N° 219 — Septembre 2023

www.linformaticien.com

L'INFORMATICIEN

Étude
Le Data Act

Cloud
Memority

TOP TECH

Les DSI et ESN à l'honneur

Retex
Michelin capitalise sur le streaming de données

DevOps
Stability AI

Logiciel
- Le LLM en France
- Natural Solutions

L 14614 - 219 - F: 8,50 € - RD

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

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, Christophe Guillemin, Guillaume Renouard, 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 : 3ième trimestre 2023

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

Toujours du nouveau avec *L'Informaticien*

Vous avez dû le constater, le magazine pèse plus lourd ce mois-ci. Auparavant, nous avions un trimestriel, *L'InfoCR*, qui couvrait les sujets de la cybersécurité. Cette période de trois mois était, à notre vue, trop longue pour être pertinente sur un sujet qui évolue rapidement, quasiment tous les jours. Nous avons donc décidé d'écourter ce délai en ajoutant un cahier mensuel dédié à ce sujet dans chaque numéro : 16 pages entièrement dédiées à ce seul sujet pour être au plus proche de l'actualité.

Dans ce numéro, nous célébrons aussi les vainqueurs de notre événement Top Tech qui a rendu ses prix lors d'une très belle soirée à l'Hôtel Intercontinental. Bravo encore à toutes nos ESN et DSI primées pour leurs projets sur trois thèmes : l'Innovation, les RH et le RSE.

Dans quelques jours, les votes pour le Palmarès 2023 vont se lancer, un événement qui est déjà devenu une référence pour notre communauté et nos partenaires, afin d'élire les produits que vous appréciez et utilisez au jour le jour. Comme toujours, vous retrouverez toutes nos rubriques habituelles et le compte-rendu des principales conférences d'importance qui se sont tenues au début de l'été. Vous voyez, ça bouge à *L'Informaticien* ! Il ne me reste plus qu'à vous souhaiter la meilleure des rentrées, qui va être sur les chapeaux de roue en ce qui nous concerne ! □

Bertrand Garé
Rédacteur en Chef

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

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

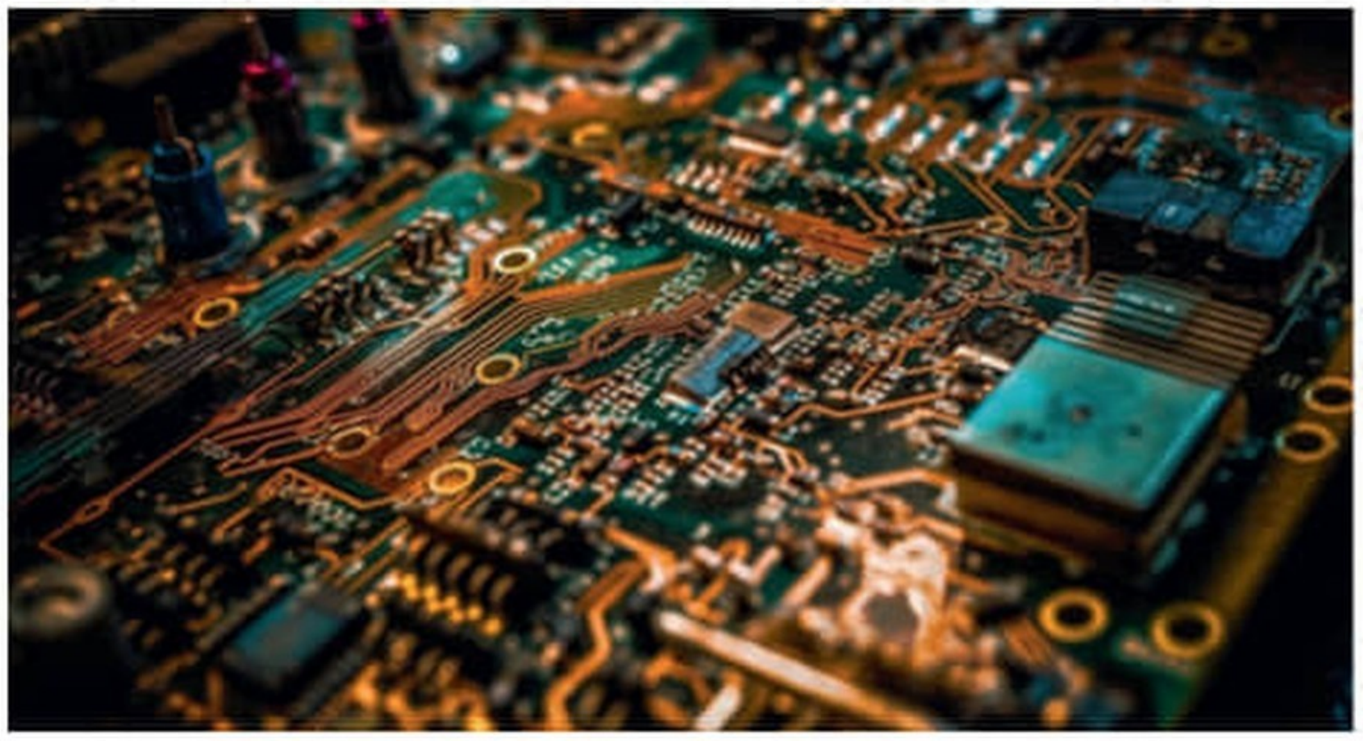
IBM

LES CHAMPIONS DE L'IT ÉCORESPONSABLE

FOCUS

Semi-conducteurs : grandes manœuvres en Europe

Alors que l'Allemagne subventionne à hauteur de près de 10 milliards d'euros l'usine Intel à Magdebourg, Stellantis prévoit un investissement similaire afin de sécuriser son approvisionnement en puces.



Les semi-conducteurs continuent d'être un sujet de préoccupation, aussi bien pour les gouvernements que les entreprises. Les uns comme les autres n'hésitent pas à sortir le chéquier pour sécuriser leurs chaînes d'approvisionnements en puces et autres composants. Ainsi, le gouvernement allemand a annoncé l'octroi à Intel d'une subvention de 9,9 milliards d'euros pour l'installation d'une usine à Magdebourg. Soit 3 milliards de plus que la somme initialement prévue, sachant que Berlin a accordé 10 milliards d'euros supplémentaires à d'autres industriels du secteur, dont TSMC et Infineon.

Ces aides, sous forme d'incitations, permettront selon le chancelier allemand Olaf Scholz de *« rattraper technologiquement les meilleurs au monde et d'élargir [leurs] propres capacités pour le développement de l'écosystème et la production de micropuces »*. L'accord passé entre Intel et l'exécutif germanique concerne deux installations de semi-conducteurs, baptisées Silicon Junction, pour un investissement total de plus de 30 milliards de dollars. Le plus important jamais réalisé par une entreprise étrangère dans le pays. *« Les investissements d'Intel jettent les bases d'un écosystème européen de puces de nouvelle génération, aidant l'Union européenne à atteindre son objectif d'une chaîne d'approvisionnement en semi-conducteurs plus résiliente »*, a déclaré l'entreprise dans un communiqué.

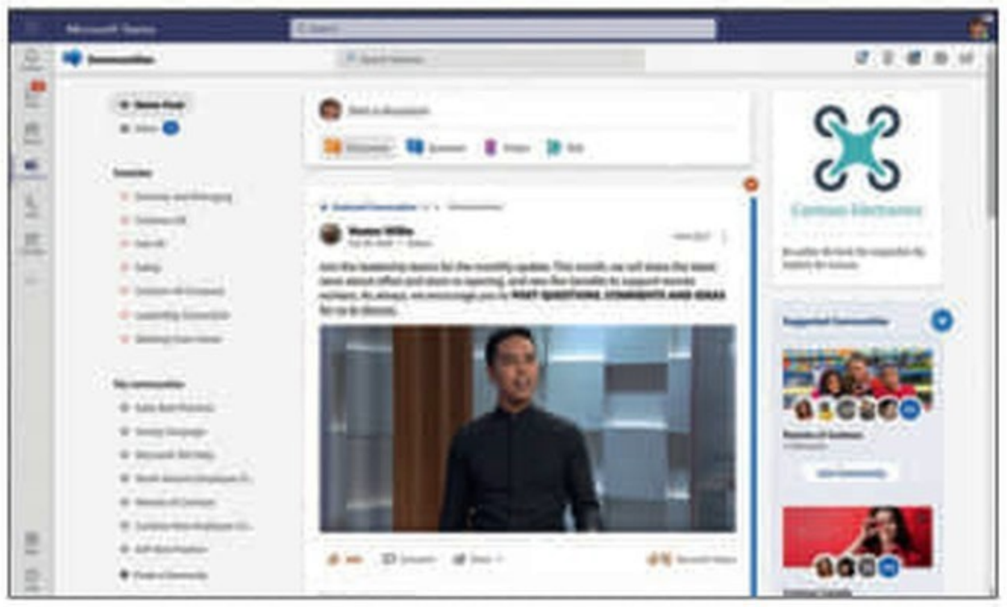
Cette nouvelle usine en Allemagne s'inscrit dans un vaste programme à 80 milliards de dollars d'investissements sur 10 ans annoncé par Intel l'année dernière. L'industriel américain opère déjà une usine de fabrication en Irlande ainsi qu'une installation d'assemblage et de test en Pologne. La première installation doit entrer en production d'ici 4 à 5 ans. La Commission européenne doit néanmoins encore approuver le programme d'incitations. Une formalité puisque l'infrastructure s'inscrit dans le Chips Act qui doit permettre à l'Union européenne d'atteindre 20 % de parts de marché des semi-conducteurs d'ici 2030 et de jouer des coudes avec ses concurrents asiatiques et américains. Au regard du calendrier qui s'étalera sur plusieurs années, Intel a décidé de revoir sa copie et de déployer une technologie plus avancée de l'ère Angstrom (1/1000 de micron). Le site servira les produits Intel et les clients d'Intel Foundry Services.

Stellantis multiplie les contrats d'achats

De notre côté du Rhin, c'est Stellantis qui dégaine le portefeuille pour sécuriser ses approvisionnements en puces. La pénurie de semi-conducteurs continue d'affecter le secteur automobile : cette année, près de trois millions de véhicules ne pourront être produits faute de composants électroniques. Le groupe franco-italo-américain a signé pour 10 milliards d'euros de contrats d'achat jusqu'en 2030. L'opération doit lui permettre de sécuriser ses approvisionnements pour construire des véhicules électriques et garantir les fonctionnalités de ses futures plateformes véhicules « STLA BEV-centric » qui doivent être lancées très prochainement. Les différents accords d'approvisionnement concernent la livraison de puces MOSFET en carbure de silicium (SiC), des microcontrôleurs (MCU), et des « System-on-a-chip » (SoC). *« Plusieurs centaines de semi-conducteurs très différents sont intégrés à nos voitures. Nous avons conçu un écosystème complet pour limiter le risque qu'une seule puce manquante puisse mettre nos lignes à l'arrêt »*, a déclaré dans un communiqué Maxime Picat, directeur des achats et de l'approvisionnement de Stellantis. La société indique également collaborer avec les fabricants de puces Infineon, NXP Semiconductors, Onsemi et Qualcomm, afin d'optimiser ses technologies et ses nouvelles plateformes STLA. Le géant travaille en parallèle à développer sa propre filière de semi-conducteur, en partenariat avec aiMotive et Silicon Auto.

Teams dans le viseur de **Bruxelles**

La Commission européenne a annoncé, jeudi 27 juillet, ouvrir une procédure antitrust visant Teams, la plateforme de communication et de collaboration du géant américain. Bruxelles soupçonne la firme de Redmond d'avoir enfreint les règles de concurrence de l'UE, par le biais d'un avantage de distribution à Teams. En effet, en incluant la plateforme collaborative à tout abonnement à Microsoft 365, l'éditeur pousserait les clients à utiliser Teams par défaut, plutôt qu'une offre concurrente. Ce qui pourrait constituer un abus de position dominante sur le marché des logiciels de productivité. La Commission craint également que Microsoft ne limite l'interopérabilité entre ses produits et ceux de la concurrence. *« Ces pratiques peuvent constituer des ventes liées ou groupées anticoncurrentielles et empêcher les fournisseurs d'autres outils de communication et de collaboration d'exercer une concurrence, au détriment des consommateurs de l'Espace économique européen (EEE) »*, écrit l'exécutif européen dans son communiqué. Cette enquête fait suite à un dépôt de plainte de Slack, le



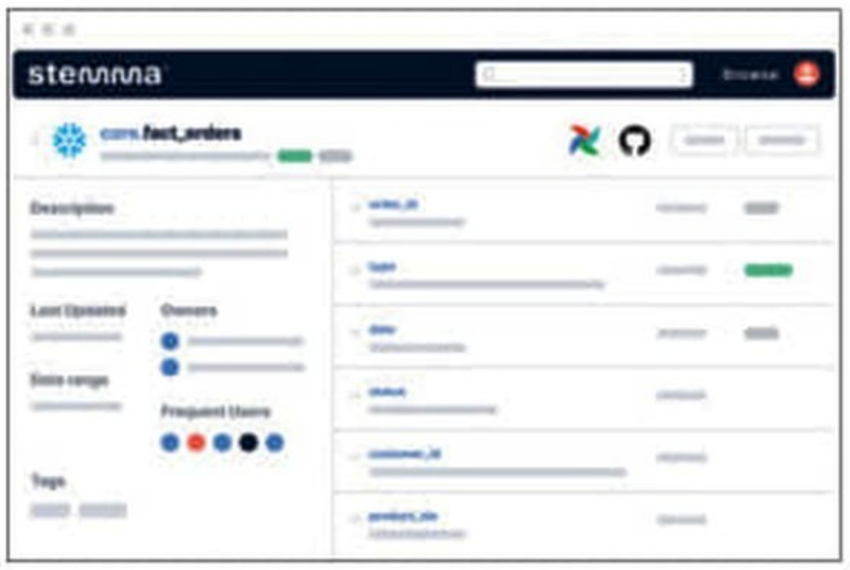
14 juillet 2020, qui accusait la firme Redmond d'avoir lié illégalement et sans surcoût Teams à ses suites de productivité. S'il est condamné, le géant de la tech risque une lourde sanction. Il a déjà dû s'acquitter de 2 milliards d'euros d'amendes à la suite d'infractions aux règles européennes de la concurrence.

Communications « hors canal » : BNP Paribas et la **Société Générale** sanctionnées

La Commodity Futures Trading Commission (CFTC) et la Securities and Exchange Commission (SEC) ont condamné BNP Paribas et la Société Générale de verser une amende de 110 millions de dollars chacune. À la suite d'une enquête, l'autorité de régulation des marchés financiers des États-Unis a révélé des communications *« "hors canal" omniprésentes et de longue dates »*. À partir de 2019 au moins, des employés d'une dizaine d'entreprises, dont ceux des deux banques françaises, ont régulièrement utilisés iMessage, WhatsApp et Signal sur leurs appareils personnels pour communiquer dans le cadre de leur activité, *« ce qui a entraîné des risques de sécurité et de transparence vis-à-vis des autorités financières, en violation des lois fédérales sur les valeurs mobilières »*, ont estimé les deux agences fédérales. La SEC a précisé dans un communiqué qu' : *« en omettant de maintenir et de conserver les dossiers requis, certaines des entreprises ont probablement privé la Commission de ces communications hors canal dans diverses enquêtes de la SEC »*. En plus des sanctions financières, les entreprises mises à l'amende vont devoir rentrer dans le rang en prenant des dispositions et s'engager à ne plus enfreindre les règles. Cela inclut par exemple, le recours à des consultants indépendants afin d'examiner leurs politiques et procédures relatives à la conservation des communications électroniques effectuées sur des appareils personnels.

RACHATS

Teradata s'offre Stemma



Le fournisseur de solutions analytiques reprend l'activité de ce spécialiste du catalogue de données, né en 2020. Stemma est connu pour avoir infusé des technologies d'intelligence artificielle dans sa solution de catalogue des données et des métadonnées afin de simplifier la recherche, la découverte et la confiance dans l'utilisation des données dans les entreprises. La solution de Stemma va enrichir la plateforme Vantage de Teradata et son architecture de data fabric par de nombreux connecteurs et ainsi améliorer la productivité de la plateforme autour des projets analytiques et d'apprentissage machine. De plus, de nombreuses fonctions comme le lignage des données, la gouvernance et le respect de la conformité vont se trouver renforcées. Aucun détail financier n'a été communiqué.

Avec le rachat d'Imperva, Thales se voit en géant de la cyber

Thales a pour projet, au 1er janvier prochain, de regrouper l'ensemble de ses activités cyber, du moins les civiles, dans sa branche Digital Identity & Security. *« Cela renforcera encore la position de DIS en tant qu'acteur incontournable pour les produits et solutions de cybersécurité civile, et facilitera les synergies au sein du portefeuille complet »* précise le groupe. Et, pour accélérer le développement de cette branche, l'entreprise française sort le chéquier. Ces derniers mois, Thales s'est offert, Tesserent (qui n'est pas encore finalisée), S21sec & Excellium ainsi que OneWelcome. Et le voilà qui annonce avoir trouvé un terrain d'entente avec le fonds Thoma Bravo, afin de mettre la main sur Imperva. Pour ce faire, Thales signe un chèque de 3,6 milliards de dollars. Installé à San Mateo, Imperva est surtout connu pour ses pares-feux applicatifs Web (WAF), étendus depuis aux API (on parle alors de WAAP). Opérant plus largement dans le secteur de la sécurité des données, comprenant découverte, gouvernance, classification, monitoring ou encore analyse de risques, la société a engrangé plus d'un demi-milliard de dollars de revenus en 2022 et compte quelque 1400 salariés. La clôture de la transaction est prévue d'ici début 2024, sous réserve de l'approbation antitrust et les réglementations habituelles. Ce faisant, Thales entend rajouter la sécurité des applications à son arc, tout en accélérant le développement de ses solutions autour de la sécurité des données.

Mazars met la main sur Advestis

Le groupe financier annonce l'acquisition d'Advestis. Cette société de recherche sous contrat parisienne fondée en 2011 est spécialisée dans le domaine de l'intelligence artificielle. Travaillant historiquement pour les institutions financières, l'entreprise propose ses services de R&D en finance et en ESG, mais a également travaillé sur des sujets de réseaux d'énergie, de maintenance prédictive ou encore de recherche médicale, pour une quarantaine de projets depuis sa création. Ce faisant, Mazars compte accélérer en matière de R&D dans l'intelligence artificielle. En France, ses équipes Data Services comptent désormais 90 collaborateurs, dont 12 dédiés exclusivement à la recherche et au développement algorithmique.

Rubrik s'empare de Laminar

Le spécialiste de la protection des données annonce l'acquisition de Laminar, éditeur d'un logiciel de gestion de la posture de sécurité des données. Les termes de l'accord n'ont pas été divulgués. Laminar associe une conception cloud-native à une expertise en matière de sécurité afin de fournir la visibilité et le contrôle dont les entreprises ont besoin pour protéger leurs données les plus sensibles. De plus, Rubrik s'appuiera également sur l'équipe de Laminar pour créer un centre de R&D à Tel Aviv, en Israël. Ce centre s'ajoutera aux centres de R&D Rubrik déjà existants à Bangalore, en Inde, et à Palo Alto, en Californie.

Hammerspace lève 57 millions de dollars

Le spécialiste de la gestion des données réalise sa première levée de fonds institutionnelle. Menée par Prosperity7 Ventures et d'autres investisseurs de premier plan, l'opération, d'un montant de 57 millions de dollars, doit permettre à l'éditeur de continuer à améliorer sa plateforme et son service. Des embauches sont prévues pour avoir des professionnels très expérimentés afin d'aider les clients à gérer et à utiliser leurs données non structurées jusqu'à leur monétisation.

55 millions pour l'Allemand NEURA Robotics

Jeune pousse d'IA et de robotique, NEURA Robotics a bouclé un tour de table à 55 millions de dollars mené auprès de Lingotto, Vsquared Ventures, Primepulse et HV Capital. La société fondée en 2019 souhaite ainsi soutenir sa croissance aux États-Unis et au Japon et étendre son usine de production en Allemagne afin d'honorer son carnet de commandes qui s'établit actuellement à 450 millions de dollars. NEURA Robotics a conçu une plateforme et un robot cognitif dopé à l'IA prêt à être commercialisé. Baptisé MAiRA et reposant sur la plateforme de l'entreprise, le robot est capable de percevoir son environnement, les personnes qui l'entourent et d'agir de manière autonome.

Quobly boucle un tour de table à 19 millions d'euros

Anciennement Siquance, l'entreprise grenobloise Quobly vient de lever 19 millions d'euros. L'opération a été menée par Quantonation, Bpifrance via le fonds Deep Tech 2030, Supernova Invest et Innovacom. Plusieurs banques comme le Crédit Agricole Alpes Développement et CEA Investissement, Caisse d'Epargne Rhone Alpes et BNP Paribas ont également mis la main au portefeuille. La levée de fonds doit donner les billes nécessaires à Quobly à la mise en place de partenariats technologiques stratégiques afin de développer son processeur de calcul quantique tolérant aux fautes, utilisant les technologies standards du calcul comme les semiconducteurs. Quobly compte mettre en place des contrats de collaboration et de sous-traitance avec des usines européennes de semiconducteurs. Dans le détail, la société souhaite doubler ses effectifs pour atteindre 50 salariés d'ici fin 2024 en embauchant de nouveaux experts de technologies silicium et des ingénieurs quantiques.

Levée à 21 millions d'euros pour Microoled

Autre société grenobloise, Microoled opère, elle, dans le secteur des solutions Oled. Fondée en 2007, cette entreprise a bouclé un nouveau tour de table de 21 millions d'euros mené par Jolt Capital, auprès du fonds souverain de Bpifrance et de ses deux actionnaires historiques, Cipio Partners et Ventech. L'opération doit permettre à la société de tripler ses capacités de production à Grenoble et de développer sa nouvelle génération de solutions Oled. La société souhaite également consolider ses positions sur le segment des lunettes de réalité augmentée. Elle mise pour cela, sur son module d'affichage tête haute ActiveLook qui permet d'intégrer dans des lunettes des informations visuelles en temps réel, offrant des cas d'utilisation dans le sport ou encore dans l'industrie de la sécurité.

Nokia et Red Hat partenaires

Dans le cadre de cet accord, les deux sociétés vont supporter et faire évoluer les clients actuels de Nokia Container Services (NCS) et Nokia CloudBand Infrastructure Software (CBIS) en développant une solution de migration vers les plateformes de Red Hat au fil du temps. Dans le même temps, Nokia va s'appuyer sur les plateformes d'infrastructure de Red Hat pour accélérer et tester les nouveautés des applications de son portefeuille cœur de réseau. Les clients de Nokia seront supportés directement par Red Hat. De plus, certaines équipes Cloud de Nokia vont rejoindre Red Hat afin d'assurer la transition et le suivi de la feuille de route de développement.

Pour résumer, Nokia va adopter les outils d'infrastructure de Red Hat comme plateforme de développement, de test et de déploiement de ses applications de cœur de réseau. Nokia va, cependant, continuer sur les applications NCS et CBIS. Les applications de cœur de réseau de Nokia seront nativement intégrées avec les piles OpenStack et Kubernetes de Red Hat. Les fonctions réseaux nativement cloud et les fonctions virtuelles bénéficieront de plusieurs options de déploiement (Bare Metal, Cloud...).

Finovox s'allie à PwC

La start-up française spécialisée dans la détection de faux documents devient partenaire du cabinet de conseil PwC dans une collaboration visant à renforcer les capacités de détection de fraude documentaire des organisations accompagnées par PwC France.

Après avoir réalisé avec succès une première mission conjointe, Finovox est désormais référencée comme solution anti-fraude au sein de PwC France. Le cabinet met désormais à disposition de ses clients sa solution permettant une analyse approfondie et rapide des documents pour vérifier leur authenticité et leur véracité. Dans un premier temps, Finovox a été mandatée par un client de PwC France pour procéder à un audit documentaire complet. Un total de 13 000 documents a été soumis à l'analyse de la plateforme SaaS de Finovox, qui a permis de détecter instantanément près de 280 falsifications (soit 2 % de l'ensemble des documents transmis). Les équipes de PwC France avaient exprimé leur volonté d'être accompagnées par un logiciel performant de détection de faux documents afin d'aller au-delà d'une simple analyse visuelle et d'accélérer le processus de détection.

Kyndryl et Veritas proposent de nouveaux services

La société de services et l'éditeur de solutions de protection de données étendent leur partenariat avec deux nouveaux services.

Les deux entités ont dévoilé deux nouvelles propositions : Data Protection Risk Assessment with Veritas et Incident Recovery with Veritas. Data Protection Risk Assessment with Veritas est délivrée par le réseau d'experts technologique de Kyndryl Consult et fournit une évaluation de la maturité de la cyber-résilience qui analyse l'infrastructure informatique et les données d'un client par rapport aux meilleures pratiques de l'industrie. Kyndryl associe son expertise de cyber-résilience aux solutions de gestion des données de Veritas pour identifier les risques, les lacunes en matière de cyber-résilience et les vulnérabilités en matière de sécurité. L'offre fournit également des informations unifiées sur les environnements on-premise, hybrides et cloud en exploitant des data points uniques qui donnent aux clients la visibilité et les informations nécessaires pour mieux gérer et protéger leurs données.

Incident Recovery with Veritas est un service entièrement géré qui englobe la sauvegarde, la reprise après sinistre et la cyber-reprise. L'un des principaux facteurs de différenciation de la solution réside dans les capacités de gestion autonome des données basées sur l'IA, qui favorisent l'automatisation intelligente, l'agilité opérationnelle, l'efficacité à l'échelle et une expérience cohérente entre les clouds pour une récupération rapide en cas de cyber-incident.

IBM et NumSpot alliés pour un SecNumCloud

Les deux entreprises annoncent un partenariat afin de fournir un cloud de confiance à travers les services de NumSpot et des logiciels IBM au travers de la marketplace du fournisseur de services Cloud.

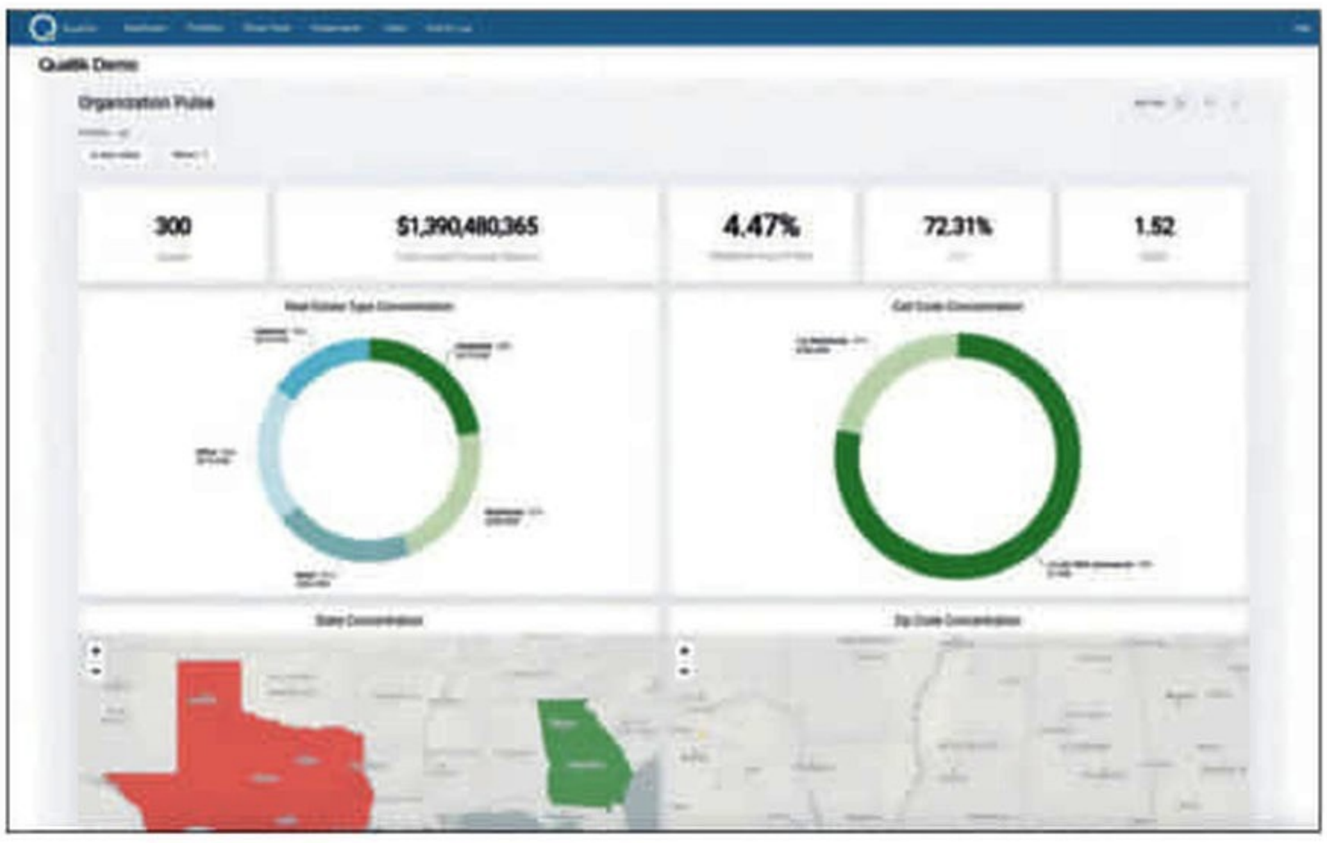
IBM a vu en NumSpot un partenaire représentant pour les clients un acteur de confiance qui porte l'ambition de devenir le Cloud de référence européen souverain et de confiance, qualifié SecNumCloud. De son côté le fournisseur de Cloud a vu en IBM un partenaire, leader de l'IA et de l'open hybrid Cloud, présent en France depuis plus de 100 ans avec des implantations sur tout le territoire et créateur de valeur pour la transformation numérique des acteurs français.

Cette annonce, qui repose sur un accord sans exclusivité, offre de nouvelles perspectives de développement et d'accélération business à de nombreux clients des secteurs stratégiques et sensibles qui pourront désormais utiliser leurs solutions sur une offre de Cloud souverain et de confiance via l'offre de NumSpot.

KPMG et Microsoft étendent leur partenariat

Les deux entreprises étendent leur partenariat existant au niveau mondial pour proposer de nouveaux services autour de l'intelligence artificielle.
Cette collaboration prévoit un investissement de KPMG de plusieurs milliards de dollars dans les services de cloud et d'IA de Microsoft au cours des cinq prochaines années. Elle constitue pour KPMG une opportunité de croissance incrémentale potentielle de plus de 12 milliards de dollars. Elle a pour objectif autant de renforcer la relation et le service au client que de décupler l'expérience collaborateurs, de manière responsable et en confiance.
D'autre part, les capacités du cloud Microsoft et d'Azure OpenAI permettront aux 265 000 collaborateurs de KPMG dans le monde d'innover, d'effectuer des analyses plus rapides et de consacrer davantage de temps au conseil stratégique. Ils pourront ainsi accompagner leurs clients, dont plus de 2 500 sont communs à KPMG et Microsoft. En tant que partenaires de premier plan pour Microsoft 365 Copilot et Azure OpenAI, les équipes de KPMG piloteront ces technologies au travers de business units sélectionnées au sein du réseau mondial.

Linedata s'associe à Qualtik



Le fournisseur de solutions pour les institutions financières ouvre un partenariat avec Qualtik, un éditeur spécialisé dans les solutions de Stress Test pour les prêts commerciaux basé aux États-Unis.
En combinant les outils de stress-test de Qualtik aux solutions d'analyse de portefeuille de Linedata, ce partenariat vise à faire évoluer la façon dont les banques gèrent leurs portefeuilles de prêts commerciaux. Cette intégration élimine les nombreuses feuilles de calcul qui prévalent dans l'industrie, pour proposer une méthode d'analyse du risque novatrice par un outil d'automatisation, permettant de renforcer le contrôle et la transparence de leurs opérations. Grâce à ce partenariat, les banques ont la possibilité d'identifier de manière proactive les prêts à risque, d'évaluer les garanties et d'utiliser des données en temps réel pour prendre des décisions.
Les outils de stress-test de Qualtik sont intégrés aux solutions de crédits et financements de Linedata, Linedata Capitalstream et Linedata Ekip360, destinées aux banques et établissements de crédit, qu'il s'agisse de banques de proximité ou d'institutions régionales et nationales. Les institutions financières dont les actifs s'élèvent à 500 millions d'euros et au-delà ont désormais accès à des informations en temps réel, à une vue d'ensemble instantanée et transparente sur l'évolution des risques et à un contrôle total de leurs portefeuilles de prêts commerciaux. La solution intégrée, disponible dès aujourd'hui, vise à offrir une approche rationalisée et efficace de la gestion des risques. Elle permet aux banques d'optimiser la prise de décision, grâce à l'analyse des données, et ainsi de structurer leur approche pour faire face aux incertitudes économiques.

AGENDA

IFA
1-5 septembre 2023
Messe Berlin, Berlin

Dreamforce
12-14 septembre
Moscone Center, San Francisco USA

SIDO Lyon
20-21 septembre 2023
Cité Internationale, Lyon

Big Data & AI
25-26 septembre 2023
Palais des Expositions Porte de Versailles, Paris

Salons Solutions
3-4 octobre 2023
Palais des Expositions Porte de Versailles, Paris

Assises de la sécurité
11-14 octobre 2023
Grimaldi Forum, Monaco

European Blockchain Convention
24-26 octobre 2023
Estrel Congress Center, Barcelone

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

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

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

TopTech 2023

Sous le signe de la nouveauté

En 2023, le TopTech a fait peau neuve en donnant la priorité aux projets présentés et développés par les ESN et leurs clients. Lors de la soirée de remise des prix, plus d'une centaine de participants sont venus récupérer leurs trophées à l'hôtel Intercontinental Paris-Opéra. Rendez-vous en juin 2024 pour une édition qui apportera également plusieurs nouveautés. Dans cette attente, nous invitons tous nos partenaires et lecteurs à nous faire part de leurs suggestions pour cette prochaine édition.

Pour cette deuxième édition du TopTech, nous avons décidé de modifier le mode de sélection des lauréats, après consultation de plusieurs DSI partenaires et bien entendu des ESN concernées. Alors que la première édition s'appuyait sur une consultation de nos lecteurs, nous avons souhaité cette année privilégier les candidatures des entreprises intéressées à participer à notre événement sur la base d'un questionnaire proposé dans les principales catégories de projets, aujourd'hui majoritairement déployés par les entreprises de services numériques. Ces catégories sont : innovation, dans laquelle nous retrouvions les sous-catégories suivantes : Cloud, cloud souverain, Stratégie-organisation, intelligence artificielle, technologies du futur, Devops et cybersécurité. Ensuite, la catégorie Green IT découpée en efficacité énergétique, impact local et économie circulaire. Enfin, la catégorie RH avec 2 sous-catégories : formation/compétences et Attractivité/rayonnement. Parallèlement, nous avons ouvert la compétition à des DSI qui pouvaient concourir dans les catégories Innovation (Transformation numérique, Gestion de la relation client, Fonction RH, Fonction Finance, Supply Chain/Achat) ; RSE (Green Infra, Économie circulaire, Communication et engagement ; RH (Diversité/recrutement, Qualité de vie au travail/marque employeur, Expérience collaborateur) pour des projets déployés dans leurs propres entreprises. Enfin, et comme vous pourrez le voir dans les infographies jointes, un certain nombre de récompenses ont été délivrées pour les ESN. Bien entendu, chacun des participants avait la possibilité de concourir dans plusieurs catégories, ce qui a d'ailleurs souri à plusieurs ESN qui ont remporté plusieurs prix.


Gaël Chervet, président du groupe Ficade/Leaders League.

LE GROUPE FICADE

Lors de la cérémonie de remise des prix, Gaël Chervet, président du groupe Ficade/Leaders League, a rappelé quelques faits sur le groupe de communication duquel fait partie *L'Informaticien*.

« Nous sommes un groupe de media et de communication B2B. Nous intervenons dans 12 pôles d'activités : la Finance, l'Immobilier, les RH, l'IT, l'Innovation, le Marketing, la Santé, le Patrimoine... Nous sommes aujourd'hui plus de 200 collaborateurs, dont une trentaine à l'international : en Espagne, Italie, Brésil et même au Pérou. Dans chacune de nos expertises, nous déclinons une offre de communication globale avec des magazines, des sites d'information, des événements, des classements, notamment dans le cadre de notre activité d'agence de notation, et de l'audiovisuel (nous tournons en moyenne 5 émissions par jour dans nos studios de Décideurs TV). Sur ce dernier point, nous prévoyons un lancement de la chaîne sur les box (Orange, Bouygues et Free) en début d'année prochaine. »

Des dossiers très complets

Les questionnaires proposés demandaient aux répondants de se prononcer sur les éléments suivants : stratégie, technologies, processus, respect du budget, respect des délais, résultats et synergies. Notre rédaction a reçu une cinquantaine de dossiers, pour la plupart très construits et argumentés. Nous avons donc envoyé ces dossiers à notre jury constitué de plusieurs DSI d'entreprises privées et publiques parmi lesquels, : Bernard Giry, Raphaël de Cormis, Sihame Allali, Jacky Galicher, et bien sûr la rédaction du magazine Bertrand Garé et Guillaume Perissat, qui ont accepté de départager les projets qui nous avaient été soumis. Les résultats définitifs ont été déterminés à l'issue d'une journée de réunion qui s'est déroulée le 9 juin dernier pour une cérémonie de remise des prix se déroulant le 19 du même mois. Les décisions ont été en totalité prises à l'unanimité de l'ensemble des membres du jury, parfois cependant à l'issue d'âpres discussions, toujours courtoises, mais déterminées dans la volonté de défendre son choix. Dans 2 ou 3 cas, les discussions ont abouti à une situation d'*ex-æquo.*

Finalement, au-delà de l'innovation et des technologies déployées, les différents projets ont majoritairement mis en avant la nécessité de former les meilleurs collaborateurs pour l'accomplissement et la mise en œuvre des différents projets, qu'il s'agisse des ESN ou des entreprises au travers de leurs DSI. *« Si la formation est un levier essentiel de la compétitivité, elle représente également un outil remarquable de motivation, de valorisation des compétences et de fidélisation des équipes »*, précise Meritis. SQORUS ajoute : *« le monde du conseil et des ESN ne prend pas toujours compte des envies des collaborateurs et de leur épanouissement professionnel. Chez SQORUS, nos valeurs sont présentes dans l'ensemble des pratiques de notre organisation (Mentoring, organisation, recrutement, stratégie) et nos pratiques managériales »*. Plus que jamais, le recrutement et la formation deviennent l'un des principaux leviers de la réussite des ESN et de leurs clients. □

Rendez-vous en 2024 pour une nouvelle édition pleine de nouveautés et de surprises.

Méthodologie du TOPTECH

Le TopTech distingue les meilleurs projets IT présentés par :

1) les DSI d'une part,

Catégories : Innovation (Cloud, Cloud Souverain, Stratégie-Organisation, Intelligence Artificielle, Technologies du futur, Devops, Cybersécurité) ; Green IT (Efficacité énergétique, Impact local, Economie circulaire) ; RH (Formation/compétences, Attractivité/rayonnement)

2) les ESN d'autre part.

Catégories : Innovation (Transformation numérique, Gestion de la relation client, Fonction RH, Fonction Finance, Supply Chain/Achat) ; RSE (Green Infra, Economie circulaire, Communication et engagement ; RH (Diversité/recrutement, Qualité de vie au travail/marque employeur, Expérience collaborateur)

Chaque dossier de candidature fait l'objet d'une analyse par un jury composé des membres de la rédaction de L'Informaticien et de directeurs informatiques.

Une méthodologie originale et innovante

Le TopTech repose sur une méthodologie originale : pour la première fois, ce sont les projets informatiques qui font l'objet d'une analyse par un jury de professionnels sur la base d'un questionnaire "métier".

Les projets sont analysés selon la grille des critères suivants : stratégie, technologies, processus, respect du budget, respect des délais, résultats, synergies.

Le jury

Le jury est composé de DSI, de partenaires technologiques et de la rédaction de L'Informaticien. Il étudie les dossiers de candidature et détermine les lauréats dans les différentes catégories.

PRIX DE LA GESTION DE PROJET
Blue Soft Group

PRIX DE LA CROISSANCE
Datasolution

PRIX DE LA RÉDACTION
Conserto

MEILLEUR PROJET RH
Sqorus

MEILLEUR PROJET GREEN IT
Axopen

MEILLEUR PROJET INNOVANT
Tenacy

ESN

INNOVATION		
Cloud	Amexio	*Amexio a fourni un dossier solide sur son projet OCAPI, étayé par des retours chiffrés de ses clients.*
Cloud	Sedona	*Sedona a su captiver le jury avec son projet "Vendor Machine", accessible et sécurisé.*
Stratégie-Organisation	Aymax Consulting	*Avec son projet entre Courbevoie et Tunis, Aymax nous présente une approche interculturelle intéressante et cohérente.*
Intelligence Artificielle	Aymax Consulting	*En intelligence artificielle, le plus difficile c'est de passer du projet à la production. Aymax est allé jusqu'au bout, en prod, et a su présenter des résultats concrets de ses modèles, dans un cadre RH*
Technologies du futur	Audensiel	*Audensiel applique ses technologies sur ses projets et présente un usage intéressant de la blockchain appliquée à l'IoT, avec un focus particulier sur la sécurité.*
Cybersécurité	Tenacy	*Avec sa plateforme SaaS, Tenacy s'impose comme un excellent tableau de bord pour les RSSI et a déjà séduit une centaine de clients.*

GREEN IT		
Économie Circulaire	Adista	*Adista couvre le champ le plus vaste en terme de matériel pris en charge.*
Efficacité Énergétique	Axopen	*Si tous les candidats sont à applaudir pour leurs efforts en matière de réduction de leur impact environnemental, Axopen s'est démarqué par son travail sur le Green Dev.*
Impact Local	HN Services	*Mise en avant de sujets d'actualité : la réinsertion professionnelle des personnes handicapées.*
Impact Local	Alteca	*Mise en avant de sujets d'actualité : les femmes dans les métiers du numérique.*

RH		
Formation/ Compétences	Meritis	*La démarche de Meritis est marquée par une hyper personnalisation de son offre de formation.*
Attractivité/ Rayonnement	Sqorus	*Les très nombreuses initiatives de Sqorus en faveur de ses employés rejaillissent positivement sur sa marque employeur.*

DSI

RSE		
Économie Circulaire	Rzilient	*Rzilient applique à lui-même ce qu'il fournit à ses clients, mettant en oeuvre une approche innovante de la circularisation des équipements en interne.*

INNOVATION		
Transformation Numérique	Cegid	*Le plan de transformation de Cegid a su retenir notre attention du fait son ampleur d'une part, et de l'autre, par ses résultats aussi bien côté clients qu'en interne.*
Supply Chain	Afnic	*L'Afnic a réécrit en profondeur son système de registre de sorte à améliorer le traitement des opérations sur les noms de domaines.*

RSE		
Green Infra	IRSN	*L'Institut de Radioprotection et de Sûreté Nucléaire a fait évoluer son infrastructure de sauvegarde afin de réduire de 75% les consommations inutiles, dans une approche de sobriété numérique.*

RH		
Diversité et Inclusion	Bouygues Telecom	*Ce prix salue les très nombreuses initiatives de Bouygues Telecom en matière de réduction des inégalités homme/femme et de lutte contre le sexisme.*

AXOPEN — EXPERTISE & DÉVELOPPEMENT INFORMATIQUE

Née en 2007 à Lyon, AXOPEN est aujourd'hui une équipe de 50 profils techniques, spécialisée dans le développement et la maintenance d'applications métiers sur-mesure. Développeurs, experts et chefs de projet y partagent des valeurs et convictions communes autour de l'informatique et du développement durable.

L'objectif principal d'AXOPEN : contribuer à bâtir, à l'aide de l'éco-conception, des systèmes d'information à la fois solides, performants et durables !

Partenaire de PME/ETI et grands comptes de tous secteurs d'activités (assurances, énergie, santé, industrie, *etc.*), l'ESN accompagne les DSI dans leurs différents défis techniques :

- conception de nouvelles applications internes
- création d'API
- réalisation d'audits de code et de performance
- maintenance et évolution d'applications existantes
- mise en place de démarches DevOps
- optimisation des performances
- expertise pointues sur des technologies web

La durabilité et l'évolutivité des applications sont plus que jamais des enjeux cruciaux pour les entreprises.

Dans cette optique, l'équipe AXOPEN fait le choix d'utiliser exclusivement les technologies connues et éprouvées du marché : Java/Spring Boot, C#/. NET, Angular, Azure...

La méthode d'AXOPEN réside également dans l'application de hauts standards de performances et dans une grande rigueur sur la qualité du code produit pour éco-concevoir et co-construire des solutions B2B sur mesure à forte valeur ajoutée.

SQORUS — People and Solutions that matter — DES EXPERTS MÉTIER ET TECHNIQUE AU SERVICE DE LA MODERNISATION DES FONCTIONS RH, FINANCE ET IT

SQORUS est un cabinet de conseil spécialisé dans la transformation digitale des fonctions RH, Finance et IT. Nos consultants interviennent depuis 33 ans auprès de grandes entreprises sur des projets stratégiques, à dimension internationale, autour des systèmes d'information : stratégie d'évolution, aide au choix, intégration, Business Intelligence, Data Management, support et conduite du changement mais également sur des enjeux autour du Cloud et de l'Intelligence Artificielle.

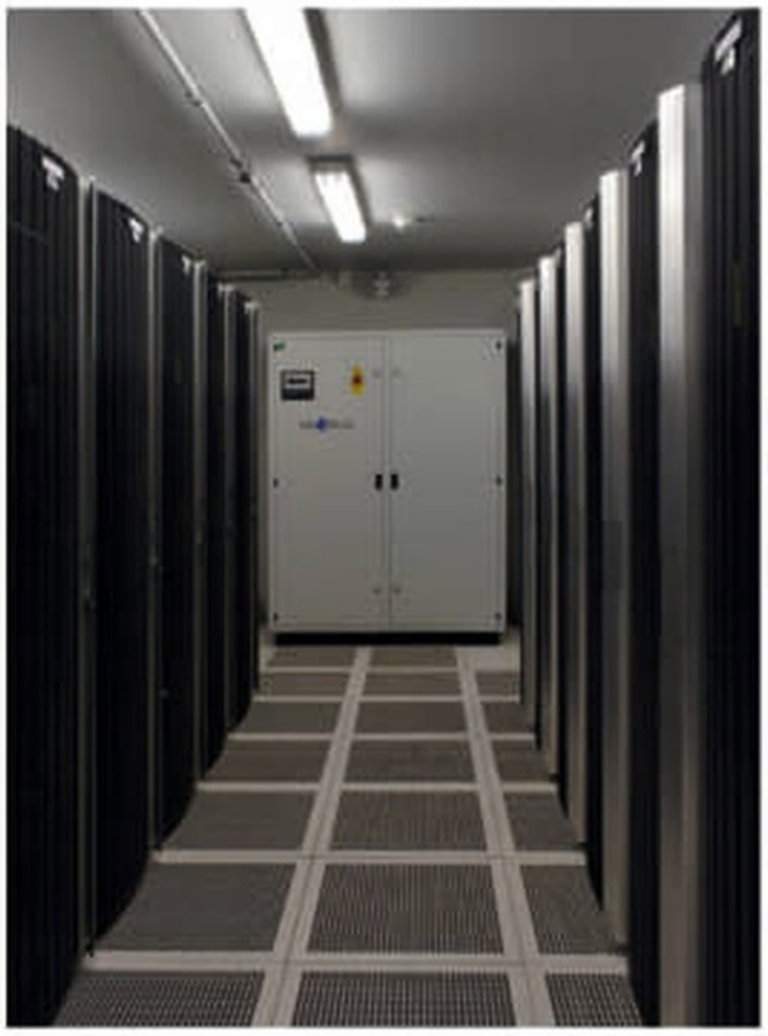
Nous avons su nous adapter aux nouveaux enjeux digitaux, à l'arrivée du Cloud, et aux évolutions des modes de travail. Nous avons réussi à tisser des partenariats forts avec les principaux éditeurs du marché et à attirer des experts métiers et techniques.

Notre force : nos 250 talents dédiés à la réussite de vos projets et partageant des valeurs fortes : la diversité, l'engagement et la solidarité, qui constituent une réelle valeur pour l'entreprise et ses clients.

Great Place to Work depuis 9 années consécutives et prix des Talents au trophée des ESN, SQORUS est sensible à l'épanouissement de ses Sqorusiens, à leur évolution de carrière et à leur formation pour imaginer ensemble les solutions du futur.

adista

Opérateur national de Services Hébergés, adista est le spécialiste des services informatiques et télécoms destinés aux entreprises et collectivités. Notre mission consiste à produire et délivrer le Système d'Information de nos clients, parfaitement adapté à leur stratégie, avec le respect prioritaire de leurs exigences de performance, d'intégrité et de sécurité.



Pour rester compétitives, les entreprises doivent s'adapter à l'évolution rapide du marché et saisir les opportunités de la transformation IT. 1er opérateur cloud et connectivité alternatif B2B, adista a développé une offre unique permettant de répondre aux besoins de services cloud, connectivité, cybersécurité, communication et collaboration. En s'appuyant sur la convergence de son métier historique d'opérateur et de ses expertises en hébergement et infogérance, adista produit, sécurise, opère, transporte le Système d'Information de ses clients, et les accompagne sur leurs enjeux numériques, de l'utilisateur final à l'application, afin qu'ils puissent se concentrer sur leur cœur de métier. adista propose une offre complète permettant de combiner le meilleur des mondes du cloud public et privé pour un SI accessible avec la même qualité et la même performance applicative qu'il se situe on premise chez le client, au sein de ses infrastructures d'hébergement ou dans un cloud public de type Microsoft Azure. Avec ses 14 Datacenters, ses 40 agences en France et ses 1100 collaborateurs, la force d'adista réside dans sa capacité à fournir des services de confiance et de proximité souverains mais aussi durables. L'entreprise est engagée de longue date dans une démarche de réduction de son empreinte carbone et emmène le SI de ses clients dans cette même trajectoire pour les aider à répondre à leurs objectifs de résilience et de sobriété.

meritis

Meritis est un cabinet de Conseil, pilotage et développement IT fondé en 2007 présent dans plusieurs grandes villes françaises : Paris, Sophia-Antipolis, Aix-en-Provence, Montpellier, Toulouse, Nantes... Et bientôt sur de nouveaux territoires ! Sa mission première est de connecter les meilleurs talents aux entreprises afin de leur donner un temps d'avance. Leurs experts accompagnent les clients dans l'intégralité de leurs besoins de transformations numériques à travers de nombreux domaines d'expertise : finance, software engineering, pilotage de projets, devops, data, cloud, cybersécurité ou encore agilité.

Fort de ses quatre valeurs portées quotidiennement par le Président Directeur Général, Sébastien Videment, d'exigence, d'humilité, de bienveillance et de proximité, le cabinet de 900 collaborateurs primé à 4 reprises en tête du palmarès Great Place To Work (n°3 en 2020, n°1 en 2017, n°7 en 2015 et n°5 en 2013) connaît une très forte croissance et projette d'atteindre 80M€ de Chiffre d'Affaires sur l'année 2023.

Actuellement, 40 % des entreprises du CAC40 sont clientes de Meritis et ses principaux clients sont : Airbus, Air France, Amundi, Axa, BNP Paribas, Crédit Agricole, La Banque Postale, Engie, Essilor, Groupama, Groupe BPCE, Médiamétrie, HSBC, Natixis, Orange, Oticon Medical, Parrot, Pierre & Vacances Center Parcs, Société Générale, Sodern, SNCF, L'Oreal, RATP, Geodis, Schneider Electric, Essilor, Veepee, EDF ou encore Valeo.

Sébastien Videment, Président Directeur Général de Meritis.

Tenacy

Tenacy a été fondée en 2019, alors que les cybermenaces étaient en plein essor et que le besoin de conformité commençait à augmenter. À cette époque, les RSSI utilisaient de très nombreux logiciels de détection et protection mais aucun pour le management de la cybersécurité.

Les RH avaient un SIRH, les commerciaux un CRM, mais les RSSI n'avaient qu'Excel. C'est pourquoi nous avons lancé la plateforme Tenacy.

Notre mission est de simplifier et d'automatiser le management de la cybersécurité pour tous les RSSI et leurs équipes. Au sein d'une plateforme SaaS tout-en-un, Tenacy aide les organisations à gérer leur cybersécurité en leur fournissant une méthodologie innovante, en rationalisant chaque opération et en garantissant la performance.

Tenacy s'impose comme un acteur majeur du management de la cybersécurité et compte aujourd'hui 40 collaborateurs, 100 clients et 2000 utilisateurs répartis dans plus de 30 pays.

En 2022, Tenacy a obtenu le label France Cybersecurity et a réalisé une levée de fonds de 2,5 millions d'euros auprès de fonds généralistes et spécialisés en cybersécurité.

Cyril Guillet, PDG et co-fondateur de Tenacy.

bouygues TELECOM

Bouygues Telecom est un opérateur global de communications qui se démarque en apportant tous les jours à ses 27,4 millions de clients le meilleur de la technologie. L'excellence de son réseau 5G, 4G qui couvre aujourd'hui 99 % de la population et ses services dans le fixe et le Cloud permettent à ses clients de profiter simplement, pleinement et où qu'ils soient, de leur vie digitale personnelle et professionnelle.
Aujourd'hui, le réseau 5G Bouygues Telecom couvre plus de 12 000 communes et plus de 7 habitants sur 10.

Depuis plus de 15 ans, Bouygues Telecom mène une politique de diversité & d'inclusion ambitieuse, basée sur l'égalité entre les femmes et les hommes, l'intégration des personnes en situation de handicap, l'inclusion des personnes LGBT+, la diversité générationnelle et socio-culturelle. Récompensée par un TopTech de la diversité et de l'Inclusion en juin 2023, l'entreprise affiche un index de l'égalité professionnelle entre les femmes et les hommes à 99/100, avec 46 % de femmes dans ses instances dirigeantes et 40 % de collaboratrices. Pour renforcer ses engagements, Bouygues Telecom a rejoint en janvier 2023 l'initiative #StOpE « Stop au Sexisme Ordinaire en Entreprise ».

Encouragées par la direction, des collaboratrices de Bouygues Telecom ont créé dès 2011 le réseau féminin « Bouygt'elles ». Les Bouygt'elles soutiennent le développement de la mixité au sein de l'entreprise, en contribuant à attirer et fidéliser des talents féminins, et en animant des actions favorisant leur épanouissement. Dans ce but, et depuis 2012, les Bouygt'elles animent Girls@Tec, un évènement dédié aux collégiennes et lycéennes, qui vise à faire découvrir de manière ludique les métiers technologiques de Bouygues Telecom et donner envie à ces jeunes filles de s'orienter vers ces métiers dans leur scolarité. La prochaine édition aura lieu le 29 novembre 2023, sur les sites Bouygues Telecom de Paris, Bordeaux et Nantes.

CYBERARK®
The Identity Security Company

Ne vous contentez pas de gérer les identités.

Sécurisez-les.

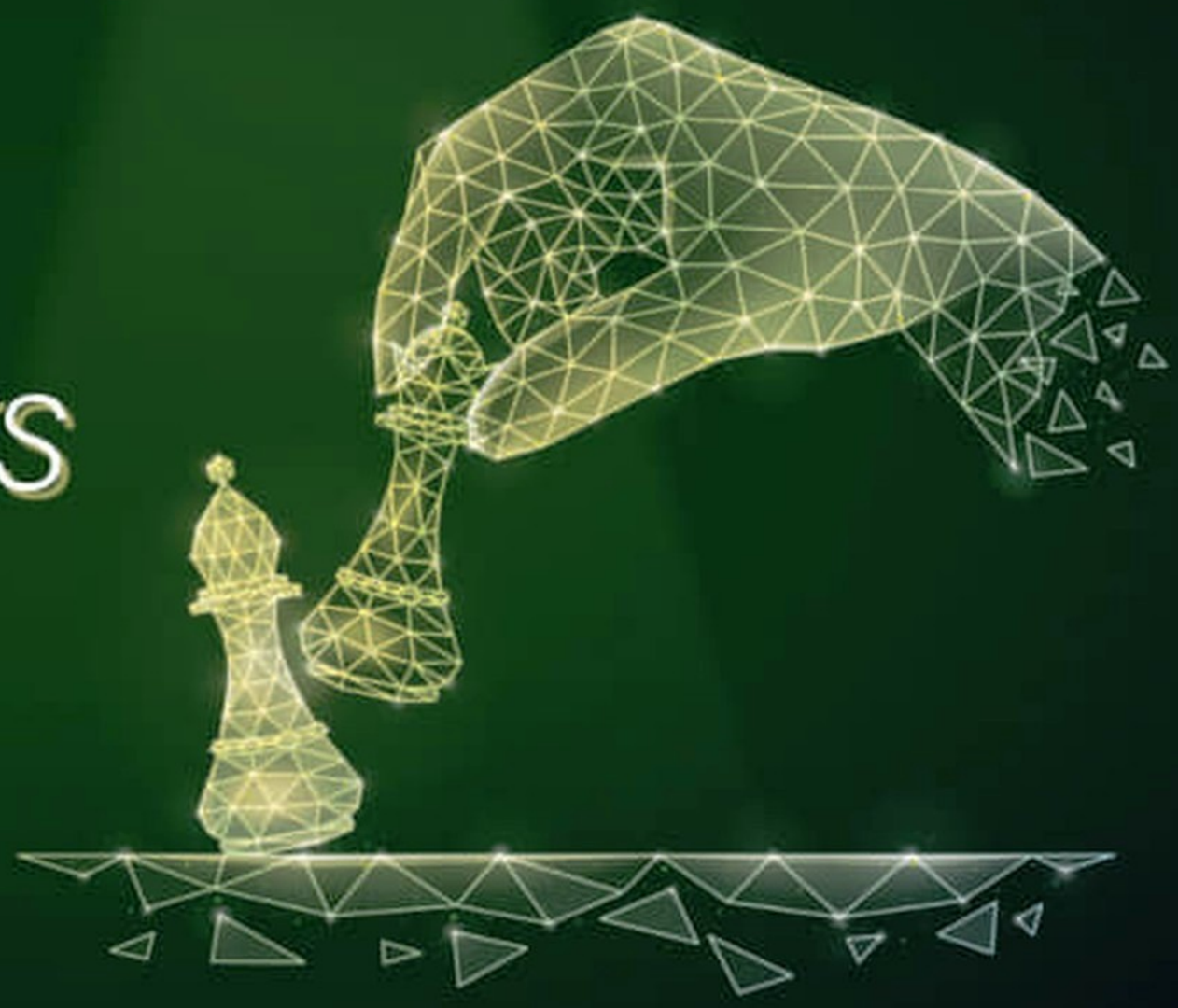
Avec CyberArk, les organisations peuvent appliquer des contrôles intelligents des privilèges à toutes les identités, humaines et non-humaines, pour une détection et prévention continues des menaces tout au long du cycle de vie de l'identité.

Chaque identité accède en toute sécurité à n'importe quelle ressource, où qu'elle se trouve et à tout moment – et cela à partir d'une seule plate-forme de sécurité des identités.

Evaluez le niveau de maturité de votre stratégie de sécurité des identités

Téléchargez notre ebook, pour accéder à la matrice et faire évoluer votre stratégie vers le niveau de maturité supérieur.

Heurs et malheurs de l'IA



par Bertrand Garé

À peine quelques jours de vacances et on n'arrive plus à suivre ce qui se passe autour de l'intelligence artificielle. Alors que le cabinet Gartner pointe la technologie de l'intelligence artificielle générative au pic de son buzz, on voit pointer les premiers signes qui annoncent le plateau de la désillusion. Une étude d'OpinionWay pour le compte d'Ekimetrics démonte que les dirigeants se montrent enthousiastes, mais peu utilisateurs de cette technologie. Une majorité des décideurs (55%) ont déjà ou vont avoir recours à l'intelligence artificielle dans leur entreprise. Dans le détail, 41% utilisent déjà cette technologie et 14% envisagent de le faire à brève échéance. Parmi les secteurs d'activité qui ont déjà recours à l'IA, le commerce figure en tête (46%), devant les services (38%) et l'industrie/BTP (37%). Néanmoins, on constate des disparités dans la mise en œuvre effective de l'IA en fonction de la taille de l'entreprise : si 43% des entreprises de plus de 500 salariés utilisent l'IA, seules 29% des entreprises de moins de 500 salariés le font également. Interrogés sur les avantages procurés par l'utilisation de l'IA en entreprise, les dirigeants qui l'intègrent déjà (soit 41% de l'échantillon) voient cette technologie comme un levier de performance opérationnelle (93%), de performance économique (85%) et un moyen d'enrichir l'expérience client grâce à de nouveaux services personnalisés (81%). Lorsque l'on donne la parole aux dirigeants qui n'utilisent pas l'intelligence artificielle pour le moment (soit 59% de l'échantillon), ces derniers justifient principalement leur refus par une inadéquation de la technologie avec les enjeux de leur entreprise (64%), un manque de compétences en interne (46%) et une absence de consensus au sein de l'équipe de direction quant à son utilisation (24%). Toutefois, fait intéressant, cette distance avec l'IA ne traduit pas une défiance vis-à-vis de cette technologie. En effet, seuls 18% ne croient pas que l'intelligence artificielle puisse avoir un impact business significatif à court terme. À noter toutefois que 7% des patrons qui n'utilisent pas l'IA ont été échaudés par leurs échecs — un taux qui atteint 11% pour les dirigeants d'entreprises de 250 à 499 salariés.

ChatGPT est loin d'être entré dans le quotidien des dirigeants français. Cette innovation reste nébuleuse pour l'écrasante majorité d'entre eux : 76% n'ont pas d'avis sur le sujet pour le moment. Quant aux autres, ils sont 6% à considérer que l'IA générative va permettre d'augmenter leurs gains de productivité, et 4% à juger qu'elle permettra d'accélérer la montée en compétences des collaborateurs. Seuls 6% des dirigeants utilisent cette forme d'IA générative et 9% envisagent de le faire dans les prochains mois. Quant aux 83% qui n'envisagent pas d'utiliser ChatGPT, trois raisons principales pourraient les amener à changer d'avis : disposer de davantage d'informations sur son fonctionnement (20%), recevoir des garanties sur la protection de leurs données personnelles (14%) et avoir des garanties sur le potentiel de ChatGPT à améliorer la performance économique de leur entreprise (10%).

Pourtant, une étude pour Slack du même institut de sondage, 71% des cols blancs et 62% des cols bleus sont convaincus que l'IA représente une avancée majeure pour la société. L'intelligence artificielle ferait gagner 6 h par semaine, en moyenne, aux travailleurs du savoir et 5 h aux travailleurs de première ligne. Un gain non négligeable lorsque l'on sait que 65% des tâches à faible valeur ajoutée pourraient être réalisées par l'IA. Encore faudrait-il que la notion de tâches à valeur ajoutée soit clairement définie. La majorité des travailleurs du savoir préfèrent en majorité (50%) que leur outil d'intelligence artificielle se trouve directement intégré à leurs outils de travail ; comme les plateformes collaboratives. L'intelligence artificielle est pour les collaborateurs un réel levier de

productivité : 63 % des cols blancs et 48 % des cols bleus déclarent être plus efficaces et 73 % des cols blancs et 64 % des cols bleus disent gagner du temps. Bon, à la vue de ces chiffres, soit l'intelligence artificielle générative est déjà largement implantée dans les entreprises au plus près du terrain, soit les chiffres peuvent prêter à caution.

Un FUD (Fear, Uncertainty, Doubt) sur la technologie

Outre ce faible enthousiasme au plus haut niveau des entreprises, voilà que des doutes se lèvent sur la pérennité d'OpenAI, la société créatrice de ChatGPT. On découvre que la société dépense 700 000 $ par jour pour faire tourner les machines afin d'entraîner et servir ses clients par son API. Bon aller, ce chiffre qui semble astronomique ne suffit pas à peser sur l'avenir de la société. Rien qu'avec l'investissement de 10Mds de dollars de Microsoft, je pose dix milliards et je divise par 700 000 et il reste encore à un datacenter près 14 700 jours à OpenAI avant de finir en faillite ou racheter par des bienfaiteurs de la technologie. L'investissement de Microsoft n'est pas la seule source de revenu d'OpenAI. Plus inquiétant pour le créateur de ChatGPT, OpenAI n'est plus seul sur le créneau et les modèles open source montent en puissance comme LLama 2 ou d'autres modèles. Le nombre d'utilisateurs baissent (-12 %) et selon les derniers chiffres et l'entreprise creuse ses pertes (540 M$). Les entreprises se tournent vers des modèles pré-entraînés gratuits et souvent interdisent à leurs salariés d'utiliser l'API d'OpenAI. Alors, beaucoup de bruit pour rien ou une fantastique innovation qui va retourner dans les limbes. On a souvent tort d'avoir raison trop tôt. Bon, le but d'OpenAI était de démocratiser l'intelligence artificielle. Sur ce point, l'entreprise a touché son but. Difficile de croire donc que ChatGPT disparaisse sans autre forme de procès du paysage alors que la plupart des logiciels vont se doter d'une technologie similaire dans les 24 mois à venir.

Des interrogations sur les conséquences de l'utilisation par de mauvaises mains

Mandiant, une société spécialisée dans la sécurité informatique, vient de livrer une étude sur les différentes exploitations de cette technologie que ce soit par des images, des textes ou des séquences audio. Mandiant met aussi en avant les risques de développement de code malveillant par des commandes sur des forums clandestins liés au contournement des restrictions sur les LLM qui sont conçues pour empêcher que les LLM soient utilisés pour le développement et la propagation de logiciels malveillants, ainsi que pour la génération de matériel de leurre. Mandiant prévoit que les acteurs de la menace, d'origines et de motivations diverses, exploiteront de plus en plus l'IA générative au fur et à mesure que la prise de conscience et les capacités entourant ces technologies se développeront. Par exemple, nous pensons que les acteurs malveillants continueront à capitaliser sur l'incapacité du grand public à faire la différence entre ce qui est authentique et ce qui est contrefait, et que les utilisateurs comme les entreprises devraient être prudents quant aux informations qu'ils ingèrent, car l'IA générative a conduit à une réalité plus malléable. Vous avez dit vérité alternative ? On en est pas loin alors que Google souhaite mettre en place une solution basée sur l'intelligence artificielle générative pour résumer les articles trop longs. Bon, si vous trouvez ce texte trop long, demandez un résumé à Google. Comment on définit un article trop long ? Allô Google, peut-on avoir une précision ? Et comment Google va assurer que son résumé est sans biais ou autres détournements de sens de ce qui a été réellement dit dans l'article ? Lire doit être une tâche à faible valeur ajoutée, alors des résumés suffiront ! □

AVANT, LA **DATA** N'ÉTAIT JAMAIS ASSOCIÉE À « **STYLÉ** ».

MAIS ÇA, C'ÉTAIT AVANT

LE PALMARÈS DE L'INFORMATICIEN.

2022

PALMARÈS
L'INFORMATICIEN

Qlik France est lauréat dans la **catégorie Business Intelligence** grâce au vote des utilisateurs et à l'accompagnement de nos partenaires. Merci à tous de votre confiance !

Qlik.com

Qlik
TO BE CERTAIN.

Framery Contact

Une capsule acoustique pour passer des appels vidéo 3D

À l'heure de la transformation post-Covid, les besoins en systèmes de visioconférence ont explosé. Spécialisée dans la conception de cabines de bureau acoustiques, l'entreprise finlandaise Framery vient de lancer un nouveau modèle intégrant une solution d'appel vidéo 3D révolutionnaire capable de simuler une présence holographique des interlocuteurs.

Plus de 50 % des personnes qui travaillent dans les open space auraient du mal à se concentrer. C'est pour répondre à cette problématique que Samu Hällfors, le fondateur et actuel PDG de Framery, a créé son entreprise en 2010. Son objectif était de concevoir un espace de bureau privé et confidentiel qui permettrait aux collaborateurs d'open space de s'isoler pour discuter ou passer des appels dans le calme et la sérénité sans déranger leur entourage. La cabine acoustique Framery est née...

Capsules bureautiques de communication

Après plusieurs modèles, le concept fait mouche. À la fois design, confortables, parfaitement insonorisées, et connectées pour les plus récentes, les cabines Framery ont été adoptées par de nombreuses entreprises à travers le monde, dont Microsoft, Tesla, Nvidia, Deloitte, LinkedIn, *etc.* Outre les appels en visioconférence, elles peuvent également servir pour des réunions ou des entretiens importants. Grâce à l'insonorisation de 29 dB, les capsules prévues pour 2, 4 ou 6 personnes selon les modèles, préservent parfaitement la confidentialité des échanges. Même si elle est placée à proximité de postes de travail au milieu par exemple d'un open space, il est impossible d'entendre ce qu'il se dit à l'intérieur. Chaque modèle dispose d'un système de ventilation et d'un éclairage LED automatisé. Un panneau de contrôle tactile intégré permet d'ajuster le débit d'air ou l'intensité de la lumière. En 2021, l'entreprise a lancé son premier modèle de cabine acoustique connecté Framery One. Équipée du système de gestion numérique Framery Connect, elle peut être connectée par exemple au calendrier de l'entreprise pour que les collaborateurs puissent réserver la cabine. Une alerte s'affiche automatiquement sur l'écran lorsqu'elle doit être libérée. Entièrement modulables, les cabines Framery peuvent être personnalisées avec différents kits de meubles, ainsi que différents accessoires comme des prises de courant, des ports USB et RJ45. Entreprise finlandaise oblige, toutes les cabines de Framery sont construites à partir de

Samu Hällfors,
CEO de Framery.

« Framery Contact utilise une combinaison de technologies avancées et analogiques pour reproduire la véritable expérience d'une réunion en face à face. »

matériaux durables et recyclables à 95 % ! Malgré son succès sur le marché en plein essor de la visioconférence, l'entreprise finlandaise a voulu aller encore plus loin en repoussant les limites des systèmes d'appels vidéo traditionnels.

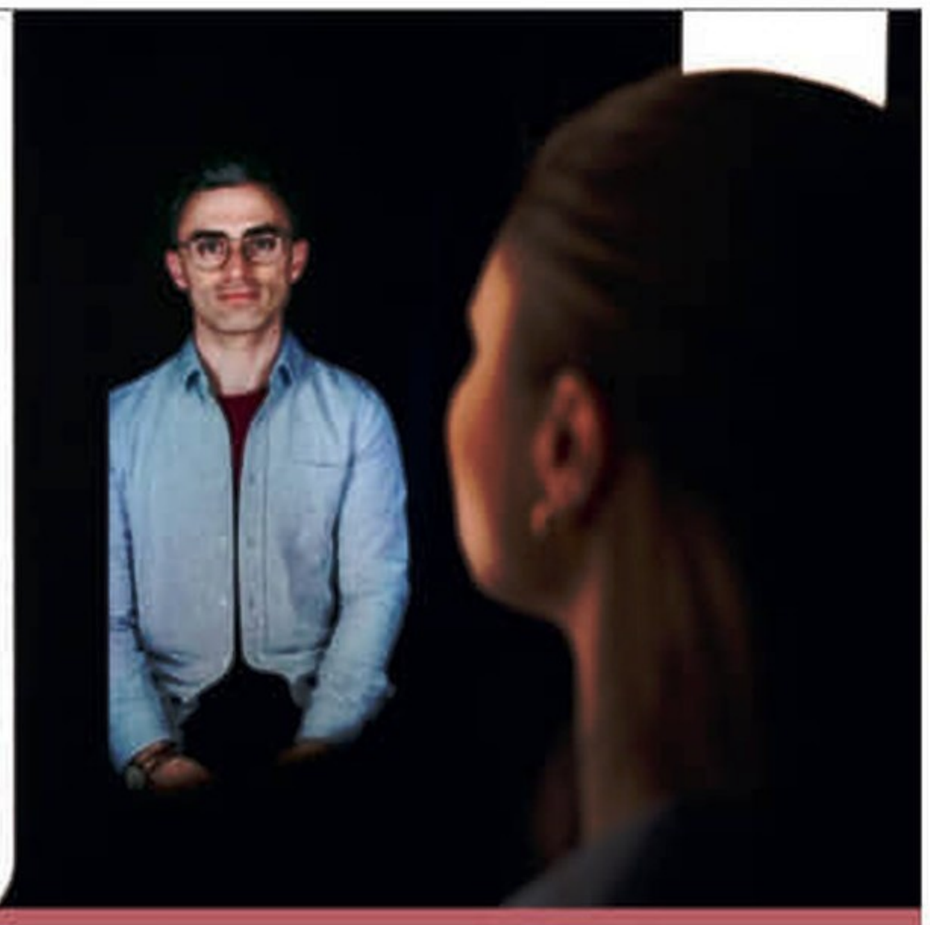
La visioconférence 3.0

Particulièrement innovante, sa dernière cabine Framery Contact propose une nouvelle technologie d'appels vidéo en 3D. La société dit vouloir améliorer les interactions du travail hybride qui promet de s'installer durablement dans le monde professionnel. Pour cela, elle a créé ce qu'elle appelle un module de réunion virtuelle permettant de simuler des conversations en face à face de collaborateurs pouvant se trouver à des milliers de kilomètres de distance. Capable d'accueillir jusqu'à 4 personnes, Framery Contact prend la forme d'une capsule isolée, aussi bien visuellement qu'acoustiquement. Avec un design digne d'une petite navette spatiale, elle peut se fondre harmonieusement dans n'importe quel open space. Framery Contact utilise une combinaison de technologies avancées et analogiques pour reproduire une véritable expérience de réunion en face à face. Concrètement, la société a combiné des technologies de projection tridimensionnelles avec des miroirs placés stratégiquement dans la cabine afin que les participants aient l'impression de se trouver dans le même espace. Outre l'isolation acoustique de haute volée connue et reconnue des cabines Framery, la société a voulu également parfaire l'expérience sonore. Le son de Framery Contact a été optimisé à l'aide d'un microphone cardioïde de haute performance ainsi qu'un moniteur audio actif capable de retransmettre la voix humaine avec une plus grande précision.

Une expérience inédite

L'objectif de Framery étant là encore d'offrir un niveau d'intimité proche, voire identique à celui qu'auraient des collaborateurs en présentiel. Des lumières LED ont été spécifiquement optimisées pour éclairer et mettre en valeur l'utilisateur sans l'éblouir. *« En cette période postpandémie, les interactions virtuelles se sont plus que démocratisées, avec 80 % à 98 % de toutes les réunions comportant au moins un utilisateur en visioconférence »* explique Samu Hällfors, CEO de Framery. *« Bien que pratiques, les plateformes d'appels vidéo présentent de nombreux défis et limites. Tous ceux ayant déjà vécu une réunion ont une compréhension aiguë de ces dernières. Au niveau le plus élémentaire, les caméras rendant parfois une qualité médiocre et le décalage audio signifient que les appels vidéo traditionnels dissipent des indices subtils et non verbaux tels que le contact visuel, le regard direct et le langage corporel, limitant ainsi la génération des idées. Framery Contact utilise une combinaison de technologies avancées et analogiques pour reproduire la véritable expérience d'une réunion en face à face. »* La date de commercialisation n'a pas encore été dévoilée, mais des modules de démonstration ont été livrés à certains clients pilotes. L'entreprise finlandaise nous a toutefois communiqué son prix qui débutera à partir de 23 000 € par unité. ☐

J.C



CARACTÉRISTIQUES TECHNIQUES
FRAMERY CONTACT

- **Nombre de places :** 4
- **Acoustique (réduction du niveau de parole) :** 29 dB /certification ISO-23351-1
- **Détecteurs de mouvement** (lumière et ventilation)
- **Éclairage LED :** 4000 K et 300 Lux
- **Ventilation réglable**
- **Connectique :** 2 x prises de courant, 2 x USB A+C, 2 ports LAN (en option)
- **Meubles :** 3 dispositions de meubles différentes (sièges, tables et écrans)
- **Dimensions extérieures (H x L x P) :** 222 cm x 220 cm x 120 cm
- **Poids :** 630 kg (sans meuble)
- **Prix :** à partir de 23 000 €

Tablette

Getac ZX70 prêt à toute épreuve !

Conçue pour les professionnels mobiles, la Getac ZX70 est une tablette Android durcie aux qualités et performances hors normes. Capable de fonctionner dans les environnements et les conditions les plus difficiles, elle répond aux besoins sur le terrain de nombreux corps de métiers.

Utiliser une tablette classique dans certains environnements est tout bonnement impossible. Avec la ZX70, Getac a créé un modèle capable de résister aux conditions environnementales les plus extrêmes. Certifié IP66 et MIL-STD 810H, le terminal ne craint ni la pluie, ni les jets d'eau à très haute pression, ni la poussière ou le sable. L'appareil peut être submergé jusqu'à 30 minutes dans 1 mètre d'eau. Ce n'est pas tout, il peut résister à de violentes chutes de plus de 1,8 mètre et fonctionner dans des températures extrêmes comprises entre -29 °C et 63 °C ! Que cela soit dans le secteur de la défense, de la sécurité, du service public, du transport, ou encore des industries de l'automobile, du pétrole ou du gaz, cette robustesse constitue un facteur clé pour bon nombre de professionnels. Le constructeur commercialise également une version ATEX certifiée pour les endroits dangereux potentiellement explosifs.

Une configuration musclée

Relativement fine et légère pour une tablette durcie (1,04 kg), elle embarque un large écran LCD de 10,1 pouces (1920 x 1200 pixels) utilisable avec les doigts, un stylet intégré, ou même des gants. Grâce à la technologie LumiBlond 2.0 de Getac, l'écran demeure parfaitement lisible dans n'importe quelles conditions lumineuses. Sa configuration se compose pour l'essentiel d'une puce Qualcomm Snapdragon 660 (8 cœurs), de 4 Go de mémoire vive, et d'un stockage eMMC de 64 Go. La Getac ZX70 fait également la part belle à la communication avec des interfaces Wi-Fi AC, le Bluetooth 5.0, une double Micro SIM LTE, ou encore un module GPS dédié. Outre un appareil photo arrière de 16 Mpx avec mise au point automatique et une Webcam frontale de 8 Mpx pour les appels vidéo, l'appareil offre une généreuse connectique comprenant une sortie casque et une entrée micro, un port Micro SD, des ports USB 3 et Type C, ou encore un connecteur pour station d'accueil. On regrette en revanche l'adapteur secteur propriétaire imposant qui ne facilite pas les choses au quotidien pour recharger l'appareil. On note l'absence assez étonnante pour une tablette professionnelle d'un lecteur d'empreinte digitale.

Autonomie et accessoires

À l'usage, l'un des gros points forts de la tablette réside dans son autonomie permettant de tenir toute une journée de travail sans avoir à la recharger. Elle peut même être utilisée plus longtemps *via* des batteries de plus haute capacité échangeable à chaud (en option). De quoi tenir non pas une, mais deux à trois journées de travail. Tablette professionnelle oblige, Getac commercialise un certain nombre d'équipements en option en fonction des besoins : combo lecteurs NFC + RFID HF i, lecteur de codes-barres, passage d'antenne RF pour GPS (WLAN et WWAN), lecteur de cartes à puce, diverses stations d'accueil (bureau, véhicule...), *etc.* Sans oublier une panoplie d'accessoires pour transporter la tablette : bandoulière, harnais d'épaule, sacoche, sangles, poignée rigide, *etc.*

Un environnement logiciel optimisé pour les entreprises

Véritable poste de travail mobile, la ZX70 repose sur Android Enterprise Recommended (AER). Pour rappel, ce système d'exploitation mobile de Google a pour but d'aider les entreprises à déployer et à gérer des appareils Android. Les terminaux AER sont certifiés par Google pour répondre aux exigences des entreprises en matière de sécurité, de gestion et de performances. L'appareil embarque évidemment tous les

La tablette durcie Getac ZX70 offre un large éventail de possibilités et d'options afin de pouvoir répondre aux différents besoins opérationnels des industriels des secteurs de la défense, de l'énergie, du transport, de l'automobile, de la production, etc.

services qui font le succès d'Android (Google Recherche, Chrome, Gmail, Maps, YouTube, Play, Drive, Play Musique, Play Films, Duo, Photos...), ainsi que des logiciels préinstallés développés par Getac tels que File Browser, Input Method, ou encore Camera. Avec l'application OEMConfig (Microsoft) ou Getac deployXpress Cloud (en option), les administrateurs informatiques peuvent facilement déployer et gérer une flotte ZX10 grâce notamment à la configuration par lots des paramètres de l'appareil et du système. Il est possible par exemple de gérer les paramètres de la batterie, de l'affichage, de la navigation, de la numérisation, du panneau de paramètres rapides, de la date et de l'heure, ou même de ses quatre boutons d'accès rapide programmables (situés sur le bord de l'écran). L'interface familière d'Android et ses millions d'applications disponibles constituent des avantages indéniables. Quelques minutes suffisent pour prendre en main la tablette et commencer à l'utiliser.

CARACTÉRISTIQUES GETAC ZX70

- **Système d'exploitation : Android 12.0**
- **Processeur : Qualcomm Snapdragon 660 (8 cœurs)**
- **Mémoire vive : 4 Go LPDDR4**
- **Stockage : eMMC 64Go**
- **Ecran : TFT LCD WUXGA de 10,1 » (1920 x 1200)**
- **Connectique : 1 x USB 3.2, 1 X USB 2.0 (hôte), 1 x USB-C, 1 sortie casque, 1 entrée micro, 1 connecteur station d'accueil**
- **Interface de communication : Wi-Fi 802.11 AC, Bluetooth 5.0, double Micro SIM, GPS dédié**
- **Dimensions (L x P x H) : 275 x 192 x 17,5 mm**
- **Poids : 1,04 kg**
- **Prix : à partir de 1 229 €**

Une offre alléchante

La Getac ZX70 constitue une excellente tablette robuste. Hormis l'absence regrettable d'un adaptateur secteur USB-C de série et d'un lecteur d'empreinte digitale, elle tient toutes ses promesses en termes de puissance, d'autonomie et de fonctionnalités. Le constructeur ne laisse en outre rien au hasard en proposant un large éventail d'accessoires et d'applications en option afin de pouvoir répondre à tous les besoins spécifiques des professionnels mobiles. Ultra polyvalente, endurante, moins chère que les modèles Panasonic Toughpad concurrents, et garantie 3 ans, la ZX70 possède indéniablement de nombreux arguments à faire valoir aux responsables informatiques. □ **J.C**

Stockage

NetApp délivre une stratégie claire

Courant juillet, Sandeep Singh, Director of Product engineering chez NetApp, était à Paris. Une occasion pour *L'Informaticien* de discuter de la stratégie produit du fournisseur de solutions de stockage.

Pour Sandeep Singh, en charge de l'ensemble des lignes de produits chez NetApp, les entreprises sont confrontées à différents problèmes comme la gestion de la complexité des environnements multicloud et leur capacité à protéger leurs données. Pour y parvenir, NetApp développe une stratégie qui repose sur trois piliers : fournir les meilleurs produits de stockage sur site, des services de stockage dans le Cloud et des services de gestion des données. Ces derniers ont pour but d'apporter une plus grande efficacité, le respect de la conformité et la gouvernance des données.

Sandeep Singh, Director of Product engineering chez NetApp.

Gérer l'hybride

Les entreprises utilisent déjà différents clouds dont elles doivent conserver les données pour leur activité ou respecter les règles de conformité. NetApp propose de le prendre en charge en apportant la possibilité de stocker en bloc, fichier et objet par une approche unifiée. L'éditeur propose, de plus, une approche hybride pour ses modèles avec, bien sûr, des baies Flash, mais contrairement à Pure Storage, il propose aussi ces baies avec des disques classiques pour conserver l'avantage économique de ce type de disque par un « tiering » des données. C'est là qu'entrent en jeu les services logiciels avec une simplification de ce placement de données pour donner une plus grande flexibilité tout au long du cycle de vie des données. L'idée finale est cependant d'apporter ces services à l'échelle pour les environnements hybrides par des fonctions d'automatisation et une couche de gestion.

La consistance entre les environnements sur site et le Cloud se réalise d'abord par l'utilisation du même système d'exploitation, OnTap, dans tous les environnements et un point central d'administration avec Blue XP qui fournit des services d'observabilité et de gouvernance des données. Toutes ces opérations se réalisent au niveau des données ou des métadonnées selon le cas. Des services d'analyse apportent la possibilité de prévoir les besoins avec des outils d'AIOps.

Aider les entreprises dans leur politique durable

NetApp n'oublie pas cette nouvelle priorité des entreprises concernant leur niveau d'émission de carbone et apporte avec l'utilisation des baies flash une baisse de consommation électrique de 70 % aux utilisateurs, alors que ceux-ci rallongent le cycle de vie des matériels pour des périodes de 7 à 10 ans. □

B.G

NETAPP OFFRE UNE **GARANTIE DE RÉTABLISSEMENT** APRÈS UN RANSOMWARE

La garantie de récupération ransomware NetApp tire parti de la combinaison exclusive de NetApp ONTAP de fonctions de sécurité intégrées et de protection contre les ransomwares. ONTAP peut bloquer automatiquement les types de fichiers malveillants connus, bloquer les administrateurs indésirables et les utilisateurs malveillants grâce à la vérification multi-administrateurs et fournir des snapshots inviolables qui ne peuvent pas être supprimés, même par l'administrateur de stockage. NetApp garantit désormais la récupération instantanée de données en cas d'attaque ransomware. Si les copies de données ne peuvent pas être récupérées avec l'aide de NetApp ou de l'assistance d'un partenaire, NetApp offrira une compensation. Le montant de celle-ci n'a pas été précisé et se met en place en fonction de certaines conditions.

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

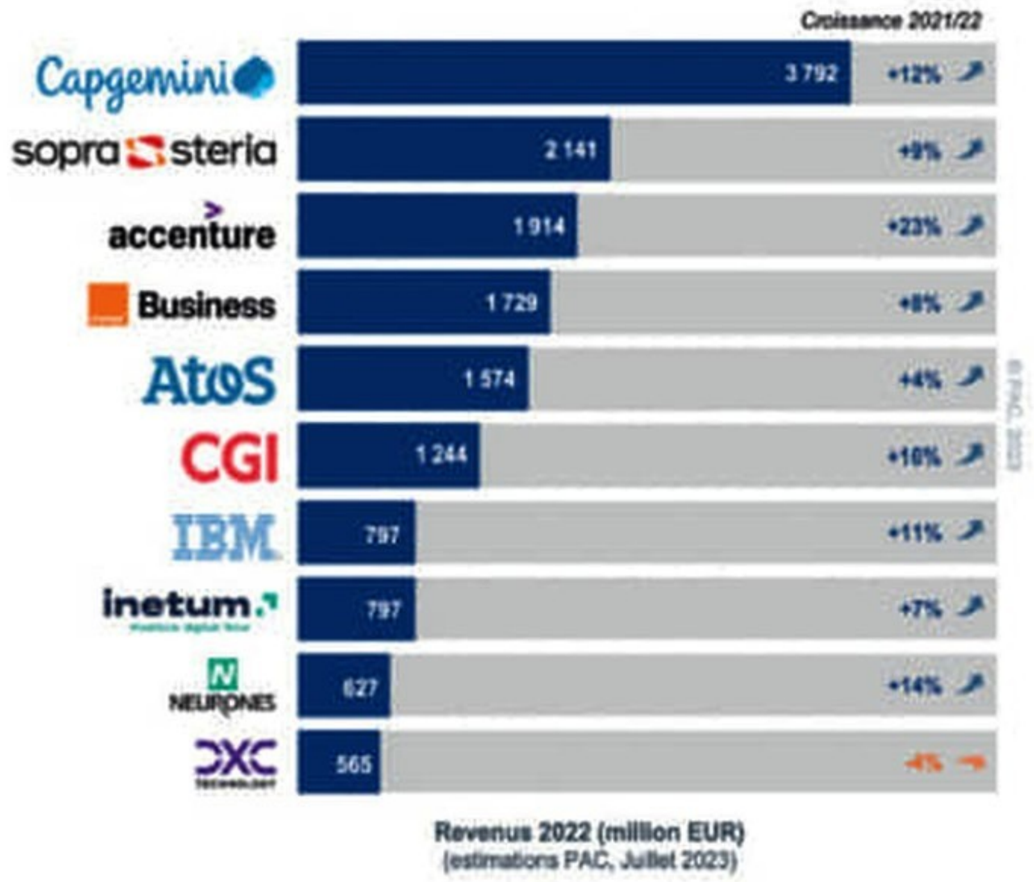
Kensington®

The Professionals' Choice™

Les ESN se portent bien

PAC vient de sortir ses estimations du marché des ESN pour 2022 qui démontrent une belle vitalité du secteur. Dans le classement des principaux acteurs, le rapport révèle peu de surprises.

Selon le cabinet d'analyses, les 10 premières ESN ont connu une belle année 2022 avec une croissance de plus de 10 % (10,9 %) bien au-dessus de la croissance du marché IT qui s'étalonne à 6,6 %. Capgemini conserve sa première place de loin devant Sopra Steria qui a vu un bon cru 2022. La stratégie de grands comptes de Sopra Steria est très efficace depuis de nombreuses années et continue de porter ses fruits avec des clients très fidèles qui renouvellent régulièrement leur confiance sur des contrats clés mais permettent aussi à l'ESN d'étendre son positionnement à travers de nouveaux domaines clés de l'évolution numérique (cloud, data, cyber, *etc.*). Accenture a connu une année exceptionnelle avec une croissance en Europe de 29 %. Cette dynamique a été portée par les activités réalisées avec les hyperscalers mais aussi Salesforce, Service Now, Adobe ou SAP entre autres. Enfin, en France Accenture a fait de la croissance externe avec l'acquisition de Linkbynet en juillet 2021 (ce qui a ajouté 100M€ de revenus en 2022) et a aussi finalisé l'acquisition de AFD. Tech en avril 2022. Derrière ce podium, suivent Orange Business, Atos, IBM, Inetum, Neurones qui apparaît pour la première fois dans le top 10. DXC ferme la marche de ce classement. Seul point noir qui devrait, hélas, perdurer, le manque de ressources humaines qui devraient freiner le marché lors de la seconde moitié de cette année. □



Si les plus grosses ESN connaissent une forte croissance, c'est aussi le cas des ESN plus spécialisées comme HRC, à la fois éditeur et intégrateur autour des solutions de logistiques de SAP, qui connaît une croissance de 50 % de son chiffre d'affaires. L'entreprise envisage une vingtaine de recrutements pour répondre à la demande dans son carnet de commandes. L'entreprise est en bonne voie pour atteindre ses objectifs stratégiques avant près d'un an d'avance. ADP, Sanofi, Panzani et JCDecaux sont des clients de l'entreprise.

LA BONNE SANTÉ DES ESN

Open up

Smile poursuit sur sa lancée

L'ESN passe d'Open Arrow à Open Up. Cette stratégie à l'horizon 2026 doit accompagner la croissance de Smile, à travers le renforcement de l'ADN du groupe, un accent mis sur le numérique responsable et le développement de ses branches internationales.

Depuis quelques années, Smile creuse son sillon dans le monde du service numérique. Et ce, sous l'égide de sa stratégie Open Arrow. *« Ce plan-là était assez ambitieux, lancé au moment où l'actionnariat a changé, en 2017 »*, se rappelle Marc Palazon président et CEO de l'ESN. À l'époque, le fonds Eurazeo entrait au capital de Smile. Parmi les axes de transformation de l'entreprise, le développement international figurait en bonne place, suivi de près par le renforcement de l'activité de conseil de la société, une direction poussée par ses clients. La croissance est à la fois organique et externe : Smile double son chiffre d'affaires et opère de nombreuses acquisitions, aussi bien pour s'étendre en Europe avec des rachats en Suisse et en Allemagne que pour amplifier certaines activités et technologies, à l'instar de l'acquisition du spécialiste Symfony SensioLabs en 2019 ou d'Alter Way en 2021. Le groupe est désormais implanté dans 9 pays, de la Belgique à l'Ukraine en passant par la Pologne ou encore le Maroc.

Marc Palazon, président et CEO de Smile.

« On a voulu, dans le cadre de notre projet sur les trois ou quatre prochaines années, un nouveau plan, sans dénaturer le projet Open Arrow. »

« On a voulu, dans le cadre de notre projet sur les trois ou quatre prochaines années, un nouveau plan, sans dénaturer le projet Open Arrow, une continuité avec des nouveautés » nous explique Marc Palazon. Cette nouvelle stratégie, c'est Open Up. Premier pilier du nouveau plan, l'ADN du groupe. Car, à force de rachats, l'ESN compte quelque 2000 salariés et six marques, outre Smile. Il s'agit donc d'exister *« en étant un groupe soudé »*, fédérer sans diluer l'ensemble de ses marques et de ses équipes dans un collectif, un projet commun, et faire travailler ensemble toutes les composantes du groupe. Cette notion baptisée One Smile se traduit notamment en termes organisationnels, avec par exemple la mise en place d'une DRH au niveau du groupe.

Du côté de ses activités, Smile ne prévoit pas de grandes manœuvres : il poursuit sa quête de nouvelles technologies et de solutions alternatives, vocation open source oblige, pour ses clients et le renforcement de sa partie infrastructure, lancée dans le milieu des années 2000, donc tardivement, mais sérieusement boostée par le rachat d'Alter Way. Notons toutefois que l'ESN s'intéresse à d'autres axes technologiques, autour de la data notamment : une « business unit » dédiée à l'IA et aux LLM devrait ainsi prochainement voir le jour. La politique de recrutement ne devrait pas connaître de brutale accélération, avec environ 600 recrutements prévus en 2024, quoique la société *« travaille activement à augmenter la part de féminin dans l'entreprise »*.

Surtout, la première priorité de la société, qui célèbre cette année ses 32 ans, est Le Numérique responsable. *« Entre Open Arrow et Open Up, le RSE est vraiment un sujet sur lequel nous voulons nous positionner. Eurazeo est très engagé dans cette démarche, tout comme Alter Way, très présent sur le numérique responsable »* indique le PDG de l'ESN. En interne, la société entend déployer une politique RSE *« concrète et mesurable »*, avec l'obtention par un millier de salariés de qualifications et de certifications numérique responsable. Côté clients, Smile prévoit de lancer une offre de conseil auprès des DSI pour les accompagner dans leurs réflexions afin d'être les plus responsables possible, avec un focus sur le Green IT, l'inclusion et la sécurité. En outre, l'entreprise veut être *« imprégnée »* de cette manière responsable de faire du numérique chez ses clients, pour la partie intégration.

Enfin, à l'international, sur les trois prochaines années, la tendance est *« plutôt à vouloir renforcer les endroits où l'on est, sauf opportunité exceptionnelle, d'ouvrir dans une nouvelle région »* précise Marc Palazon. Avec quelques objectifs chiffrés : depuis 2017, la part de l'international au chiffre d'affaires de Smile a grimpé de 5 à 20 % : Open Up vise 30 % à l'horizon 2026. De même, *« nous voulons que, au-delà du business, notre effectif atteigne 50 % à l'international [aujourd'hui entre 35 et 40 %] sur les trois prochaines années »*. □

G.P

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

Conf23

Splunk se tourne vers l'IA et l'OT

Le spécialiste de l'observabilité et de la sécurité tenait sa conférence du 17 au 20 juillet dernier à Las Vegas. Le principal thème de l'événement a été la résilience du système d'information. Pour aider les entreprises dans cette vaste tâche, Splunk ajoute de l'intelligence artificielle et une visibilité de bout en bout avec des nouveautés pour le « Edge ».

Pour Gary Steele, le CEO de Splunk, la résilience est le principal problème des entreprises et chaque arrêt des systèmes ou chaque brèche coûte beaucoup d'argent. Selon lui, le coût moyen d'une attaque est de 9,44 M$ et chaque arrêt ou panne obère les finances de 365 K$ par heure. Pour régler la question, la visibilité est donc un élément primordial. Et la réponse de Splunk est d'apporter cette résilience du numérique par une visibilité complète dans les environnements multiclouds par une sécurité unifiée et de l'observabilité dopée à l'intelligence artificielle. Pour le multicloud, l'éditeur met en avant ces différents partenariats avec les principaux acteurs du Cloud public, en particulier celui avec Microsoft Azure qui vient d'être étendu à la zone européenne après son déploiement sur la zone américaine. Les logiciels de Splunk peuvent être achetés et déployés depuis la boutique applicative de Microsoft pour devenir un service natif sur Azure. Ce service a été développé de concert avec Microsoft. De plus, par l'unification des données issues des outils d'observabilité et de celles provenant des outils de sécurité, l'éditeur vise à parfaire la résilience tout en étant dans un environnement consistant et unifié. Les analyses et le contenu sont persistants par ce partage des données. De plus, il est possible d'y déverser les propres modèles de l'entreprise et non d'utiliser seulement ceux de Splunk. Avec Edge Hub et son Edge processor, les fonctions de visibilité s'étendent désormais jusqu'en périphérie du réseau afin de remonter différentes informations.

Les principales annonces produits

L'ajout de Splunk Attack Analyzer (anciennement Twinwave) à cette expérience unifiée inaugure une nouvelle approche permettant aux équipes de sécurité d'automatiser l'analyse

Gary Steele lors de son keynote d'ouverture.

La présentation d'Edge Hub.

des attaques de phishing et par malware afin de mettre au jour des techniques d'attaque complexes utilisées pour échapper à la détection. Grâce à une intégration avec Splunk SOAR, Splunk Attack Analyzer permet aux analystes de sécurité d'automatiser l'investigation des menaces afin d'assurer des détections rapides et précises, et de réduire le temps et les ressources nécessaires aux investigations manuelles.

Une nouvelle fonctionnalité d'unification des identités permet d'accéder immédiatement aux données de Splunk Cloud Platform et Splunk Observability Cloud avec les mêmes identifiants.

L'utilisation d'outils de dépannage et de workflows centralisés améliore les expériences clients. Avec la version anticipée de l'OpenTelemetry Collector comme extension technique (TA), les clients de Splunk Cloud Platform peuvent plus facilement adopter Splunk Observability Cloud et déployer le Collector parallèlement à leurs forwarders existants pour capturer les métriques et les traces. Grâce à cette nouvelle fonctionnalité qui offre aux clients une vue unifiée de leur infrastructure et de leurs services, plus besoin de déployer et de gérer deux agents. L'arrivée de l'OpenTelemetry Collector marque une étape importante dans l'engagement de Splunk envers Open Telemetry et la communauté open source en aidant les clients à transmettre leurs données plus facilement.

Ingest Actions enrichit ses fonctionnalités pour acheminer les données vers plusieurs buckets Amazon S3 distincts, pour une meilleure granularité en matière de gestion des données.

La nouvelle version anticipée de Federated Search for Amazon S3 offre une expérience de recherche unifiée dans les données au repos des buckets Amazon S3 — sans avoir à importer les données dans Splunk — ainsi que des instances Splunk et des data lakes tiers grâce à son intégration dans Ingest Actions et Edge Processor pour faciliter les mouvements de données. Ainsi, les clients évitent les temps de latence et les dépenses inutiles.

Le Edge du futur ?

Edge Processor featuring SPL2 permet maintenant l'importation et l'exportation de données vers Splunk avec HTTP Event Collector (HEC), ce qui facilite la gestion des données. De plus, pour répondre aux exigences de souveraineté des données et de conformité, les utilisateurs peuvent spécifier des destinations par défaut avec Edge Processor pour plus de flexibilité dans l'acheminement.

Alors que l'Edge Computing est désormais un moteur de l'innovation, le processus d'identification et de collecte de grandes quantités de données à partir de plusieurs sources physiques et virtuelles peut être très complexe, fastidieux et coûteux. Splunk Edge Hub rationalise la collecte et l'investigation de données périphériques en abattant les frontières et les silos de l'accès aux données dans des environnements physiques et virtuels et en agissant comme un agrégateur de données provenant des plateformes d'autres fournisseurs. Le dispositif est prêt à l'emploi et peut être placé dans un environnement physique ou sur le matériel OT existant du client. Par ailleurs, il peut facilement être configuré pour collecter et transférer immédiatement les données dans la plateforme Splunk.

La solution permet de surveiller les conditions météorologiques et environnementales, telles que l'eau, la température, l'humidité et les gaz, pour identifier et remédier rapidement et efficacement aux conditions problématiques. Elles effectuent des analyses prédictives pour identifier les anomalies dans les processus de production ainsi que les signes précurseurs de besoins de maintenance des équipements ou de pannes, afin de minimiser les temps d'arrêt opérationnels. De cette manière, on obtient une visibilité plus complète sur les environnements IT et OT afin de mieux détecter, étudier et résoudre les menaces et les facteurs de stress informatiques à partir d'une seule plateforme. Enfin, il devient possible de construire des solutions sur mesure à l'aide d'experts de l'industrie pour différents environnements où la collecte de données a toujours été difficile, comme c'est le cas pour le transport, le pétrole, le gaz et la supply chain, entre autres. Splunk Edge Hub sera exclusivement distribué par des partenaires experts en la matière, qui pourront adapter la solution pour résoudre des problèmes opérationnels et commerciaux critiques dans leur secteur d'activité. Splunk Edge Hub est actuellement disponible en version à disponibilité limitée aux États-Unis, et il est prévu de l'étendre aux régions EMEA et APAC. □

B.G

Wi-Fi

Des usages parfois douteux

En dehors des systèmes filaires et des réseaux cellulaires, le Wi-Fi est le moyen privilégié des Français pour se connecter. Son usage est parfois à la limite de l'acceptable comme le prouve une étude réalisée par ExpressVPN.

Le Wi-Fi reste le moyen le plus utilisé pour se connecter à Internet. Selon ExpressVPN, 63 % des Français ont au moins 4 appareils connectés à un réseau Wi-Fi personnel. De plus, 59 % des sondés partagent leur Wi-Fi domestique avec d'autres personnes. Parmi eux, seuls 18 % le font avec leur partenaire, tandis que 74 % partagent leurs identifiants avec leur famille.

94 % des Français disposent d'un mot de passe sur leur routeur. Si se plaindre d'un mot de passe trop long est la norme, seuls 31 % le mettent à jour régulièrement et moins d'un tiers (30 %) connaissent le type de chiffrement utilisé pour accéder à leur routeur. Seuls 13 % des utilisateurs français optent pour la technologie la plus sécurisée à ce jour (WPA 2). Cette méconnaissance des bases de la sécurité Wi-Fi est préoccupante, car elle laisse la porte ouverte aux abus et aux piratages du Wi-Fi. 36 % des utilisateurs ont déjà changé le nom de leur réseau (SSID) pour un nom plus amusant. 13 % des personnes interrogées ont essayé de contacter quelqu'un en repérant le nom de son Wi-Fi. Moins de la moitié des personnes interrogées (46 %) pensent aux risques

Un routeur Wi-Fi VPN Aircove d'ExpressVPN.

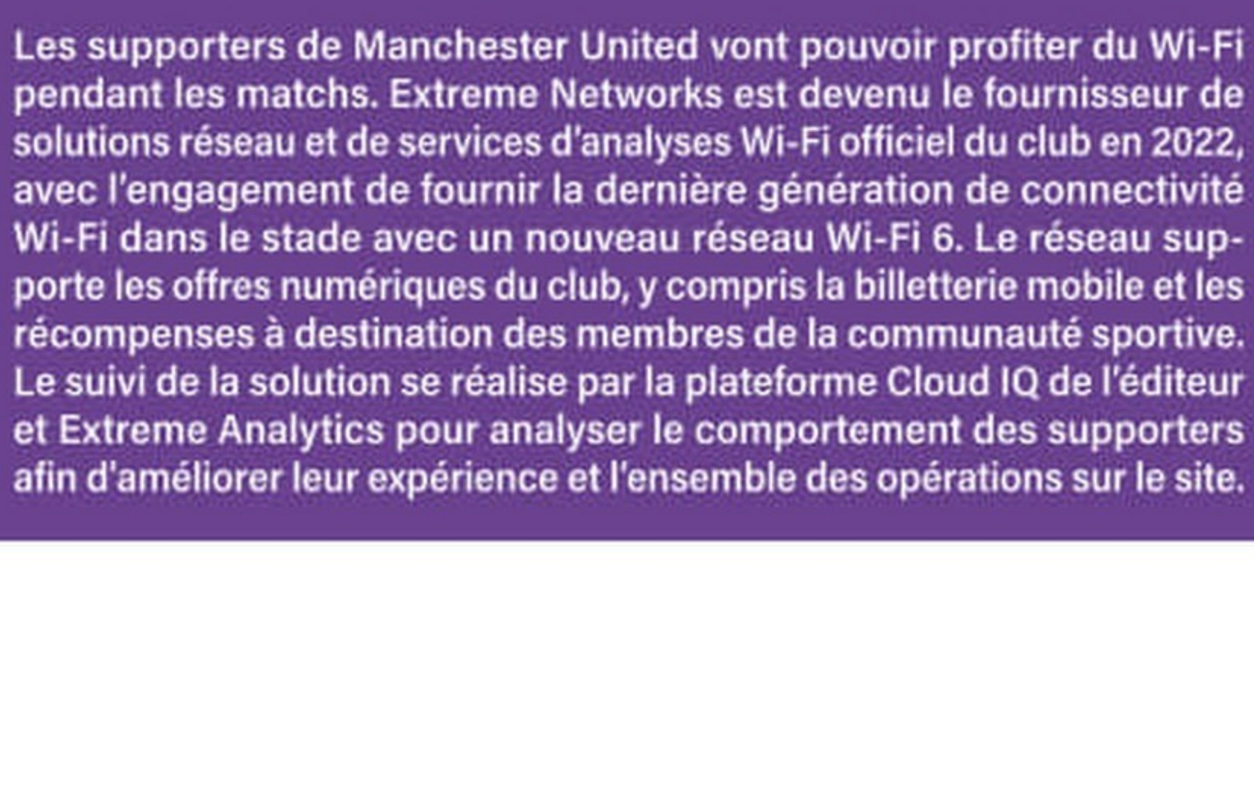
liés à la connexion à un réseau Wi-Fi. Dans un contexte où le télétravail est définitivement entré dans les mœurs, près d'un Français sur trois (29 %) fait plus attention à l'endroit où il se connecte avec son ordinateur professionnel qu'avec son ordinateur personnel. Un sondé sur cinq (20 %) a déjà demandé à un voisin s'il pouvait accéder à son réseau Wi-Fi, tandis que 56 % de ces mêmes personnes déclarent qu'elles n'envisageraient pas de partager leur connexion Wi-Fi avec un voisin, par manque de confiance... Cette crainte semble pourtant justifiée quand on sait que près d'un Français sur cinq (18 %) a déjà subi une intrusion non désirée sur son réseau Wi-Fi.

Des usages sans restriction

18 % des personnes interrogées reconnaissent avoir consulté des contenus pornographiques sur un réseau qui ne leur appartenait pas. Ce chiffre atteint 45 % chez les 18-24 ans, dont 6 % avouent l'avoir regardé sur leur lieu de travail. 18 % des personnes interrogées ont déclaré avoir visité des sites douteux, voire dangereux, ou avoir consulté le dark web en utilisant un réseau Wi-Fi privé qui n'était pas le leur. □

B.G

EXTREME NETWORKS FAIT ENTRER LE WI-FI À OLD TRAFFORD



Les supporters de Manchester United vont pouvoir profiter du Wi-Fi pendant les matchs. Extreme Networks est devenu le fournisseur de solutions réseau et de services d'analyses Wi-Fi officiel du club en 2022, avec l'engagement de fournir la dernière génération de connectivité Wi-Fi dans le stade avec un nouveau réseau Wi-Fi 6. Le réseau supporte les offres numériques du club, y compris la billetterie mobile et les récompenses à destination des membres de la communauté sportive. Le suivi de la solution se réalise par la plateforme Cloud IQ de l'éditeur et Extreme Analytics pour analyser le comportement des supporters afin d'améliorer leur expérience et l'ensemble des opérations sur le site.

Gestion

En finir avec la fragmentation

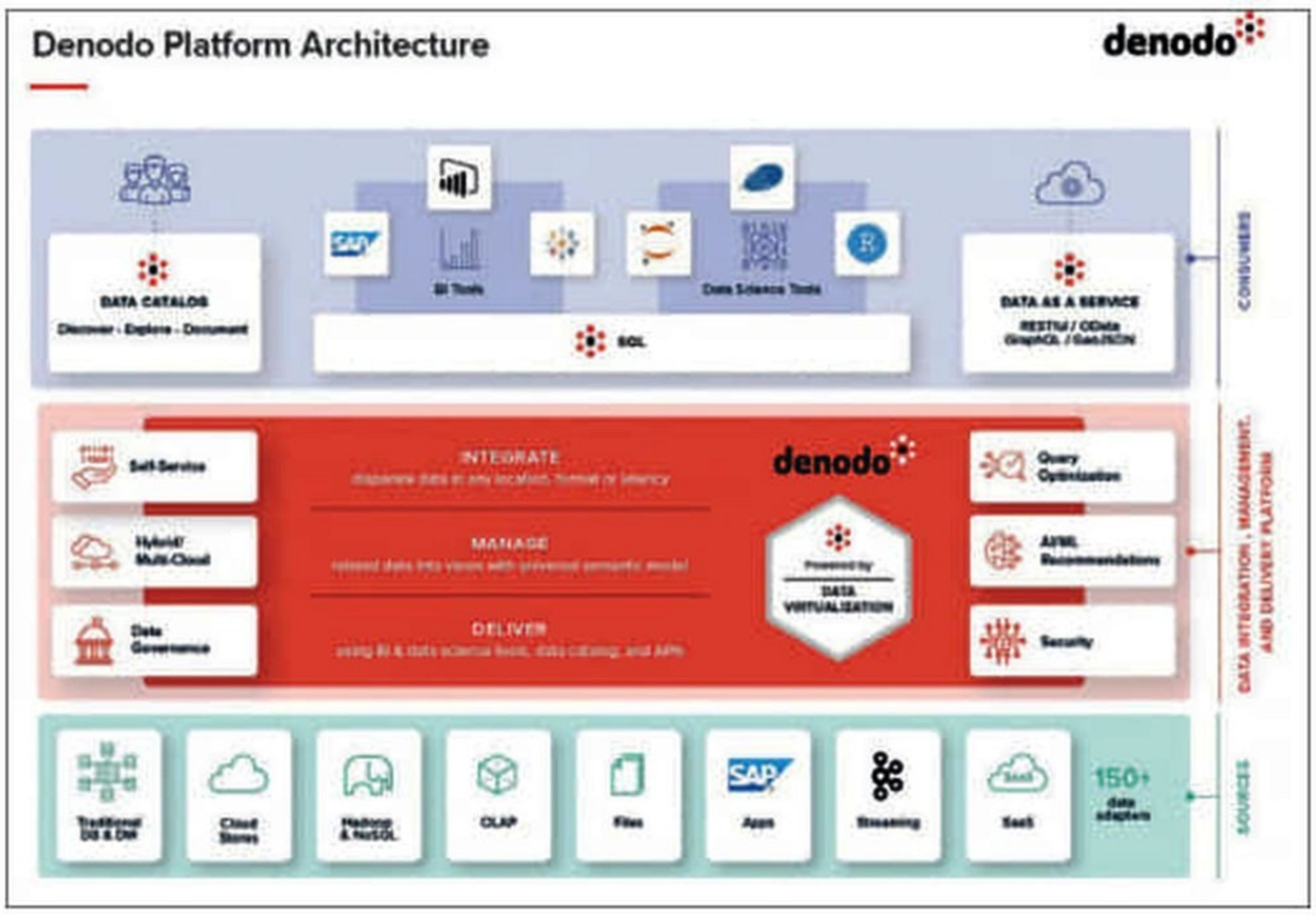
Denodo a tenu récemment une matinée au Cloud Business Center de Paris pour ses clients, partenaires et prospects, avec la venue de son CEO, Angel Viña. Le principal thème de cet événement, casser le silo des data lakes par une approche différente.

Comme Angel Viña l'explique à *L'Informaticien* : *« dès le début de notre entreprise, nous avons voulu traiter le problème de la fragmentation des données par la gestion et l'intégration des données pour que les entreprises puissent les traiter et les utiliser en temps réel »*. Il ajoute : *« aujourd'hui, cela devient encore plus complexe alors que plus de 25 % de nos clients indiquent qu'il est critique pour eux d'interagir avec leurs données »*.

Une simplification par la virtualisation

Pour apporter une solution à ces différents problèmes, Denodo passe par une couche de virtualisation des données pour simplifier et masquer la complexité du travail d'intégration et de gestion des données que réalise la plateforme. Par ce moyen, l'éditeur unifie les données de l'entreprise afin de pouvoir les utiliser plus facilement. Olivier Tijou, Regional VP et General Manager France indique différents cas d'usages comme le partage des données au Crédit Agricole ou pour obtenir plus d'agilité avec les données comme chez Total Energies ou à la Coface. Il continue : *« notre approche propose un changement sur la gestion et l'utilisation des données. Toutes les entreprises ne sont pas prêtes, mais la contrainte de s'adapter va dans notre sens »*.

Par la virtualisation, les données sont utilisées sans avoir de besoin de les répliquer dans les différents systèmes grâce à un travail au niveau sémantique par les interfaces. La principale annonce de cet événement a été l'introduction d'un moteur de traitement en parallèle des données (MPP ou Massively Parallel Processing). Avec cette intégration, l'objectif de Denodo est de démocratiser le MPP et de casser le silo de données qu'est le data lake. De plus, Denodo simplifie la gouvernance des data lakes grâce à des outils de gestion inédits sur le marché, avec une interface « graphique », à la différence des interfaces habituellement « très techniques » que l'on doit généralement utiliser dans ce domaine. Un cluster MPP Denodo déployé dans le cloud au-dessus des services de stockage d'objets de l'entreprise permet le traitement de données au plus proche des sources, sans devoir sortir les données du cloud en extrayant uniquement celles qui sont nécessaires, afin de minimiser les coûts de sortie. De plus, ce point permet des utilisations très proches du temps réel sur les données. Le MPP apporte du calcul supplémentaire, lance les requêtes en temps réel, fournit l'accès rapide et simplifié aux résultats des données issues des data lakes. Au-dessus, Denodo intègre d'autres sources tout en gérant la sécurité et la gouvernance des produits de données qui sont ensuite exposés dans des outils familiers de métiers comme les outils de business intelligence ou des interfaces applicatives (API).



Vers le data mesh

Le data mesh consiste à faire abstraction de la complexité des couches d'exécution et d'intégration. C'est un tableau de bord qui s'assure que, quand une direction est donnée, la data est bien protégée et accessible, d'où qu'elle vienne. C'est pourquoi l'exécution d'un MPP, couplée à la puissance de Denodo, permet de livrer véritablement les promesses du data mesh. □

B.G

LA 23

LES ASSISES

Retrouvez les incontournables

et les pépites de la cyber

11.10.23 →→ 14.10.23

/MONACO///

→ 23e édition :

Prenons de la hauteur !

→ **lesassisesdelacybersecurite.com**

DG CONSULTANTS

COMEXPOSIUM

Villes intelligentes

SystemX simule la logistique urbaine

Un projet de R&D mené par un consortium européen, et par l'IRT SystemX en France, s'est concrétisé par un simulateur de l'activité de livraison à domicile à Lyon et de ses effets, en particulier sur le bilan carbone. Il facilite la création de scénarios en fonction de nombreux facteurs. L'outil a été développé en Python et a largement tiré parti de bibliothèques open source et de données publiques.

S'inscrivant dans la mouvance des villes « intelligentes », le projet Lead a pour objectif de développer un outil capable d'aider les décideurs à mieux comprendre les leviers efficaces sur lesquels jouer pour réduire l'empreinte environnementale liée aux livraisons de marchandises en ville, dans les commerces et surfaces commerciales et à domicile. Les déplacements des colis livrés par DHL, Chronopost *etc.* sont pris en compte, avec une attention particulière sur les livraisons à domicile. Cette catégorie BtoC devrait doubler d'ici 2030 selon certaines estimations. *« Il s'agit d'un outil d'aide à la décision stratégique pour assister des politiques désormais très concernées par cette problématique »*, résume Yann Briand, référent de la thématique Mobilités & Logistique au sein de l'IRT SystemX. *« Et, peut-être encore plus, d'un outil qui devrait faciliter la concertation entre les différentes parties prenantes, les collectivités comme les acteurs économiques. »* Originalité du projet, il tient compte de l'énergie consommée et du bilan carbone, mais également de données économiques, coûts et durée des livraisons entre autres *« pour générer des simulations réalistes pour les entreprises du secteur qui opèrent avec des marges réduites, et apprécier la soutenabilité des scénarios alternatifs »*, ajoute Yann Briand.

Génération d'indicateurs de performance et comparaison des scénarios.

Lancé en 2020 pour une durée de trois années, financé dans le cadre du programme H2020, le projet a impliqué 26 partenaires, académiques et collectivités. Il avait pour objectif de créer les jumeaux numériques des réseaux logistiques urbains de six villes. Il vient d'être clos en septembre. SystemX a créé ce simulateur sur le Grand Lyon. *« La première étape consiste à dresser un panorama de l'activité existante »*, décrit Yann Briand. Puis, d'identifier les paramètres permettant de calibrer ces simulations, et enfin, de les faire varier pour construire différents scénarios prospectifs et générer les indicateurs associés : évolution de la demande consommation énergétique, usage de l'espace public... L'ajout de facteurs comme la massification des flottes de véhicules électriques, l'usage de vélos-cargos, ou encore, la prise en considération des hausses des coûts de l'énergie permettent d'affiner les scénarios. *« Ces simulations permettent de comparer l'impact des différentes mesures en termes de réduction de bilan carbone tout en éclairant les efforts opérationnels et économiques qu'elles impliquent pour les opérateurs du secteur »*, résume Yann Briand.

Très logiquement, à Lyon, des structures publiques chargées de l'aménagement du territoire se sont associées au projet. En l'occurrence, Lyon Parc Auto, qui opère les parkings, les services d'autopartage, et Lyon Confluence, Société Publique Locale, chargée d'aménager une partie de Lyon, La Confluence. Elles devraient utiliser l'outil pour, par exemple, choisir où localiser les bornes de recharges, ou encore, décider des zones interdites aux véhicules polluants.


Sébastian Hörl, ingénieur chercheur.

Des développements open source

Pour développer l'outil, les chercheurs se sont d'abord penchés sur les bibliothèques open source disponibles. Côté

traitement, Python a été choisi. *« Nous avons utilisé plusieurs solveurs, en particulier Vroom »*, explique Sébastian Hörl, ingénieur chercheur. Ce projet open source disponible sur GitHub modélise des problèmes de routage. Il prend en entrée la description de véhicules, les tâches de ramassage ou de livraison sur un seul lieu et celles qui doivent avoir lieu sur le même itinéraire et optimise les routes. Il peut également intégrer d'autres paramètres comme les temps de service, les priorités, les temps de service, les pauses des chauffeurs... *« Des développements ont été réalisés pour adapter l'outil aux besoins »*, ajoute Sébastian Hörl.

Yann Briand, référent de la thématique Mobilités & Logistique chez SystemX.

Pour les données liées aux volumes livrés, les chercheurs ont d'abord pioché dans celles accessibles publiquement, notamment celles de l'Insee pour le nombre d'habitants par foyer, âge et catégorie socio-professionnelle. *« Le nombre de colis moyen reçu par ménage est issu d'une enquête d'un laboratoire de recherche lyonnais, le LAET — Laboratoire Aménagement Économie Transports — »*, précise le chercheur. Le répertoire Sirene (Système national d'identification et du répertoire des entreprises et de leurs établissements) a servi à identifier les opérateurs, Chronopost, DHL... et localiser leurs centres de distribution. *« Concernant le nombre de colis livrés par chaque opérateur, en l'absence de données précises, nous nous sommes basés sur les chiffres publiés sur leur site web ou sur des estimations »*, ajoute Sébastian Hörl. Une liste de sources pas exhaustive. Des zones de chalandise ont été affectées aux opérateurs logistiques pour optimiser les trajets. Côté interface graphique, des bibliothèques standards ont été utilisées.

Pour obtenir une vision réaliste de la circulation sur les espaces publics, le simulateur a également intégré les déplacements attendus de la population. Ces flux n'ont pas été construits à partir de données réelles. L'approche s'est basée sur des populations synthétiques (voir encadré). *« Nous générons des données qui représentent l'ensemble d'une population dans une zone géographique, avec ses caractéristiques socio-démographiques, les chaînes d'activités quotidiennes de chacun des individus (travail, loisir, éducation,...) et donc leurs déplacements sur le territoire »* détaille Sébastian Hörl.

Les chercheurs ont visé à rendre l'outil le plus générique possible pour faciliter la reproductibilité sur d'autres villes européennes. *« Quelques adaptations demeurent nécessaires, par exemple la prise en compte de la topologie de chaque zone urbaine »*, ajoute le chercheur. Fonctionnel, le simulateur permet de jouer sur les facteurs, comme la part de véhicules électriques et/ou décarbonés par exemple, et de comparer différents scénarios en termes de bilan carbone, de trafic, ou d'utilisation des infrastructures.

Après Lead, l'Europe va financer dans la continuité un autre projet baptisé Disco — Data-driven, Integrated, Syncromodal, Collaborative and Optimised urban freight meta-model — sur le même sujet. Le but de ce nouveau projet est toujours d'accompagner le processus de transition numérique dans la planification de la logistique urbaine. Il est prévu pour une durée de 42 mois à partir de septembre 2023 et associe pas moins de 47 partenaires, dont SystemX. Copenhague a été choisie comme site cobaye pour modéliser les flux et les données de fret urbain. □

P Br

DES POPULATIONS SYNTHÉTIQUES POUR MODÉLISER LA VILLE

Reconstruction des chaînes d'activités quotidiennes pour la population du territoire.

Les chercheurs considèrent, entre autres, les zones urbaines comme des systèmes complexes, en l'occurrence des systèmes socio-environnementaux. Le comportement des « agents sociaux », individus ou foyers, comme les déplacements par exemple, est très dépendant de leurs attributs, (CSP, ...) ou encore de leurs liens avec d'autres agents. Dans l'objectif d'analyser ces déplacements, SystemX a généré des jeux de données anonymisées à partir de l'open data. L'institut a développé depuis quelques années des compétences dans la création de ces jeux de données appelés populations synthétiques. Ces recherches ont fait l'objet de publications scientifiques. Ces données sont indispensables pour analyser finement les patterns de mobilité.

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 €

Avant-première

Les nouveaux et nombreux chantiers de l'USF

L'association française des utilisateurs de SAP prépare sa prochaine convention prévue en octobre. Passage à S/4Hana, Rise, Cloud foundry ou encore, arrêt du support de GRC et de Solution Manager par l'éditeur en 2027, les chantiers comme les points d'achoppements sont nombreux.

Comme nous l'avions évoqué dans l'édition de juin, l'évènement Sapphire de SAP n'a répondu que (très) partiellement aux attentes de ses utilisateurs. L'USF bataille depuis des années notamment pour obtenir des modèles de licencing plus lisibles de l'éditeur. Si les avancées sont réelles, *« au niveau des accès indirects, les 9 documents générés, par exemple un ordre de maintenance ou un enregistrement financier, sont à date clairement définis. Mais formellement, à part l'engagement moral réitéré plusieurs fois par SAP, rien n'empêche l'éditeur d'allonger cette liste si de nouveaux use cases apparaissent »*, illustre Gianmaria Perancin, président de l'USF. *« De plus, il existe clairement un risque de double tarification, à la fois en fonction de métriques externes sur ces accès et, plus classiquement, par utilisateur. Un risque qu'il est absolument indispensable de maîtriser pour éviter de payer deux fois pour la même chose. Et ceci nécessite côté entreprise un véritable travail de management des usages et des licences. »* Point plus positif, Gianmaria Perancin souligne *« l'ouverture et l'écoute des interlocuteurs français du Licence Management intégrés désormais à la nouvelle équipe en place au niveau régional, comprend France et Benelux. »* Autre sujet, la relation commerciale reste parfois compliquée. Certains commerciaux ont tendance à commercialiser des *« bouquets »* de services logiciels dépassant les besoins réels des clients. À ce jour, *« une enquête de l'Autorité de la concurrence a été lancée à l'encontre de SAP »*, indique notre interlocuteur, qui se demande aussi pourquoi d'autres éditeurs ne bénéficient pas du même traitement...

Gianmaria Perancin, président de l'USF et du Sugen.

Vers une solution hybride

Côté migration S/4Hana, obligatoire à terme sous peine de ne plus bénéficier du support de l'éditeur sur ECC, *« rien de très nouveau »*, décrit le responsable de l'USF. *« Certaines entreprises internationales migrent pour rationaliser leur SI en intégrant leurs filiales. D'autres se lancent pour constituer un socle de base destiné à faciliter leur transformation digitale »*. Le support de GRC et de Solution Manager dont l'arrêt est prévu pour 2027 va également poser problème pour les utilisateurs qui ont toujours ECC. S'ils veulent continuer à utiliser ces outils, dont une alternative sera proposée en ligne, ils devront gérer une architecture hybride.

Toujours des questions autour du Cloud

Au-delà de ces questions, somme toute récurrentes, le passage sur le cloud pose toujours plusieurs questions de fond. Sur la sécurité d'abord. *« Le problème est que SAP pousse très fortement vers S/4Hana, et le recours au cloud qui va avec. Et opter aujourd'hui pour un hyper-scaler revient à risquer d'ouvrir ses données à des entreprises américaines à travers le Cloud Act »*, résume Gianmaria Perancin. Reste alors la possibilité d'opter pour un cloud de confiance, dont la liste se limite pour l'instant à quelques noms, OVH, OODrive et OutScale dans la catégorie Informatique en nuage. Même si des entreprises comme Bleu, issue d'un partenariat entre Capgemini, Orange et Microsoft, ont obtenu l'aval de la Commission européenne, elles ne possèdent pas à ce jour le sésame SecNumCloud de l'ANSSI. La question se complique encore avec la montée en puissance du chinois Alibaba. *« Christian Klein, le DG de SAP, a annoncé en réunion avec le SUGEN* que cette alternative restera limitée aux seules entreprises implantées en Chine. Par cette posture, SAP prend en compte les risques géopolitiques actuels, ce qui reste plutôt rassurant »*, souligne notre interlocuteur. Aujourd'hui, *« il est également possible de chiffrer les données sans donner la clé à SAP mais à un partenaire tiers. Ce qui devrait compliquer toute enquête juridique effectuée au nom du Cloud Act ou lors d'activités « d'intelligence indésirables »*, ajoute le Président l'USF.

Le cloud (re)met également en exergue la question de l'interopérabilité. Gianmaria Perancin illustre : *« l'offre SAP Business Transformation Platform, la solution qui porte entre autres les codes spécifiques qui ne peuvent plus résider sur S/4HANA en cloud public, est disponible sur Google Cloud Platform, Microsoft Azure ou AWS. Rien ne garantit une interopérabilité pour le portage des services en cas de changement d'hyper-scaler. »* Autre exemple, le décommissionnement de Neo implique de passer sur Cloud Foundry. *« La question est : va-t-on retrouver les mêmes services »*, souligne le président. Pour y répondre, l'USF a déjà organisé un atelier *« qui a connu un certain succès. Plus de 120 personnes représentant 70 entreprises étaient présentes »*, souligne notre interlocuteur. Certitude à ce jour, l'USF a du pain sur la planche. □

Pbr

Large Language Models

La France est-elle distancée dans la course à l'IA ?

Confrontée au succès spectaculaire d'intelligences artificielles (IA) conversationnelles telles que ChatGPT, la France tente de rester dans la course aux Larges Modèles de Langages (LLM). Peut-elle y parvenir malgré un nombre réduit de champions et une faible puissance de calcul comparée aux GAMMA (Google, AWS, Microsoft, etc.) ? Pourquoi les petites IA BtoB qui ciblent les métiers semblent une bonne alternative ?

Fin 2022, le lancement par l'américain OpenAI de ChatGPT, une intelligence artificielle (IA) conversationnelle aux performances étonnantes, a créé une véritable onde de choc dans l'industrie du Numérique et dans le grand public. Elle a d'ailleurs battu tous les records de visiteurs détenus jadis par les réseaux sociaux. ChatGPT aurait franchi le cap des 100 millions d'utilisateurs 2 mois après son lancement !

La percée spectaculaire de la V3 de cette puissante AI conversationnelle, disponible en version 4 désormais..., a créé un tel séisme que les politiques, les DSI et les ESN de tous les pays se sont emparés de la question. Les Européens et les Français ont en effet mesuré le retard pris sur le développement des Larges Modèles de Langages (LLM) qui motorisent les GPT (Generative Pre-trained Transformers).

Peu inquiet, semble-t-il, par la quasi-absence de champions français (re)connus dans ce domaine, Bruno Le Maire, le ministre de l'Économie, des Finances et de la Souveraineté industrielle et numérique, a déclaré début juillet que l'Europe devait se donner l'objectif de *« répliquer Open.ai à horizon de 5 ans »*.

Françoise Soulié, conseillère scientifique au Hub France IA.

Guillaume Avrin, coordinateur national IA de la Direction Générale des Entreprises.

Un nouveau fiasco ?

Tous les ténors français du secteur de l'AI se sont insurgés immédiatement ! La plupart redoutent en effet que la France ou l'Europe réédite avec l'IA le fiasco du Cloud et laisse ainsi le champ libre aux GAMMA. Dans ce combat pour le leadership dans l'IA, même Google s'inquiète de voir Microsoft s'allier à OpenAI, dont il finance la puissance de calcul nécessaire à ChatGPT grâce à Azure.

Guillaume Autier, directeur général du site Meilleurtaux.com, résume l'ampleur du challenge auquel sont confrontés les éditeurs et ESN françaises dans ce combat titanesque autour de l'IA : *« Google a ringardisé le Minitel, ChatGPT est en train de ringardiser Google. Ce que nous devons construire n'est pas ChatGPT, mais tout autre chose qui va ringardiser ChatGPT ! »*.

Hélas, les Européens en sont loin. Certes, la France forme certains des meilleurs mathématiciens au monde, dont quelques-uns travaillent pour la crème des centres de recherches en IA... majoritairement anglo-saxons, mais dispose-t-elle déjà d'un vrai outil d'IA prédictif ou génératif commercialisé, et dont le modèle d'apprentissage peut combiner de multiples sources ?

Françoise Soulié, conseillère scientifique au Hub France IA, estime que *« seuls deux éditeurs européens, le français LightOn et l'allemand Aleph Alpha, disposeraient déjà d'offres au niveau du marché »*. Ces deux leaders seraient en effet capables

MISTRAL AI SE POSITIONNE SUR L'IA BTOB ET EN OPEN SOURCE

Soutenue par Bpifrance, Mistral AI a récemment levé 105 millions d'euros grâce au fonds américain Lightspeed Venture, avec le concours de fonds européens et d'investisseurs emblématiques tels que Xavier Niel ou Eric Schmidt, l'ex-Pdg de Google. Les trois cofondateurs de cet éditeur sont des experts des modèles de langage. Arthur Mensch, son PDG, a travaillé trois ans pour DeepMind, le laboratoire d'IA de Google. Guillaume Lample est l'un des créateurs du modèle LLaMA présenté par Meta (Facebook) en février 2023. Enfin, Timothée Lacroix était lui aussi chercheur chez Meta.

« L'INQUIÉTUDE EST TRÈS PROFONDE CONCERNANT L'IA ACT »

Idem à la Commission Européenne, qui a modifié ce printemps son IA Act en urgence pour les mêmes raisons. Ce projet de loi, qui doit encadrer l'utilisation de l'IA en Europe dès fin 2024, inquiète les spécialistes. *« L'inquiétude est très profonde sur notre capacité d'innover en Europe si la Commission Européenne conserve son IA Act en l'état. Le texte devrait être évolutif pour être applicable, alors qu'il est généraliste actuellement »* estime Guillaume Avrin, coordinateur national IA de la Direction Générale des Entreprises (DGE).
Le problème réside selon lui et d'autres experts français dans une définition trop large de l'IA et de ce qu'est un algorithme, une position défendue initialement par l'OCDE. L'IA Act prend aussi très peu en compte les défis liés aux techniques d'apprentissage et aux traitements des données. *« Attention, personne ne pourra utiliser ChatGPT ou Bard en Europe si l'IA Act maintenu en l'état »* prévient Françoise Soulié du Hub France IA. Une opportunité pour les ESN ?

de concevoir rapidement des Modèles Larges de Langages (LLM) exploitables. Contrairement à la start-up française Mistral AI créée en avril 2023, dont les premiers produits d'IA générative en open source destinés aux entreprises (BtoB) ne sortiront qu'en 2024.

Les entreprises en ont-elles vraiment besoin ?

Non, pas plus que d'un super calculateur — sauf si on s'appelle Météo France — pour créer et faire tourner de petites IA conversationnelles BtoB. Ce que confirme Bassem Asseh, le responsable des ventes en France d'Hugging Face, une start-up franco-américaine développant des outils d'apprentissage automatique : *« très coûteux et gourmands en ressources, les LLM n'ont pas forcément la capacité de répondre aux besoins métiers des entreprises, contrairement aux plus petits modèles de langages »*.

Katya Lainé, la présidente de l'éditeur TALKR.ai et de la commission IA du syndicat Numeum, confirme : *« Open AI investi environ 1 M$ par mois pour seulement faire tourner ChatGPT »*. Elle encourage donc *« les éditeurs français à se spécialiser sur certains sujets IA à forte valeur ajoutée, en créant des verticaux métiers pour les entreprises par exemple, au lieu d'essayer de toujours vouloir rattraper leur retard en termes d'avancement ou d'investissements sur les seuls leaders des LLM »*.

Il faut dire que le marché professionnel (BtoB) est très porteur en France tant l'IA fascine et inquiète les entreprises. *« La principale source d'inquiétude de leurs dirigeants est de prendre du retard sur des concurrents qui utiliseraient l'IA pour devenir des leaders »* explique Jérôme Malzac, directeur de l'innovation de l'ESN Micropole.


Jean-Martin Jaspers, préfet qui dirige la délégation ministérielle pour IA (Dmia).


Katya Lainé, Présidente de TALKR.ai et de la commission IA de Numeum.


Laurent Daudet, DG LightOn.

Mais, attention, préviennent les DSI, si les directions des métiers sont facilement séduites par cette technologie, c'est parce qu'elle leur masque sa complexité. *« Pour la première fois dans l'histoire des technologies IT, l'IA n'est plus une affaire de spécialistes »*, explique Laurent Daudet, le directeur général de l'éditeur LightOn. *« Les éditeurs et ESN peuvent donc parler directement aux métiers (R&D, marketing, relations client, etc.) et déployer des modèles d'IA qui leur donnent rapidement de vrais bénéfices »*. À condition que *« les données de l'entreprise soient très bien structurées... ce qui est rarement le cas »* souligne Philippe Limantour, le CTO de Microsoft en France.

Trouver la puissance de calcul

Toutes ces entreprises partagent un même problème en matière d'IA : celui de trouver une puissance de calcul « souveraine » suffisante pour les entraîner et les faire tourner 24/7 à un prix acceptable. Or, la France manque encore cruellement de puissance de calcul et de GPU pour les grands LLM. Sauf si les entreprises acceptent de mettre leurs données dans les clouds publics des GAMMA... voire dans celui d'OVHCloud, qui lance cet été quelques offres dédiées IA.

Le Gouvernement français estime que ce problème sera en partie corrigé par le lancement dès 2023 d'appels à projets en IA et en HPC dans le cadre de l'initiative France 2030. Jean-Martin Jaspers, le préfet qui dirige la délégation ministérielle pour l'IA (DMIA), constate effectivement un *« phénomène de rattrapage actuellement dans les ministères, qui ont conscience des enjeux de l'IA depuis l'introduction de ChatGPT »*. □

Olivier Bellin

Quand l'IA et le Big Data se mettent au service du vivant

L'entreprise Natural Solutions développe des outils Open Source visant à valoriser les données environnementales indispensables au recensement et à la préservation de la biodiversité. Pour passer à la vitesse supérieure, l'entreprise tente de lever 2 millions d'euros dans le but de développer des outils musclés à l'intelligence artificielle qui permettraient d'accélérer la collecte, l'exploitation et l'interprétation de ces données.

Oiseaux, reptiles, insectes, mammifères, végétaux... il ne se passe pas une journée sans que des espèces animales ou végétales disparaissent en silence, dans ce qui est désormais qualifié de *« sixième extinction de masse »*. Une catastrophe écologique dont l'Homme, lancé dans son inlassable course au progrès, est l'unique responsable.

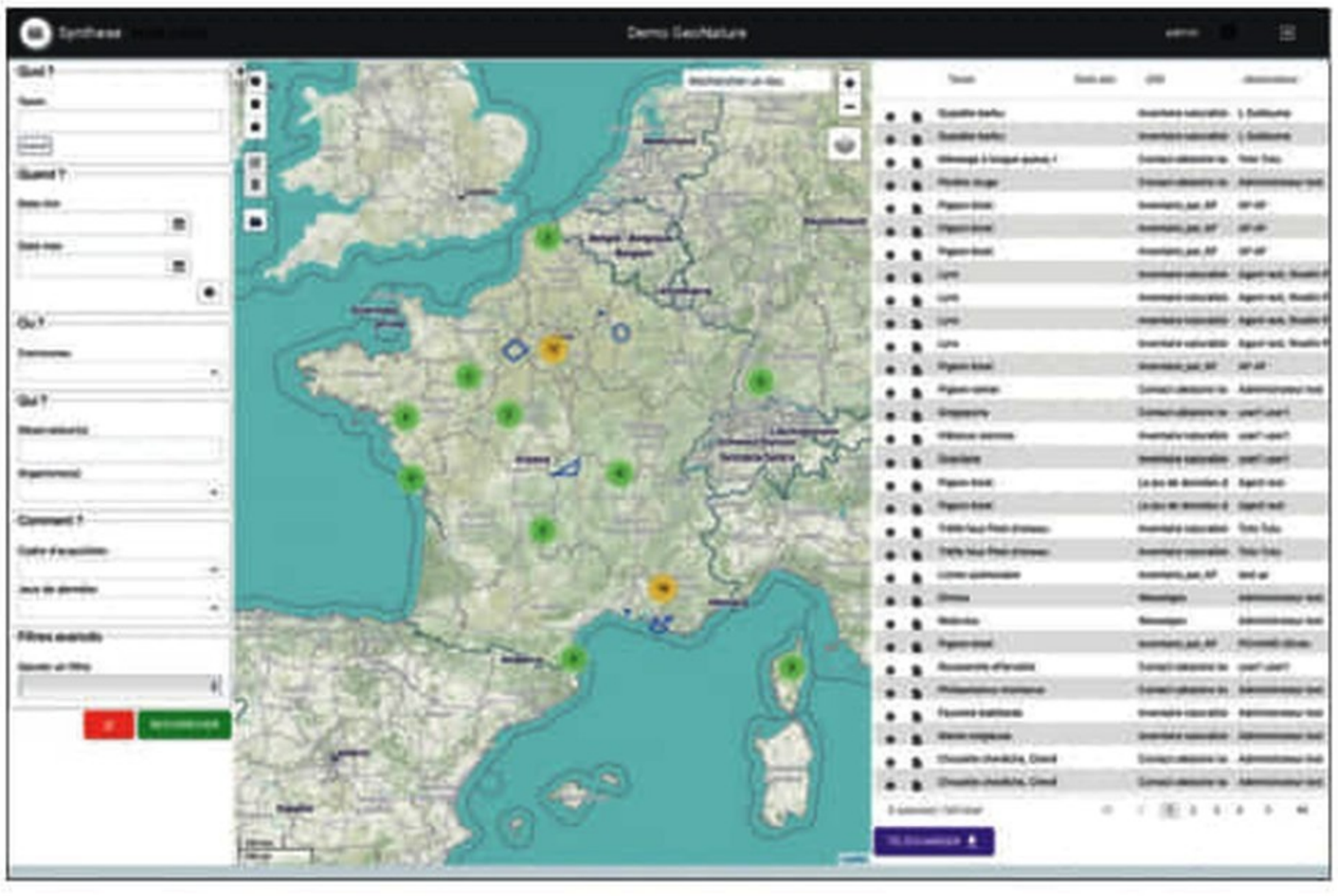
Ironiquement, c'est peut-être ce même progrès qui pourrait, à défaut de régler le problème, du moins apporter des solutions permettant de mieux sauvegarder la biodiversité. Comment ? En exploitant le Big Data, afin de recenser et de mieux rendre compte de la complexité et de la richesse du vivant. Un indispensable pour appliquer les bonnes méthodes pour sa préservation.

C'est en tout cas ce que soutient la société marseillaise Natural Solutions. Fondée en 2008 par Olivier Rovellotti, son PDG, l'entreprise emploie actuellement une trentaine de salariés. Elle est présente en Europe, sur le continent américain, mais aussi et surtout dans la péninsule arabique, où elle participe avec Reneco, une société de services basée à Abu Dhabi et spécialisée dans la gestion et la coordination de projets d'écologie et de conservation, à un programme de conservation d'oiseaux victimes de la chasse.

Des capteurs pour chasser les données de biodiversité

Sur le papier, la mission de Natural Solutions est relativement élémentaire : localiser et documenter le vivant dans toute sa complexité pour faciliter la mise en place de programmes de préservation et/ou de restauration. Pour ce faire, *« nous nous occupons de l'acquisition, de la structuration et de la valorisation des données de biodiversité »*, explique Olivier Rovellotti. L'entreprise se base sur trois types de capteurs mobilisés sur différents sujets (insectes, végétaux, mammifères, oiseaux), afin de recueillir un large panel d'informations. Ce sont d'abord des capteurs professionnels, comme des scientifiques, chargés de recenser et documenter le vivant. Ce sont ensuite des capteurs citoyens, soit des personnes lambda et volontaires, alimentant des bases de données à l'aide de photos par exemple. Ce sont enfin des capteurs électroniques, comme des satellites, des caméras vidéo, ou encore des capteurs bioacoustiques.

L'entreprise travaille avec des capteurs variés (données satellites, photographies, pièges...) pour collecter un maximum de données, ensuite bancarisées et mises à disposition d'acteurs du territoire.



Ces montagnes de données sont ensuite centralisées dans la boîte à outils OpenSource de l'entreprise. Natural Solutions développe, en effet, plusieurs plateformes répondant chacune à des usages différents. Parmi elles : EcoTeka, un outil qui permet de mettre en place des stratégies de renaturation des villes en croisant données de biodiversité avec le cadastre (plan) ; GeoNature, un logiciel de saisie et de gestion de données naturalistes initié par les Parcs nationaux français ; eco-Relevé, un outil de cartographie numérique ; Biodisport, une solution qui aide à inventorier les usages des espaces pour les croiser ensuite avec des données de biodiversité et de mesurer ainsi l'impact des activités humaines sur un écosystème ; ou encore EcoBalade, une application à portée éducative qui aspire à reconnecter le citoyen à la nature.

Informaticien de formation, Olivier Rovellotti est le cofondateur et président directeur général de Natural Solutions.

Des données pour accompagner la prise de décision

Quid de l'exploitation de ces données ? Toutes ces informations sont accessibles aux gestionnaires des territoires afin de les accompagner dans la prise de décision. Concrètement, sur le terrain, des données de biodiversité précises aident par exemple à déterminer les types de végétaux les mieux adaptés aux changements climatiques sur une zone donnée et à renseigner les services écosystémiques rendus par les essences sélectionnées, comme le rafraîchissement des zones urbaines ou encore la pollinisation...

L'Intelligence artificielle pour doper la taxonomie

Lors de la 15e conférence des Parties à la Convention des Nations-Unies sur la diversité biologique (COP) qui s'est tenue à Montréal en 2022, les signataires ont convenu d'inverser le déclin de la biodiversité. Comment ? En protégeant 30 % des terres et des mers d'ici 2030. Une nouvelle ligne à ajouter dans le glossaire des promesses non tenues ? L'avenir nous le dira. Au-delà de la seule volonté politique, c'est aussi un défi technique qui se pose. Déclarer une zone protégée est un long processus qui peut prendre des décennies. En raison notamment de la difficulté à recenser la biodiversité, à évaluer son évolution et l'efficacité des mesures prises pour la conserver.

Or, il y a urgence. Et l'intelligence artificielle pourrait bien répondre à cet impératif, selon Olivier Rovellotti. *« L'IA peut nous permettre d'avancer plus rapidement dans notre mission de conservation en multipliant les capteurs, en améliorant leur efficacité et en accélérant la taxonomie* (la discipline de classification et d'organisation des organismes vivants, ndlr)».

Et alors qu'il faut des années pour former un botaniste ou un naturaliste, *« il suffit de cinq minutes pour entraîner une personne ordinaire équipée d'un smartphone »*. L'objectif est clair : déployer sur le terrain des scientifiques, des capteurs et une armée de citoyens équipés d'outils dopés à l'IA. Le tout, afin de récupérer plus efficacement et plus régulièrement une masse de données de terrain inédites, sans avoir à les interpréter. Les scientifiques épaulés par l'IA s'en chargeront.

Voilà pour la théorie. Mais en pratique, tout reste à faire pour Natural Solutions. L'entreprise travaille à lever 2 millions d'euros auprès d'investisseurs, afin de recruter les développeurs et data scientists, indispensables au développement de ces futurs outils. □

V.M

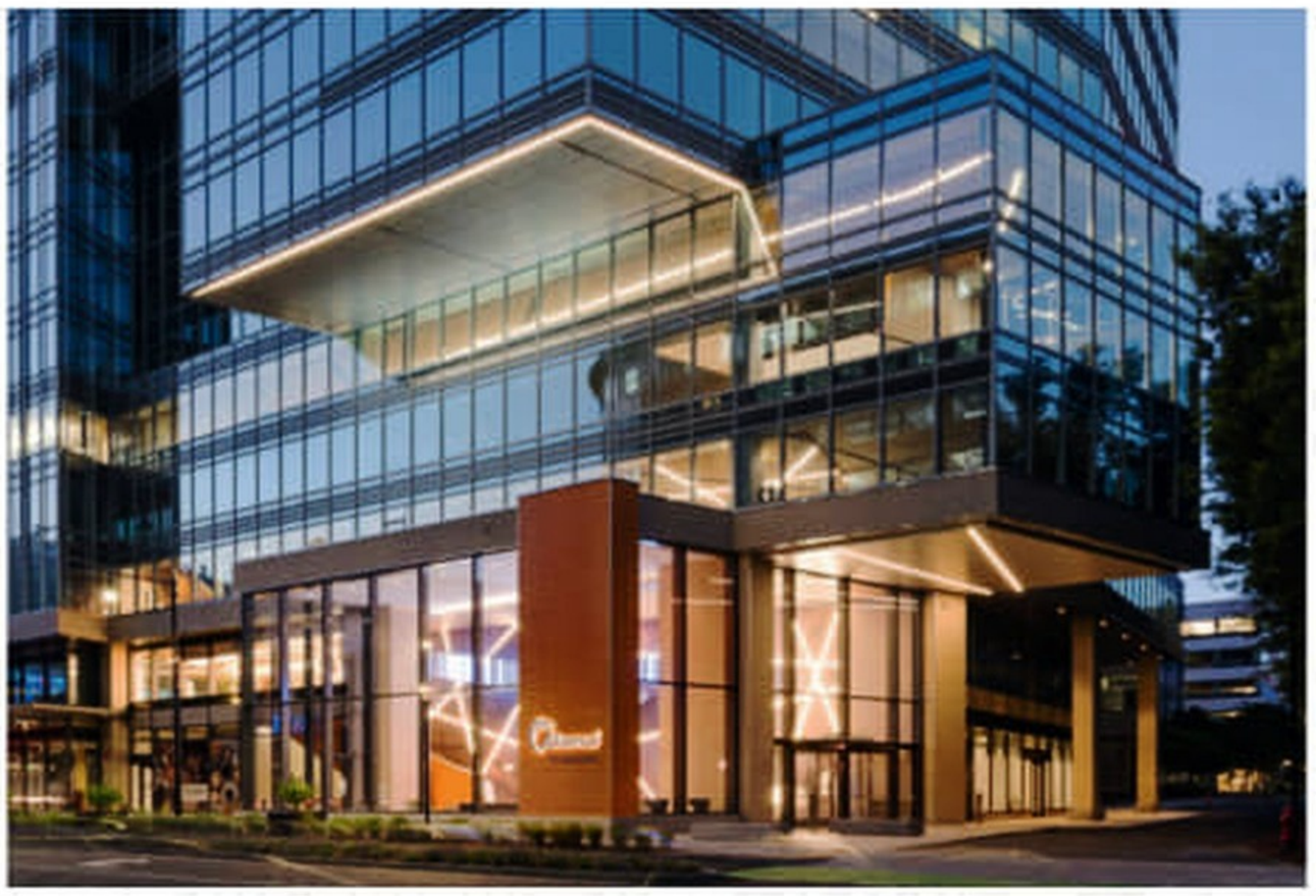
LA **BLOCKCHAIN** AU SERVICE DE L'ENVIRONNEMENT

Fondée en 2021 par Guillaume Leti et Ramzi Laieb, la startup française Carbonable développe une solution destinée aux entreprises, reposant sur la technologie Blockchain et qui doit faciliter la gestion de la compensation carbone. La compensation carbone consiste, pour une organisation, à acheter des crédits carbone et à compenser l'empreinte carbone de son activité en finançant des projets vertueux et certifiés par des cabinets d'audit indépendants.
Carbonable utilise la Blockchain afin de sélectionner ce qu'elle considère comme les meilleurs projets de régénération de la nature et de mettre directement hors-jeu les projets qui pourraient être associés à du greenwashing. Des NFT représentant les divers projets sont vendus aux entreprises sur la plateforme de Carbonable qui reçoit les crédits associés auxdits projets et qui sont ensuite placés sur le marché en pleine expansion des crédits carbone. *« En stockant leurs NFTs, les détenteurs obtiennent un rendement continu »*, promet la société dans une vidéo promotionnelle. À l'aide d'une technologie de monitoring, des rapports d'impact personnalisés et uniques sont générés, sécurisés dans la blockchain et fournis aux détenteurs des NFT/crédits. La startup a récemment levé 1,2 million d'euros auprès de La Poste Ventures et Ethereal Ventures.

Akamai

Du CDN au Cloud Computing

Le géant du CDN poursuit sa diversification. S'appuyant sur son infrastructure et sur son expérience de la livraison de contenus, Akamai se lance dans le Cloud Computing avec le lancement de trois sites, dont un à Paris.



Akamai a depuis longtemps quitté le champ du seul Content Delivery Network pour fournir des services divers et variés autour du cloud, du Edge et de la sécurité. Le 12 juillet, l'entreprise américaine a franchi un cap supplémentaire en inaugurant trois sites dédiés au Cloud Computing, les deux premiers aux États-Unis (Washington DC et Chicago) et le dernier plus près de nous, à Paris même. *« Nous adressons le marché à travers trois piliers : le CDN, notre pilier historique, notre deuxième pilier, la cybersécurité, qui fut un virage important et domine le chiffre d'affaires d'Akamai depuis le deuxième trimestre 2023 »*, nous explique Jérôme Renoux, regional vice-president France d'Akamai. *« Enfin, nous avons ouvert un troisième pilier, dans le cloud computing, avec le rachat de Linode »*.

En février 2022, Akamai annonçait le rachat de Linode. Cette société fondée au début des années 2000 est un fournisseur d'Infrastructure as a Service, visant principalement un public de développeur. En déboursant 900 millions de dollars pour cette acquisition, le géant du CDN entendait concevoir *« une plateforme cloud unique pour créer, exécuter et sécuriser des applications du cloud à la périphérie »* selon Tom Leighton, CEO et co-fondateur d'Akamai. Dans un premier temps, Linode a continué d'opérer indépendamment. *« Le mariage des produits de calcul et de stockage de Linode avec les solutions serverless, CDN et de sécurité d'Akamai offrira aux clients une gamme plus large de services pour créer, moderniser et faire évoluer la prochaine génération d'applications »* explique de son côté Christopher Aker, fondateur et directeur général de Linode.

Une infrastructure adaptée aux workloads distribués

Ces trois nouveaux centres représentent donc un premier pas pour Akamai dans le lancement d'un service mêlant calcul, stockage ou encore base de données. Une offre IaaS, en d'autres termes. *« Nous répondons à une demande de nos clients, puisqu'il est possible dans notre CDN de faire du serverless et du stockage distribué. La brique computing nous manquait »* souligne Jérôme Renoux. Ce produit s'adresse d'ailleurs au client final. On peut alors se demander comment

UN SITE EN FRANCE

Pour se lancer dans le cloud computing, Akamai a ouvert trois sites, dont un à Paris. Un choix qui peut paraître surprenant, compte tenu de l'ancrage très américain des deux autres sites, et du prochain, prévu à Seattle. D'autant que l'on a pris l'habitude, avec les hyperscalers, d'attendre un certain temps, voire un temps certain, l'ouverture de sites dans l'Hexagone. Il s'agit toutefois pour la plateforme de répondre aux enjeux de souveraineté des données grâce à un premier centre dans l'Union européenne. Or, Paris dispose de la capacité de datacenter la plus dense d'Europe. Et ce n'est qu'un début puisque, de l'aveu de Jérôme Renoux, regional vice-president France d'Akamai, un autre centre ouvrira à Marseille dans quelques mois. Un site distribué cette fois-ci, pour offrir des fonctions allégées et du backup. *« Chez Akamai depuis 15 ans, je n'ai jamais vu autant d'investissements que ce que l'on fait aujourd'hui pour le cloud, avec une liste de tous les points stratégiques cloud où on veut se déployer »* précise-t-il.

Akamai compte tirer son épingle du jeu, dans un marché ultra-concurrentiel et dominé par les hyperscalers. D'autant que, si l'entreprise a annoncé de nouvelles fonctionnalités de gestion, un doublement de sa capacité de stockage objet et un nouveau load balancer, son offre est des plus basiques : computing, stockage objet, base de données.

« Nous sommes partis d'un constat : la grande majorité des clients des hyperscalers n'utilisent pas tous les services, toutes les options. Le besoin est concentré sur environ 20 % de la galaxie de solutions qui est proposée. Nous, on se lance, mais on va se concentrer sur l'essentiel » précise le responsable France d'Akamai. *« Ce que nous visons, ce sont des besoins de création de workloads très distribués »*. Sur ce point, le fournisseur peut s'appuyer sur son infrastructure, soit 350 000 serveurs répartis sur 4200 points de présence physique dans 134 pays, et un maillage très fin issu des accords avec les opérateurs télécom et les ISP.

DES LANCEMENTS ORIENTÉS CLOUD

En parallèle de l'annonce de ses nouveaux sites, Akamai a annoncé plusieurs nouvelles fonctionnalités en lien avec son offre de cloud computing. À commencer par des fonctions de gestion « premium », comprenant une allocation prévisible des ressources et du budget, ainsi qu'une gestion plus simple des SKU. En outre, Akamai a doublé la capacité de son produit de stockage d'objets, atteignant un pétaoctet et un milliard d'objets par conteneur. Cette mise à niveau permet aux entreprises d'accéder à des volumes de données plus importants pour créer des applications et des solutions d'analyse dans le cloud, évolutives, performantes et à faible latence. Les clusters dont les limites ont été augmentées seront disponibles sur les nouveaux sites. Enfin, la plateforme commercialise Akamai Global Load Balancer, service hérité de Linode NodeBalancers pour l'équilibrage de la charge du trafic local et les services Akamai Global Traffic Manager et Application Load Balancer. Cette intégration permet aux utilisateurs de choisir entre l'équilibrage de charge local et global sur le réseau d'Akamai.

Jérôme Renoux, regional vice-president France d'Akamai.

Fait pour le multicloud

Les nouveaux sites et capacités de cloud computing sont intégrés à Akamai Connected Cloud, une plateforme Edge et Cloud massivement distribuée, annoncée en février. À noter que l'entreprise a prévu d'ouvrir deux sites supplémentaires, l'un aux États-Unis, l'autre en Inde, dans le courant du trimestre. Pour le responsable français d'Akamai, *« le cloud computing est un marché en pleine évolution, qui va encore croître. Même les hyperscalers réorientent leurs investissements sur l'IA qui va avoir besoin d'être très distribuée. Le cloud a besoin de distribution, d'élasticité »*. Quant aux clients, ils demandent de plus en plus que leurs workloards soient sur des infrastructures distribuées, *« d'où une vraie pertinence à rapprocher l'expérience d'Akamai dans le CDN et la cyber et le cloud computing »*.

Pour la plateforme, il n'est pas question d'aller taquiner les géants sur leur terrain de chasse, mais de s'inscrire dans une approche multicloud, voire répondre à certaines de ses problématiques. *« En ouvrant ces datacenters, on ne veut pas entrer en confrontation frontale avec les hyperscalers, mais se poser avec nos forces, nos atouts, et réunir le meilleur de deux mondes, à savoir notre savoir-faire dans le CDN et le cloud computing »* soutient Jérôme Renoux. Outre son infrastructure et sa distribution, qui permettent de rapprocher les applications et les données de l'utilisateur, Akamai capitalise sur son expérience du capacity planning, géré pour le cloud computing de la même manière que pour le CDN, *« avec des centaines de personnes chez nous qui savent faire ça »*, et sur sa proximité avec les autres cloud providers, surtout les hyperscalers, pour s'imbriquer dans l'écosystème cloud avec son propre écosystème de partenaires. □

G.P

Identité

Un rachat pour bâtir un leader

Gilles Castéran et Francis Grégoire prennent les rênes de la plateforme SaaS Memority afin de proposer une vision souveraine de la gestion des identités, une dimension stratégique de la cybersécurité à l'ère du cloud hégémonique.

Ce n'est pas tous les jours qu'une jeune pousse est rachetée par des Français à un groupe américain. Encore moins quand ce sont les fondateurs de la start-up eux-mêmes qui accomplissent ce rachat.
Six ans après avoir revendu Arismore, spécialiste de l'architecture d'entreprise au cabinet Accenture, les Français Gilles Castéran et Francis Grégoire ont en effet décidé de racheter Memority (montant de l'opération non communiqué), filiale d'Arismore spécialisée dans la gestion des identités, des habilitations, de l'authentification et du contrôle des accès aux services numériques, afin de créer un leader européen dans le secteur stratégique de l'identité en tant que service (IDaaS).

Construire une identity factory européenne

« Notre offre est centrée sur le concept d'identity factory ("usine d'identités"), qui consiste à gérer tous les services ayant trait à l'identité au sein d'une seule plateforme, pour tous les cas d'usage et tous les types de populations : les employés qui veulent se connecter aux systèmes d'information, les particuliers qui se rendent sur des sites de commerce en ligne ou utilisent des objets connectés, ou encore les entreprises qui entrent en contact dans une logique BtoB », confie Gilles Castéran, directeur général (CEO) de Memority, à *L'Informaticien*.
Dans l'IoT, l'entreprise gère cinquante millions d'objets connectés et s'occupe des véhicules de Stellantis. Elle répond également à des cas d'usage dans la santé et l'industrie connectées.

S'il a choisi de se focaliser sur l'identité, c'est parce que celle-ci constitue selon lui la clef de voûte de toute stratégie de cybersécurité digne de ce nom. *« Aujourd'hui, 85 % des incidents cyber sont en lien avec l'identité numérique. Avec des enjeux de cybersécurité sous haute tension, la gestion de l'accès et de l'identité numérique est plus que jamais critique pour les entreprises. Notre ambition est de bâtir une identity factory européenne autonome qui réponde aux enjeux de nos clients, »* commente-t-il.

Vers le passwordless

En plus des deux cofondateurs, l'équipe de la start-up nouvellement indépendante compte une quarantaine de personnes, la plateforme, la propriété intellectuelle et les services déjà réalisés pour les clients existants.

Elle entend profiter des douze prochains mois pour doubler ses effectifs et innover sur plusieurs axes stratégiques. D'abord, l'analyse du risque contextuel lié à l'identité, afin de permettre de se passer du mot de passe (« passwordless ») dans certains cas où l'identité de la personne est assurée.

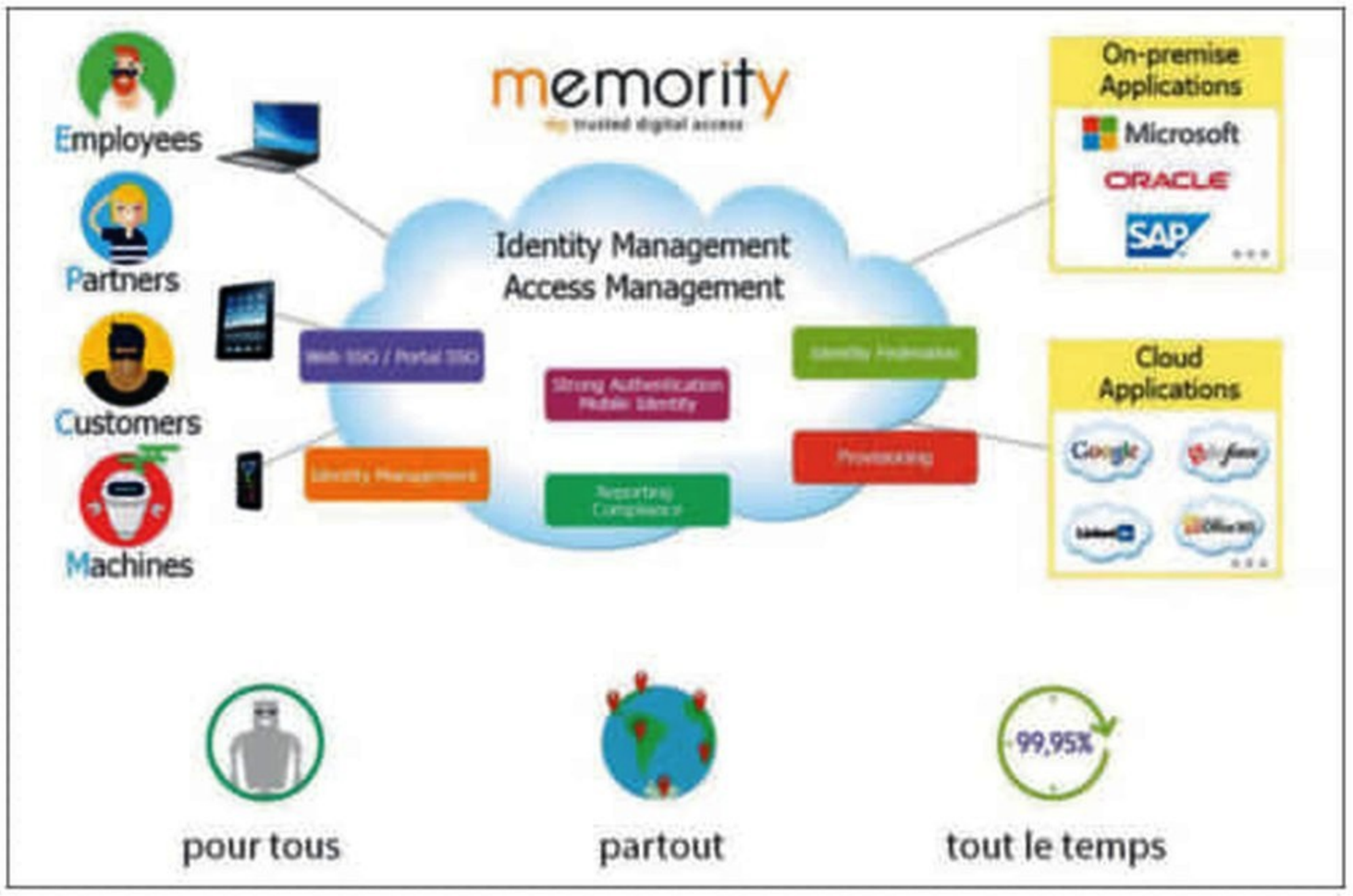
« On s'appuie par exemple sur des applications sur lesquelles l'utilisateur est déjà identifié sur son ordinateur ou son téléphone, on vérifie que celles-ci sont bien à jour, qu'il n'y a pas de vulnérabilité, on analyse le comportement de l'utilisateur, et en fonction de toutes ces informations internes et externes, on attribue un score de confiance qui, s'il est suffisamment élevé, lui permet de se connecter sans mot de passe. C'est donc un système à la fois plus confortable et plus sécurisé que le mot de passe seul », précise Gilles Castéran.

L'automatisation *via* l'intelligence artificielle, ensuite, pour démocratiser la solution et toucher un marché jusqu'à présent peu atteint par Accenture : celui des PME.


À droite Gilles Castéran et son associé Francis Grégoire.

« L'apprentissage automatique est très utile pour analyser le contexte et faire de la détection de menaces. L'IA est un outil essentiel au service de l'automatisation, et pour démocratiser, il faut forcément automatiser, faire en sorte qu'une entreprise de taille intermédiaire puisse facilement raccorder notre solution à sa plateforme. »

Le multicloud, enfin, pour offrir de la flexibilité aux clients en leur permettant d'être sur plusieurs hyperscalers.



Identité et souveraineté

Les cyberattaques sont en augmentation constante depuis plusieurs années, et plus encore depuis le déclenchement des hostilités en Ukraine. Dans ce contexte, la cybersécurité est en plein boom, et l'identité numérique devient particulièrement stratégique à l'heure où les systèmes d'information sont en migration vers le cloud et où la complexité des environnements ne fait que croître.

« Nous avons voulu relocaliser une plateforme dont la propriété intellectuelle était partie à l'étranger afin de donner une autonomie stratégique à cette activité-là en France. Nos concurrents sont de grands acteurs américains comme SalesPoint ou ForgeRock, et les fonds américains comme Thoma Bravo ont tendance à racheter la plupart des jeunes pousses stratégiques européennes, y compris dans ce domaine.

Nous voulons donc proposer une vraie approche française et démocratisée de la gestion des identités afin d'améliorer la cyber-résilience de notre écosystème. C'est un problème dont les autorités sont de plus en plus conscientes : l'ANSSI a par exemple mis en avant la nécessité de mieux gérer les accès à l'identité dans le cadre du plan France Relance », explique Gilles Castéran.

Comme tous les acteurs numériques jouant sur la notion de souveraineté, Memority doit toutefois manœuvrer entre d'une part, l'impératif d'efficacité qui implique de travailler avec les hyper-scalers et d'autre part, l'extraterritorialité de lois américaines comme le CLOUD Act qui rendent difficile le fait de faire rimer cloud et souveraineté. L'entreprise, cliente d'AWS et Google Cloud, affirme être partenaire des projets de clouds de confiance européens S3 ns (Google Cloud et Thalès) et Bleu (Orange et Capgemini).

« Le fait qu'on tourne sur AWS et Google Cloud est une très bonne chose pour séduire les clients internationaux. Si l'on veut défendre une technologie européenne qui joue dans la cour des grands, on peut difficilement se passer des hyper-scalers », concède l'entrepreneur. *« Ensuite, nous voyons au cas par cas avec nos clients ce dont ils ont besoin dans le cadre de leur autonomie stratégique, certains doivent impérativement échapper aux lois extra-territoriales américaines, tandis que pour d'autres, ce n'est pas vraiment un sujet. »*

Unifier accès et identité

Outre la question de la souveraineté, la volonté de proposer un acteur européen de l'identité se justifie aussi par les divergences avec le marché américain, selon Gilles Castéran.

« La vision anglo-saxonne du marché tend à séparer la gestion des accès de celle de l'identité. La plupart des acteurs de ce marché sont donc spécialisés dans l'une ou dans l'autre. Ce modèle a notamment été poussé par les grands cabinets de conseil américains, mais il est selon nous beaucoup plus efficace de gérer les deux en même temps.

Par exemple, mettons que vous accédiez à votre voiture via votre smartphone. Si vous la prêtez à un ami, il faut qu'un dispositif soit mis en place pour déléguer ce droit d'accès. Cependant, vous ne déléguez pas tous les droits à chaque fois : le propriétaire doit avoir accès à tout, le garagiste simplement à la configuration de la voiture ainsi qu'à l'environnement pilotage et à l'entertainment, alors que quand vous déléguez à un ami, il a simplement besoin de ce qui lui permet de conduire la voiture...

On ne devrait donc jamais dissocier accès et identité, marier les deux permet de contrôler en temps réel que les gens qui accèdent à un service ont bien droit d'y accéder, ainsi que de garantir la qualité de l'ensemble des données. La spécificité du marché européen consiste justement à lier ces deux grands sujets. C'est aussi cohérent avec notre plus grande sensibilité à la protection des données par rapport aux Américains. » ☐

G.R

SUSECON 2023

Observabilité et sécurité en lien avec l'IA

À Munich, en juin dernier, SUSE a organisé le SUSECON 2023 avec de nombreuses annonces autour du cloud natif. Au programme : innovation, sécurisation, gestion améliorée des calculs et des charges de travail dans les conteneurs et enfin de nouvelles fonctions d'observabilité basées sur l'IA avec la solution Opni.

Au cours de la dernière convention SUSECON 2023, qui s'est déroulée du 20 au 22 juin à Munich, SUSE a fait plusieurs annonces autour du cloud natif avec en toile de fond l'innovation, la sécurisation et la modernisation des infrastructures. D'origine allemande, l'entreprise est un acteur reconnu pour la fourniture de technologies open-source sécurisées, spécialisé dans les solutions Linux critiques pour les entreprises, l'orchestration Kubernetes, la gestion des conteneurs d'entreprise et les solutions de périphérie. Dirk-Peter van Leeuwen, le nouveau directeur général de SUSE (il a été nommé en mai) confie : *« nos clients disent qu'ils apprécient les solutions SUSE parce qu'ils les considèrent comme parfaitement configurables. »*

Au SUSECON 2023, SUSE a lancé des packages HPC avec des conteneurs à grande vitesse pour réduire la complexité des calculs et des charges de travail.

Parmi tous les sujets évoqués lors de ce rendez-vous, les développeurs de SUSE ont fait un large focus sur les nouvelles fonctions d'observabilité basée sur l'intelligence artificielle avec la solution Opni. Les équipes en charge du développement d'Opni ont intégré des métriques d'OpenTelemetry dans Opni Monitoring dans la version 0.10 qui est sortie début juin. *« Les utilisateurs ont maintenant la possibilité de sélectionner leur méthode de collecte de métriques préférée : agent Prometheus ou OpenTelemetry. Ce changement entre Prometheus et OpenTelemetry peut être facilement géré dans l'interface utilisateur d'Opni, ce qui simplifie le déploiement des deux collecteurs. L'intégration d'OpenTelemetry offre un avantage clé : il collecte les métriques plus efficacement que Prometheus. Dans des configurations de cluster spécifiques, le collecteur OpenTelemetry d'Opni a démontré jusqu'à 90 % d'économie de mémoire, ce qui en fait une option plus efficace en termes de ressources. » « Cette mise à jour est particulièrement intéressante pour ceux qui collectent des métriques à partir de petits clusters, car elle préserve la simplicité et la facilité d'utilisation des composants d'observabilité d'Opni »*, ont indiqué les développeurs. De fait, Opni offre une visibilité totale sur les charges de travail et des mesures complètes. La conteneurisation des charges de travail a également été introduite pour déplacer les charges de travail organisationnelles en toute sécurité et flexibilité à l'aide d'images de conteneurs de base SUSE Linux Enterprise (SLE).

Dirk-Peter van Leeuwen, le directeur général de SUSE, lors de son keynote inaugural le premier jour de SUSECON 2023.

SUSE Linux Enterprise et Rancher

Outre les nouveautés annoncées sur Opni, la société SUSE a aussi abordé la sécurisation de l'infrastructure informatique et l'accélération de la confiance numérique. À ce titre, l'entreprise a annoncé plusieurs innovations sur SUSE Linux Enterprise (SLE) et des mises à jour pour Rancher

avec comme axe majeur la sécurité. Pour Rancher, SUSE ambitionne d'en faire la console de contrôle de tous les marchés qui utilisent Kubernetes. Parmi les autres priorités de Rancher, la version Rancher Prime appuyée par l'intelligence artificielle figure aussi sur les tablettes. Pour le moment en version limitée, cette nouvelle fonctionnalité apporte une meilleure expérience utilisateur et de nombreux autres avantages comme le durcissement de la sécurité et l'analyse prédictive grâce à l'intelligence artificielle.

SUSE a annoncé plusieurs innovations sur SUSE Linux Enterprise (SLE) et des mises à jour pour Rancher avec la sécurité comme priorité.

Lors de SUSECON 2023, l'entreprise a aussi évoqué la gestion de clusters cloud natif afin d'offrir aux entreprises la possibilité d'exécuter Kubernetes partout, de comprendre le cycle de vie du cluster, d'optimiser et d'évoluer très rapidement. En combinant cela avec la sécurité et la gestion des politiques cloud natif, les sociétés peuvent augmenter les charges de travail des conteneurs, simplifier la gestion des politiques et comprendre la sécurité des conteneurs. Afin d'aider les entreprises dans leur transformation numérique, SUSE propose une solution Linux qui entend protéger les données, fonctionner n'importe où et offrir une évolutivité facile entre les différents sites. Avec cette annonce, SUSE promet également d'apporter une sécurité maximale dans le cloud et un modèle de paiement à l'utilisation ou d'abonnement à la carte. Comme la grande majorité des développeurs, SUSE intègre donc de plus en plus l'intelligence artificielle et le machine learning. C'est notamment le cas avec des solutions de calcul haute performance (HPC). SUSE lance des offres HPC en package qui s'appuient sur des conteneurs à grande vitesse. L'objectif est de réduire la complexité des calculs et des charges de travail. Il faut aussi noter la présentation de SUSE Smart Linux Manager, un outil qui peut gérer tous les systèmes Linux à partir d'une seule console. En bref, SUSE a montré la voie que l'entreprise a choisie, à savoir de proposer des offres pour que les sociétés se modernisent dans les meilleures conditions et en toute sécurité. □

Michel Chotard

VERS DE NOUVEAUX DÉFIS EN MATIÈRE DE SÉCURITÉ

Lors de la session 2023 de SUSECON, l'entreprise a présenté son rapport baptisé « Securing the cloud » mettant en lumière les nombreux défis auxquels sont confrontées les équipes informatiques en matière de sécurisation des environnements cloud et propose des solutions efficaces. L'enquête, réalisée auprès de plus de 500 chefs d'entreprises et responsables informatiques, met en évidence l'état d'avancement de l'adoption du cloud, les principales préoccupations en matière de sécurité et les moyens de les résoudre. *« Nous sommes conscients que chaque entreprise est sur la voie de la transformation numérique, une transformation qui sera considérablement accélérée par les solutions open source. Notre rapport sur les tendances* « Securing the Cloud » met en lumière les perspectives des équipes informatiques confrontées à l'adoption croissante de technologies cloud natives complexes. Le paysage mondial des menaces évolue en permanence pour créer de nouveaux défis en matière de sécurité. Nous sommes bien placés pour aider les entreprises à choisir des solutions open source sécurisées pour leurs charges de travail les plus critiques et les plus innovantes, à mesure qu'elles se transforment avec le cloud », a expliqué Thomas di Giacomo, directeur technologique et chef de produit de SUSE. En résumé, il semble que les décideurs (88 %) des professionnels reconnaissent que s'ils étaient certains de l'intégrité de leurs données, ils seraient plus enclins à migrer des charges de travail supplémentaires dans le cloud. D'ailleurs, ils sont plus d'un tiers à avoir comme principale préoccupation la sécurité du stockage de leurs données dans le cloud. Le rapport livre aussi d'autres enseignements intéressants. On apprend que 36 % des sondés consacrent plus d'un tiers de leur budget à la sécurité « cloud natif ». On notera que les Américains investissent plus massivement dans ce poste que les Européens. Par ailleurs, plusieurs pratiques sont plus populaires parmi les décideurs informatiques basés aux États-Unis que parmi leurs homologues européens. Il s'agit notamment des solutions CSPM (Cloud Security Posture Management), CWPP (Cloud Workload Protection Platform) et CNAPP (Cloud Native Application Protection Platform), qui sont plébiscitées par 42 % des décideurs basés aux États-Unis contre 26 % en Europe. Pour finir, SUSE met en avant le fait que les logiciels open source présentent des avantages clés comme la possibilité collective d'identifier les vulnérabilités potentielles en matière de sécurité.

CONVENTION USF 2023
11 & 12 OCTOBRE - NANTES

WWW.CONVENTION-USF.FR

"LES CRISES, SOURCES DE "NOUVEAUX" MODÈLES DE PENSÉES"

L'ÉVÉNEMENT INCONTOURNABLE DE L'ÉCOSYSTÈME SAP

100	75	6	3171
PARTENAIRES EXPOSANTS	ATELIERS	CONFÉRENCES PLÉNIÈRES	VISITEURS CUMULÉS

CHIFFRES CONVENTION USF 2022

Association des Utilisateurs Francophones de toutes les solutions SAP

ÉTUDIER · PARTAGER · RÉFLÉCHIR · INFLUENCER

6 RAISONS D'ADHÉRER À L'USF

1. Rejoindre un réseau de 450 entreprises
2. Être au cœur de l'écosystème SAP
3. Accéder à toutes nos publications via notre Réseau Social d'Entreprise
4. Échanger sur des problématiques communes
5. Rester informé de l'actualité SAP grâce aux événements USF
6. Participer aux Commissions & Groupes de Travail USF liés aux solutions SAP

USF

3700 MEMBRES

450 ENTREPRISES

180 RÉUNIONS EN 2022

www.usf.fr
www.lelieu-usf.fr
adherer@usf.fr

UTILISATEURS SAP FRANCOPHONES
AU CŒUR DE L'ÉCOSYSTÈME SAP

Bâtiments publics

La Lorraine pilote son chauffage

Pour respecter la nouvelle réglementation sur la réduction de la consommation d'énergie dans les bâtiments publics, la région de la Lorraine a mis en place des outils numériques optimisant notamment le pilotage du chauffage.

En charge des lycées, la région Lorraine a lancé un projet de maîtrise et de réduction de la consommation d'énergie dans ces bâtiments dans le cadre du Dispositif Eco Efficacité Tertiaire (DEET). L'objectif est de respecter ces objectifs à savoir une réduction à minima de 30% à horizon 2030 et, à terme, de 60% à horizon 2050. En 2021, un appel d'offres composé de plusieurs lots est lancé pour 60 lycées. Le groupement Engie-Siemens est retenu pour les lots d'automatisation des installations de chauffage, *« qui représentait environ deux tiers du marché »*, explique Mathieu Picaude, chef de projet chez Siemens. Le fournisseur prend en charge la fourniture des équipements : compteurs, sondes de température et automates, et logiciels chargés de la supervision et de l'optimisation du chauffage. Engie s'occupe de l'envoi des données sur ses réseaux et opère la plateforme. Depuis 2021, les équipes IT des lycées ont repris en interne la partie réseau et récupéreront la partie hébergement des serveurs du projet dans le futur.

Le projet est globalement terminé et sera totalement finalisé à la fin de l'année. Livré par Engie, un serveur virtuel sous Windows embarque l'application Desigo CC chargée notamment du monitoring et des alertes. L'outil supervise l'ensemble des sites. Il est géré à travers Hyper-V, l'hyperviseur natif de Windows. Sur le terrain, Siemens a d'abord installé et programmé des automates, localisés dans les armoires électriques, chargés de recueillir les données issues des chaudières et des réseaux de distribution (mesures de température, durée de fonctionnement...) et de piloter ces *« producteurs d'énergie »*. Ces automates sont connectés aux LAN des lycées. Les transferts de données entre les automates et Desigo CC s'appuient sur le protocole ouvert BacNet sur IP.

Les données sont acheminées jusqu'aux box dédiées d'Engie. Pendant la phase initiale du projet, *« nous avons défini dans Desigo CC des scénarios et les alertes connexes »*, explique Mathieu Picaude. *« Par exemple, si une chaudière fonctionne plus d'un certain nombre d'heures sans que la température cible ne soit atteinte, une alerte est générée. »* Siemens a ajouté une deuxième couche logicielle avec son outil Navigator. Cette plateforme cloud compare entre autres la consommation entre les différents bâtiments similaires sur plusieurs sites et fournit une approche analytique de ces différences par m², *« ce qui permet d'identifier les défaillances en termes de rendement de chaudière, d'isolation... et ensuite, de contrôler l'efficacité des mesures prises »*, détaille Mathieu Picaude.

La cybersécurité dépend pour l'instant de toutes les parties prenantes. *« Les équipes IT des lycées sécurisent les switchs et nous ont dédié des VLAN. Ils nous ont demandé une matrice des flux, une liste des équipements et filtrent ces derniers par adresse MAC. Une démarche de cybersécurité très soutenue pour le monde de l'éducation et qui devrait protéger efficacement leur SI. Ils sont remarquablement vigilants »*, souligne Mathieu Picaude. De son côté, Engie prend en charge la cyber à partir de l'arrivée des données sur ses box. Coté données, l'obligation légale de renseigner la plateforme Operat[1] avec les chiffres, n'est pour l'instant pas automatisée. Cette plateforme institutionnelle a vocation à recueillir et suivre les consommations d'énergie du secteur tertiaire au niveau national. Le logiciel Coviso génère un fichier CSV une fois par an pour renseigner Operat, la fréquence réglementaire actuelle.

Des évolutions de l'application sont envisagées. *« Pour l'instant, le chauffage est géré au niveau des chaudières et des circuits de distribution. Il sera possible d'affiner dans le futur en descendant jusqu'aux émetteurs, aux radiateurs dans les salles. Ce qui imposera notamment de remplacer les têtes de vannes actuelles des radiateurs par des équivalents connectés et pilotables »*, explique Mathieu Picaude. Parallèlement, l'application sera interfacée avec l'emploi du temps des cours dans le but évident de ne chauffer que les salles amenées à être occupées. Autre évolution envisagée, l'automatisation de l'envoi des données sur Operat *via* une API. Enfin, l'outil Coviso pourrait également prendre en charge les informations liées à l'éclairage, à la sécurité et à la protection incendie. □

P. Br.

1 : Observatoire de la Performance Énergétique, de la Rénovation et des Actions du Tertiaire.

UN PROTOCOLE RÉSEAU POUR LE « BÂTIMENT INTELLIGENT »

Mis au point par l'organisation ASHRAE, une association de constructeurs et d'utilisateurs dans le domaine du chauffage, de la ventilation et de la climatisation, le protocole Bacnet *« Building Automation and Control Networks »* est aujourd'hui une norme nationale dans plus de 30 pays et une norme ISO. Il porte sur la normalisation des « messages/services » et des protocoles réseaux, MSTP, IP...

Event Driven Architecture

Michelin passe du batch au streaming

Le fabricant de pneus évolue vers la fourniture de services pour satisfaire ses clients. Pour y parvenir, il a transformé son système opérationnel avec des résultats probants.

Olivier Jauze, CTO et architecte chez Michelin, entre rapidement dans le vif du sujet : *« au départ, nous étions à la recherche d'une solution dans le domaine EDA (Event Driven Architecture) et nous nous sommes tournés rapidement vers Kafka, que nous avons testé avec quelques PoC (Proof of Concept) pour valider nos idées de base »*. Cette volonté venait d'un système d'information encore largement dépendant de traitement par lot des données sur les gros systèmes comme ceux de la chaîne d'approvisionnement, des prises de commandes ou les ERP. Cela créait un vrai hiatus entre les besoins de réactivité face au client et les opérations dans les usines ou les magasins. Ces systèmes envoyaient des volumes importants de données et le traitement prenait... des heures, *« parfois dix heures »* indique Olivier Jauze. Il fallait donc rendre les systèmes plus réactifs, d'où le choix rapide de Kafka, leader du marché dans le domaine de l'EDA. *« Nous souhaitons une approche plus événementielle et modulaire pour faciliter l'évolution de notre SI »* précise l'architecte de Michelin. Il ajoute : *« nous avons trop souffert de grands programmes où il fallait coordonner des centaines d'équipes. Cela devenait trop long pour ajouter de nouvelles fonctionnalités »*.

Olivier Jauze, CTO et architecte chez Michelin.

Le streaming par l'IoT

Depuis des années, Michelin a des points d'activité connectés dans les véhicules par différents boîtiers qui envoient des flux de données en temps réel et traitées au fil de l'eau. À partir de là, ont été vus des usages du streaming sur d'autres sujets comme un orchestrateur de commandes en interne qui gérait près de 20 processus transverses. Cet orchestrateur était cependant difficile à maintenir car trop monolithique. Il a été découpé en plus petits morceaux et certains de ceux-ci ont permis de revoir le processus de la chaîne d'approvisionnement. Depuis, la technologie a été étendue aux flux financiers par des librairies au-dessus de Kafka pour reproduire un traitement au fil de l'eau, tout en permettant de ne pas stocker les messages, mais juste de les consommer en temps réel.

Des résultats probants

Devant la difficulté et les ressources nécessaires pour gérer les clusters Kafka, Michelin fait surtout appel au service managé de Confluent, ce qui a permis d'accélérer la mise en œuvre. Le plus gros cluster est dans le Cloud et gère 1,5 To de données avec des flux de 2,5 Mo de données par seconde.

D'autres clusters sont dans un centre de données privé de Michelin pour la sécurité et la gestion des données confidentielles. Au bilan, Michelin estime économiser 35 % sur ses coûts depuis qu'il a choisi Confluent (par rapport au fonctionnement sur site et à la gestion de Kafka), en tirant parti de la plateforme cloud native qui réduit considérablement les difficultés opérationnelles. Michelin a pu réduire son délai de déploiement de la technologie d'environ huit à neuf mois, en s'appuyant sur les millions d'heures d'expérience dont disposent les équipes de Confluent en matière de gestion de Kafka dans le cloud, avec un taux de disponibilité des données de 99,99 % assurant que les flux de données critiques sont toujours disponibles dans le cloud. □ **B.G**

Gestion des talents

Brest'aim opte pour l'intuitivité avec Empowill

L'entreprise publique chargée des grands équipements de Brest était limitée par une ancienne solution rigide et coûteuse. Pour ses campagnes d'entretiens et la gestion des plans de formation, elle est passée sur la plateforme d'Empowill, plus spécialisée qu'un SIRH, mais aussi agile et simple d'utilisation.

Brest'aim, gère les grands équipements sportifs, scientifiques, éducatifs, touristiques et culturels de Brest Métropole, à l'instar d'Océanopolis et de Brest Arena. Pour ce faire, l'entreprise publique emploie 250 salariés permanents. Lorsque Maïa Wolff arrive au poste de responsable développement RH, *« Brest'aim utilisait déjà un logiciel pour la gestion des compétences, des formations et des entretiens »*. Une solution bien connue, mais qui *« n'était pas intuitive, qui obligeait à une formation pour la prendre en main et, de surcroît, s'avérait être une usine à gaz qui nécessitait, pour l'utiliser à son plein potentiel, d'y mettre une quantité de données faramineuse »*. Les trames d'entretiens proposées par cet outil étaient figées, la moindre demande de changement se soldant par l'envoi par le fournisseur *« d'un devis de plusieurs milliers d'euros »*. *« Je voulais quelque chose de simple et de hautement paramétrable par moi, qui me permette de changer les trames comme bon me semble, de créer de nouveaux entretiens, autres qu'annuels et professionnels »* nous explique Maïa Wolff.

Sis au-dessus de l'anse du Moulin Blanc, Océanopolis est autant un aquarium qu'un centre de Culture Scientifique, Technique et Industrielle.

Un appel d'offres aboutit, en octobre 2022, à la mise en place d'Empowill. Cette plateforme est spécialisée dans la gestion du parcours collaborateur, *« contrairement aux grands SIRH du marché qui font tout, paie, congés, etc. »* indique Kevin Guez, cofondateur d'Empowill. Surtout, l'outil se veut clés en main : l'utilisateur peut lancer ses campagnes et créer des trames d'entretiens comme il l'entend, l'éditeur se contente d'intervenir dans le support client.

Une mise en place rapide

La fin de la solution précédente fut *« très laborieuse »* : *« j'ai dû tout faire à la main »* souligne la responsable développement RH. *« On a extrait les PDFs de l'ancienne plateforme pour les mettre sur Empowill, un processus long, mais nous n'avions pas d'urgence à ce moment-là »*. La mise en place du nouvel outil est, quant à elle, plus rapide, grâce à son intuitivité et aux tutoriels fournis par l'éditeur. Tant et si bien que, dès octobre, Brest'aim a pu lancer sa campagne d'entretiens annuels, puisqu'une fois la trame d'un entretien rédigée, il suffit de créer une campagne dans le logiciel, de sélectionner les salariés qui devront y participer et l'évaluateur.

À l'heure où nous écrivons ces lignes, Brest'aim a ainsi réalisé 215 entretiens annuels, 226 entretiens professionnels, 44 entretiens forfait annuel jour, 14 rapports d'étonnement et 6 entretiens de fin de période d'essai. *« De mon point de vue, les résultats sont excellents : la prise en main par les utilisateurs est simple et rapide et on a un très bon taux d'utilisation, ainsi qu'un SAV réactif »* se réjouit Maïa Wolff. Enfin, Empowill permet de planifier le plan de formation, certifications incluses. *« On peut voir les certifications qui arrivent à échéance, mettre des attributs aux collaborateurs »* explique la responsable développement RH de Brest'aim. Car les 250 salariés de la société publique représentent quelque 160 métiers, des équipes techniques aux commerciaux, en passant par des scientifiques ou encore des marins. Soit des besoins de certifications et de formations particulièrement variés, dont Empowill permet de gérer simplement le catalogue, d'en piloter le plan et d'effectuer le suivi. □

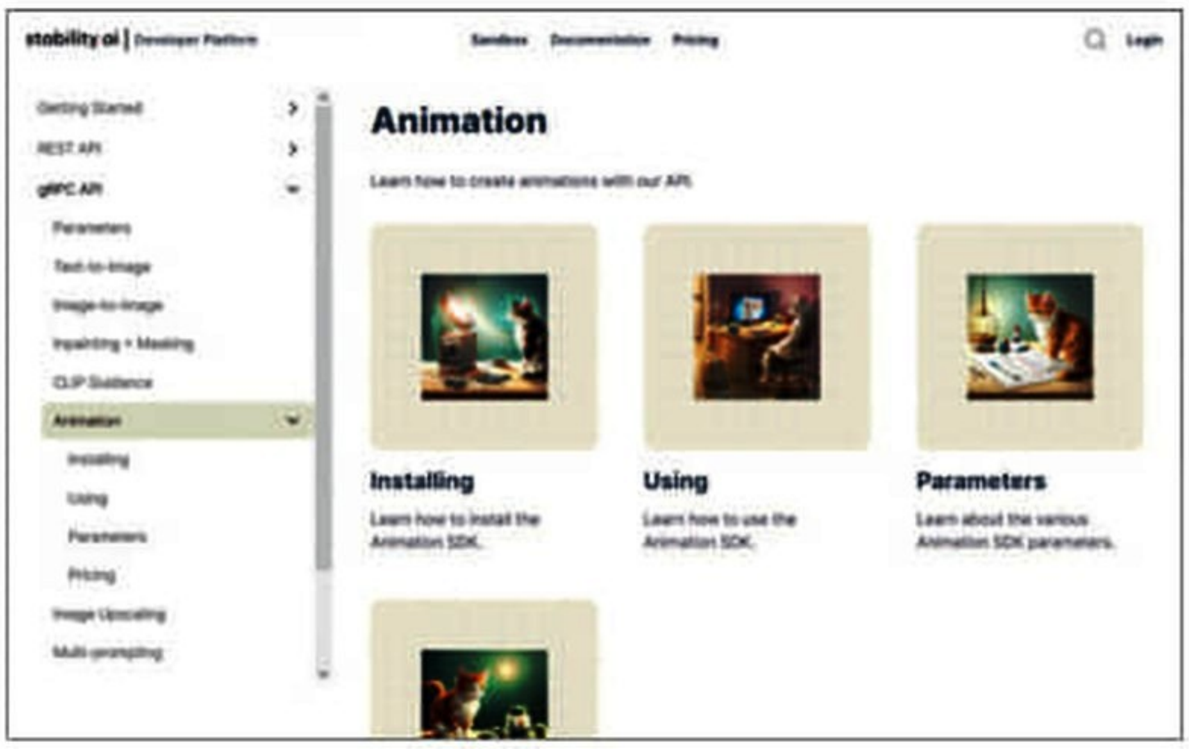
G.P

LLM

Stability AI, légendes et réalités

Stability AI, la société à l'origine du générateur d'images par Intelligence Artificielle (IA) Stable Diffusion, vient de rendre publique la version alpha de StableLM, son IA conversationnelle open source. Nous allons voir dans cet article ce qu'il en est ainsi que de Stability Diffusion, son générateur d'animations.

La guerre de l'IA continue de faire rage, mais le domaine de la génération d'images par intelligence artificielle semble un peu épargné. À l'exception de MidJourney et de Stable Diffusion, c'est même plutôt le calme plat en ce moment. Il faut tout de même citer l'efficace Craiyon et les débuts assez impressionnants de Firefly d'Adobe. C'est, en revanche, la grande déception concernant Dall-E, l'outil de génération d'images d'OpenAI. Après plusieurs mois de soi-disant améliorations, il ne parvient toujours pas à produire des résultats intéressants. Nous sommes presque au début de la mythologie des IA mais aussi au tout début de résultats vraiment concrets. L'ère précédente, jusqu'aux années 70/80, avait d'abord séduit puis éloigné pendant longtemps sinon les scientifiques au moins les investisseurs. Trop d'espoir d'obtenir des résultats incroyables en peu de temps avait démotivé les « croyants » de l'IA. Après divers aléas, la reprise s'est faite assez récemment, boostée par les GAFAM, l'apprentissage machine et l'apprentissage profond pour aboutir enfin aux prémices d'une nouvelle ère avec, pour le grand public, ChatGPT, Midjourney et consorts. Stability vient ajouter de l'eau au moulin des légendes avec ses annonces et actions quelque peu douteuses qui viennent se mélanger à de vraies avancées.



Pour savoir précisément comment utiliser le SDK de Stable Diffusion et ce qu'il vous en coûtera d'un point de vue pécunier, rendez-vous sur sa plateforme de développement à l'adresse https://platform.stability.ai/docs/features/animation

EMAD MOSTAQUE, CRÉATEUR ET TUEUR DE LICORNE ?

Kenrick Cai et Iain Martin ont publié le 4 juin dernier dans Forbes un article au vitriol sur Mostaque. Voici, dans une traduction approximative, un exemple des quelques gentillesses déclarées à son égard : « *Mostaque est titulaire d'une licence, et non d'un master d'Oxford. Les Nations unies ne travaillent plus avec lui depuis des années. Stable Diffusion a été la principale raison de l'ascension de sa startup alors que son code source a été dérobé à un groupe de chercheurs sans accord ni rémunération.* » Pour créer le buzz autour de Stability, Mostaque semble s'être livré à une pléthore de mensonges et d'exagérations, enjolivant largement son rôle dans plusieurs grands projets d'IA. Il a aussi inventé purement et simplement une transaction avec Amazon, en faisant un partenariat stratégique. Malgré cela, Stability AI reste tout de même une des entreprises les plus actives du domaine de l'IA et surtout l'une des plus performantes du secteur complexe de la génération d'images par IA. Un an après le lancement de Stable Diffusion, et malgré l'épidémie de départs qu'elle vient de connaître, la situation pour l'entreprise n'est pas si mauvaise. Il est néanmoins et même encore plus regrettable d'avoir ces problèmes de réputation qui viennent entacher de manière indélébile son image.

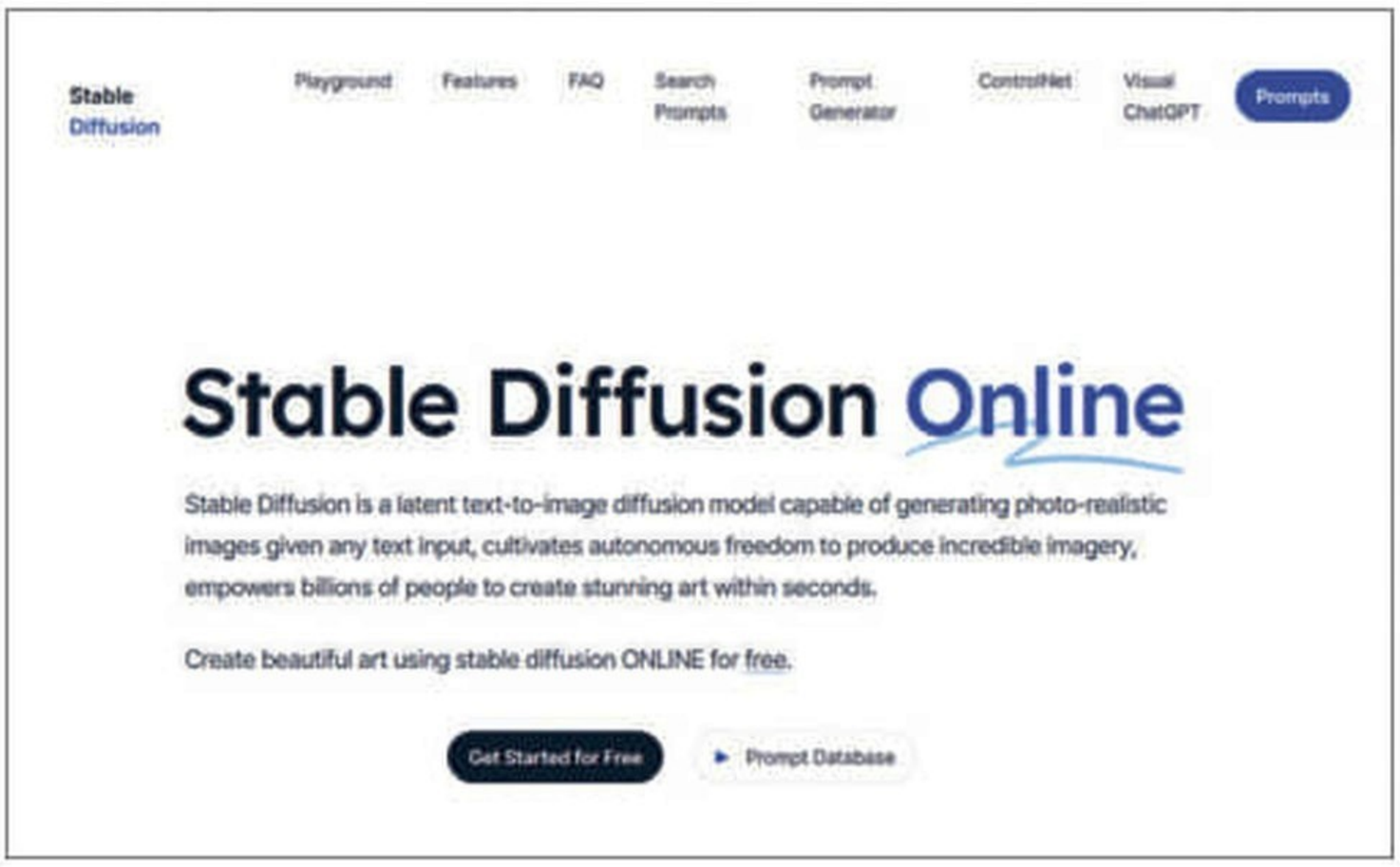
StableLM, un chatbot open source concurrent de ChatGPT

« *Petite et efficace* », dixit Stability AI dans un post de blog à propos de son produit StableLM (https://stability.ai/blog/stability-ai-launches-the-first-of-its-stablelm-suite-of-language-models). Elle utiliserait de trois à sept milliards de paramètres, ce qui peut paraître beaucoup « *de loin* », mais ne représente en fait que 2 à 4% du modèle de son rival OpenAI. Le modèle de langage

employé a été entraîné sur un ensemble de données open source d'EleutherAI, The Pile. Cela a permis à StableLM de dialoguer et aussi d'écrire du code avec des résultats plutôt satisfaisants. Elle serait plus efficace sur la génération de texte et de code que ChatGPT.

Tester StableLM

La version alpha de StableLM a été mise à disposition du public sur GitHub par Stability AI (https://github.com/stability-AI/stableLM/), avec les instructions d'installation et d'utilisation détaillées. Un très grand nombre de personnes essayent de l'utiliser, ce qui allonge inévitablement la durée nécessaire pour obtenir des réponses, même si la génération est rapide. La seule langue maîtrisée par le chatbot est, pour l'instant, l'anglais. A la question : *« Est-elle une meilleure IA que ChatGPT ? »* StableLM aurait répondu : *« ChatGPT est un modèle de langage par IA puissant avec un large corpus de données variées, mais il peut ne pas être capable de comprendre et d'interpréter le langage humain de la même manière que le font d'autres modèles [comme moi]. De plus, ChatGPT peut ne pas bien comprendre le contexte et les nuances du langage et, du coup, produire des réponses incomplètes ou pas assez pertinentes. »* Un peu frimeuse, la StableLM, vous ne trouvez pas ? La modestie ne semble en tout cas pas l'étouffer. Vraie rivalité d'IA ou texte enregistré spécifiquement pour l'occasion ? Difficile de le savoir — même si nous avons notre avis là-dessus — excepté bien entendu pour les développeurs de StableLM. Quoi qu'il en soit, la guerre des IA a indéniablement commencé. Qui gagnera ? L'IA en général et les humains aussi, s'ils l'utilisent intelligemment.



Vous pouvez utiliser Stable Diffusion en ligne en vous rendant à l'adresse https://stablediffusionweb.com

Stable Diffusion

La future version de Stable Diffusion, le générateur d'images IA basé principalement sur des invites textuelles, mais pas seulement, devrait produire des images encore plus réalistes. Une amélioration notable et fortement attendue, une meilleure génération des mains, devrait être au rendez-vous — si Stability AI n'a pas fermé d'ici là au vu des rumeurs néfastes qui circulent. Cette version, la SDXL 0.9, fera directement suite à Stable Diffusion XL. Elle *« produira des images et des détails de composition largement améliorés par rapport à ses prédécesseurs »*. Cette petite annonce est apparue dans un post de blog qui a été supprimé depuis. L'agence Bloomberg l'a signalée un peu avant sa suppression. La prochaine version de Stable Diffusion devrait donc enfin générer des mains de bonne facture. L'entreprise a décrit son nouveau modèle comme offrant *« un véritable bond dans les usages créatifs pour l'imagerie via l'IA générative »*. Des exemples dans le post montrent les avancées réalisées en utilisant les mêmes éléments d'introduction dans Stable Diffusion XL beta et dans SDXL 0.9. Les images générées avec le nouveau modèle offrent des détails plus fins et surtout des mains plus réalistes. Jusqu'à l'arrivée de Midjourney v5 en mars dernier, les mains représentaient une manière simple de détecter une image générée par une IA de par leur imperfection systématique. *« SDXL 0.9 représente un vrai bond dans les usages créatifs pour*

Kenrick Cai et Iain Martin ont publié le 4 juin dernier dans Forbes un article peu élogieux — c'est le moins que l'on puisse dire — sur le CEO de Stability AI, Emad Mostaque.

SDXL 0.9, qui fait directement suite à Stable Diffusion XL, « produira des images et des détails de composition largement améliorés par rapport à ses prédécesseurs », dixit Stability AI. À gauche, SDXL Beta, à droite, SDXL 0.9 (source : Stability AI)

l'imagerie via IA générative », a déclaré Stability AI, *« tout en étant capable de fonctionner sur un ordinateur assez conventionnel. La capacité de générer des créations vidéos hyperréalistes placent SDXL en première ligne des applications pour l'imagerie IA. »*

Des améliorations conséquentes

Stability AI a aussi expliqué que c'est *« l'augmentation significative du nombre de paramètres correspondant à la somme de tous les éléments utilisés par le réseau neuronal pour entraîner le modèle »* qui permet d'obtenir ces améliorations. Si vous voulez faire tourner SDXL 0.9, il vous faut un PC avec au moins 16 Go de RAM et une carte graphique GeForce RTX 20 et 8 Go de VRAM sous Windows (10 ou 11 ou Server 2016 à 2022) ou Linux (distribution récente — il y en a trop pour toutes les citer). Une configuration plus puissante sera forcément la bienvenue, mais vous pourrez démarrer avec cela. Toujours d'après le post de blog, ce modèle devrait être prochainement disponible sur l'outil web Clipdrop de Stability AI. Il sera ajouté prochainement à son application DreamStudio. Stability AI a par ailleurs précisé que la version open-source de SDXL 1.0 serait disponible en juillet, donc peut être lorsque vous lirez cet article.

Il n'y a pas que des bonnes nouvelles

Malgré l'euphorie des investisseurs autour de l'IA générative, la start-up britannique n'a pas réussi à boucler une nouvelle levée de fonds. Stability AI visait une valorisation de quatre milliards de dollars. Selon l'agence Bloomberg, elle a dû se contenter d'un prêt convertible en actions d'un montant inférieur à… 25 millions de dollars. Cet échec est peut-être le signe d'un assagissement sur le secteur de l'IA générative. Stability AI doit aussi affronter la concurrence de Midjouney et d'OpenAI avec son générateur d'images Dall-E, quand bien même celui-ci n'est pas encore au même niveau. Cet échec pourrait aussi s'expliquer par les difficultés et les polémiques grandissantes autour de Stability AI. Le site Sifted a révélé en avril dernier que l'entreprise n'était pas détentrice de la propriété intellectuelle sur le modèle d'IA qui alimente Stable Diffusion. Il aurait été développé par une université allemande et Stability AI se serait servi du code sans vergogne. L'université en question a bien confirmé l'information. De plus, une enquête publiée par Forbes au début du mois de juin a fait état d'un véritable *« historique d'exagérations »* de la part du fondateur et CEO, Emad Mostaque, sur les comptes et affaires en cours (niveau du chiffre d'affaires, partenariat fantôme avec Amazon) ainsi que sur lui-même. Stability AI est, de plus, ciblée par deux procédures judiciaires initiées par un groupe d'artistes et par la banque d'images américaine Getty. L'entreprise n'est rien moins qu'accusée d'avoir violé leur propriété intellectuelle sans aucun consentement ni contrepartie pour *« éduquer »* son modèle d'IA. Pour couronner le tout, trois cadres dirigeants de Stability AI ont quitté la start-up en peu de temps. David Ha, directeur de la recherche et ancien chercheur de Google Brain, a démissionné. Christian Cantrell, un ex d'Adobe, avait lui aussi quitté son poste de vice-président chargé des produits en avril. Le directeur opérationnel Ren Ito a, quant à lui, été remercié. L'équipe ne s'étoffe pas vraiment et cela paraît assez inquiétant quant à la confiance envers l'entreprise. Les intelligences artificielles aiguisaient pourtant l'appétit des investisseurs depuis le succès fabuleux de ChatGPT, le robot conversationnel public d'OpenAI financé depuis à hauteur de plus de 10 milliards de dollars par Microsoft. Stability AI était déjà

devenue une licorne (1 milliard de dollars de valorisation) avant d'essayer de quadrupler l'investissement. Elle en est bien loin désormais. Est-on prêt de l'éclatement d'une bulle spéculative autour de l'IA ? Emad Mostaque assure que non (ce qui n'est guère rassurant au final, vu son manque de sérieux désormais notoire). L'impact de l'IA sera *« bien plus grand que la 5G ou les voitures autonomes »* d'après lui. Sans doute, mais reste à savoir qui en profitera.

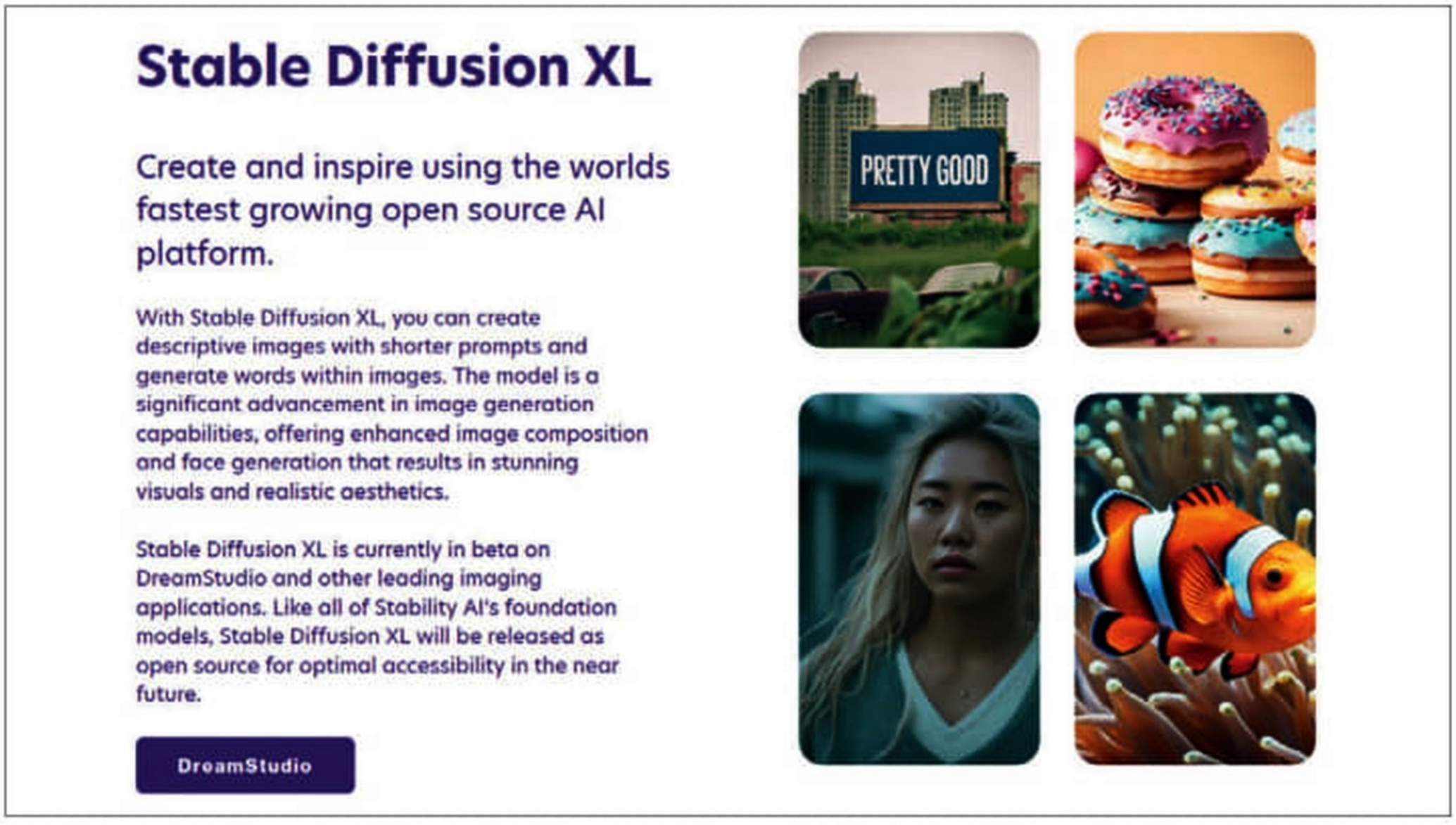
Balivernes et vol caractérisé d'images

Le patron de Stability AI est toujours animé par la même fascination pour l'intelligence artificielle, qu'il veut *« transparente et accessible à tous »*. Il fait pourtant partie des cosignataires de la lettre ouverte de quelques personnalités — comme Elon Musk — qui s'inquiètent du danger que pourrait représenter le développement trop rapide de l'IA pour l'humanité et demandent l'interruption, pendant au moins six mois, de tous les travaux sur le sujet. Ne serait-ce pas plutôt au moins pour Mostaque et Musk pour prendre de l'avance sur les autres ou du moins ne pas se faire doubler ? Il n'est, comme d'ailleurs le patron de Twitter, pas à une incohérence prête. Son générateur d'images a été lancé avec très peu de restrictions sur les représentations sexuelles ou violentes, par exemple. *« C'est aux gens de savoir s'ils sont éthiques, moraux et respectueux de la loi »*, a-t-il défendu sans gêne aucune dans le journal The Verge. Sa morale et sa notion de légalité semblent assez souples. Le fait d'avoir entraîné son modèle sur des banques d'images de Getty Images sans se soucier aucunement d'en posséder ou non les droits le montre assez clairement. Quel que soit l'avis que l'on ait sur la question de la propriété intellectuelle, il est assez étonnant qu'un patron d'entreprise numérique se permette ce genre de choses, même si des Apple et autres Facebook ne se sont guère gênés avec les droits des autres dans le passé. □

T.T

CONVERSION DE TEXTE EN ANIMATION

Vous avez peut-être déjà entendu parler de la conversion de texte en image ? Il est également possible de convertir du texte en animation grâce à l'IA. C'est ce que fait principalement Stable Diffusion. Ses modèles permettent de générer des animations à partir de simples textes. L'outil nommé plus précisément Stable Animation SDK donne la possibilité de générer des vidéos à partir de trois types de sources différentes : du texte (seul), du texte avec une image initiale ou encore du texte avec une vidéo initiale. Ce n'est pas pour autant un outil pour béotiens. Des compétences techniques assez avancées sont nécessaires pour l'installer et le faire fonctionner. Il est bien plus complexe à prendre en main qu'un DALL-E ou un Bing Image Creator, par exemple. Il n'est pas gratuit. Le coût d'une opération est basé sur un système de crédit et va varier en fonction des dimensions de la vidéo et du mode de rendu 3D.



Les modèles de Stable Diffusion permettent de générer des animations à partir de trois types de sources différentes : du texte (seul), du texte avec une image initiale ou encore du texte avec une vidéo initiale.

Slack La sécurité au cœur des solutions

Au cours des dernières années, Slack s'est imposé comme une plateforme collaborative de référence au sein des entreprises de toutes tailles. Elle offre des gains de productivité immédiats aux différentes équipes métiers tout en permettant un passage accéléré et en souplesse au modèle de travail hybride qui s'est imposé depuis la pandémie mondiale.

En ayant une place centrale au sein des organisations, Slack a toujours prêté une attention particulière à la sécurité. Ainsi tous les aspects de la collaboration entre les utilisateurs et de la gestion de projets dans Slack sont protégés par un système de sécurité de niveau professionnel sans impact sur l'ergonomie ; ceci afin que les clients puissent tirer le maximum de Slack et travailler le plus efficacement possible. Larkin Ryder, Senior Director, Product Security décrit les avantages des solutions Slack pour une meilleure sécurisation des communications des entreprises.

Quelles sont les spécificités de Slack qui en font une solution particulièrement sécurisée ?

Larkin Ryder : La sécurité de niveau entreprise est intégrée à chaque aspect du produit Slack, ce qui en fait un moyen plus sûr de communiquer et de collaborer que les applications de messagerie ou de communication grand public. Le courrier électronique nécessite des couches supplémentaires pour se protéger en permanence contre les spams et les attaques de phishing. Slack est conçu pour être une solution de collaboration plus sécurisée, et nous nous efforçons de prévenir et d'éliminer les principaux risques de sécurité liés aux e-mails.

Par ailleurs, alors que certaines applications grand public offrent un chiffrement de bout en bout, les entreprises ont généralement besoin d'accéder aux données des employés à des fins de conformité. Elles doivent donc trouver un équilibre entre la protection des communications d'entreprise et la garantie d'une gouvernance et d'une surveillance efficaces. Une véritable communication de niveau entreprise repose sur des fonctionnalités prenant en charge les deux modèles.

Pouvez-vous détailler le concept de « défense en profondeur » ?

Il s'agit d'un investissement constant et régulier. Ce concept de « défense en profondeur » signifie sécuriser notre organisation et les données de nos clients, à tous les niveaux. Nous continuons de d'intégrer dans nos solutions des certificats de sécurité répondant aux principales normes actuelles, offrons des solutions pour aider les entreprises à remplir ses obligations en matière de conformité et employons des mesures draconiennes sur les plans architecturaux et opérationnels pour garantir la sécurité de vos données

Quels conseils donneriez-vous aux entreprises victimes de ces attaques, particulièrement dans un contexte de travail hybride ?

Les cyberattaques continuent de gagner en ampleur et en complexité. Les hackers ont profité du changement au cours des deux dernières années pour créer des exploits sans précédent. Bien qu'il n'y ait aucun moyen d'éliminer ces types de menaces, il existe des pratiques pour les dissuader tout en continuant à profiter des avantages du travail hybride :

- Reconnaître ces risques
- Réduire la dépendance au courrier électronique
- Proposer à ses employés des outils d'entreprise
- Renforcer les contrôles de gestion des identités et des appareils
- Adopter un changement de mentalité en matière de sécurité.

À propos de Larkin Ryder

Larkin Ryder dispose de plus de 25 ans d'expérience dans le domaine de l'IT dont 20 ans dans le secteur de la sécurité. Elle a travaillé pour les plus grandes entreprises de la Silicon Valley, parmi lesquelles, Twitter ou HPE. Elle a intégré Slack en 2016 et occupe aujourd'hui les fonctions de directrice de la sécurité au sein de l'entreprise. A ce titre, elle encadre une équipe dédiée en charge de la sécurité de l'entreprise et des produits & solutions fournis par Slack à ses clients. Elle est diplômée en science informatique ainsi qu'en biologie, tous deux délivrés par l'université de Vermont. Elle est également titulaire de nombreuses certifications de compétences dans le domaine de la sécurité informatique et la protection des données et de la vie privée.

Méthode

Le renseignement offensif, ou comment tout savoir sur tout le monde

L'auteur est détective privé en Belgique et a compilé les différentes méthodes, trucs et astuces à disposition des attaquants pour profiler une cible ou pour apprendre beaucoup sur sa vie et ses habitudes. Il révèle ce que beaucoup de services de renseignements ou autres utilisent de manière quotidienne et simple pour cerner quelqu'un. À portée de tous, l'ouvrage est aussi une sonnette d'alarme sur nos usages sur les réseaux sociaux ou dans notre vie numérique, laissant de nombreuses clés pour ouvrir la porte de notre vie par le vol d'identité ou d'autres types d'attaques. Bref, un ouvrage salutaire pour ce numéro de rentrée. Visant cependant un public de professionnels, il complète largement ce qui est à disposition pour les spécialistes de la veille concurrentielle, sociétés de recouvrement de créances, notaires, juristes spécialisés en droit des affaires ou de la propriété intellectuelle, dirigeants de PME, responsables du marketing, du recrutement, ou de la sécurité.

LINKEDIN

Votre concurrent est-il actif sur LinkedIn ? Probablement. Mais en dehors de ses formidables fonctions de sourcing, LinkedIn est moins intéressant en matière d'analyse compétitive que d'autres sites. Tout simplement parce que votre concurrent ne vend pas ses produits ici. En dehors de l'analyse compétitive, LinkedIn est bien entendu une source d'informations sur les personnes. Vous aurez des données, non vérifiées, sur la scolarité et les différents jobs de la personne. Souvent dans nos métiers, nous ne souhaitons pas être identifié. Or, sur LinkedIn, lorsque vous visitez un profil, la cible sera notifiée de votre passage. Il s'agit d'un paramètre par défaut. Il est possible de modifier vos paramètres pour ne pas être identifiable.

Cliquez sur l'icône « Vous » en haut de la page d'accueil de votre compte puis cliquez sur « Voir le profil », cliquez sur « préférences et confidentialité ». Vous allez sur « confidentialité », dans la section *« Comment les autres voient votre activité sur LinkedIn »*, cliquez sur *« options vues de profil »*. Une liste déroulante va s'ouvrir, c'est le module *« Sélectionner ce que les autres voient lorsque vous consultez leur profil »* qui va s'afficher. Vous cliquez sur « Utilisateur LinkedIn Anonyme ». La personne saura que son profil a été visité, mais ne pourra pas vous identifier. Si vous êtes hautement paranoïaque, ou que pour une raison ou une autre vous devez aller régulièrement sur un profil et ne voulez pas éveiller la méfiance de votre cible, il est tout à fait possible de voir un profil sans que la personne ne sache qu'on est venu sur son profil. Cela prend juste quelques minutes.

Pour commencer, vous tapez le nom de votre cible sur votre moteur de recherche habituel, accompagné du mot « LinkedIn ». Vous voyez en tête de page le profil de votre cible. Vous allez sur le titre du lien et vous utilisez le clic droit de votre souris. Cliquez sur « copier le lien ».

Ensuite, vous allez sur https://search.google.com/test/mobile-friendly qui à la base, sert à savoir si une page web est compatible avec votre téléphone. Vous copiez le lien dans la barre de recherche et vous verrez apparaitre le profil LinkedIn de votre cible. Mais comme le profil sera incomplet, vous cliquez sur « html » en haut à droite de la page. La suite de codes qui apparait est peu soluble dans mon intelligence. Difficile à utiliser. Alors, je clique sur le bouton « copier ».

Ensuite, vous ouvrez la page https://codebeautify.org/htmlviewer et vous collez l'information qui se trouve dans le presse-papier. Enfin, vous cliquez sur le bouton « run » et vous obtenez le profil de la cible.

Pour en revenir à votre concurrent, commencez par faire une recherche pour voir s'il possède un compte LinkedIn. Si vous ne le trouvez pas, c'est soit que vous avez mal cherché (recommencez !), soit que votre concurrent n'est pas très dangereux.

Passe-t-il des annonces sur LinkedIn ?

Pour accéder aux annonces d'une page commerciale LinkedIn, allez sur la page et cherchez l'onglet "Ads" à gauche. Cliquez sur cet onglet et vous verrez une liste d'annonces associées à la page.

Vous ne pouvez pas afficher les commentaires ou les interactions sur les annonces LinkedIn directement à partir de la section annonces, mais vous pouvez consulter ces informations de manière détournée.

Cliquez sur les trois points en haut à droite d'un message et sélectionnez *« Copier le lien vers le message »*. Ensuite, collez ce lien dans votre navigateur pour afficher le message en question, ainsi que les commentaires éventuels.

Localiser une personne via LinkedIn

Sous le titre d'un utilisateur et avant son nombre de connexions, vous trouverez sa localisation. Il s'agit d'un autre champ obligatoire, mais ne vous y fiez pas trop, car les utilisateurs peuvent choisir ce qu'ils veulent ici sans aucune validation. De plus, les utilisateurs peuvent modifier ce champ comme ils le souhaitent, et ce, autant de fois qu'ils le souhaitent. Le champ peut être aussi large que le pays ou aussi précis qu'une ville ou une zone métropolitaine. Les données de localisation de votre cible peuvent facilement contribuer à réduire le champ des correspondances potentielles à des degrés divers, mais elles doivent être vérifiées à l'aide d'autres points du profil si possible.

Cependant, avec un peu de recherche, nous pouvons parfois réduire leur localisation. Imaginons que votre cible soit un ingénieur et son profil nous dit qu'il habite en région parisienne. Si les informations données sur le profil sont correctes, croisez la région avec l'entreprise où il travaille actuellement, et vous obtenez son adresse professionnelle. Un simple appel téléphonique à la réception de l'entreprise vous confirmera si vous avez trouvé votre cible ou non. Cela ne vous donne pas son adresse privée, mais réduit fortement le champs de recherche à un rayon maximum de deux heures de transport autour de son entreprise.

Il existe cependant un moyen d'obtenir l'adresse privée de votre cible via LinkedIn : lui envoyer une offre d'emploi qui soit à la fois crédible et qui donne envie de vous répondre. Si la cible est intéressée, demandez-lui de vous envoyer son CV et vous avez son adresse. Vous pouvez l'envoyer en même temps qu'une demande de connection.

Pour ça, vous avez trois options :

a) Utilisez votre vrai profil. Cette option est la plus simple mais aussi la plus improbable. Si vous êtes détective privé ou journaliste, envoyer une offre d'emploi ne vous renverra certainement pas du bonheur.

b) Demandez à quelqu'un que vous connaissez et qui a un profil acceptable pour la mission d'envoyer cette offre d'emploi.

c) Créer un faux profil pour l'occasion. Ce n'est pas si compliqué, mais ça prend du temps et vous devrez prendre certaines précautions. LinkedIn traque les faux profils et les règles de sécurité sont de plus en plus strictes. LinkedIn utilise une intelligence artificielle qui détecte beaucoup de faux profils mal construits. Voici les étapes :

- Créer une nouvelle session chrome dédiée à votre faux profil. Si vous ne le faites pas, Linkedin découvrira des cookies partagés et au revoir.
- Créer un faux nom qui tient la route. Ni trop commun ni trop bizarre. Vous pouvez utiliser un générateur de fausse identité comme www.fakenamegenerator.com
- Créer une adresse email dédiée. Eviter les trucs trop exotiques comme Yopmail ou quelque chose se terminant en « .ru ». Une adresse Gmail sera très bien, pour le moment. Attention qu'à l'avenir, LinkedIn pourrait demander une confirmation avec une adresse professionnelle.
- Il vous faut une photo. Mais surtout, surtout, n'allez pas prendre une photo trouvée sur le net. Vous seriez disqualifié. Utilisez https://unsplash.com/ pour obtenir une photo libre de droit. Ou mieux encore https://generated.photos/ qui vous créera une photo d'une peronne qui n'existe pas. Vous pouvez l'essayer trois jours gratuitement, ça devrait être suffisant.
- Ensuite, vous créez votre compte en le complètant au minimum à un niveau intermédiaire. Utilisez un vpn, afin que votre adresse ip soit dissimulée. Précaution utile car si Linkedin détecte que votre ip est déjà utilisée, votre nouveau profil sera rejeté. Ça m'est arrivé.
- N'oubliez pas de vous faire de nouveaux amis en faisant des demandes de connection à vos relations du deuxième degré. Likez des posts, vous aurez l'air encore plus vrai.

En cliquant sur le bouton « plus », vous pouvez savoir quand le profil a été créé et quand il a été mis à jour. Tout le monde ne le sait pas, mais le risque existe que votre cible découvre que votre profil a été créé la semaine passée.

LinkedIn et la recherche inversée de photos

La photo de profil et l'image d'arrière-plan d'un profil LinkedIn peuvent être téléchargées et faire l'objet d'une recherche d'image inversée à l'aide de n'importe quel moteur de recherche d'images. Pour n'en citer que quelques-uns : Google Images, Yandex Images, Tin Eye, Shutterstock, etc.

En cliquant sur la photo de profil, on obtient l'image agrandie. On peut faire de même en ajoutant « /detail/photo » à l'URL du profil.

Une fonctionnalité utile que possède tout profil LinkedIn est la possibilité de télécharger le contenu du compte dans un document de type CV grâce à l'option « Enregistrer en PDF ». Vous ne téléchargerez pas d'informations ou d'activités personnelles, mais seulement un aperçu du profil.

Fouiller un profil LinkedIn

Le nom de famille d'un utilisateur peut être masqué en raison de ses paramètres de confidentialité. Cependant, il y a quelques éléments que nous pouvons examiner pour découvrir le nom de famille complet.

On peut également examiner le reste de la page et rechercher des indices susceptibles de confirmer le nom de famille, tels que des fichiers, des avenants, etc.

TITRE

Le titre apparaît sous le nom de l'utilisateur dans le profil et est également un champ obligatoire. Par défaut, il est tiré des informations sur le travail ou la formation initiale fournies par l'utilisateur lors de son inscription. Ce champ doit être modifié séparément de l'expérience professionnelle et de la formation, ce qui signifie qu'un utilisateur peut supprimer son expérience professionnelle ou sa formation initiale et, s'il oublie de mettre à jour son titre, celui-ci peut encore contenir ces informations. En plus de ce titre initial, les utilisateurs peuvent également modifier ces informations pour qu'elles contiennent des informations qu'ils veulent que les autres voient en premier lieu.

CONNEXIONS

Le nombre de connexions apparaît après les informations de localisation sur un profil et peut ou non être affiché en fonction des paramètres de confidentialité de la cible et de votre connexion avec la cible.

Si les informations sont visibles, les enquêteurs peuvent cliquer sur l'hyperlien bleu pour ouvrir la liste des connexions, sinon elles apparaîtront en texte noir et ne seront pas cliquables.

Les informations de localisation sont suivies d'un lien permettant d'afficher les coordonnées de l'utilisateur dans une fenêtre contextuelle. L'exploitation des informations de contact peut s'avérer difficile selon la quantité d'informations fournies par l'utilisateur et si vous êtes une personne de premier degré ou non. Malgré le nom de cette section, elle peut contenir bien plus que de simples informations de contact. Cette section contiendra, au minimum, l'URL du profil. Elle peut également contenir le numéro de téléphone de l'utilisateur, son adresse, ses identifiants de messagerie, sa date de naissance, ainsi que les URL de ses sites Web personnels et professionnels. Il convient également de noter que, par défaut, l'adresse électronique LinkedIn est partagée avec toutes les connexions au premier degré.

À PROPOS DE

Certains profils Linkedin peuvent contenir des informations supplémentaires dans leur section « à propos », qui ne figurent pas dans la section "expérience" du profil. Comme le titre, il s'agit d'une zone de texte libre du profil qui permet à l'utilisateur de saisir tout ce qu'il juge pertinent de faire savoir aux autres utilisateurs. C'est pourquoi vous pouvez trouver des informations précieuses telles que des URL, d'autres adresses électroniques, d'autres lieux pertinents, des informations sur le travail passé et actuel, ainsi que des loisis, etc.

ACTIVITÉ

Cette section fournit un aperçu des publications récentes que l'utilisateur a commentées, partagées, aimées, etc. J'ai constaté l'absence de cette section sur certains profils, mais il est possible de la localiser en manipulant l'URL du profil pour ajouter "/detail/recent-activity/" à la fin (c'est-à-dire https://www.linkedin.com/in/nomdelapersonne/detail/recent-activity/).

Sinon, vous pouvez obtenir une vue complète de l'activité de l'utilisateur en cliquant sur le bouton « Voir tout » qui ouvrira une nouvelle vue et affichera une vue historique des entrées suivantes :

Toute l'activité : Il s'agit de la vue par défaut. Elle montre toute l'activité d'un utilisateur comme les commentaires, les likes, les partages, les posts, etc. Si cette section est modeste et pas trop longue, il peut être intéressant de collecter ces informations pour voir avec quels autres comptes la cible interagit le plus fréquemment.

Articles : Cette section affiche les articles écrits par l'utilisateur et publiés sur le site.

Messages : Contrairement à la vue de l'ensemble des activités, la section des messages n'affiche que les messages rédigés par l'utilisateur et exclut ceux qu'il a simplement commentés ou aimés. Sachez que les messages d'autres utilisateurs que la cible partage apparaîtront également ici. Cette vue peut être utile pour recueillir rapidement des informations sur la cible sans avoir à parcourir des centaines ou des milliers de messages aléatoires.

Documents : Cette vue affiche les documents téléchargés par l'utilisateur. Vérifiez qu'ils ne contiennent pas d'informations pertinentes qui auraient pu être oubliées lors du téléchargement, comme le nom du fichier, les liens intégrés ou les informations que l'utilisateur n'a pas censurées.

EXPÉRIENCE

La section "expérience" est souvent la partie la plus utilisée de LinkedIn. Par défaut, cette section comporte au moins une entrée, à condition que l'utilisateur ne se soit pas inscrit en tant qu'étudiant et qu'il n'ait pas supprimé cette information après son inscription. Chaque entrée d'expérience peut inclure un ou tous les points d'information suivants :

Titre : Il s'agit d'un champ de texte libre qui affiche le poste ou le titre de l'emploi que le sujet a occupé.

Type d'emploi : Il s'agit d'une liste déroulante de types d'emploi tels que plein temps et temps partiel, apprentissage, indépendant, etc.

Entreprise : Il s'agit d'un champ obligatoire dans lequel l'utilisateur peut indiquer le nom de l'entreprise pour laquelle il a travaillé. La connaissance de cette information permet à un enquêteur de déterminer la structure de l'e-mail utilisé pour l'envoi d'e-mails de phishing ou d'identifier un lieu si l'entreprise n'opère que dans une région spécifique.

Lieu : Il s'agit d'un champ de texte libre qui contient le lieu, généralement au niveau de la ville, où l'utilisateur a physiquement travaillé dans cette entreprise. Bien que de nombreuses fonctions puissent être exercées à distance, les utilisateurs qui travaillent à domicile peuvent indiquer leur ville de résidence dans ce champ. J'ai également vu des travailleurs à distance utiliser la ville du bureau le plus proche.

Dates de début et de fin : Cette section comprend des sélecteurs déroulants. L'utilisation des dates connues auxquelles une cible travaille pour une organisation permet à un enquêteur de rechercher les communiqués de presse et les publications sur les réseaux sociaux de l'entreprise à cette époque pour voir si l'utilisateur a été tagué ou commenté, donnant ainsi des informations sur ses autres comptes de réseaux sociaux.

FORMATION

La section "Formation" d'un utilisateur suit généralement immédiatement son expérience professionnelle. Il est important de noter que cette section contient par défaut des informations si l'utilisateur s'est inscrit en tant qu'étudiant et n'a pas supprimé ces informations après son inscription. Veillez également à effectuer des recherches sur la syntaxe de l'école pour la création d'e-mails si vous devez élaborer une tentative de phishing ciblée.

Cette section n'est pas toujours complète, mais chaque entrée peut inclure les points d'information suivants :

- Nom de l'école
- Diplôme
- Domaine d'études
- Années de début et de fin

Activités et sociétés : Formulaire de texte libre qui contient souvent les sociétés ou groupes du campus dont l'utilisateur a fait partie pendant ses études. Je ne vois pas souvent ce formulaire rempli.

Description : Un autre formulaire de texte libre, peut inclure une combinaison des informations trouvées dans ce qui précède ou peut inclure des informations concernant leurs classes ou leurs principales réalisations.

Médias : Cette zone peut contenir des fichiers qui sont téléchargés et peuvent inclure des transcriptions, des présentations ou d'autres rapports ou projets importants. Soyez attentif aux noms de fichiers qui pourraient contenir des informations supplémentaires.

EXPÉRIENCE DU BÉNÉVOLAT

La section relative à l'expérience de bénévolat est très utile pour obtenir des informations sur le mode de vie d'un utilisateur ainsi que des informations sur sa localisation. En outre, si les utilisateurs peuvent faire de longs trajets pour des emplois bien rémunérés, peu d'entre eux seront prêts à faire de longs trajets pour un travail non rémunéré, à moins qu'ils ne soient extrêmement dévoués à la mission.

RECOMMANDATIONS

Les recommandations ne sont pas le point d'exploitation le plus courant, mais les profils qui en possèdent peuvent laisser échapper une grande quantité d'informations sur un sujet via leurs recommandations données et reçues. Cela est particulièrement vrai pour les recommandations reçues, qui peuvent fournir des informations que la cible n'avait pas initialement incluses dans son profil. Plus il y a de recommandations données et reçues, plus il y a de chances que l'une d'entre elles divulgue des informations pertinentes sur votre cible.

PUBLICATIONS

Requiert un titre de publication et peut également inclure l'éditeur ou des informations sur la publication, la date de publication, un lien vers la publication, ainsi qu'une description. La meilleure façon d'exploiter ces informations est de localiser la publication elle-même, car elle peut contenir le titre de l'utilisateur, son nom (en tant qu'auteur) et d'autres informations que l'utilisateur ne partage pas forcément ailleurs dans son profil. □

« Le renseignement offensif »
par Philippe Dylewski,
éditions Agakure 2023,
495 pages,
ISBN 13 : 979-1096819010

CLUB DECISION DSI

1er Club Français de décideurs informatiques & télécoms
1250 MEMBRES

Véronique Daval
Présidente

Un réseau indépendant et privé au sein duquel siègent 11 DSI ambassadeurs de leur secteur d'activité

Julien Daval
Vice-Président

LES MEMBRES DU BUREAU ET AMBASSADEURS DU CLUB

Armand ASSOULINE
CIO
MSC FRANCE

Christian DOGUET
DSI
CHAINE THERMALE DU SOLEIL

Trieu HUYNH-THIEN
DSI ADJOINT
CENTRE GEORGES POMPIDOU

Dominique TROUVE
DSI
HÔPITAUX AVICENNE

Gilles BERTHELOT
RSSI
GROUPE SNCF

Damien GRIESSINGER
CTO
EPPO

Stéphane MALGRAND
DSI
Laboratoire national de Métrologie et Essais

Claude YAMEOGO
ARCHITECT SI
ALSTOM

Christophe BOUTONNET
SOUS-DIRECTEUR
SCHÉMA DIRECTEUR ET POLITIQUE SI

Christophe GUILLARME
DSI
GROUPE AB TÉLÉVISION

Lionel ROBIN
DSI
GROUPE LA RESERVE

Le Club accompagne les DSI à faire les bons choix technologiques et aligner l'informatique sur la stratégie de l'entreprise

EVOLUTION DU CLUB DECISION DSI

LES MEMBRES DU CLUB

1200 CIO, DOSI, DSI, DI Membres du Club, sociétés de + 300 salariés PARIS/IDF

TAILLE SALARIALE

SECTEURS D'ACTIVITÉ

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

@clubdecisiondsi

Industrie du luxe

Le numérique pour personnaliser les offres

Le Numérique n'est plus un intrus dans l'industrie du luxe, surtout depuis la Covid. Au contraire, ses outils et logiciels motorisent toute la « Beauty Tech » car ils aident les grandes maisons de luxe à se démarquer, comme nous l'ont expliqué plusieurs d'entre elles sur le salon Viva Tech 2023.

Longtemps méfiantes à l'égard du Numérique et d'Internet, les grandes maisons spécialisées dans le luxe (mode, cosmétiques, bijouterie, *etc.*) sont nombreuses à avoir changé d'avis dès 2020. Et pour cause, le visitorat de leurs magasins physiques s'était raréfié pendant les confinements successifs de la pandémie Covid.

Séduire les « Digital Natives » et les générations Y et Z

Les enseignes du luxe ont donc décidé d'utiliser de manière plus systématique — une nouveauté — des outils numériques afin d'augmenter leurs visitorats en magasin, mais aussi pour élargir l'expérience omnicanale des clients au-delà de leurs murs. Toutes veulent ainsi séduire les « Digital Natives » et la génération Z. À juste titre, puisque des études indiquent que ces derniers représenteraient près de 30 % des achats de luxe aujourd'hui. Celle réalisée fin 2019 par le cabinet Bain & Company révèle que la part de marché dans le luxe des générations Y et Z pourrait bondir à 80 % d'ici à 2035 !

Pourtant, *« il a été longtemps inenvisageable pour les acteurs du Luxe de se positionner sur Internet »*, explique Bruce Leduc, analyste de marché de l'intégrateur digital SQLI. *« D'un point de vue technique, le numérique n'a pas immédiatement été en mesure de fournir au secteur du luxe les innovations permettant aux consommateurs de vivre l'expérience souhaitée. Mais le numérique diversifiant son éventail d'opportunités pour les marques au fil des années, il est devenu impossible pour ces enseignes de s'en passer »*.

© Marie rouge

© Olivier Bellin

Miroir, miroir, dis-moi qui est la plus belle !

Effectivement, les grandes maisons de luxe ont rivalisé en termes d'innovations sur le salon Viva Tech 2023. Toutes présentaient cet été une ou plusieurs solutions numériques de « Beauty Tech ». Certaines combinaient la gestion et l'essayage d'objets (robes, sacs à main, lunettes, *etc.*) en réalité augmentée pour améliorer l'expérience utilisateur sur site ou en ligne.

Traités comme des VIP lorsqu'ils s'abonnent à ce type de service, les visiteurs de leurs stands pouvaient également utiliser ce type d'outils pour tester des maquillages ou maquiller leurs avatars sur Teams ou sur les réseaux sociaux. De grandes marques (LVMH, L'Oréal, *etc.*) proposaient aussi l'achat d'images virtuelles (NFT) aux clients voulant également s'offrir des baskets ou des sacs à main de luxe virtuels en série très limitée. Enfin, les visiteurs ont aussi pu tester des scanners afin de vérifier l'état de leur peau, de leur cuir chevelu, *etc.* (voir encadré ci-contre).

Le numérique devient aussi un outil de support et d'aide à la vente collaborative pour les vendeurs des boutiques de luxe qui, s'ils sont bien formés, se muent alors en conseillers « augmentés ». *« Nos vendeurs doivent être digitalisés pour être au cœur de la relation client »* estime Franck Le Moal,

le directeur des innovations de LVMH. Sur VivaTech, ceux de Dior (LVMH) montraient aux visiteurs comment accéder à distance à des experts beauté ou à des stylistes afin d'obtenir des conseils beauté, mode, *etc*, depuis un miroir (écran) connecté accessible *via* Teams par exemple. Il est d'autant plus facile pour ces vendeurs de les influencer qu'ils collectent leurs préférences déclarées sur le site de la marque, mais aussi sur les réseaux sociaux. Avec la complicité de certaines influenceuses ?

Des revenus additionnels et une meilleure reconnaissance des DSI

La commercialisation effective, dès fin 2023, de la plupart de ces nouveaux terminaux et outils numériques révèle deux choses. Primo, les marques de luxe veulent générer de nouvelles lignes de revenus additionnels, récurrents de préférence, sur la base de nouveaux services de conseil vendus autour de leurs produits. Elles ont donc dépassé le stade de l'expérimentation à petite échelle car elles estiment, de concert, qu'il existe enfin une fenêtre de tir propice à l'introduction commerciale de leurs solutions numériques de « Beauty Tech », au moins dans certains pays développés. Cette stratégie est une source importante de nouveaux budgets pour leurs DSI, mais aussi pour les développeurs, les éditeurs et les sociétés de services IT (ESN).

Secundo, ces enseignes partagent une même ambition, qui est d'industrialiser le mariage du e-marketing et du Numérique pour fidéliser une clientèle accro aux réseaux sociaux et demandeuse de davantage de personnalisation et d'exclusivité. Avant cette approche, la satisfaction de ces demandes était réservée à la clientèle très fortunée visitant leurs magasins de luxe physiques, lesquels demeurent des piliers centraux dans leurs stratégies commerciales... grâce au Numérique désormais.

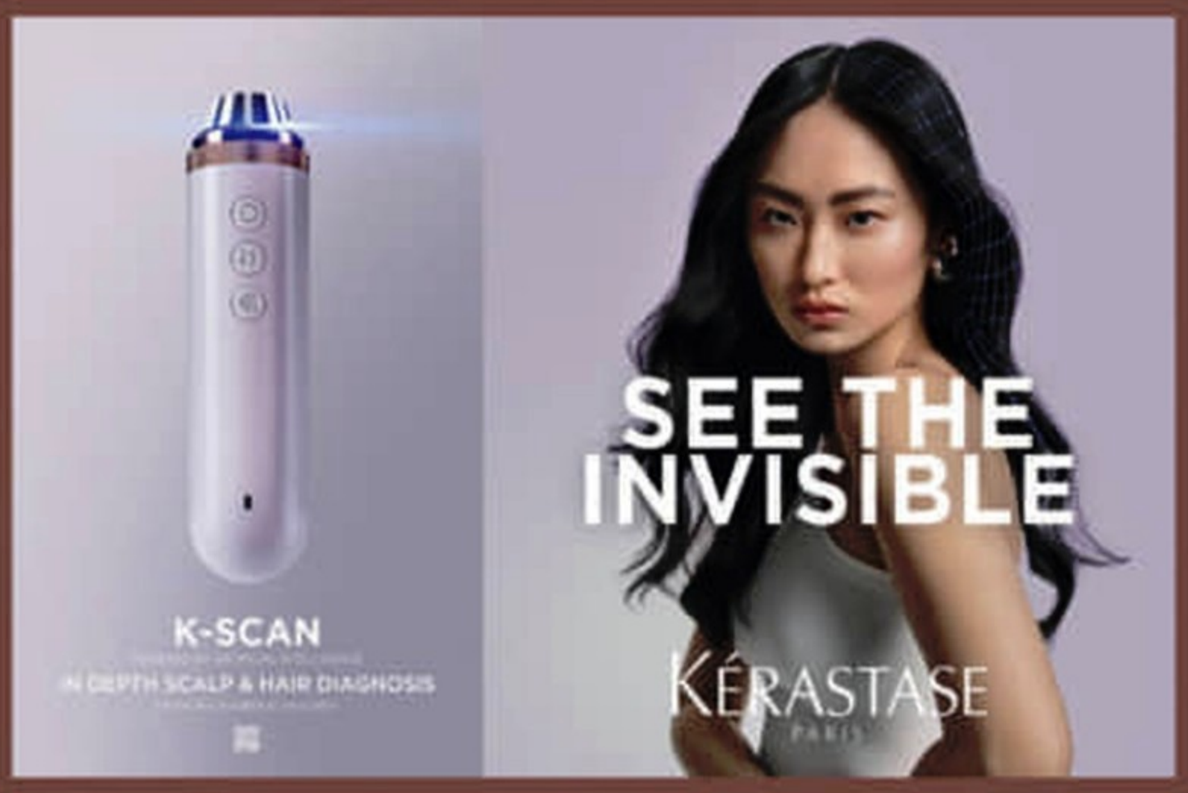
Et si leurs sites d'e-commerce leur capturent quelques parts de marché, essentiellement sur une tranche de la clientèle plus jeune, on l'a vu, ils en drainent un certain nombre vers eux dans une logique de « web-to-store ». D'autant que leurs catalogues de produits sont souvent moins larges que ceux des produits en boutique. L'e-commerce aurait dépassé 10 % du chiffre d'affaires total d'un géant du luxe comme LVMH.

Alors quoi de neuf sous le soleil, me direz-vous, car Burberry, Gucci, Hermès et Tiffany, figurent parmi les premières marques de luxe à avoir testé la vente en ligne il y a presque 20 ans. Effectivement, pas grand-chose dans l'absolu car la plupart de ces technologies numériques existent depuis des années. « *En revanche, leur appropriation systématique et combinée par autant de marques de luxe, et surtout le niveau de maturité plus élevé de leurs solutions, montrent clairement que leurs DSI ne sont pas les seules à prendre le numérique au sérieux désormais* », nous a déclaré un DSI du secteur du luxe.

Le numérique permet donc aux marques de luxe d'hyper personnaliser enfin leurs offres pour que chaque consommateur ait l'impression d'être unique. Le Graal ! Mais pour quel retour sur investissement ? Ces enseignes et leurs DSI restent très discrètes sur leurs investissements dans ces outils... et sur les plâtres essuyés. □

Olivier Bellin

L'ORÉAL MULTIPLIE LES INNOVATIONS



Le leader mondial des produits de beauté a présenté au salon VivaTech 2023 plusieurs solutions de « Beauty Tech ». L'Oréal utilise désormais le numérique afin d'hyper personnaliser ses produits et traitements vendus en mode premium, tant sur site qu'en ligne. Et parmi eux, la caméra K-Scan de Kérastase. Ce scanner mobile n'équipera dès l'automne que les salons de coiffure de son réseau dans certains pays. Sa caméra utilise trois types de lumière (blanche, polarisée croisée et UV) pour scanner les cheveux et analyser ensuite leur état avec de l'intelligence artificielle. Fort de ces informations « objectives » issues des images HD obtenues avec la K-Scan, les coiffeuses pourront alors réaliser des recommandations très personnalisées... et des ventes additionnelles. L'Oréal démontrait aussi d'autres outils de diagnostic et de coaching, tels que le Spotscan de La Roche-Posay, ou encore le scanner de peaux Meta Profiler de Giorgio Armani.
L'Oréal présentait également des outils virtuels utilisables en ligne et à domicile, comme le 3D shu: brow de Shu Uemura, une imprimante portable pour « sculpter » les sourcils sur la base d'un scan du visage et d'une technologie de réalité augmentée. Enfin, l'application Maybelline Beauty App propose aux utilisateurs de Microsoft Teams un relooking et un maquillage virtuel. La plupart de ces produits et services seront disponibles dans certains pays dès fin 2023.

Conformité

Le Data Act, atout ou menace pour l'industrie européenne ?

Bataille de chiffres autour du Data Act, le nouveau règlement européen relatif au partage des données dans l'Union européenne. La Commission y voit un énorme gisement de croissance, les industriels une menace sur leur Business Model.

Selon les technocrates de Bruxelles, 270 milliards d'euros supplémentaires d'ici à 2028, soit près de 2 % de PIB, c'est le surplus de croissance que devrait générer le Data Act. La logique est simple ; puisque les GAFAM ont la mainmise sur les données des citoyens européens, les contraindre à entrouvrir leurs entrepôts de données aux start-up digitales et entreprises européennes devrait permettre de ramener de la valeur sur le vieux continent. C'est aussi un moyen de valoriser ces 80 % des données industrielles générées au sein de l'Union européenne qui ne sont pas encore exploitées.

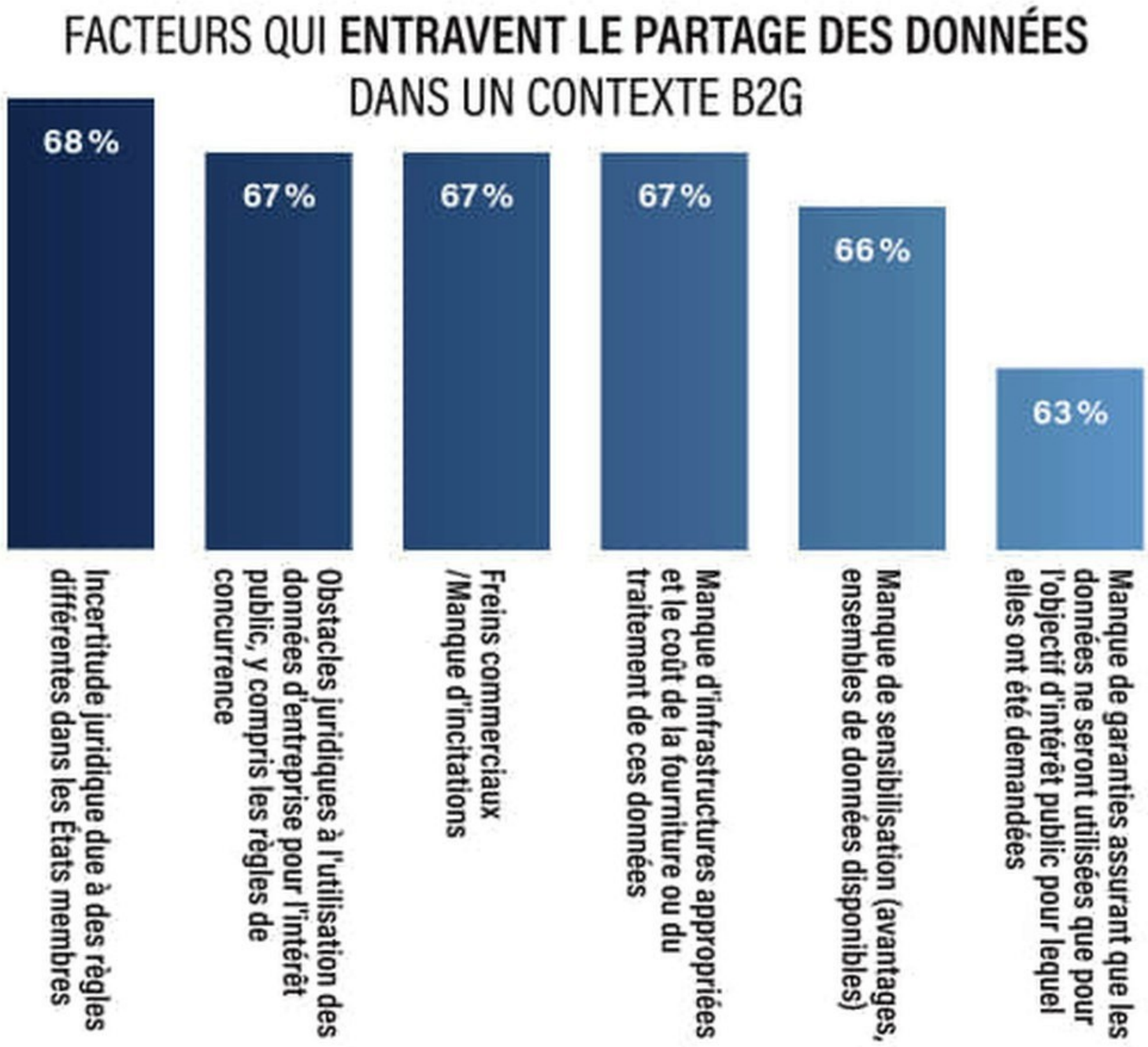
Selon eux, la régulation de l'économie des données doit générer ce pactole en jouant sur 4 grands leviers. D'une part, le texte doit permettre aux utilisateurs de dispositifs connectés d'avoir accès à leurs données et les partager librement avec des tiers. Les auteurs du texte espèrent que cette mesure stimulera la fourniture de nouveaux services. Le deuxième point porte sur le rééquilibrage des relations entre PME et grandes entreprises dans les contrats de partage de données. La Commission va rédiger des clauses contractuelles type pour que ces contrats soient équitables. La Commission veut aussi que le secteur public puisse accéder aux données en cas d'urgence (le texte évoque les cas d'inondation, de feux de forêt) ou pour exécuter un mandat juridique. Enfin, l'Europe veut mettre en place de nouvelles règles afin de faciliter les changements de fournisseurs de services de traitement de données Cloud, tout en prenant des garanties contre les transferts illicites de données.

MAÎTRE SARDAIN, ASSOCIÉ CHEZ JEANTET

Le Data Act instaure plusieurs mesures importantes et novatrices qui s'imposent aux entreprises telles que :

- l'obligation de portabilité et d'accès des données qui sont générées par les produits connectés ;
- le renforcement de l'exigence d'interopérabilité entre les services de cloud ;
- la mise en place de garanties contre les accès illicites de gouvernements de pays tiers aux données non-personnelles contenues dans le cloud ;
- la mise en place de mécanismes permettant aux organismes du secteur public et institutions, organes ou organismes de l'Union d'accéder aux données détenues par le secteur privé et de les utiliser en raison d'un besoin exceptionnel (par exemple, en cas d'urgences publiques telles que les incendies ou inondations) ;
- l'interdiction des clauses abusives relatives à l'accès aux données et à la réutilisation des données interentreprises qui seraient imposées unilatéralement à une micro, petite ou moyenne entreprise.

À cet égard, l'objectif principal de ce nouveau cadre juridique est d'harmoniser les règles et faciliter l'accès et le partage des données générées (notamment industrielles, mais aussi personnelles) entre entreprises (B2B), entre entreprises et consommateurs (B2C) et entre entreprises et gouvernement (B2G).
Son application est très large puisqu'il concerne les acteurs publics et privés du marché de la donnée sur le territoire européen. Il s'applique notamment aux fabricants d'objets connectés, aux fournisseurs de services en ligne, aux plateformes de cloud, aux constructeurs industriels dont les produits génèrent des données (santé, automobile...) ainsi qu'aux grandes entreprises technologiques en général.



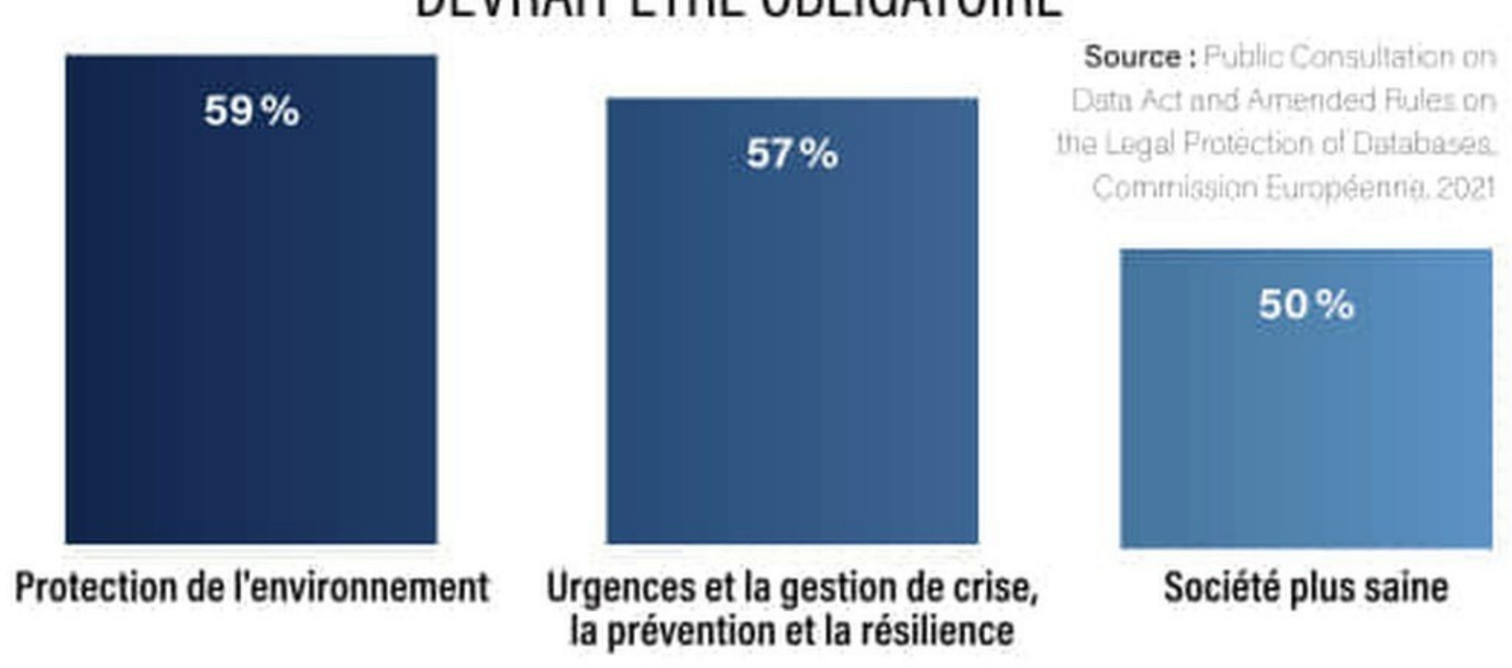
Alors que l'Europe reste à la traîne des États-Unis sur le digital, fluidifier le marché européen à du sens, mais toutes les entreprises européennes ne sont pas du même avis. En octobre 2022 déjà, l'ETNO (Association européenne des opérateurs Télécom) publiait une étude pointant les coûts du Data Act, de l'ordre de 410 millions d'euros d'investissements pour l'industrie, puis 88 millions par an de coûts récurrents, mais aussi demandant que les données de trafic (de type ECS) soient exclues du périmètre du Data Act.

Plus récemment, c'est l'industrie allemande qui est montée au créneau contre le texte. En mai dernier, les CEO de Siemens Healthineers, Siemens AG, SAP SE publiaient une lettre ouverte destinée à la Commission, soulignant tous les dangers de ce texte. Leurs arguments sont multiples : augmentation des coûts de traitement des données venant s'ajouter à ceux engendrés par le RGPD, dégradation de la sécurité du fait de l'obligation de faciliter l'accès et le partage des données, risque accentué de divulgation des secrets industriels par l'obligation de partager les données industrielles. Enfin, les industriels allemands dénoncent une baisse de leur compétitivité face à des rivaux internationaux non concernés par le « Data Act ».

De facto, cette ouverture du marché de la Data à l'échelle du continent va entraîner un certain nombre d'obligations pour les industriels qui vont au-delà du RGPD. Maître Sardain, associé chez Jeantet, cabinet d'avocats internationaux, souligne : *« le "Data Act" oblige les entreprises à rendre accessibles les données générées par l'utilisateur d'un produit ou d'un service. Cela implique que lesdits produits et services doivent être conçus dès l'origine pour que les données soient facilement accessibles. À ce titre, l'entreprise devra respecter le principe du "privacy by design" prévu par le RGPD. »* De plus, le texte renforce le RGPD, notamment sur les droits d'accès et de portabilité. L'avocat ajoute que *« le "Data Act" impose aux entreprises de prendre toutes les mesures techniques, juridiques et organisationnelles afin d'éviter le transfert international ou l'accès gouvernemental à des données non personnelles détenues dans l'Union lorsque cela pourrait créer un conflit avec le droit de l'Union ou droit de l'État membre concerné »*. Enfin, les entreprises vont devoir publier des informations liées à la nature des données qu'elles partagent dans *« un format clair et compréhensible »*, une obligation nouvelle qui vient s'ajouter aux exigences de transparence et d'information prévues aux articles 12 à 14 du RGPD, prévient Maître Sardain...

Le 27 juin 2023, le Conseil et le Parlement européen sont parvenus à un accord « politique » sur ce projet. On devrait assister à une bataille de lobbies à Bruxelles jusqu'à l'adoption définitive d'un texte qui devrait s'appliquer entre mi/fin 2025. □

AC



Source : Public Consultation on Data Act and Amended Rules on the Legal Protection of Databases. Commission Européenne. 2021

Cloud

Oracle University propose un programme gratuit

Le manque de ressources est une antienne que tout le secteur informatique entonne depuis des mois. Pour essayer de limiter les conséquences de ce manque, Oracle University propose des formations et des certifications gratuites.

Disponible dans le monde entier, le nouveau programme inclut des formations et une certification sur des compétences recherchées pour Oracle Cloud Infrastructure (OCI), l'IA et le ML, la gestion des données et les applications SaaS. Oracle Fusion Cloud est accessible à tous les professionnels de l'industrie IT, quel que soit leur niveau de compétence et leur poste. Il est disponible en 13 langues et vise à aider les apprenants à acquérir des compétences très demandées, en particulier celles liées à la conception et à l'implémentation de solutions à l'aide d'OCI, de l'IA et du ML et de la gestion des données, ainsi qu'à Oracle Fusion Applications. Le cursus comprend différents parcours de formation numériques à la demande qui fournissent tous les éléments nécessaires, depuis les cours de préparation jusqu'aux examens de mise en pratique en passant par les tests et les informations d'identification. Ces formations étaient disponibles officiellement jusqu'au 31 août 2023. Il est fort possible, vu les tensions sur le marché, que ce programme soit étendu. La formation numérique sur OCI restera accessible gratuitement.

Des formations reconnues

Le programme gratuit de certification d'Oracle comprend l'accès à l'ensemble du catalogue de formation numérique, des sessions en direct enseignées par des experts d'Oracle, une expérience de certification Oracle complète ainsi que des ressources de carrière pour les certificats suivants :

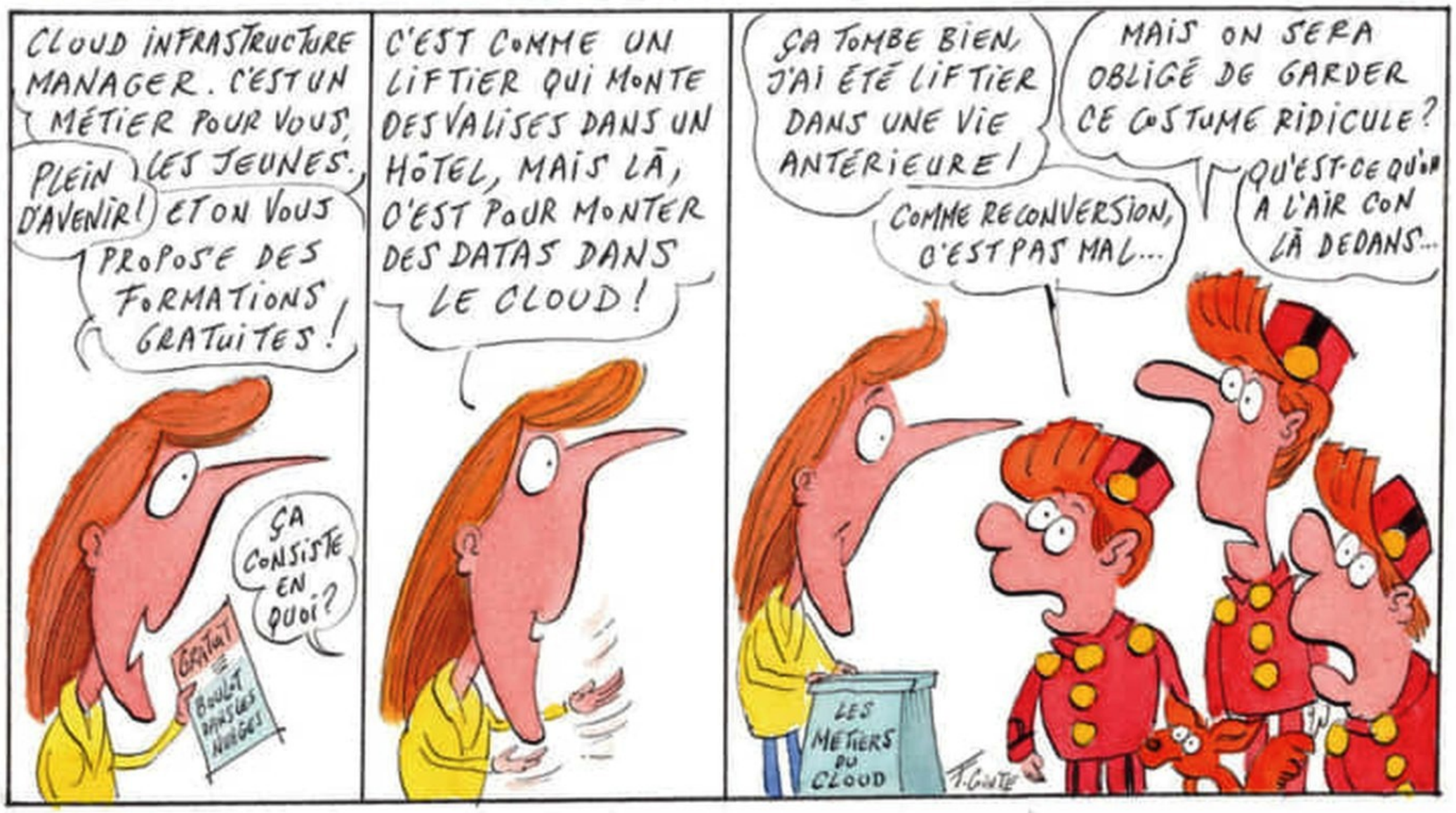
Oracle Cloud Infrastructure (OCI) Certification : couvre l'IA/ML, les analyses, l'architecture, le développement cloud, les opérations cloud, le DevOps et la sécurité.

Oracle Data Management Certification : couvre Database Migration and Integration, Autonomous Database, Oracle Database Services et Oracle APEX (« Application Express », le programme de low code d'Oracle).

Oracle Fusion Applications Business Process Foundations Certification : couvre les flux métier critiques automatisés par Oracle Fusion Applications, tels qu'Oracle Fusion Cloud Enterprise Resource Planning (ERP), Oracle Fusion Cloud Human Capital Management (HCM), Oracle Fusion Cloud Supply Chain & Manufacturing (SCM) et Oracle Fusion Cloud Customer Experience (CX). □

B.G

FORMATIONS GRATUITES POUR LE CLOUD



www.linfocr.com

L'INFO CYBER-RISQUES

by L'INFORMATICIEN

Chatbot

L'enjeu des fuites de données

Sommaire

Bienvenue dans ce cahier

L'InfoCyber-risques. Trois mois, en cybersécurité, c'est une éternité. Notre trimestriel disparaît donc au profit d'un supplément de 16 pages publiées tous les mois dans *L'Informaticien*, afin de raccourcir le cycle entre l'événement et notre analyse, et vous donner au plus vite les informations dont vous aurez besoin pour faire face aux menaces lorsqu'elles apparaissent.

CYBERATTAQUE DE GROUPE LEADER :

«Une sauvegarde trouvée in extremis a permis d'éviter la catastrophe !»

En quelques heures, 100 % des serveurs du spécialiste français de l'intérim étaient chiffrés par le ransomware Cuba, y compris les sauvegardes. Une situation critique, heureusement débloquée grâce à une sauvegarde retrouvée dans une mémoire tampon, à seulement quelques jours de son effacement. Retour sur une gestion de crise épique, mais où les responsables ont su garder leur sang-froid.

«Le pire moment pour être victime d'une cyberattaque !» C'est ce qui a marqué l'esprit de ceux qui ont vécu l'incident, survenu au début du mois de février 2021. Le Groupe Leader, spécialiste français de l'intérim (170 agences en Europe et plus de 1500 collaborateurs permanents) est alors en période de paye de 13 000 intérimaires. Autant dire qu'un blocage de l'informatique à ce moment crucial est un des pires scénarios que pouvait vivre l'entreprise. Car une de ses principales activités est de prendre en charge la gestion temporaire d'un poste en entreprise, en fournissant la ressource humaine mais aussi en gérant la paye.

Ce scénario catastrophe, le Groupe Leader l'a pourtant vécu. Et il s'en est aujourd'hui relevé. Mais son dirigeant, Jean-Philippe Papin, évoque encore un *«traumatisme»* et compare cette cyberattaque à un *«coup de massue»*, tant elle a surpris toute l'entreprise par sa brutalité. Pourtant, l'ETI était préparée. Elle venait de recruter un nouveau DSI, dont l'une des missions était justement de renforcer la sécurité du SI, face à la vague de cyberattaques qui déferlait sur la France, ciblant des entreprises comme des collectivités.

«J'ai pris mes fonctions six mois avant l'attaque», se remémore Christophe Benoist, DSI du Groupe Leader. *«Il y avait des enjeux prioritaires d'organisation et de management. Je me suis donc d'abord concentré là-dessus.»* Le système d'information du Groupe Leader se compose alors d'une centaine de serveurs, principalement sous Windows, et de 600 postes de travail dont la moitié sont des PC classiques et l'autre des clients légers connectés à la plateforme Citrix Cloud. Côté software, le cœur du SI est un ERP qui permet de facturer les clients et de gérer la paye. Cet ERP est hébergé sur les serveurs internes du groupe, déployés dans un datacenter situé dans le Val-d'Oise, près d'Eaubonne où du siège de l'entreprise. L'ETI possède également des ressources de secours, hébergées dans un cloud privé dans le cadre de son PRA (plan de reprise d'activité).

Une attaque fulgurante

C'est le vendredi 5 février que les premiers signes de l'attaque remontent jusqu'à la DSI. *«Certains utilisateurs se plaignaient de problèmes techniques pour accéder à l'ERP et de fichiers inaccessibles»*, poursuit le DSI. Rapidement, ces problèmes se généralisent à tous les collaborateurs de l'entreprise. *«On nous appelait de toutes parts et nous commencions à prendre conscience de l'ampleur de l'incident»*. En quelques heures, ce vendredi matin, la quasi-totalité

du SI est inaccessible. Tous les serveurs sont *« cryptolockés »*, des serveurs de fichiers à ceux hébergeant les bases de données. *« Notre premier réflexe a été de tout éteindre pour stopper la propagation. Avec le recul, nous estimons aujourd'hui qu'il aurait été préférable de simplement déconnecter les machines et de les isoler du réseau, plutôt que de tout éteindre. Car il est ainsi possible de récupérer des informations sur la cyberattaque dans la RAM des serveurs. Mais dans l'urgence. Nous avons fait ce qui était le plus protecteur pour le SI »*.

En moins d'une heure, la centaine de serveurs est donc éteinte. Ensuite, l'ETI réalise les démarches administratives classiques, en prévenant l'ANSSI et en déposant plainte auprès de la gendarmerie. Mais l'ANSSI est à l'époque concentrée sur des attaques d'hôpitaux, et Groupe Leader n'aura aucun retour de la part de l'autorité nationale. L'entreprise se tourne alors vers la plateforme en ligne cybermalveillance.gouv.fr auprès de laquelle elle obtient un contact d'entreprise cyber qui pourrait l'accompagner. Mais finalement, elle va plutôt se rapprocher de la société Anetys, qui connaît bien l'entreprise car elle possède un contrat de maintenance sur l'environnement Citrix. *« Je me suis rendu sur place dès le vendredi matin et j'ai découvert un black-out complet du SI. Notre première action a été d'étudier l'état des sauvegardes »*, explique Maxime D'Anna, alors consultant ingénieur sécurité système et réseau chez Anetys. Il a aujourd'hui monté sa propre entreprise de cybersécurité (Lighteam).

Dans le datacenter, la DSI et le consultant d'Anetys auditent donc les sauvegardes pendant plusieurs heures. Mais mauvaise surprise, elles sont toutes chiffrées et donc inexploitables. Parallèlement, les premières études de la cyberattaque permettent d'identifier le code malveillant utilisé par les cybercriminels. Il s'agit de « Cuba », un ransomware relativement peu repandu en France. Il a fait des ravages aux États-Unis en ciblant des agences gouvernementales, des établissements de santé et des entreprises (lire encadré). *« Il y avait dans les fichiers chiffrés un lien pour contacter les cybercriminels et connaître le montant de la probable rançon. Mais nous ne l'avons pas fait »*, indique le DSI.

Constitution de la cellule de crise

Dès le vendredi après-midi, la cellule de crise est constituée, en intégrant le PDG de l'entreprise, la direction de la communication, la DSI actuelle ainsi que l'ancien DSI. Ce dernier a pris d'autres fonctions mais vient en soutien. La question de la communication sur la cyberattaque, en interne et en externe, est alors mise sur la table. Mais sans aucun moyen de communication fonctionnant dans l'entreprise, communiquer sur l'incident va être complexe. *« Nous avons décidé d'utiliser Whatsapp en créant différents groupes pour assurer la communication de crise en interne comme en externe avec nos clients »*, indique Christophe Benoist. Une messagerie en ligne, de type hotmail.com, a également été utilisée en secours. Les réseaux sociaux, dont Facebook, sont également

« Notre premier réflexe a été de tout éteindre pour stopper la propagation. »

Christophe Benoist,
DSI du Groupe Leader.

utilisés pour communiquer auprès du grand public. Dans la semaine, un numéro vert est aussi mis en place, notamment pour répondre aux questions des intérimaires qui attendent leur paye.

Dès le début de la semaine, la DSI et la DRH se penchent sur l'épineux problème du paiement des salaires des 13 000 intérimaires. L'ERP ne fonctionne plus et il faut donc trouver une solution de substitution. *« La direction nous a dit : la priorité est de trouver un moyen de payer les intérimaires »*, se souvient Maxime D'Anna. La tâche est cependant loin d'être évidente. Fort heureusement, une solution est trouvée, en exploitant un fichier Excel intégrant des bribes d'informations sur les précédentes payes. L'ETI récupère alors le RIB de chaque collaborateur et lui verse un acompte financier correspondant aux salaires. Mais il ne peut pas encore émettre de bulletin de salaire. *« Les salaires ont été versés au plus tard le 15 février, sans même un jour de retard. Dès la semaine suivant l'attaque, nous avions donc résolu le premier problème qui était la paye des collaborateurs »*. Les payes de Groupe Leader sont en effet versées en décalé, le 15 de chaque mois.

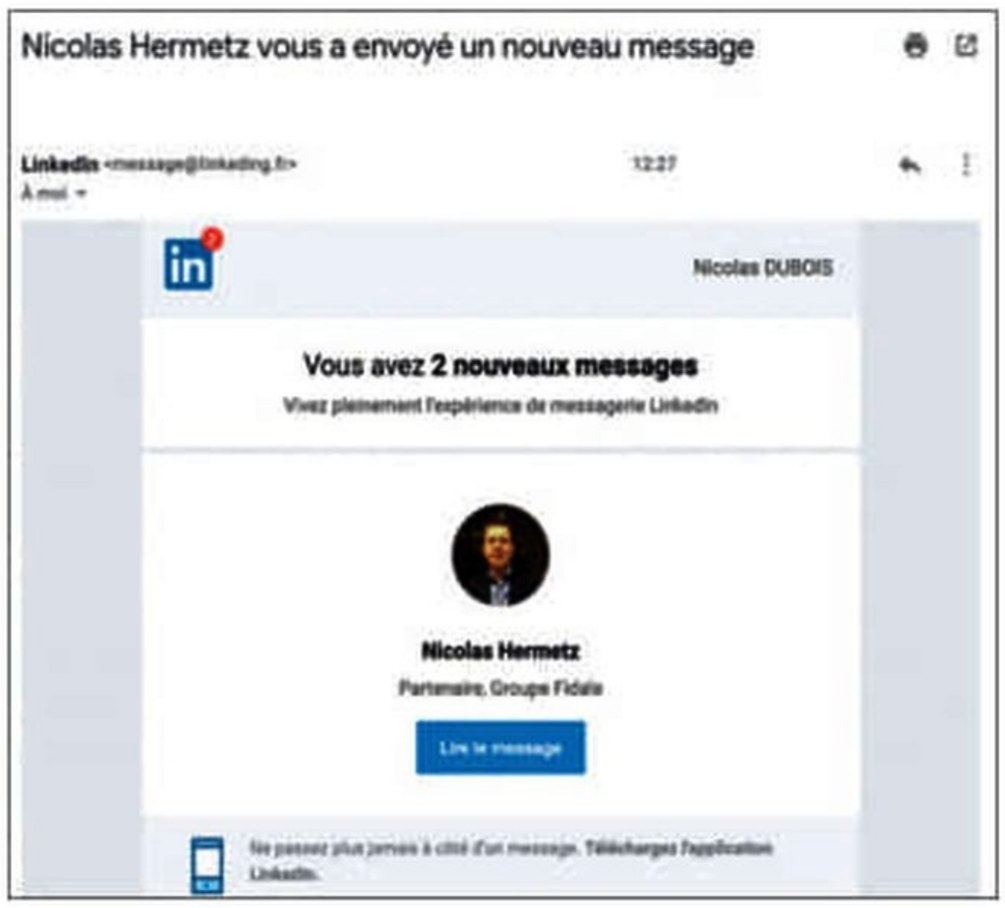
Une intrusion par phishing d'un collaborateur

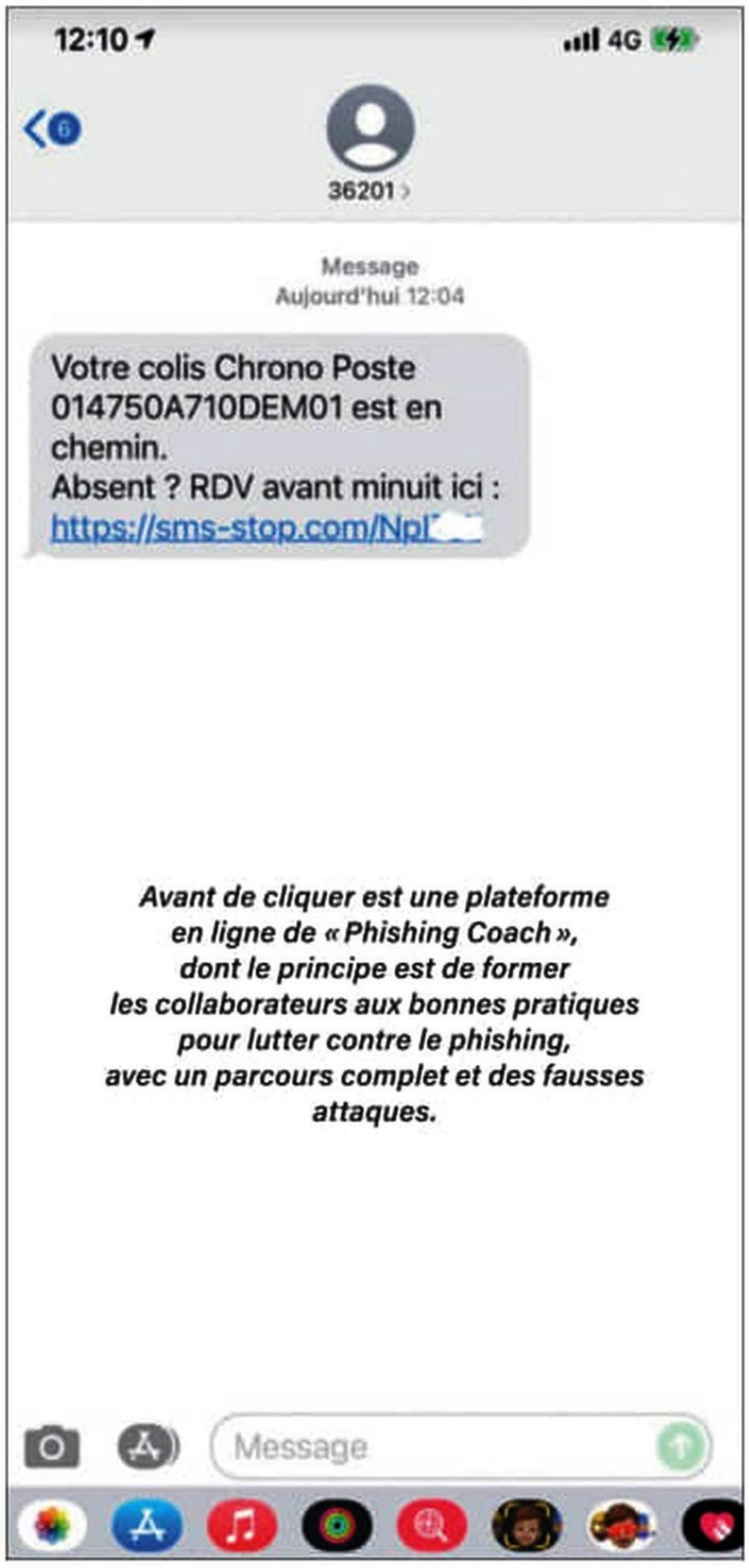
Durant la première semaine, les investigations se poursuivent pour déterminer l'origine de la cyberattaque. Elles remontent jusqu'au 2 juin, soit deux jours avant le chiffrement du SI. *« Nous avions alors constaté des lenteurs réseau. Nous avons découvert qu'il s'agissait en fait des premières actions menées par les cybercriminels. Ils déposaient discrètement sur notre SI des codes malveillants, ce qui causait des lenteurs sur le réseau »*, explique le DSI. *« Ils analysaient également l'architecture du SI, vraisemblablement pour déterminer comment organiser l'attaque pour qu'elle cause le maximum de dégâts en un minimum de temps »*.

Ces investigations permettent également d'identifier le « patient zéro », qui a permis d'ouvrir une brèche sur le SI. La source de l'attaque est un collaborateur ayant reçu un e-mail piégé, selon le principe très classique du phishing. Classé dans ses spams et rédigé en anglais, le message est suffisamment attractif (les détails ne sont pas publics) pour l'inciter à l'ouvrir. Il va cliquer sur un lien dans le message et récupérer un fichier hébergé dans un Google Doc. Il s'agit cependant d'un programme malveillant qui va ouvrir un accès aux cybercriminels. Ils vont ensuite se déplacer latéralement, en augmentant leurs privilèges. Et deux jours plus tard, ils lancent leur attaque en chiffrant les serveurs en seulement quelques heures. *« Selon les résultats des investigations, il n'y a pas eu d'exfiltration de données, juste le chiffrement des serveurs »*, indique Maxime D'Anna.

Reconstruire le SI

Dès la première semaine, la DSI et Anetys commencent à travailler sur le plan de remédiation. Mais la perspective de n'avoir aucune sauvegarde, et donc de devoir tout reconstruire, est plutôt sombre. La direction en conclut qu'il faut que l'entreprise retourne au papier, en attendant que le SI soit reconstruit. *« Je me revois encore dans le bureau du PDG à lui dire que nous n'avons aucune*





Avant de cliquer est une plateforme en ligne de « Phishing Coach », dont le principe est de former les collaborateurs aux bonnes pratiques pour lutter contre le phishing, avec un parcours complet et des fausses attaques.

donnée de sauvegarde… plus rien ! Il m'a alors expliqué que l'entreprise allait retourner aux anciennes façons de travailler, avec le téléphone et le stylo, comme 20 ans auparavant », confie Christophe Benoist. *« Il a fait preuve de sang-froid et n'a pas envenimé la situation en cherchant un responsable. Mais pour lui comme pour nous, ce fut tout de même une sacrée claque ! »*

De retour dans le datacenter, la DSI et Anetys cherchent encore la trace de données qui pourrait permettre de ne pas repartir d'une feuille blanche. Et une lueur d'espoir leur apparaît. *« Les solutions de sauvegardes sont répliquées sur plusieurs sites et nous avons commencé à éteindre une des baies répliquées, pour être certain qu'elle ne bougerait plus. Mais c'était une solution de type data domain et il y avait une corbeille où sont stockées les données avant d'être supprimées tous les 7 jours »*, indique Maxime D'Anna. *« Nous étions le samedi soir et la suppression était programmée pour le mardi suivant. Il y avait donc encore des données ! »*

Dans cette mémoire tampon des serveurs, l'ETI y retrouve une sauvegarde intacte et complète du SI datant d'avant le 2 février. Elle est donc antécédente aux premières actions des cybercriminels. *« Nous étions sauvés ! »*, se rappelle Christophe Benoist. *« Mais à trois jours d'intervalle, c'était la catastrophe »*.

Grâce à cette sauvegarde retrouvée *in extremis*, la reconstruction du SI va pouvoir commencer. L'entreprise décide cependant de ne pas reconstruire à l'identique, mais de profiter de l'occasion pour renforcer les protections cyber. *« Dans ce type de situation, même s'il y a urgence, il faut savoir prendre le temps de reconstruire le SI en améliorant les processus et les outils de sécurité. Sinon, vous risquez d'être victime d'une nouvelle attaque à plus ou moins long terme »*, estime Maxime D'Anna.

« Nous avons passé des nuits blanches », confie pour sa part Christophe Benoist. *« Le principe était de rouvrir les services au fil de l'eau, en fonction de leur priorité »*. Et la principale priorité est de relancer l'ERP, agence par agence. Une opération qui démarre dès le mercredi suivant l'attaque. Puis, c'est au tour de la messagerie et des autres applications d'être relancées. *« L'annuaire a été reconstruit en quelques jours, mais en recréant un serveur propre à partir d'une ISO et en réinjectant des données manuellement. L'idée était de ne pas simplement restaurer les serveurs »*, souligne Maxime D'Anna. En parallèle, un renfort des protections du SI est donc réalisé, avec notamment un passage d'un antivirus traditionnel à un XDR. Une solution anti-spam est également déployée ainsi que de nouveaux firewalls. Progressivement, le Groupe Leader retrouve donc son SI. La majeure partie des outils, dont l'ERP et la messagerie, sont opérationnels en trois semaines. Mais l'accès Internet n'est rouvert que très progressivement aux collaborateurs. Au final, ce n'est qu'au bout d'un mois et demi que le retour à la normale intervient réellement.

Un coût financier d'environ 1 million d'euros

L'impact financier de l'incident est estimé à environ 1 million d'euros, en intégrant la gestion de crise, le manque à gagner du fait du blocage du SI, et aussi en ajoutant les nouvelles solutions de cyberprotection. Une mise à niveau qui a coûté environ 250 000 euros.

L'ETI a également embauché un RSSI à temps partiel (5 jours par mois) pour épauler la DSI. Une feuille de route cyber a aussi été rédigée. Elle a notamment permis le déploiement de la solution de sensibilisation des collaborateurs « Avant de cliquer ». Il s'agit d'une plateforme en ligne de « Phishing Coach », dont le principe est de former les collaborateurs aux bonnes pratiques pour lutter contre le phishing, avec un parcours complet et des fausses attaques. La plateforme va par exemple envoyer des mails sur lesquels les collaborateurs ne sont pas supposés cliquer. Des messages très réalistes comme un mail d'une banque, une demande de la DSI ou un rappel de

Cuba : le ransomware à 60 millions de dollars

Actifs depuis 2019, le groupe de cybercriminels derrière le ransomware Cuba a surtout ciblé des entités américaines telles que des agences gouvernementales, des services financiers, des entreprises IT ou des établissements de santé.

Selon une fiche du FBI et de la CISA (Cybersecurity and Infrastructure Security Agency), parue en janvier 2023, Cuba ransomware a servi à extorquer plus de 60 millions de dollars en 2022, sur 145 millions de rançons réclamées aux victimes. *« Depuis décembre 2021, le nombre d'entités américaines compromises par Cuba ransomware a doublé, les rançons demandées et payées étant en augmentation »*, peut-on lire dans cette fiche. En 2022, 101 entités ont été compromises, dont 65 aux États-Unis et 36 dans d'autres pays, notamment la France avec le cas de Groupe Leader. En France, Cuba a également été utilisé fin 2022 pour perpétrer une attaque contre la mairie de Chaville (Île-de-France), paralysant tout le SI de la commune. Contrairement à ce que leur nom pourrait laisser penser, le groupe de cybercriminels exploitant Cuba n'a pas de lien direct avec la république de Cuba, et serait plutôt d'origine russe.

contravention. Si le collaborateur clique sur le message, il est renvoyé vers une page qui l'alerte sur son erreur.

La solution intègre un parcours personnalisé, basé sur de l'e-learning et ces fausses attaques, avec quatre niveaux de compétences à acquérir. Il est censé diviser par 10 le risque de phishing. *« Vu que l'origine de la cyberattaque est une erreur humaine, la sensibilisation de nos collaborateurs aux bonnes pratiques de cybersécurité est essentielle »*, indique la DSI.

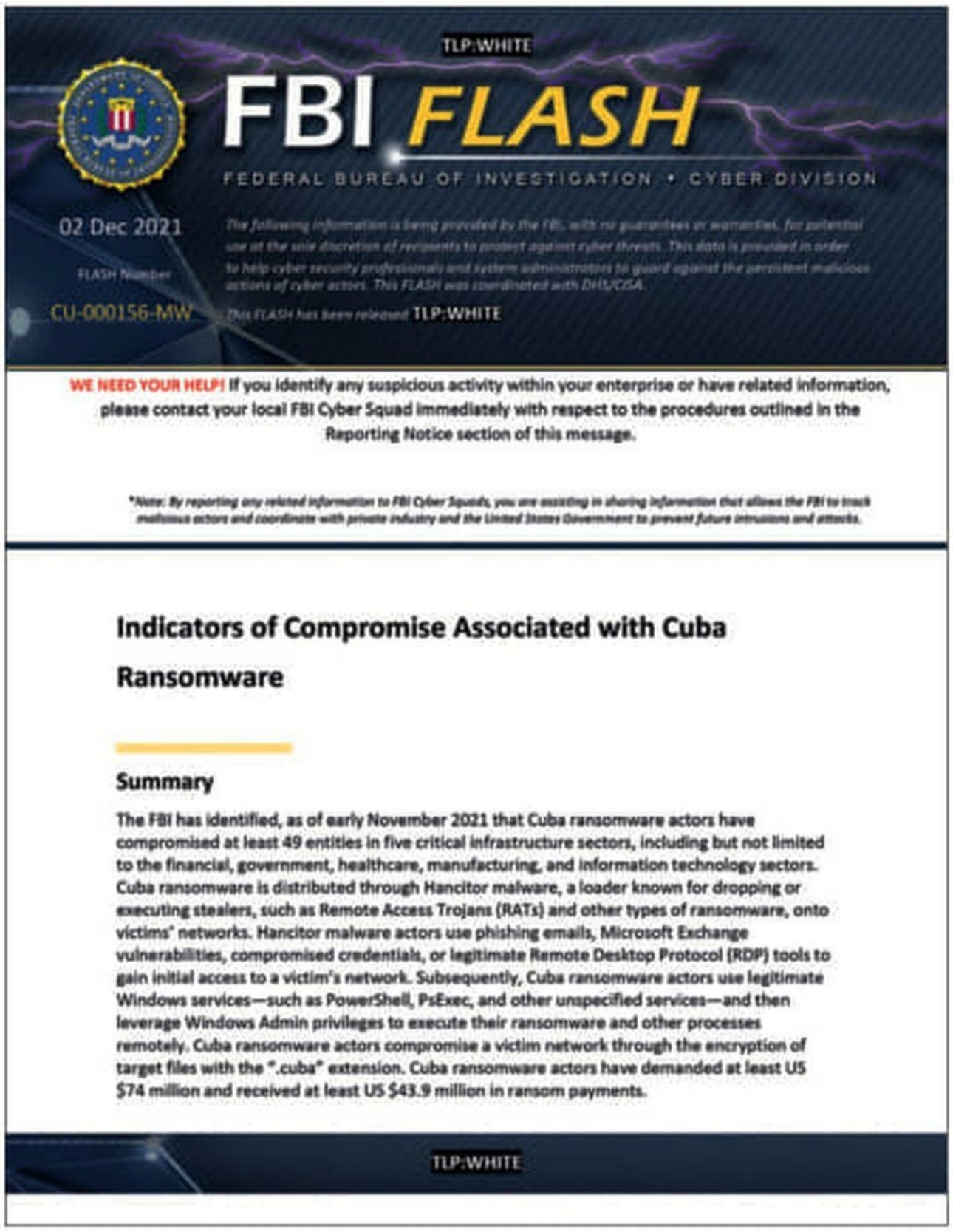
La feuille de route a aussi permis la mise en place de nouvelles solutions de sauvegardes déconnectées, notamment sur bandes. *« Un des principaux enseignements de cet incident est qu'il vaut mieux avoir des sauvegardes isolées du reste du réseau afin de pouvoir reconstruire le SI. Sinon, en cas de chiffrement complet du SI, comme nous l'avons vécu, la situation devient réellement critique »*, confie Christophe Benoist.

Une recommandation faite également par Maxime D'Anna. *« Les sauvegardes doivent être isolées. Et le serveur de sauvegarde ne doit jamais être rattaché à un domaine Active Directory »*. Et de préciser : *« sans sauvegarde, je connais des entreprises dont la cyberattaque les a menées à la faillite. La sauvegarde, c'est la clé de la survie ! »*. Et selon le consultant, il convient bien entendue de vérifier au moins une fois par an minimum que les sauvegardes sont restaurables. *« Il faut faire des tests de restauration. Qui sont autant d'entraînements face à une cyberattaque. »*

Autre enseignement : disposer d'un plan de retour d'activité (PRA) orienté cyber afin d'accélérer la remédiation. *« Nous n'en disposions pas mais c'est le cas dorénavant »*, indique Christophe Benoist. Pour Maxime D'Anna : *« il faut identifier les personnes clés à mobiliser en interne et en externe, et avoir anticipé quel rôle elles auront chacune à jouer »*.

Enfin, sur le moment, il faut savoir garder son sang-froid, souligne Maxime D'Anna, ce qui a été le cas avec le Groupe Leader. *« Je suis intervenu sur plus d'une dizaine de cyberattaques et un des éléments notables de celle-ci est que la direction n'a pas mis de pression inutile sur la DSI durant la gestion de crise. Le DSI a, quant à lui, bien géré les nombreuses demandes des collaborateurs pour récupérer leurs outils le plus vite possible. Il a réussi à prioriser la remédiation, à rester toujours positif et a joué un rôle de tampon entre les différentes entités impliquées, ce qui est loin d'être évident dans ce type de situation »*. Il tient à rappeler qu'une cyberattaque peut entraîner un niveau de stress très élevé au niveau des équipes informatiques, qui peuvent même parfois craquer. *« Je suis intervenu sur une cyberattaque suite à un burn-out du RSI qui a terminé à l'hôpital. Préserver la santé des équipes informatiques n'est donc pas quelque chose à prendre à la légère ! »* ■

Chritophe Guillemin


TLP:WHITE

FBI FLASH

FEDERAL BUREAU OF INVESTIGATION • CYBER DIVISION

02 Dec 2021

FLASH Number

CU-000156-MW

The following information is being provided by the FBI, with no guarantees or warranties, for potential use at the sole discretion of recipients to protect against cyber threats. This data is provided in order to help cyber security professionals and system administrators to guard against the persistent malicious actions of cyber actors. This FLASH was coordinated with DHS/CISA.

This FLASH has been released TLP:WHITE

WE NEED YOUR HELP! If you identify any suspicious activity within your enterprise or have related information, please contact your local FBI Cyber Squad immediately with respect to the procedures outlined in the Reporting Notice section of this message.

**Note: By reporting any related information to FBI Cyber Squads, you are assisting in sharing information that allows the FBI to track malicious actors and coordinate with private industry and the United States Government to prevent future intrusions and attacks.*

Indicators of Compromise Associated with Cuba Ransomware

Summary

The FBI has identified, as of early November 2021 that Cuba ransomware actors have compromised at least 49 entities in five critical infrastructure sectors, including but not limited to the financial, government, healthcare, manufacturing, and information technology sectors. Cuba ransomware is distributed through Hancitor malware, a loader known for dropping or executing stealers, such as Remote Access Trojans (RATs) and other types of ransomware, onto victims' networks. Hancitor malware actors use phishing emails, Microsoft Exchange vulnerabilities, compromised credentials, or legitimate Remote Desktop Protocol (RDP) tools to gain initial access to a victim's network. Subsequently, Cuba ransomware actors use legitimate Windows services—such as PowerShell, PsExec, and other unspecified services—and then leverage Windows Admin privileges to execute their ransomware and other processes remotely. Cuba ransomware actors compromise a victim network through the encryption of target files with the ".cuba" extension. Cuba ransomware actors have demanded at least US $74 million and received at least US $43.9 million in ransom payments.

TLP:WHITE

Selon la fiche du FBI, Cuba ransomware a servi à extorquer plus de 60 millions de dollars en 2022, sur 145 millions de rançons réclamées aux victimes. Outre le Groupe Leader, Cuba a également été utilisé en France fin 2022 pour perpétrer une attaque contre la mairie de Chaville (Île-de-France), en paralysant tout le système d'information de la commune.

« Sans sauvegarde, je connais des entreprises dont la cyberattaque les a menées à la faillite. »

Maxime D'Anna,
Consultant en cybersécurité.

Développement de l'EUCS par l'ENISA

La Commission européenne a fait pression pour inclure des exigences de souveraineté dans le système de certification de la cybersécurité pour les services cloud (Cybersecurity Certification Scheme for Cloud Services ou EUCS).

La Commission européenne avait demandé à l'ENISA, l'Agence de l'Union européenne pour la cybersécurité, en charge du développement de l'EUCS, d'y ajouter des exigences de souveraineté. Nous allons voir dans cet article ce qu'il en est et quelles avancées ont été réalisées.

L'ENISA a été créée en 2004. Elle joue un rôle clé en matière d'aide au développement des capacités nationales de cybersécurité et de soutien à la coopération entre les États membres. L'EUCS est un acte de législation dit secondaire de la loi européenne sur la cybersécurité visant à renforcer la confiance et la sécurité dans les produits et services numériques jugés importants. Il s'agit d'un cadre volontaire, à l'échelle de l'Union, pour les certificats de cybersécurité. Son but est de lutter contre la fragmentation entre les législations des États membres et de faciliter la compréhension des besoins en matière de sécurité. L'EUCS ou projet de schéma européen de certification de cybersécurité pour les services de cloud inclut des exigences de souveraineté sur la localisation des données européennes ainsi que l'immunité face au droit étranger. Certains États membres ainsi que le secteur privé s'y opposent fortement, allez savoir pourquoi… Il est écrit dans l'ébauche du dit document que *« l'objectif de ces exigences spécifiques est de prévenir et de limiter de manière adéquate les éventuelles interférences d'États extérieurs à l'UE avec le fonctionnement des services de cloud certifiés »*. Cette approche ressemble à s'y méprendre aux exigences introduites récemment dans le schéma national français de certification de la cybersécurité, le SecNumCloud. Elle affecte les fournisseurs de services de cloud qui travaillent sur le marché de l'UE en garantissant que le droit de l'UE est prioritaire et que la maintenance, les opérations et le stockage des données doivent être localisés dans l'UE. L'immunité contre les accès extérieurs à l'UE serait également garantie. Les fournisseurs de services de cloud devront être basés en Europe et surtout ne pas être contrôlés par des entités extérieures à l'Union européenne. La notion de contrôle y est définie de manière très précise. Les entreprises concernées doivent être totalement indépendantes des lois autres que celles de l'UE. En effet, les relations établies par les notions de propriété et de droit ainsi que les contrats ont une influence non négligeable. Les échanges entre les fournisseurs de services cloud et ceux basés hors UE devront répondre à des exigences très spécifiques en termes d'autorisation de sécurité et de supervision. Quand bien même une entreprise a son siège dans l'UE, si certains de ses investisseurs ou des opérations sont localisés à l'étranger, elle pourra n'avoir qu'un accès limité via ce dispositif. *« Cela nuira directement aux fournisseurs de services de cloud et signifiera, plus largement, que l'économie européenne y perdra en termes de choix et de qualité des offres de cloud »*, aurait déclaré un porte-parole de Digital Europe. Évidemment, la perspective de perdre de juteux contrats ne les emballe guère. Bien que le projet de texte spécifie qu'il s'agit de mesures techniques, quelques états de l'UE ainsi que des représentants de l'industrie essayent de faire pression pour que les discussions s'étendent au niveau politique. Les utilisateurs devraient être informés du risque en matière de cybersécurité via trois niveaux de garantie : basique, substantiel et élevé. Le dernier indique qu'un service a passé les tests de sécurité les plus élevés. Les exigences de souveraineté ne s'appliqueraient en fait qu'à ce niveau.

Les oppositions aux exigences de souveraineté

Quelques pays tels que l'Irlande, les Pays-Bas ou la Suède ont écrit en collaboration un document (officieux) faisant valoir que les fournisseurs de services de cloud s'efforceront sans doute d'obtenir une certification de troisième niveau *« car les fournisseurs de services de cloud sont souvent parties intégrante de la chaîne d'approvisionnement de secteurs tels que le gouvernement et les infrastructures et services vitaux. »* Ces exigences sont plébiscitées notamment par la France, l'Allemagne, l'Italie et l'Espagne. Les experts s'attendent quant à eux à ce que la certification devienne obligatoire à l'avenir. Le processus d'élaboration a également été critiqué en raison de *« la transparence insuffisante et du manque d'engagement des parties prenantes »*, du moins c'est ce qu'ont déclaré des représentants de l'industrie technologique comme l'AmCham EU, le BSA, l'ITI ou encore le CCIA. Ils ne sont bien entendu pas des plus objectifs. L'ENISA devrait présenter sa recommandation finale pour le dispositif EUCS en septembre prochain. ■

T.T

IA conversationnelles

L'enjeu des fuites de données

Le succès de ChatGPT et des robots conversationnels basés sous intelligence artificielle ne se dément pas. Des centaines de millions de personnes les utilisent désormais chaque jour que cela soit pour travailler, étudier, ou à titre personnel. Après l'engouement général, de nombreuses voix s'élèvent pour dénoncer les risques que ces technologies représentent pour la sécurité des données.

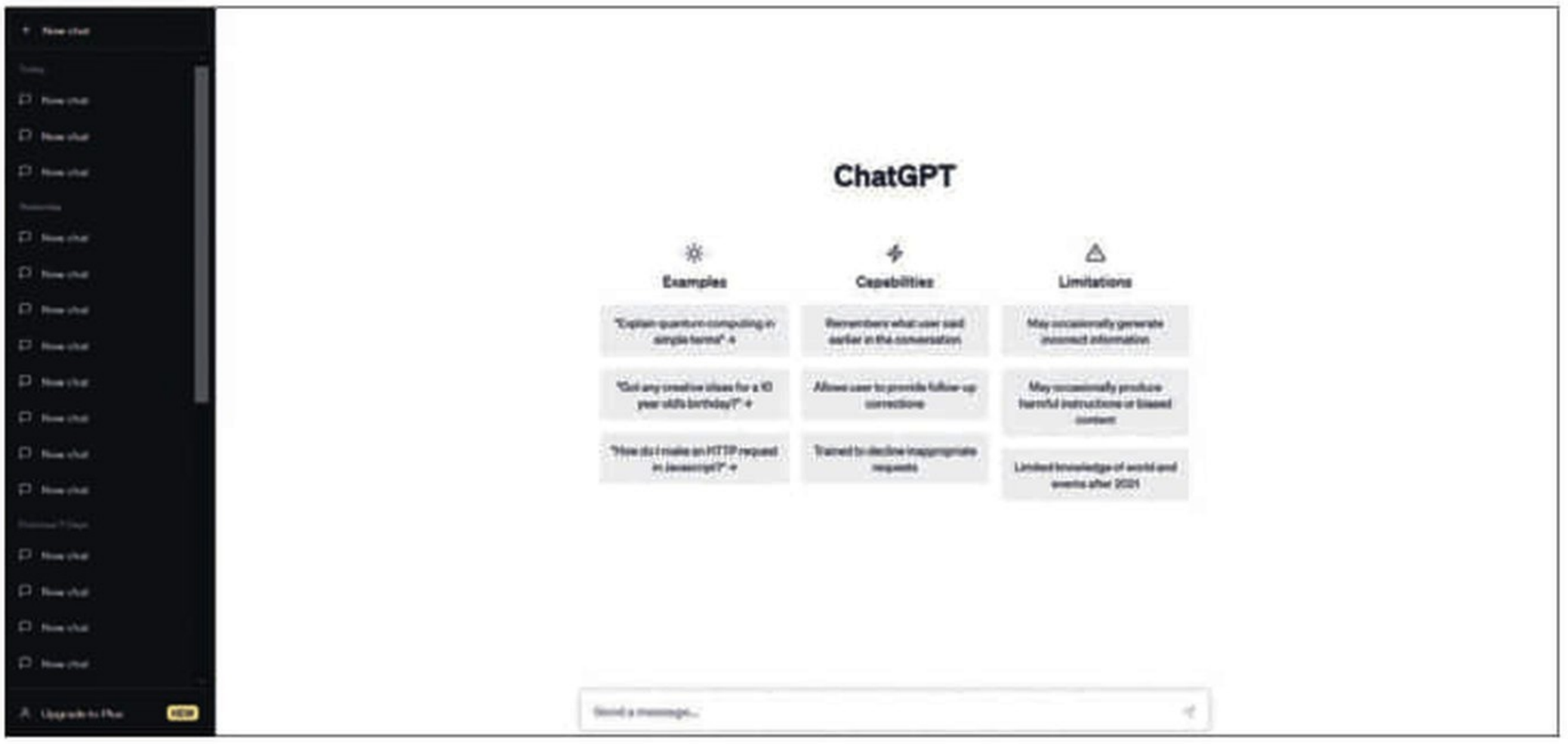
Le 31 mars dernier, le gouvernement italien a créé une véritable onde de choc en annonçant l'interdiction temporaire pure et simple de ChatGPT dans le pays. Si ChatGPT était d'ores et déjà interdit dans des pays comme l'Afghanistan, la Corée du Nord, la Chine, Cuba, la Russie, l'Iran, le Bhoutan, ou encore la Syrie, l'Italie est le premier pays occidental à avoir pris une telle décision. Celle-ci a été prise par l'autorité nationale de protection des données personnelles (GPDP : l'équivalent de la CNIL en France) suite à des soupçons de violations des règles de l'Union européenne en matière de protection des données. L'organisme reprochait à OpenAI, la maison mère de ChatGPT, de ne pas s'être conformée aux règles du RGPD en vigueur depuis 7 ans sur le vieux continent. Le service n'avait, par ailleurs, pas de système de vérification de l'âge de ses utilisateurs, sachant que certaines réponses de l'IA peuvent être inappropriées pour des enfants.

Interdiction temporaire de ChatGPT en Italie

La GDPD accusait également le manque de transparence d'OpenAI qui n'informe pas ses utilisateurs que leurs données sont automatiquement réinjectées dans les modèles d'entraînement de l'IA. Autre manquement au règlement européen, la jeune pousse californienne n'a pas signalé que certains utilisateurs italiens ont été victimes d'une fuite de données *via* son service Premium ChatGPT Plus. L'organisme de surveillance italien a laissé 20 jours à OpenAI pour se conformer aux exigences du RGPD sous peine d'une lourde amende pouvant aller jusqu'à 4 % de son chiffre d'affaires. Au regard des enjeux colossaux que représente une interdiction dans un pays européen comme l'Italie, OpenAI a mis tout en œuvre pour que la sanction soit levée. Le 29 avril, le PDG d'OpenAI, Sam Altman, a annoncé que ChatGPT était de nouveau accessible en Italie. Le service a notamment mis en place une limite d'âge pour que les mineurs ne puissent plus accéder à ChatGPT sans l'accord d'un adulte. En ce qui concerne le traitement des données par OpenAI, de nombreuses zones d'ombre subsistent.

Un service sous haute surveillance

Après l'Italie, les régulateurs d'autres pays comme le Canada, l'Allemagne, ou même la France ont lancé des procédures de contrôle à l'encontre du chatbot d'OpenAI. Celles-ci font notamment suite à des plaintes pour des infractions sur la protection des données. Le service payant de ChatGPT Plus a subi en effet plusieurs bugs qui ont généré des fuites de données. OpenAI a admis que 1,2 % de ses abonnés ont pu voir certaines de leurs données exposées. Certains utilisateurs ont en effet vu l'historique de



conversations d'autres utilisateurs apparaître dans leur fil de discussion avec l'IA. Pire encore, des informations sensibles des abonnés payants ont fuité suite à un bug survenu à la fin du mois de mars. *« Dans les heures qui ont précédé la mise hors ligne de ChatGPT, certains utilisateurs ont pu voir le nom et le prénom, l'adresse électronique, l'adresse de paiement, les quatre derniers chiffres (uniquement) d'un numéro de carte de crédit et la date d'expiration de la carte de crédit d'un autre utilisateur actif »*, déclarait l'entreprise américaine sur son blog. Des incidents qui ne risquent pas de faire taire les nombreuses polémiques sur l'IA générative.

Les risques pour la confidentialité et la souveraineté des entreprises

Après l'enthousiasme mondial pour ChatGPT, certains responsables d'entreprises commencent à réaliser que l'utilisation du service peut poser de sérieux problèmes de confidentialité. Comme les GAFAM, OpenAI exploite les données de ses utilisateurs pour pouvoir offrir le meilleur service possible. C'est clairement indiqué dans les conditions générales d'utilisation (GGU) de ChatGPT : *« lorsque vous utilisez nos services, nous pouvons collecter des informations personnelles qui sont incluses dans les données, les téléchargements de fichiers ou les commentaires que vous fournissez à nos services »*. Concrètement, les données servent à alimenter et entraîner le modèle de ChatGPT. De ce fait, elles peuvent réapparaître par exemple sur une requête d'une personne extérieure à une entreprise. C'est ce qui est arrivé à Samsung au début du mois d'avril 2023 après que des collaborateurs aient utilisé ChatGPT et dévoilé malencontreusement des données confidentielles à l'IA. Des ingénieurs auraient notamment soumis le code source d'une application de Samsung pour demander à l'IA de corriger des bugs. Un autre employé aurait également demandé au chatbot de créer une synthèse de certains documents internes confidentiels. Pour stopper les fuites de données sensibles, le géant sud-coréen a pris le taureau par les cornes en bannissant purement et simplement l'accès à ChatGPT, mais aussi les autres IA génératives comme Google Bard à ses employés. Plusieurs grandes entreprises, dont Apple, Amazon, et JP Morgan Chase lui ont depuis emboité le pas pour proscrire à leur tour l'utilisation des chatbots à leur personnel. ■

Jérôme Cartegini

« Il y a des entreprises du CAC 40 qui ont volontairement contractualisé avec des géants du numérique qui ne sont pas régis par la loi européenne, mais américaine. »

Arnaud Muller, cofondateur et directeur général de Cleyrop.

Cleyrop se présente comme le premier hub de données européen et une plateforme de données souveraines de bout en bout. Nous avons rencontré Arnaud Muller, cofondateur et directeur général de Cleyrop, pour évoquer les récentes fuites d'informations stratégiques via les IA génératives comme ChatGPT.

Que pensez-vous des fuites de données via ChatGPT ? Les agents conversationnels sont-ils suffisamment sécurisés ?

Il est très intéressant de parler de ce sujet par l'angle de la sécurité, car il y a plusieurs façons d'aborder les problématiques que peut amener ChatGPT aux citoyens, aux organisations publiques et privées, ou même l'État. Cette nouvelle génération d'intelligence artificielle que sont les « large knowledge model » a besoin de quantités astronomiques de données d'apprentissage pour être pertinentes et amener un bon niveau de performances comme celui qui vient d'être constaté par tous les utilisateurs de Google Bard. Depuis quelques jours, ce dernier a pris l'ascendant en termes de performances sur ChatGPT. Il est difficile de se projeter sur la prochaine bonne réponse à fournir à quelqu'un qui nous interroge si l'on n'a pas emmagasiné des quantités monstrueuses diverses et variées d'informations en amont. Ces informations, il faut pouvoir les trouver pour les fournir à nos nouveaux robots qui vont nous aider dans nos travaux quotidiens à être plus efficaces. Aujourd'hui, on prend conscience que finalement, c'est avant tout et surtout, les GAFAM qui ont ces données *via* leurs services de mails, de cloud, *etc.* Lorsqu'on n'a pas cette chance de pouvoir fournir des outils gratuits, on ne peut pas capter de la donnée et entraîner des modèles pour développer des IA efficaces. Tout cela s'est fait avec le consentement des personnes, car on a tous donné notre consentement pour utiliser les produits de Google, Microsoft, Apple, Facebook, *etc.* Il n'y a donc pas de failles de sécurité ni de failles d'éthique non plus. D'autres sociétés qui voudraient aller sur ce marché-là n'ont peut-être pas la masse d'informations dont bénéficie un Google, un Amazon, *etc.*

La confidentialité des particuliers est-elle également menacée par les IA génératives ?

On va voir que finalement, en tant que citoyens, on utilise même au moment où l'on se parle dans nos organisations des outils comme Google Drive, par exemple. Bien que très pratique au quotidien, ce service va prendre plein d'informations qui ne nous appartiennent peut-être pas à nous en tant que citoyens, mais aux personnes qui nous emploient. Là encore, on donne ces données à Google, ce qui signifie concrètement qu'on laisse entrer le loup dans la bergerie. On fait confiance aux GAFAM pour faire les choses bien, mais il ne faut pas après s'étonner que nos données se retrouvent quelque part. Par le passé, j'ai travaillé chez Airbus, et avant cela chez Safran. À l'époque, j'ai ouvert un dossier Google Drive avec des données qui appartiennent à Safran pour collaborer avec Airbus, on peut donc s'attendre à

découvrir demain les données d'Airbus et Safran qui se retrouvent quelque part. En fait, c'est sur ces jeux de données que les géants du numérique, ou en tous les cas les producteurs d'intelligence artificielle, vont devoir entraîner leurs modèles. Ils vont avoir besoin d'une infrastructure puissante, avec des dizaines de milliers de GPU, des dizaines de milliards de paramètres, mais aussi beaucoup de données. On n'a pas toujours la traçabilité et l'origine de la donnée avec ce que prévoit le droit européen, c'est-à-dire la gestion du consentement sur toute la chaîne de valeur.

S'il n'y a pas de solutions pour réglementer les IA génératives afin d'empêcher des fuites de données sensibles, les entreprises ne devraient-elles pas interdire leur usage ?

Dans certains cas, surtout lorsqu'on sent qu'il y a un changement de paradigme tel que celui qui est en train de se dessiner sous nos yeux avec ChatGPT, la prudence est de mise. Concrètement, je pourrais poser des questions à ChatGPT pour savoir quels sont les secrets industriels de telle ou telle entreprise. Si vous avez laissé un loup entrer dans la bergerie, et qu'il a attrapé une chèvre et qu'il la redonne au public (en mode open source, parce que c'est comme ça qu'il fonctionne), c'est bien qu'il y avait un berger qui n'a pas fait son boulot et qui a laissé rentrer le loup. Il ne faut donc même pas se demander s'il faut fermer l'accès, car bien sûr, il faut que mes chèvres soient en sécurité. C'est mon rôle en tant que gardien du temple que de sécuriser une propriété privée. Encore une fois, quand j'ouvre la porte à Google et que j'ai donné mon consentement pour le faire, je ne peux pas dire après que Google est le loup. Quand Bard de Google répond à mes questions en ayant appris avec toutes les données que j'ai partagées avec lui, il a le droit de le faire, car je lui ai donné mon consentement. Chacun en tant que client prend ses responsabilités. Les fuites ou les failles n'en sont pas à partir du moment où l'on est d'accord.

Qui est responsable des fuites de données sur ChatGPT ?

Qui a autorisé des personnes qui pourraient notamment être des loups et qui viennent pour voler des choses à rentrer dans une bergerie ? Il y a quand même des directions informatiques, il y a des RSSI (Responsable de la Sécurité des Systèmes d'Information) qui sont les garants de la protection du patrimoine informationnelle de l'entreprise. *A priori*, ces personnes compétentes limitent l'exposition aux risques de l'entreprise de livrer des secrets industriels qui pourraient appartenir à l'armée, ou par exemple à une entreprise comme Thalès, à des compétiteurs ou à des tiers qui pourraient avoir des intérêts divergents. Les entreprises doivent en principe être protégées. Il y a des gens qui ont bien fait ça en empêchant Google, Amazon ou d'autres de rentrer en tous les cas dans des zones privées et réputées de confiance pour protéger les secrets industriels. Il y a des entreprises du CAC 40 qui ont volontairement contractualisé avec des géants du numérique qui ne sont pas régis par la loi européenne, mais américaine. Cela signifie qu'elles ont donné leur consentement pour utiliser des produits et des services qui sont sur une réglementation qui n'est pas maîtrisée ni par leur direction ni par les personnes de l'État français, ou de l'Europe. Quand je vois aujourd'hui des groupes comme Thalès qui essayent d'imposer Google à tout le monde, et que les entreprises attendent toutes, aussi responsables et éthiques qu'elles soient, que Google soit souverainisé par un fleuron industriel de l'armement, je me dis que même Thalès n'a pas dû lire les CGU de Google. Je vais citer, Paul Stefanut, qui est un éminent chercheur notamment dans le domaine de la deepTech et qui monte les plus gros consortiums informatiques dans le domaine scientifique en Europe. Je lui ai demandé s'il utilisait ChatGPT pour l'aider à répondre à de nouveaux appels à projets de la Commission européenne. Sa réponse a été : *« je ne nourris pas mon ennemi »*. ■

PROPOS RECUEILLIS PAR JÉRÔME CARTEGINI

Arnaud Muller, cofondateur et directeur général de Cleyrop.

LA SÉCURITÉ INFORMATIQUE EST UNE JUNGLE.

Et comme toute jungle, cela peut être un endroit dangereux
sans les PRÉCAUTIONS APPROPRIÉES.

SAFECONSOLE

GATEKEEPER

DriveLock

> Gestion centralisée
> Contrôle des Périphériques
> Filtrage des Applications
> Gestion de BitLocker
> Chiffrement partiel ou complet
> Périphériques sécurisés
> Connexion sans mot de passe
> Audits et Rapports...

Query Informatique

www.query-informatique.com

1 bd Charles de Gaulle
92700 Colombes - FRANCE
Tél. : +33 (0)1 49 97 33 00

Démantèlement de Genesis Market,

l'immense marché noir de données dérobées

Le 4 avril 2023, les forces de l'ordre de 18 pays, en collaboration avec Europol, ont réussi à démanteler Genesis Market, un marché noir spécialisé dans la vente d'identités numériques volées.

Le FBI, qui surveillait Genesis Market depuis quelque temps, a contacté la Sûreté du Québec en février dernier afin de la faire participer à cette grande frappe internationale. Six Québécois, quatre hommes et deux femmes, ont été arrêtés lors de cette opération appelée Cookie Monster et menée conjointement par plusieurs pays contre Genesis, l'un des plus grands sites de piratage au monde. Les suspects québécois n'étaient apparemment pas du menu fretin mais au contraire des super-utilisateurs. Sur ce marché en ligne, il était possible d'acheter des profils de victimes infectées par des virus et d'ainsi accéder à leurs comptes : courriels, réseaux sociaux, accès professionnels liés à l'employeur et bien entendu services bancaires. Des perquisitions ont eu lieu, principalement dans la région de Montréal. Le FBI avait dépêché pour cela un de ses représentants ainsi qu'un chien renifleur spécialisé dans la recherche d'une minuscule clef USB dans le fouillis d'une maison ou d'un appartement. Ce brave labrador est l'un des rares chiens policiers au monde entraîné à cette fin. S'il a été prêté au Québec, ce n'est ni par hasard ni pour des raisons de proximité géographiques. C'est surtout au vu du nombre très important d'acheteurs d'identités numériques corrompues sur Genesis Market dans le pays. « *Malheureusement, le Québec était fort représenté* », a déclaré le lieutenant Jean Le Bel. D'après le FBI, Genesis Market a mis en vente depuis sa mise en ligne en mars 2018 les données de près de deux millions de machines infectées. Le ou plutôt les virus employés permettaient aux pirates de reproduire dans un navigateur développé spécialement pour cela tout l'environnement de navigation de la victime : les sites auxquels la cible s'était déjà connectée, ceux bien sûr pour lesquels elle avait enregistré son mot de passe, les comptes de courrier électronique associés, les cookies et autres données intéressantes pour un vilain pirate.

Profils à vendre

Les profils à vendre pouvaient être très rémunérateurs pour les clients de Genesis : des traders, des infrastructures essentielles et même des agences gouvernementales. Néanmoins, les clients québécois semblaient préférer la « petite » fraude classique à la grand-papa (usurpation d'identité, de données bancaires,...) aux informations sensibles rattachées à de l'espionnage ou à du racket comme des informations sur des organisations gouvernementales ou des secrets commerciaux. « *L'objectif principal semblait être le gain financier* », a confirmé le sergent Marc-André Piché de la Sûreté du Québec. Pour accéder à ce site, il fallait juste être invité par un de ses membres, comme pour tout bon club privé. Celui-ci n'était même pas dissimulé sur le dark web et son utilisation était d'une facilité déconcertante d'un point de vue technique. Cela le rendait encore plus dangereux au vu des autorités car accessible à n'importe quel truand en herbe. Absolument n'importe qui, sans avoir aucune compétence en hack ni même en informatique, pouvait pirater et abuser les victimes. Le bon côté des choses, c'est que cela rendait les utilisateurs de Genesis assez facile à repérer, du moins ceux incapables de prendre un minimum de précaution pour s'y connecter. Cerise sur le gâteau : les criminels avaient accès à des données en temps réel, leur permettant d'être notifiés de tout changement de mot de passe et d'accéder aux comptes des victimes sans déclencher les mesures de sécurité. Les autorités américaines ont peu d'espoir de procéder à l'arrestation des têtes dirigeantes du réseau, ceux-ci étant apparemment dans des pays alliés de la Russie. Les victimes, elles, peuvent être n'importe où dans le monde. Les prix des bots étaient variables et dépendaient de la nature des données volées. Cela démarrait à soixante-dix cents et pouvait aller jusqu'à plusieurs centaines de dollars. Les plus chers étaient ceux donnant des informations financières permettant de pirater des comptes bancaires.

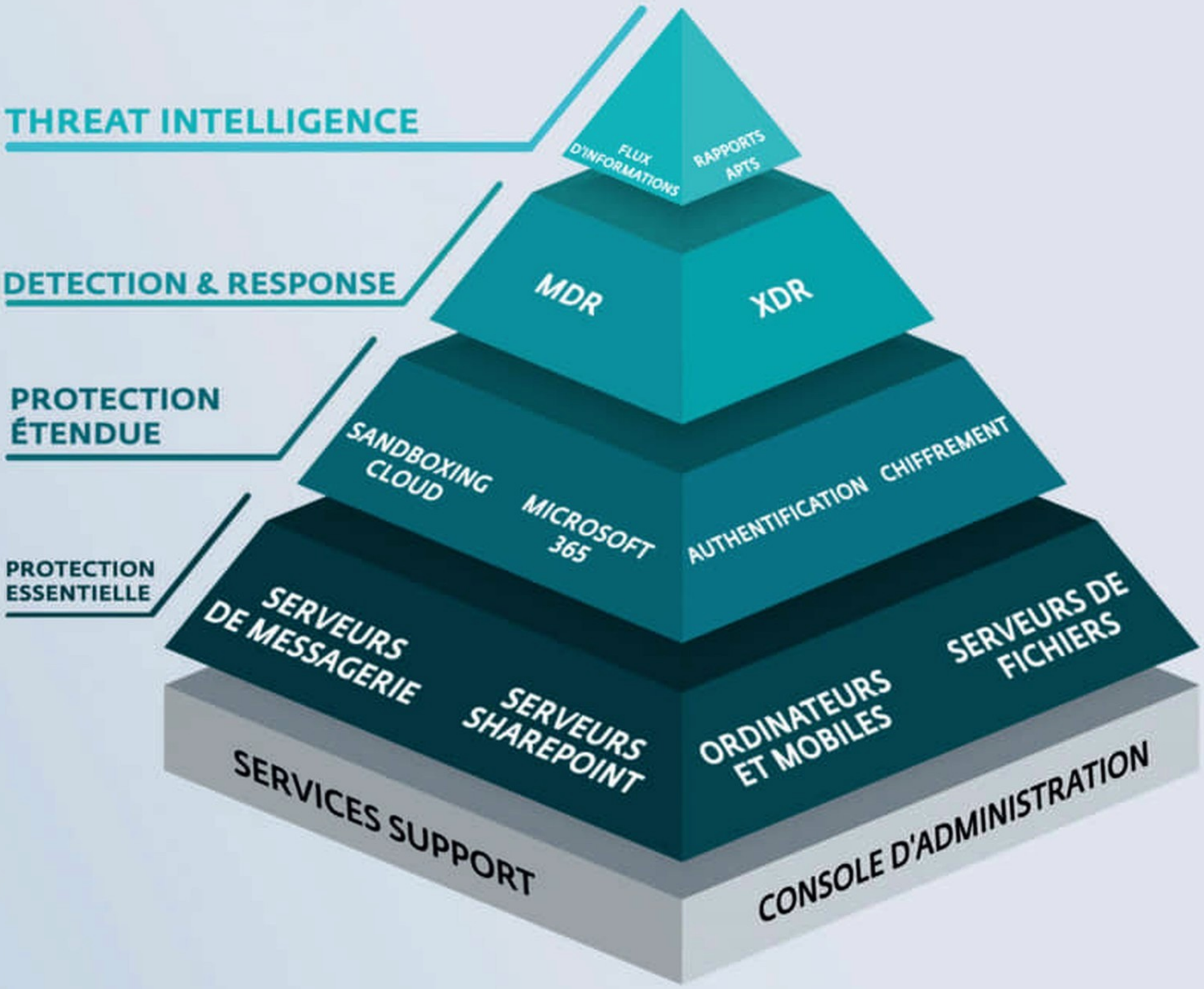
Des enquêteurs spécialisés dans la lutte contre la cybercriminalité

Les cyber-enquêteurs de la sous-direction de la lutte contre la cybercriminalité et de la direction de la police judiciaire de Lyon ont, eux aussi, participé à l'opération. Trois individus impliqués dans cette affaire auraient été arrêtés en Île-de-France et dans la région lyonnaise. La lutte contre la cybercriminalité est enfin devenue une priorité pour les autorités judiciaires du monde entier et de plus en plus de cyber-enquêteurs sont formés et spécialisés dans ce domaine. La collaboration internationale est vraiment nécessaire pour traquer ces cybercriminels qui peuvent être n'importe où dans le monde, tout comme leurs cibles. L'affaire Genesis Market n'en est qu'une preuve supplémentaire. La lutte contre les hackers de ce genre est un véritable défi pour la sécurité numérique à travers le monde. Le démantèlement de Genesis Market représente une avancée majeure dans la lutte contre la cybercriminalité internationale, mais celle-ci est bien loin d'être terminée. 24 arrestations au Royaume-Uni, 17 aux Pays-Bas, 3 en France, 6 au Québec,... Edvardas Sileris, responsable du Centre européen de lutte contre la cybercriminalité d'Europol, a déclaré : « *nous avons gravement perturbé l'écosystème cybercriminel en supprimant l'un de ses principaux catalyseurs* ». Rappelons qu'Europol avait démantelé en avril 2022 le site RaidForums qui vendait l'accès à des fuites de bases de données de sociétés américaines. Un an avant, l'agence de sécurité européenne avait pris le contrôle d'EMOTET, un logiciel malveillant considéré comme le plus dangereux du monde. Si vous voulez savoir si vous faisiez partie des victimes de Genesis, la police néerlandaise a mis à disposition un outil permettant de vérifier si une adresse email était compromise : www.politie.nl/en/information/checkyourhack.html#check ■

T.T

Digital Security
Progress. Protected.

DÉVELOPPEZ VOTRE SOCIÉTÉ LOIN DES CYBERMENACES



RETROUVEZ-NOUS SUR :

WWW.ESET.COM/FR

Loi de programmation militaire : la France à l'assaut des cybermenaces

L'extension du cyberespace est un phénomène global qui impose pour y répondre le développement de capacités de cyberdéfense efficientes. La LPM (Loi de Programmation Militaire) 2019-2025 y avait déjà contribué. 4 articles de la nouvelle LPM viennent les compléter, et c'est ce que nous allons voir maintenant.

La Loi de programmation militaire 2019-2025 visait déjà à renforcer les moyens militaires de la France et, en particulier, son arsenal pour lutter contre les cybermenaces telles que des rançongiciels. Cependant, les opérateurs télécoms n'avaient pas le droit d'analyser le contenu du trafic qui passait dans leurs tuyaux — sauf dérogation exceptionnelle.

Surveillance des réseaux et obligation de transparence

C'est justement ce que cherche à combler l'un de ces articles de la LPM, le 19. Il s'agirait de faire installer aux opérateurs français des systèmes de détection en temps réel des virus qui circulent sur les réseaux. Le cas échéant, les opérateurs seront tenus de prévenir immédiatement leurs abonnés du danger encouru et du potentiel impact sur leurs systèmes. Il n'est, pour autant, pas question que cela se transforme en espionnage généralisé de tout un chacun, comme l'a fait la NSA, a promis le ministère de la Défense. Pour éviter cette dangereuse dérive, l'article 19 du projet de loi stipule que « *les données recueillies autres que celles directement utiles à la prévention des menaces devront être immédiatement détruites* ». Il n'empêche que le procédé pourrait ouvrir la porte à de mauvaises pratiques.

Protection accrue des OIV

Dans le cas d'une attaque imminente contre des autorités publiques ou des OIV (opérateurs d'importance vitale), l'ANSSI sera habilitée à installer des systèmes de détection de menaces directement chez les opérateurs ou hébergeurs. Le personnel de l'agence de sécurité nationale pourra alors recueillir et analyser les données en transit afin de bien caractériser la future attaque. Cela constituera une véritable nouveauté puisque, jusqu'alors, l'ANSSI n'avait pas le droit de prendre le contrôle total d'un hébergeur afin de découvrir qui se cache derrière une attaque. Les données concernées pourront être conservées jusqu'à cinq ans. L'extension du cyberespace à l'échelle planétaire conduit à de potentiels risques d'attaque sur les systèmes électroniques équipant les systèmes d'armement et nécessite pour les contrer le développement de capacités et d'outils de cyberdéfense adaptés. La LPM 2019-25 a, concrètement, permis sur le plan opérationnel l'extension aux cyber-combattants de « *l'excuse pénale* » dont bénéficient les militaires français en mission.

Vous pouvez consulter l'avis du conseil d'état sur la nouvelle LPM sur le site de l'Assemblée nationale à l'adresse www.assemblee-nationale.fr/dyn/16/textes/l16b1033_avis-conseil-etat.pdf

Cette logique est identique pour tous les systèmes, qu'ils soient utilisés par des particuliers ou des entreprises en raison de la dépendance globale de notre société vis-à-vis de l'informatique et des réseaux. L'ANSSI mettra en œuvre ce dispositif à des fins de protection des autorités publiques ou des OIV et ce dans une logique globale. La permanence et l'accroissement continu des menaces de type cyber ont conduit à l'adoption d'une PPC (Posture Permanente Cyber). Placée sous le contrôle opérationnel du COMCYBER, la PPC regroupe l'ensemble des mesures prises afin d'assurer la défense des forces armées dans le cyberespace, que ce soit en temps de paix ou de guerre : détection des menaces, sécurisation des déploiements, contre-attaques et blocage immédiat des agressions numériques. Les effectifs qui seront dédiés à cette PPC viendront

renforcer le COMCYBER ainsi que le CALID (Centre d'Analyse et de Lutte Informatique Défensive) et le CIAE (Centre Interarmées des Actions sur l'Environnement). D'autres effectifs spécialisés auront pour rôle de renforcer les SOC (Security Operation Center ou centres opérationnels de sécurité des armées).

LPM 2024-2030

Quatre articles de la nouvelle LPM prévoient le renforcement des pouvoirs de l'ANSSI et de son champ d'intervention à la faveur de la prochaine loi de programmation militaire 2024-2030 (https://www.assemblee-nationale.fr/dyn/16/textes/l16b1033_projet-loi). Ces dispositions doivent permettre à l'agence de sécurité *« d'augmenter sa connaissance des modes opératoires des cyberattaquants, de mieux remédier aux effets de leurs attaques et d'alerter plus efficacement les victimes des incidents ou des menaces pesant sur leurs systèmes d'information »*, a précisé le gouvernement. Ce projet de loi doit être l'occasion, *via* son article 35, de revoir les dispositions relatives aux sondes et à la recherche de marqueurs techniques. Ces mesures déjà introduites dans la précédente LPM avaient, à l'époque, fait couler pas mal d'encre. Néanmoins, pour l'ANSSI, le résultat n'avait pas été à la hauteur de ses attentes. L'agence s'était notamment heurtée à une forte divergence avec le régulateur des télécoms qui a une lecture différente des autorisations de collecte des données. L'ANSSI n'a accès pour l'instant qu'aux effets des activités malveillantes, les flux réseaux qui en sont issus, et non à leurs causes, le code qui a permis l'intrusion, les logs ou le contenu stocké. Il s'agirait, par exemple, de permettre à l'agence d'obtenir une copie de serveur(s) utilisé(s) par des attaquants. L'ANSSI table également sur une extension du périmètre aux opérateurs du cloud pour prendre en compte l'évolution de la menace. Le gouvernement a en effet souligné la *« fréquente utilisation par des attaquants de serveurs compromis, qui sont loués par des hébergeurs étrangers mais auprès d'opérateurs de centres de données qui sont, eux, basés sur le territoire national »*. Cet article de la LPM prévoit de plus de rendre obligatoire la mise en place de capacités de détection directement chez les opérateurs de communications considérés comme des OIV. Le gouvernement souhaite élargir aux hébergeurs l'obligation de communication *« à des fins exclusives d'alerte »* aux utilisateurs de systèmes vulnérables ou attaqués. Cela permettrait à l'ANSSI de mieux comprendre les modes opératoires des attaquants et ainsi de pouvoir identifier et alerter bien plus de victimes.

Pour suivre l'avancement de la nouvelle LPM, rendez-vous à l'adresse www.vie-publique.fr/loi/288878-loi-programmation-militaire-2024-2030-lpm

Obligation de signalement et filtrage DNS

En plus de cette première grosse partie législative, le gouvernement planche sur l'introduction d'une nouvelle obligation de signalement pour les éditeurs de logiciels victimes d'attaque informatique ou ayant découvert une faille de sécurité sur un logiciel utilisé sur le territoire national. Le projet de loi veut donc imposer de communiquer ce type d'information à l'ANSSI ainsi qu'aux clients et utilisateurs des logiciels concernés. Cela devrait améliorer la transparence et la réaction aux attaques. Il faut aussi disposer d'un bon bâton pour convaincre les plus récalcitrants. L'ANSSI pourrait faire du *« name and shame »*, c'est-à-dire signaler les injonctions restées sans réponse faites à des éditeurs. La méthode douce n'ayant pas fonctionné, on passe à des techniques plus dures et contraignantes. L'article 32 du projet de loi doit, quant à lui, permettre à l'ANSSI de prescrire des mesures de filtrage de noms de domaine pour neutraliser certaines attaques les exploitant. Cette disposition pourrait prendre la forme d'une injonction à un blocage suivi d'une suspension afin de contrer rapidement une action malveillante. Il est aussi possible d'effectuer une redirection et un transfert du nom de domaine, à des fins de renseignement cette fois. *« Les opérateurs contribueraient ainsi à assurer aux utilisateurs finaux un flux sécurisé de données dans le cadre de leur navigation sur Internet »*, dit encore l'étude d'impact effectuée. *« Cela permettrait aussi d'augmenter de manière significative les capacités nationales de détection des attaques informatiques et donnerait à l'ANSSI la capacité de neutraliser des menaces graves et avérées. »*
Pour finir, le quatrième article prévoit de communiquer à l'agence de sécurité des *« données techniques, non identifiantes, enregistrées temporairement par les serveurs DNS qui établissent la correspondance entre le nom de domaine et l'adresse IP des machines d'un réseau »*. Cela permettrait d'après le gouvernement de combler un vide juridique existant et surtout de détecter les serveurs mis en place par les attaquants afin d'établir la chronologie de leurs attaques. Le Conseil d'État a jugé ces différentes dispositions *« proportionnées »*, mais il a en revanche suggéré de retirer l'une des mesures de ce texte, jugée douteuse. Celle-ci prévoit en effet la possibilité pour l'Agence de sous-traiter le recueil de données techniques à un autre service de l'État. Le projet de loi a été déposé à l'Assemblée nationale et examiné par les députés en mai. Une navette vers le Sénat devrait être effectuée en juin pour une promulgation, si tout est validé rapidement, aux alentours de la fête nationale du 14 juillet, date symbolique s'il en est. ■

T.T

International Security Conference West

Des solutions pour lutter contre les menaces

Grand rendez-vous du monde de la sécurité, le salon International Security Conference West (ISC West) s'est tenu à Las Vegas fin mars.
Lors de cet évènement qui rassemble tous les acteurs du marché et qui couvre tous les domaines (contrôle d'accès, biométrie, IoT, informatique, cybersécurité, etc.), de nombreuses nouvelles solutions ont été présentées pour couvrir des menaces toujours plus importantes.
Le salon a aussi été marqué par le discours inaugural de Theresa Payton, la première femme à avoir occupé le poste de DSI à la Maison-Blanche.

Organisé par Reed Expo en partenariat avec la Security Industry Association (SIA), le salon International Security Conference and Exposition (ISC) se tient deux fois par an aux États-Unis avec une session en novembre sur la côte est et une autre sur la côte ouest. Pour les visiteurs, ce rendez-vous bisannuel est l'occasion de rencontrer des centaines de marques et de découvrir de nouveaux produits et solutions couvrant le contrôle d'accès, la biométrie, les distributeurs, les appareils compatibles IoT, l'informatique et la cybersécurité, la sécurité publique, la sécurité autonome et bien d'autres domaines encore. Organisée à Las Vegas du 28 au 31 mars au Venetian Expo, la session de la côte ouest a rassemblé plus de 27 000 professionnels de l'industrie.

Un keynote inaugural très attendu

Pour l'ouverture du salon, les organisateurs ont choisi de donner la parole à Theresa Payton, la première femme à avoir occupé le poste de DSI à la Maison Blanche et qui s'est fait remarquer pour son engagement dans la lutte contre la cybercriminalité. Bref, une pointure dont le discours

Organisé fin mars à Las Vegas, le salon International Security Conference West a rassemblé quelque 27000 visiteurs, représentant tous les secteurs d'activité de la protection.

inaugural était très attendu. Theresa Payton a ainsi levé le voile sur la manière dont les pirates informatiques opèrent et sur ce que les professionnels de la sécurité peuvent faire pour y remédier. Outre son discours, elle a également partagé de nombreuses ressources en matière de cybersécurité et elle a aussi alerté sur les menaces présentées par ChatGPT, l'un des nouveaux venus dans le domaine de l'IA générative. Sur ce sujet, Theresa Payton a souligné que d'ici à la fin 2024, plus de la moitié du trafic internet généré par un foyer ne sera pas le fait de l'homme, mais de dispositifs et appareils connectés. Les industries déploient des milliards d'appareils connectés — et donc piratables — dans leurs usines. Par ailleurs, les technologies permettant d'exploiter et de sécuriser les installations sont, elles aussi, connectées et vulnérables. *« Les chiffres sont stupéfiants et cela représente toute la vie d'un utilisateur. Il faut y penser et en tenir compte dans les conceptions des produits. C'est très important pour la sécurité et la protection de la vie privée. Les cybermenaces continuent de se répandre dans le monde physique et la façon de s'attaquer à ces menaces est de s'assurer, en tant que communauté de la sécurité, que nous concevons nos produits pour les utilisateurs humains et que nous les prenons en considération »*, a-t-elle déclaré en citant une étude menée par le fournisseur de plateformes de données Domo. *« Notre monde est entièrement numérique, toujours en activité et totalement mobile. Par exemple, 5,9 millions de recherches sont effectuées sur Google, 1,7 million de contenus sont partagés sur Facebook et 66 000 photos sont téléchargées sur Instagram chaque minute. « Lorsque je regarde ces statistiques, je me dis que cela fait beaucoup de données. Sont-elles toutes cryptées ? Sont-elles toutes protégées ? Ces données restent-elles confidentielles ? »*, s'interroge-t-elle.

Première femme à avoir occupé le poste de DSI de la Maison-Blanche, Theresa Payton a réalisé un discours inaugural très attendu. Durant son intervention, elle a expliqué que le risque de menaces, notamment les cyberattaques, était grandissant. Selon elle, la création d'identités synthétiques sera encore plus automatisée grâce à l'intelligence artificielle et à l'analyse des données.

Le décryptage de trois futures menaces

Enfin, l'ancienne DSI de la Maison-Blanche a souhaité faire de la prospective en évoquant trois prédictions sur l'origine des menaces en 2024. Selon elle, la création d'identités synthétiques sera encore plus automatisée grâce à l'intelligence artificielle et à l'analyse des données. *« Des acteurs malveillants créeront des travailleurs numériques qui occuperont des postes à distance leur permettant d'accéder aux systèmes d'une organisation »*, prédit-elle. Concernant les ransomwares, Theresa Payton estime que les cybercriminels pourraient s'organiser d'une autre façon. *« Voyant que les organisations s'améliorent dans la gestion de leur sécurité afin de ne pas payer les incidents liés aux ransomwares, les cybercriminels pourraient passer au piratage d'installations intelligentes et au verrouillage de bâtiments et de zones avec des personnes à l'intérieur, en exigeant une rançon pour leur libération »*, estime-t-elle. Enfin, en utilisant les flux de renseignements sur les menaces, le machine learning et les algorithmes d'intelligence artificielle, les cybercriminels risquent aussi de créer des robots automatisés capables de mener une surveillance numérique et de recueillir des informations sur les organisations, de la direction aux réseaux et aux systèmes. En clair, si les entreprises et administrations publiques améliorent leurs moyens de protection, c'est également le cas du côté de la sphère cybercriminelle.

Des fabricants et développeurs sortent du lot

Au cours de cette édition 2023, les organisateurs ont, comme chaque année, décerné des prix à des fabricants et développeurs qui se sont particulièrement fait remarquer à travers les New Products & Solutions Awards. Parmi eux, la société américaine Alocity a reçu le prix du meilleur nouveau produit 2023 avec Alocity Access Control Platform dans la catégorie *« dispositifs et périphériques de contrôle d'accès sans fil »*. En quelques mots, Alocity Access Control Platform est une plateforme de sécurité intelligente qui gère le contrôle d'accès avec des capteurs vidéo et connectés, un lecteur multifonction avec vérification faciale 3D, des identifiants mobiles *via* les technologies Bluetooth et NFC. *« Le panneau de contrôle d'accès intégré permet de contrôler les serrures de porte électroniques, les boutons de sortie et les contacts de porte sans fils »*, indique le fabricant qui développe aussi un logiciel de contrôle d'accès utilisant le cloud avec vidéo en direct. Cette solution facilite la gestion, la surveillance et le contrôle des portes à tout moment, n'importe où, depuis n'importe quel appareil. Toujours dans le registre de la biométrie, la société taïwanaise RogersAI a également démontré tout son savoir-faire avec un terminal utilisant une

technologie de traitement d'image 3D développée en interne avec un algorithme de reconnaissance 3D breveté. *« La fonction principale de notre terminal IA de reconnaissance d'identité 3D est d'utiliser uniquement la caméra 3D pour enregistrer et extraire en temps réel les caractéristiques biométriques de l'utilisateur afin de traiter le résultat de la reconnaissance d'identité sans prendre de photo couleur. Ce processus permet de résoudre les problèmes de confidentialité, de conditions d'éclairage et de lutte contre les usurpations d'identité liées aux systèmes traditionnels de reconnaissance faciale à partir de photos en couleur »*, précise l'entreprise.

Identifier et prévenir les menaces

De son côté, Resolver Software a présenté une nouvelle application de protection contre les menaces, qui aide les équipes de sécurité. *« La plupart des entreprises ont du mal à établir rapidement des profils solides pour les menaces potentielles et ne sont pas formées à l'application de méthodologies d'évaluation des menaces, ce qui rend difficile l'évaluation fiable des menaces à grande échelle »*, explique Ryan Thiessen, vice-président des produits de sécurité et d'investigation. Il poursuit : *« avec le lancement de Threat Protection, les responsables de la sécurité disposent ainsi d'une meilleure visibilité sur les mesures prises par les équipes pour lutter contre les menaces afin de protéger l'organisation et d'empêcher les incidents de se produire »*. En effet, l'application Threat Protection va relier les renseignements sur les menaces provenant de n'importe quelle source, ce qui permet aux entreprises de trouver des liens entre les ensembles de données et de repérer les signes avant-coureurs. Cette application est intégrée au logiciel de gestion des incidents et des cas de Resolver. À noter que Resolver s'est également associé aux entreprises LifeRaft et Topo.ai.

Parmi les autres lauréats, le jury a souhaité récompenser la société IPVideo Corporation avec un prix spécial pour sa solution Sentry ERS. *« Sentry ERS est un système de verrouillage et d'intervention d'urgence spécialement conçu pour les écoles »*, explique l'entreprise. D'une simple pression sur un bouton, les protocoles de verrouillage sont lancés et des alertes immédiates sont envoyées à la police, ce qui permet une meilleure connaissance des incidents avec des données vidéo, vocales, textuelles et de localisation GPS en direct dans les zones où les caméras vidéo traditionnelles ne peuvent pas être déployées.

Mieux exploiter la vidéosurveillance

Dans la catégorie des services, le logiciel AI-rgus, mis au point pour la Duke University (Caroline du Nord), rend possible la vérification automatique des caméras de sécurité pour savoir si elles produisent bien leurs vidéos. *« Grâce à l'utilisation d'AI-rgus, l'équipe de sécurité de la Duke University a réduit le temps passé à inspecter plus de 2 000 caméras de 4 heures par jour à 5 minutes, réduisant considérablement la charge de travail et la durée moyenne de fonctionnement des caméras »*, indique l'entreprise. La vidéosurveillance étant devenue un élément majeur de la sécurité, elle nécessite aussi de lourdes capacités de stockage. À ce titre, Wasabi Technologies et sa solution Wasabi Surveillance Cloud ont apporté une réponse à cette problématique. *« La prolifération des caméras haute résolution et les exigences strictes de conservation et de conformité entraînent un besoin de capacités de stockage plus important. Avec Wasabi Surveillance Cloud, nous proposons une offre groupée qui intègre notre application logicielle WSC Cloud Bridge avec un abonnement de stockage via le cloud de Wasabi. Les utilisateurs de tous les principaux systèmes de gestion vidéo (VMS) ont désormais la possibilité de décharger les données de vidéosurveillance de leur environnement de stockage local vers le cloud sans modifier leurs opérations existantes »*, annonce l'entreprise qui est repartie avec un prix dans la catégorie stockage de données pour la vidéosurveillance.

Pour finir sur ces innovations qui ont marqué cette International Security Conference and Exposition, il faut aussi citer Bosch qui a reçu un award pour l'ensemble de son travail dans la sécurité. *« En sensibilisant aux nouveaux produits et technologies qui améliorent la sécurité et les opérations, le programme New Products & Solutions contribue à faire progresser notre industrie. Avec ce programme, les intégrateurs, les consultants et les utilisateurs finaux participant à ISC West peuvent identifier plus facilement les derniers produits et solutions qui aident à résoudre les problèmes de sécurité et de sûreté courants »*, a déclaré Chuck O'Leary, vice-président des ventes de la division systèmes et solutions vidéo de Bosch.

La prochaine édition du salon ISC, pour la côte est des États-Unis, se tiendra du 14 au 16 novembre 2023 à New York. En 2024, ISC West reviendra à Las Vegas du 9 au 12 avril. ■

Michel Chotard

Durant le salon ISC West, les entreprises présentes ont dévoilé de nombreuses nouveautés dans des secteurs comme le contrôle d'accès, la biométrie, les IoT, l'informatique et la cybersécurité.

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

by weyou group
Professional Exhibitions and One to One Meetings Exhibitions

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.