, 32% seulement ont désigné un membre du conseil d'administration pour assurer la supervision de la cybersécurité. Pire encore, à peine un quart des exercices de simulation de crise cyber implique le conseil d'administration.

18 mois

Force est néanmoins de constater que ces études sont très américaines. Un élément d'explication sur cette relation entre RSSI et ComEx nous vient peut-être d'Erik Gaston, VP of Global Executive Engagement chez Tanium. *« En moyenne, le mandat d'un RSSI dure 18 mois. Je pense que cela s'explique par le fait que pendant les six premiers mois, le RSSI essaie de se faire une place au sein de l'organisation. Il apprend le rôle de chacun. Les six mois suivants sont consacrés à essayer d'influer sur la politique »* explique-t-il. *« Ces six mois sont cruciaux : soit il se heurte à une résistance interne trop forte et ne parvient pas à améliorer la posture de sécurité de l'entreprise, soit il réussit à mettre en œuvre des changements significatifs. Les six derniers mois sont consacrés à la mise en conformité et à l'aide aux retardataires… ou à la recherche d'un emploi qui leur permettra d'aider une autre organisation. Les RSSI sont une espèce particulière. Ils veulent aider, mais s'ils ont les mains liées, ils ne sont pas prêts à rester pour assumer le risque d'une organisation qui n'est pas disposée à travailler dur et à réduire son exposition au risque. Ils aiment aussi les défis. Une fois qu'ils ont mis une organisation sur la bonne voie, ils sont prêts à s'attaquer à leur prochain défi cyber. L'ensemble des compétences d'un RSSI est tout à fait unique — c'est un mélange d'introversion et d'extraversion, de technique et de stratégie, de communication et d'écoute. Si vous avez un bon RSSI, vous avez tout intérêt à le garder le plus longtemps possible ».*

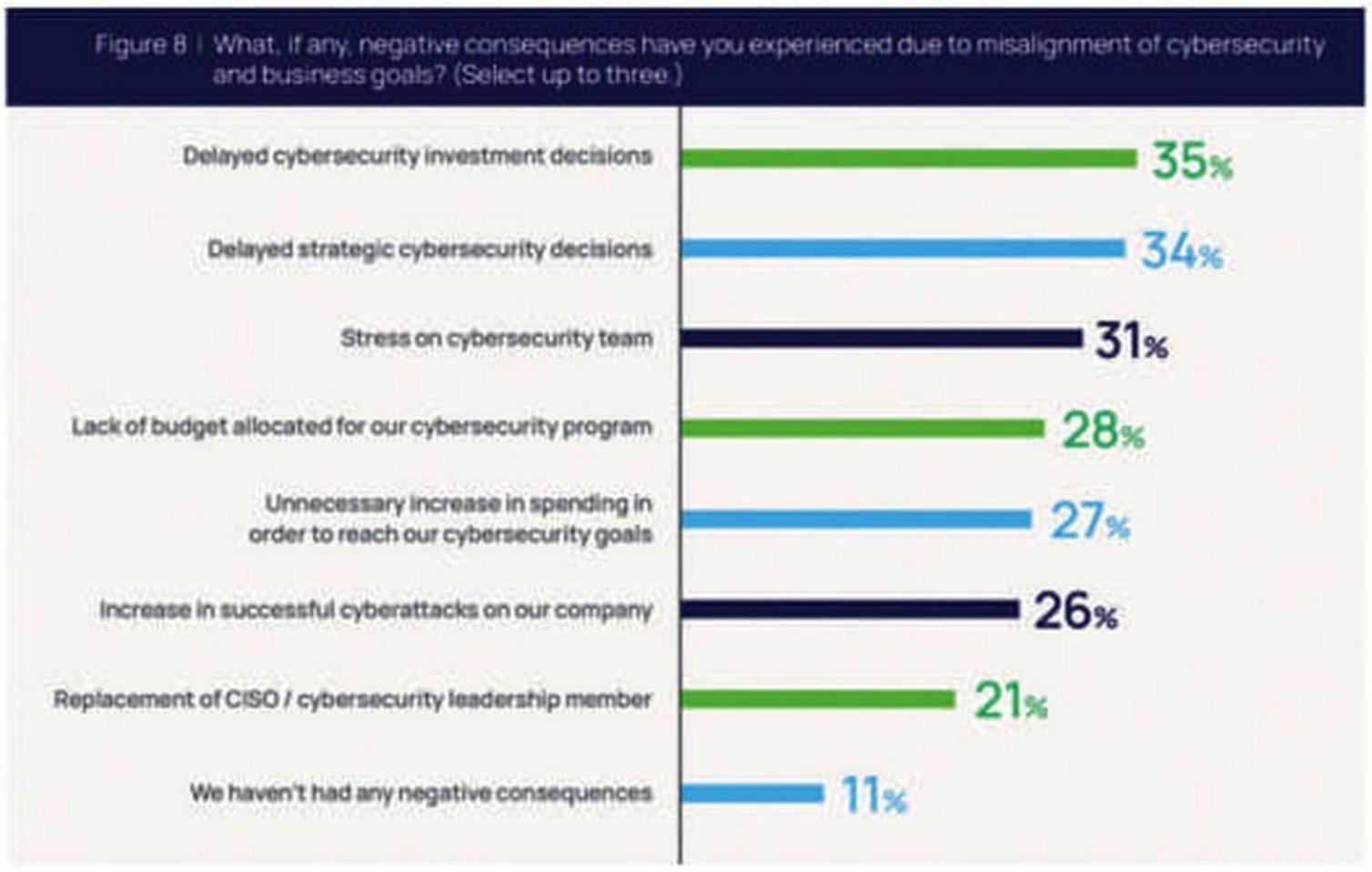
L'éternelle question du rattachement du RSSI

Quel est le positionnement du RSSI au sein de l'entreprise ? Cette interrogation en fait couler de l'encre, tant les enjeux et les prérogatives vont varier en fonction du rattachement du RSSI. Nous l'écrivions déjà en 2021, entre DSI, CTO, CIO, CISO, RSSI voire DPO, l'organisation est bien plus étalée qu'avant. Il faut également compter sur les évolutions de l'informatique, toujours plus distribuée (de l'avis de l'IT) quand elle n'est pas fragmentée (de l'avis des équipes cyber), sur l'explosion du nombre de cyberattaques et sur une pression réglementaire toujours plus forte avec l'arrivée prochaine de SREN, de NIS 2, du Data Act ou encore de DORA. Bref, la posture du RSSI a évolué, et évolue encore. Il ne s'agit donc pas de brosser un tableau complet des rôles et rapports hiérarchiques, mais d'exposer dans les grandes lignes ce qui se pratique aujourd'hui en entreprise. Dans le cas le plus courant, le RSSI dépend de la Direction des Systèmes d'Information, ou répond au CRO. Auquel cas il ou elle doit composer entre les exigences de sécurité, le bon fonctionnement des systèmes informatiques et les projets de transformation numérique, sans oublier les habituelles contraintes budgétaires. Parfois, il est directement rattaché à la Direction Générale de l'entreprise. Sa position sera alors stratégique et transverse, on attendra de lui qu'il ne soit pas (seulement) un technicien, mais qu'il ait une vision d'ensemble des problématiques métiers, financières, juridiques, RH… Le *« mouton à cinq pattes »* évoqué par le président du Clusif. On trouvera en outre des RSSI dépendant de la direction des risques. Ce poste, fréquemment rencontré dans les secteurs assurantiel et bancaire, fait de la cybersécurité un outil de la conformité et du RSSI son garant. Définition des processus de sécurité et conduite des audits seront le lot de ces responsables. Enfin, il peut être rattaché au responsable de la sûreté ou des opérations, un périmètre plus large englobant l'informatique, la sécurité des personnes et des bâtiments, etc.

Dans un précédent numéro de *L'InfoCyberrisques*, nous avions interrogé Benoît Fuzeau. Celui-ci nous expliquait alors que, pour lui, *« le RSSI n'est pas aujourd'hui un décideur »*. Selon le président du Clusif et RSSI de CASDEN, *« nous avons un titre qui est « responsable ». Mais moi, je ne me sens pas responsable. Ce R me pose un problème, parce qu'aujourd'hui, je suis un accompagnateur, je suis une fonction de support pour accompagner au mieux les métiers »*. Des propos qui font écho avec ceux d'Erik Gaston, pour qui, *« en fin de compte, [les RSSI] sont responsables de l'identification et de la communication des risques au sein d'une organisation. Ils doivent élaborer des stratégies de cybersécurité et veiller à ce qu'elles soient appliquées et respectées. Ils sont responsables des outils d'atténuation des risques et de la mise en œuvre des réponses aux incidents. Ainsi, s'il dispose des ressources suffisantes, le RSSI dirige l'équipe et la stratégie qui permettent d'éviter les compromissions de données les plus graves. Tous les secteurs sont confrontés à une vague de cybermenaces sans précédent, mais un bon RSSI saura préserver la sécurité des données »*. Une approche très américaine, où l'on ne parle pas de Responsable, mais de Chief Officer. Le Vice-président de Tanium estime d'ailleurs qu'une compromission peut avoir un impact sur la carrière d'un

RSSI, ou plus exactement *« la façon dont le RSSI va réagir. Nous avons vu des exemples de RSSI qui ont tenté de cacher la vérité ou de participer à des opérations de dissimulation de la vérité. Leur responsabilité pénale a alors été engagée et leur carrière de RSSI s'est terminée. D'autant plus qu'ils risquent une peine de prison pour ces faits. En revanche, un RSSI qui réagit de manière appropriée à une compromission de données, qui la signale comme il se doit et qui agit en tant que communicant et leader en temps de crise, peut conseiller efficacement d'autres personnes occupant des postes similaires, que ce soit au sein de la même organisation ou même dans des organisations plus importantes »*. Benoît Fuzeau, pour sa part, voyait plutôt dans l'émergence de nouvelles fonctions, à l'instar de Directeur de la cybersécurité, de nouveaux enjeux *« là, on est attendu sur des engagements forts. C'est peut-être l'évolution sur laquelle il faut travailler »*. Le CISO est-il la prochaine évolution, en France, du RSSI ?

Figure 8 | What, if any, negative consequences have you experienced due to misalignment of cybersecurity and business goals? (Select up to three)



Un langage commun à apprendre

Encore faudra-t-il que le responsable cyber et la direction générale parlent le même langage. *« Je pense, sur le métier, qu'on est aujourd'hui à un moment charnière : nous sommes passés d'une vision très technique à une version plus managériale. Il y a deux phénomènes qui le montrent : quatre ou cinq entreprises du CAC40 ont pris des managers métiers, et pas des RSSI, pour remplir cette fonction. Puisque, maintenant, la cyber est montée aux comités de direction, ils attendent des gens qu'ils arrivent à comprendre, et je pense que nous avons encore du mal à faire passer notre message »* soulignait Benoit Fuzeau. *« C'est une vraie problématique aujourd'hui, on voit au niveau des directions générales qu'il y a une évolution et qu'on arrive à en parler, mais il n'y a pas encore de changement significatif, selon moi »*. C'est également le constat auquel est parvenu Wipro. Les entreprises doivent optimiser les canaux de communication pour les RSSI au niveau du conseil d'administration et investir dans l'apprentissage à tous les niveaux de leur organisation. Cela étant, de leur côté, les RSSI doivent améliorer leurs compétences en matière d'échanges afin d'obtenir des financements et une réelle prise en compte par le conseil d'administration de ce qui est nécessaire du point de vue de la cybersécurité. Pour le président du Clusif, *« si on prend un peu de recul, ce qui intéresse les chefs d'entreprise, et à juste titre, c'est le chiffre d'affaires, les bénéfices, les marges, mais le risque SSI est un risque parmi d'autres. Je pense qu'il faut qu'on essaie de limiter cet entre-soi que je perçois depuis quelques années. Quand je prends le sujet des tableaux de bord, on n'arrive pas à en sortir quelque chose qui prenne de la hauteur et qui soit compréhensible. Et moi le premier, je tombe dans le panneau. Quand je compare mes tableaux de bord avec ceux des collègues, nous avons tous à peu près les mêmes choses. Je me mets à la place d'un chef d'entreprise : qu'est-ce qu'il comprend de mes indicateurs et de mes messages. Quand je lui dis qu'il y a 400 vulnérabilités sur mes environnements, à quoi ça correspond ? La seule phrase qu'il devrait me répondre c'est « mais qu'est-ce que tu attends pour les corriger ? » »*

D'autres façons de mesurer le risque, ou pourquoi pas la confiance dans le numérique, si l'on prend le problème à l'envers, peuvent donc servir à se faire entendre des ComEx et des conseils d'administration. De la simulation de crise aux conséquences métier d'un pentest, avec des informations factuelles et un contexte compréhensible des non-initiés, les responsables de la cybersécurité, à qui la porte des directions est ouverte, pourront sans doute devenir audibles. Et, pour reprendre IANS, en cultivant quelques soft skills, de s'asseoir à la même table et participer à égalité à la prise de décision. ▮

« Les RSSI veulent aider, mais s'ils ont les mains liées, ils ne sont pas prêts à rester pour assumer le risque d'une organisation qui n'est pas disposée à travailler dur et à réduire son exposition au risque. »

Erik Gaston,
VP of Global Executive Engagement chez Tanium.

Oktane 2023

Okta dessine le futur de l'IAM

Lors de sa conférence qui s'est tenue du 3 au 5 octobre dernier à San Francisco, l'éditeur de solutions de gestion des identités et des accès a tracé les contours de ce que devrait être son secteur d'activité dans les mois et années à venir avec l'ajout de l'intelligence artificielle, la fin des mots de passe et une connaissance plus fine des menaces.

Un rapport dans Identity Threat Management avec ses widgets.

Le thème de la conférence annonçait clairement le message que voulait porter Okta lors de sa conférence Oktane 2023 : « *plus loin que l'identité* ». Todd McKinnon, le CEO d'Okta, précisait lors de sa session plénière que l'entreprise, depuis 15 ans, définissait le libre usage des nouvelles technologies avec sa solution de gestion des accès et des identités par son indépendance et sa vision pionnière autour du Cloud. Sa volonté est de continuer sur ce chemin en portant sa solution à l'échelle des besoins actuels. Pour lui, l'Intelligence artificielle représente la nouvelle révolution sur laquelle il faut s'appuyer pour y parvenir.

L'IA pour surfer sur la nouvelle révolution technologique

Dans la même session plénière, il annonçait donc Okta AI, une suite de fonctionnalités d'intelligence artificielle qui apporte aux entreprises les moyens de maîtriser les possibilités de l'intelligence artificielle pour proposer une meilleure expérience aux utilisateurs des logiciels d'Okta et de mieux se protéger face aux menaces et attaques contre les identités. La nouvelle solution sera embarquée dans les différents clouds de l'éditeur, Workforce Identity Cloud et Customer Identity Cloud. Les deux clouds peuvent interagir entre eux, mais visent des cas d'usages différents. Les modèles développés sont exclusivement entraînés afin de proposer des actions en temps réel pour gérer les identités. La solution n'est pas exclusivement une solution d'intelligence artificielle générative et combine l'apprentissage machine et l'intelligence artificielle prédictive et générative suivant les usages et les besoins. Les différents modèles sont entraînés et enrichis avec les données issues de la plateforme Okta selon des règles définies en collaboration avec les services juridiques et de gouvernance d'Okta afin d'établir des règles claires sur l'utilisation de l'IA. La plateforme combine différents moteurs qui vont de l'apprentissage machine à l'intelligence artificielle générative avec des modèles sur Vertex AI de Google Cloud Platform.

Le stand de Backupta sur Oktane 2023.

De nouvelles fonctions

Face à la recrudescence des attaques de phishing ou contre les identités (+ 47 % selon Todd McKinnon), Okta souhaite simplifier grâce à l'intelligence artificielle en apportant des outils puissants pour renforcer les équipes de sécurité, tout en préservant les futurs choix technologiques des clients. Il pense donc que les solutions de gestion des identités doivent elles aussi évoluer pour faire face à ce contexte. L'apport de l'IA vise d'abord à casser la fragmentation des silos autour des identités numériques dans les entreprises et de combiner cette possibilité avec la

Backupta **sécurise les configurations** d'Okta

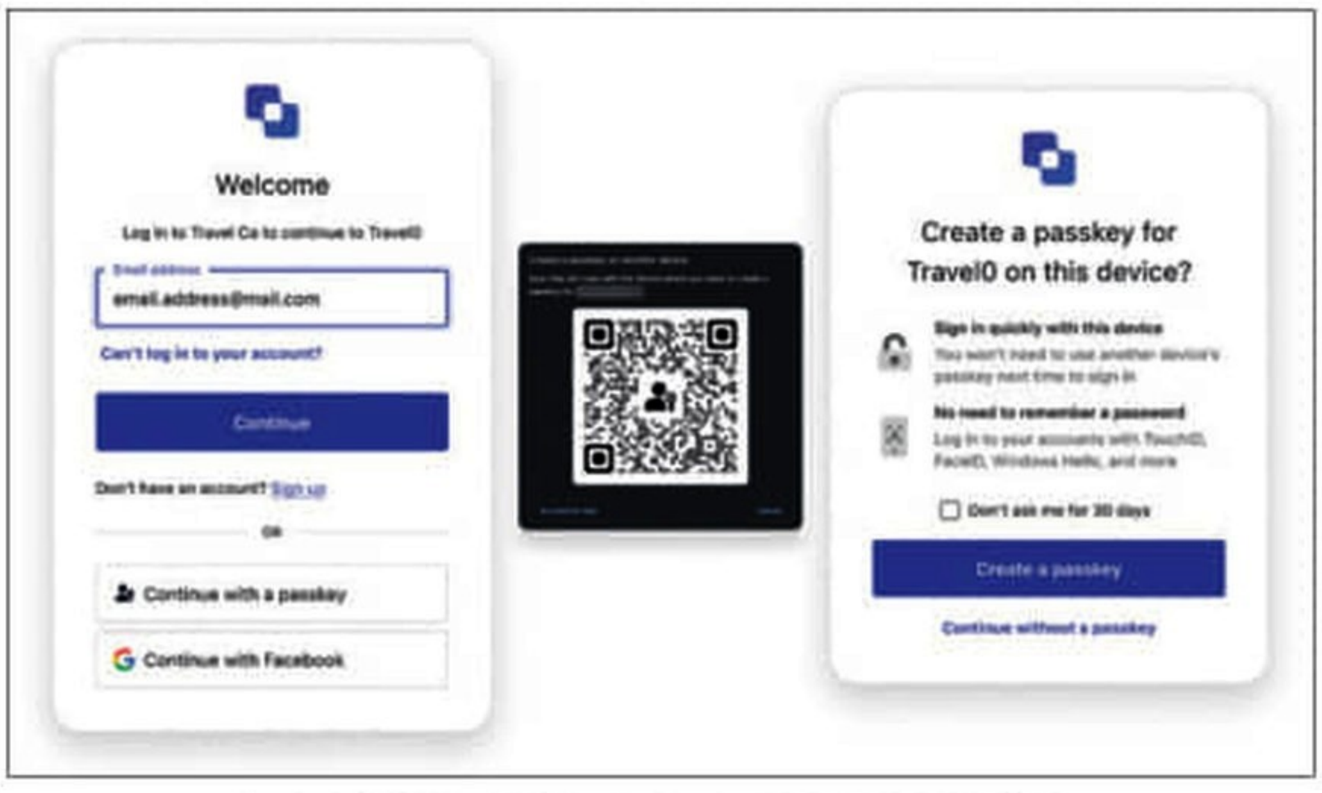
Cette startup franco-américaine est très spécialisée. Elle propose le backup et la restauration des tenants Okta. La solution autorise la récupération après un sinistre ou une erreur par un administrateur de la base de données des utilisateurs et des configurations des comptes Okta. De plus, la solution supervise toutes les actions des administrateurs et détecte tous les changements dans les configurations sur Okta et alerte les administrateurs dans ce cas selon les règles et les politiques de l'entreprise. Un logiciel de gestion des déploiements permet de tester les mises à jour ou de nouvelles configurations avant la mise en production. En version Beta actuellement, l'éditeur travaille de plus à une solution de migration des tenants Okta. L'ensemble est géré par une console dans le Cloud.
Plus précisément, la solution sauvegarde tous les éléments s'appuyant sur l'API d'Okta : les utilisateurs et les attributs, le hash des mots de passe, les groupes et règles de groupes, la configuration de l'application et ses cartes, les politiques et les règles, le zonage réseau... La solution sauvegarde les données Okta une fois par jour par défaut, mais il est possible de réaliser des sauvegardes manuelles à partir de la console d'administration.

gestion des accès et des autorisations pour attribuer le bon accès au bon utilisateur.
Ainsi dans Workforce Identity Cloud, Identity Threat Protection with AI propose une détection et des réponses en temps réel des menaces qui s'appuient sur l'identité. La principale différence de la solution est de ne pas se cantonner au point de login mais de monitorer l'ensemble de la session. De plus, la solution complète la solution de gestion des risques de l'éditeur et renforce son dispositif d'authentification multiple (MFA). Elle corrèle l'ensemble des données issues de l'écosystème de sécurité de l'entreprise. Elle propose également des réponses qui s'adaptent aux différents contextes relevés avec, par exemple, la fonction d'Universal Logout qui permet instantanément de déconnecter un utilisateur de toutes ses sessions si nécessaire afin de lui demander de nouvelles authentifications, dans le but de créer un contexte sain. Cette fonction renforce les politiques Zero Trust autour de l'identité et de l'authentification. De plus, la solution peut s'enrichir de données provenant d'autres sources comme Jamf, Netskope, Zscaler ou Palo Alto Networks. La solution sera disponible en accès limité au début de l'année prochaine.

Un futur sans mot de passe

Lors de la conférence, Okta a de plus annoncé le support de Passkey avec l'offre de son acquisition Auth0 en accès anticipé. Les développeurs vont pouvoir rapidement intégrer cette solution dans leurs applications de manière sécurisée et résistante à l'hameçonnage. La solution s'appuie sur les standards FIDO et W3C. De plus, la solution est la plus utilisée par les développeurs selon l'éditeur.
Cette intégration va simplifier la mise en œuvre des passkeys en réduisant les problématiques de loging et protéger les entreprises contre les attaques sur les certificats. Autre fonction intéressante, Workflows No Code Automation for Customer Identity donne la possibilité aux équipes de développeurs d'améliorer la posture de sécurité et l'expérience des utilisateurs sans avoir à écrire de code. Le support des numéros de téléphone comme unique identifiant autorise un support à l'échelle des utilisateurs dans les pays où ce numéro est une forme attendue d'authentification comme dans certains pays d'Asie ou d'Amérique Latine. Une option sans mot de passe autorise une authentification par le simple envoi du numéro.
Customer Identity Cloud intègre de plus des fonctions d'améliorations pour la restauration des mots de passe en ajoutant pour les développeurs la possibilité d'injecter une fonction d'authentification multifacteurs dans le workflow de réinitialisation du mot de passe.
Il devient possible de personnaliser des prompts pour créer des processus d'enregistrement directement par Universal Login. Les prompts se personnalisent selon les préférences du client pour des besoins de localisation, de respect des données privées, la gestion du consentement...
Disponible en accès anticipé, le support de Passkey sera en disponibilité générale d'ici la fin de cette année. La solution de workflows est disponible immédiatement, ainsi que celle pour supporter l'authentification par le numéro de téléphone et les options de réinitialisation des mots de passe qui seront en accès anticipé au cours du mois d'octobre et en disponibilité générale au cours du premier trimestre 2024.
Finalement, cette édition d'Oktane 2023 a été riche en contenu et annonces. L'ensemble ne représente cependant que les premières étapes de la vision d'Okta sur le futur de la gestion des accès et des identités. Celle-ci reste dans la droite ligne de la vision définie au démarrage de l'entreprise : simplifier et donner accès aux utilisateurs à toutes les technologies.

B.G



Un login sur plusieurs terminaux avec passkey.

Asylum Ambuscade

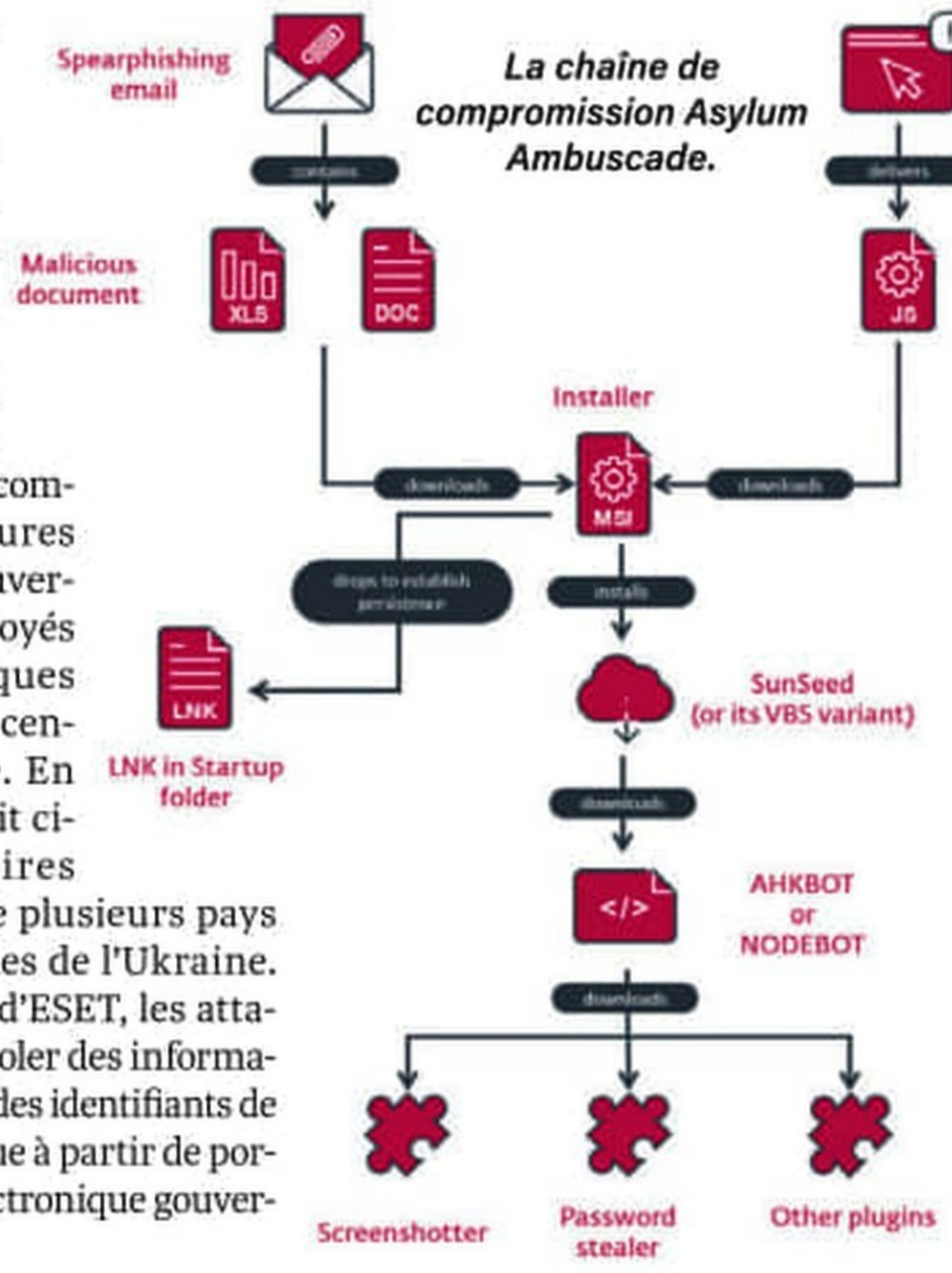
Un outillage simple mais efficace

Lors des dernières assises de la sécurité, ESET a présenté les travaux de son centre de recherche sur le groupe Asylum Ambuscade qui sévit dans le cybercrime et le cyber espionnage avec un kit d'outils assez basique, mais qui reste efficace.

Le groupe qu'ESET a nommé Asylum Ambuscade s'est fait remarquer par des attaques sur des personnalités de pays limitrophes de l'Ukraine, ou des organisations s'occupant des réfugiés ukrainiens. Clairement, les opérations étaient alignées sur les intérêts russes ou biélorusses, constate Mathieu Tartare, un expert d'ESET qui œuvre dans le laboratoire de recherche de l'éditeur à Montréal. Cette attribution provient de chaînes de caractères en russe, découvertes dans les codes employés par Asylum Ambuscade.

Sur tous les fronts

Un point remarquable de ce groupe : il sévit à la fois dans le cybercrime et l'espionnage, ce qui est somme toute assez rare d'être sur l'ensemble de ces opérations. Il est actif depuis au moins 2020 et cible des particuliers, des petites et moyennes entreprises, des utilisateurs d'applications bancaires et de cryptomonnaies dans différentes régions, notamment en Amérique du Nord et en Europe. Depuis janvier 2022, ESET Research a recensé plus de 4 500 victimes dans le monde entier. Du côté espionnage, ESET a découvert des opérations avant 2022. ESET a découvert des compromissions antérieures de fonctionnaires gouvernementaux et d'employés d'entreprises publiques dans des pays d'Asie centrale et en Arménie. En 2022, le groupe aurait ciblé des fonctionnaires gouvernementaux de plusieurs pays européens limitrophes de l'Ukraine. Selon les recherches d'ESET, les attaquants cherchaient à voler des informations confidentielles et des identifiants de messagerie électronique à partir de portails de messagerie électronique gouvernementaux officiels.



La chaîne de compromission Asylum Ambuscade.

Un outillage assez simple

Les outils utilisés par le groupe sont assez simples et s'appuient sur des scripts VBS. Comme beaucoup de groupes, les attaques sont initiées après une campagne de spear phishing et une infection par des formats de documents usuels comme des fichiers doc ou xls. Ceux-ci téléchargent un *installer* (MSI). Celui-ci devient persistant après son stockage sous la forme d'un fichier LNK dans le startup folder. Il contient les raccourcis vers des applications qui s'ouvrent lorsque vous avez signé un compte Windows 10 ou 11 local. Dans une étape suivante, un virus de type SunSeed ou ses variantes VBS sont installés. Ensuite, des malwares tels qu'AHKBOT sont téléchargés. Ce dernier est un téléchargeur qui peut être étendu avec des plugins pour espionner la machine de la victime. Ces plugins offrent diverses fonctionnalités, notamment la capture d'écran, l'enregistrement des frappes de clavier, le vol de mots de passe des navigateurs web, le téléchargement de fichiers et l'exécution d'un voleur d'informations.

Une des particularités du groupe est de développer en permanence de nouveaux scripts ou de nouvelles variantes pour éviter les défenses mises en place. Il est même étonnant de constater que des tests de ces variantes ont été effectués sur la plateforme en ligne VirusTotal, un service appartenant à Google qui permet l'analyse de fichiers suspects et facilite la détection rapide des virus, vers, chevaux de Troie et toute sorte de logiciels malveillants détectés par les moteurs antivirus ! Sur ces tests, le groupe essayait des fichiers publisher en commençant par des analyses statiques jusqu'à ce que ceux-ci ne soient plus détectés par la plateforme. Les attaques suivent une fréquence assez identifiable, avec des pics environ tous les 2 mois, ce qui correspond fortement à des cycles de sprints de développement.

Finalement, le groupe emploie des outils peu sophistiqués, mais les remet à jour régulièrement pour éviter les détections. Certaines de ses pratiques sont parfois à la limite du professionnalisme pour un groupe cybercriminel, mais son outillage et ses méthodes restent cependant assez efficaces même si la fin des VBS dans les prochaines versions de Windows va un peu freiner le groupe du fait du but avoué de Microsoft d'aider les utilisateurs de ses produits à bloquer plus facilement la diffusion de logiciels malveillants sur leurs appareils. ▮

B.G

Cybermenaces :

recrudescence des fausses notifications de mises à jour

Les spécialistes de la cybersécurité Proofpoint ont observé une augmentation exponentielle des fausses notifications de mises jour des navigateurs Internet dissimulant des charges malveillantes. Les cybercriminels misent sur la confiance que les utilisateurs accordent à Google Chrome, Firefox ou encore Edge pour les piéger.

Grâce aux techniques éprouvées d'ingénierie sociale, les cybercriminels parviennent à mener des cyberattaques avec des techniques pourtant relativement anciennes comme les fausses notifications de mises à jour. Elles apparaissent généralement sur des sites web déjà compromis et prennent la forme d'une alerte provenant directement du navigateur utilisé. Que cela soit Google Chrome, Firefox ou Edge, ces notifications de mises à jour semblent familières pour les utilisateurs qui n'hésitent malheureusement pas à cliquer sur des liens de téléchargement dissimulant une charge malveillante. Alors qu'elles étaient avant uniquement en anglais, ces attaques se sont répandues dans toute l'Europe en français, en espagnol, en allemand et en portugais.

Une forme d'attaque ancienne

Les chercheurs de Proofpoint ont constaté que de nouveaux groupes -RogueRaticate, SmartApeSG et ClearFake- ont repris à leur compte une méthode déjà utilisée depuis quelques années par TA569 pour diffuser le logiciel malveillant SocGholish : une redoutable attaque par téléchargement au volant. SocGholish essaye d'inciter ses victimes à exécuter un fichier ZIP se faisant passer pour une mise à jour légitime d'un navigateur, ou d'un logiciel de visioconférence. Ces groupes développent leurs propres campagnes pour diffuser leurs charges malveillantes, mais celles-ci reposent sur les mêmes caractéristiques et suivent le même cheminement.

Jérôme Cartegini

Xavier Daspre, Directeur Technique chez Proofpoint revient sur cette technique d'attaque qui s'avère particulièrement efficace.

C'est une méthode que l'on a observée assez récemment chez différents prédateurs notamment au travers de la messagerie. Le premier vecteur de ces attaquants est tout d'abord de compromettre toute ou partie d'un site web pour héberger le signalement de fausses mises à jour. Il faut ensuite qu'ils aillent chercher, si je puis dire, les victimes. Pour cela, ils vont leur envoyer des emails pour leur dire d'aller voir telle update ou tel sujet sur ce site. Si je parle de sujet, c'est parce que là où on a le plus de mal à les détecter, c'est justement quand ils ont compromis des sites sur des forums de discussion. Ils vont poser une fausse mise à jour sur une des pages qui traite l'un des sujets auxquels les utilisateurs sont abonnés. Ils peuvent aller chercher les victimes par ingénierie sociale via le forum ou en corrompant la base d'utilisateurs du site pour récupérer leurs adresses email. Ensuite, ils n'ont

plus qu'à envoyer un message du type : *« Quelqu'un a répondu à votre sujet sur votre forum de discussion. »* Les victimes cliquent sur l'URL pour consulter la réponse et tombent sur la page qui contient le code avec la mise à jour. À partir de là, le plus gros du boulot est fait, car en arrivant, ils voient un message du type *« Vous ne pouvez pas lire ce contenu si vous n'avez pas mis à jour votre navigateur. »* Dans la plupart des cas, ils cliquent instantanément et les dégâts commencent... Ce n'est pas une mise à jour qui est installée, mais un malware avec une charge qui va permettre de faire soit ce qu'on appelle un Remote Access Trojan (prise de contrôle à distance du poste), soit installer un cryptomalware ou tout autre type de cybermenaces. C'est une méthode d'infection assez massive qui demande en réalité aux attaquants un minimum de recherches par ingénierie sociale. Ils utilisent des sites à partir desquels les utilisateurs ont l'habitude de recevoir des emails, si bien qu'ils ne sont pas forcément surpris de recevoir un message les invitant à consulter une page.

mgen

GROUPE VYV

EMPLOYEZ-NOUS

À VOUS METTRE AU CŒUR DE LA TRANSFORMATION

EXPERT(E) SÉCURITÉ

**Chez MGEN, innovez dans un cadre professionnel favorisant l'esprit collectif et les initiatives individuelles.
Vous avez la possibilité de conjuguer les nouvelles technologies aux exigences de sécurité et d'efficacité pour optimiser nos applications et nos process.
Avec nous, relevez de nouveaux défis en donnant du sens à votre carrière.**

REJOIGNONS-NOUS SUR RECRUTEMENT.MGEN.FR

Crédit photo : Roman Jehanno. Groupe MGEN – DRH & Affaires générales – HAVAS PARIS PEOPLE.

#mutuellement

Faux départ pour le cyberscore

Les critères d'application du texte et des audits du cyberscore n'ont toujours pas été publiés au Journal officiel, alors que ce nouvel indicateur, censé informer les internautes du niveau de sécurité de leurs données sur certaines plateformes, est obligatoire depuis le 1er octobre 2023. Dans l'attente, certains professionnels s'inquiètent des conditions de mise en œuvre peu contraignantes.

Le nutriscore sauce cyber devait entrer en vigueur le 1er octobre 2023, en vertu de la loi du 3 mars 2022 pour la mise en place d'une certification de cybersécurité des plateformes numériques destinées au grand public. Ce cyberscore, présenté sous la forme d'un code couleur à l'image de ce qui se pratique pour le nutriscore, doit en fait représenter le niveau de sécurisation et la localisation des données des grandes entreprises technologiques. Pour ce faire, il matérialise les résultats d'un audit effectué par des prestataires qualifiés par l'Agence nationale de la sécurité des systèmes d'information (ANSSI). Il doit être accompagné d'une note d'information afin d'éclairer au mieux le consommateur au moment de choisir sa plateforme.

Une boîte noire partiellement ouverte

Cependant, un mois après, un projet d'arrêté fixant certains critères de la loi a bien été rendu public par le ministère de l'Économie, des Finances et de la Souveraineté Industrielle et Numérique et dont l'entrée en vigueur serait prévue pour le 1er janvier 2024. Il donne quelques indications précieuses, comme la durée de validité de l'audit qui pourrait être fixée à 1 an, ou l'obligation de rendre le cyberscore obligatoire pour les sites comptant plus de 25 millions de visiteurs uniques par mois en France, à partir de 2024. Une jauge revue à la baisse à 15 millions l'année suivante. L'arrêté expose également toute une liste de critères d'audit en vue de la détermination du cyberscore, notamment : « *la société délivrant le service est assujettie au droit européen* », « *les données techniques et/ou personnelles des usagers sont revendues et/ou partagées à des tiers* », « *localisation des infrastructures d'hébergement du service numérique en UE* ». Le projet d'arrêté précise toutefois que « *l'audit réalisé pour la définition du cyberscore est réalisé sur la base d'informations ouvertes, librement accessibles et de manière non intrusive par le prestataire.* » Une méthode qui semble avoir trouvé des échos au cours de tables rondes autour du texte, lors desquelles « *les autorités ainsi que la Direction générale des Entreprises (DGE) ont défendu le principe d'audits qui ne soient pas trop contraignants pour les entreprises* », explique Maxime Alay-Eddine, directeur général de Cyberwatch, une société française éditrice de logiciels de sécurité informatique, et vice-président d'Hexatrust, une association loi 1901 qui regroupe les acteurs français et européens de la cybersécurité ou encore du cloud de confiance. Une stratégie que regrette Maxime Alay-Eddine : « *cela reviendrait à dire 'je dois mesurer l'efficacité d'une boîte noire, mais sans avoir le droit de l'ouvrir'.* »

Auditer le cheminement réel et détaillé des données

Dans le principe, les audits devront s'attarder sur le niveau de sécurisation et le cheminement des données au sein d'une organisation en plus d'auditer des éléments liés à la seule sécurité technique. Lors des consultations avec les professionnels autour du cyberscore, « *il a été question de regarder les niveaux de protection et de configuration mis en œuvre au niveau du chiffrement TLS (Transport Layer Security, ndlr)* », fait remarquer Maxime Alay-Eddine. Un sujet sur lequel l'expert ne doute pas que les grandes entreprises technologiques concernées par le cyberscore sont parfaitement en mesure de répondre. « *Il s'agit d'un élément technique simple à mettre en œuvre. Cela revient à viser un critère qui, de facto, sera respecté par tout le monde.* »

Tout l'enjeu doit consister, selon lui, à juger efficacement de la protection des données personnelles. Qu'en est-il de leur exploitation et du cheminement réel et détaillé au sein d'une organisation ? Sont-elles hébergées par des entreprises françaises, européennes, extraterritoriales ? Chose difficile à déterminer avec précision si l'on n'ouvre pas cette fameuse boîte noire, en consultant des documents émis par les sociétés concernées et donc en conditionnant le cyberscore à des audits plus poussés, prévient Maxime Alay-Eddine. Si d'aventure la V1 du cyberscore devait être peu contraignante, « *elle aura le mérite de constituer un premier pas. Mais il faudra envisager une seconde version afin de relever les curseurs* », conseille Maxime Alay-Eddine. Réponse le 1er janvier 2024, sauf nouveau report de calendrier. ▮

Victor Miget

Niveau	Critères atteints par niveau	Avancée	Avancée
A+	0/62	0%	Palier non atteint
A	0/59	0%	Palier non atteint
B	0/55	0%	Palier non atteint
C	0/46	0%	Palier non atteint
D	0/21	0%	Palier non atteint
E	0/10	0%	Palier non atteint
F	-	-	Palier atteint

Capture d'écran de la proposition de visuel de la notation du rapport d'audit, issue du projet d'arrêté fixant les critères pour l'application de la loi n° 2022-309 du 3 mars 2022.

Loi SREN : un Data Act avant l'heure

Une part non négligeable du projet de loi visant à sécuriser et réguler l'espace numérique est dédiée à la lutte contre certaines pratiques anti-concurrentielles en matière de cloud et à favoriser l'interopérabilité et la portabilité des données, avec de nouvelles compétences à la clé pour l'Arcep.

Mardi 17 octobre, l'Assemblée nationale a voté en première lecture en faveur du projet de loi visant à sécuriser et réguler l'espace numérique, ou SREN, par 360 voix contre 77. Le texte avait été adopté par le Sénat en juillet, il devra désormais passer en Commission mixte paritaire, probablement en décembre. La partie du texte qui nous intéresse ici s'étend des Articles 7 à 14. Il y est question de données et de Cloud. Sur ces sujets, le projet de loi est en avance de phase, puisqu'il anticipe le Data Act européen pour y adapter le droit français. Il s'agit, en outre, de lutter contre certaines pratiques qui relèveront, au titre du SREN, de la concurrence déloyale. Dans le viseur, les hypersclers, évidemment.

Plus tôt en 2023, l'Autorité de la concurrence tirait le signal d'alarme, s'inquiétant notamment de la pratique des « crédits cloud » qui enferment les entreprises, notamment les startups qui en bénéficient, dans l'écosystème du fournisseur. Autre abus, les frais de transfert et de sortie, véritables coûts cachés et souvent exorbitants. Sur le premier point, les fameux « crédits gratuits » que peut gracieusement offrir un fournisseur de cloud, le législateur, lui, parle d' *« avoir d'informatique en nuage »*. Soit *« un avantage octroyé par un fournisseur de services d'informatique en nuage à un client, [...] utilisable sur ses différents services, sous la forme d'un montant de crédits offerts ou d'une quantité de services offerts »*. Le projet de loi édicte que ces « avoirs » ne pourront être octroyés que *« pour une durée limitée »* (qui ne pourra excéder un an) et, surtout, *« ne peut être assorti d'une condition d'exclusivité, de quelque nature que ce soit, du bénéficiaire vis-à-vis du fournisseur de cet avoir »*. De quoi limiter la dépendance à certains fournisseurs, bien que les modalités d'application de ces articles doivent être déterminées par décret.

L'Arcep joue la Cnil

Le texte s'attaque ensuite aux frais de transfert, en interdisant aux fournisseurs de facturer des frais de transfert *« supérieurs aux coûts supportés par le fournisseur et directement liés à ce changement »*. L'Arcep et le ministère chargé du numérique fixeront en outre par arrêté le montant maximal de tarification. Notons que les fournisseurs auront également une obligation de transparence, en ce qu'ils devront indiquer aux clients et prospects, *« de façon claire et compréhensible, notamment avant la signature du contrat »*, les frais de transfert de données et de changement de fournisseur, y compris sur la nature et le montant de ces frais. En outre, les fournisseurs de cloud doivent se conformer à quelques nouvelles exigences :

« 1° D'interopérabilité, dans des conditions sécurisées, avec les services du client ou avec ceux fournis par d'autres fournisseurs de services d'informatique en nuage pour le même type de fonctionnalités ;

2° De portabilité des actifs numériques et des données exportables, dans des conditions sécurisées, vers les services du client ou vers ceux fournis par d'autres fournisseurs de services d'informatique en nuage couvrant le même type de fonctionnalités ;

3° De mise à disposition gratuite aux clients et aux fournisseurs de services tiers désignés par ces utilisateurs à la fois d'interfaces de programmation d'applications nécessaires à la mise en œuvre de l'interopérabilité et de la portabilité ».

En cas de litige, que ce soit sur les frais de transfert, sur l'interopérabilité et la portabilité des données ou sur l'intermédiation, l'Arcep pourra être saisie. En cela, l'autorité devient plus ou moins l'équivalent B2B de la Cnil. Elle peut mener contrôle et enquête, mettre en demeure et infliger des sanctions pécuniaires d'un montant maximal de 3 % du chiffre d'affaires mondial du dernier exercice clos du contrevenant, taux porté à 5 % en cas de réitération du manquement, voire ordonner la suspension du service si le fournisseur ne se met pas en conformité.

Filtre anti-arnaque

Sur le volet cybersécurité, le projet de loi prévoit la mise en place d'un filtre de cybersécurité anti-arnaque à destination du grand public. S'appuyant sur une base de données qui rassemblera les sites malveillants identifiés et signalés par les victimes aux autorités, ce filtre avertira les citoyens par un message d'alerte lorsque, après avoir reçu un SMS ou un courriel frauduleux, elles se dirigent vers un site malveillant. La liste est fournie et gérée par l'Arcom, mais le "blocage" d'un site malveillant se passe de l'intervention d'un juge : c'est à la requête de la police qu'un navigateur devra afficher ledit message d'alerte. Si le message reste contournable par l'internaute (le gouvernement ne souhaitait pas lui en laisser la possibilité dans le texte initial), ce dispositif a provoqué une levée de boucliers, notamment de Mozilla et de la Quadrature du Net qui y voit une *« censure administrative »*. Le texte prévoit en outre l'expérimentation, pendant trois ans, d'un guichet administratif unique, chapeauté par France Identité. Cette plateforme agrégera *« l'accès à l'ensemble des services publics nationaux et locaux, y compris les organismes de sécurité sociale et les organismes chargés des droits et des prestations sociales des citoyens »*, citoyens auxquels elle doit permettre d'effectuer l'ensemble de leurs démarches administratives et sociales. A noter que l'Etat aura pour mission de fournir API et autres connecteurs pour automatiser la gestion et le transfert des données entre administrations et collectivités.

Guillaume Périssat

DORA : toujours des interrogations

Le règlement européen DORA (Digital Operational Resilience Act) crée un cadre pour les institutions financières. Il a été adopté et doit entrer en vigueur le 1er janvier 2025. Encore plus contraignant que le RGPD, ce texte continue d'interroger sur les actions à entreprendre dans les entreprises.

Cyril Amblard-Ladurantie, GRC Product Marketing Manager chez MEGA International, voit dans ce texte cinq points fondamentaux et un aspect lourd et massif de cette réglementation qui vise à créer un cadre homogène et global pour tout le secteur financier en mettant en avant la résilience du système, et ce jusqu'aux partenaires technologiques des institutions financières. « *Le texte est vraiment là pour assurer la stabilité financière et éviter les effets domino possibles* » précise-t-il.

S'appuyer sur les bonnes pratiques

Pour beaucoup, la réglementation s'appuie sur une bonne dose de bon sens et de pratiques connues pour renforcer la résilience du système d'information. En premier lieu, la mise en place d'un système de gestion des risques dynamique, ce qui demande de mettre les moyens pour cela et que les instances dirigeantes de l'entreprise comprennent bien le risque engendré par l'informatique. Cela implique, de plus, une connaissance fine du système informatique de l'entreprise et de son architecture afin d'identifier et de cartographier les services les plus critiques et leur infrastructure sous-jacente et de gérer les risques des impacts possibles sur toute la chaîne. Ces différentes opérations doivent pouvoir être auditées. Tout cela doit se partager et avoir un langage commun pour tous les intervenants avec la mise en place de règles de gouvernance. Des échanges et un partage des informations par la threat intelligence entre pairs est un élément intéressant.

Une attention particulière pour les tiers

L'ensemble doit prendre en compte les tiers qui interviennent dans cette chaîne de valeur du SI. Dans le cadre de DORA, il s'agit de répertorier tous les tiers et de s'assurer de leur résilience et des niveaux de services qu'ils peuvent proposer. Ils sont d'ailleurs censés aider dans la résolution d'un incident. Ils doivent eux aussi être prêts à recevoir des demandes d'audit de leurs partenaires ou clients en cas d'externalisation.

« Le texte est vraiment là pour assurer la stabilité financière et éviter les effets domino possibles. »

Cyril Amblard-Ladurantie,
GRC Product Marketing Manager chez MEGA International.

Amundi sera prêt !

Wilfried Lauber, Global CISO chez Amundi, une société de gestion française, voit dans DORA une préparation à ce que Vincent Strubel qualifiait de « grand soir » dans sa session plénière des Assisses de la sécurité en parlant d'un risque systémique autour de systèmes d'information. Sous la houlette de Wilfried Lauber, Amundi se prépare depuis 2019 sur cette réglementation. En 2022, la société a réalisé une analyse d'écarts entre l'existant et ce qui est nécessaire pour être conforme. Cette analyse a été poussée jusqu'au début de cette année avec de multiples échanges avec des juristes, le régulateur, etc.
Cela a permis de formaliser plusieurs choses comme le cadre de risques, le reporting, le suivi des tiers. Il précise : « *nous nous appuyons sur l'existant et nous le renforçons* ». Dans le cadre de la réglementation, il prévoit des plans de tests renforcés vers les prestataires et les solutions internes (pentests). Il a aussi fallu adapter la gouvernance présente pour suivre la réglementation.

Tester encore et encore

Tout ce qui sera mis en place doit être testé pour juger de la continuité d'activité. Ce processus de tests doit être réalisé en continu pour s'adapter au contexte changeant des attaques et des menaces. Une solution doit réaliser un scan en continu du SI.

Des sanctions fortes

Si un incident majeur survient, le texte prévoit, à l'instar du RGPD, une procédure de déclaration de l'incident aux autorités de surveillance nationale ou européenne suivant les cas. Cela sera à l'institution financière d'apporter la preuve qu'elle avait mis en place les procédures et outils adéquats pour traiter et identifier les causes profondes de l'incident et de documenter l'ensemble. Le non-respect du texte peut aller jusqu'à la responsabilité pénale des dirigeants et les institutions financières peuvent se voir infliger une amende pouvant aller jusqu'à 10 millions d'euros ou 5 % de leur chiffre d'affaires annuel total, le montant le plus élevé étant retenu, en cas d'infraction grave au règlement. Sur ce point, les avis diffèrent et certains observateurs ne relèvent pas de plafond sur l'amende comme dans le RGPD.

Des questions récurrentes

Les personnes interrogées pour cet article indiquent des interrogations de leurs clients sur le sujet pour des motifs divers. Baptiste David, responsable avant-vente et déploiement chez Tenacy, met en avant des interrogations des tiers pour savoir si eux aussi doivent se conformer strictement à cette réglementation. ▮

B.G

La fonction de Délégué/déléguée à la Protection des Données (DPD/DPO)

ne devrait-elle pas collaborer avec la fonction RSE ?

Muriel Glatin, administratrice AFCDP.

La fonction de Délégué à la Protection des Données (DPD ou DPO pour Data Protection Officer) est directement liée à la protection des données personnelles au sein d'une organisation, conformément au Règlement Général sur la Protection des Données (RGPD) de l'Union européenne. Son rôle principal est de veiller à ce que l'entreprise respecte les réglementations en matière de protection des données et de s'assurer que les données personnelles sont traitées de manière légale et éthique.

Le département Responsabilité Sociétale des Entreprises (RSE) est responsable de la mise en œuvre des initiatives visant à intégrer des considérations sociales, environnementales et éthiques dans les opérations de l'entreprise. La RSE englobe un large éventail de domaines, tels que la durabilité environnementale, les droits des travailleurs, l'engagement communautaire, *etc.*

DPO et RSE : des synergies évidentes

Comment se fait-il que le département RSE, en charge de vérifier les pratiques de l'entreprise, mobilise si peu la fonction DPO et intègre peu la question de la protection des données dans l'exercice de leur mission ? Bien que la fonction DPD/DPO et le département RSE aient des domaines de responsabilité différents, il peut y avoir de réelles synergies entre eux.

L'intégration de la protection des données personnelles dans les initiatives RSE peut être considérée comme une pratique responsable et éthique. Si une entreprise collecte des données personnelles dans le cadre d'initiatives RSE (comme des enquêtes sur les conditions de travail des employés), il est important de s'assurer que ces données sont traitées conformément aux réglementations de protection des données et que la vie privée des individus est respectée. Bien que la fonction DPO et le département RSE aient des responsabilités distinctes, il peut être bénéfique pour une entreprise de faciliter la communication et la collaboration entre ces deux domaines pour garantir une gestion responsable et conforme des données personnelles dans le cadre des initiatives RSE.

DPO et RSE : cassons les silos

L'entrée en application du RGPD en 2018 a donné naissance à une nouvelle fonction qui s'est installée progressivement dans les entreprises : celle du Délégué à la Protection des Données (DPD/DPO). Pourtant, même 5 ans plus tard, la question de sa position dans l'organigramme se pose toujours. Si le Règlement ne donne pas de précision sur le sujet, la nécessaire neutralité de la fonction interdit de l'envisager à la Direction Marketing et l'exigence de son indépendance suppose qu'elle puisse rapporter facilement et directement à la Direction, comme l'exige le RGPD.

Les principales directions de rattachement sont la Direction Générale, la Direction Juridique, la Direction Conformité / Audit. Notons que le rattachement à une Direction RSE apparaît rarement dans les statistiques. Au-delà des organigrammes, il est surprenant de voir à quel point les équipes DPO et RSE semblent s'ignorer dans l'exercice de leur métier. Les entreprises les plus investies sur le développement durable ont tendance à agir comme les autres : il n'y a pas forcément de relation directe entre les aspects RSE et une éthique particulière concernant l'utilisation des données des clients. Pour réconcilier ces deux missions qui participent à faire l'entreprise responsable, la fonction DPO pourrait collaborer plus étroitement avec l'équipe RSE. Cette option organisationnelle mérite d'être envisagée. Elle témoignerait du fait que le respect des données des personnes, clients comme collaborateurs, s'inscrit dans la responsabilité sociétale de l'entreprise. Elle participerait à faire en sorte que le respect du RGPD soit moins perçu comme une contrainte juridique, mais soit bien un projet mobilisateur en interne.

Avec l'arrivée des nouveaux textes encadrant le traitement de toutes les données comme les Règlements sur les données (Data Act), sur la gouvernance des données (DDGA) et sur l'Intelligence artificielle (IA Act), le métier de DPD/DPO va logiquement évoluer vers une fonction plus globale, se rapprochant d'un « Data Ethics Officer ». Alors pourquoi ne casserions-nous pas les silos DPD / DPO et RSE pour consolider l'ambition d'une entreprise responsable !

Cohesity continue de rassembler

L'éditeur spécialisé dans la gestion de données a lancé, l'an dernier, son Alliance pour la sécurité des données. D'une dizaine de membres au départ, celle-ci en compte désormais 21, avec l'arrivée récente de six partenaires tournés vers la Data Security Posture Management.

Il y a un an, nous interrogions déjà dans ces pages Jean-Baptiste Grandvallet, SE Manager de Cohesity. À l'époque, l'entreprise venait de lancer sa Data Security Alliance, Alliance pour la Sécurité des Données dans la langue de Molière. Que ce soit le XDR avec Cisco et Palo Alto Networks, la partie SIEM et SOAR avec Splunk et Service Now ou encore Tenable pour l'aspect gestion des vulnérabilités, le groupe où siègent Alex Stamos et Kevin Mandia, rien que ça, entendait fournir une stratégie complète de protection et de résilience des données. *« La stratégie reste la même côté Cohesity. Nous avons créé cette Alliance pour pouvoir avoir un écosystème dans lequel on est intégré de manière forte de sorte à résoudre de manière plus efficace les problématiques de cybersécurité »* nous explique aujourd'hui Jean-Baptiste Grandvallet. En un an, la Data Security Alliance s'est élargie, d'un Okta sur la partie PAM ou encore de Netskope et Zscaler dans le Zero Trust.

En quête des données sensibles éparpillées

Mi-octobre, voilà que BigID, Cyera, Dig Security, Normalyze, Sentra et Securiti rejoignent le groupe. Leur point commun ? Ces six entreprises opèrent dans le domaine de la gestion de la posture en matière de sécurité des données (ou DSPM, pour Data Security Posture Management). *« Cohesity aide certaines des plus grandes entreprises du monde à protéger leurs données contre les ransomwares et les cybermenaces dans les environnements de cloud hybride »*, indique Amer Deeba, PDG et cofondateur de Normalyze. *« Grâce à l'intégration avec la plateforme DSPM de Normalyze, les clients bénéficient désormais d'une visibilité totale sur leurs données à travers les différents clouds, SaaS et sur site. Cette solution commune offre aux équipes de sécurité une visibilité sans précédent sur les emplacements et les types de données sensibles. Elle identifie et hiérarchise les risques en fonction de l'impact financier le plus élevé pour l'organisation en cas de violation de données, et protège de manière proactive les données contre les ransomwares et les cyberattaques. »*. Cette catégorie de solutions permet schématiquement aux administrateurs, services IT et équipes cybersécurité de comprendre où se trouvent leurs données sensibles, qui y a accès, comment elles sont utilisées et où elles sont stockées. *« L'adoption accélérée du cloud, combinée à une explosion des microservices et un taux élevé de changement (induit par les pratiques modernes de DevOps) exposent les clients à une prolifération importante des données. De par leurs lacunes en matière de visibilité, les données les plus sensibles sont cachées des yeux des équipes informatiques et, la plupart du temps, ne sont pas protégées »* décrit Cohesity. En rajoutant une solide brique DSPM à son arsenal, l'éditeur surmonte ce problème.

Jouer en équipe

« On ne peut défendre que ce que l'on connaît. Encore faut-il déjà découvrir ces assets là. Donc ces outils ont pour but de les découvrir, principalement dans le cloud, mais aussi de pouvoir faire de la classification de données » précise le responsable de Cohesity pour l'Europe du Sud. *« Nous, nous intervenons en intégration, pour pouvoir faire le mapping et avoir tout de suite derrière un plan de sauvegarde et de remédiation »*. Car c'est là, l'essence même de la Data Security Alliance : regrouper les principaux fournisseurs de cybersécurité, de gestion des données et de services, et établir un lien entre l'informatique d'entreprise et la sécurité, en partageant les informations relatives à la protection des données pour les sécuriser au mieux.
« C'est notre façon de penser. Nous avons fait le choix d'une approche best of breed où l'on travaille en écosystème. Plutôt que de racheter des solutions pour les intégrer, nous avons pris le parti inverse de tirer parti des solutions existantes. C'est le cas sur cette partie DSPM, où nous réunissons les six leaders du marché » poursuit Jean-Baptiste Grandvallet. Car Cohesity ne vend pas de produit de cybersécurité : c'est avant tout un fournisseur de solutions de sauvegarde. L'idée de l'éditeur est ainsi, en fonction des partenariats qu'il parvient à nouer, de couvrir un maximum de secteurs de la cybersécurité, en intégrant des solutions déjà présentes chez ses clients. Objectif : un effet boule de neige.

GUILLAUME PÉRISSAT

« Nous avons créé cette Alliance pour pouvoir avoir un écosystème dans lequel on est intégré de manière forte, de sorte à résoudre de manière plus efficace les problématiques de cybersécurité. »

Jean-Baptiste Grandvallet,
SE Manager de Cohesity.

Les Assises de la sécurité visent plus haut

Les Assises de la sécurité ont pour leur 23ème édition à Monaco regroupé près de 3000 personnes de l'écosystème de la cybersécurité. La première session générale est un moment très attendu de la manifestation. En voici un résumé.

La première session plénière a fait le constat global que les choses avancent dans la cybersécurité, mais que des efforts doivent encore être fait. Pierre Dartout, directeur général d'Europol, a ainsi dressé un tableau au niveau européen en insistant sur un contexte international qui évoluait de plus en plus rapidement où les États ont une responsabilité *a minima* morale dans la lutte contre le crime numérique. Il a d'ailleurs mis en avant les réussites de la collaboration internationale dans plusieurs opérations comme le démantèlement de Hive, ChipMixer ou Qakbot. Il a ensuite dépeint tous les moyens que déploie Europol pour aider les entreprises ou les États en cas d'attaque. Il a ainsi décrit les procédures et les ressources mises en place si une attaque majeure survenait. Il a finalement appelé les experts présents à décloisonner les silos dans les mondes cyber et d'échanger des informations en temps réel sur les menaces afin d'autoriser une prise de hauteur globale face au cybercrime et de souhaiter un passage à l'échelle européenne avec plus de coopération internationale.

Passer à l'échelle

Ce passage à un niveau supérieur était le sujet principal de l'intervention de Vincent Strubel, le directeur général de l'ANSSI. Pour lui, ce besoin est là pour longtemps face aux attaques étatiques ou autres. Le plus souvent, ces attaques frappent les plus petits ou les secteurs un peu en retard sur leur protection comme les collectivités, les hôpitaux ou les PME. Selon lui, il s'agit aussi de se préparer à une attaque majeure. Il souhaite doter notre pays d'une « super résilience ». La transposition de NIS 2 au printemps prochain devrait y aider selon lui. Il a ensuite dressé le tableau des différents intervenants dans la cybersécurité avec la volonté de continuer à travailler les réseaux déjà existants, mais aussi de se tourner vers de nouveaux entrants. Il veut aussi simplifier et rendre plus abordables les outils avec par exemple des référentiels plus abordables pour les prestataires. Il a, de plus, annoncé la construction d'un corpus doctrinal sur les pratiques de remédiation. Création de CERT, meilleur travail avec les opérateurs et fournisseurs de Cloud. Il s'est ensuite félicité de l'accueil européen aux initiatives françaises avec SecNumCloud. Lui aussi a souhaité une meilleure collaboration internationale dans la réponse aux attaques en s'appuyant sur les réseaux de prestataires et de partenaires afin de mettre en œuvre une véritable solidarité face aux attaques. Il y voit aussi un moyen de beaucoup y apprendre des intervenants de cette solidarité pour encore renforcer la résilience souhaitée.

Les autres sessions plénières

Cloudflare et Thales avaient aussi leur accès à la scène du Grimaldi Forum. Le keynote de Cloudflare avait pour sujet l'émergence de différentes technologies comme l'intelligence artificielle générative et l'informatique quantique qui vont ou ont déjà bouleversé le paysage de la cybersécurité pour plusieurs secteurs d'activité… Elles représentent à la fois des opportunités et des défis à relever pour les entreprises. Guillaume Cécile, RSSI du groupe Carrefour, et Michelle Zatlyn, présidente et co-fondatrice de Cloudflare, ont abordé comment se dessinait le nouveau paysage des menaces et la mise en avant de stratégie proactive pour sécuriser ce monde numérique en constant changement.
La session de Thales partageait une perspective sur la menace que fait peser le quantique sur les RSSI et a proposé des pistes et des plans de mise en œuvre pour limiter les risques. Comme à chaque édition, il est possible de retrouver sur le site des Assises les différentes sessions plénières.

Guillaume Cécile, à gauche, Michelle Zatlyn, au centre et Boris Lecoeur, à droite lors du keynote de Cloudflare.

Bertrand Garé

#SIDO2023

Le rendez-vous des technologies
IoT, IA, Digital Infra et Cybersécurité
pour concrétiser la transformation digitale
des entreprises !

PARIS 3e

SIDO

IoT – AI – DIGITAL INFRA – CYBERSECURITY

6 & 7 Décembre 2023

Palais des Congrès, Paris

120 Exposants
30 Conférences
120 Speakers

Créer mon badge gratuit

CODE : P-INFSP23

www.sido-paris.com

MÊMES DATES - MÊME LIEU

OPEN SOURCE EXPERIENCE

Découvrez Open Source Experience

L'événement Européen Tech - Usage - Business de l'Open Source !

Hall Maillot - Niveau 1

Ce badge vous donne accès aux deux événements

UN ÉVÉNEMENT

infoprodigital TRADE SHOWS

Tenacy

ALL YOUR CYBER IN ONE PLACE

tenacy.io