N° 220 — Octobre 2023

www.linformaticien.com

L'INFORMATICIEN

Hardware
Les biohackers arrivent

ESN
TCS en France

Logiciel
Comment les DSI voient la Gen AI

DOSSIER

LES NOUVEAUX HABITS DE L'ERP

Retex
Cdiscount

Bonnes feuilles
Donnerons-nous notre langue au ChatGPT ?

L 14614 - 220 - F: 8,50 € - RD

Tenacy

ALL YOUR CYBER IN ONE PLACE

tenacy.io

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, Jérôme Cartegini, Michel Chotard,
Alain Clapaud, François Cointe, Victor Miget et Thierry Thaureaux.

SECRÉTAIRE DE RÉDACTION : Boutheïna Saddi

MAQUETTE ET RÉALISATION : Franck Soulier (chef de studio)

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

VENTE AU NUMÉRO

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

ABONNEMENTS

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

Toutes les offres :
www.linformaticien.com/abonnement

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

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

IMPRESSION

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

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

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

ISSN 1637-5491
Une publication PCpresse,

GROUPE FICADE

PRÉSIDENT, DIRECTEUR DE LA PUBLICATION :
Gaël Chervet

Tout change parce que rien ne change

Les ERP ont bien évolué depuis leurs débuts au siècle dernier. D'ailleurs, ils ne s'appellent plus comme cela mais plate-forme d'applications d'entreprise. Cela rappelle ainsi le chemin parcouru. Ils connaissent de nombreuses évolutions avec l'apport de technologies comme la mobilité, le low code ou l'intelligence artificielle. Ils se couvrent de nouveaux habits pour répondre aux nouveaux besoins des entreprises. Ils ne laissent cependant pas leur place à d'autres et restent la colonne vertébrale de l'activité de l'entreprise. Ils avaient donc toute leur place pour un dossier dans *L'Informaticien*.

De plus, ce numéro est résolument tourné vers le monde de demain et l'innovation avec des articles sur l'intelligence artificielle, les bio-hackers ou les hommes augmentés de demain, les stylos enregistreurs… Il effleure ce que pourra être le travail ou notre vie demain avec tous ces outils en main.

En outre, ce numéro marque le début de la troisième édition de notre Palmarès. Je ne peux que vous encourager à vous rendre sur les pages de notre site dédié pour mettre en avant les produits que vous appréciez ou que vous voulez promouvoir. Il vous suffit de se rendre à cette adresse : https://enquete.linformaticien.com/index.php/336279?newtest=Y&lang=fr pour le faire !

Comme toujours vous retrouverez nos rubriques habituelles et notre supplément dédié à la cybersécurité qui traite de la sécurité des environnements OT. □

Bertrand Garé
Rédacteur en Chef

Conseil, pilotage et développement IT

meritis

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

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

TOP 3

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

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

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

Nous recherchons de nombreux profils !
Venez nous rencontrer.



Paris
75008
36 Avenue Pierre 1er de Serbie

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

Aix-en-Provence
13290
240 Rue Paul Langevin

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

Nantes
44000
1 rue Eugène Varlin







DOSSIER ..... P 15
Les nouveaux habits de l'ERP

BIZ'IT ..... P 8

BIZ'IT PARTENARIAT ..... P 12

TACTIC ..... P 23
L'anglais, le nouveau SQL ?

HARDWARE ..... P 26
Getac
Erase4good
Biohacker

ESN ..... P 32
TCS
Numeum

RÉSEAU ..... P 36
Cato Networks

LOGICIEL ..... P 39
Python dans Excel
Teradata
GenAI et les DSI
Stack Overflow

CLOUD ..... P 48
mWise
Dreamforce
Snowflake Summit

RETEX ..... P 55
Axeptio
Keolis
Cdiscount

DEVOPS ..... P 58
gRPC

BONNES FEUILLES ..... P 63
Donnerons-nous notre langue au ChatGPT ?

INNOVATION ..... P 68
OSTIF.org
Stylo Philips

ÉTUDE ..... P 70

RH ..... P 72
Tendances salaires IT

INFOCR ..... P 73
Cahier spécial Sécurité

ABONNEMENTS ..... P 38

Construire des applications métiers solides, performantes et durables !

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



AXOPEN

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

axopen.com

L'ERP IDÉAL


DATA COMPRESSOR
DOPÉ À L'IA DÉGÉNÉRATIVE
INJECT NEW DATA
TOXICO CLOUD
LA MIGRATION VERS NOTRE NOUVEL ERP, C'EST UNE CALAMITÉ...
PLUS RIEN NE MARCHE...
IL Y A DES ÂMES DATAS COUPÉES EN MORCEAUX DANS LES NUAGES.
LES PIRATES, ILS SONT ENTRÉS PENDANT LE TRANSFERT ET ONT PIQUÉ TOUS NOS FICHIERS CLIENTS.
300 MILLIARDS!
ON LIVRE N'IMPORTE QUOI À N'IMPORTE QUI... ET ON LEUR FACTURE ET DÉLIVRE 10 FOIS LE MÊME PRODUIT.
C'EST PARFAIT. C'EST EXACTEMENT CE QUE JE VOULAIS.
ET ON NE PEUT PAS RÉPARER: TOUS NOS PRESTATAIRES ONT FAIT FAILLITE, COMME ON NE LES PAYE PAS...
C'EST L'ENFER, ICI. CE N'EST PAS LE PARADIS.
NOS CLIENTS, ILS SONT LÀ POUR EN CHIER...
F. COINTE

FOCUS

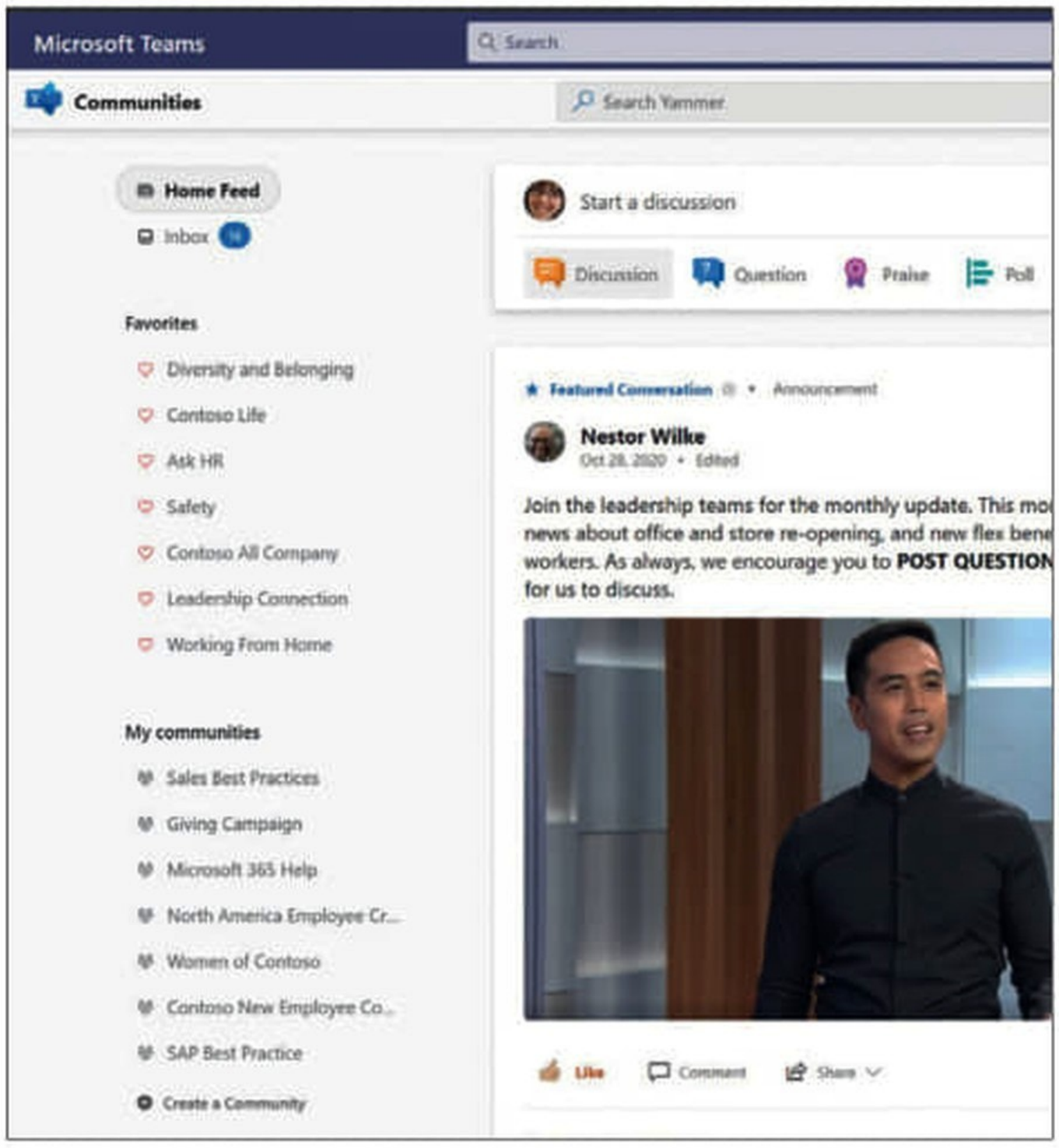
Teams et Office 365 se séparent en Europe

Menacé par une enquête de la Commission européenne, le géant américain a pris les devants et a décidé de ne plus intégrer systématiquement sa plateforme collaborative dans ses offres Microsoft 365 et Office 365. Une séparation effective à compter du 1er octobre prochain.

Fin juillet, la Commission européenne annonçait l'ouverture d'une enquête quant aux possibles pratiques anticoncurrentielles de Microsoft. Bruxelles considère que, en intégrant sa plateforme collaborative Teams à ses offres Microsoft 365 et Office 365, l'éditeur avantage honteusement sa solution, aux dépens de la concurrence.

L'éditeur de Redmond a choisi de prendre les devants, annonçant fin août une série de changements à venir pour rentrer dans les clous et satisfaire les exigences des autorités européennes et de ses concurrents *« même si l'enquête de la Commission européenne se poursuit et que nous coopérons avec elle »*. *« Nous reconnaissons notre responsabilité en tant que fournisseur technologique majeur de soutenir un environnement concurrentiel sain »* poursuit Microsoft dans un communiqué.

Ainsi, à compter du 1er octobre, dans l'Espace économique européen et en Suisse, les clients de Microsoft pourront opter pour une suite professionnelle sans Teams. Et ce, pour un prix inférieur de 2 euros par mois. Teams reste disponible pour les nouveaux clients, seul, au prix de 5 euros par mois. *« Les entreprises clientes existantes qui disposent déjà d'une suite avec Teams peuvent choisir de conserver leur suite de productivité actuelle ou de passer à une suite sans Teams »* précise l'éditeur. Les PME et indépendants auront droit aux mêmes types d'offres.



Une solution « pragmatique »

En outre, le géant promet d'améliorer ses ressources existantes en matière d'interopérabilité avec Microsoft 365 et Office 365. S'il documente déjà ses API, Microsoft explique que, *« dans le cadre du processus d'enquête, nous avons entendu des commentaires selon lesquels, compte tenu des vastes capacités de Microsoft 365, [il] pourrait faire davantage en termes de support et de simplification du développement »*. Au menu, de nouvelles ressources de support à destination des développeurs d'applications tierces, notamment pour la réutilisation et la suppression des données de Teams. Enfin, l'éditeur s'engage à permettre à des solutions tierces d'héberger des fichiers Office, avec les mêmes fonctionnalités que dans la solution de Microsoft.

L'éditeur explique ne pas agir avec *« le sentiment que cela résoudra nécessairement toutes les préoccupations, qu'elles émanent de la Commission ou de nos concurrents »* mais y voit une étape *« constructive »*. *« Nous continuerons à dialoguer avec la Commission, à écouter les préoccupations du marché et à rester ouverts à l'exploration de solutions pragmatiques qui profiteront à la fois aux clients et aux développeurs en Europe »* conclut-il.

L'amende européenne d'Intel réduite



En 2009, la Commission européenne avait condamné Intel à une amende d'1,06 milliard d'euros. À l'époque, elle accusait à Intel d'avoir accordé des remises totales ou partielles aux fabricants d'ordinateurs, à conditions qu'ils achètent leurs processeurs x86 et retardent ou arrêtent le lancement de produits contenant des processeurs x86 concurrents. Intel avait fait appel de la décision et après plusieurs années de bataille judiciaire, le Tribunal de l'Union européenne avait partiellement annulé la décision de la Commission européenne en 2022. Suite à ce jugement, la Commission a ajusté son amende en conséquence. *« La Commission a donc décidé de réimposer une amende d'environ 376,36 millions d'euros à Intel. L'amende inférieure imposée par la décision d'aujourd'hui reflète la portée plus étroite de l'infraction par rapport à la décision de la Commission de 2009 »*, écrit-elle dans son communiqué. La fin d'un feuilleton judiciaire ? Rien n'est moins sûr. Intel envisage un recours devant les tribunaux après analyse de la décision et du montant, pour déterminer quelles sont ses chances de l'emporter. *« Bien que nous soyons déçus par une amende de ce montant, nous continuons à nous concentrer sur nos futurs investissements dans l'UE et à coopérer avec la Commission pour aider à faire progresser l'industrie européenne des semi-conducteurs »*, a néanmoins précisé l'entreprise dans un communiqué.

L'État met 2,5 millions d'euros dans dix startups

Le Fonds d'Accélération des Startups d'État et des Territoires (FAST) de la direction interministérielle du numérique a annoncé qu'il allait financer dix jeunes pousses à hauteur de 2,5 millions d'euros afin d'accélérer la transformation numérique de l'État. Le fonds dispensera un accompagnement opérationnel et stratégique de 6 mois et financera les lauréats à hauteur de 50 % du budget du projet sur l'année, dans la limite de 300 000 € par startup. Les candidatures pour la 14ème édition sont d'ores et déjà ouvertes, jusqu'au 1er décembre prochain.

La direction interministérielle du numérique (DINUM), un service de l'État qui élabore la stratégie numérique et accompagne les projets numériques de l'État a ainsi retenu pour cette 13ème édition du programme :

- A-Just, une solution de Pilotage de l'affectation des ressources humaines dans les juridictions pour réduire les délais de justice.
- EnvErgo, un outil de prise en compte de l'environnement dans les projets d'aménagement.



- L'Annuaire des collectivités qui doit fournir un site web à chaque commune de France.
- Réfugiés.info, un service qui vise à favoriser l'intégration des réfugiés en France en livrant une information simple et traduite.
- Data.Subvention, qui ambitionne de réunir les informations sur les associations et leurs subventions afin de simplifier la vie des associations et des agents publics.
- DossierFacile, afin de rétablir la confiance au centre de la relation entre propriétaires et locataires.
- Ma Cantine, pour l'accompagnement des acteurs de la restauration collective afin de proposer une alimentation plus qualitative et durable.
- Docurba, qui souhaite faciliter l'élaboration et le suivi des documents d'urbanisme en améliorant les échanges entre les collectivités et l'État.
- Mano, qui veut soutenir les équipes mobiles dédiées à améliorer la vie des populations en rue.
- Mobilic, qui cherche à simplifier le suivi et le respect du temps de travail des travailleurs mobiles.

RACHATS

Cisco s'offre Splunk

Acquisition XXL pour Cisco. L'équipementier et le spécialiste du SIEM et de l'observabilité Splunk ont annoncé, jeudi 21 septembre, avoir conclu un accord définitif pour l'acquisition de Splunk par Cisco. Montant de l'opération : 28 milliards de dollars. *« Nous sommes ravis de réunir Cisco et Splunk. Nos capacités combinées seront à l'origine de la prochaine génération de sécurité et d'observabilité basées sur l'IA »* indique Chuck Robbins, PDG de Cisco. S'il est encore trop tôt pour dire ce qui ressortira concrètement de cette union, les deux sociétés ambitionnent de former un leader mondial de la sécurité et de l'observabilité qui exploitera l'Intelligence artificielle afin de fournir des solutions de protection et renforcer la résilience des organisations, de leurs appareils, applications et environnements cloud. Un indispensable selon les deux partenaires qui estiment qu'à l'avenir, avec l'adoption des solutions d'IA générative, les entreprises s'exposeront à une surface de menace toujours plus grande, et à un niveau de complexité *« sans précédent »* du fait de la multiplicité des environnements cloud. Selon le communiqué annonçant le rachat, *« les capacités complémentaires de Cisco et de Splunk offriront une observabilité dans les environnements hybrides et multicloud, permettant aux clients de l'entreprise de proposer des expériences applicatives fluides qui dynamisent leurs activités numériques »*.



Netskope rachète le français Kadiska

Netskope, l'un des premiers à s'être placés sur le créneau du SASE, a annoncé le rachat d'une jeune pousse tricolore. Kadiska est en effet une société née en 2020 du côté de Rouen, et toujours sise dans la région. Elle édite une plateforme de Digital Experience Monitoring, ou gestion de l'expérience numérique, décrite par Netskope comme *« un élément clé d'une architecture SASE, où la sécurité et le réseau convergent pour connecter de manière sécurisée et optimale les utilisateurs, les appareils et les sites aux applications, aux sites web et aux données, quelle que soit leur localisation »*. La plateforme de Kadiska combine la surveillance de l'expérience utilisateur réelle avec la visibilité des performances du réseau et la surveillance des applications sur les plateformes d'hébergement cloud hybride, SaaS et PaaS.

Atmosec rejoint Check Point

Toujours sur le terrain du SASE, Check Point s'empare d'Atmosec, pour un montant non divulgué. Cette jeune pousse fondée en 2021 est spécialisée dans la sécurité du SaaS, entendre par là qu'elle propose des outils dédiés à la découverte des connexions et accès à des applications tierces, à la détection des droits et des erreurs de configuration et au blocage des applications malveillantes. L'éditeur entend intégrer les différentes fonctions d'Atmosec dans sa plateforme Infinity, de sorte à lui ajouter la gestion de la posture SaaS à travers une brique technologique comprenant visibilité complète sur les applications SaaS autorisées et non autorisées, déconnexion des applications malveillantes, correction des erreurs de configuration et MFA.

Exclusive Networks s'installe en Europe du Sud

Après s'être étendu en Europe centrale avec l'acquisition du distributeur à valeur ajoutée polonais Veracomp, Exclusive Networks remet le couvert. Dans son viseur cette fois-ci, l'Europe du Sud. L'entreprise française, cotée à Euronext et passée sous la direction britannique, a jeté son dévolu sur Ingecom. Cette société espagnole fondée en 1996 est spécialisée dans les solutions de cybersécurité et de cyber intelligence. Installée à Bilbao, elle est forte d'une cinquantaine de salariées, mais aussi et surtout de quelque 500 partenaires. Ce réseau permettra à Ignition Technology, la branche distribution dédiée à la cyber d'Exclusive Networks, d'accélérer son expansion en Europe du Sud. Le montant de l'opération n'a pas été divulgué. Aux termes de l'accord, Exclusive Networks détiendra 70 % d'Ingecom, le reste du capital demeurant détenu par ses dirigeants actuels.

Une **Serie C** pour **AI21 Labs.**



La startup a annoncé avoir bouclé un tour de table de série C de 155 millions de dollars, ce qui porte sa valorisation à 1,4 milliard de dollars. L'opération a été bouclée auprès d'investisseurs tels que Walden Catalyst, Pitango, SCB10X, b2venture, Samsung Next, le professeur Amnon Shashua, Google et NVIDIA. Avec cette nouvelle enveloppe, le fondateur et président de la société, Amnon Shashua, dit vouloir développer *« le prochain niveau d'IA avec des capacités de raisonnement dans plusieurs domaines »*. La société souhaite également augmenter ses effectifs et poursuivre le déploiement de solutions de langage naturel, basées sur ses propres grands modèles de langage (LLM) et système neuro-symboliques. Fondée en 2017, AI21 développe des solutions reposant sur le traitement du langage naturel.

Nord Security lève **100 millions de dollars**

Nord Security est l'éditeur spécialisé en cybersécurité et propose le bien connu NordVPN, ainsi que le gestionnaire de mot de passe NordPass et le logiciel de sécurité d'accès réseau NordLayer. L'entreprise lithuanienne fondée en 2012 lève de nouveau 100 millions de dollars, dans un second tour de financement auprès de Warburg Pincus, Novator Ventures et Burda Principal Investments. En avril 2022, Nord Security avait déjà levé 100 millions de dollars lors de son tout premier tour de table. Ces fonds lui serviront à accélérer la mise en place de nouveaux produits et accélérer sa croissance par des acquisitions.

Stoïk se lance **en Allemagne**

Stoïk poursuit son développement et se projette désormais à l'international. L'insurtech annonce la levée de 10 millions d'euros auprès de quatre fonds d'investissement. Munich Re Ventures mène la danse, accompagné d'Opera Tech Ventures et des investisseurs historiques Andreessen Horowitz et Alven. Cette opération doit permettre à Stoïk de se lancer sur le marché allemand, avec l'ouverture d'un premier bureau à Cologne et de constituer une équipe. Celle-ci sera dirigée par Franziska Geier (ci-contre), l'ancienne directrice de la stratégie européenne de l'assureur allemand Markel.



10 millions d'euros pour **Stane**

La start-up lyonnaise Stane a annoncé avoir bouclé une levée de fonds de 10 millions d'euros auprès du fonds souverain Auvergne Rhône-Alpes et du fonds Mutuelles Impact gérés par Siparex. La société, qui se présente comme le premier réseau intégré de santé en ville, s'est spécialisée dans la création et le pilotage de structures de soins primaires et de coordination territoriales. Avec ce nouveau financement, Stane prévoit d'embaucher 70 nouveaux collaborateurs et de lancer Stane App pour l'été 2024, une plateforme de données de santé en ville visant à garantir une gestion confidentielle et sécurisée de données médicales.

Arm arrive au **Nasdaq**

Arm a débuté sa cotation au Nasdaq le 14 septembre. Le concepteur de puces, toujours détenu à 90% par Softbank, a été évalué à 60 milliards de dollars après avoir mis en vente 95,5 millions d'action à 51 dollars pièces, donc dans la fourchette haute des prévisions. 735 millions de dollars d'actions ont notamment été vendus à un groupe d'investisseurs comprenant Samsung, Google, Apple, Nvidia, AMD, Intel, Samsung et TSMC. L'entreprise ne réalise pourtant qu'un chiffre d'affaires de 2,7 milliards de dollars pour 520 millions de bénéfices. D'autant que la société a annoncé une baisse de son chiffre d'affaires de 1% le mois dernier. Pourtant, les prochaines années s'annoncent radieuses pour l'industriel ô combien stratégique, dont les architectures de puces, peu énergivores, alimentent la quasi-totalité de smartphones, tablettes, ainsi qu'une bonne partie des voitures entre autres...

Kudelski et Hunters deviennent partenaires

Le fournisseur de solutions de sécurité va intégrer la solution d'Hunters dans ses SOC (Security Operation Centers).

Dans le cadre de ce partenariat, Kudelski Security intégrera la plateforme SOC de Hunters dans la chaîne de valeur de son Cyber Fusion Center (CFC) afin de renforcer ses services MDR (Managed Detection and Response) et d'obtenir de meilleurs résultats en matière de sécurité. La plateforme SOC de Hunters intègre, normalise et analyse les données provenant de toutes les sources de sécurité (IT/OT). S'appuyant sur la plateforme Snowflake, Hunters facilite le stockage, la connexion et le traitement de quantités considérables de données afin de fournir des analyses pointues. La plateforme offre des capacités de détection et d'investigation intégrées, transparentes et régulièrement mises à jour, et s'appuie sur une corrélation entre les sources de données, des modèles de détection, des recherches et un regroupement des alertes en fonction de leur contexte. La plateforme réduit le coût et la complexité des opérations de sécurité et minimise le temps nécessaire pour comprendre, répondre et contenir les menaces réelles.

Un nouveau partenariat pour Sysdig

L'éditeur de solutions de sécurité pour les applications nativement Cloud signe un nouveau partenariat avec Cybereason.



La forme concrète du partenariat tient en une intégration entre le XDR de Cybereason et la détection et réponse Cloud de Sysdig. La plateforme de protection des applications Cloud-native (CNAPP) de Sysdig offre une détection et une réponse Cloud (CDR) en temps réel, ainsi qu'une gestion des vulnérabilités, des droits et de la posture. Combinées à la plateforme Cybereason XDR, les organisations peuvent désormais étendre la protection, la détection et la réponse aux menaces centrées sur les opérations pour l'ensemble de l'organisation. Le module de Sysdig qui s'appuie sur la technologie open source Falco va servir à détecter les événements suspicieux et générer des alertes. Cela inclut des informations sur le runtime. Les informations sont ensuite poussées pour enrichir le XDR de Cybereason qui va corréler ces signaux avec ses propres données. Ces événements sont ensuite corrélés avec les données issues des terminaux, du réseau, des identifications et du Cloud pour décrire un historique d'une attaque avec des recommandations de réponse et de tri en 24/7 en provenance des équipes de l'offre de service managé de détection et réponse de Cybereason. Cette intégration fait suite à celle avec la plateforme Checkmarx One annoncée le 8 août dernier lors de la Black Hat et celle avec ServiceNow en avril dernier.

Teradata partenaire avec Nordcloud

L'éditeur de solutions analytiques collabore avec Nordcloud, un intégrateur spécialisé dans le giron d'IBM, pour aider leurs clients européens à migrer leurs données sur site et leurs environnements analytiques vers la plateforme Teradata VantageCloud Analytics and Data.

Avec plus de 1000 déploiements en nuage, Nordcloud est spécialisé de plus dans le développement d'applications, de services managés et de formation. L'entreprise est également triplement certifiée AWS, Microsoft Azure et Google Cloud. Teradata et Nordcloud seront ainsi en mesure d'accélérer les déploiements cloud, de répondre aux différentes attentes de leurs clients en matière de cloud et de permettre aux entreprises de tirer pleinement parti de la prochaine génération d'analyses avancées et d'IA dans le cloud. Pour rappel, Teradata VantageCloud est une plateforme complète d'analyse et de données dans le cloud, désormais dotée d'un déploiement cloud-native de nouvelle génération et de ClearScape Analytics, qui permet aux entreprises de résoudre rapidement des problèmes complexes grâce aux capacités d'IA/ML et aux opérations de Machine Learning.

IBM et Salesforce étendent leur collaboration

Les deux entreprises ont annoncé une nouvelle collaboration afin d'accélérer l'adoption de l'intelligence artificielle pour la gestion de la relation client.

IBM Consulting mettra son expertise et ses modèles de prestations innovants, notamment sa méthode IBM Garage dans l'adoption et le déploiement des technologies d'IA de Salesforce. En plus d'aider les clients à déployer efficacement les outils d'IA générative de Salesforce, IBM Consulting pourra compléter ces solutions avec IBM watsonx. Pour rappel, IBM watsonx permet d'identifier les données stockées dans les systèmes back-end pour aider à créer des expériences utilisateurs et employés dynamiques. Avec IBM Consulting Managed Services for Salesforce, les clients en commun auront accès à un ensemble de cas d'usages et de mise en place de solutions d'IA. Cette offre est conçue pour aider les clients à déployer, mettre à l'échelle et améliorer Salesforce.
Il est à noter qu'IBM a utilisé l'IA générative de Salesforce, Slack et IBM watsonx pour sa propre transformation afin de créer une expérience client à 360 degrés. Le service client et les organisations commerciales d'IBM peuvent dorénavant, avoir une vision holistique du parcours client. Les équipes du monde entier collaborent et travaillent ensemble sur une plateforme unique pour fournir une réponse rapide, basée sur des données, répondant aux besoins des clients là où ils se trouvent. IBM a utilisé l'architecture API ouverte de Salesforce pour intégrer IBM watsonx Assistant dans Salesforce Customer 360.

Cisco et Nutanix partenaires

Les deux entreprises se sont accordées autour d'un partenariat stratégique global pour accélérer le déploiement des environnements hybrides multicloud.

La nouvelle offre comprend une solution complète de déploiement avec un environnement virtualisé, le réseau, le stockage pour les centres de données et le Cloud public en combinant les serveurs de Cisco (serveurs UCS avec Cisco Intersight) et l'ensemble des éléments de la plateforme de Nutanix (Nutanix Cloud Infrastructure, Nutanix Cloud Manager, Nutanix Unified Storage et Nutanix Desktop Services). La solution sera vendue par Cisco et son réseau de partenaires. Ainsi, les clients vont bénéficier d'une solution vendue, construite, gérée et supportée pour une expérience de bout en bout. La solution se veut modulaire avec des déclinaisons en racks et serveurs lames avec initialement des serveurs C-Series et plus tard des X-Series. Les solutions de Cisco de sécurité et de gestion du réseau vont être intégrées avec le logiciel de Nutanix. La solution sera disponible 90 jours après l'annonce de la solution.

Sinequa collabore avec NVidia

L'éditeur d'une solution de recherche d'origine française va s'appuyer sur les modèles DGX de NVidia pour développer des modèles d'intelligence artificielle.



Sinequa va en effet utiliser les systèmes NVIDIA DGX H100 de NVIDIA pour développer de grands modèles linguistiques personnalisés et entraînés afin d'offrir des capacités de recherche neuronale assistées par l'IA. Egalement, Sinequa s'appuiera sur la puissance des systèmes et des logiciels NVIDIA pour améliorer la précision des modèles existants en vue de les déployer rapidement dans sa plateforme. Cette dernière associe la solution Neural Search et le service Open AI disponible dans l'environnement Microsoft Azure à n'importe quel grand modèle de langage génératif. Cette alliance permet d'enrichir les fonctionnalités d'IA de Sinequa en ajoutant des cas d'utilisation d'IA générative innovants pour des secteurs clés tels que la production et les sciences de la vie.

AGENDA

World summit AI
11-12 octobre 2023
Taets park, Amsterdam, Pays-Bas

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

Big Data & AI Toronto
18-19 octobre 2023
Metro Toronto convention Center, Toronto, Canada

NetApp Insight
23-25 octobre 2023
MGM Grand, Las Vegas, USA

European Blockchain Convention
24-26 octobre 2023
Fira Barcelona, Barcelone, Espagne

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

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

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

Votre réussite,
Notre engagement.

SQORUS
People and Solutions that matter

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

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

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

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

www.sqorus.com

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



Les nouveaux habits de l'ERP

Trouvant son origine dans les années 60 du siècle dernier, le terme ERP qui intègre le mot Entreprise prend son envol dans les années 90 par sa création par le cabinet Gartner, en étendant les fonctions purement opérationnelles et de gestion des stocks à d'autres fonctions du back-office. Depuis, la notion a encore largement évolué. Ce type de logiciel s'enrichit de plus des nouvelles tendances technologiques comme la mobilité ou l'intelligence artificielle. De plus ces outils se spécialisent de plus en plus par des orientations verticales davantage poussées.

Dossier réalisé par Bertrand Garé

SOMMAIRE

- Une notion étendue
- Des tendances technologiques claires
- Verticalisation et spécialisation
- Des exemples actuels de mise en œuvre

Une **notion étendue**

Apparu sous cette appellation dans les années 90, le concept d'ERP a beaucoup évolué pour aujourd'hui quasiment disparaître au profit du concept d'application d'entreprise, ce qui est bien loin de ce que l'ERP était à ses débuts.

Le concept est apparu dans les années 1960 avec le MRP (Mangement Resource Planning). Un consultant américain avait mis en avant ce concept afin de répondre aux besoins de Toyota pour gérer les ressources sur ses sites de production, de sorte que les pièces soient présentes au bon moment sur la ligne de production. 30 ans plus tard, le cabinet Gartner a remplacé le M par un E en créant le vocable Entreprise Resource Planning (ERP). Il élargissait le concept premier aux autres éléments d'importance pour la production comme la chaîne d'approvisionnement ou la finance. L'idée était de conserver dans une base de données unique toutes les données concernant l'activité de l'entreprise afin de proposer une vérité unique pour les lignes de métiers dans les entreprises. À cette époque les logiciels de gestion de la production était au plus haut comme Tolas, Mapics, Baan, QAD...

L'ERP étendu

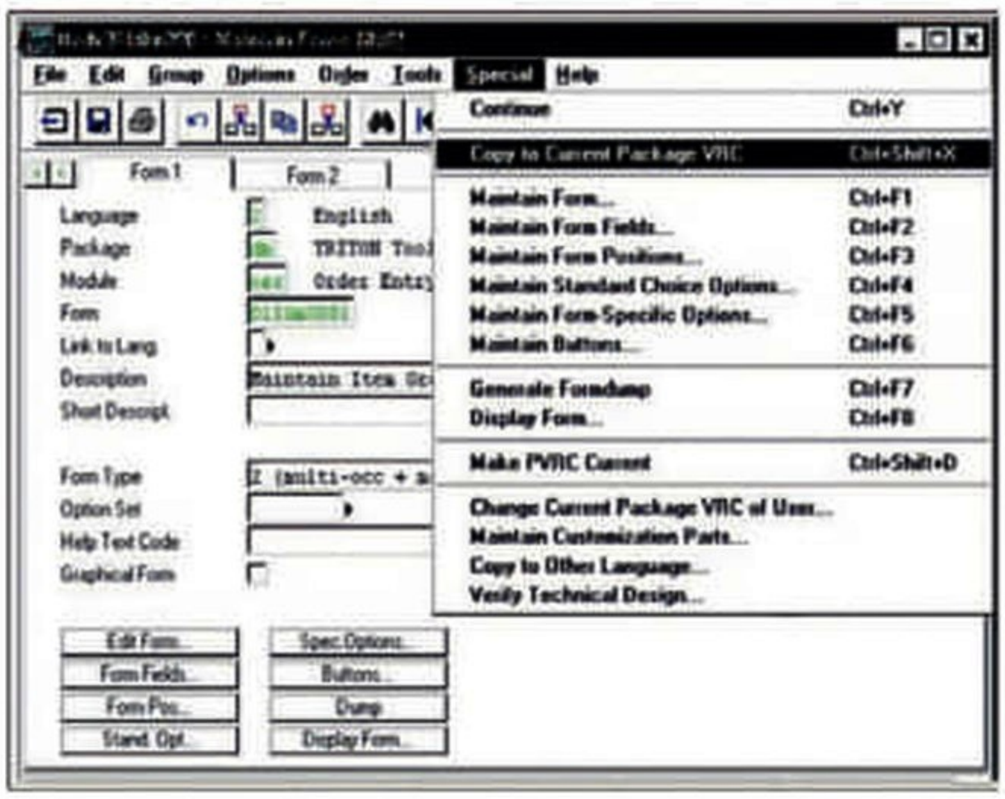
Il est vite apparu que cette approche intéressante pouvait s'étendre à d'autres lignes de métiers dans l'entreprise comme les ventes, les achats ou encore les ressources humaines. L'intégration de ces fonctionnalités dans l'ERP avait pour but de renforcer la synergie autour de l'information dans l'entreprise et donc de pouvoir facilement partager celle-ci, où que vous soyez dans l'entreprise sans avoir, comme à l'époque, des intégrations point à point entre les applications tierces et l'ERP. De plus, les entreprises changeaient peu à peu de modèles d'affaires et se dirigeaient de plus en plus vers la vente de services, sans forcément rester sur un modèle de production et de vente de produits.

Ces intégrations étaient vues comme un plat de spaghetti difficile à maintenir et qui créait trop de rigidité lorsque survenaient des mises à jour ou des changements de version d'un bout ou l'autre de la chaîne d'intégration. De nouvelles idées étaient apparues comme les services Web concurremment à la montée en puissance d'Internet dans les entreprises.

Cloud et SaaS

Après des essais en ASP (Application Service Provider) où l'ERP proposait une instance en ligne pour chaque client, les éditeurs se sont ralliés au nouveau concept d'une plateforme unique multitenant que revendiquaient les évolutions et les acteurs de ce qui allait devenir le Cloud. Un exemple de cette évolution est le logiciel Business ByDesign de SAP qui a commencé en ASP et a évolué vers une plate-forme Cloud après que SAP ait abandonné la volonté d'héberger la solution dans ses propres datacenters.





L'interface de l'ERP Baan à l'époque.

Devenu la colonne vertébrale de l'activité de l'entreprise, la migration des ERP vers le Cloud est donc un axe primordial de leur transformation numérique. Le marché des ERP dans le Cloud est estimé pour l'année dernière, à peu de choses près, à 60 Mds$ et, selon certains analystes de marché, la croissance serait de 71% pour 2023. SAP compte réaliser un peu plus de 14 Mds$ dans le Cloud cette année, soit environ un cinquième du chiffre d'affaires de l'éditeur allemand. Il est à noter que cette proportion est en augmentation constante et qu'elle est constatée chez tous les acteurs du secteur. En dehors des acteurs nativement dans le Cloud, cette proportion est à peu près la même chez les éditeurs historiques du secteur.

Actuellement, tous les acteurs du marché proposent une possibilité de leur ERP dans le Cloud. Certains privilégient même cette possibilité comparativement à leur autre offre sur site pour inciter les entreprises à migrer ou directement aller sur cet environnement.

Cette tendance accompagne aussi la tendance de long terme de travail déporté avec le télétravail mais aussi sur le travail en mobilité ou à distance. En ce sens, l'ERP suit l'organisation des entreprises clientes et n'impose plus comme auparavant une organisation type qui faisait de l'ERP un logiciel très structurant pour les entreprises.

Comme le remarque Marc Genevois d'IFS, *« nous laissons le choix au client de l'installer chez lui ou dans le Cloud ou nous pouvons même le gérer pour lui »*. Cette hybridation entre des modules sur site car considérés comme critiques et certains dans le Cloud est une tendance importante dans les entreprises.

Autre cas plutôt vu dans les grandes entreprises, le multicloud avec l'utilisation de différents ERP dans le Cloud suivant les spécialisations de ces logiciels ou l'excellence sur certaines fonctions. Ainsi Workday complète souvent un autre ERP tout en conservant les fonctions finance ou RH.

Les avantages mis en avant

L'ERP dans le Cloud présente plusieurs avantages en termes de flexibilité et d'agilité. Il évite de plus que les entreprises aient à prévoir une infrastructure pour les périodes de pics d'activité en permettant de lisser l'usage du logiciel. En outre, la configuration l'ERP en Cloud évite la maintenance ou l'écriture de spécifiques dans l'ERP qui bloquaient ou retardaient souvent les évolutions autour de ce type de logiciel. Il amène ainsi une rationalisation de l'usage autour du logiciel en évitant les évolutions de confort pour se concentrer sur les évolutions importantes pour le modèle d'affaires de l'entreprise.

Financièrement les entreprises prisent véritablement la possibilité d'utiliser les logiciels sous forme d'abonnement et ainsi ne payer que ce qu'elles consomment réellement sans avoir à conserver des licences sur étagère pour faire face à des imprévus.

La désintégration de l'intégré

Leur décomposition est initiée depuis plusieurs années avec la montée en charge des services web puis ensuite des changements d'architectures avec les containers et les micro services. Les logiciels intégrés, on les nomme PGI ou Progiciels de Gestion Intégrée en français, se sont peu à peu décomposés avec une infrastructure dans le cloud et la possibilité de poser sur celle-ci des applications pour les différents lignes de métiers de l'entreprise. Les éditeurs ont une couverture plus ou moins large mais tous ont au moins les fonctions principales comme la finance, les ressources humaines, la relation client... Certains éditeurs jouent le jeu des interfaces de programmation et proposent de construire leur ERP par une extension de leur plateforme par des API vers des éditeurs partenaires qui offrent les fonctions que l'ERP ne propose pas. Parmi ces nouveaux outils, on peut citer Workday qui a gagné sa place au soleil depuis plusieurs années ou Dynamics de Microsoft qui repose de plus en plus sur l'infrastructure d'Azure et qui profite de l'intégration verticale avec Office 365 et Teams.

L'open source est présent

Plusieurs éditeurs s'appuient sur les éléments issus de l'open source pour proposer des ERP alternatifs aux grands acteurs historiques du marché. ERPNext, Dolibarr, ERP5 ou Axelor ont trouvé leur place sur le marché. A noter que le dernier cité prône aussi le low code pour permettre aux utilisateurs de prendre la main sur la solution.

La notion d'ERP a donc largement évoluée depuis son apparition. Elle s'est adaptée aux changements technologiques mais aussi aux évolutions des modèles d'affaires et de l'organisation des entreprises. L'ERP n'est donc pas figé et son histoire n'est pas encore terminée... loin de là ! □

Des **tendances technologiques** claires

Les ERP connaissent des évolutions technologiques assez claires qui veulent mettre en avant la simplicité, l'automatisation et l'ubiquité de l'usage.

Nous l'avons déjà évoqué dans l'article précédent, le virage vers le modèle SaaS des ERP est la priorité à la fois des entreprises et des clients. La solution, comme nous l'avons vu, présente beaucoup d'avantages. Les entreprises y voient aussi une ouverture plus large, un usage plus dynamique des solutions et une plus grande facilité des mises à jour ou montées de version qui étaient parfois de véritables projets.

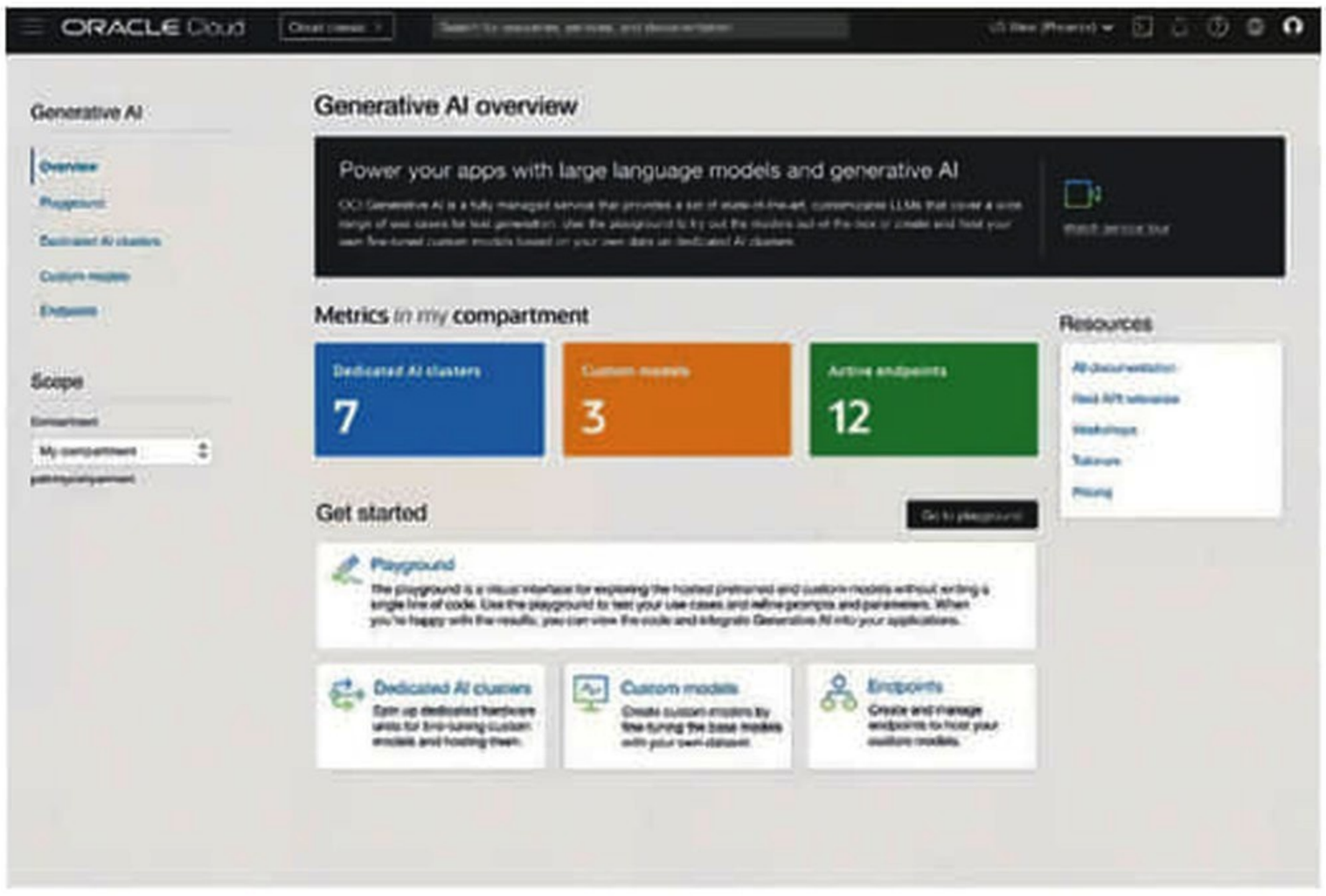
Le cloud hybride s'impose durablement du fait du temps que prend la migration des outils sur site vers le cloud, des différents choix des entreprises désormais présentes sur plusieurs clouds ou du placement sur différents clouds de workloads précis. De plus, le mode SaaS s'adapte aux nouveaux usages de travail mis en place depuis la fin de la pandémie de la Covid.

Des fonctions en mobilité

Dans le contexte de travail à distance, les ERP se sont depuis plusieurs années adaptés à un contexte de mobilité. Cette tendance perdure aujourd'hui et devrait même s'accentuer. Le travail est principalement concentré sur l'interface pour favoriser l'accessibilité. Celle-ci se veut donc plus simple pour permettre aux utilisateurs de trouver soit la bonne fonction soit la bonne information simplement. Les informations proposées sont évidemment plus réduites que celles dans l'ERP sur site ou dans le Cloud mais apporte celles nécessaires pour un usage distant en mobilité. SAP ou encore Sage ont revu d'ailleurs leur interface avec des outils « responsives » pour s'adapter aux différentes tailles d'écrans des mobiles des utilisateurs et aux différents OS déployés. D'autres comme Sylob sont allés un peu plus loin avec directement le développement d'applications correspondant aux différents besoins des utilisateurs. Contrairement aux solutions mobiles disponibles sur le marché, les applications Sylob ne sont pas limitées en termes d'informations disponibles sur la version mobile et les clients peuvent récupérer l'ensemble des champs de l'ERP, y compris leurs champs spécifiques, ce qui en fait un outil très puissant.

Plus d'intégrations

Pendant longtemps, la personnalisation des ERP a été un problème pour les entreprises, ce qui les obligeait le plus possible à rester au plus près du standard de l'ERP choisi. La maintenance et l'évolution des spécifiques développés autour de l'ERP devenaient un véritable frein pour les évolutions du logiciel et alourdissaient le plus souvent ses montées de version ou ses mises à jour. Les architectures en plateforme et les intégrations plus légères que les solutions point à point d'antan autorisent aujourd'hui des intégrations plus simples par des interfaces de programmation largement documentées. Ces interfaces jouent plusieurs rôles. Tout d'abord, elles autorisent des extensions et des personnalisations non plus par des développement spécifiques mais par des outils tiers apportant une spécialisation sur la fonctionnalité recherchée.



Une vue d'un rapport généré par l'intelligence artificielle générative dans Oracle Cloud.

Les ERP ne font pas tout et il est souvent besoin de les étendre pour répondre à différents besoins métiers. Par le biais des APIs, les ERP répondent au plus juste aux besoins des utilisateurs. Cette possibilité a fait entrer les éditeurs dans le monde de l'API Economy, où ils génèrent un flux de revenus à partir des licences des produits tiers qui sont présents sur leurs boutiques applicatives. Pour certains éditeurs, ces revenus peuvent représenter plus de la moitié de leur chiffre d'affaires annuel du fait d'un écosystème très large.

Le low code/no code

Le low code/no code est aussi un élément important pour les ERP en permettant à des personnes avec pas ou peu de culture informatique de développer par eux-mêmes des applications métiers qui affinent les plateformes pour arriver à des usages quasiment à la demande. Cela demande cependant un certain encadrement pour ne pas dévoyer les processus dans les entreprises, mais allège largement le recours à l'informatique pour des petits logiciels automatisant une tâche précise ou pour simplifier des appels à des bases de données. Des plateformes permettent cependant des exploitations plus poussées comme Axelor qui propose une plateforme ERP open source et low code. Elle permet de développer des fonctions complexes avec un minimum de code.



Un écran de Sylob 9.

Incontournable IA

2023 sera l'année de la démocratisation de l'intelligence artificielle. Le domaine des ERP n'y échappe pas avec l'intégration de fonctions d'intelligence artificielle prédictive ou générative dans la plupart des produits du marché. SAP vient d'annoncer un robot du nom de Joule, un copilote d'IA générative en langage naturel reposant sur l'utilisation des données de l'ensemble de la gamme de solutions SAP. Pour sa part, Oracle a annoncé lors de sa conférence annuelle Oracle World la généralisation de l'utilisation de l'intelligence artificielle dans sa gamme de produits. Il en est de même pour la plupart des éditeurs qui ajoutent des modèles LLM open source ou s'appuyant sur Open AI.

La tendance est cependant de développer des modèles plus sobres en paramètres entraînés sur les données interne de l'entreprise avant de les enrichir avec des flux de données externes. Ces outils visent à assister le salarié dans ses tâches en le recentrant sur les *« tâches à valeur ajoutée »*. L'IA a ainsi un rôle d'automatisation sur des actions récurrentes ou manuelles rébarbatives, voire sans intérêt économique pour l'entreprise ou de proposer des actions à celui-ci en lui fournissant un contexte pour qu'il prenne la meilleure des décision possibles. A noter que ce type de solutions a toujours des défauts, biais ou hallucinations, et que l'humain reste au cœur du processus avant de prendre la décision.

Cela permet de plus de prendre en compte le besoin d'informations exactes en temps réel en particulier dans le monde industriel avec des volumes de données importants issus des capteurs des usines ou appareils. □

L'USF HAUSSE LE TON

Si les entreprises et les éditeurs s'accordent pour mettre en avant le Cloud, tout ne se passe tout le temps dans le meilleur des mondes. Devant la hausse annoncée par SAP du coût de la maintenance de leurs licences des produits on-premise pour 2024, l'association des utilisateurs francophones a donné de la voix. Beaucoup de ces utilisateurs sont dans un contexte hybride, avec donc des éléments de SAP encore sur site. Cette augmentation est pour eux une mauvaise nouvelle. Elle suit de plus une autre annonce indiquant que désormais toutes les innovations des produits SAP seraient réalisées uniquement dans les versions cloud. Les clients utilisant des versions on-premise ont ainsi le désagréable sentiment de subir une double peine : plus aucune évolution porteuse de valeur pour leurs utilisateurs assortie d'une augmentation des coûts de la maintenance. L'USF a en outre l'impression que SAP pratique une politique de moins de produits pour plus de licences et de maintenance. L'USF rappelle enfin que la plupart des clients historiques de SAP utilisent toujours des versions on-premise et n'ont à ce jour pas prévu de passer à des versions cloud, ce pour différentes raisons : pas suffisamment de valeur identifiée, pas dans les priorités stratégiques de l'entreprise ou encore pas de moyens budgétaires en raison d'une conjoncture économique difficile. La prochaine tenue de la convention annuelle de l'organisation, qui se tient les 11 et 12 octobre 2023 à Nantes, devrait rapidement éclairer ce débat.

Verticalisation et spécialisation

La verticalisation et la spécialisation des ERP existent depuis plusieurs années, cependant la tendance s'affirme et des éditeurs font même le choix de ne se concentrer que sur certains secteurs d'activité pour mieux répondre aux besoins de leurs clients.



La couverture fonctionnelle chez Infor.

Jusqu'à présent, les éditeurs d'ERP comptaient sur leurs partenaires intégrateurs ou cabinets de conseil pour accompagner les entreprises lorsqu'il était nécessaire d'adapter le logiciel à des fonctions ou des activités spécifiques de l'entreprise. Il y a environ une décennie, le patron d'Intentia, racheté tout d'abord par Lawson Software,l ui-même tombé entre les mains d'Infor, expliquait : *« on ne fait pas des ERP pour les chaseurs d'ours »*. Il n'en existe toujours pas mais des éditeurs jouent la carte de la spécialisation métier pour se différencier, à l'instar d'IFS. Marc Genevois, Regional President Southern & Western Europe and LatAm chez IFS, precise : *« notre stratégie est de se concentrer sur six secteurs d'activité et de devenir le partenaire incontournable sur ces secteurs. Le marché évolue positivement avec peu de demandes particulières à l'exception du secteur de la défense »*. Infor suit à peu près la même stratégie avec ses différents ERP. Ainsi la gamme LN se concentre sur les domaines de la production discrète, tandis que M3 est plutôt dédié au secteur public.



Marc Genevois,
Regional President Southern & Western Europe and LatAm chez IFS.

« Le marché évolue positivement avec peu de demandes particulières à l'exception du secteur de la défense. »

Les solutions sont souvent des logiciels préconfigurés qui vont plus loin que de simples templates car des secteurs comme le « food & beverage » demandent parfois des réglages plus poussés. Philippe Michel, Sirector Solution Consulting chez Infor, souligne : *« on peut ainsi se concentrer rapidement sur le prototypage avec des contenus et des paramètres adaptables et copiables, ce qui permet de créer des variantes à partir du préconfiguré et si, in fine, la configuration finale ne convient pas, il est possible d'étendre la solution par une gamme d'outils ou des développements, des exit points dans le glossaire d'Infor. Il est possible d'aller très loin sur des fonctions très avancées comme les règles de rangement des palettes »*.

L'apport du Low Code

Le low code permet aussi ce type de spécialisation ou de personnalisation des logiciels par les experts métiers dans des délais très courts. Thyssenkrupp Materials France a ainsi mis en œuvre l'ERP d'Axelor, un ERP low code et open source qui permet d'adapter l'ERP aux besoins spécifiques de l'entreprise dans des délais très courts. Divalto, un éditeur français, a récemment publié des applications s'appuyant sur sa solution Divalto One qui remplace du développement par de la formule. Des utilisateurs clés, non développeurs, pourront adapter fortement les solutions aux enjeux de leur entreprise avec un langage proche d'Excel. L'utilisateur peut ainsi créer son expérience et personnalise ses outils selon ses propres envies, goûts et besoins. La principale raison de cet engouement pour ce type d'outil est assez simple : un existant inadapté aux nouvelles volontés de transformation des entreprises. *« Les entreprises sont en forte demande de solutions métiers rapides à mettre en œuvre et simples d'utilisation. Si, dans le passé, il était dans la norme de voir des projets d'intégration ERP nécessiter plusieurs mois de développement, ce n'est plus le cas »* indique Jérémy Grégoire, Chief Product and R&D Officer chez Divalto. □

Des **exemples** de mises en œuvre

Les ERP sont toujours la colonne vertébrale de l'activité des entreprises mais leur mise en œuvre évolue à l'aune des besoins des clients. Retour sur différents exemple récents.

Lors d'Oracle World, Michelin a accepté de parler de sa migration d'Entreprise Business Suite vers le Cloud. Si le projet peut se résumer à un « shift and lift » de la solution avant d'explorer plus avant une migration sur Oracle Cloud Infrastructure, le projet est assez emblématique de la demande de transformation par le cloud. Le logiciel EBS, qui soutient la majeure partie de l'activité de Michelin en couvrant l'ensemble des sociétés du groupe et leurs implantations dans les différents pays, avait plus de 10 ans et fonctionnait sur des serveurs Exadata en fin de vie. Michelin s'est donc interrogé sur un projet de migration technique avec la volonté d'obtenir, en plus des gains de performance, plus de flexibilité et de mise à l'échelle. Il a été alors décidé de migrer vers le Cloud sur le périmètre existant. L'infrastructure d'Oracle semblait la plus à même de réaliser cette migration avec succès. Il s'est posé la question d'aller sur Microsoft Azure mais, finalement, l'équipementier s'est rangé à son idée avec Oracle. Accompagné par Orange Consulting, le projet s'est réalisé rapidement et dans les temps : il est passé en production au quatrième trimestre 2022. Au total, 15 environnements dont 3 de production sont effectifs, sauf un dernier environnement de production qui contient des téraoctets de données. 50 000 utilisateurs sont sur la solution qui sous tend une part substantielle des revenus du groupe. La solution est placée sur des centres de données à Francfort et dans la région parisienne. Il n'y a eu aucun impact lors du démarrage de la solution en quasi big bang sur un week-end et, sur les procédures de clôture pour les entreprises du groupe présentes aux USA, il a été constaté une baisse importante du temps de traitement. Si le côté Finops est encore à affiner et à maîtriser, les coûts de fonctionnement de la solution sont attendus en baisse de 20 à 30 %. Ces chiffres restent cependant à confirmer.

No Code et intégration

Basée à Toulouse avec 95 employés, MECANO ID développe des sous-systèmes mécaniques et thermiques pour le secteur spatial. En 2021, à la suite d'une forte croissance, l'entreprise choisit l'ERP Simax pour piloter son activité, un ERP no code qu'elle intégrera elle-même à sa structure. À l'origine, MECANO ID se reposait sur un intranet et cumulait les tableurs Excel pour gérer ses différents projets et l'ensemble de ses processus métiers. En 2018, l'entreprise double la taille de ses locaux et sa capacité de production. Dans ce contexte, il devenait difficile de superviser l'ensemble de son activité sans faire évoluer ses pratiques. La mise en place d'un ERP s'est imposée, pour répondre aux objectifs d'aide à la production, mais également d'aide à la gestion des temps, à la comptabilité, à l'organisation des équipes et à l'avancement des projets. Deux solutions sont retenues et, finalement, Simax est choisi, puisque cette solution no code peut être intégrée en interne sans exiger de nouvelles compétences. L'ERP est totalement sur-mesure, modifiable grâce aux ressources internes. La solution correspondait donc parfaitement aux besoins très spécifiques de leur activité de niche. C'est pourquoi cette dernière a été privilégiée. L'équipe de MECANO ID a bénéficié d'une semaine de formation, avant que les trois membres chargés d'intégrer la solution au SI démarrent leur mission en toute autonomie. Ensuite, quelques rendez-vous de projet ponctuels ont suffi à paramétrer l'ERP selon les besoins de l'entreprise. Le logiciel couvre 80 % des besoins de gestion de l'entreprise. Il est utilisé au quotidien par une centaine d'utilisateurs. □



Une vue dans les locaux de MECANO-ID.

#SIDO2023

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

PARIS 3e

SIDO

IoT – AI – DIGITAL INFRA – CYBERSECURITY

6 & 7 Décembre 2023

Palais des Congrès, Paris

120 Exposants
30 Conférences
120 Speakers

Créer mon badge gratuit

CODE : P-INFSP23

www.sido-paris.com

MÊMES DATES - MÊME LIEU

OPEN SOURCE EXPERIENCE

Découvrez Open Source Experience

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

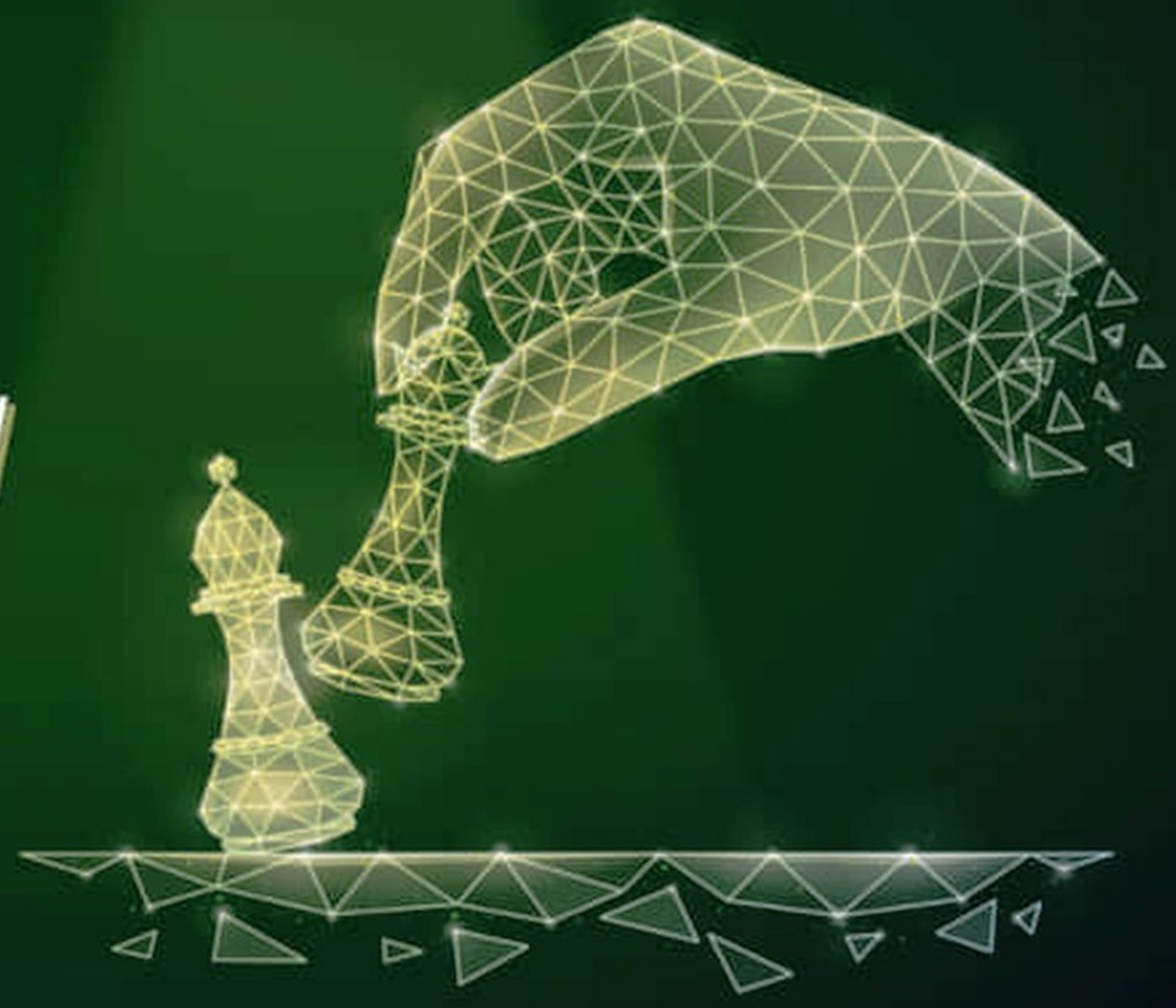
Hall Maillot - Niveau 1

Ce badge vous donne accès aux deux événements

UN ÉVÉNEMENT

infoprodigital TRADE SHOWS

L'anglais, le nouveau SQL ?



par Bertrand Garé

Ah ! Il n'y a pas encore si longtemps que celui qui savait réaliser de belles requêtes SQL s'auréolait d'une aura de geek ou d'expert en informatique que lui enviaient tous ceux qui en fait ne s'étaient jamais intéressés à la question. Il est vrai que de faire un select/from était du meilleur goût pour épater les petits camarades du bureau. Tout cela est en train de changer largement avec l'avènement des modèles LLM et la possibilité d'utiliser le langage naturel pour effectuer des requêtes. C'est donc avec promptitude que les utilisateurs se sont mis à jour pour manipuler des données dans des bases par le simple pouvoir du verbe. Pour l'instant, ils ne peuvent le faire que par un texte dans leur langue maternelle. Le titre de cette chronique est un peu trompeur, car il est ainsi possible de le faire dans n'importe quelle langue aujourd'hui... ou presque. Il est déjà possible de le faire dans la langue de Molière et heureusement, car le niveau de nos concitoyens en anglais est parfois limité.

Un peu plus d'un quart des Français déclarent comprendre et parler l'anglais (28 %), soit une progression de 10 points en 15 ans. La dynamique de la langue anglaise au sein de la société française s'explique principalement par un effet générationnel. 48 % des 18-24 ans déclarent comprendre et parler anglais, dont 14 % couramment, contre seulement 15 % des personnes âgées de 65 ans et plus. Comme la plupart des LLM sont développés par des entreprises américaines, cela promet de beaux jours devant nous. Heureusement, quelques fleurons de notre start-up nation se collent au problème. Mistral AI a donc annoncé un modeste modèle à 7 milliards de paramètres. Il semblerait qu'il fasse mieux que d'autres modèles open source comme LLAMA 2 ou 3 avec des besoins en traitements bien moindres. Super, mais le modèle parle surtout... anglais ! Bon, l'entreprise développe de plus gros modèles qui seront polyglottes. Elle devra aussi se confronter avec la concurrence de nouveaux acteurs comme Poolside, un acteur américain qui vient de s'installer en France et qui a le même investisseur, Xavier Niel. De toute manière, les premiers modèles de Mistral AI seront disponibles au début de l'année prochaine. Encore le temps de voir venir.

De toutes façons, les modèles LLM se distinguent par leur traduction, comparativement aux anciens outils de traduction assistée par ordinateur. Il suffira donc de faire traduire par l'IA la requête en une langue autre que l'anglais, puis de faire la requête depuis cette traduction ! On n'arrête pas le progrès !

SQL, un sous langage

En fait, SQL ne va perdre sa place mais se trouver comme une passerelle entre les modèles d'intelligence artificielle générative et les bases de données pour effectuer le travail que ce langage sait si bien faire : manipuler des données dans une base relationnelle. Certains outils comme Spark découvrent même depuis peu de temps la possibilité d'utiliser l'anglais et non du code pour réaliser des requêtes.

Un changement profond

Cela va entraîner un véritable changement dans le rapport que les gens ont avec les données. Si, aujourd'hui, c'est par le texte ou l'image, demain cela sera par la parole et par une simple demande vocale vers le prompt qui déclenchera la requête.

« Historiquement, les tâches manuelles et routinières ont été celles automatisables, principalement parce qu'elles obéissent à des règles claires et explicites. L'IA permet d'élargir ce champ d'application par le développement de machines qui sont de plus en plus performantes pour accomplir des tâches

manuelles et routinières qui demandent de la dextérité fine et de la précision. L'IA permet aussi, entre autres grâce à des développements au niveau de la perception sensorielle, des senseurs et de la dextérité manuelle, d'automatiser certaines tâches manuelles non routinières. L'IA permet également d'automatiser des tâches cognitives. Ici encore, les tâches routinières sont celles qui sont les plus susceptibles d'être automatisées. À titre d'exemple, l'IA permet entre autres d'automatiser les tâches cognitives et routinières relatives au service à la clientèle, aux transactions financières, à la collecte de données pour l'attribution de prêts hypothécaires, etc. Même des tâches cognitives non routinières peuvent être automatisées avec l'IA. Ici, nous parlons surtout de tâches qui nécessitent l'analyse d'importants jeux de données dans le but de découvrir des relations ou des tendances. Par exemple, l'IA permet d'automatiser les tâches liées à la détection de fraude, ce qui nécessite d'être à la fois capable de découvrir des relations et de prendre des décisions sur la base de ces relations » indique un rapport de la Commission de l'éthique en sciences et en technologie de Québec.


La puce Neuralink d'Elon Musk

Ce changement profond ne va pas juste avoir des conséquences sur notre manière de travailler, mais aussi sur les instruments avec lesquels nous travaillons. Il y aura un impact sur l'infrastructure pour faire tourner tous ces magnifiques modèles révolutionnaires de notre quotidien.

Nous ne reviendrons pas sur les conséquences sociales et sociétales de l'intelligence artificielle générative. Les colonnes des médias et autres essais sont pleins de possibilités, défauts et avantages d'une technologie qui, rappelons-le, n'en est qu'à ses débuts et qu'il est encore difficile de voir jusqu'où elle peut aller. Au minimum, celle-ci va avoir pour conséquence de créer un super-travailleur, un salarié augmenté qui va s'appuyer sur l'outil pour trouver de nouvelles idées, réaliser plus de tâches durant son temps de travail. Justement, et je vous conseille fortement de lire l'article dans ce numéro sur les bio-hackers, un autre moyen de créer un homme augmenté, est l'implant de puces et de capteurs pour devenir « plus qu'humains ». Cette vision est celle d'Elon Musk avec Neuralink qui vient d'obtenir la possibilité d'essayer ses implants pour aider les individus paralysés à communiquer grâce à des implants qui suivent et activent certaines zones du cerveau en le stimulant électriquement.

Alors, entre apprendre à parler l'anglais ou se faire poser des implants dans le cerveau, il va bien falloir se faire au monde de demain et en tirer le meilleur parti pour que tout cela ne devienne pas la vision des pires romans de science-fiction. □



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

Poste de travail

Un portable semi-durci performant

Getac a présenté un nouveau portable semi-durci pour des environnements exigeants. Le matériel propose de nombreuses nouveautés mais aussi des performances de haut niveau.



Le S410 G5 de Getac est le premier appareil de ce type à supporter les processeurs Intel de 13e génération avec des processeurs I5 et I7 et cela en standard. Le constructeur vise des publics exigeants comme ceux de la défense, de l'industrie, de la sécurité publique et des collectivités, qui n'ont pas besoin d'un appareil entièrement durci, mais qui souhaitent néanmoins travailler en toute tranquillité d'esprit dans des environnements exigeants ou difficiles. De plus, la machine s'appuie sur les processeurs graphiques Intel Iris Xe. Les performances sont assez remarquables et la visibilité est optimisée à la fois par les capacités de la puce graphique et du réglage automatique de la luminosité. L'écran de 14 pouces, doté de la technologie Getac de lecture en plein soleil, garantit une excellente visibilité (1 000 nits) dans les environnements internes et externes, tandis que les modes multitouches prennent en charge divers cas d'utilisation, ce qui signifie que les tâches peuvent être accomplies rapidement et efficacement. Une puce GPS dédiée en option offre une précision de localisation considérablement améliorée par rapport aux générations précédentes.

En matière de connectivité, le S410 de nouvelle génération est équipé en standard du Wi-Fi 6E et du Bluetooth 5.3, et en option de la 4G LTE et/ou de la 5G Sub-6 avec GPS intégré, ce qui permet aux utilisateurs de rester connectés même dans les endroits les plus reculés. Le poids de l'appareil est de 2,38 Kg, ce qui n'est pas excessif pour ce type de matériel semi-durci.

Une grande autonomie

L'autonomie est importante, jusqu'à 22 heures avec la possibilité d'utiliser 3 batteries remplaçables à chaud, ainsi que de nombreuses options dans la baie média, avec le contrôleur graphique NVIDIA GeForce GTX 1650, un lecteur de codes-barres 1D/2D, un lecteur de DVD ou Blu-ray, jusqu'à un second périphérique de stockage SSD ou une batterie supplémentaire. Une large gamme d'accessoires compatibles et des options de transport et de fixations sécurisées améliorent encore les fonctionnalités, pour une meilleure productivité sur le terrain.



Des fonctions de sécurité de haut niveau

Des fonctions de sécurité améliorées permettent également de protéger les données sensibles des utilisateurs. Il s'agit notamment des technologies TPM2.0 et Intel VPro, du SSD PCIe NVMe remplaçable par l'utilisateur et des options d'authentification multifactorielle telles que la webcam Windows Hello, le lecteur RFID HF, le lecteur de cartes à puce et le lecteur d'empreintes digitales.

Plus écologique mais sans concessions

La nouvelle génération de S410 est l'appareil le plus écologique que Getac ait conçu à ce jour, avec plus de 24 % du châssis fabriqué à partir de matériaux recyclés post-consommation (PCR). Cette nouvelle approche de conception réduit à la fois les émissions de carbone et les déchets électroniques au cours du processus de fabrication, contribuant ainsi à promouvoir un avenir plus respectueux de l'environnement. Malgré ce changement dans la conception du châssis, aucun compromis n'a été fait sur la fiabilité. Tout comme son prédécesseur, le S410 de nouvelle génération est certifié MIL-STD-810H et IP53, et résiste aux vibrations et aux chutes jusqu'à 0,9 m, ce qui permet de le protéger contre les dommages accidentels dans les environnements de travail exigeants ou difficiles. Ce nouveau modèle sera disponible à la commande en décembre prochain. À noter que les options configurables sont mutuellement exclusives. Le prix en entrée sans option est de 1949 € HT, soit l'équivalent d'une belle configuration « *gamer* ».

ERRATUM

Lors de notre dernier numéro, nous avions fait un test sur une tablette Getac. Hélas, les lunettes de notre collaborateur ont besoin d'une légère révision et nous avons parlé de la tablette ZX 70 au lieu de la tablette ZX 10. Désolés, et toutes nos excuses à Getac. Notre collaborateur a été puni par une visite chez l'oculiste.

GETAC EXPLORE LE LIFI



Un scénario d'utilisation du LiFi avec la solution Trulifi de Signify.

Par ailleurs, le constructeur explore, en partenariat avec Signify, un spécialiste de l'éclairage, la possibilité d'intégrer la technologie LiFi dans ces appareils durcis. Pour rappel, la technologie LiFi utilise la lumière pour transmettre les données plutôt que par radiofréquence comme les technologies Wifi, LTE, 4G, 5G... Comparativement à ces dernières technologies, le LiFi apporte une latence faible, une confidentialité et une sécurité renforcée, ainsi qu'une qualité de connexion supérieure, notamment dans les environnements dépourvus de radiofréquences. L'intégration de la technologie LiFi de Signify se réalisait par l'ajout d'un dongle externe sur les appareils durcis de Getac. Désormais, cette technolgie est directement intégrée dans les appareils. De plus, Signify et Getac font partie de la Light Communication Alliance (LCA), une communauté de leaders industriels, de chercheurs et de précurseurs qui souhaitent développer la communication optique sans fil pour transformer la manière dont les entreprises et organisations se connectent et communiquent. Des cadres de Getac ont cependant précisé que l'entreprise explorait actuellement cette opportunité en testant le marché avec ces nouvelles offres.

Des différenciateurs notables

Si la machine en elle-même a de quoi être distinguée des logiciels, le système de garantie opéré par Getac représente un véritable différenciateur pour les utilisateurs. Il est ainsi possible, sous certaines conditions, de faire des réparations légères sans perdre la garantie, et en cas de problèmes plus graves, le remplacement ou la réparation du matériel ne prend que 5 jours au maximum. Il est aussi possible d'étendre la garantie de 3 à 5 ans.

Plusieurs options logicielles aident, de plus, les utilisateurs sur des utilisations métiers comme Virtual GPS, Driving Safety qui coupe l'écran embarqué dans un véhicule au-delà d'une certaine vitesse pour ne pas perturber le conducteur, ou encore Key Wedge, qui un outil de scan de code barre avec la caméra arrière d'un appareil mobile.

De nombreux outils aident les utilisateurs à déployer, configurer ou gérer la flotte des matériels Getac comme Getac Device Monitoring, un système en ligne qui permet de maintenir en condition opérationnelle les matériels pour assurer un temps d'utilisation maximale et de réduire les risques d'incidents. Le logiciel indique ainsi à l'utilisateur qu'il doit insérer une nouvelle batterie pour continuer son activité.

À l'analyse, le S410 G5 se révèle assez polyvalent et bénéficie d'améliorations heureuses comparativement à la génération précédente, il profite de nombreux autres avantages en termes de garantie ou de support, qui sont sur ce marché précis de réels différenciateurs. □

B.G

Le GSM Effacez totalement vos données !

Le GSM, une entreprise créée en 2012 par Lionel Uzzan pour reconditionner les appareils électroniques, vient de lancer une nouvelle solution innovante hardware qui permet d'effacer totalement les données sur les appareils collectés.

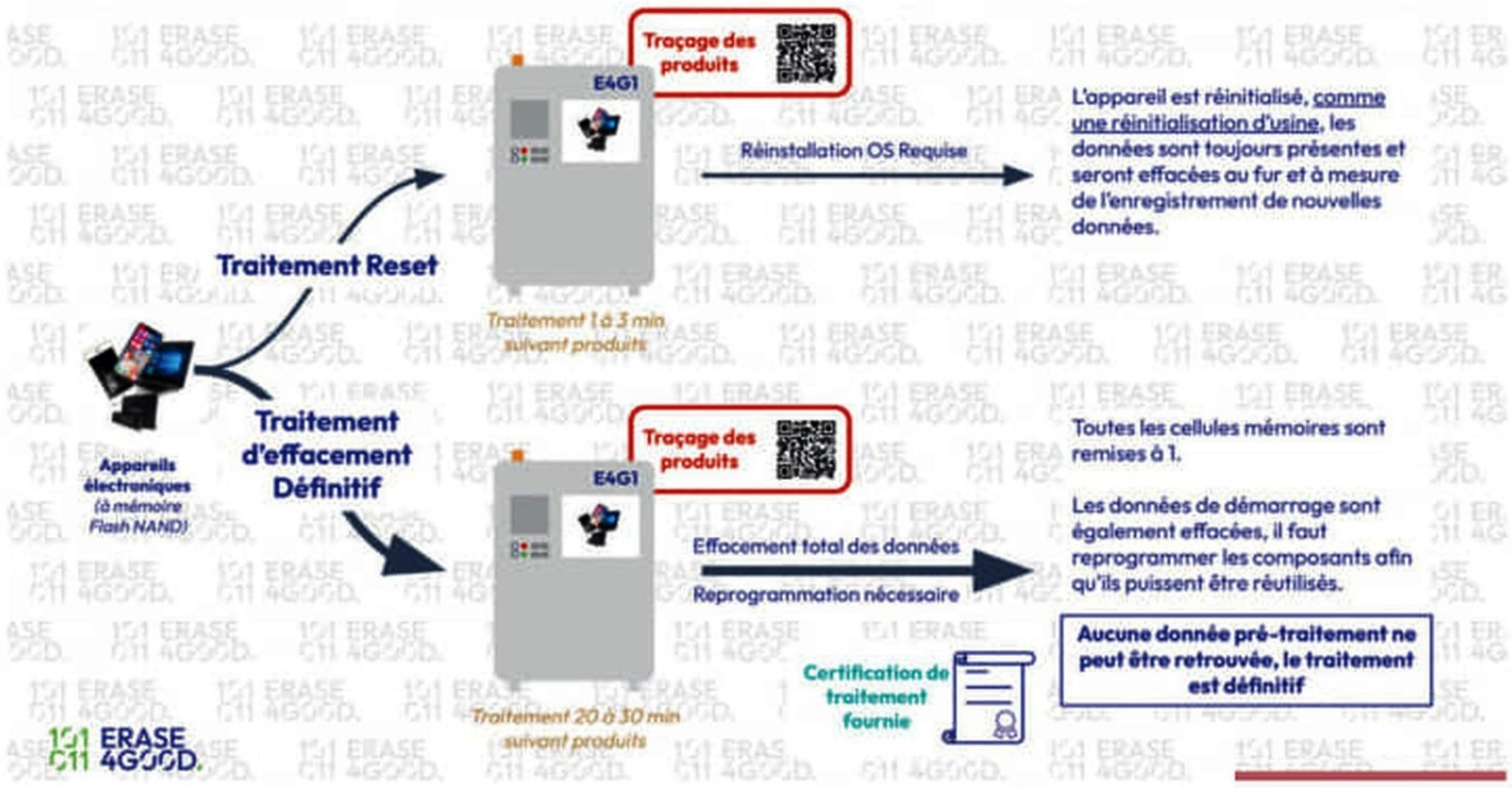
La société réalise l'ensemble des activités de reconditionnement dans son usine basée à Ivry-sur-Seine. Elle collecte environ 100 000 produits de tous types par an pour les reconditionner et les revendre sur des plateformes professionnelles ou grand public en France et en Europe. Dans son activité, la société collecte de nombreux équipements auprès de grandes entreprises ou d'opérateurs où sont encore présentes des données. Certains clients veulent s'assurer que les équipements n'embarquent plus de données de l'entreprise ou visent à reconditionner les équipements si cela est possible. Lionel Uzzan précise : *« nous récupérons des produits fonctionnels ou cassés sur lesquels la valeur résiduelle est faible et donc économiquement inintéressante, mais les donneurs d'ordre souhaitent avoir l'assurance que les données possiblement présentes soient totalement effacées ».*

Une nouvelle méthode hardware

Il existe déjà des solutions pour effacer les données, comme celles de réécrire sur les mémoires des disques durs jusqu'à la disparition des données d'origine. Une autre méthode consiste à réaliser une vaste décharge magnétique sur le support, ce qui efface les données. Hélas, cette possibilité ne fonctionne que sur les supports magnétiques mais pas sur les mémoires Flash NAND qui sont présentes dans les téléphones ou tablettes actuelles.

Pour la méthode d'Erase4Good de GSM, Lionel Uzzan est reparti sur les bancs de l'université pour suivre un master à Polytechnique afin de mettre à jour ses connaissances et pouvoir travailler avec différents laboratoires. À la suite de cela, il a conçu une machine qui utilise un traitement thermique qui va changer la configuration des mémoires. Les informations dans les mémoires sont réinitialisées pour ne plus présenter que des 1, ce qui est le signe d'une cellule vide comparativement à une cellule 0 où une information est présente. Plus précisément, un courant à faible voltage dans les trappes de charge transforme les données textes, images et autres en trappes de charges vides.

L'opération prend entre 20 et 25 minutes avec la version de la machine actuelle, soit environ 200 produits par jour. L'idée est d'industrialiser le processus avec une machine plus grande pour traiter des milliers d'appareils. Pour cela, le GSM va utiliser une machine auto-protégée dans un coffrage de plomb, peu consommatrice d'électricité et équipée de circuits fermés d'eau et d'huile refroidissante. Respectueuse de l'environnement, cette machine ne consomme qu'environ 6 kWh, et en plus des économies d'énergie réalisées, les appareils reconditionnés peuvent être tout simplement réemployés plutôt que broyés et recyclés. De plus, Lionel Uzzan souhaite rendre plus mobile sa technologie pour éviter l'envoi des produits, mais aller directement à la source pour effectuer les opérations. L'internationalisation du service est une autre priorité après un accueil assez enthousiaste de la technologie lors d'un récent salon aux USA. Ce développement se réalisera normalement par la création d'une filiale pour conserver la propriété intellectuelle. ☐ **B.G**



Homme augmenté

Len Noe : un biohacker au service de la lutte contre la cybercriminalité

Biohacker, hacker éthique, et chercheur en cybersécurité chez CyberArk, Len Noe s'est fait implanter pas moins de 6 puces dans le corps pour devenir « plus qu'un humain » et plus performant dans son métier. Ce personnage hors du commun nous explique comment les cybercriminels pourraient utiliser les implants et les technologies sans contact pour mener des cyberattaques.

Ce n'est pas (ou plus) de la science-fiction. Passionné de technologies, Len Noe s'est fait implanter six puces électroniques (NFC, RFID...) et des biocapteurs aimantés sous la peau pour repousser les limites de la recherche en cybersécurité. Grâce aux modifications de son organisme, il a augmenté ses capacités humaines et il est par exemple capable de pirater des objets du quotidien, ouvrir des zones d'accès restreintes sans les toucher, accéder à des appareils technologiques, *etc.* Le chercheur se présente comme un évangélisateur qui aide les entreprises à comprendre comment des biohackers pourraient utiliser leurs implants pour attaquer leur système d'information. **J.C**

« Je ne voulais pas juste étudier la cybersécurité, je voulais aussi la vivre. J'ai subi une série de bio-implantations sur plusieurs années pour devenir "plus qu'humain" et meilleur dans ce que je fais. »

Len Noe, biohacker et chercheur en cybersécurité chez CyberArk.

Pouvez-vous nous parler brièvement de votre parcours dans la cybersécurité ?

Mon intérêt et ma passion pour la technologie viennent de mon père. C'est un amateur de gadgets et un adepte précoce de la technologie qui m'a fait découvrir le Commodore 64 au début des années 80. Pour moi, la fascination s'est transformée en véritable obsession lorsque j'ai lu une newsletter qui décrivait les étapes pour développer un jeu pour PC simple appelé « Frogger ». J'ai commis une erreur de développement en suivant les instructions, mais cette erreur a paradoxalement empêché ma grenouille de mourir dans le jeu. C'est à ce moment-là que j'ai eu le déclic et que j'ai commencé à réfléchir de manière plus critique aux raisons de cette erreur et à la manière dont je pouvais manipuler les résultats. Depuis ces débuts, j'ai passé des dizaines d'années à essayer de m'améliorer encore et encore. J'adore trouver de nouveaux moyens créatifs d'exploiter les systèmes technologiques et de repérer les moindres brèches afin que les organisations puissent renforcer leurs protections et prévenir les attaques. J'ai présenté mes recherches sur les menaces dans plus de 20 pays.

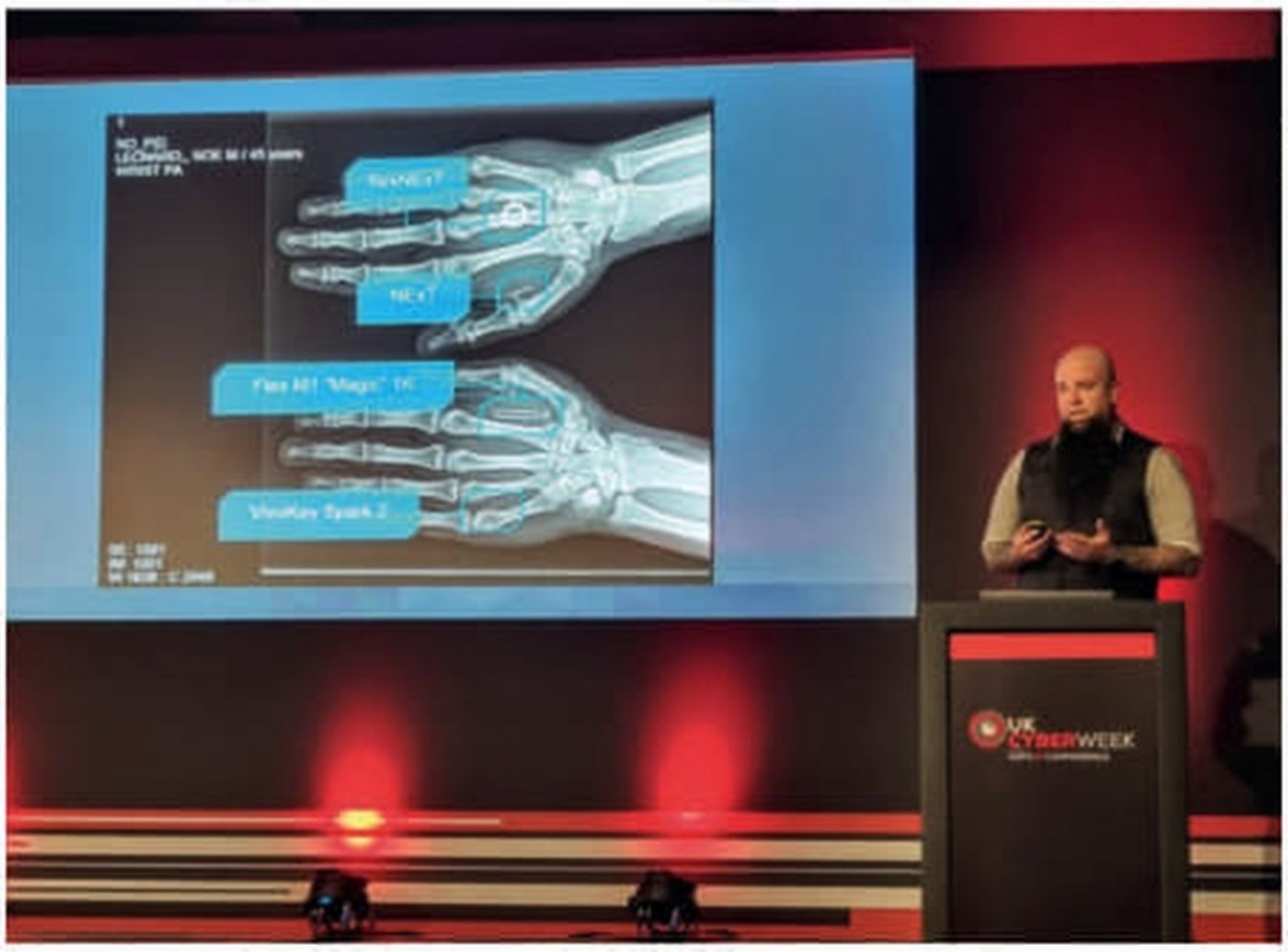


© Nick Bowman

Qu'est-ce qui vous a motivé à devenir un biohacker ?

Tout d'abord, il y a eu le piratage. Pendant un certain temps, j'ai été un hacker « black hat ». C'est ma famille qui m'a incité à devenir un hacker « white hat » lorsque mon premier petit-enfant est né. Cela a été un moment charnière qui a changé ma vie. C'était un changement d'état d'esprit plutôt

que quelque chose d'instantané. Pour moi, il a toujours été question de résoudre une énigme. C'est la raison pour laquelle j'ai commencé à hacker, et le biohacking est une nouvelle étape. Je ne voulais pas juste étudier la cybersécurité, je voulais aussi la vivre. J'ai subi une série de bio-implantations sur plusieurs années pour devenir « plus qu'humain » et meilleur dans ce que je fais.



© Nick Bowman

Est-ce que des implants sous-cutanés ont déjà été utilisés pour mener des cyberattaques ?
Pour être honnête, nous ne savons pas. En raison de la nature des implants utilisés dans le cadre d'une attaque — une redirection d'URL ou une autre attaque de même nature — il serait très difficile de déterminer si un implant sous-cutané a été utilisé comme déclencheur initial de la chaîne d'attaque.

Des « Red Teams » utilisent ces techniques dans le cadre de tests d'intrusion. Cela m'amène à penser que, oui, ces techniques ont été utilisées dans des attaques réelles. Malheureusement, en raison de la nature de la technologie, il est extrêmement difficile de le prouver. Il n'y a pas de piste à suivre pour ainsi dire.

Les implants sous-cutanés permettent notamment d'utiliser le NFC et la RFID. L'un des cas d'utilisation que je montre lorsque je m'adresse à des clients, ou lors d'événements, concerne l'accès physique. En exploitant une carte d'accès à un bâtiment, en l'inscrivant sur un implant et en compromettant ensuite des lieux physiques, il devient extrêmement facile de voir la relation univoque entre le cas d'utilisation et la technologie. L'implant NFC que je possède pourrait être utilisé contre n'importe quel type d'appareil mobile. Il peut être employé pour télécharger des chevaux de Troie « Reverse Shells », un type spécifique de logiciel malveillant utilisé par les attaquants pour obtenir un accès non autorisé au système informatique d'une victime. Les applications malveillantes pourraient également être redirigées vers des sites web corrompus. Les capacités des biohackers continueront d'évoluer au même rythme que les technologies.

Quelles sont selon vous les failles de l'authentification biométrique ? Comment les entreprises peuvent-elles se protéger ?
Toutes les authentifications biométriques actuellement utilisées ont été soit usurpées, soit contrefaites, soit contournées. Toute authentification biométrique utilisée comme facteur unique d'authentification n'apporte pas beaucoup de sécurité supplémentaire. Pour améliorer la situation, il faut considérer l'authentification biométrique comme un élément d'une véritable authentification multifactorielle (c'est-à-dire plus qu'un simple mot de passe et un mot de passe à usage unique). Lorsque nous commencerons à ajouter des éléments tels que les empreintes digitales des appareils, ou leur emplacement géographique, ou encore la question de savoir si cette demande est reçue pendant les heures normales d'ouverture, les entreprises auront une bien meilleure chance de comprendre le contexte d'une demande d'authentification. Par conséquent, elles seront également en bien meilleure position pour choisir le type d'authentification à appliquer.

Est-ce qu'il faut craindre le futur du biohacking et des bioimplants ?
Si l'on se réfère à l'époque où l'email a fait son apparition, il n'y avait pas d'antivirus pour le courrier électronique ni de détection des menaces pour les liens Internet. Nous avons évolué en même temps que les menaces. Tout comme pour l'IA, l'industrie et les organisations en général doivent accepter le fait que des gens comme moi sont là. De ce fait, nous devons commencer à envisager des contrôles pour répondre aux capacités augmentées. Ce n'est pas quelque chose qu'il faut craindre en tant que tel.

Les hackers vont-ils devenir des cyborgs ?
Cela fait des dizaines d'années que l'on améliore la condition humaine grâce à la technologie. Je pense par exemple aux personnes équipées de pompes à insuline ou de pacemakers, ou à celles qui disposent d'un système de gestion de la douleur par implant. Je pense donc que de plus en plus de hackers deviendront des cyborgs. Davantage de personnes suivront le même chemin que moi, en regardant ce que les implants peuvent leur permettre de faire et en ayant le désir d'interagir physiquement avec les systèmes informatiques. Si l'on considère la capacité d'innovation et de réflexion des hackers compétents, on peut conclure que les gens tireront parti de tout type de technologie susceptible de les aider à faire avancer leur cause. Cependant, je pense également que la nature invasive du processus de mise en place de ces dispositifs dissuadera un certain nombre de personnes. Tout le monde n'est pas prêt à se faire opérer ou piquer avec des aiguilles. □

Propos recueillis par Jérôme Cartegini

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.

Infogérance

TCS, le plus français des grands intégrateurs IT indiens ?

Implantée en France depuis 1995, la SSII indienne Tata Consultancy Services (TCS) engrange désormais de beaux dossiers auprès des grands comptes. Son succès s'explique-t-il uniquement par des clichés, tels que des tarifs agressifs sur les services ? Des prestations offshore de haute qualité en Inde ? Décryptage avec son DG, Rammohan Gourneni.



L'Informaticien : Qu'est-ce qui différencie vraiment Tata Consultancy Services (TCS) des grands intégrateurs IT français ?
Rammohan Gourneni, directeur général de la filiale française de la société de service IT indienne Tata Consultancy Services (TCS) : La principale force de TCS provient de ses quelque 50 ans d'expérience dans l'informatique à travers le monde. TCS est connu à l'international pour son approche centrée sur le client et pour sa capacité à lui délivrer ce qu'elle a promis. Le groupe possède d'ailleurs de nombreux centres de services capables de répondre localement à leurs besoins dans plusieurs régions ou pays, dont les États-Unis, l'Inde, la France, *etc.* Un client peut même être suivi par nos équipes dans le monde entier avec une gouvernance et des processus uniques. L'une des grandes forces de TCS est également de savoir nouer des partenariats avec les fournisseurs IT les plus innovants dans un écosystème au service du client.

Ne pensez-vous pas que vos principaux concurrents français et européens auraient pu faire une réponse similaire ?
La même réponse ? Sans doute parce que toutes les grandes SSII (Accenture, Atos, CapGemini, IBM, *etc.*), françaises notamment, possèdent aussi des centres de développement IT en Inde. Mais sont-elles meilleures dans l'exécution que TCS ? Ma certitude est que TCS est très en avance sur la plupart d'entre elles en matière d'infogérance et de « delivery offshore » notamment.

Sur quels plans TCS serait-il plus compétitif qu'eux ? L'outsourcing ? Les processus ? Le service ?
La qualité de service grâce à nos processus standardisés et éprouvés au niveau global et dans chaque région où TCS est implanté. Notre succès réside dans la qualité et le niveau d'exécution unifié des processus, des outils et des services demandés par les clients. Dans ce domaine, TCS fait partie des meilleures au plan mondial. Pour preuve, 96 % de la croissance de TCS provient de ses clients existants !

Et sur les prix des services aussi ?
Même si l'IT devient de plus en plus un produit de commodité, TCS reste un acteur unique dans son domaine car il est compétitif sur les prix dans certains domaines, tout en délivrant des services à valeur ajoutée. C'est possible car le groupe possède une bonne compréhension des processus, des outils et besoins des clients, ce qui lui permet de réussir des projets de transformation importants.

L'organisation interne et commerciale de TCS France est-elle encore différente de celle de votre maison-mère indienne et de celles de vos concurrents français ?
Non, pas depuis le rachat en 2013 d'Alti, une société de services IT française. TCS France a investi ensuite des millions d'euros pour aligner les processus et offres de notre maison-mère sur les besoins des entreprises françaises. Aujourd'hui, nous ne sommes pas alignés à 100 % car nous tenons compte des particularismes de la France. Cela nous a pris un peu de temps pour adapter nos processus et acquérir les bons talents mais le résultat est là.

TCS possède-t-il aujourd'hui les parts de marché et une place conformes à ses ambitions en France ?
Nos succès ces cinq dernières années auprès de grands comptes français, ainsi que leur reconnaissance, nous ont donné confiance dans nos capacités à faire de TCS un vrai « *game changer* » sur le marché français. TCS a doublé ses revenus sur ces six dernières années en France

(317 M€ NDLR). Et nous continuons de délivrer une croissance à deux chiffres en 2023. Nous allons continuer à investir et à recruter en France.

Les secteurs qui tirent la croissance du groupe TCS au plan mondial (28 Md$ de CA (+13,7 %)) sont-ils les mêmes qu'en France ?
Nous n'avons pas accès au secteur public pour des questions d'éligibilité, mais pour le reste, la réponse est oui. TCS France a de grands clients dans les secteurs de l'Energie, de l'Automobile, de l'Hospitalité, du Luxe, des Utilities, *etc.*

TCS n'adresse-t-il que les grands comptes parisiens ou démarche-t-elle également d'autres comptes plus petits en région désormais ?
Oui. Pourtant, ce n'était pas le cas il y a quelques années car nous étions beaucoup plus sélectifs sur les clients avec lesquels TCS voulait travailler en France. Aujourd'hui, nous travaillons davantage avec de PME sur leurs projets de transformation. La taille ne compte pas si le client désire vraiment travailler avec TCS. Y compris dans des secteurs de niche.

Les clients français de TCS ont-ils beaucoup recourent au nearshore, voire à l'offshore en Inde ou ailleurs ?
Cela dépend des besoins des clients français. Et malgré la qualité de service offerte par TCS, certains d'entre eux ne souhaitent pas recourir à l'offshore en Inde, pour des questions de souveraineté et/ou de sécurité notamment. Raison pour laquelle TCS leur propose localement des talents, des processus ainsi qu'un niveau de service très élevé, avec un suivi en mode « Follow the sun ». Notre centre de services basé à Paris-La Défense totalise environ 250 sièges, auquel s'ajoutent les quelque 150 sièges de notre centre à Poitiers, mais aussi d'autres à Lyon, à Bordeaux, *etc.*

Des conseils à donner aux entreprises qui déclarent rencontrer des difficultés à travailler avec des prestataires en Inde ?
Oui, cela dépend autant de l'état d'esprit du client que de ses processus et de sa capacité à travailler à l'étranger et dans une nouvelle langue. Dans le secteur du retail par exemple, de nombreux clients de TCS travaillent en Inde, et nous formons donc localement des collaborateurs francophones à leurs processus et métiers. Nous en recrutons même en France ou en Afrique du nord que nous établissons en Inde pour localiser la réponse à leurs besoins.



TCS France souffre-t-il, comme ses confrères, de la pénurie de talents et du turnover élevé dans certains domaines ? Et comment TCS combat-il cette tendance ?
Oui. C'est le cas dans le monde entier, car la demande des entreprises pour une transformation numérique de leurs processus et organisation est très élevée. TCS a lancé de grands programmes de recrutement et de formation. Le groupe déploie aussi les moyens nécessaires pour retenir les meilleurs talents en France et dans d'autres pays. TCS affiche le plus faible taux de turnover des intégrateurs en Inde car nous offrons de nombreuses opportunités et promotions à nos collaborateurs. Et cela fonctionne en France car le taux d'attrition est aujourd'hui bien inférieur à 10 % à Paris, alors qu'il était d'environ 30 % quand je suis arrivé à la direction générale de TCS France en 2015. Et il est encore plus faible en province !

L'Inde compte d'excellentes SSII, dont TCS, mais pourquoi a-t-on parfois l'impression qu'elles peinent à pénétrer vraiment les marchés européens ? Quels sont les obstacles ? (TCS CA +9,2 % en Europe vs 11 % en UK vs 24 % en Amérique du Nord en 2022 NDLR)

TCS est arrivé sur le marché européen un peu plus tard que sur les marchés américains ou anglais par exemple, pays dans lesquels le groupe est déjà présent depuis presque une cinquantaine d'années. En outre, l'Europe est constituée de différents pays et marchés. Il nous a donc fallu davantage de temps pour nous adapter à leurs différentes cultures, langages et besoins spécifiques.

Vos efforts ont-ils payé en Europe ?
Nos efforts ont payé puisque TCS a enregistré chaque année une bonne croissance en Europe ces 10 dernières années. Et malgré deux années difficiles de Covid, TCS a enregistré sur la période des croissances de l'ordre de 15 à 18 % dans la plupart des pays européens. Ce qui n'a pas été le cas au Royaume-Uni ou aux États-Unis par exemple. L'Allemagne et les Pays-Nordiques sont des marchés qui pèsent désormais un milliard d'euros chacun. □

Olivier Bellin

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

Tendance

Bonne croissance en 2022 du secteur du Numérique mais ralentissement à prévoir en 2023

Numeum a dévoilé en septembre son étude réalisée avec la société de conseil KPMG sur les performances 2022 des Entreprises de Services du Numérique (ESN) et d'Ingénierie et de Conseil en Technologies (ICT) en France. C'est un bon cru malgré une baisse de leur rentabilité et une pénurie de talents qui devraient s'accentuer en 2023.

« *Les entreprises du numérique n'ont pas été épargnées en 2022, et ont subi de plein fouet les tensions géopolitiques et l'inflation qui en découlent. Néanmoins, la plupart des acteurs ont enregistré une croissance à deux chiffres. La pénurie de talents reste un défi de taille* » affirme Charles Mauclair, président du Collège ESN et ICT du syndicat de Numeum.

Xavier Niffle, associé Technologie, Media et Télécoms de KPMG, est plus circonspect pour 2023, même s'il se déclare lui aussi « *bluffé par la performance des ESN en 2022, malgré le retour de l'inflation, la tension sur les talents, la guerre en Ukraine, etc. Toutefois, leur dynamique s'est un peu cassée et je table sur un ralentissement de leur croissance dès le second semestre 2023. Je table également sur un niveau de rentabilité en baisse dans les ESN car impossible pour elles de répercuter systématiquement les augmentations de salaire sur les donneurs d'ordre* ».

Une croissance principalement portée, selon la société de conseil KPMG, par le développement d'offres à valeur ajoutée (80%), le recrutement (74%) et le positionnement sur des secteurs porteurs (62%) tels que les services financiers, l'énergie et l'industrie. Résultat, 98% des 150 ESN (VAR, intégrateurs, SSII, éditeurs) et ICT sondées se disent confiantes ou très confiantes dans leurs objectifs de croissance à 3 ans (+3%).



Véronique Torner, présidente de Numeum.

Quant aux services et solutions IT les plus dynamiques en 2022, le conseil IT (25%) prend la tête du classement devant le cloud (21%) et la conception de solutions IT (16%). « *2023 a également marqué l'entrée de technologies émergentes telles que les intelligences artificielles génératives, source d'opportunités pour les ESN et ICT, tant pour optimiser l'efficacité interne de leurs processus que pour apporter de la valeur à leurs clients* » ajoute Xavier Niffle de KPMG.

Course au talent : le défi des ESN

Le recrutement, la fidélisation et la formation des talents se sont accélérés pour soutenir la croissance des ESN et ICT. Leurs objectifs de recrutement pour 2023 sont même ambitieux, même s'ils sont en recul par rapport à 2022. 81% des sondés ont confiance dans leur capacité à recruter suffisamment de talents à 3 ans, soit une baisse de 8 points sur un an. Pour y parvenir, elles investissent davantage dans la formation et la fidélisation des talents : 3,4% de la masse salariale sera consacrée aux actions de formation en 2023.

Et pour pallier la pénurie de talents qui touche particulièrement le secteur de la tech, les ESN et ICT rencontrent davantage de jeunes diplômés lors de salons et forums.

Par ailleurs, 58% des entreprises interrogées prévoient d'augmenter les salaires pour fidéliser leurs salariés. Selon Numeum, les rémunérations ont augmenté de 4% en moyenne en 2022. En prime, 85% des ESN et ICT proposent deux à trois jours de télétravail par semaine afin de répondre aux attentes de leurs collaborateurs.

Les ESN et ICT investissent davantage dans la R&D

Les ESN et ICT ont investi en moyenne 7% de leur chiffre d'affaires dans la R&D et l'innovation en 2022. 13% de leurs effectifs s'y consacrent à temps plein (+8% par rapport à 2021). Ces investissements concernent cinq technologies et méthodologies en priorité : le cloud (18%), la conception de solutions technologiques (14%), le conseil en transformation digitale (14%), l'intelligence artificielle (14%) et la cybersécurité (12%). Mais KPMG souligne que seuls 31% des projets se concrétisent par une mise en production. □

Olivier Bellin

Sécurité

Cato Networks prône le modèle SASE

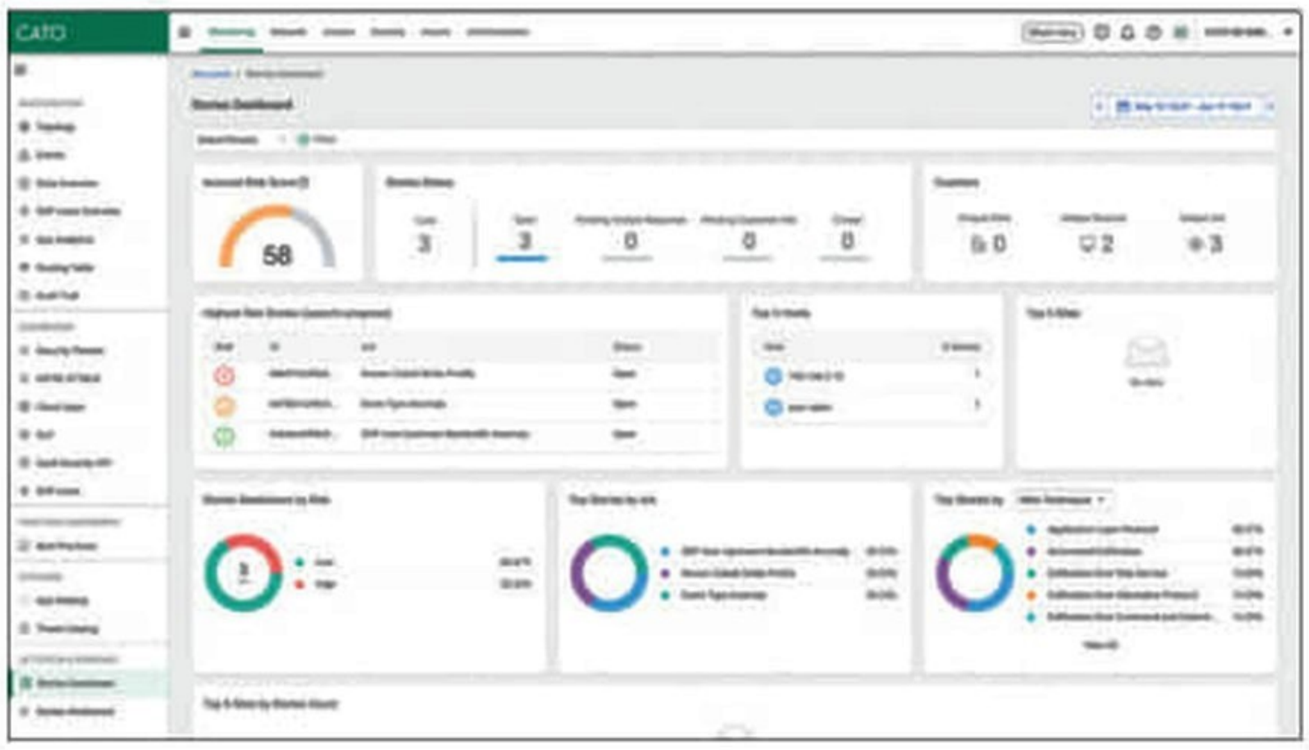
Développé par le cabinet Gartner, le modèle SASE vise à combiner sécurité et observabilité réseau pour assurer une meilleure protection des entreprises. Cato Networks propose sa propre approche.

Lors d'une démonstration, *L'Informaticien* a pu voir en action la plateforme SaaS de Cato Networks. En pratique, l'éditeur propose un nouveau modèle pour SASE qui s'appuie sur une architecture unifiée relié à un plan de contrôle dans le Cloud sous la forme d'un data lake pour gérer l'ensemble des opérations.

Sur leur propre cloud

L'éditeur a des clients de tous types, grands comptes ou plus petites entreprises comme des cabinets d'avocats. Benjamin Simon, Sales Engineer chez Cato Networks, précise : *« nous avons des grands comptes qui ont choisi une approche full SASE comme l'appelle le Gartner et des comptes plus petits ayant aussi des services critiques et nous essayons de leur apporter les meilleures solutions réseaux et de sécurité avec notre proxy web et notre bridge pour leurs systèmes hétérogènes vers notre cloud »*. Il ajoute ; *« le modèle consiste à déporter l'intelligence vers le Cloud »*.

L'idée est de faire converger les services présents vers la plateforme cloud de Cato Networks. Celle-ci est opérée par l'éditeur dans des centres d'Equinix avec des points de présence partout dans le monde pour autoriser une sécurité 24/7/365 tout autour du globe. Le data lake est distribué et l'infrastructure est ainsi à l'échelle nécessaire pour fournir



Un rapport dans Cato Networks.

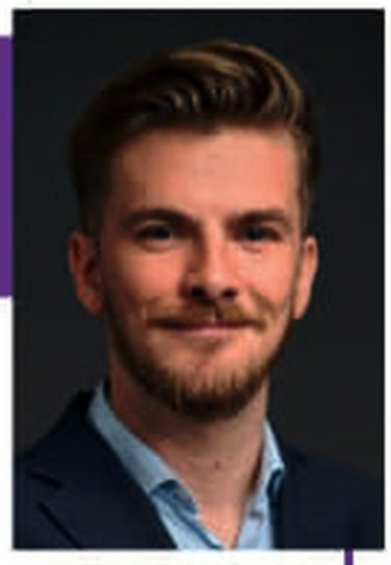
des services quasi temps réels aux clients sur leur sécurité. Il en est de même pour la bande-passante réseau. *« Le tunnel chiffré est de 6 Go chez nous, il est de 500 Mo chez les hyperscalers »* précise Benjamin Simon. *« Nous pouvons offrir des niveaux de services à 99,999 »*. Ce chiffre s'explique par une architecture full mesh du réseau et des points de présence au plus près de l'exécution des applications des clients pour augmenter la résilience et réduire la latence. Cato s'occupe aussi du routage et du trafic vers son Cloud. Chaque point de présence applique les politiques de sécurité et des mécanismes d'optimisation protocolaires avec des algorithmes propriétaires. Le protocole ainsi optimisé travaille en une seule passe en interception et déchiffrement. Le trafic est ensuite analysé et rechiffré avec les clés du client si nécessaire (BYOK ou Bring Your Own Key). Le moteur fonctionne en temps réel et analyse de plus le contexte pour les routines de sécurité. Enfin, tout est fait pour assurer la performance et améliorer le trafic : compression IP, répartition de charge dynamique, QOS adaptative.

Des fonctions de firewall au niveau 4, de la micro-segmentation et du contrôle d'accès renforcent la sécurité de la solution. Benjamin Simon ajoute : *« nous faisons la même chose du côté centre de données ou dans la version virtualisée ou nous montons simplement un tunnel IPSEC au niveau des points de présence pour l'analyse »*.

GROSSE LEVÉE DE FONDS POUR CATO NETWORKS

Récemment, Cato Networks a levé 238 millions de dollars en fonds propres portant le financement total à 773 millions de dollars. Cato utilisera les nouveaux fonds pour développer son organisation dans trois domaines clés : transmettre la vision de Cato et le succès de ses clients à un public plus large, étendre l'écosystème de partenaires offrant des services gérés Cato SASE et développer l'équipe d'ingénierie et de produits. Cette dernière levée de fonds a été menée par LightSpeed Venture Partners avec la participation d'Adams Street Partners, Softbank Vision Fund 2, Sixty Degree Capital et Singtel Innov8. À l'issue de cette levée de fonds, Ravi Mhatre, fondateur et directeur général de LightSpeed Venture Partners, rejoint le conseil d'administration de Cato.

Benjamin Simon,
Sales Engineer
chez Cato Networks.



« Le tunnel chiffré est de 6 Go chez nous, il est de 500 Mo chez les hyperscalers. »

Vers le XDR

Cato Networks a développé son propre SIEM (Security Incident and Event Management) et s'oriente maintenant vers le XDR, un outil de détection et réponse qui analyse à la fois réseau et événements de sécurité. *« Sur ce point nous faisons beaucoup d'effort sur l'expérience client avec la recherche de la simplicité dans la mise en œuvre et l'exploitation pour que les clients ne se retrouvent pas à la tête d'une usine à gaz »*.

Une mise en œuvre simple

Dès la souscription à la solution de Cato Networks, il est installé un boîtier dont la seule utilité est de se connecter au Cloud de l'éditeur. De là, l'entreprise s'enregistre et le boîtier se connecte au point de présence le plus proche. Une zone de maintenances est alors définie pour les mises à jour. L'administrateur peut ensuite ajouter les services DHCP. Le déploiement, les montées de version et le suivi se réalisent au niveau de la couche 3 en actif avec visibilité sur ce qui transite, les analyses des applications, ce qui se passe sur les machines des utilisateurs... Ce niveau va encore s'enrichir à l'avenir, indique Benjamin Simon. Le boîtier peut être minimaliste et de nombreux clients choisissent un simple Rasperry Pi pour le faire afin de monter le tunnel et d'avoir accès aux services de sécurité de l'éditeur, ce qui est son offre de base. Les autres services s'activent à partir de la console d'administration.

Un des services proposés est de réaliser les mises à jour des boîtiers par un script afin de dégager du temps pour les équipes des clients et non d'avoir à s'occuper de la mise à jour d'un élément qui ne monte qu'un tunnel IPSEC. Il est possible de programmer de nombreuses actions sur la plateforme par des développements Infrastructure as code sur un mode déclaratif vers Ansible pour les déployer et les orchestrer.

Une gestion des accès rigoureuse

Pour les accès, l'éditeur supporte de nombreuses possibilités comme LDAP, Active Directory, Okta et Eidas. À partir de là, un périmètre applicatif est attribué à l'utilisateur avec différents attributs qui correspondent à ses besoins dans l'entreprise selon les politiques de sécurité définies par celle-ci. S'y ajoute la posture de sécurité du matériel utilisé. Un catalogue applicatif et une base de connaissances réalisent une sorte d'audit de la plateforme du client pour définir s'il respecte la posture globale de sécurité ou non.

Si des opérations doivent s'effectuer en dehors du périmètre défini, un agent actif se relie au point de présence le plus proche pour activer les services et garantir la posture de sécurité. Il en est de même dans des localisations jugées difficiles comme la Chine, par un bypass du Grand Firewall en place tout en respectant la législation chinoise sur le Smart Egress. Il est de plus possible de réserver une IP de sortie.

Un service de Threat Intelligence

Dans la panoplie de services développés par Cato Networks, un service de Threat Prevention apprend de ce qui se passe sur la plate-forme de Cato Networks afin de créer des signatures et me mettre à jour les équipements. L'opération se réalise en mutualisant le trafic sur la plateforme pour valider cette signature avant de les déployer automatiquement chez les clients. Benjamin Simon assure que cette solution est plus efficace que les IPS existants. □

B.G



Une topologie du réseau à partir de Cato Networks.

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 €

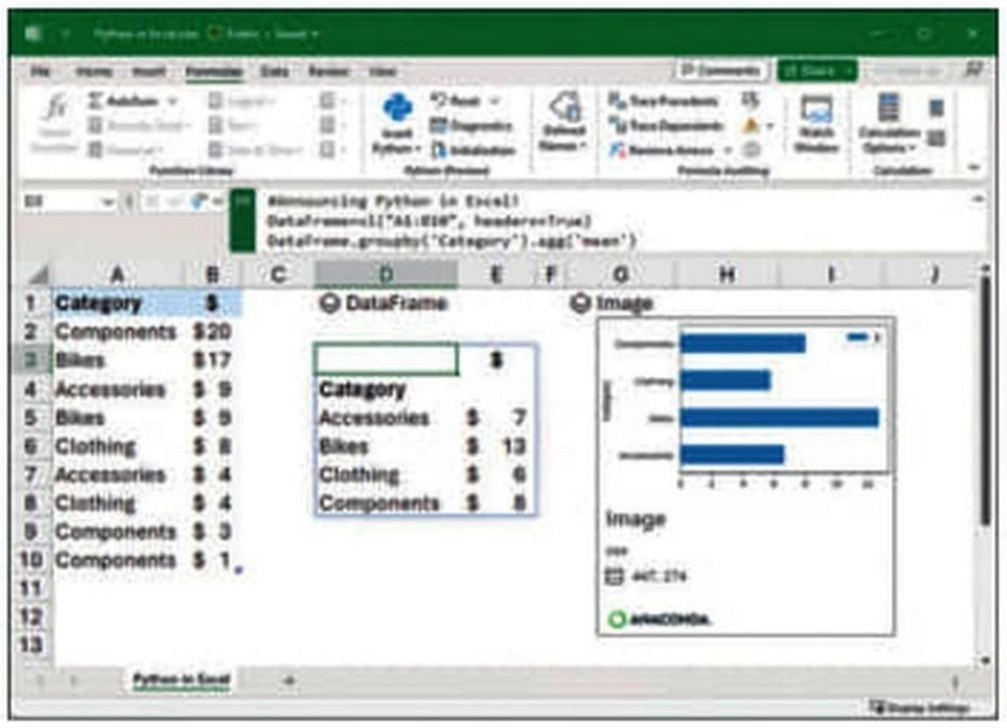
Intégration

Python dans Excel : Microsoft rapproche son tableur des Data Science

Insérer une formule en Python dans une feuille Excel, c'est actuellement possible pour les membres du programme Microsoft 365 Insider. Simple curiosité technique ou vraie avancée pour les inconditionnels du tableur Microsoft ?

En dépit de son âge canonique (sa version 0.9.0 date de 1991), Python reste l'un des langages informatiques les plus populaires auprès des développeurs et notamment des Data Scientists chargés de développer des algorithmes avancés d'analyse des données.

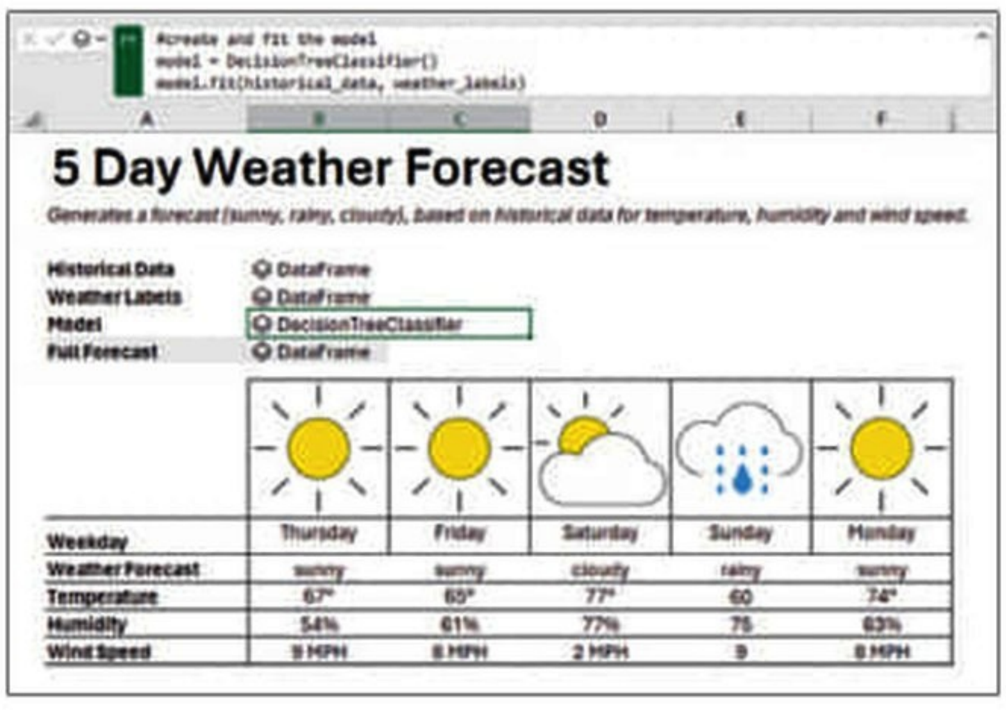
Désormais, ce sont les inconditionnels d'Excel qui vont pouvoir se frotter au reptile et glisser du code Python dans les cellules de leur tableur préféré. En pratique, Python dans Excel est encore en préversion. Il faut faire partie du programme Microsoft 365 Insider pour pouvoir le tester. Dès lors, il suffit de taper « =PY » dans une cellule pour activer Python, ou cliquer sur le « Insert Python » dans le ruban Excel dédié aux formules. La fonction xl() permet de faire référence à une cellule ou un groupe de cellules ou à un DataFrame. Une capacité clé de Python dans Excel est d'importer des données externes dans la feuille Excel. Pour cela, il faut passer par Power Query pour importer les données, puis les traiter en Python *via* la fonction xl() en passant le nom de la requête en paramètre.



La mission de Python dans Excel est de faire cohabiter des éléments de reporting et des algorithmes de Data Science au sein d'une même feuille Excel.

Les librairies Anaconda présentes à l'appel

Python dans Excel embarque les librairies rassemblées dans la distribution Anaconda. Outre Matplotlib, NumPy, Pandas, Seaborn et Statsmodels, il est possible d'importer d'autres librairies Anaconda, notamment les fameux PyTorch et scikit-learn, bien connus des Data Scientists. Microsoft a bridé la librairie Pandas dédiée à la manipulation des données afin de limiter les risques d'attaque informatique. Cette problématique Cyber se pose tout particulièrement lorsque les feuilles Excel sont partagées sur Internet ou envoyées par des sources non approuvées. Microsoft a conservé les stratégies de sécurité d'Excel lorsqu'on ouvre des classeurs à partir d'Internet ou de sources non approuvées. Le mode protégé d'Excel va empêcher l'exécution des scripts Python dans le classeur, et si le classeur est ouvert avec Microsoft Defender Protection d'application, les formules Python ne s'exécutent pas par défaut.



Faire appel à des algorithmes d'IA exploitant les librairies Python scikit-learn et Statsmodels directement dans une feuille Excel, c'est d'ores et déjà possible avec cette préversion de Python dans Excel.

S'il est déjà possible d'exécuter des scripts Python sur Power BI en local, pour Excel, Microsoft a fait le choix d'exécuter le code Python uniquement dans un conteneur sur Azure Container Instances, un conteneur qui embarque Python et ses bibliothèques Anaconda. Microsoft précise que cette architecture empêche le code Python d'avoir accès aux ressources de la machine ou au compte de l'utilisateur. Le code Python n'ayant pas d'accès réseau, toute référence à des données externes doit passer par Power Query.

Python dans Excel est disponible pour Excel pour Windows, mais pas encore pour les versions Web, Mac, et mobiles. □

AC

Teradata

Un arsenal pour opérationnaliser l'IA

En capitalisant sur sa position de géant de l'analyse de données, Teradata a résolument mis le cap sur l'opérationnalisation de l'intelligence artificielle lors de son événement Possible 2023, à Londres, les 12 et 13 septembre derniers. Mais au-delà des déclarations et de la présentation d'une boîte à outils bien garnie, l'adoption généralisée de l'IA au sein des entreprises est encore loin d'être une réalité.

Comme tant d'autres entreprises depuis le lancement de ChatGPT en novembre dernier, et le raz-de-marée d'IA génératives qui en a découlé, Teradata, le spécialiste de l'analyse de données, suit logiquement le mouvement et prend le train (à grande vitesse) de l'IA en marche. *« Nous sommes les rois de la data, donc l'intelligence artificielle générative est une excellente opportunité pour nous »*, expliquait Stephen Brobst, le Chief Technology Officer de la société. C'était, en substance, l'essentiel du message que Teradata a voulu faire passer lors de son événement Possible 2023, à Londres, début septembre.



« Ils (les patrons d'entreprises ndlr) *s'accordent tous à dire qu'investir dans l'IA doit offrir une expérience véritablement différenciée, basée sur de bonnes données sinon, ce n'est qu'un gaspillage d'argent. »*
Steve McMillan, President and Chief Executive Officer (CEO) de Teradata.

VantageCloud Lake sous stéroïdes avec ask.ai

Passé les déclarations fracassantes sur les potentialités de l'IA, Teradata s'est lancée, ces derniers mois, dans une vaste campagne faite d'acquisitions et de présentation de nouvelles solutions dopées à l'IA. En juillet dernier par exemple, Stemma Technologies, une solution cloud native de catalogue de données et métadonnées entièrement gérée, est passée sous son giron. Stemma est connue pour avoir introduit des technologies d'intelligence artificielle dans sa solution de catalogue afin de simplifier la recherche, la découverte et la confiance dans l'utilisation des données des entreprises.

Autre exemple, Teradata a annoncé, début septembre, un partenariat avec NordCloud pour accompagner les clients européens dans la migration de leurs données sur site et des environnements analytiques vers la plateforme Teradata VantageCloud Analytics and Data. D'une pierre deux coups, par ce biais, la société entend accélérer les déploiements cloud de ses clients, tout en les amenant dans un écosystème de cloud et d'analyse avancée saupoudré d'IA/ML.

De retour à Londres, l'entreprise a présenté ask.ai, un nouvel assistant d'IA générative dédié à sa plateforme analytique de données cloud VantageCloud Lake. Sur le papier, cette solution fournit aux data scientists une interface en langage naturel conçue afin qu'un utilisateur puisse faire des requêtes sur les montagnes de données d'entreprises complexes, parfois difficiles à dénicher et donc à analyser, puis de recevoir ensuite des réponses instantanées et complètes, censées garantir une analyse cloud fiable et améliorer la prise de décision de l'organisation.

Développer une IA "responsable"

Et ce n'est d'ailleurs pas qu'aux data scientists que se destine ask.ai, mais plus globalement à tous les employés autorisés à n'importe quel niveau, devant visualiser et analyser des données/métadonnées, ou encore générer du code automatiquement sans avoir à l'écrire manuellement. Un collaborateur n'ayant, par exemple, pas une grande expérience en codage pourra créer des extraits de code en exprimant ses attentes en langage naturel. Les développeurs, eux, peuvent ainsi en théorie se concentrer sur la logique de haut niveau et la résolution de problèmes. Stephen Brobst reconnaît toutefois que

« plutôt que d'embaucher de nouveaux data scientists, cet outil devra fournir une assistance qui augmentera la productivité de ceux déjà en place de 50 %, par exemple. »

Pour vulgariser, ask.ai ne serait-il pas une sorte de ChatGPT sauce entreprise, tout simplement ? Teradata fait une distinction avec l'outil d'OpenAI. *« Du point de vue de l'IA – beaucoup d'attention est portée sur ChatGPT car c'est gratuit. Mais si c'est gratuit, vous devenez le produit. Tout ce que vous demandez à ChatGPT lui sert ensuite de base de connaissances »*, prévient Stephen Brobst. Une perspective qui n'enchante pas forcément des organisations ayant un besoin de traitement de données potentiellement sensibles. Et c'est bien sûr cette crainte que Teradata compte capitaliser. Notamment en déployant des IA présentées comme responsables et protégeant la confidentialité des données *« qui n'iront jamais dans le domaine public »*, garantit Stephen Brobst.

Des entreprises encore indécises

Mais fondamentalement, les entreprises sont-elles prêtes à adopter l'IA générative ? Teradata le reconnaît, ça ne sera pas une mince affaire. Une étude IDC Executive Preview, sponsorisée par l'entreprise et intitulée *« The Possibilities and Realities of Generative AI »* a été menée auprès de 900 décideurs et cadres supérieurs, issus de grandes entreprises autour du globe. Les conclusions ne sont à première vue guère encourageantes et mettent en exergue ce qui pourrait s'apparenter à une crise de confiance. Même si ces conclusions sont à remettre en perspective puisqu'*a priori*, l'IA générative n'en est qu'à ses balbutiements. Les résultats révèlent que si neuf dirigeants sur dix reconnaissent le potentiel de l'IA générative, deux sur trois s'inquiètent de la création de partis pris et de la diffusion de fausses informations. Une autre donnée révèle que 86 % des répondants estiment qu'il est nécessaire de renforcer la gouvernance, afin de garantir la qualité et l'intégrité des résultats de l'IA générative.

À quoi s'ajoute que *« seulement 30 % des entreprises se disent extrêmement préparées ou prêtes à tirer avantage de cette technologie »*, indique Teradata dans un communiqué. La faute à une pénurie de « talents » autour de l'IA, estime l'étude. Pour vanter les mérites des capacités d'analyse de l'intelligence artificielle, on a vu mieux. Mais ladite étude étant sponsorisée par Teradata, l'entreprise voit le verre à moitié plein et semble bien décidée à poser les premières briques. L'étude avance également qu'avec l'avènement du télétravail et du travail hybride, ou encore les préoccupations grandissantes autour des questions sociales, environnementales et de gouvernance, 70 % des répondants reconnaissent que les données au sein de leur organisation ont gagné en complexité. Et toutes ces données complexes, il va bien falloir les traiter efficacement pour en tirer des informations utiles à l'entreprise. Et la complexité de la donnée Teradata aime ça. □

V.M

DE L'EXPÉRIMENTATION À L'INDUSTRIALISATION

Avec l'intégration, en mai dernier, de Vertex AI de Google Cloud à Teradata VantageCloud et ClearScape Analytics, la société vise un objectif précis : faire passer les entreprises de l'expérimentation à l'industrialisation afin d'opérationnaliser l'IA au sein de leur organisation. Et la marche est haute. Car à en croire une étude publiée par Accenture intitulée *« The art of IA maturity, Advancing from practice to performance »*, 63 % des entreprises n'ont pas de stratégie d'IA suffisamment matures pour tendre vers cette opérationnalisation. Avec l'intégration de Vertex AI dans ses outils, Teradata dit vouloir permettre *« aux entreprises de mettre en production des modèles IA/ML plus sophistiqués, plus rapidement, et de mettre à l'échelle ces modèles dans toute l'organisation. »* Concrètement, les utilisateurs sont en mesure d'intégrer des ensembles de données répartis dans différents environnements, de construire et d'entraîner des modèles d'IA/ML pour l'entreprise en s'appuyant sur les ensembles de données préparés par ClearScape Analytics et d'opérationnaliser les modèles de Vertex AI dans Vantage Cloud.



Hillary Ashton, Chief Product Officer (CPO) de Teradata.

GenAI Pro

Les entreprises sont séduites mais prudentes

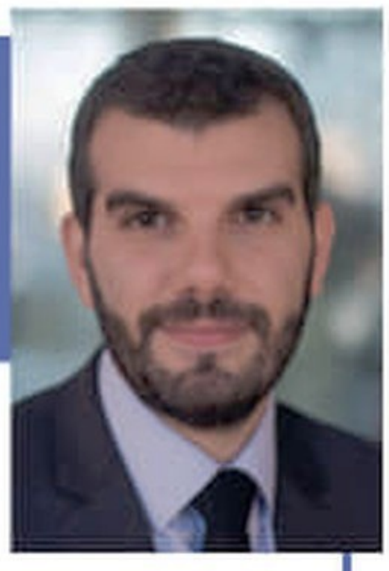
OpenAI, l'éditeur américain de ChatGPT, ainsi que ses principaux concurrents (Google, AWS, Microsoft, etc.), ont tous dégainé cet été des versions Entreprise de leurs chabots ou Intelligences Artificielles conversationnelles (GenAI) grand public. Suffiront-elles à convaincre les entreprises de généraliser leurs utilisations en interne ?

Petits ou grands, propriétaires ou en open source, les modèles de langage (LLM) qui sous-tendent les outils d'Intelligence Artificielle (IA) existent depuis des années. Ils sont passés de l'ombre à la lumière grâce à *« OpenAI, qui a créé fin 2022 la sidération et un engouement général pour l'IA chez tout le monde grâce au lancement marketing très réussi de la version grand public de son chabot ChatGPT »* analyse Chadi Hantouche, un partenaire du cabinet de conseil en technologies WaveStone en charge de l'IA.


La Gen AI fascine tout autant les entreprises qu'elle les inquiète.

À peine huit mois plus tard, cet éditeur américain, ainsi que ses principaux concurrents, principalement des Gamma (Google, AWS, Microsoft, *etc.*), ont tous dégainé dès l'été des versions Entreprise de leurs chabots ou Intelligences Artificielles conversationnelles (Gen IA). Toutes sont basées sur de grands modèles de langage (LLM) (voir tableau des offres ci-dessous). La plupart de ces versions Entreprise vendues sur étagère sont également disponibles en France désormais, et souvent en français.

Mais les entreprises sont-elles enfin prêtes à aller au-delà des premiers tests départementaux réalisés au premier semestre 2023 sur les versions de GenAI grand public de ChatGPT 3 et 3,5 ou d'Amazon Bedrock, Google Vertex AI, *etc.* Henri d'Agrain, délégué général du Cigref, en est certain.



Chadi Hantouche, partenaire du cabinet de conseil en technologies WaveStone.

« OpenAI a créé fin 2022 un engouement général pour l'IA grâce au lancement réussi de son chabot ChatGPT. »

Selon lui, tous les adhérents de cette association qui regroupe beaucoup de DSI des grandes sociétés françaises, *« utilisent déjà ces versions Entreprise, mais avec des temporalités différentes, qui varient en fonction du caractère très concurrentiel de leurs activités. Ceux qui sont encore sur des zones de confort ne vont pas autant se précipiter sur la GenAI que ceux dont l'activité est très concurrentielle, et qui ont peur de perdre des parts de marché s'ils n'adoptent pas ces outils ».*

Les versions Entreprise sont-elles plus sécurisées ?

Henri d'Agrain confirme ainsi que la plupart des DSI sont séduites voire rassurées, *a priori*, par les caractéristiques de ces premières versions Entreprise. Les éditeurs et hyper scalers ont tenté de répondre à leurs craintes en matière de sécurisation et d'administration des données. Et pour cause, ils redoutent de voir davantage d'entreprises interdire à leurs salariés d'utiliser les versions grand public de leurs GenAI, afin de limiter les risques, bien réelles, de fuites de données.

« La sécurité est bien davantage au cœur des versions professionnelles de leurs chatbots conversationnels ou de leurs LLM, ce qui est une très bonne chose », confirme Jérôme Malzac, directeur de l'Innovation pour l'ESN Micropole. *« Mais quand j'en parle à nos clients des secteurs tels que ceux de la banque, des assurances, etc., certains s'inquiètent encore de devoir fournir à ces éditeurs des données sensibles de l'entreprise, qu'ils ne veulent pas révéler »*

Une inquiétude partagée par les DSI qui échangent avec Guillaume Gérard, responsable Gen AI pour l'Europe Sud de l'intégrateur Capgemini : *« ces versions Entreprise ont certes énormément d'intérêt pour les entreprises, et notamment parce qu'elles permettent d'élargir les cas d'usage. Toutefois, la plupart de nos clients ont encore besoin de s'assurer que la couche sécurité est bien au rendez-vous pour qu'ils puissent les intégrer dans leurs processus d'entreprise »*.

On l'aura compris, les éditeurs de ces chabots et GenAI doivent encore rassurer les clients des secteurs stratégiques ou réputés « sensibles ». OpenAI déclare pourtant sur sa brochure garantir aux entreprises que *« leurs conversations professionnelles avec notre chatbot ne sortiront pas de votre structure et ne seront pas utilisées pour entraîner les modèles de langage d'OpenAI. Toutes les données sont chiffrées « au repos comme en transit, avec les protocoles AES-256 et TLS 1.2+, et en conformité au regard de la norme SOC 2 »*.



Henri d'Agrain, délégué général du Cigref.

« Les grandes DSI utilisent déjà ces versions Entreprise avec des temporalités différentes. »

EXEMPLES D'OFFRES DE GENAI EN VERSION ENTREPRISE

Catégories GenAI	Ses composants	Amazon AWS	Google Cloud	IBM	Microsoft	Open AI
Modèles de langage Large (LLM) de base	Runtime	Amazon Bedrock	Vertex AI	Watsonx	Azure OpenAI, Azure ML for Llama	ChatGPT Entreprise
	Texte / Chat	Titan (Amazon), Jurrassic (AI21Labs), Claude (Anthropic), Cohere	Palm (modeles Text ou Chat-Bison)	WatsonX Assistant / Watsonx.ai	GPT-4, Turbo	ChatGPT 4
	Production de Code	Claude (Anthropic)	Codey	Watson code assistant models + selection of open source code foundation models	GPT-4, Turbo, DALL-E	ChatGPT
	Génération Image	Stable Diffusion (Stability.ai)	Imagen	-	Dall-E	Dall-E 2
	Traduction	Titan (Amazon), Jurrassic (AI21Labs), Claude (Anthropic), Cohere	Chirp	-	Azure AI Translator	ChatGPT Translator
Modèle au Catalogue	Commercial	Amazon Bedrock & Sagemaker Jumpstart (Model Hub)	Vertex AI Model Garden	Watsonx.ai foundation models	Azure ML Model Catalog, Azure OpenAI	ChatGPT
	Open Source	Amazon Sagemaker Jumpstart (Model Hub)	Vertex AI Model Garden	Foundation models from Hugging Face,	Azure ML Model Catalog	nc

Sources : Fournisseurs, ESN, AlliancesTech © 09-2023

Précisions : *certaines offres GenAI Entreprise ne figurent pas dans ce tableau non exhaustif, car pas d'informations fournies*

Les entreprises peuvent-elles réentrainer leurs GenAI Pro ?

Guillaume Gérard nous précise la situation en matière de réentrainement, laquelle est un peu floue pour beaucoup de personnes : *« les données fournies en entrée à la version premium de ChatGPT peuvent être réutilisées potentiellement par OpenAI pour continuer d'entraîner son LLM. En revanche, les clients de ChatGPT Entreprise ne peuvent pas réentrainer ses modèles, et notamment pas avec les données ou du contenu appartenant à l'entreprise. Celles-ci sont donc obligées de faire du scrapping à partir des données publiques sur le web »*. Beaucoup de sociétés ne le feront pas systématiquement, de peur d'être attaquées en justice sur des questions de droit d'auteur et de copyright.

OpenAI et ses concurrents peuvent-ils alors réussir à convaincre les entreprises lorsqu'ils affirment garantir une réelle confidentialité de leurs données sensibles et des droits d'auteur associés ? Les entreprises savent que ces éditeurs ou hyper scalers utilisent massivement les techniques de « scrapping » pour entraîner leurs IA conversationnelles. Ils ont donc déjà pillé et agrégé des milliards de données disponibles en ligne, puis les ont exportées massivement aux États-Unis. Malgré les lois européennes (DMA, DSA, IA Act, RGPD, *etc.*) protégeant, en théorie, les données de nos entreprises… Henri d'Agrain confirme cette situation et précise que *« nos adhérents ne tiennent pas à ce que ces LLM agrègent cette fois-ci leurs données stratégiques »*.



Guillaume Gérard, responsable Gen AI / Europe Sud - Capgemini.

« Les Entreprises ont encore besoin de s'assurer que la couche sécurité soit bien au rendez-vous. »



Jérôme Malzac, directeur de l'Innovation pour l'ESN Micropole.

« Nos clients s'inquiètent encore de devoir leur fournir des données sensibles de l'entreprise. »

Les versions Entreprise s'interfacent mieux au SI de l'entreprise

Par ailleurs, l'administration des données est l'un des points forts des versions Entreprise de ces logiciels de Gen AI. Leur console d'administration permet de gérer les API et les utilisateurs, d'administrer leurs droits et leurs utilisations de l'outil. Ils peuvent d'ailleurs employer le même identifiant sur toutes les applications grâce à la technologie SSO (Single Sign-On).

Ces consoles fournissent des informations précises sur leurs consommations de jetons et de requêtes. Les clients de ChatGPT Entreprise reçoivent d'ailleurs davantage de jetons leur permettant d'obtenir de réponses jusqu'à quatre fois plus longues. Cette version utilise aussi Code Interpreter, un plugin facilitant l'exécution du code et l'analyse de données complexes. Grâce à l'utilisation de GPT-4, ChatGPT Entreprise fonctionnerait jusqu'à 2 fois plus rapidement que ChatGPT Plus, une version intermédiaire basée elle sur GPT 3.5. Enfin, côté tarifs, OpenAI est moins transparent que la plupart de ses concurrents. L'éditeur annonce que les tarifs de ChatGPT Entreprise varient en fonction de l'utilisation de chaque entreprise… Selon nos informations, les différentes versions Entreprise de ces différentes GenAI sont facturées de 20 à 40 euros HT par utilisateur et par mois, hors (ré) entraînement et hébergement dans le Cloud. Un budget qui peut s'avérer vite conséquent. □

Olivier Bellin

LES VERSIONS ENTREPRISE HALLUCINENT-ELLES TOUJOURS AUTANT ?

Les éditeurs d'outils de GenAI sont très discrets au sujet des « hallucinations » produites par leurs modèles de langage. Pourtant, il leur arrive assez fréquemment de fournir des réponses non conformes à la réalité observable. *« Les entreprises doivent encore prendre leurs résultats avec beaucoup de précautions et s'assurer que les résultats obtenus sont conformes à ceux qu'elles sont en droit d'en attendre »*, explique Henri d'Agrain du Cigref.

Dans les coulisses, les éditeurs tentent de corriger le tir sur leurs versions Entreprise, comme le confirme Jérôme Malzac, directeur de l'Innovation de l'ESN Micropole : *« Micropole a abandonné cet été le déploiement de la version 3,5 de ChatGPT, car nos tests révèlent un taux de réponse sans hallucinations de seulement 60 %, contre environ 92 % pour ChatGPT 4 »*. Il en conclut que *« certains grands clients finiront par se rendre compte que la qualité de ces versions Entreprise n'est pas encore suffisante, car elles produisent encore beaucoup d'hallucinations »*.

adista

Pour un Système d'Information agile, durable et sécurisé

La synergie des services Connectivité, Cloud et Cybersécurité

TOPTECH
GREEN IT Économie circulaire | 2023

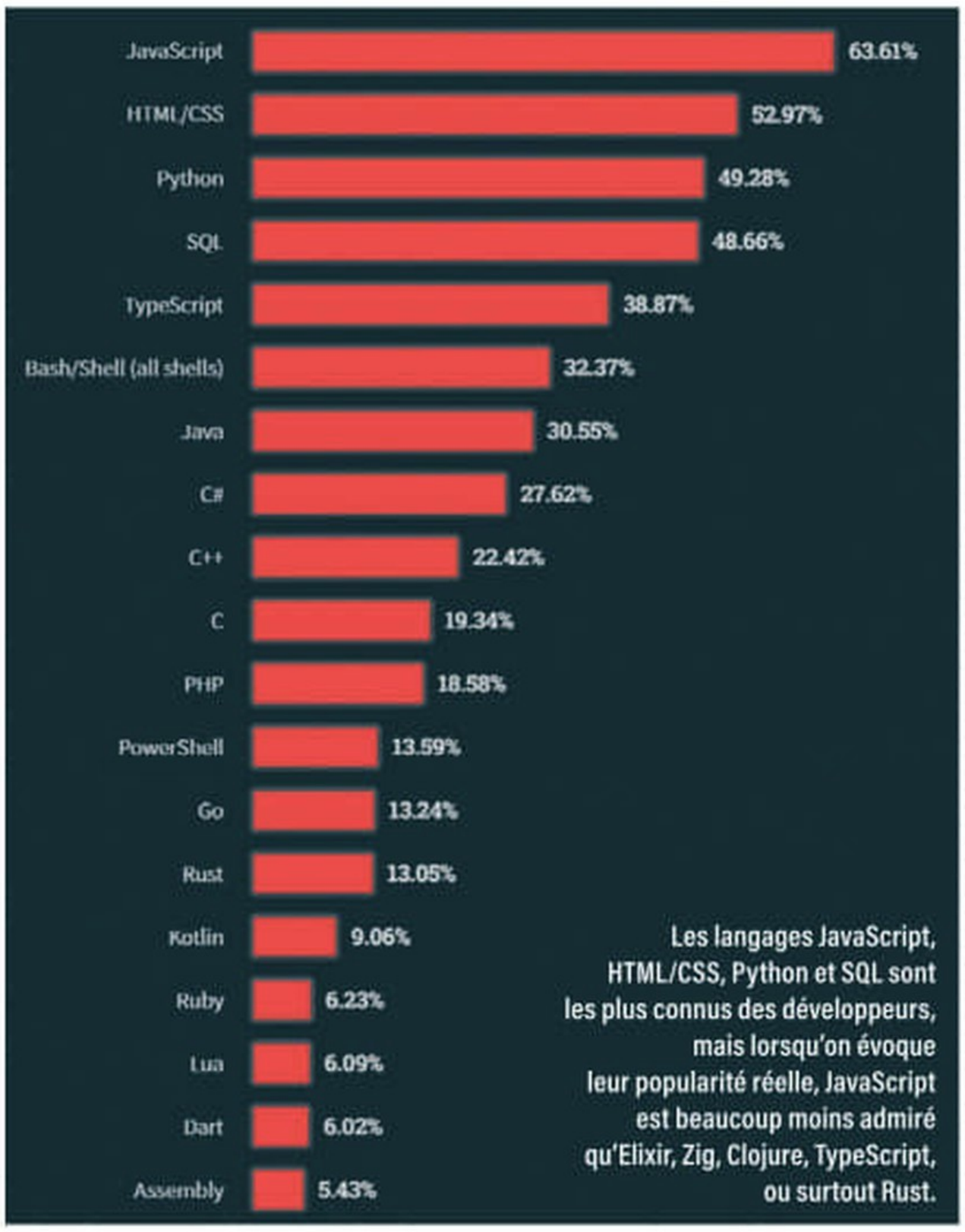
adista.fr
contact@adista.fr - 03 57 54 54 00

Tendances

Développeurs : quels sont vos outils préférés ?

Stack Overflow vient de publier les résultats de sa grande enquête annuelle auprès des développeurs. Avec près de 90 000 répondants, elle livre le catalogue idéal des solutions appréciées des développeurs. Avec quelques surprises à la clé !

Cette année, le questionnaire proposé par Stack Overflow relatif à leurs outils et pratiques, a été complété par 89184 développeurs dans 185 pays. L'occasion de faire le point sur les usages réels des technologies au-delà des débats et de l'actualité. Ainsi, le langage le plus connu des développeurs est JavaScript, devant HTML. L'incontournable Python qui arrive en troisième position devant SQL et, plus étonnant, TypeScript. Suivent ensuite les langages de shell, Java, le trio C# / C++ / C, Php et Powershell. La plus grosse progression est à mettre au compte de Lua, mais qui, avec 5,2 % des répondants, reste un langage de niche.



Les langages JavaScript, HTML/CSS, Python et SQL sont les plus connus des développeurs, mais lorsqu'on évoque leur popularité réelle, JavaScript est beaucoup moins admiré qu'Elixir, Zig, Clojure, TypeScript, ou surtout Rust.

Du côté des bases de données, la solution la plus citée n'est plus MySQL, n°1 l'an dernier, mais PostgreSQL, tirée vers le haut par les développeurs classés professionnels. Suivent MySQL, SQLite, MongoDB et Microsoft SQL Server. Il est à noter que les étudiants placent MongoDB en deuxième place, derrière MySQL. Nul ne sera surpris du classement des frameworks de développement Web, avec un duo Node.js, React dans cet ordre au classement général ou inversé chez les Pro, suivis de jQuery, Express et Angular. Les étudiants plébiscitent Next.js qui est passé de la 11e à la sixième place en un an. Du côté des librairies de programmation, les professionnels placent .NET 5, et plus en tête, devant les librairies Python NumPy et Pandas, bien poussées par les étudiants.

Pas de surprise chez les fournisseurs de Cloud. Les votes des développeurs collent aux parts de marché, avec AWS devant Microsoft Azure et Google Cloud. Derrière, Firebase devance Cloudflare, DigitalOcean et Heroku. Les « frenchies » OVH et Scaleway pointent en 14e et 22e place seulement avec, respectivement, 3,42 % et 0,9 % de citations...

Côté outillage, Visual Studio écrase le classement avec 73,71 % des citations pour sa version Open Source Visual Studio Code, et 28,43 % pour le Visual Studio classique. IntelliJ IDEA pointe en troisième position, devant Notepad++, Vim, Android Studio et PyCharm.

Jira pointe en tête des outils collaboratifs avec plus de 52 % des réponses, devant Confluence, Markdown File, Trello, Notion et GitHub Discussions, l'outil numéro 1 des étudiants. Pour les outils de communication synchrone, le classement est serré : Microsoft Teams obtient 51,71 % des mentions, Slack 47,59 %, Zoom 45,25 % tandis que Discord apparaît en 4e position grâce au vote massif des étudiants qui l'utilisent à 68,12 %...

Interrogés sur leurs outils d'IA, ChatGPT arrive en tête des outils de recherche avec plus de 83 % des répondants, devant Bing AI à un peu plus de 20 %, puis Wolfram|Alpha et Google Bard AI. En tant qu'aide au développement, GitHub Copilot est citée par 54,77 % des développeurs, puis viennent Tabnine et AWS CodeWhisperer.

Mais quelles technologies aiment vraiment les développeurs ?

Cet état des lieux répertorie les outils mis en œuvre au quotidien ou appris par les développeurs lors de leur cursus, mais ceux-ci en sont-ils vraiment fans ? Quand on leur demande leurs avis, les classements ne sont pas totalement chamboulés, mais on observe quelques écarts. Ainsi, JavaScript reste le langage le plus désiré (40,15 % des mentions), mais il est loin d'être le plus admiré. Même SQL fait mieux… Le langage le plus admiré est Rust avec 84,66 % des suffrages alors qu'il n'est désiré que par 30,56 % des répondants.

Pour Java, on se rend compte que seulement 44,11 % des développeurs admirent encore le langage qui a révolutionné l'informatique de la fin des années 90, mais c'est MATLAB qui est le langage le plus honni des développeurs, une courte tête devant Cobol, c'est dire !

Côté base de données, pas de surprise, PostgreSQL, MySQL, MongoDB et Redis dominent le classement, mais quelques bases de données relativement confidentielles ont la cote : Datomic, TiDB, DuckDB, RavenDB et Supabase.

Les services Cloud AWS, Azure, Google Cloud et Cloudflare sont les plus désirés, mais en termes d'admiration, il y a quelques surprises. Hetzner et Vercel sont les services les plus admirés et désirés des développeurs ! Le mauvais classement d'OVH (17e) et de Scaleway (22e) s'explique sans doute par leur faible présence commerciale à l'étranger, alors que leurs services obtiennent de bons scores en termes d'admiration.

React, Node.js et Next.js sont les frameworks Web les plus populaires, alors qu'Angular.js ne compte que très peu de supporters. Sur client lourd, .NET 5 et ses versions ultérieures caracolent en tête, devant NumPy, mais aussi des frameworks d'IA type TensorFlow et Torch/PyTorch.

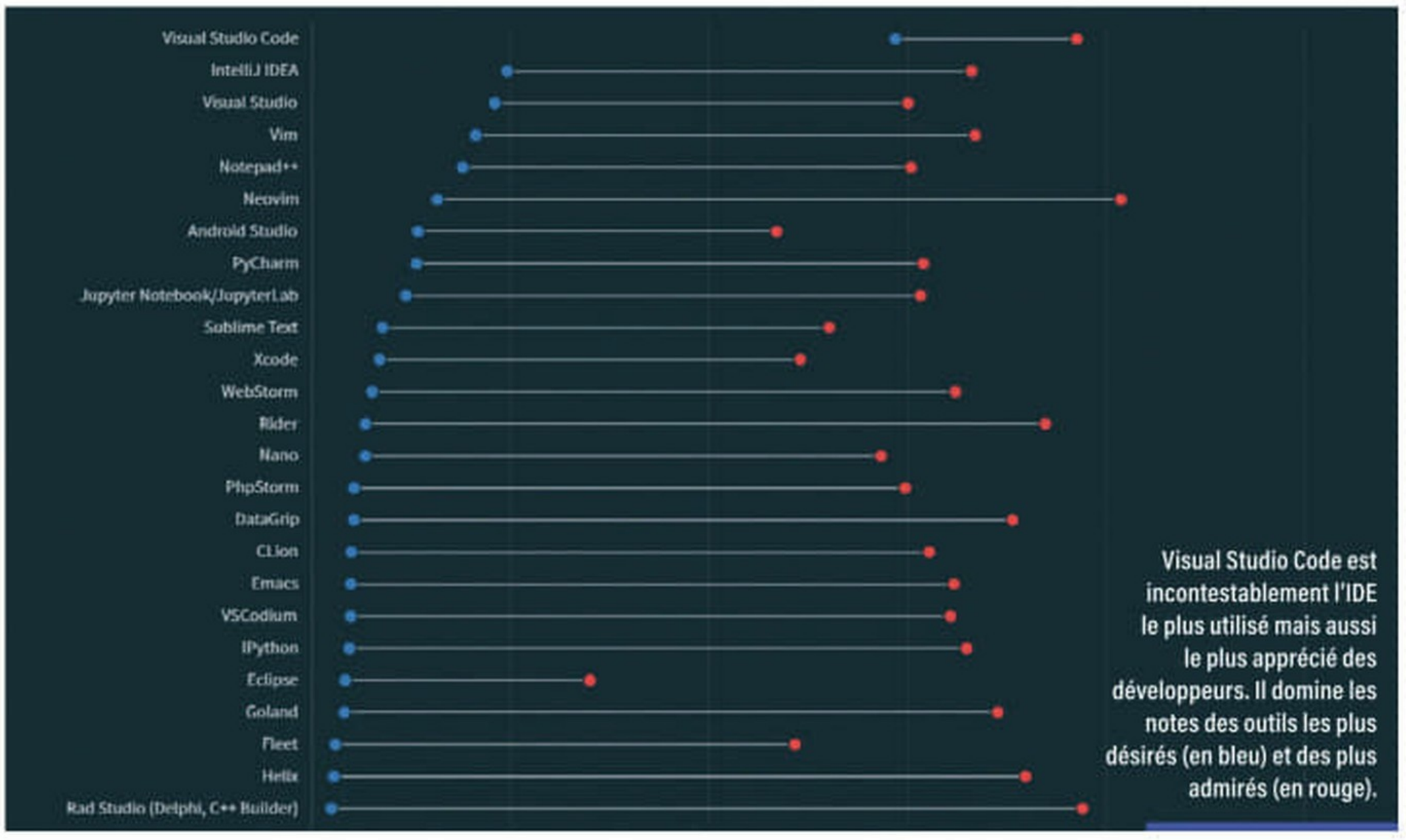
Si Jira est l'outil collaboratif n°1 des développeurs, ces derniers ne semblent pas des inconditionnels de Teams pour les communications temps réel. Face à cette plateforme « corporate », ceux-ci plébiscitent Slack et Discord…

Les technologies vues… du bulletin de salaire

L'enquête Stack Overflow comporte un volet particulièrement intéressant sur la rémunération des développeurs. Managers, développeurs seniors, SRE et les gens proches du marketing touchent les plus gros salaires, mais une autre grille de lecture est de croiser les données de salaires avec les technologies mises en œuvre. Surprise : la technologie qui rapporte le plus, c'est le langage Zig ! Le salaire moyen du développeur Zig atteint 103 611 $ par an… une moyenne calculée sur 259 réponses. Donc si vous voyez passer une annonce recherchant un développeur Zig, ne passez pas à côté ! Clojure qui était la compétence la mieux payée en 2022 a vu le salaire moyen baisser de 10 % cette année. De même, les adeptes de Crystal, Fortran, Erlang et Julia ne peuvent que constater la chute des rémunérations dans leur domaine.

Ces chiffres issus de données déclaratives non vérifiables sont bien évidemment à prendre avec des pincettes, ils servent à donner un éclairage sur les technologies choisies par les entreprises, indépendamment des parts de marché des éditeurs. □

AC



Visual Studio Code est incontestablement l'IDE le plus utilisé mais aussi le plus apprécié des développeurs. Il domine les notes des outils les plus désirés (en bleu) et des plus admirés (en rouge).

Événement

Durcir la défense contre les cyberattaques

À l'occasion de mWISE 2023 qui s'est tenu à Washington DC du 18 au 20 septembre, Mandiant (Google Cloud) a présenté plusieurs mises à jour pour sa plateforme Chronicle Security Operations, et toute l'importance d'évaluer stratégiquement la surface d'attaque, de hiérarchiser les vulnérabilités en fonction de leur probabilité d'exploitation et de déployer l'automatisation. On notera aussi que l'intelligence artificielle générative vient également en support pour améliorer la productivité.

Au cœur de Washington DC, la conférence a mis en exergue toutes les problématiques liées à la cybersécurité. Un sujet véritablement d'actualité avec tout ce qui s'est passé ces dernières semaines aux États-Unis, et particulièrement à Las Vegas où les groupes MGM et Caesars Entertainment ont été visés par des cyberattaques. En raison de ces attaques, le groupe MGM aurait perdu entre 4 et 8 millions de dollars par jour. Ce n'est pas tout puisque les risques venant de Chine et de Corée du Nord ont aussi été largement évoqués durant mWISE. *« La Chine a beaucoup évolué dans ses campagnes de cyberattaques. Au tout début, les attaques étaient très basiques. Mais aujourd'hui, elles sont très sophistiquées avec un comportement de la Chine plus agressif »*, a souligné Sandra Joyce, vice-présidente de Mandiant Intelligence, Google Cloud. Bref, la cybersécurité est devenue un élément majeur du développement et du bon fonctionnement des entreprises.



Directeur général de Mandiant, Kevin Mandia a profité de son keynote pour revenir sur l'importance de la sécurité face à l'accroissement des cyberattaques, venant notamment de Chine et de Corée du Nord.

Des mises à jour pour renforcer la sécurité

Durant la conférence, plusieurs nouveautés, dont les dernières mises à jour de Chronicle Security Operations, ont été annoncées. Cette plateforme unifie notamment les solutions SOAR (Security Orchestration, Automation and Response) et SIEM (gestion des informations et des événements de sécurité) avec la technologie de gestion de Mandiant. *« Ces mises à jour offrent une application plus robuste du renseignement sur les menaces pour aider les défenseurs à prendre de l'avance sur les plus récentes »*, explique l'entreprise américaine. Autre annonce : la solution Mandiant Attack Surface Management (ASM). Il s'agit-là d'une approche de la sécurité qui permet aux équipes dédiées d'évaluer stratégiquement la surface d'attaque, de hiérarchiser les vulnérabilités en fonction de leur probabilité d'exploitation et de déployer l'automatisation pour consacrer plus de temps aux tâches à forte valeur ajoutée, telles que l'investigation et la réponse aux incidents.

Détecter de manière proactive

Avec Chronicle Security Operations, une suite cloud native, les équipes de sécurité peuvent mieux détecter les cybermenaces, enquêter et surtout y répondre grâce aux informations, à la vitesse et à l'évolutivité de Google. *« Nous sommes conscients du fait que, pour garder une longueur d'avance sur les menaces, les entreprises doivent aller au-delà de la simple collecte de données, car les équipes de sécurité peuvent mettre beaucoup trop de temps à trouver ce qui est vraiment pertinent, ou elles sont confrontées à des lacunes dans les informations disponibles pour la recherche et l'analyse »*, ont expliqué les équipes de Mandiant et Google Cloud durant mWISE. Avec Chronicle SIEM et Chronicle SOAR, le géant américain assure fournir un contexte riche et un basculement facile entre les alertes, les cas, les enquêtes et les playbooks dans une seule console. L'objectif est d'apporter aux utilisateurs une solution rationnelle et intégrée pour la détection des menaces et la réponse aux incidents (TDIR en anglais). *« Désormais, chaque alerte repérée par Chronicle sera regroupée dans un cas pour consolider les alertes liées et fournir un accès à l'enrichissement pour aider les équipes de sécurité à prendre des décisions plus rapides »*, indique Google Cloud.



Durant mWISE 2023, plusieurs partenaires de Mandiant ont présenté des solutions pour prévenir les menaces des cyberattaques.

Faire face aux menaces modernes

Face aux nouvelles menaces, Mandiant Google Cloud a ajouté des capacités plus puissantes et des résultats basés sur les risques à Chronicle Security Operations. L'idée est de permettre aux équipes de sécurité des entreprises d'être plus proactives et d'être à même d'anticiper les menaces potentielles. Baptisée Applied Threat Intelligence, cette nouvelle implémentation, disponible en avant-première, vient tirer parti de l'évolutivité de Chronicle pour enrichir et contextualiser automatiquement chaque événement avec les dernières informations sur les menaces provenant de Google Cloud, Mandiant et VirusTotal. Applied Threat Intelligence utilise l'intelligence artificielle ainsi que le machine learning (ML) afin de hiérarchiser les menaces en fonction de l'environnement de chaque client. Selon Mandiant, cet outil va aider les équipes de sécurité à se concentrer sur le traitement des menaces les plus critiques. On notera aussi que chaque événement pertinent qui correspond à un indicateur de menace sera instantanément enrichi avec des associations de cybercriminels, de campagnes de menaces ou de familles de logiciels malveillants qui peuvent être utilisées pour des recherches ou des détections personnalisées. Mandiant Google Cloud a aussi travaillé sur les brèches de façon à ce qu'elles puissent immédiatement être visualisées sur la console Chronicle. Cette fonction analyse en permanence les données des clients et les informe rapidement des nouvelles techniques d'attaque repérées par Mandiant.

Quand l'IA améliore la productivité

S'appuyant sur les innovations de Google en matière d'intelligence artificielle générative (Duet AI) et de modèles de base spécifiques à la sécurité, Chronicle Security Operations facilite la détection, l'investigation et la réponse aux menaces. Cela vient également réduire la charge de travail et augmenter l'efficacité des entreprises dans la défense de leurs infrastructures et de leurs actifs numériques (les datas). Chronicle fournit désormais automatiquement un résumé clair de ce qui se passe, donne un contexte et des conseils sur les menaces importantes et propose des recommandations sur la manière de réagir. Duet AI est également à l'origine de la nouvelle recherche en langage naturel de Chronicle. Les équipes de sécurité peuvent ainsi saisir des questions en langage naturel, et Chronicle générera la requête à partir de leur information, présentera une syntaxe entièrement cartographiée pour la recherche, et permettra d'affiner et d'itérer rapidement sur les résultats.

Concernant Mandiant Attack Surface Management (ASM), désormais disponible pour tous les clients Chronicle, la solution permet aux clients d'identifier et de valider en permanence les points d'entrée exploitables dans leurs entreprises. En effet, les zones d'attaque des sociétés sont de plus en plus étendues. Avec les nouvelles fonctionnalités de Mandiant ASM, notamment les flux de travail, les responsables de la sécurité peuvent aisément évaluer les résultats de la surface d'attaque en spécifiant le type d'activités d'analyse effectuées en fonction du résultat qu'ils souhaitent obtenir. On peut citer l'identification des actifs et vulnérabilités inconnus, évaluer le niveau de sécurité externe des filiales, des partenaires et des fournisseurs de la chaîne d'approvisionnement ou encore d'identifier les violations de l'identité d'une marque ou l'utilisation non authentifiée de la marque. Selon Mandiant, cette nouvelle approche simplifie efficacement l'analyse et l'action sur les risques externes. □

Michel Chotard

Dreamforce 2023

L'événement IA de l'année

La plupart des débats se concentrent sur l'intelligence artificielle qu'elle soit prédictive ou générative. Elle est désormais la pierre angulaire de la plateforme de Salesforce et l'éditeur revendique que cette édition est l'événement le plus important de l'année dans le domaine de l'intelligence artificielle.

L'IA est omniprésente à Dreamforce 2023. Marc Benioff en a fait le fil rouge de son intervention lors de la session générale d'ouverture. Plus de 70 sessions techniques ou business sont consacrées au sujet avec une session dédiée et 20 workshops sont là pour apporter les moyens de l'utiliser sur la plate-forme de Salesforce. Une étude à l'appui, Salesforce veut démontrer l'importance que prend l'intelligence artificielle. Selon celle-ci, 85 % des responsables informatiques français s'attendent à ce que l'IA générative joue un rôle important dans leur entreprise et, à 77 %, ils pensent que son rôle est bien défini dans leur organisation. Ils sont cependant 61 % à s'inquiéter de l'aspect éthique de son utilisation. Marc Benioff a d'ailleurs fait de la confiance une des valeurs fondamentales de l'intelligence artificielle sur la plateforme de Salesforce. Il a rappelé que si 51 % des dirigeants d'entreprises (CEO) voyaient dans l'IA leur priorité numéro 1, 52 % des consommateurs s'inquiétaient de la sécurité et de l'innocuité de cette technologie. Biais, toxicité dans son utilisation, captation des données, ilots de données dans les entreprises, hallucinations des résultats étaient les principaux sujets d'inquiétude.

Einstein 1

La nouvelle plateforme Einstein 1 s'intègre avec la nouvelle CDP de Salesforce Einstein 1 Data Cloud. Elle infuse l'intelligence artificielle dans l'ensemble des applications de Salesforce. L'ensemble s'appuie sur le réseau de métadonnées qui sous-tend la plateforme de l'éditeur. Elle vise à permettre aux clients de connecter l'ensemble de leurs données aux applications gonflées à l'intelligence artificielle par des outils low code pour fournir des expériences clients nouvelles. Le réseau de métadonnées aide les entreprises à unifier et à comprendre les données en fournissant l'équivalent d'un langage commun afin de permettre aux applications de dialoguer entre elles. Les métadonnées décrivant la structure, les modèles d'IA, les relations et les comportements des données au sein du système peuvent mieux comprendre le contexte des interactions clients, les processus métier et les résultats de certaines interactions. Ces informations peuvent ensuite être utilisées pour perfectionner de grands modèles de langage afin qu'ils s'améliorent au fil du temps.

LES DISPONIBILITÉS DES DIFFÉRENTES ANNONCES DE DREAMFORCE 2023

- Einstein 1 Platform
  - Einstein 1 Data Cloud
  - Einstein 1 Copilot
  - Einstein 1 Sales
    - Copilot for Sales Pilot : Q1 24
    - Automated Prospecting : Q2 24
    - Sales GPT : disponible
    - Einstein Forecasting : disponible
  - Einstein 1 Service
    - Copilot for Service Pilot : Q1 24
    - Field Service Revenue Generation : GA Q1 24
    - Service Intelligence : GA Q4 23
    - Service & Field Service GPT : disponible
  - Einstein 1 Marketing
    - Segment Intelligence : GA Q4 23
    - Marketing GTP : GA Q4 23
    - Typeface Partnership : GA Q4 23
    - Personalization Real Time Event stream : GA Q4 23
  - Einstein 1 Commerce
    - Copilot for Commerce Pilot : Q3 23
    - Commerce Intelligence Pilot : Q3 23
    - Commerce GPT : disponible
  - Einstein 1 Platform Services
    - Prompt Builder : GA Q1 24
    - Einstein for Developers Open Beta : disponible
    - Salesforce Backup : disponible
  - Einstein 1 Tableau
    - Tableau Pulse GA : Q4 23
    - Copilot for Tableau GA : Q2 24
    - Intelligents App : disponible
  - Einstein 1 Canvas (Quip)
    - Canvas Custom Templates : H2 24
    - Canvas API & Analytics : H2 24
    - Workflows in Canvas : disponible
  - Einstein 1 Mulesoft
    - Einstein for Anypoint Code Builder : H1 24
    - Intelligent document processing : H1 24
    - Accelerators for Data Cloud : disponible
  - Einstein 1 Industries
- Life Sciences Cloud : GA Q2 24
- Éducation Skills Generator Pilot : Q2 24
- Personalized Finance with planning : GA Q2 24
- Consumer Goods Einstein Pilot : Q4 24

Une intégration profonde avec Data Cloud

Data Cloud, le moteur de données hyperscale en temps réel de Salesforce, unifie et harmonise les données clients structurées ou non afin d'offrir une vue unique dans ce framework de métadonnées. Avec cette intégration native, Einstein 1 Platform prend désormais en charge plusieurs milliers d'objets dotés de métadonnées par client, chacune pouvant contenir plusieurs milliards de lignes. En outre, les plateformes Marketing Cloud et Commerce Cloud ont été remaniées au sein d'Einstein 1 Platform. De gigantesques volumes de données sont en mesure d'être intégrés à Einstein 1 Platform à partir d'autres systèmes et rendus immédiatement disponibles en tant qu'objets Salesforce exploitables. Des flux peuvent être déclenchés à la suite de n'importe quel changement sur n'importe quel objet à grande échelle. En outre, la plateforme peut interagir avec n'importe quel système dans l'entreprise, systèmes existants inclus, via MuleSoft. De plus, Salesforce offre une variété de solutions d'extraction de connaissances et analytiques pour divers cas d'usage : Reports et Dashboards, Tableau, CRM Analytics et Marketing Cloud Reports. Grâce au schéma commun et au modèle d'accès aux métadonnées d'Einstein 1 Platform, toutes ces solutions fonctionnent sur les mêmes données.



Marc Benioff et Sam Altman, CEO d'OpenAI, lors d'un entretien sur scène à Dreamforce.

Un assistant conversationnel dopé à l'IA

Copilot est intégré en natif à chaque application Salesforce et accompagne l'utilisateur dans ses requêtes en langage naturel et lui répond de la même manière en utilisant les données propriétaires et sécurisées issues de Data Cloud. Il est capable de recommander par exemple un plan d'action à la suite d'un appel commercial, en vérifiant le statut de la commande d'un consommateur, ou est en mesure de mettre à jour la date d'expédition. Copilot Studio vise à aider les utilisateurs à créer des prompts métiers et des procédures automatiques s'appuyant sur un ensemble de compétences. Einstein Copilot et Einstein Copilot Studio reposent sur Einstein Trust Layer, une architecture d'IA sécurisée intégrée nativement à Einstein 1 Platform. Les équipes bénéficient ainsi de la puissance d'une IA générative, tout en respectant les normes de confidentialité et de sécurité des données de leur entreprise. □

B.G



Snowflake Summit 2023

Snowflake déroule le tapis rouge aux développeurs

Pour éviter la mésaventure d'Hadoop qui n'a jamais réellement réussi à réunir assez de développeurs pour créer des applications sur sa plate-forme, Snowflake fait tout pour simplifier la vie des développeurs pour qu'ils créent des applications sur son data cloud.

La première annonce de cette édition 2023 a été la disponibilité de Snowflake Native App Framework. Les Snowflake Native Apps fournissent aux développeurs les outils nécessaires pour créer rapidement des applications grâce à la haute disponibilité et à l'auto-scalabilité de Snowflake. Elles les aident également à éliminer les obstacles liés à la sécurité et à la confidentialité pour les clients car les applications fonctionnent directement dans leurs comptes Snowflake. Le Snowflake Native App Framework offre aux fournisseurs de Snowflake Native Apps les éléments de base nécessaires pour développer plus rapidement, déployer plus facilement et opérer plus efficacement. Grâce à la facturation personnalisée des événements et à la monétisation sur la plateforme via la Snowflake Marketplace, les entreprises peuvent distribuer et monétiser leurs applications de manière transparente sans avoir à mettre en place des systèmes de facturation.



Le CEO de Snowflake et celui de NVidia lors de l'annonce de l'extension du partenariat entre les deux entreprises.

Plus de 25 organisations ont déjà publié des applications natives Snowflake disponibles dès aujourd'hui sur la Snowflake Marketplace et plus d'une centaine de fournisseurs développent actuellement des applications couvrant de multiples industries et cas d'utilisation. Parmi les organisations qui créent des applications natives Snowflake, on peut citer la Depository Trust & Clearing Corporation (DTCC).

L'extension de Snowpark

Snowpark continue d'assurer le déploiement et le traitement sécurisés du code non SQL de Snowflake avec divers runtimes et bibliothèques, élargissant ainsi les possibilités de construction et le champ d'application du Data Cloud. Il permet aux créateurs de travailler plus efficacement avec les données dans les langages de programmation et les outils de leur choix, tout en offrant aux entreprises les garanties d'automatisation, de gouvernance et de sécurité qui font défaut aux datalakes et aux environnements big data existants.

Avec le lancement de Snowpark Container Services, Snowflake élargit la portée de Snowpark afin que les développeurs puissent débloquer des options d'infrastructure plus larges. Par exemple, l'accélération du calcul avec les GPU NVIDIA et les logiciels d'IA pour exécuter davantage de charges de travail au sein de la plateforme sécurisée et gouvernée de Snowflake sans complexité, y compris une gamme plus large de modèles d'IA et de Machine Learning, d'API, d'applications développées en interne, et plus encore. Grâce à Snowpark Container Services, les clients de Snowflake ont également accès à un vaste catalogue de logiciels et d'applications tiers, notamment des grands modèles de langage (LLM), des Notebooks, des outils MLOps... Les clients peuvent utiliser les ordinateurs portables Hex pour l'analyse et la Data Science et aussi les plateformes d'IA et les fonctions de Machine Learning d'Alteryx, Dataiku et SAS pour exécuter des traitements d'IA et de ML plus avancés. Ils peuvent également gérer ces flux de données avec la plateforme d'Astronomer basée sur Apache Airflow, le tout entièrement au sein de Snowflake. Il ne s'agit là que de quelques exemples, car Amplitude, CARTO, H2O.ai, Kumo AI, Pinecone, RelationalAI, Weights & Biases et bien d'autres proposent également leurs produits et services avec Snowpark Container Services. NVIDIA et Snowflake construisent des intégrations

logicielles et informatiques accélérées transformatrices pour Snowpark Container Services. Cette collaboration apporte également NVIDIA AI Enterprise, le pilier logiciel de la plateforme NVIDIA AI, à Snowpark Container Services, ainsi que la prise en charge du calcul accéléré de NVIDIA.

Un référentiel unifié

Snowflake annonce le nouveau Snowpark Model Registry, un référentiel unifié pour les modèles d'apprentissage automatique des entreprises. Le registre permet aux utilisateurs de centraliser la publication et la découverte des modèles, rationalisant ainsi la collaboration entre les scientifiques des données et les ingénieurs ML afin de déployer les modèles en production de manière transparente.

Snowflake fait également progresser l'intégration de Streamlit dans Snowflake, permettant aux data scientists et autres développeurs Python d'accroître l'impact de leur travail en créant des applications qui comblent le fossé entre les données et l'action de l'entreprise. Avec Streamlit dans Snowflake, les créateurs peuvent utiliser Python pour développer leurs applications, transformant une idée en une application prête pour l'entreprise avec seulement quelques lignes de code, puis déployer et partager rapidement ces applications en toute sécurité dans le Data Cloud.

Un développement simplifié

Snowflake rend le développement au sein de sa plateforme unifiée plus facile et plus familier grâce à de nouvelles fonctionnalités, notamment l'intégration native de Git pour soutenir des flux de travail CI/CD transparents, et l'interface native en ligne de commande (CLI) pour un développement et des tests optimisés au sein de Snowflake.

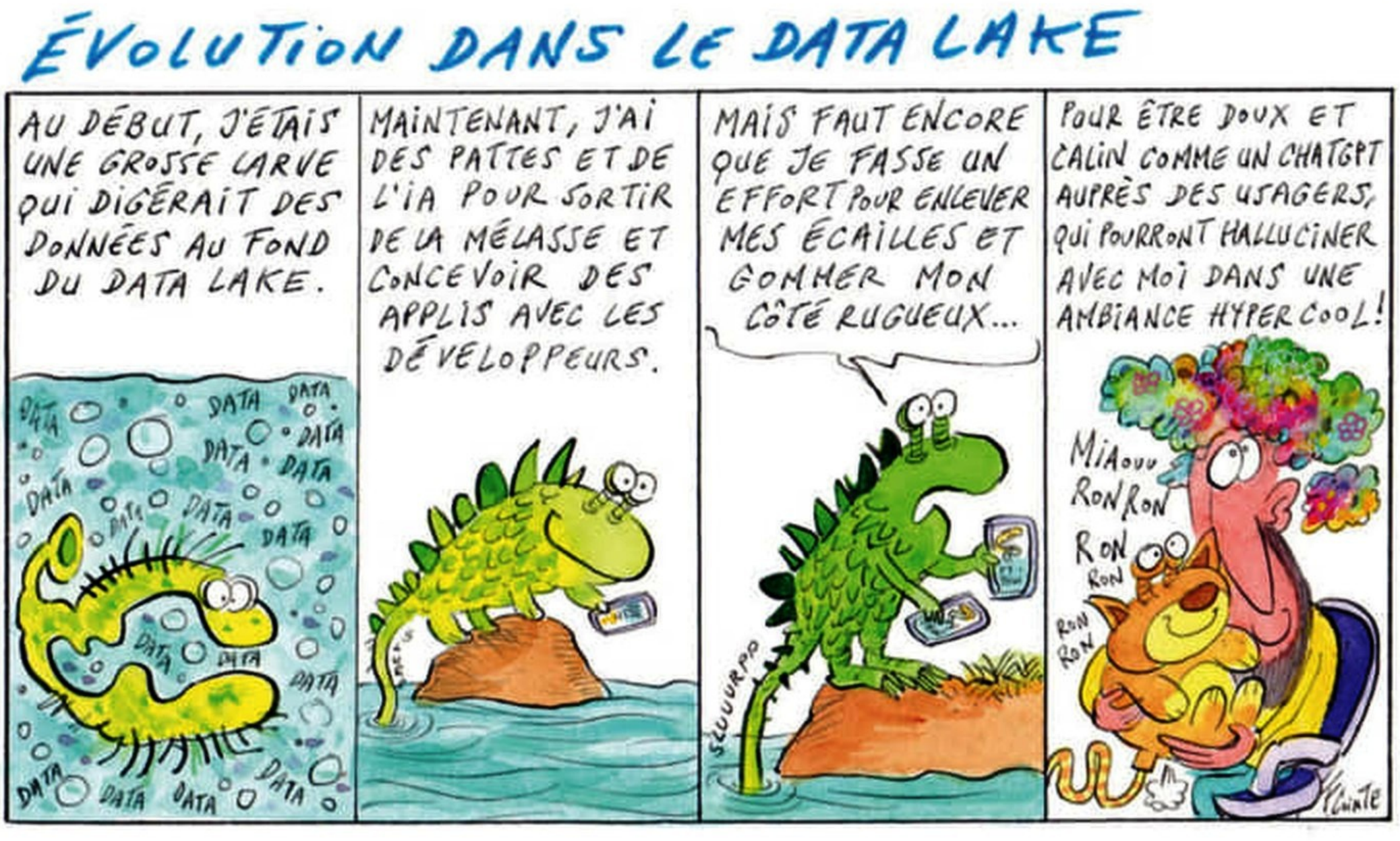
Un nouveau modèle LLM

Snowflake lance Document AI, un nouveau grand modèle de langage (LLM) construit à partir de la technologie d'IA générative pionnière d'Applica. Snowflake annonce également des mises à jour d'Iceberg Tables. Ceci permet d'éliminer davantage les silos de données et offre aux organisations la possibilité d'utiliser des formats Open Table.

Avec Iceberg Tables, les entreprises peuvent travailler avec les données de leur propre stockage au format Apache Iceberg, que ces données soient gérées par Snowflake ou en externe, tout en bénéficiant de la facilité d'utilisation, des performances et de la gouvernance unifiée de Snowflake. Cela simplifie la gestion des données en éliminant la nécessité pour les organisations de déplacer ou de copier les données entre les systèmes, tout en augmentant la flexibilité et en réduisant les coûts. En outre, l'écosystème croissant d'Apache Iceberg, composé de divers adoptants, contributeurs et offres commerciales, assure la pérennité du stockage, en évitant le verrouillage des fournisseurs et les migrations fréquentes. Des clients comme Booking.com exploitent aujourd'hui les tables Iceberg pour apporter la puissance du Data Cloud à l'ensemble de leurs données.

En intégrant ce modèle LLM dans la plateforme de Snowflake, les entreprises pourront facilement extraire des documents des contenus tels que les montants des factures ou les termes des contrats et affiner les résultats à l'aide d'une interface visuelle et du langage naturel. Il est prévu d'étendre ces capacités à d'autres types de données non structurées. □

B.G





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™

Consentement

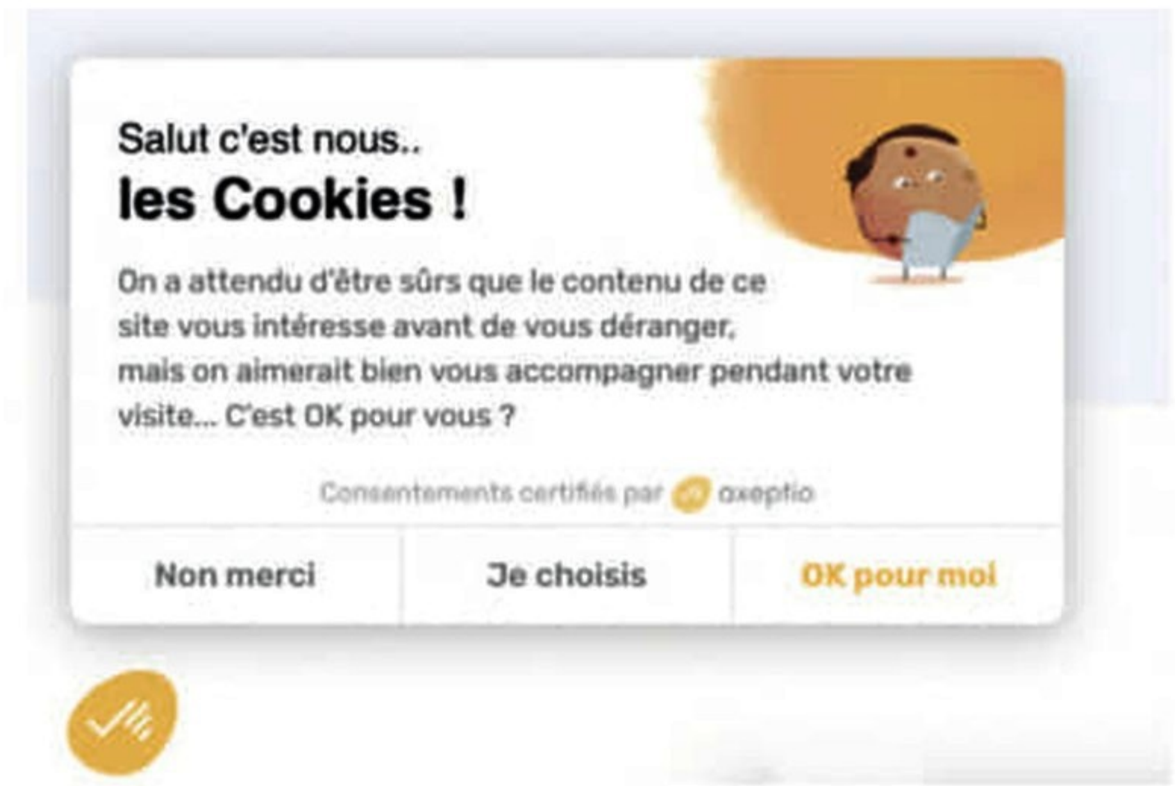
Axeptio se repose sur Snowflake

La start-up spécialisée dans la gestion du consentement sur les sites Web a choisi Snowflake et son Data Cloud pour gérer son activité.

Si vous allez sur des sites comme celui du PMU ou de l'Opéra de Paris, vous avez, sans le savoir, utilisé la plateforme d'Axeptio de gestion du consentement selon vos choix vis-à-vis des informations ou cookies que vous acceptez de partager. La plateforme aide les entreprises à se mettre en conformité pour leurs sites Web ou leurs applications mobiles vis-à-vis des règles de respect des données personnelles. Pour les applications mobiles, Axeptio propose deux SDK sur IOS et Android. Aujourd'hui, la start-up fondée en 2017 a des milliers de sites sous sa plateforme.

Romain Gabilan, Tech Lead chez Axeptio, précise : « *nous gérons 1,8 to de consentement et nous avons environ 5 To de données sur Snowflake. La solution était auparavant sur une base MongoDB, puis les données ont migré sur le datalake de Snowflake. Une partie est là pour analyser l'interaction avec notre Widget, et si tout cela est conforme avec leur outil de tracking pour le consentement préalable. La solution est totalement paramétrable et nous poussons les clients à respecter la symétrie des consentements, soit accepter ou refuser avec des textes paramétrables. Nous ajoutons de plus des outils pour s'assurer de la conformité RGPD* ».

Si tout cela fonctionne bien pour les sites Web, c'est une autre affaire avec les services marketing qui ont besoin des mêmes données de tracking des interactions des utilisateurs, mais sans les demandes de consentement. L'éditeur propose deux types de services distincts qui s'appuient sur la même technologie. Elle fonctionne de manière assez simple avec l'injection d'un script qui ne collecte pas de données personnelles dans le code du site



Un exemple d'écran de présentation du consentement par Axeptio.



Romain Gabilan,
Tech Lead
chez Axeptio.

« La solution est totalement paramétrable et nous poussons les clients à respecter la symétrie des consentements. »

dans la balise <Head> ou mieux dans <body> pour obtenir de meilleures performances si nécessaire. Suivant les sites, Axeptio a d'ailleurs différentes manières de s'installer, mais reste toujours aussi simple d'accès.

Un besoin pour l'analytique

Le recours à Snowflake s'est fait il y a un peu plus d'un an avec un biais sur la requête serveur pour injecter le code dans le navigateur, ce qui faisait que la requête n'était pas loggée et qu'il était impossible de facturer le client. La facturation se réalise au nombre de pages vues selon différentes formules qui vont d'une offre d'essai gratuite à une offre payable mensuellement à un peu plus de 89 € pour 6 millions de pages vues ou plus par an. Pour remédier au problème, l'éditeur a décidé d'envoyer des événements dans sa solution, ce qui génère de très gros volumes. L'éditeur a alors décidé de migrer vers Snowflake pour traiter les données et obtenir une facturation au plus juste avec des rapports indiquant les appels au widget, le nombre de pages vues et les chargements du widget. Romain Gabilan ajoute : « *nous n'avions pas une agrégation aussi poussée que maintenant* ». Le projet s'est fait dans le cadre du programme « Powered by Snowflake » qui donne à des start-ups les moyens de construire et de faire croître des solutions utilisant des larges volumes de données. De plus, une bifurcation directe vers AWS S3 devrait être annoncée rapidement. □

B.G

PCA

Keolis Métropole Orléans simplifie son système d'information avec Nutanix

Keolis Métropole Orléans, opérateur du réseau TAO de la Métropole orléanaise, a fait le choix des solutions de Nutanix afin de renouveler son infrastructure pour garantir la fiabilité et la sécurité des services offerts aux voyageurs.

Avec Nutanix, Keolis Métropole Orléans a gagné en simplicité d'administration et s'est libéré des tâches chronophages en permettant aux collaborateurs d'avoir plus de temps à consacrer à la valeur métier. Les migrations et les mises à jour se font désormais sans interruption de service en plus d'obtenir des économies significatives sur les licences, 50 % sur la consommation énergétique et l'espace occupé dans le datacenter a gagné 35 %. De plus, la sécurité de l'opérateur de transports publics se retrouve renforcée et n'a connu aucun dysfonctionnement en deux ans. Finalement, le DSI a énormément gagné en simplicité sur la gestion de son PCA.

Un SI d'importance

L'ensemble du système d'information de l'opérateur de transport est composé d'une centaine de VM et est relié par un réseau de 40 kilomètres en fibre noire à des milliers d'équipements et une centaine de sites répartis sur l'agglomération. Keolis Métropole Orléans gère au total plus de 2 000 adresses IP. La moindre latence ou défaillance du système d'informations peut provoquer de graves dysfonctionnements du réseau de transport de la Métropole. La société souhaitait renouveler son infrastructure hébergeant des systèmes critiques pour gagner en fiabilité, flexibilité, scalabilité et surtout simplicité.



Un bus de la TAO.

Un choix après des tests

Le choix d'une infrastructure hyper convergente s'est imposé après des tests de plusieurs solutions du marché. Aujourd'hui, le SI est opéré sur 13 nœuds Nutanix, dont 8 redondés dans les deux datacenters de Keolis Métropole Orléans. La société a profité de la migration pour abandonner l'hyperviseur existant au profit de AHV pour des raisons économiques et de simplicité.

Les critères de choix

Nutanix s'est distingué par sa facilité de mise en œuvre, la convivialité des interfaces et les nombreuses fonctionnalités qui font gagner un temps précieux, selon un des cadres de la filiale de Keolis. □

B.G

KEOLIS MÉTROPOLE ORLÉANS EN BREF

Filiale de l'opérateur de transports publics Keolis présent dans 15 pays à travers le monde, Keolis Métropole Orléans exploite le réseau TAO (Transports de l'Agglomération Orléanaise) pour le compte de la Métropole depuis 2019, date à laquelle elle a remporté le contrat de délégation de service public (DSP) pour six ans. Le réseau TAO est composé à 60 % d'applications métier (Billettique, SAEIV, etc.) et à 40 % d'applications de gestion classiques (RH, comptabilité, etc.) appartenant à l'opérateur. La société accompagne chaque jour 125 000 voyageurs dans 22 communes. Elle emploie près de 750 collaborateurs, dont 500 conducteurs de bus et de tramway. Keolis Métropole Orléans opère également le système d'information du réseau TAO.

LES GAINS CONSTATÉS

En plus d'obtenir des économies significatives sur les licences, Keolis Métropole Orléans a réduit de 50 % la consommation énergétique et l'espace occupé dans le datacenter a gagné 35 %. De plus, la sécurité de l'opérateur de transports publics se retrouve renforcée.

Chatbot

Cdiscount répond à ses clients avec iAdvize

La filiale du groupe Casino a intégré, depuis juin dernier, l'agent conversationnel d'iAdvize. Pour l'heure cantonné à l'électroménager, le chatbot s'avère, selon Cdiscount, capable de traiter complètement 40 % des conversations et génère plus de 70 % de satisfaction.

Avec le succès de ChatGPT, la plupart des marques regardent de très près à l'intégration de l'intelligence artificielle générative à leurs produits et services. Le monde de l'e-commerce est au premier rang, sur notamment la partie conseil et service client. Chez Cdiscount, on a fait le choix d'iAdvize. L'entreprise nantaise, grande star de l'époque des chatbots, s'est, elle aussi, inévitablement penchée sur les Large Language Models. Pas de développement maison avec des centaines de milliards de paramètres à travailler : pour développer son IA générative, iAdvize s'appuie sur les modèles d'Azure OpenAI Service. C'est le LLM construit par l'éditeur français sur cette base qui a été connecté au catalogue de Cdiscount.

Ainsi, l'agent conversationnel a accès aux informations contenues dans les bases de données produits du e-commerçant qui, conjuguées aux capacités de NLP (Natural Language Processing) et d'interactions du modèle, donnent des réponses fiables à l'internaute. Et ce, en ne basant ses réponses que sur les caractéristiques fournies par la marque. Lors du PoC (Proof of Concept) et pour le moment, l'outil fourni par iAdvize se concentre sur la partie électroménager du catalogue, mais il a vocation à être déployé sur d'autres catégories de produits tels que les téléviseurs, les ordinateurs portables et le mobilier de jardin.

Le chatbot a été déployé en juin 2023, après deux mois de tests. *« Les premiers résultats sont enthousiasmants. En seulement quelques semaines, l'IA est déjà capable de traiter complètement 40 % des conversations et génère plus de 70 % de satisfaction »* souligne Antoine Pierart, Directeur Marketing et Expérience Client chez Cdiscount.



Geppetto, l'agent conversationnel développé par iAdvize et boosté à l'IA générative, s'appuie sur le catalogue de produits de Cdiscount pour répondre aux questions des clients, pour l'heure sur la partie électroménager.

D'autant que l'agent transfère à un conseiller humain dès qu'elle n'a pas la réponse, permettant aux conseillers de se concentrer sur *« des missions à plus forte valeur ajoutée »*.

Chatbot amélioré

Cdiscount cherchait à garantir deux éléments essentiels : la fiabilité des réponses, la protection et la confidentialité des données. iAdvize s'est appuyé sur les services de Microsoft sachant que ceux-ci sont, sur ce périmètre, certifiés (HDS, ISO 27001, ISO 27018, HIPAA BAA...) et que, contrairement à ChatGPT, la version de Microsoft d'Open AI est conçue pour les entreprises : elle n'est pas ouverte au public et assure une meilleure sécurité et confidentialité. En outre, les données sont stockées en Europe pour une durée de 30 jours à des fins de prévention de fraude uniquement. L'entreprise nantaise précise avoir signé avec le géant américain un Data Processing Agreement et avoir réalisé différentes études d'impact sur la protection des données relatives à l'utilisation des intelligences artificielles, pour un maximum de conformité au RGPD.

Avec un taux de satisfaction client trois fois plus élevé que les précédentes générations de chatbot, Cdiscount est particulièrement satisfait de l'expérience. *« Nos deux marques partagent la conviction que le futur de l'e-commerce est conversationnel. Conforme, connectée et contrôlable, notre IA générative permet à Cdiscount d'offrir des expériences conversationnelles de grande qualité, à grande échelle et d'ainsi accélérer ses ventes »*, explique Julien Hervouët, Fondateur et CEO d'iAdvize. □

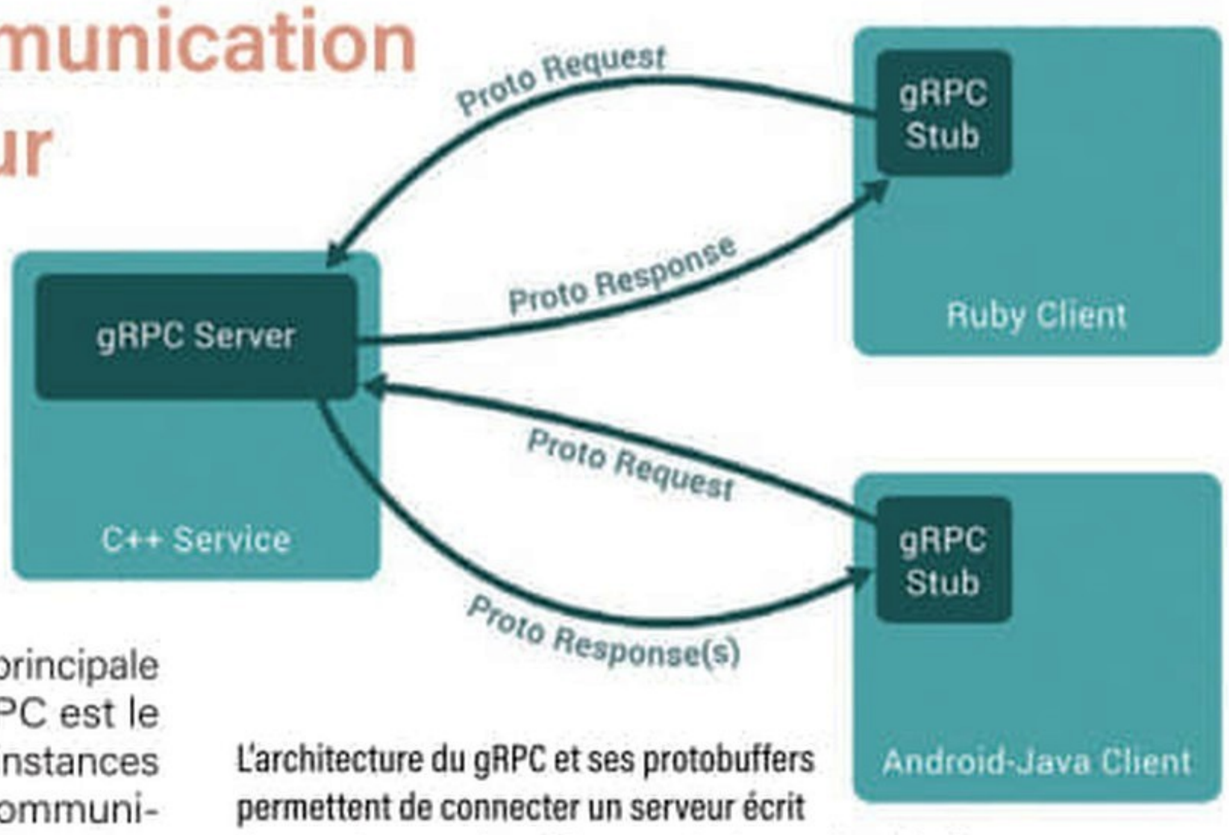
G.P

gRPC

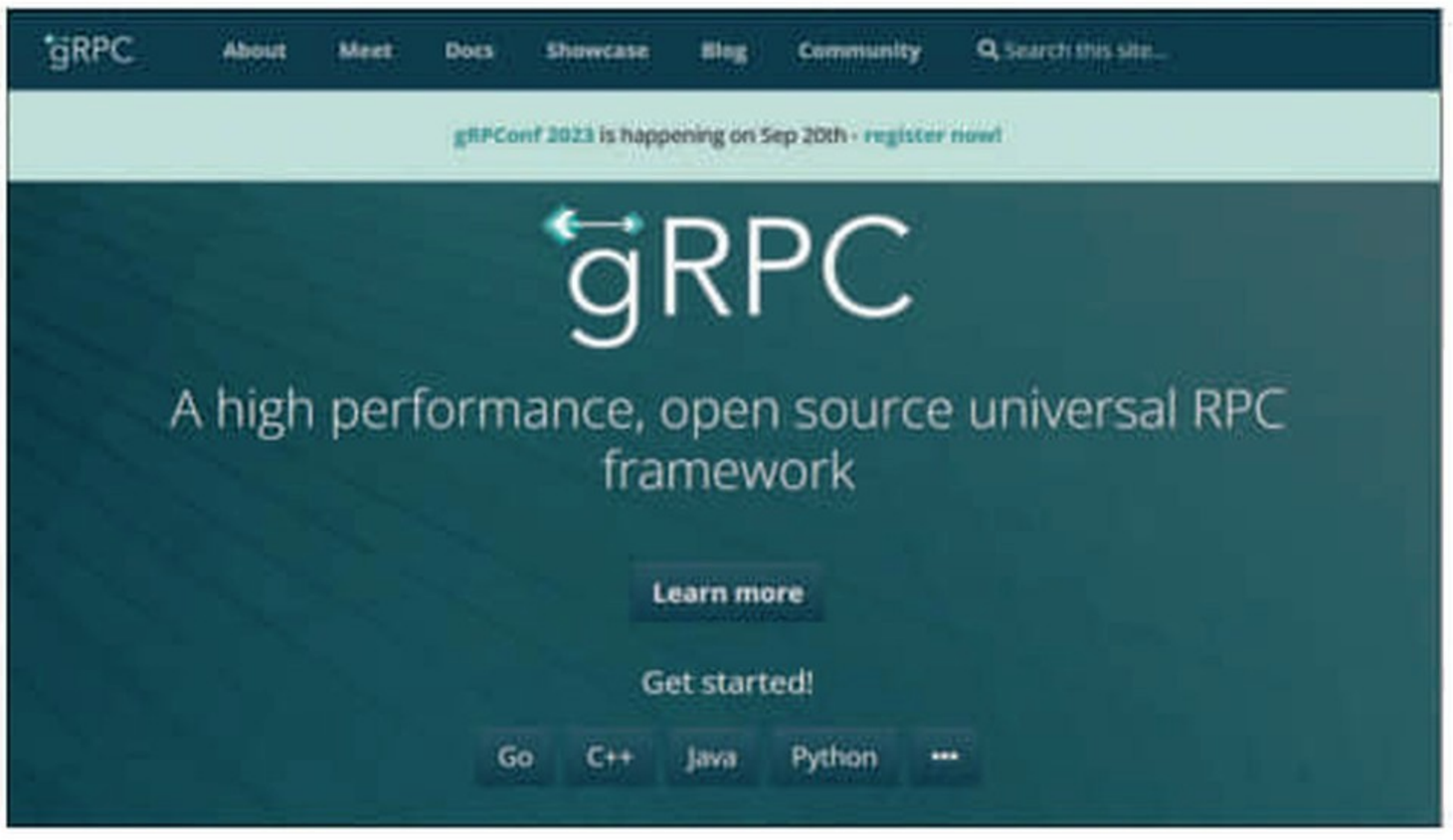
Le protocole de communication client/serveur du futur

gRPC, Kesako ?

Le gRPC est basé sur le « bon vieux » RPC (Remote Procedure Call ou appel de procédure à distance). Il permet une communication particulièrement efficace au sein d'architectures client/serveur distribuées grâce à des technologies assez innovantes. Ce protocole fonctionne au niveau des processus, tout comme le RPC. La caractéristique principale de la communication inter-processus *via* gRPC est le principe de transparence : la relation entre des instances distantes est aussi simple et directe qu'une communication entre plusieurs processus internes d'une même machine. Le gRPC a été initialement conçu en 2015 par Google, d'où le g. Il est open source et c'est désormais la Cloud Native Computing Foundation qui prend en charge sa diffusion et son développement. Le gRPC gère le transport de flux de données entre des ordinateurs distants de manière normalisée en utilisant le protocole HTTP/2. La structuration et le traitement des données sont pris en charge par les Protocol Buffers de Google. Ce sont des fichiers textes contenant du code source et portant l'extension.proto. Ils sont translatés dans le langage de votre choix parmi ceux disponibles (C, C++, C#, Java, Python, ...). Il faut pour cela employer le binaire dédié à cette tâche et adapté à votre plateforme d'exécution, système d'exploitation (Android, Linux, Mac OS, UNIX, Windows, ...) et processeur (motorola arm64, intel x86, amd64, ...). Le gRPC est généralement vu comme un framework. Cela veut dire qu'il met un environnement de programmation à disposition des développeurs, un compilateur (ou plutôt un transpiler) et quelques plugins et bibliothèques diverses. La structure normalisée de gRPC intègre différents éléments et fonctions qui peuvent, pour certains, être utilisés directement sans qu'il ne soit toujours nécessaire de les reprogrammer. Le framework gRPC définit des interfaces normalisées pour des sources définies, comme par exemple des bases de données. Il est capable de connecter efficacement des services dans et entre des datacenters tout en prenant en charge l'authentification, le traçage, la vérification de l'état, et même l'équilibrage de charge. gRPC est, de plus, très intéressant dans le « dernier kilomètre » de l'informatique distribuée, lorsqu'il s'agit de connecter des appareils, des applications mobiles et des navigateurs à des services de type backend.



L'architecture du gRPC et ses protobuffers permettent de connecter un serveur écrit dans un langage donné à un ou plusieurs clients écrits dans n'importe quel autre langage (ou le même).

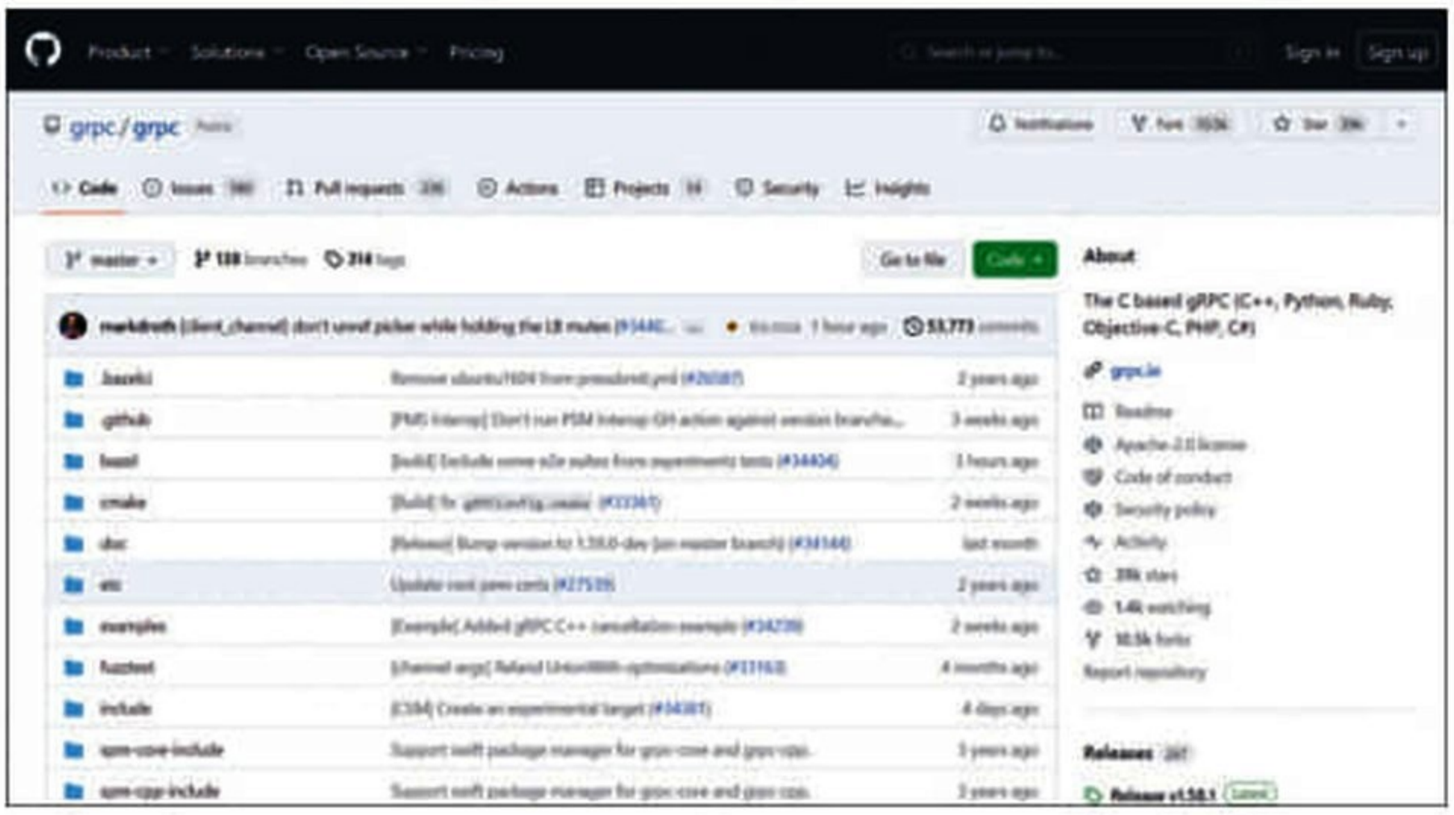


Si vous voulez en savoir plus sur ce formidable protocole de communication, rendez-vous sur le site officiel du gRPC, grpc.io.

Transpilation via les Protocol Buffers

Les Protocol Buffers (Protobuf pour les intimes) ont plusieurs rôles dans le gRPC. Ils offrent un IDL (Interface Definition Language ou langage de description d'interface) permettant de décrire une interface de manière globale avec la syntaxe « proto ». Après traitement par le programme exécutable protoc, ils sont convertis dans le langage de programmation cible de votre choix. Ils permettent de définir les services à utiliser et d'implémenter des fonctions afin de les mettre à

disposition du client et du serveur. Ces fonctions, de manière classique, permettent de spécifier les paramètres à envoyer avec une requête ainsi que la valeur de retour attendue. Les Protocol Buffers servent de langage commun pour définir des services et des messages avec leur structure, leurs types et leurs objets. Ils permettent au(x) client(s) et au(x) serveur(s) de communiquer et d'opérer conjointement, fonctionnellement et aussi efficacement que possible, quelle que soit la distance qui sépare les machines. Une communication gRPC se déroule de la manière suivante, avec par exemple la consultation d'une base de données du type « Recherche d'articles » :



Le code source du gRPC et de nombreuses ressources associées sont disponibles et ouverts à tous sur son dépôt Github à l'adresse https://github.com/grpc/grpc

• Avant de passer à la recherche, des préparatifs sont nécessaires tant côté client que serveur. En se basant sur les Protocol Buffers, les fichiers .proto (qu'il faut bien sûr écrire), il faut en premier lieu implémenter un serveur gRPC et un ou plusieurs services. Ensuite, il faut créer un stub pour le client auteur de la requête, autonome ou intégré à une application. Si le serveur est disponible, l'application client peut appeler la fonction qui l'intéresse *via* le réseau. Elle doit pour cela spécifier l'adresse IP de la machine hébergeant le serveur et le port qu'il utilise pour l'écoute (le socket réseau). L'adresse IP de la machine client doit, quant à elle, être autorisée par l'application serveur. Le port utilisé couramment (port par défaut) pour le protocole gRPC est le 50051.

• La requête est envoyée au serveur.

• Il la réceptionne et la traite avec une interface de service développée à cette fin.

• Le serveur gRPC exécute le traitement (ici une recherche de produits dans une base de données).

• Le serveur envoie la réponse au client qui retransmet cette valeur de retour à l'instance à l'origine de l'appel (ici le nombre d'articles trouvés).

Les applications côté client et côté serveur peuvent être écrites dans différents langages de programmation — une bonne dizaine pour l'instant, et d'autres viendront. Les élus sont, pour le moment, les langages C++, C#, Dart, Go, Java, Kotlin, Node.js, Objective-C, PHP, Python et Ruby. Le langage des Protocol Buffers est le langage commun de définition de la communication attendue. Le binaire protoc permet de créer une interface complète pour les messages et les services dans un des langages disponibles. Il est possible de développer clients et serveurs dans des langages différents, cela ne pose aucun problème particulier, pas même d'adaptation. Si un serveur gRPC est en cours d'exécution et en écoute, il répondra aux clients qui rentreront en interaction avec un des services qu'il propose. Peu importe le langage de programmation utilisé pour développer l'un ou l'autre ou le système d'exploitation sur lequel ces programmes s'exécutent. Tout ce qu'il faut c'est une connexion réseau. Le gRPC fait abstraction de la plupart des obstacles grâce à des interfaces et à ses mécanismes de traduction spéciaux. Il utilise le protocole HTTP/2 qui est intégré à des protocoles réseaux, comme notamment TCP et UDP sur IP. L'échange de flux de données entre machines (requête et réponse) se fait *via* des données binaires compactes générées lors de la sérialisation (Marshalling) typique des RPC. Les flux transmis sont désérialisés (Unmarshalling) pour le traitement complet des structures de données abstraites côté client et côté serveur.

INCONVÉNIENTS

Parmi les points faibles de gRPC, les messages codés avec protobuf ne peuvent pas être lus par des humains. Lors de l'analyse du trafic de données et, notamment, lors de la recherche d'erreurs et des opérations de débogage, cela peut être gênant. D'un autre côté, le format binaire est le prix à payer pour compacter les données et améliorer la vitesse d'exécution. D'autres inconvénients résultent de cette mise en réseau d'architectures client/serveur distribuées, dont principalement la sécurité. Le gRPC interconnecte des ordinateurs à distance, ce qui le rend donc plus vulnérable que des programmes s'exécutant localement. Il dépend fortement de la disponibilité d'un réseau sécurisé. Il ne prend pas non plus en charge la multidiffusion. Les navigateurs modernes ne supportent pas le gRPC à l'heure actuelle. Chez Microsoft, le pari est de favoriser l'adoption du framework Blazor qui, lui, propose un client web compatible avec gRPC. Il faut enfin signaler que gRPC a des limitations en termes de broadcast en temps réel sur un réseau. Un framework comme SignalR sera bien plus approprié dans ce cas de figure.

Le Workflow gRPC

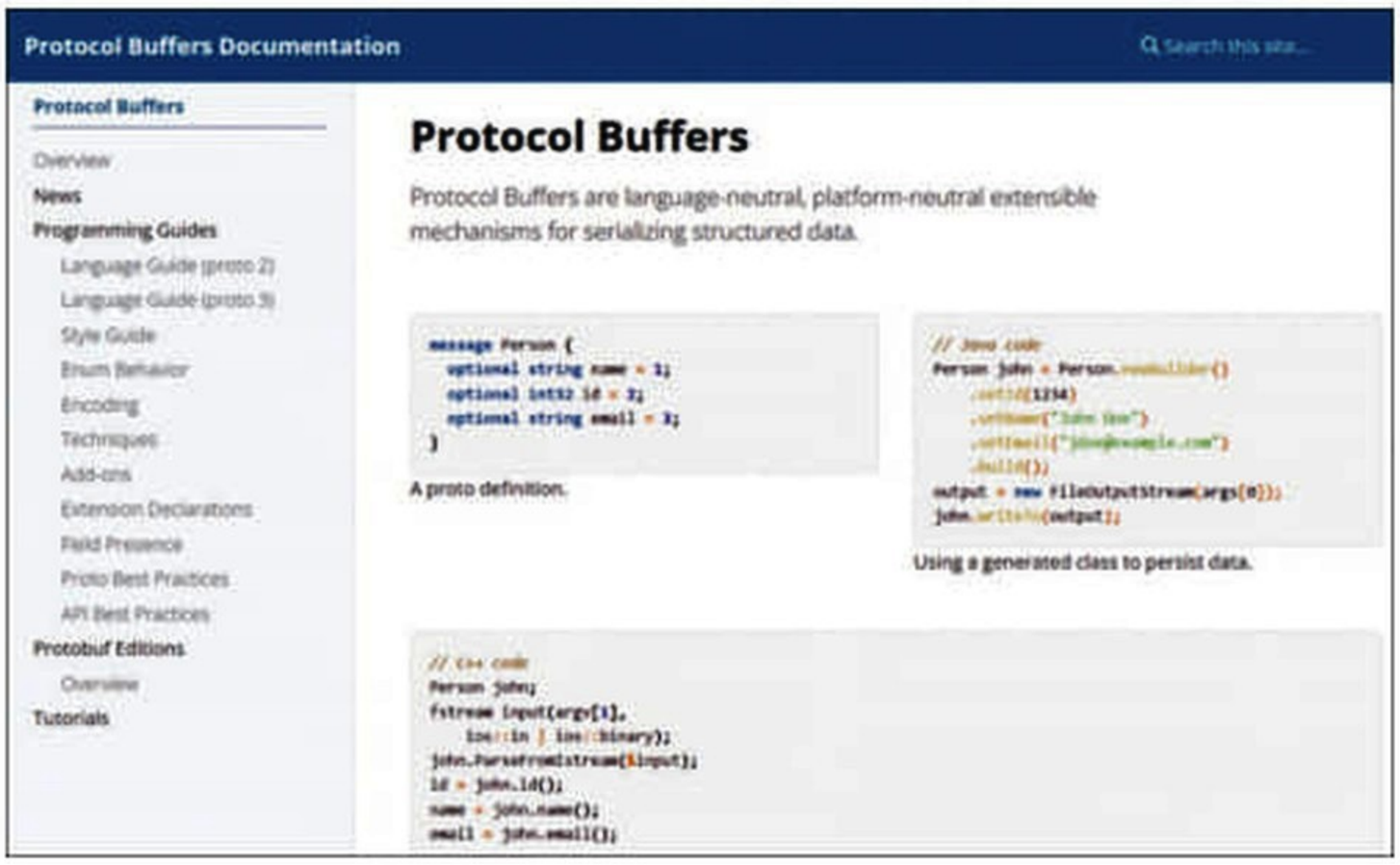
Un Workflow gRPC typique peut être décomposé en quatre étapes :

1. Définition du contrat de service : pour la communication inter-processus, il faut déterminer les services à appliquer, les « messages » qui les constituent et qui permettent de définir les requêtes et les réponses ainsi que les types des éléments constituants ces messages.

2. Génération du code gRPC : à partir du/des fichier(s).proto, un compilateur spécial (un transpiler), un outil ligne de commande nommé protoc, va générer le code opérationnel de la classe correspondante dans un des langages cibles disponible (C++, Python, Ruby, Java,...). Il est possible de faire ce travail pour d'autres langages mais cela ne sera pas aussi simple et direct.

3. Implémentation du serveur : « à la main » (et oui, il faut quand même bosser un petit peu, non mais...) dans le langage cible. Quelques exemples sont disponibles sur le site du gRPC (grpc.io) mais ce n'est pas encore très détaillé pour l'instant. Il y a au moins le minimum légal.

4. Création du stub client : il faut ensuite coder la partie client, celle qui va appeler un (ou plusieurs) des services disponibles. La/ les requête(s) sera/seront ensuite exécutée(s), si tout se passe bien, par le serveur gRPC. Le serveur est représenté, rappelons-le, par un programme en cours d'exécution, un processus si vous préférez, en écoute sur un socket réseau.



Vous trouverez la documentation des Protocol Buffers, des exemples et des tutoriels dans les différents langages de programmation disponibles à l'adresse https://protobuf.dev/

Le fichier.proto

Voilà ce que peut donner la consultation d'une base de données pour rechercher un produit en langage « Protobuf » (version proto3) :

```
syntax = « proto3 »;
package grpc_service ;
import google/protobuf/wrappers.proto ;
service RechercheProduit {
rpc getItemByName(google.protobuf. StringValue) returns (Items) ;
rpc getItemByID(google.protobuf. StringValue) returns (Item) ;
rpc addItem(Item) returns (google.protobuf. BoolValue) ;
}
message Items {
string itemDesc = 1 ;
repeated Item items = 2 ;
}
message Item {
string id = 1 ;
string name = 2 ;
string description = 3 ;
}
```

Dans cet exemple, la consultation de la base de données se fait *via* des bibliothèques spéciales du framework gRPC, les wrapper, importées grâce à l'instruction import. Dans des architectures client/serveur multilingues et multi-systèmes, ces bibliothèques assurent la communication entre des interfaces qui, sans elles, seraient incompatibles. C'est à partir de ce code générique que sont fabriquées les classes nécessaires à la gestion des messages dans un

GRPC VERSUS REST

De par ses nombreux avantages, le gRPC s'impose de fait comme une solution concurrentielle au REST (Representational State Transfer). REST est plutôt une norme qu'une technologie, mais particulièrement adaptée à l'exécution de services simples, alors que le gRPC déploie ses services au sein d'interfaces (API) et d'autres services plus complexes. REST utilise prioritairement le format de données JSON pour échanger des données entre applications. Son format est donc plus lisible mais plus volumineux que du binaire et du coup plus coûteux en termes de performances. Le gRPC peut, à l'inverse, organiser un flux de données plus compact. L'air de rien, les besoins en mémoire par sérialisation et binarisation des données sont réduits de près de 70 % par rapport à du JSON ou autre format texte. Le streaming bidirectionnel assure, de plus, un fonctionnement sans blocage de l'échange de données, offrant des performances et une vitesse d'exécution bien plus élevées que REST. Ce dernier reste néanmoins plus accessible du fait que le protocole HTTP est pris en charge par tous les navigateurs. Les développeurs du gRPC travaillent sur d'autres solutions afin de faciliter sa compatibilité avec les outils basés sur le web, comme le gRPC web.

des langages disponibles. En C++, par exemple, ce sont des fichiers.cc et.h, une paire pour la partie client et une pour la partie serveur.

Communication avec HTTP/2

Le protocole HTTP/2 tient un rôle central dans le gRPC. C'est lui qui permet le transfert de données binaires plus compactes que du JSON ou d'autres formats du même genre, ainsi que l'échange de messages et de données. Il met à disposition quatre types de RPC :

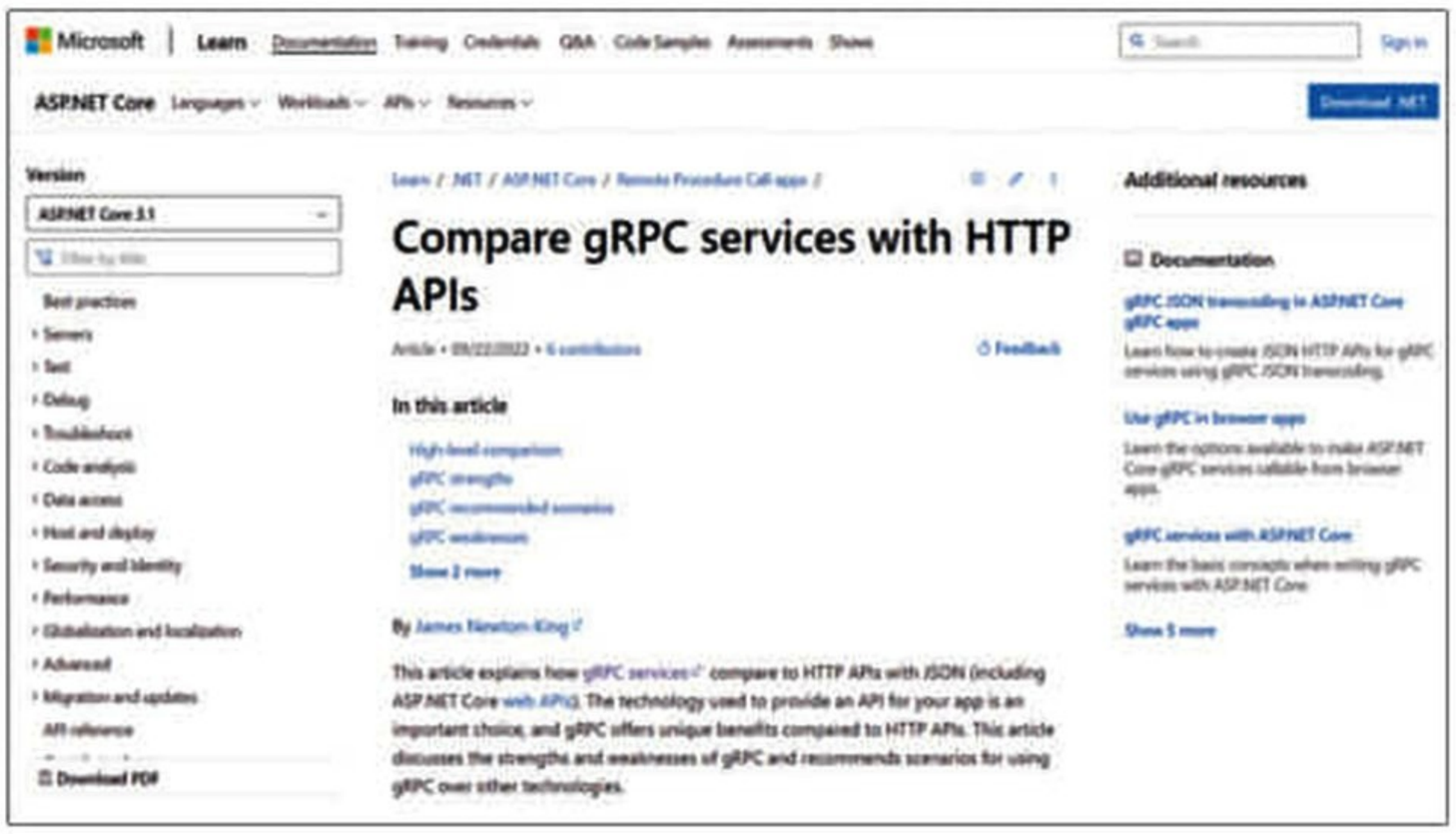
1. Les RPC unaires qui représentent le modèle de gRPC le plus simple. Le client émet une demande individuelle au serveur. Comme pour un appel fonctionnel classique, il reçoit ensuite une réponse individuelle du serveur. Exemple : rpc SayHello(HelloRequest) returns (HelloReply)
2. Les RPC streaming côté serveur permettent l'échange plus complexe de messages au sein d'un appel RPC unique. Le client émet une demande au serveur qui répond non pas par une réponse unique mais par un flux (stream) composé d'une suite de messages. Le client lit le flux jusqu'à épuisement des messages. Exemple : rpc ListFeatures(Rectangle) returns (stream Feature) {}
3. Les RPC streaming côté client qui, en quelque sorte, inversent le processus. Le client écrit une suite de messages et l'envoie au serveur *via* un flux (stream). Lorsque le client a envoyé tous les messages, il attend que le serveur les lise et renvoie la réponse. Exemple : rpc RecordRoute(stream Point) returns (RouteSummary) {}
4. Les RPC streaming bidirectionnel qui constituent la forme de communication la plus complexe. Cette fois, les deux côtés envoient un flux de messages, tous deux indépendants l'un de l'autre. Le client et le serveur peuvent lire et écrire dans l'ordre qu'ils souhaitent. Tout est possible : le serveur peut attendre de recevoir tous les messages du client avant d'écrire ses réponses tout comme il peut alterner la lecture d'un message avec l'écriture d'un autre. Toutes les combinaisons sont disponibles. Exemple : rpc RouteChat(stream RouteNote) returns (stream RouteNote) {}

Le protocole HTTP/2 prévient, grâce à ses hautes performances, du blocage du trafic des données. Les différentes variantes, à l'exception de la première, permettent d'établir un multiplexage performant à l'aide de requêtes imbriquées. Plusieurs signaux peuvent alors être regroupés sur une même connexion TCP et transférés simultanément sur un réseau.

Les avantages de gRPC

Le gRPC présente d'indéniables avantages. Il est relativement simple de le mettre en œuvre ainsi que de le greffer à des programmes existants. Il suffit d'intégrer le code du client au programme principal et de coder, de l'autre côté, un programme serveur. Le gRPC est hautement évolutif et capable de mener à bien des communications complexes, même au sein d'architectures client/serveur connectées à l'échelle internationale. HTTP/2 augmente ses performances, notamment ses capacités de multiplexage et de streaming bidirectionnel. Il est également possible d'effectuer des compressions d'en-têtes lorsque le volume de données des messages est trop important et doit être réduit de manière significative. La structure multicouches et normalisée du framework gRPC permet de réduire quelque peu les efforts de programmation. Les développeurs peuvent se concentrer en priorité sur l'implémentation du code du client et du serveur. Les fichiers protos, assez faciles à écrire, sont transformés en fichiers source grâce aux plugins du framework. Les Protocol Buffers et les compilateurs Protobuf permettent une communication enfin débridée. Systèmes d'exploitation, composants divers et variés des architectures client/serveur et langages de programmation peuvent être mélangés sans problème, un peu sur le même principe que les ORB (Object Request Broker) comme CORBA. Un logiciel écrit en C s'exécutant sous Linux peut communiquer avec un autre logiciel Java s'exécutant sur Mac OS, par exemple. Grâce à son impressionnante flexibilité, gRPC peut être utilisé de la même manière pour l'échange de données entre micro services (surtout si la faible latence et le haut débit sont de rigueur), entre applications de toute sorte et, de manière générale, dans les environnements « polyglottes » où plusieurs langages de programmation se côtoient. Il met aussi à disposition des technologies de sécurité aguerries comme une fonction d'authentification intégrée et la possibilité d'utiliser SSL/TLS pour l'authentification et le cryptage des communications. Le gRPC régule la dernière phase du traitement des données distribuées en connectant les appareils, les applications mobiles et les navigateurs avec les services backend. □

T.T.



Microsoft croit fortement au gRPC et compare l'efficacité de ses services aux API HTTP classiques, REST, ou non.

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

IT AND CYBERSECURITY

MEETINGS BY WEYOU GROUP

WWW.IT-AND-CYBERSECURITY-MEETINGS.COM

19, 20 & 21 MARS 2024

PALAIS DES FESTIVALS ET DES CONGRÈS DE CANNES

ILS SONT DÉJÀ INSCRITS

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

by weyou group

Professional Exhibitions and One to One Meetings Exhibitions

Donnerons-nous notre langue au ChatGPT ?



L'innovation portée par ChatGPT est comparée à celle de l'imprimerie ou l'Internet en démocratisant l'utilisation de l'intelligence artificielle. Les tenants du pour ou du contre rivalisent d'arguments parfois sans discernement ou réalité. L'ouvrage de Gilles Moyse, docteur en intelligence artificielle et fondateur d'une start-up dédiée au traitement automatique du langage et des documents par l'intelligence artificielle, apporte une vue rationnelle autour de l'utilisation de ces outils et les perspectives qu'ils ouvrent pour les citoyens, les salariés... Plus largement, cet essai analyse les conséquences sur la démocratie, les équilibres géopolitiques et économiques. Un ouvrage salutaire pour éveiller les consciences et comprendre réellement ce que peut faire les nouvelles formes d'intelligence artificielle. La préface d'Etienne Klein pose le débat autour de l'intelligence artificielle en rappelant les notions de base pour comprendre le sujet et donner une perspective philosophique à son utilisation. À lire absolument pour éviter d'entrer dans de faux débats ou des peurs issues de la science-fiction.

L'IA RÉELLE, MAGIQUE ET TRAGIQUE

Le chapitre précédent a montré les différents fantasmes associés à l'intelligence artificielle, mais cette dernière a néanmoins des applications bien réelles. Les utilisateurs, s'ils sont fascinés par les IA magique ou tragique, ne sont néanmoins pas dupes et savent que leurs usages quotidiens du numérique sont traversés par l'IA. Une étude WPP Research Consulting publiée en avril 2023 révèle que 80 % des Français sont parfaitement conscients que des algorithmes d'IA sont à l'œuvre derrière les applications de reconnaissance vocale et faciale de leurs téléphones. Ils sont 75 % à dire l'utiliser quotidiennement, notamment pour la traduction automatique et la recommandation de produits. Nous allons dans ce chapitre présenter ces différents usages, mais également les hiérarchiser. Les applications bien réelles de l'IA, exposées dans une première section, sont dans un second temps comparées à l'une d'entre elles, le moteur de recommandation, responsable de l'émergence des géants du numérique dans les années 2000 du fait des revenus gigantesques que ces modèles ont générés. Enfin, le chapitre se conclut sur une discussion concernant les données personnelles, indispensables au fonctionnement des moteurs de recommandation, dont les enjeux financiers entraînent des effets de bord négatifs.

Où est l'IA aujourd'hui ?

Partout ! Dans notre vie personnelle, lorsque nous posons une question à un moteur de recherche, des algorithmes d'IA sont à l'œuvre pour renvoyer les résultats, mais aussi pour compléter la question que nous

sommes en train de saisir, pour en corriger l'orthographe, pour afficher des publicités qui lui sont liées, pour trier les réponses les plus pertinentes, etc. Cette utilisation est loin d'être marginale puisque 9 milliards de requêtes sont traitées tous les jours par un moteur comme Google, soit plus d'une requête par habitant et par jour dans le monde !

Lorsque nous débloquons notre téléphone en montrant notre visage, des algorithmes de vision par ordinateur s'assurent qu'il est connu. Lorsque nous parlons pour saisir un message, ce sont des modèles de conversion de la voix en texte qui sont mobilisés. À l'inverse, lorsque notre GPS nous demande de tourner à droite dans 300 mètres, des algorithmes de conversion du texte en voix sont exploités. L'application de guidage se base aussi sur des algorithmes d'IA, de planification cette fois, pour proposer un chemin optimal du point A au point B, évitant les autoroutes et les bouchons par exemple.

Avez-vous remarqué que votre téléphone se décharge plus vite lors des premiers jours d'utilisation et que sa batterie dure ensuite beaucoup plus longtemps ? Normal : un algorithme d'IA analyse vos usages pour interrompre les applications inutiles et ajuster l'éclairage de l'écran afin d'augmenter la durée de vie de la batterie106. Toujours sur les téléphones, une des applications les plus connues d'IA est la « complétion automatique » des mots que l'on écrit, lorsque l'on rédige un SMS par exemple. C'est un modèle de langue très simple, qui fonctionne au niveau des lettres, et qui prédit les quelques lettres suivantes étant donné les précédentes.

L'IA est présente aussi dans les bureaux. Tout le monde connaît le correcteur d'orthographe... C'est de l'IA ! Peut-être avez-vous pu tester la capacité de Google Mail à compléter certaines phrases quand vous rédigez un message... C'est de l'IA, encore un modèle de langue, qui ici prédit des mots étant donné les précédents. Dans les outils de visioconférence qui sont devenus le quotidien des travailleurs du secteur tertiaire (bureaux, services, administrations...), peut-être avez-vous remarqué que vous pouviez flouter et même modifier le décor filmé par votre caméra. Ici encore, un algorithme de vision par ordinateur est utilisé pour séparer le personnage au premier plan (vous) du décor et remplacer ce dernier.

Des logiciels de traitement des grandes masses de données présentes dans les entreprises (Big Data) se sont également répandus, avec des applications extrêmement diverses. Les entreprises qui commercialisent ces logiciels s'appellent Dataiku, Databricks, Snowflake... Elles permettent à leurs clients de stocker les données de l'entreprise et d'en tirer parti avec des algorithmes d'IA pour en extraire autant d'informations que possible.

Parmi les innombrables cas d'usage de ces solutions, mentionnons la détection d'attrition (ou churn en anglais), qui permet, à partir de l'étude des données d'interaction entre un client et une entreprise, de prédire s'il va résilier son abonnement dans quelques mois. Signalons aussi, dans le domaine financier, la détection de fraude bancaire à partir des différents usages d'une carte de crédit (nombre et lieux des retraits, achats en ligne, en magasin, etc.). Autre exemple : la gestion de la relation client avec l'usage de chatbots (pas toujours très satisfaisants avant ChatGPT...) et/ou de réponses automatiques ou semi-automatiques pour préparer et accélérer le travail des conseillers et gestionnaires. Dernier exemple enfin : la lecture et l'analyse automatique des documents (factures, bulletins de souscription, papiers d'identité...) pour réduire les temps de traitement des dossiers.

Ces applications sont plus banales, moins fabuleuses que celles exposées au chapitre précédent. Elles sont néanmoins utilisées dans la moitié des entreprises dans le monde, selon une étude McKinsey publiée fin 2022 réalisée auprès d'entreprises de toutes tailles et de tous secteurs. Le patron de Databricks, entreprise qui propose un produit d'analyse de données générant un milliard de dollars de chiffre d'affaires en 2022, qualifie même cette IA d'« ennuyeuse »... Ennuyeuse mais lucrative.

Dernier exemple de cas d'utilisation de ces IA « banales » : le commerce en ligne ou e-commerce. La vente en ligne en France représente 147 milliards d'euros en 2022 alors qu'elle n'en représentait que 8 en 2005. Le développement des chaînes logistiques au cours des vingt-cinq dernières années est largement responsable de cet essor. Là encore, l'IA est abondamment utilisée. Chez Amazon, des algorithmes par renforcement permettent d'optimiser la vitesse de livraison sur le dernier kilomètre. Le français Exotec propose des entrepôts et des robots pour traiter les commandes et préparer les colis. Pour Carrefour, le système permet l'exécution de 4 000 commandes quotidiennes et des livraisons de produits à domicile en deux heures.

La poule aux œufs d'or

Toutes ces applications de l'IA sont bien réelles et utilisées quotidiennement. Elles exploitent des algorithmes issus des différentes branches du domaine (voir la première partie) : traitement automatique du langage, vision par ordinateur, machine learning, base de connaissances, etc.

Parmi ces algorithmes néanmoins, il en est un qui tient le haut du pavé et qui est en bonne partie responsable de l'explosion de l'intelligence artificielle depuis le début des années 2000 : le moteur de recommandation.

Comme le rappelle l'enseignant-chercheur à l'École polytechnique El Mahdi El Mhamdi pour Usbek et Rica en mai 2023 : *« Quand on pense IA désormais, on pense ChatGPT. Mais les IA les plus importantes en termes de conséquences sociales, ce sont les systèmes de recommandation algorithmiques des réseaux sociaux »*. En termes de conséquences sociales... et économiques.

Avant d'explorer les répercussions de l'usage en masse de ces systèmes, expliquons ce qu'ils sont. Les systèmes de recommandation algorithmiques, ou moteurs

	Chiffre d'affaires*	Bénéfice net*	Part reco.	Chiffre d'affaires reco.*	Bénéfice net reco.*
Alphabet	280	60	80 %	224	48
Amazon	514	10	35 %	180	4
Meta	117	23	98 %	115	23
Apple	394	102	-	20	-
Microsoft	198	83	-	18	-
TOTAL	**1 503**	**278**		**535**	**75**

**En milliards de $ en 2022*

de recommandation, sont des algorithmes qui prennent en entrée toutes les informations à leur disposition sur une personne, comme ses habitudes d'utilisation des logiciels, son historique de navigation, ses centres d'intérêt, etc., et lui « proposent » quelque chose : une publicité (Google, Facebook, Instagram), un autre produit à acheter (Amazon), une vidéo (Netflix, YouTube), une musique (Spotify), ou pourquoi pas un partenaire (Meetic, Tinder).

Ces moteurs de recommandation sont à la base du développement économique des géants technologiques depuis 2000, principalement Google, Meta (la maison mère de Facebook, Instagram et WhatsApp) et Amazon, mais également de la myriade d'acteurs qui se sont inscrits dans leur sillage. Business Insider le rappelle début 2023 : *« Une grande partie de la Silicon Valley gagne vraiment de l'argent grâce à la publicité en ligne. »*

Le tableau ci-dessus montre pour 2022, en milliards de dollars, les chiffres d'affaires, les bénéfices nets et la part de ces chiffres imputables aux moteurs de recommandation pour Alphabet (la maison mère de Google), Amazon, Meta, Apple et Microsoft :

La colonne « Part reco. » dans le tableau ci-dessus indique la part de chiffre d'affaires réalisée à l'aide de moteurs de recommandation. Les colonnes suivantes « Chiffres d'affaires reco. » et « Bénéfice net reco. » sont calculées en appliquant la Part reco. au chiffres d'affaires et au bénéfice net. Le chiffre d'affaires des GAFAM[1] lié à la recommandation s'élève donc à 535 milliards de dollars en 2022.

À ce montant s'ajoutent les 70 milliards de dollars de chiffres d'affaires publicitaires d'Alibaba (concurrent chinois d'Amazon) et ByteDance (éditeur de TikTok).

1 : Les GAFAM représentent les compagnies américaines Google, Amazon, Meta (anciennement Facebook), Apple et Microsoft.

À l'aide des moteurs de recommandation, le chiffre d'affaires généré par les plus grands acteurs de la tech américaine et chinoise s'élève donc à un peu plus de 600 milliards de dollars en 2022.

En comparaison, le marché de l'IA, en comptant le logiciel et le matériel, s'élève à 62 milliards de dollars sur la même période, soit un dixième de la valeur générée par les moteurs de recommandation. Même une entreprise très en croissance comme Nvidia, qui crée des puces informatiques utilisées pour accélérer les calculs en IA, ne fait « que » 27 milliards de chiffre d'affaires en 2022.

Parmi les GAFAM, Google, Amazon et Meta se sont développées grâce à la recommandation. Seules Apple et Microsoft, les deux plus anciennes de ce groupe, ne se sont pas construites sur ce modèle, même si elles génèrent toutes deux en 2022 environ 20 milliards de dollars grâce à la publicité en ligne (et donc à la recommandation). Il faut dire qu'Apple et Microsoft ont été fondées autour de 1980 (Apple en 1976 et Microsoft en 1981), quand les trois autres ont été créées au voisinage des années 2000 (Amazon en 1994, Google en 1998 et Facebook en 2004). Apple et Microsoft ont donc bâti leur empire sur l'apparition de l'ordinateur personnel tandis qu'Amazon, Google et Facebook ont érigé le leur avec le développement de l'internet grand public.

La recommandation de contenus et de publicités en ligne est donc le moteur financier de l'IA aujourd'hui. Quel en est son carburant ?

La fin de la vie privée : les données personnelles

Le carburant des moteurs de recommandation qui participent à l'explosion commerciale de l'intelligence artificielle, ce sont les données. Ces données peuvent être personnelles ou d'usage.

Selon la CNIL[2], *« une donnée personnelle est toute information se rapportant à une personne physique identifiée ou identifiable »*. Certaines données personnelles comme le nom et le prénom permettent de retrouver directement une personne. D'autres comme un numéro de Sécurité sociale ou une adresse mail doivent être rapprochées d'un référentiel pour réaliser l'identification. D'autres, enfin, sont croisées pour identifier une personne, par exemple le rapprochement d'un métier et d'une adresse.

Les données d'usage sont celles que nous créons sans nécessairement le savoir lorsque nous utilisons des logiciels et des services en ligne. Par exemple les requêtes que nous saisissons dans Google, le temps que nous restons sur la page de résultat, les liens sur lesquels nous cliquons, les mails que nous envoyons et recevons sur Gmail, les posts que nous regardons sur Facebook, les jeux auxquels nous jouons, les articles que nous achetons sur Amazon, etc. Toutes ces actions sont enregistrées et constituent les données d'usage, qui fournissent des indications précises sur nos goûts, nos centres d'intérêt, nos questionnements à un moment donné, etc.

Par ailleurs, les cookies, qui sont des fichiers déposés sur notre ordinateur lorsque nous naviguons sur Internet, permettent également de remonter des informations à Google et à Facebook même lorsque nous sommes sur d'autres sites.

En plus de celles créées lorsque nous naviguons sur Internet, les données d'usage sont aussi envoyées par nos téléphones portables (localisation GPS, appels, caméra, applications...), mais également nos montres connectées, nos enceintes « intelligentes » de type Alexa ou OK Google, même nos imprimantes !
En somme, nous envoyons en permanence des données d'usage, souvent sans le savoir.

Des fiches ultraprécises

Le rapprochement des données d'usage avec les données personnelles permet d'établir des fiches d'identité extrêmement précises nous concernant. Même lorsque nous ne sommes pas connectés sur une application en particulier, la simple trace de notre ordinateur, c'est-à-dire son système d'exploitation (Windows, iOS, Linux...), sa version, l'adresse de la box Internet, la résolution de notre écran, etc., permet de nous identifier.

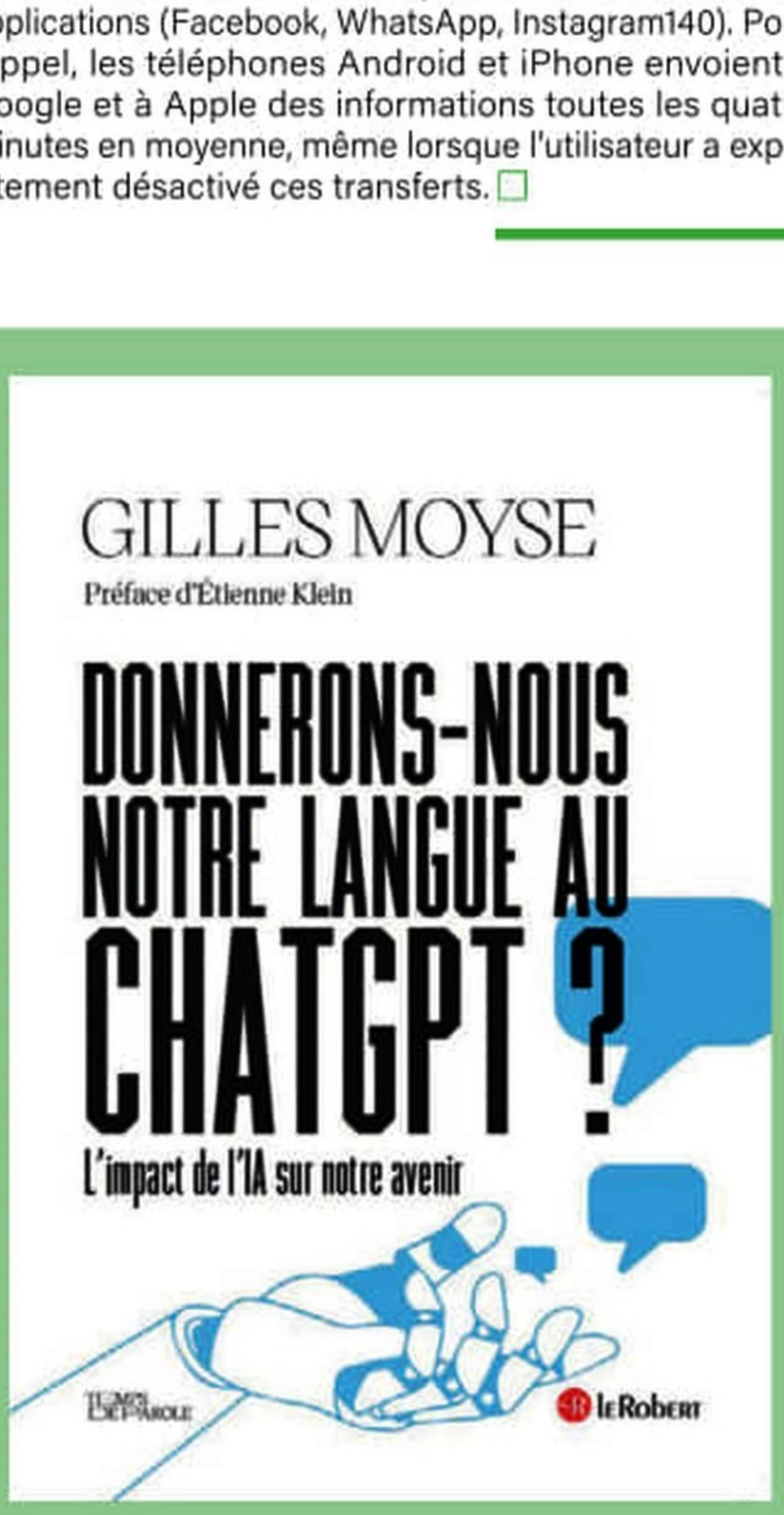
Ces données personnelles et d'usage sont la matière première des moteurs de recommandation qui génèrent plus de 600 milliards de dollars par an pour les géants américains et chinois du numérique.

En connaissant nos goûts, nos habitudes, nos centres d'intérêt, nos projets, notre localisation, ces services peuvent nous recommander le « bon » produit, le « bon » article, la « bonne » idée, la « bonne » vidéo, au « bon » moment.

La quantité d'informations par personne détenue par ces géants du numérique est ahurissante : emplacements visités, sexe, hobbies, carrière, relations amoureuses, revenus, poids, historique de navigation...

De plus, le nombre de personnes pour lesquelles ces informations sont connues est également vertigineux. On compte en 2023, pour Google, 1,8 milliard de comptes Gmail, 3,6 milliards de téléphones Android, pour Apple 1,2 milliard d'iPhone actifs début 2022, pour Meta plus de 3 milliards d'utilisateurs quotidiens d'une de leurs applications (Facebook, WhatsApp, Instagram140). Pour rappel, les téléphones Android et iPhone envoient à Google et à Apple des informations toutes les quatre minutes en moyenne, même lorsque l'utilisateur a explicitement désactivé ces transferts. □

GILLES MOYSE
Préface d'Étienne Klein



Donnerons-nous notre langue au ChatGPT ?

Gilles Moyse
Préface d'Etienne Klein
Edition Le Robert - Collection Temps De Parole
EAN : 9782321019732 - ISBN : 2321019735
Nombre de pages 240 - Prix 17,90 €

2 : Dans l'univers numérique, la Commission nationale de l'informatique et des libertés (CNIL) est le régulateur des données personnelles.



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.

Audit

OSTIF.org : le garant de la sécurité des projets

L'Open Source Technology Improvement Fund (OSTIF.org) est une organisation indépendante sans but lucratif dont la mission est de renforcer la sécurité des applications open source par des audits.

L'OSTIF profite d'une large communauté qui regroupe plus de 1000 experts en cybersécurité afin de réaliser ses audits de sécurité. À ce jour, l'organisation a audité 22 projets open source avec plus de 50 failles critiques identifiées et patchées à la suite de son intervention en plus de 5000 heures de revue des codes. Ainsi, en septembre dernier, elle a réalisé en collaboration avec X41 D-Sec l'audit du code du projet Open Search, un projet de moteur de recherche qui évidemment contient des données sensibles. Le but de l'audit était de trouver les vulnérabilités par une revue et une analyse statique du code. Cette analyse statique a été utilisée par X41 pour réaliser des tests de pénétration en recherchant des vulnérabilités spécifiques comme les possibilités de montée en privilège, de fausses requêtes côté serveur, l'injection de commandes... Deux vulnérabilités à criticité basse et six résultats informationnels ont été détectés lors de l'audit.



Amir Montazery, Managing Director de l'OSTIF.

Une méthode d'audit structurée

La méthode de l'organisation suit un processus quasi immuable. La première étape consiste en un rendez-vous de visu pour comprendre les besoins et définir le périmètre d'intervention à travers un réseau large d'auditeurs avec une analyse selon les coûts et les expertises nécessaires. Après approbation, les équipes se mettent au travail avec des points réguliers sur l'avancement de l'audit. L'OSTIF gère le processus et sert de tiers indépendant entre les parties, le projet et les experts. A la suite de l'analyse, les auditeurs fournissent les résultats de leur évaluation et aident les entreprises s'il est nécessaire de corriger des bugs ou de renforcer le code. Le code mis à jour et un rapport sont rendus publics assurant ainsi les futurs utilisateurs que le projet a bien été audité pour sa sécurité.

Des possibilités de partenariats multiples

Organisme à but non lucratif, l'OSTIF est ouvert à plusieurs possibilités de travail ou de participation. Ainsi il est possible de réaliser des don pour soutenir l'organisation (qui ne roule pas sur l'or). Il est possible d'entrer dans le réseau d'experts pour réaliser des audits. Il est de plus possible pour une entreprise de sponsoriser la publication d'un rapport. □

B.G

OSTIF.ORG EN BREF

Derek Zimmer est le président et directeur exécutif de l'organisation. Il est un fervent supporter du respect des données personnelles, ce qui l'a poussé à s'engager et à fonder l'OSTIF. Il est aidé par Amir Montazery, un Américain de Chicago. Après des débuts dans la finance, il a travaillé dans de multiples startups puis a fini par devenir auditeur sur la gouvernance et la sécurité durant son temps libre. Il est maintenant très occupé avec l'OSTIF ! Zach Graves a en charge la conception et le développement du site de l'organisation et Steve Donley anime la communauté autour de l'organisation. Un conseil accompagne les dirigeants de l'organisation. La plupart sont présents dans des entreprises ou des organisations comme la Linux fondation, OpenVPN Project ou OpenSSL. Red Hat, F-Secure, Quarkslab, Kudelski Security, DuckDuck GO et Veracrypt sont aussi représentés dans ce conseil.





Enregistreur audio

Philips réinvente la Plume à Papote

Ça ressemble à un stylo, ça écrit comme un stylo et pourtant… c'est un enregistreur audio. Philips a récemment lancé le DVT 1600 VoiceTracer Audio Recorder Pen, capable d'enregistrer jusqu'à 129 h d'audio. Idéal pour ne rien perdre d'une réunion ou d'une conférence, en toute discrétion.

Dans Harry Potter, la journaliste Rita Skeeter utilise une « Plume à Papote », une plume qui note les propos de son interlocuteur. L'outil n'est désormais plus réservé au monde de la magie, puisque Philips vient de lancer un stylo enregistreur audio qui, par le biais d'un logiciel Speech-to-Text, permet de convertir les paroles en texte. Le DVT 1600 VoiceTracer Audio Recorder Pen se présente en effet comme un stylo à cartouche d'encre rechargeable tout à fait classique (avec des dimensions de 15×145×11 mm pour un poids de 24 g), mais il renferme un microphone mono, enregistrant au format WAV les sons à 360°.

Avec un bitrate de 512 kbps pour 16 kHz, l'appareil est relativement sensible et l'enregistrement se déclenche et s'arrête avec une unique touche. Il est doté d'une mémoire NAND de 32 Go, pour un total de 129 h d'enregistrement audio, et d'une connectivité USB qui permet de le connecter directement à un PC ou un Mac pour transférer les fichiers audio. Sa batterie 190 mAh permet une durée de vie d'environ huit heures et Philips promet une charge complète en deux heures.



Le DVT 1600 VoiceTracer Audio Recorder Pen de Philips ressemble en tout point à un stylo classique. Mais son micro mono et ses 32 Go de mémoire garantissent jusqu'à 129 heures d'enregistrement audio.

DVT 1600 VOICETRACER AUDIO RECORDER PEN



USB : USB-C 2.0 haut débit
Capacité mémoire intégrée : 32 Go
Type de mémoire intégrée : NAND Flash
Microphone intégré : mono
Format d'enregistrement : WAV (PCM)
Fréquence d'échantillonnage : 16 kHz
Débit binaire : 512 kbps
Durée d'enregistrement : 129 h
Autonomie de la batterie : jusqu'à 8 h d'enregistrement
Dimensions du produit : 15 × 145 × 11 mm
Poids : 24 g

Speech-to-Text

Surtout, le DVT 1600 VoiceTracer Audio Recorder Pen peut être associé au logiciel de reconnaissance vocale Sembly de Philips, lequel assure que la transcription de l'audio au texte est *« jusqu'à trois fois plus rapide que la saisie manuelle »*. Malheureusement, nous n'en sommes pas encore au point où le stylo enregistreur enverrait instantanément l'audio dans le cloud afin de convertir en simultané les propos en texte.

Il sera nécessaire d'importer le fichier sur un ordinateur et de le télécharger sur Sembly (version Web ou application Android et iOS) pour obtenir un document écrit. Il existe d'autres logiciels Speech-to-text, mais on notera que l'achat d'un DVT 1600 VoiceTracer inclus une heure de téléchargement audio par mois et un bon pour 15 heures supplémentaires. En plus, il faudra de nouveau passer à la caisse. Sembly fonctionne dans une trentaine de langues, dont l'anglais, le français et le néerlandais. □

G.P



Adoption

L'IA de plus en plus génératrice de revenus

D'une mesure de réduction des coûts, l'intelligence est perçue de plus en plus comme une source de revenus, ou du moins un moyen de générer de nouveaux revenus, au sein des organisations.

Selon une étude de Weka, 69 % des organisations déclarent avoir au moins un projet d'IA en production, tandis que 28 % expliquent que l'IA est passée à l'échelle dans leur entreprise. Ces derniers, que le cabinet d'étude qualifie de *« pionniers de l'IA »*, ont dépassé le stade des projets pilote : l'intelligence est chez eux non seulement en production, mais aussi intégrée dans les flux de travail et les propositions de valeur. Notons que l'enquête a été menée auprès de 1516 décideurs IT dans des entreprises comptant plus de 250 employés et plus de 10 millions de dollars de revenus annuels en Amérique du Nord, Europe, Moyen-Orient, Afrique et Asie-Pacifique.

Sans surprise, Weka a remarqué dans cette étude divers niveaux d'adoption de l'intelligence artificielle dans les entreprises. Pour 28 %, l'IA est largement mise en œuvre au sein de l'organisation quand 30 % déclarent qu'elle n'est qu'un élément mineur. *« Quoi qu'il en soit, pour la plupart des organisations, il est clair que l'utilisation de l'IA n'est plus limitée à un petit groupe de spécialistes en informatique ou en science des données, mais constitue plutôt une capacité interfonctionnelle utilisée par un ensemble d'équipes métiers »* note le cabinet. Ajoutons qu'un tiers des personnes interrogées utilisent l'IA générative et les Large Language Models. Soit une adoption majeure de technologies relativement jeunes dans les entreprises, mais dont les analystes prévoient que le marché représentera 36 milliards de dollars à l'horizon 2028.

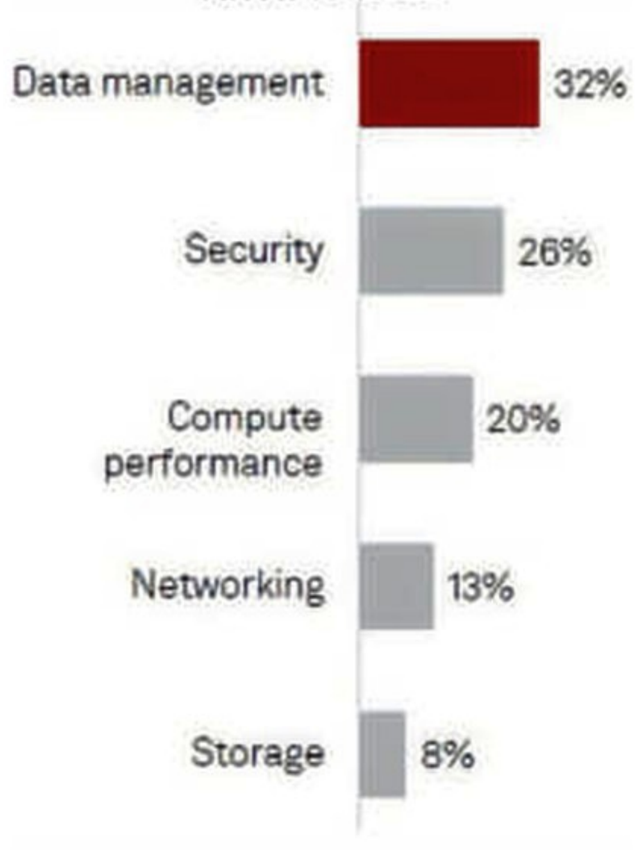
De la réduction de coûts à la création de revenus

L'un des faits marquants qui ressort de cette étude, c'est une évolution dans l'approche autour de l'IA. Là où ils étaient auparavant perçus et utilisés comme une mesure de réduction des coûts à un moteur de revenus, les projets d'intelligence artificielle et de machine learning s'achoppent de plus en plus sur la génération de revenus. Si, comme pour de nombreuses autres technologies d'automatisation, sa valeur est généralement à la réduction des coûts, 69 % des réponses reçues par Weka quant aux motivations derrière les projets d'IA citent des facteurs axés sur les revenus, contre 31 % qui sont axés sur les coûts.

« Même si des économies de coûts et des gains d'efficacité sont indéniablement réalisables grâce aux applications d'IA/ML, le rapport 2023 Global Trends AI Report montre que les organisations se tournent de plus en plus vers l'IA pour les aider à débloquer de nouvelles sources de revenus » écrit le cabinet. Il s'agit globalement d'employer l'IA/ML pour créer de nouveaux produits et services ou améliorer la qualité des existants, stimuler les initiatives commerciales, personnaliser la communication vers le client ou le prospect, formuler des recommandations plus pertinentes, *etc.* On notera en outre que les *« pionniers de l'IA »* sont 70 % à estimer que l'IA est génératrice de revenus, contre 66 % chez ceux qui sont à un stade moins avancé, ce qui suggère que l'accent mis sur le potentiel de l'IA à générer des revenus augmente à mesure que les initiatives d'IA mûrissent.

Pour autant, le recours à l'IA ne se fait pas sans heurts, à commencer par des infrastructures IT qui ne sont pas nécessairement adaptées. Ainsi, de nombreuses organisations ressentent de manière aiguë la pression que les modèles d'IA exercent sur leur infrastructure de données. Les ensembles de données de plus en plus volumineux nécessaires à l'entraînement des modèles d'IA sont composés de divers types de données et nécessitent des calculs complexes, repoussant les limites des architectures informatiques et de données traditionnelles.

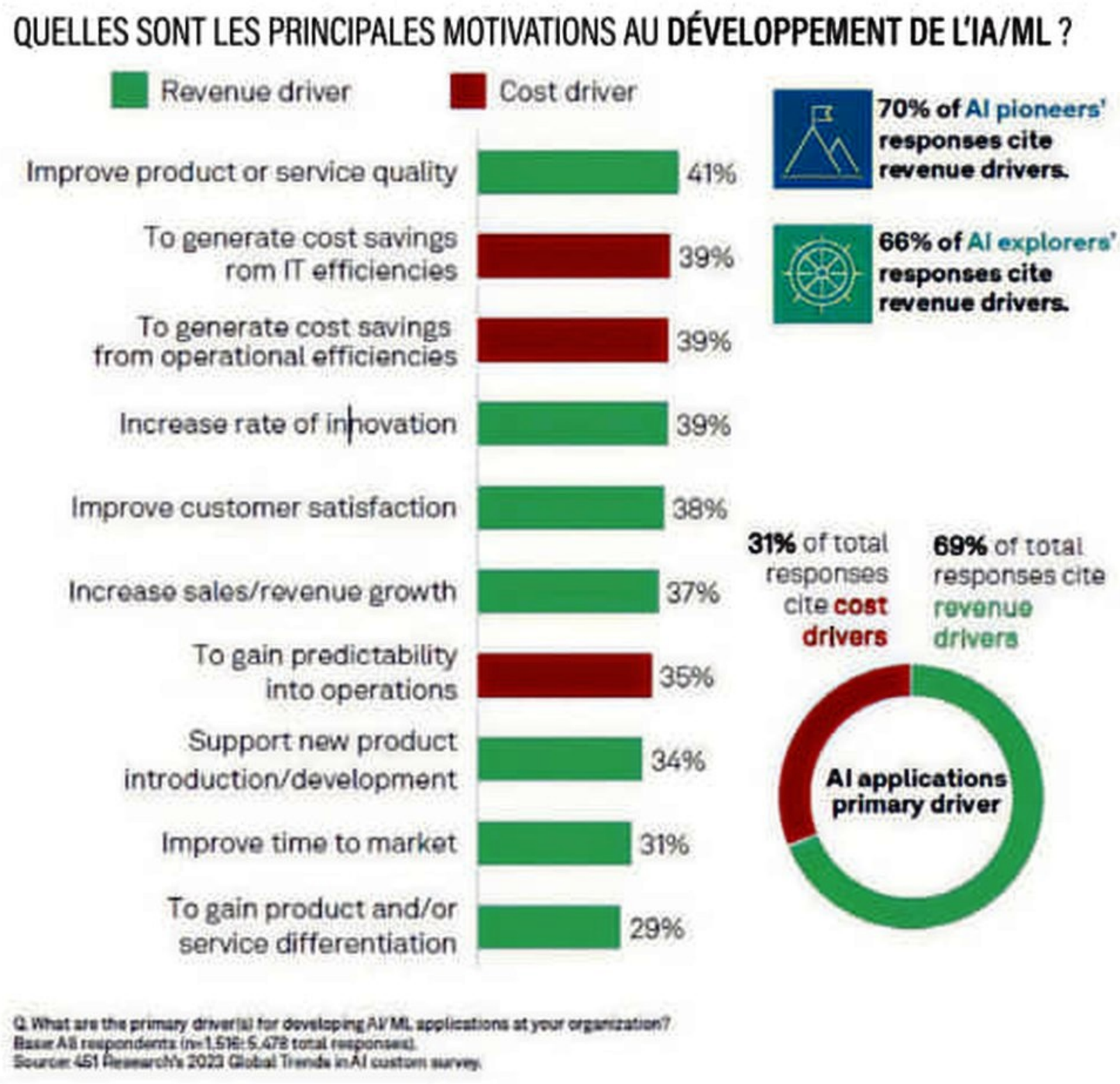
LES PRINCIPAUX OBSTACLES À L'UTILISATION DE L'INTELLIGENCE ARTIFICIELLE



Les architectures IT, obstacle n°1

Ces défis en matière d'infrastructure et de données sont exacerbés par l'essor rapide de l'IA générative, qui a rythmé une grande partie de

l'évolution du marché de l'IA en 2023. La gestion des données est la difficulté la plus fréquemment citée, à 32%, devant les problématiques de sécurité (26%) et les performances de calcul (20%). En tête des préoccupations, l'hétérogénéité des données, et des volumes trop importants. Si les données structurées sont utilisées par 66% des personnes interrogées, 52% des répondants utilisent aussi des données en streaming telles que les données de télémétrie IoT, 51% les logs et 43% des données semi-structurées, à l'instar des e-mails (43 %). S'y ajoutent avec l'IA générative et la vision par ordinateur les données Rich Media non structurées (37 %), images incluses, et le texte non structuré (35%). Les décideurs IT interrogés s'inquiètent notamment des difficultés d'approvisionnement, de préparation, de normalisation des données et d'inférence d'un modèle, tout au long du cycle de vie des applications IA/ML. D'autant que, lors du passage du POC à la production, le développement et la mise en œuvre de modèles inférentiels sont ralentis car, bien souvent, l'architecture informatique existante ne peut pas prendre en charge les applications IA/ML. Les lacunes en matière de gouvernance des données achèvent l'ensemble, entre manque de compétences, absence de contrôle, de règles et silos.



UNE ÉTUDE SECTORIELLE

L'enquête de Weka se penche également sur les usages de l'intelligence artificielle et du machine learning dans certains secteurs. Ainsi, on apprend que dans le domaine des services financiers, près de la moitié des personnes interrogées déclarent investir en priorité dans la sécurité des données. Outre le traitement des paiements et les prévisions financières, la détection et la prévention de la fraude constituent une priorité pour de nombreuses entreprises. Dans la défense et l'aérospatiale, il s'agit principalement de travailler sur des modèles d'inférence de vision par ordinateur qui prennent des décisions instantanées critiques sur les systèmes autonomes tels que les drones ou les véhicules automatisés. Côté secteur automobile, sans surprise, l'IA est mise à profit pour optimiser la production de véhicules ainsi que leur qualité, et dans la recherche autour de la conduite assistée/autonome, génératrices d'immenses volumes de données. De même, l'industrie pharmaceutique s'appuie sur l'IA pour les activités de fabrication tout comme pour l'accélération du développement de médicaments en R&D et le respect des processus de conformité, pour une mise sur le marché plus rapide.

Néanmoins, il ne faut pas brosser un tableau trop négatif de ces problèmes d'infrastructures, puisque l'étude pointe que l'IA est aussi un catalyseur essentiel de la performance par rapport aux objectifs de développement durable des entreprises. Par ailleurs, les pionniers de l'IA tirent parti d'une approche hybride et d'un plus grand nombre de sites de déploiement pour prendre en charge les demandes des charges de travail IA/ML, allant du cloud public aux centres de données d'entreprise et, de plus en plus, aux sites périphériques. Les répondants ayant des projets IA/ML dans des environnements de production exploitent en moyenne davantage de ces emplacements (3,2 emplacements de déploiement pour la formation, 2,5 pour l'inférence) que les autres (2,9 et 2,3 emplacements, respectivement). Cependant, avec les applications d'IA complexes et gourmandes en données, le cloud public offre un démarrage plus facile. Il est d'ailleurs le principal lieu de déploiement pour la formation des modèles IA/ML (47%) et l'inférence (44%). □

G.P

Études Les salaires s'assagissent

Différentes études font le point sur les tendances des salaires dans le secteur IT. Pour 2024, elles prévoient une accalmie sur les salaires.

Hayes a récemment rendu publique son analyse des salaires par secteur, dont celui des technologies de la communication. Elle constate un marché toujours dynamique tiré par plusieurs tendances de fond comme le cloud ou l'analytique. Hayes résume la situation d'une simple phrase : *« le marché de l'emploi est abondant mais nuancé par une tension importante. la plupart des entreprises du secteur recrutent, mais la grande majorité d'entre elles ont des difficultés à trouver les compétences. Cette tension peut donc dans de nombreux cas entraîner des augmentations de salaires. En effet, face à la pénurie de compétences, il arrive souvent que les entreprises proposent une rémunération supérieure à celles pratiquées normalement aux experts aux compétences rares, afin de les attirer et devancer la concurrence »*. L'étude continue : *« une hausse des recrutements et des salaires a été par exemple constatée dans le domaine de l'Architecture SI (fonctionnelle ou technique) et du Big Data avec les profils de Data analysts notamment. Ainsi, les jeunes diplômés peuvent se positionner entre 35 et 40 K€/an et les profils les plus expérimentés (de 5 à 15 ans d'expérience) peuvent prétendre à un salaire de 60 à 80 K€/an. Les profils de Développeurs sont également toujours très recherchés et donc bien rémunérés. On observe quelques écarts selon les langages, mais un jeune Ingénieur diplômé peut prétendre à minima à un début de carrière à 35 K€/an »*.

Systèmes d'Information

RÉMUNÉRATION ANNUELLE BRUTE EN K€

FONCTIONS DE DIRECTION	10 ans et +	TREND
Directeur des systèmes d'information	90 - 250	↑
Responsable - Directeur informatique	70 - 100	→
Directeur des études	80 - 150	↑
Directeur des infrastructures et de la production	80 - 150	↑
Directeur du digital/de la transformation numérique	80 - 130	↑
Directeur data	80 - 130	↑
Directeur de la sécurité des systèmes d'information	100 - 200	↑

RÉMUNÉRATION ANNUELLE BRUTE EN K€

INFRASTRUCTURES ET PRODUCTION	0 à 2 ans	2 à 5 ans	5 à 15 ans	TREND
Technicien support (helpdesk/infrastructure/site proximité)	18 - 26	24 - 33	30 - 45	→
Technicien d'exploitation	23 - 27	26 - 30	55 - 70	→
Administrateur systèmes/réseau	30 - 36	34 - 40	38 - 60	→
DBA	37 - 45	42 - 55	50 - 70	↑
Ingénieur/Responsable systèmes	35 - 45	40 - 60	60 - 90	↑
> Ingénieur cloud	40 - 50	50 - 65	> 65	↑
Ingénieur/Responsable systèmes	35 - 45	45 - 60	60 - 90	↑
Delivery Manager/Service Manager	-	45 - 60	60 - 90	↑
Responsable bureautique	-	45 - 65	65 - 90	→
Responsable support/helpdesk	-	40 - 60	60 - 90	→
Architecte technique	-	70 - 80	80 - 100	↑

RÉMUNÉRATION ANNUELLE BRUTE EN K€

ÉTUDES & DÉVELOPPEMENT	0 à 2 ans	2 à 5 ans	5 à 15 ans	TREND
Technicien support applicatif	27 - 35	30 - 40	38 - 55	→
Ingénieur d'études et développement (C#, Net, Java, Php, JS, etc.)	38 - 45	40 - 60	55 - 70	↑
> Ingénieur DevOps	38 - 45	45 - 60	> 60	↑
AMOA/Business analyst	35 - 42	40 - 55	50 - 65	→
Ingénieur tests/recettes	35 - 42	40 - 55	50 - 60	↑
DBA	37 - 45	42 - 55	50 - 70	↑
Data Miner/Data scientist/Data analyst	35 - 45	45 - 60	55 - 70	↑
Product Owner	-	45 - 60	50 - 70	→
Scrum Master	-	45 - 55	50 - 65	→
Chef de projet fonctionnel (ERP, CRM, BI, etc.)	-	45 - 60	55 - 70	→
Chef de projet technique	-	42 - 55	55 - 70	↑
Responsable de domaine/Responsable SI métier	-	45 - 60	55 - 80	→
Architecte logiciel	-	70 - 80	80 - 100	↑

Un tableau des rémunératrions dans le secteur IT dans le rapport de Michael Page.

L'embellie est terminée

Après les années d'hyper croissance durant la pandémie avec un vaste jeu de chaises musicales entre les entreprises à la recherche d'experts rapidement opérationnels, une étude de Michael Page sur le même sujet que l'étude de Hays voit déjà cette année un retour à la normale pour les salaires, même si la course aux experts n'est pas encore terminée. Pour les postes moins stratégiques, le cabinet constate un processus de recrutement allongé pour recruter les bons profils et des salaires qui n'explosent pas. Il en est ainsi dans les fonctions support. Par contre, les profils de haut niveau vont continuer à croître fortement, particulièrement pour les architectes du SI et les experts en cybersécurité, note l'étude. Les autres profils recherchés sont les développeurs web applicatif, les chefs de projets SAP/Salesforce, les ingénieurs cloud, en data et machine learning. Ces profils ne sont pas forcément ceux qui touchent les plus gros salaires. Il faut ainsi relativiser leur importance pour les entreprises qui ne sont donc pas prêtes à faire banco sur ce type de poste.

L'étude constate par ailleurs qu'il existe toujours une forte disparité dans les salaires suivant les régions. L'Île-de-France conserve la palme des salaires les plus élevés devant la région Grand Ouest. Suivent Rhône-Alpes/Auvergne, le Nord de la France et la région Provence Côte d'Azur.

Bref un avenir radieux avec quelques nuages pour les salariés du secteur IT. ☐

B.G

www.linfocr.com

L'INFOCYBER-RISQUES

by L'INFORMATICIEN



Sécurité industrielle

Des équipements à (cyber)protéger

Sommaire

DOSSIER
Connectée, l'OT est en danger..... P. 74

OUTILS
Murena Fairphone 5 : un smartphone équitable sans Google ! ..... P. 81

MENACES
Des serveurs Gitlab victimes de cryptojacking et proxyjacking ..... P. 82
8Base, le groupe de l'été 2023 ..... P. 84
Bilan Cyber du 1er semestre 2023 : les attaquants accélèrent ..... P. 85

CONFORMITE
La Cnil consulte sur les traitements sensibles ..... P. 86
'Data Privacy Framework' : une bonne nouvelle, mais pas une solution parfaite ..... P. 87

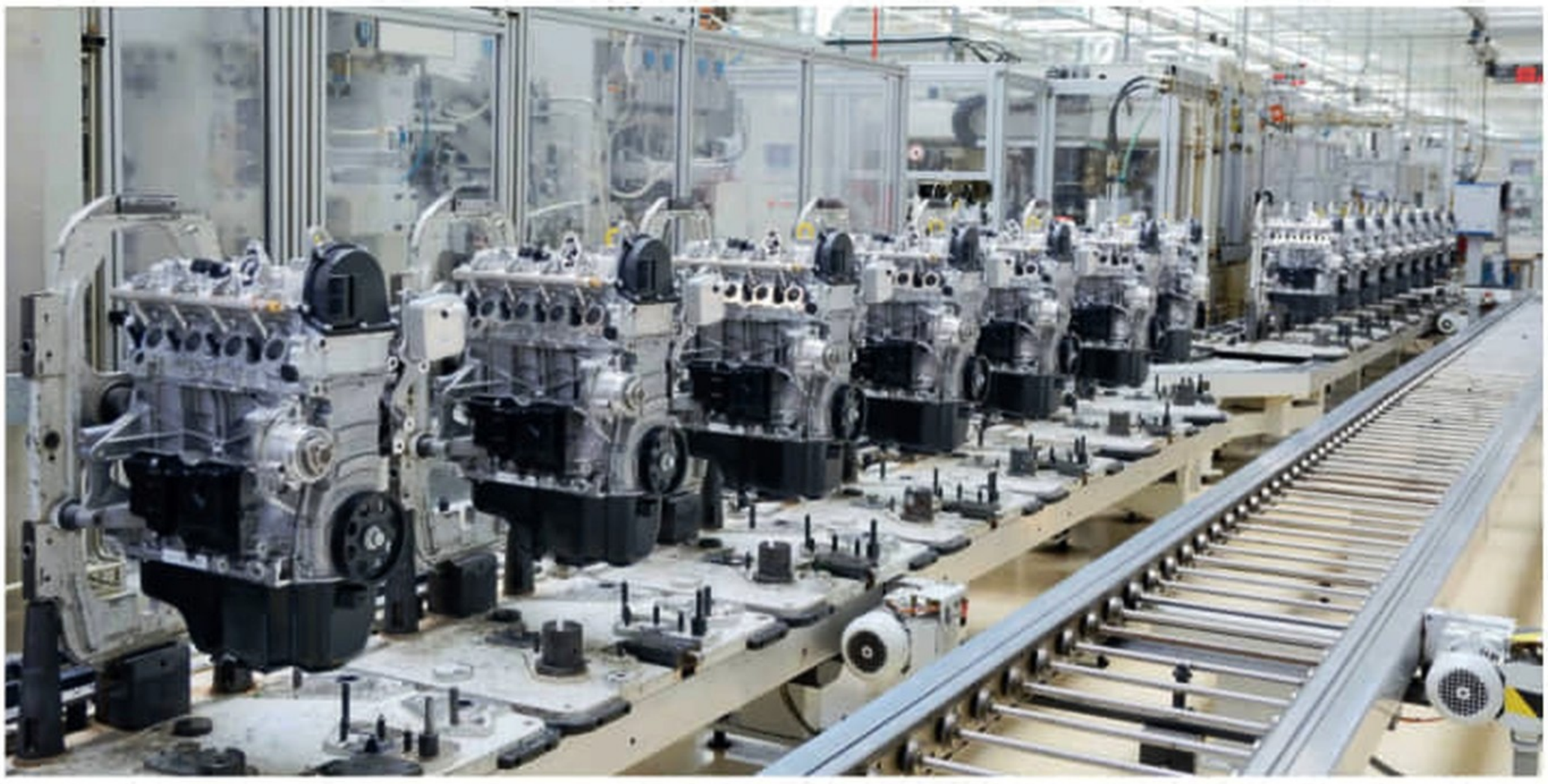
GOUVERNANCE
TikTok et ChatGPT ne sont pas la priorité des RSSI ..... P. 88
Assurance cyber : des conditions de souscription de plus en plus dures..... P. 89

ECOSYSTEME
FAL.CON 2023 : des outils pour mieux sécuriser le cloud et les app ..... P. 90

L'InfoCyberRisques prend le parti de descendre de quelques étages pour mettre les mains dans le cambouis. Le dossier de ce numéro est en effet consacré à la sécurité OT, un domaine dans lequel les éditeurs renforcent leur présence, mais où la prise de conscience sur le terrain ne fait que commencer. Pourtant, ce sont nos usines, nos hôpitaux, nos voies ferrées, nos centres de traitement des eaux qui sont touchés.

Comme le dit fort justement Amaury Ortega, responsable de l'activité cyber chez NTT, *« un ransomware qui touche un serveur, ça ne va tuer personne... »*. Mais un attaquant qui modifie la composition d'un médicament ou augmente la quantité d'un produit nocif dans l'eau potable, c'est autrement plus grave.

Connectée, l'OT est un danger

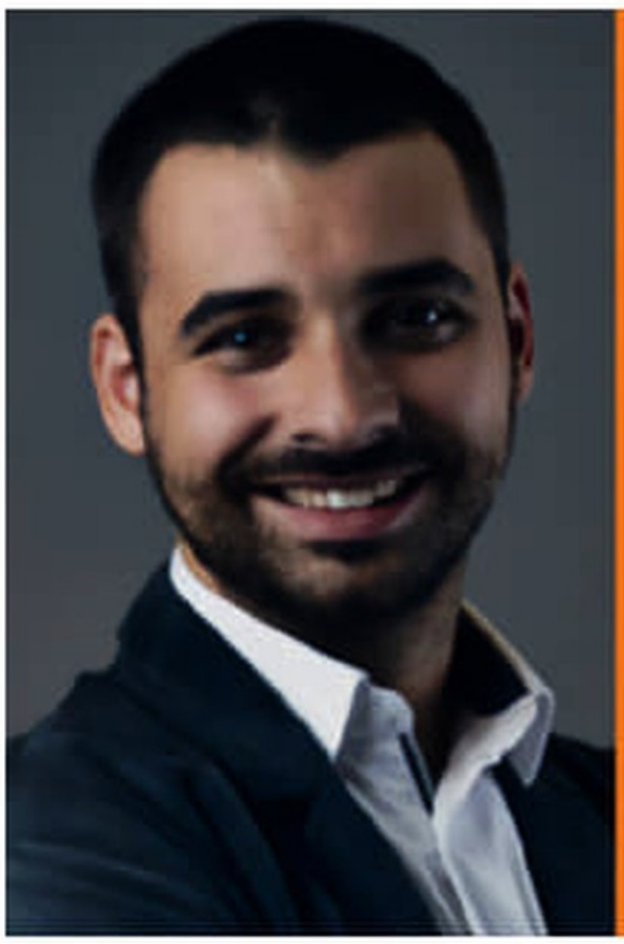


La convergence entre l'IT et l'OT étend aux environnements industriels la surface de menaces. Désormais exposés, les équipements sont aussi bien susceptibles de servir de porte d'entrée sur les systèmes informatiques que d'être ciblés par des cyberattaques, avec des conséquences potentiellement dramatiques.

On limite souvent l'OT aux seuls équipements industriels orientés production, machines-outils et robots en tête. Une définition bien trop réductrice, puisque la technologie d'exploitation concerne un vaste éventail d'équipements dans de nombreux secteurs, de la médecine à l'énergie en passant par l'aviation, le bâtiment ou encore le ferroviaire. Un système de contrôle des dosages de produits chimiques dans une usine de traitement des eaux usées, les climatiseurs d'une maison de retraite, une IRM dans un hôpital… tous ces équipements relèvent de l'OT. Si l'on veut définir plus large et schématique encore l'OT, on peut considérer qu'elle traite les équipements physiques, là où l'IT traite la donnée. À l'informaticien de l'IT répond l'automaticien de l'OT. Ce faisant, l'Operational Technology, ce ne sont pas seulement le matériel, les machines, mais aussi les technologies, protocoles, langages, logiciels et réseaux permettant leur fonctionnement. Et si, pour débuter ce dossier, nous opposons IT et OT, ce n'est en rien innocent.

Convergence

En effet, pendant fort longtemps, et jusqu'à très récemment, *« IT et OT étaient deux mondes différents, silotés, sans réelle porosité entre eux »* selon Amaury Ortega, Manager Business Development Cybersecurity chez NTT Ltd. France. Mais ça, c'était avant. Vincent Dély, Technical Sales Engineering chez Nozomi Networks, explique que *« dans un monde où les flux sont de plus en plus tendus, il faut pouvoir lancer la production dès que la commande arrive. D'où les interconnexions de plus en*



« On ne change pas un haut fourneau en sidérurgie tous les deux ans, comme on le ferait pour un serveur »

Amaury Ortega,
Manager Business Development Cybersecurity chez NTT Ltd. France.

plus fortes entre l'IT et l'OT ». Maintenance à distance, quand elle n'est pas prédictive, augmentation de l'efficacité de la production, de la qualité des produits grâce à la collecte de données industrielles, IIoT… les raisons ne manquent pas à relier IT et OT, on parle de convergence IT/OT, où les composants des systèmes industriels, contrôleurs et autres SCADA, vont être connectés aux systèmes et réseaux informatiques. Pourtant, si la convergence IT-OT vise l'amélioration des performances, elle provoque une augmentation considérable des risques cyber. En effet, un environnement industriel était par essence isolé du monde extérieur, se retrouve désormais connecté à Internet par le biais d'un réseau informatique. Or les appareils et systèmes OT n'ont, en règle générale, pas été conçus avec une sécurité informatique intégrée, parce qu'on supposait qu'ils ne seraient pas exposés aux menaces. D'autant que les équipements ne sont pas renouvelés, ni mis à jour, aussi

La réglementation, moteur de la sécurisation

Il suffit de jeter un œil à la liste des entités concernées par NIS2 pour comprendre que l'OT est en première ligne de la réglementation européenne. On trouve ainsi l'énergie, les transports, la santé, l'eau, la gestion des déchets, la fabrication, production et distribution de produits chimiques… *« NIS2, c'est vraiment la sécurité opérationnelle, le cœur du dispositif, c'est l'industrie, l'OT »* nous explique Marc-Antoine Ledieu, avocat spécialiste du numérique. Avec 10 000 entreprises concernées en France, une multiplication par 30 par rapport à NIS1, le champ des entités concernées est substantiellement élargie, qu'elles soient entités essentielles (EE) ou entités importantes (EI). Les nouvelles obligations, particulièrement détaillées quant aux mesures à mettre en place, au signalement d'incidents aux autorités ou encore de formations des dirigeants et collaborateurs, assorties à un régime de sanctions qui n'est pas sans rappeler le RGPD, accéléreront-elles la prise de conscience et la maturité des industriels ? Amaury Ortega le pressent, NIS2 *« va élever les standards de sécurité de nos clients »*. *« Une des premières choses qu'elle implique, c'est de mettre en place des politiques et des analyses de risques, donc il faut a minima connaître ses assets et par extension, travailler la réponse à incident »* note-t-il. Marc-Antoine Ledieu voit, quant à lui, un régime de sanctions plus efficace que dans NIS1 et, *« dans l'esprit, on vous oblige à organiser votre gouvernance, à vous former et à vous sensibiliser au risque. Enfin, vous devez prendre des mesures de sécurité techniques obligatoires qui permettent d'être à l'état de l'art. C'est une directive technique comme on n'en a jamais vu, un niveau de détails inédit : l'UE a pris un texte volontairement détaillé qui colle à 27 001 »*. D'autant que ces obligations sont vérifiables puisque quantifiables. L'avocat tempère toutefois le propos, puisqu'il manque dans NIS2 le dispositif touchant les prestataires, laissé à la charge des entités régulée. *« Un vœu pieu, peut-être, qui oblige de surveiller tout l'écosystème. Sur le papier, très bien pensé, mais il faut que ça monte au cerveau de tout le monde. Or, la cyber donne souvent l'impression que c'est du pognon dépensé pour rien »*. Et le juriste de conclure : *« ça va prendre, mais ça va prendre du temps »*.



Dans le secteur hospitalier, les équipements biomédicaux relèvent de l'OT, au même titre que le matériel régissant la température ou la pression dans les bâtiments. Autant d'appareils qui sont désormais connectés à Internet.

fréquemment que leurs homologues de l'IT. *« Un investissement OT s'investit sur 10, 20 ou 40 ans. Ce n'est pas du tout la même temporalité que l'IT : on ne change pas un haut fourneau en sidérurgie tous les deux ans, comme on le ferait pour un serveur »* souligne Amaury Ortega. Ce n'est pas la seule différence avec les environnements informatiques tels que l'on les connaît. *« L'IT, c'est un ensemble de protocoles relativement similaires, qu'on retrouve dans toutes les entreprises »* rappelle Vincent Dély. *« Dans l'OT, ce n'est pas le cas : il y a un caractère d'hétérogénéité très fort, avec un grand nombre de protocoles différents »*.

Surface d'attaque étendue

Et pour cause… dans les usines, les hôpitaux ou les sites de traitement des déchets, on trouve des équipements généralement propriétaires, divers et variés, qui n'utilisent pas les mêmes protocoles, là encore propriétaires. C'est une réalité d'un site à l'autre dans un même groupe, mais aussi au sein de l'usine elle-même, où les machines ne sont généralement pas standardisées et dont on ne sait généralement pas comment elles communiquent entre elles. Ce qui pose, de prime abord, quelques difficultés pour comprendre le fonctionnement de l'environnement OT, cartographier les assets et identifier les vulnérabilités. *« Lorsque nous arrivons chez un client, nous faisons l'inventaire, avec des sondes spécialisées pour lire la majeure partie des protocoles »* précise Amaury Ortega. *« C'est le premier sujet, et une grande partie des clients nous adresse sur cette partie-là : ils ne savent pas ce qu'ils ont, donc ils ne peuvent pas quantifier le risque »*. Or, les sondes elles-mêmes, comme tout nouvel outil intégré au réseau OT pour y collecter des données, ont longtemps été, et sont toujours dans certains cas, un risque en soi pour la production. Le premier enjeu de l'OT, c'est en effet la disponibilité : on n'éteint pas un robot sur une chaîne de production comme on rebooterait un serveur pour appliquer un patch. *« D'où, au départ, l'utilisation d'agents passifs, pour ne pas perturber le réseau tout en ayant la capacité de voir qui s'y trouve et quel équipement communique avec quel équipement »* se rappelle le Technical Sales

Engineering de Nozomi Networks. Vincent Dély signale néanmoins que la situation a évolué depuis les débuts de l'industrie 4.0 et que de plus en plus de sondes actives sont aujourd'hui adaptées aux environnements OT. Mais les enjeux de disponibilité et la temporalité demeurent des problèmes, et on trouve toujours dans les usines des postes d'opérateur, par exemple, sous des versions antédiluviennes de Windows, soudain connectés à Internet et au réseau informatique de l'entreprise. Cette faille peut être utilisée par un attaquant comme point d'entrée dans les systèmes informatiques d'une entreprise, mais un pirate visant l'IT d'une organisation peut également latéraliser et atteindre l'OT. Avec des conséquences autrement plus graves. Pour Amaury Ortega, *« en cas d'attaque, ce sont des problématiques qui peuvent impacter l'humain. On se rappellera, il y a quelques années, d'une attaque contre un centre de traitement des eaux aux États-Unis, où les attaquants avaient changé les réglages de l'ajout de produits chimiques qui, ultimement, se retrouvaient dans l'eau traitée. L'impact de la cyber dans le milieu industriel est critique. Un ransomware qui touche un serveur, ça ne va tuer personne… »*.



En 2021, aux Etats-Unis, une usine de traitement des eaux usées était victime d'une cyberattaque.

Des conséquences gravissimes

Certains contrôles ont pu éviter le pire, un niveau de seuil ayant permis aux agents de ce centre en Floride d'éviter que la teneur en hydroxyde de sodium, hautement corrosif en grande quantité, n'explose. Mais l'OT, ce sont des équipements vitaux dans des centres hospitaliers, tels que des pousse-seringues ou même la climatisation des salles d'opération, des centrales nucléaires, des raffineries, des chaînes de production de médicaments, des systèmes d'aiguillage ferroviaire… Autant d'équipements dont les dysfonctionnements peuvent avoir des conséquences en vies humaines. Évidemment, le ransomware reste un sujet de première importance, pour la simple et bonne raison qu'il touche directement la disponibilité et donc les chaînes de production. Même sans toucher l'OT, la paralysie par exemple d'un ERP ou d'un système de suivi des commandes peut affecter l'usine. On pensera aux cas de Norsk Hydro ou encore de Merck. La situation pourrait bien ne pas aller en s'arrangeant. Il y a en effet, selon le responsable Business Development Cybersecurity de NTT Ltd. France, *« une vraie velléité du marché à digitaliser »*, portée par l'industrie 4.0, la servicisation et une supply chain toujours plus connectée. *« Ce sont des enjeux métiers qui sont aussi des enjeux de transformation »* explique-t-il. Mais les sujets de transformation prennent du temps et la cybersécurité n'est pas nécessairement une priorité dans ces projets, malgré *« une prise de conscience, selon le niveau de maturité des clients, qu'elle est obligatoire »*. Un constat partagé par Vincent Dély, qui nous assure que *« la cyber ne fait pas partie des préoccupations principales des usines »*. Ainsi, les opérateurs sont un vecteur important de risque puisqu'ils manquent de maturité sur la cyber. *« On voit souvent en usine ce qui s'apparente à du Shadow IT, l'installation de systèmes pour se simplifier la vie, qui ouvrent des portes sur l'infrastructure OT »* note-t-il.

Maturité

Mais qui doit être en charge, côté usine, des aspects cybersécurité ? C'est la première question que NTT pose à ses clients et, souvent, ce sont des responsables IT qui vont vers l'OT dans une démarche de gestion des risques. C'est vrai, aussi bien d'un SOC interne que d'un RSSI. *« Si le CISO arrive auprès d'un patron d'usine avec cet état d'esprit, le projet va soit prendre énormément de temps, soit avoir du mal à être mis en place. Il faut vraiment qu'il y ait d'abord une volonté du top management à traiter ces problématiques. C'est la première chose. Ensuite, il faut identifier qui va être responsable des sujets cyber, car un projet sécu ne pourra pas commencer sans quelqu'un côté usine pour s'en emparer »* indique Amaury Ortega. D'autant que s'ajoute à l'aspect organisationnel la question des compétences, puisque *« généralement, la cybersécurité OT devient la charge des gens qui font de la sécurité IT »*, nous explique Vincent Dély. Or, on l'a bien compris, entre des efforts de standardisation tout naissants, des environnements



hétérogènes et des enjeux métiers bien différents de ceux de l'IT, mieux vaut pouvoir mettre tout le monde autour d'une table et que les RSSI aient une démarche qualité, bien comprise par les directeurs d'usine, qu'une démarche risque qui fait passer les responsables de la cybersécurité pour des empêcheurs de tourner en rond. Et, pourquoi pas, que la cyber devienne une part intégrante de la charte qualité d'une usine.

Une fois cette première étape accomplie, ce qui atteste déjà d'un certain niveau de maturité côté OT, on peut commencer à parler technique. La sécurité OT ne consiste pas à *« réinventer la roue »*, pour reprendre les termes de Vincent Dély. On retrouve dans les environnements industriels peu ou prou les mêmes types d'outils que dans les systèmes informatiques classiques. La démarche elle-même est similaire, puisqu'il faut avant tout une visibilité complète et approfondie du réseau, pour découvrir les anomalies évidentes (Shadow IT, mauvaises configurations, malwares déjà présents…), puis des actions qui vont découler de ces découvertes. On pourra ensuite réfléchir à de la détection en continu, pour détecter les vulnérabilités et les problèmes connus et inconnus. Donc du firewall, pour commencer, puis de la défense en profondeur, notamment l'inclusion des flux OT dans un SOC, pour les monitorer. Ensuite, la mise en place d'un EDR, puisque dans les environnements industriels, les stations d'ingénieur pour opérer les connecteurs dans une usine sont bien souvent sur des vieux serveurs, sur des vieux OS non patchés. Il reste donc à trouver des EDR susceptibles de fonctionner dans ces architectures et, par chance, les éditeurs s'engouffrent dans ce domaine et vont jusqu'à travailler avec les éditeurs de sondes. Après quoi on peut encore et toujours rajouter des couches, avec de la deceptive security, du pentest, la mise en place de bastions sur le plan de l'identité et de la gestion des accès. Mais ça, ce n'est pas pour tout de suite. *« Des clients industriels qui ont ce haut niveau de maturité, c'est un sur dix »* conclut Amaury Ortega.



« Généralement, la cybersécurité OT devient la charge des gens qui font de la sécurité IT. »

Vincent Dély,
Technical Sales Engineering chez Nozomi Networks.

CHU de Brest

Un environnement OT à défendre

Responsable de la sécurité informatique du CHU de Brest, Jean-Sylvain Chavanne nous dresse le portrait de l'OT en environnement hospitalier, ses enjeux et ses problématiques.

Dans le milieu hospitalier, l'OT est représenté par deux groupes distincts, mais d'égale importance : la GTB, ou gestion technique bâtimentaire, qui fait partie de la GTC (gestion technique centralisée) et gère les bâtiments, y compris la pression, la température, *etc.*, et tous les appareils biomédicaux, scanners, IRM, mécanismes pousse-seringues, pompe à insuline connectée, pacemaker connecté, dispositifs de suivi des patients, souvent RFID. *« La première chose pour le pôle SSI consiste à accompagner les pôles de l'hôpital en demande d'OT sur les spécifications cyber que doivent avoir les équipements, par exemple »* nous explique Jean-Sylvain Chavanne, RSSI du CHU de Brest et du GHT de Bretagne Occidentale. « Notre rôle est de faire en sorte que les équipements respectent les standards de cybersécurité.

Visibilité

Autre tâche du responsable cyber du CHU, avoir l'observabilité la plus exhaustive possible sur les équipements déployés. Pour les systèmes *« ultra-propriétaires »*, entendre par là de véritables boîtes noires sur le réseau de l'hôpital, le CHU a recours à des mécanismes de protection réseau, pour qu'il ne puisse pas y avoir de latéralisation possible sur le reste du périmètre de l'hôpital. Enfin, les pare-feux permettent de voir si un équipement communique avec d'autres, ou avec Internet, et si la connexion est légitime ou non. *« C'est une question de lisibilité et de visibilité sur notre environnement OT »* souligne Jean-Sylvain Chavanne. *« Aujourd'hui, il y a de plus en plus d'interconnexion IT/OT, c'est pour cette raison que nous essayons de rapprocher les exigences de sécurité OT de celles de l'IT. Ces équipements s'intègrent dans le système d'information, donc le plus difficile pour nous c'est de suivre le référencement des équipements ».*

« *Nous utilisons un EDR qui nous permet d'avoir une visibilité sur tout le système d'information, sauf les très propriétaires. Ainsi, on va avoir une visibilité sur le poste de travail qui commande l'IRM, mais pas sur l'appareil IRM lui-même. C'est une visibilité partielle, mais c'est déjà ça. Ensuite, nous avons un pare-feu périmétrique pour contrôler les flux entrants et sortants de l'environnement OT* » poursuit le RSS. Quant à la brique NDR, le sujet est, de son aveu, en réflexion. Pour la gestion des identités et des accès, la SSI demande « *au maximum* » aux équipementiers de s'interfacer avec son annuaire centralisé. Ce qui était « *compliqué* » il y a encore quelques années, mais est aujourd'hui de plus en plus « *simple et efficace* ».



« Un pousse-seringue ou la climatisation d'un bloc opératoire qui ne fonctionnent plus à la suite d'une mise-à-jour et qui requièrent un roll back, c'est un vrai risque. »

Jean-Sylvain Chavanne,
RSSI du CHU de Brest et du GHT de Bretagne Occidentale.

Les accès, ce n'est pas open bar

Ces différents outils n'empêchent pas des problèmes de perte de visibilité de l'environnement, un point crucial pour Jean-Sylvain Chavanne. « *Dans le cas de boîtes noires et de protocoles propriétaires, nous ne pourrons pas voir grand-chose, sinon ouvrir le port et vérifier si le matériel fonctionne correctement. Or, de plus en plus d'éditeurs demandent une ouverture sur Internet pour des questions de surveillance et de maintenance proactive, c'est le cas notamment pour tout ce qui est imagerie médicale, et aussi pour de la remontée statistique d'utilisation de leurs appareils. Et ça, ça nous pose un problème, parce qu'il est hors de question que nous donnions des autorisations wild cards à des équipements qui sont connectés à Internet : ce sont donc des autorisations au cas par cas dans le pare-feu* ». Car de moins en moins d'éditeurs biomédicaux viennent sur place pour intervenir sur des machines, ce qui nécessite un accès à distance H24 sur le CHU. « *Un risque en soi* », estime le RSSI. « *Nous avons mis en place la double authentification, le whitelisting IP et la ségrégation de ressources, grâce à un micrcloisonnement logique. Nous ne laissons pas d'accès permanent, à quelques exceptions près, avec des mesures de sécurité ultra renforcées* ».

Aux yeux du RSSI, la principale menace qui pèse sur les équipements OT est une interruption de service, causée par une surcharge réseau. « *Les attaquants visent plus l'IT, parce qu'ils maîtrisent mieux ces environnements. L'OT peut servir de point d'entrée sur le CHU, parce que les équipements sont connectés à Internet et les vulnérabilités ne sont pas patchées. Ça c'est la principale menace, d'où l'importance des matrices de flux* ».

Le patching est un sujet en effet très complexe puisque l'OT dans le milieu hospitalier est très lié au patient. Rappelons à toute fin utile que le déploiement de correctif est une procédure, non seulement de mise à jour, mais aussi de roll back en cas de dysfonctionnement. « *Un pousse-seringue ou la climatisation d'un bloc opératoire qui ne fonctionnent plus à la suite d'une mise-à-jour et qui requièrent un roll back, c'est un vrai risque* » indique Jean-Sylvain Chavanne. « *C'est pour ça aussi que les éditeurs sont très frileux, car ils ont du mal à savoir l'impact que ça peut avoir sur le fonctionnement de l'OT. Nous, nous sommes entre deux chaises : on veut faire en sorte que OT patché, corrigé, sécurisé, mais les éditeurs doivent tester longuement les patchs et garder possibilité de roll back* ».

De nombreux systèmes nécessitent en outre de fonctionner 24 heures sur 24, et 7 jours sur 7. « *Si on prend le cas de l'imagerie médicale, lorsque les appareils doivent être rebootés, nous n'avons pas beaucoup d'heures possibles pour interrompre le service. On a mis en place des process pour fluidifier, avertir les praticiens, se laisser de la marge de manœuvre. C'est quelque chose à laquelle on accorde une attention assez forte et que nous négocions avec les services en amont, puisqu'interrompre leurs systèmes sans les prévenir désorganise leur travail* ».

Du point de vue organisationnel, au CHU, un service d'ingénieurs biomédicaux fait l'interface entre OT et la DSI. « *Souvent, je fais des réunions avec eux pour leur expliquer les mesures de sécurité à exiger des éditeurs pour être conforme à la politique de sécurité. Ce sont mes interlocuteurs pour le biomédical. Pour la GTC, ce sont les ingénieurs des bâtiments du CHU. Là, on manque d'un interlocuteur, mais nous réfléchissons à une solution pour avoir un ingénieur qui puisse faire l'interface* » explique Jean-Sylvaine Chavanne. « *Il y a tellement de choses dans l'OT d'un environnement hospitalier qu'il n'est pas possible d'avoir un seul responsable. Moi, mon rôle, c'est de la sensibilisation et de la formation auprès de ces responsables. Je fais régulièrement des audits pour m'assurer du niveau de sécurité, et discute avec les responsables de ce qui peut être amélioré, toujours dans un but pédagogique* ». ▮

Effet de bord

La cyberattaque du 9 mars dont le CHU de Brest a été victime n'a pas affecté directement l'OT. Elle s'est arrêtée à une ferme RDS sur Internet. Puisqu'elle a été détectée assez tôt, avant la latéralisation, elle n'a pas eu d'impact sur les équipements. Cependant, par effet de bord, Internet ayant été coupé par mesure préventive, si les appareils fonctionnaient, ils ne pouvaient communiquer avec les éditeurs, faute d'ouvertures en télémaintenance et de remontées d'alertes. Et ce, pendant un mois. « *On a dû trouver des fonctionnements annexes avec nos éditeurs* » précise Jean-Sylvain Chavanne.

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

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

Murena Fairphone 5

Un smartphone équitable sans Google !



Avec le nouveau Fairphone 5, le fabricant néerlandais pousse son concept de smartphone écoresponsable encore plus loin. Plus puissant et plus durable que jamais avec ses dix modules remplaçables, l'appareil est désormais garanti 5 ans et bénéficie de mises à jour logicielles durant 8 ans ! Ce dernier se décline dans une version baptisée Murena Fairphone 5 dite « déGooglisée » ! Basé sur le système d'exploitation open source /e/OS, ce modèle permet de se prémunir de la collecte des données personnelles des services du géant du web.

Deux après le Fairphone 4, la société néerlandaise renouvelle son fameux smartphone modulaire unique sur le marché. Baptisé Fairphone 5, ce nouvel opus dispose, comme ses aînés, de composants modulables interchangeables permettant de le garder de nombreuses années au meilleur de sa forme en changeant soi-même si nécessaire les pièces défectueuses. L'appareil dispose de 10 modules que l'on peut acquérir sur le site officiel du constructeur tels qu'une dalle OLED, un port USB-C, une batterie, une coque, des capteurs photo, *etc.* Côté design, on est loin de l'effet « waouh » que peuvent provoquer les derniers terminaux mobiles d'Apple ou Samsung. Ce n'est pas l'effet escompté par le constructeur qui prône essentiellement son modèle éthique réparable conçu avec 70 % de matériaux recyclés. Le Fairphone 5 monte tout de même en gamme et abandonne l'écran LCD de son prédécesseur au profit d'une dalle OLED de 6,46 pouces. Protégée par un revêtement Gorilla 5, cette dernière affiche une définition de 1224 × 2770 pixels pour un contraste de 1000000:1 et une luminosité impressionnante de 800 nits. Le taux de rafraîchissement de 60 Hz par défaut peut heureusement être configuré à 90 Hz *via* le menu. Sous le capot, la configuration évolue également en passant d'une puce Snapdragon 750G à une Qualcomm QCM6490 2,7 GHz (8 cœurs) épaulée par 8 Go de mémoire vive. L'appareil dispose en outre de 256 Go de stockage pouvant être complété *via* une carte SD (jusqu'à 2 To).

Conçu pour durer...

Côté communication, sa compatibilité avec la 5G et le Wi-Fi 6E devrait lui permettre de fonctionner sans problème durant de longues années. Equipé d'une batterie de 4 200 mAh, le terminal offre une autonomie d'environ une journée en utilisation intensive et peut récupérer 50 % de charge en seulement 20 minutes. Capable de résister aux chutes, à la poussière et aux projections d'eau, il est certifié IP55 (contre IP54 auparavant). Le constructeur n'a pas lésiné sur la qualité du système photo qui se compose d'un capteur de 50 Mpx avec ouverture *ƒ*/2,45 à l'avant, et d'un combiné de capteurs (grand angle et ultra grand angle) de 50 Mpx à l'arrière (*ƒ*/1,88) avec un zoom x20 et un module Flash. Là encore, il ne faut pas à s'attendre aux prouesses d'un Pixel 7 Pro, par exemple, mais les résultats s'avèrent tout de même satisfaisants dans l'ensemble. Sans oublier la possibilité de réaliser d'excellentes séquences vidéo 4 K à 30 images par seconde.

Android sans Google !

Strictement identique en termes de configuration, la version Murena Fairphone 5 « déGooglisée » est basée sur le système d'exploitation /e/OS (une forme épurée d'Android 13). Le fabricant a supprimé tous les logiciels de Google connus pour convoiter les données des utilisateurs au profit d'applications open source capables de répondre à tous les besoins courants : navigateur, courrier électronique, calendrier, cartes, appareil photo, *etc.* Au moins 5 années de mises à jour majeures du système d'exploitation sont garanties et l'entreprise s'engage à assurer 8 à 10 ans de support et mises à jour de sécurité. Disponible dans une seule configuration et 3 coloris (Matte Black, Sky Blue et Transparent Edition), le Murena Fairphone est affiché au tarif assez élevé de 769,90 € (contre 699,99 € pour la version classique). Le prix à payer pour un téléphone durable, réparable et libéré de l'emprise de Google...

Jérôme Cartegini

Caractéristiques Murena Fairphone 5

- **Système d'exploitation :** /e/OS Android 13
- **Processeur :** Qualcomm QCM 6490 (8 cœurs)
- **Mémoire vive :** 8 Go
- **Stockage :** 256 Go
- **Écran :** POLED de 6,46 » (1224 × 2770)
- **Interface de communication :** Wi-Fi 6E, Bluetooth 5.2, double Micro SIM, 5G
- **Dimensions (L x P x H) :** 161,60 x 75,83 x 9,6 mm
- **Poids :** 212 gr.
- **Prix :** 769,90 €

Des serveurs GitLab

victimes de cryptojacking et proxyjacking

Des attaques assez sophistiquées employant des techniques et des outils furtifs et évasifs ont été lancées contre des serveurs GitLab, les rendant vulnérables à de l'exécution de code à distance. Les pirates en ont profité pour mettre en place du cryptominage ainsi que de la monétisation de bande passante via un logiciel proxy.

Ce sont des chercheurs de la société de sécurité Sysdig qui ont donné l'alerte au sujet de cette campagne d'attaque de cryptojacking et de proxyjacking. Les logiciels malveillants utilisés sont des rootkits multi-plateformes avec de multiples couches d'obfuscation leur permettant le plus souvent d'échapper à la détection en abusant de services légitimes. « *Cette opération est bien plus sophistiquée que la plupart des attaques observées jusqu'alors* », ont déclaré les chercheurs de Sysdig. « *La plupart des attaquants ne se soucient guère du côté furtif mais plutôt de l'intrusion en soi. Les techniques et outils furtifs et évasifs employés dans cette opération rendent la défense et la détection de cette attaque bien plus difficile* ». Les attaquants à l'origine de cette campagne baptisée LABRAT par Sysdig recherchent des serveurs GitLab vulnérables à un problème de sécurité critique connu. Cette faille est répertoriée sous le doux nom de CVE-2021-22205. Elle provient d'un problème de validation des fichiers images traités par GitLab avec ExifTool et peut permettre le pire du pire : l'exécution de code à distance. Bien qu'elle ait été corrigée en avril 2021, elle reste exploitée dans de nombreuses attaques. En clair, les pirates trouvent encore de nombreux serveurs n'ayant pas installé la correction ou téléchargé une version récente pour s'en protéger.

Le service TryCloudflare compromis

Après avoir obtenu l'exécution de code à distance grâce à la faille susnommée, les crackers exécutent une commande curl qui télécharge et lance sur la machine compromise un script permettant d'accéder à un serveur de commande et de contrôle (C2) avec le nom d'hôte trycloudflare.com. Ce dernier est un service gratuit fourni par la société Cloudflare, qui n'a rien à voir avec ces truands, mais qui donne la possibilité à tout un chacun de tester les fonctionnalités de la plateforme. Les pirates en usent et en abusent pour obfusquer l'emplacement réel de leur serveur C2. Le CDN (réseau de diffusion de contenu) de Cloudflare sert en quelque sorte de proxy entre le « client » compromis et le C2. Le script malveillant commence par vérifier si le processus watchdog est en cours d'exécution et, si c'est le cas, tente de le tuer. Rappelons qu'un watchdog est une protection destinée à redémarrer le système si une action bien définie n'est pas exécutée dans un certain laps de temps. Le script supprime les fichiers d'éventuelles infections précédentes, désactive les mesures de défense diverses et variées, télécharge encore d'autres binaires malfaisants pour

CVE List • CNAs • WGs • News & Blog • Board • About • NVD Go to for: CVSS Scores CPE Info

Search CVE List | Downloads | Data Feeds | Update a CVE Record | Request CVE IDs

TOTAL CVE Records: 212420

NOTICE: Transition to the all-new CVE website at WWW.CVE.ORG and CVE Record Format JSON are underway.

NOTICE: Legacy CVE List download formats will be phased out beginning January 1, 2024.
New CVE List download format is available now.

HOME > CVE > CVE-2021-22205

Printer-Friendly View

CVE-ID

CVE-2021-22205 Learn more at National Vulnerability Database (NVD)
• CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information

Description

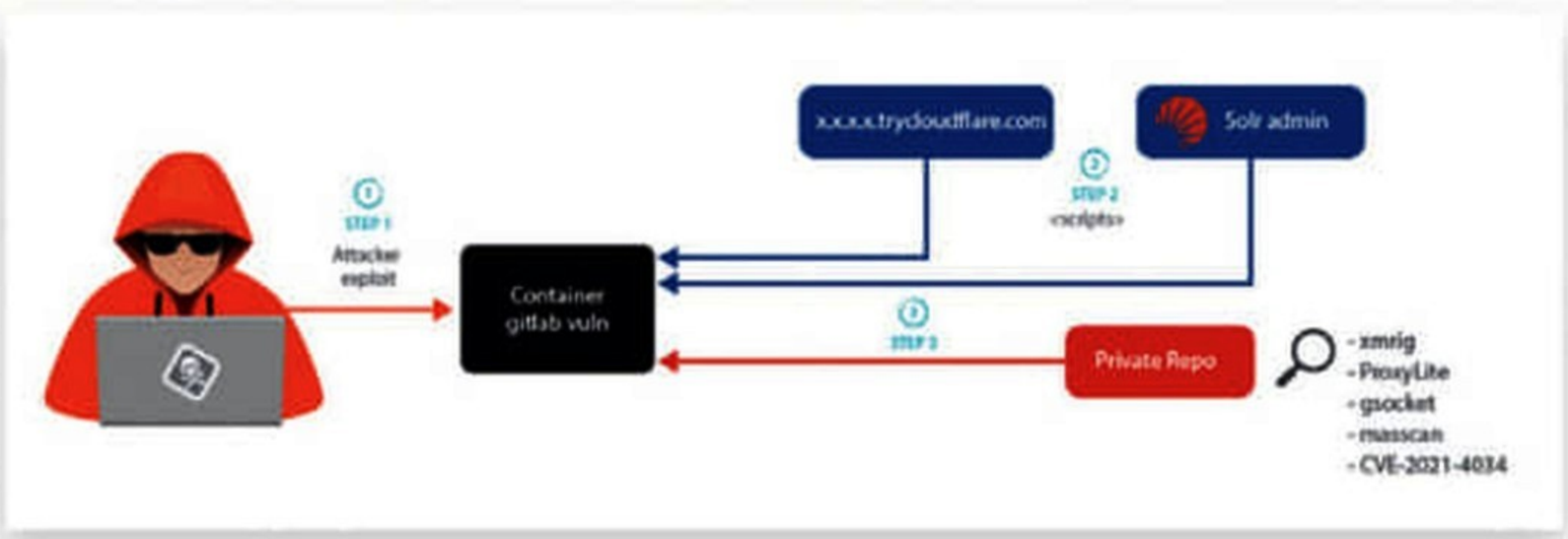
An issue has been discovered in GitLab CE/EE affecting all versions starting from 11.9. GitLab was not properly validating image files that were passed to a file parser which resulted in a remote command execution.

References

Note: References are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.

- CONFIRM:https://gitlab.com/gitlab-org/cves/-/blob/master/2021/CVE-2021-22205.json
- URL:https://gitlab.com/gitlab-org/cves/-/blob/master/2021/CVE-2021-22205.json
- MISC:http://packetstormsecurity.com/files/164768/GitLab-Unauthenticated-Remote-ExifTool-Command-Injection.html
- MISC:http://packetstormsecurity.com/files/164994/GitLab-13.10.2-Remote-Code-Execution.html
- MISC:https://gitlab.com/gitlab-org/gitlab/-/issues/327121
- URL:https://gitlab.com/gitlab-org/gitlab/-/issues/327121

not use TryCloudFlare, but a Solr server instead. The IP is listed as harmless in VirusTotal and it points to a webpage that appears to be legitimate. It is possible that this IP was compromised and was being used by the attackers. We found Chinese forums posts [1,2] reporting to suffer cryptojacking incidents that fit the LABRAT operation. These attacks used the same private GitLab repository seen in the previous attack.



In this case, the attackers downloaded a pwnkit (CVE-2021-4034) binary from the private repository to elevate privileges in addition to another file that now responds as 404.

finir le job et met en place de nouveaux services système. Il modifie ensuite les tâches planifiées (la crontab Linux) en vue de relancer des processus qui se seraient arrêtés et, enfin, collecte les clés SSH stockées en local pour s'en servir dans des attaques latérales contre d'autres systèmes reliés en réseau à la victime. Un bon petit travail de fourmi plutôt vicieux mais très efficace. Le déploiement par les attaquants du tunnel CloudFlare permet à ses utilisateurs d'exposer des services locaux *via* le réseau sécurisé de l'éditeur sans aucune modification des paramètres du pare-feu ni redirection de port. D'autres chercheurs, ceux de GuidePoint Security cette fois, ont signalé récemment une augmentation assez significative du nombre d'attaques utilisant ce vecteur.

Les outils des pirates

En analysant les attaques LABRAT, les chercheurs de Sysdig ont constaté que de nombreux outils « prêts à l'emploi » étaient employés, comme notamment GSocket (Global Socket). Ce logiciel open source permet à deux systèmes situés dans des réseaux privés différents de communiquer sans avoir à activer le suivi de port. Ceci est rendu possible grâce à un réseau de serveurs proxy employant des connexions chiffrées ainsi que le réseau Tor, ces deux éléments rendant la découverte de l'autre machine très difficile. GSocket est utilisé comme une backdoor (porte dérobée) afin de permettre aux hackers d'accéder à distance au système et de lui faire exécuter des commandes. Les pirates essayent également d'exploiter la vulnérabilité d'élévation de privilèges PwnKit (CVE-2021-4034) pour déployer GSocket en tant que service lancé au redémarrage de la machine sur les systèmes Linux et d'ainsi obtenir la persistance.
Un rootkit open source répondant au patronyme de hiding-cryptominers-linux-rootkit et conçu pour cacher les fichiers des explorateurs et les processus et l'utilisation de l'unité centrale des gestionnaires de tâches a aussi été utilisé par LABRAT. Son but final est de masquer les activités de cryptomining (ou cryptojacking). Ces attaques sont clairement destinées à rapporter de l'argent aux hackers. Le but recherché ici n'est pas le vol de données, ou du moins ce n'est pas le principal. C'est le cryptomining et le proxyjacking qui sont principalement visés. La monétisation des serveurs piratés passe donc par le déploiement d'une variante personnalisée du programme de minage de crypto-monnaie open source XMRig. Celui-ci est déployé par un loader écrit en Go. Il s'assure que le programme de minage est bien déployé en tant que service en usurpant le service légitime sshd (le « démon » SSH). Cela permet bien évidemment de complexifier sa détection. Les LABRAT ont hébergé leurs binaires malveillants sur un serveur GitLab privé en ligne depuis septembre 2022. S'il ne leur appartient pas, il est pour le moins compromis et employé à mauvais escient à l'insu de son propriétaire.

IPRoyal ou la location de type proxyjacking

Une autre méthode assez efficace pour gagner encore plus d'argent consiste à déployer un outil associé au service IPRoyal afin que les utilisateurs partagent leur bande passante avec d'autres moyennant la rétribution. Ils doivent pour cela déployer un logiciel proxy sur leur machine. Cette technique d'exploitation de systèmes compromis, baptisée proxyjacking, a le vent en poupe. Les chercheurs ont aussi découvert des fichiers associés à un autre service de proxy, ProxyLite. L'outil qu'il emploie, écrit en .NET Core, est multi-plateformes. Il a recours à des techniques d'obfuscation très avancées afin de rendre tant la détection que l'analyse plus difficiles. L'opération LABRAT est d'autant plus rémunératrice qu'elle dure longtemps. C'est ce qui motive son côté furtif. Le proverbe *« le temps, c'est de l'argent »* est, on ne peut plus vrai dans ce cas.

Thierry Thaureaux

8Base, le groupe de l'été 2023

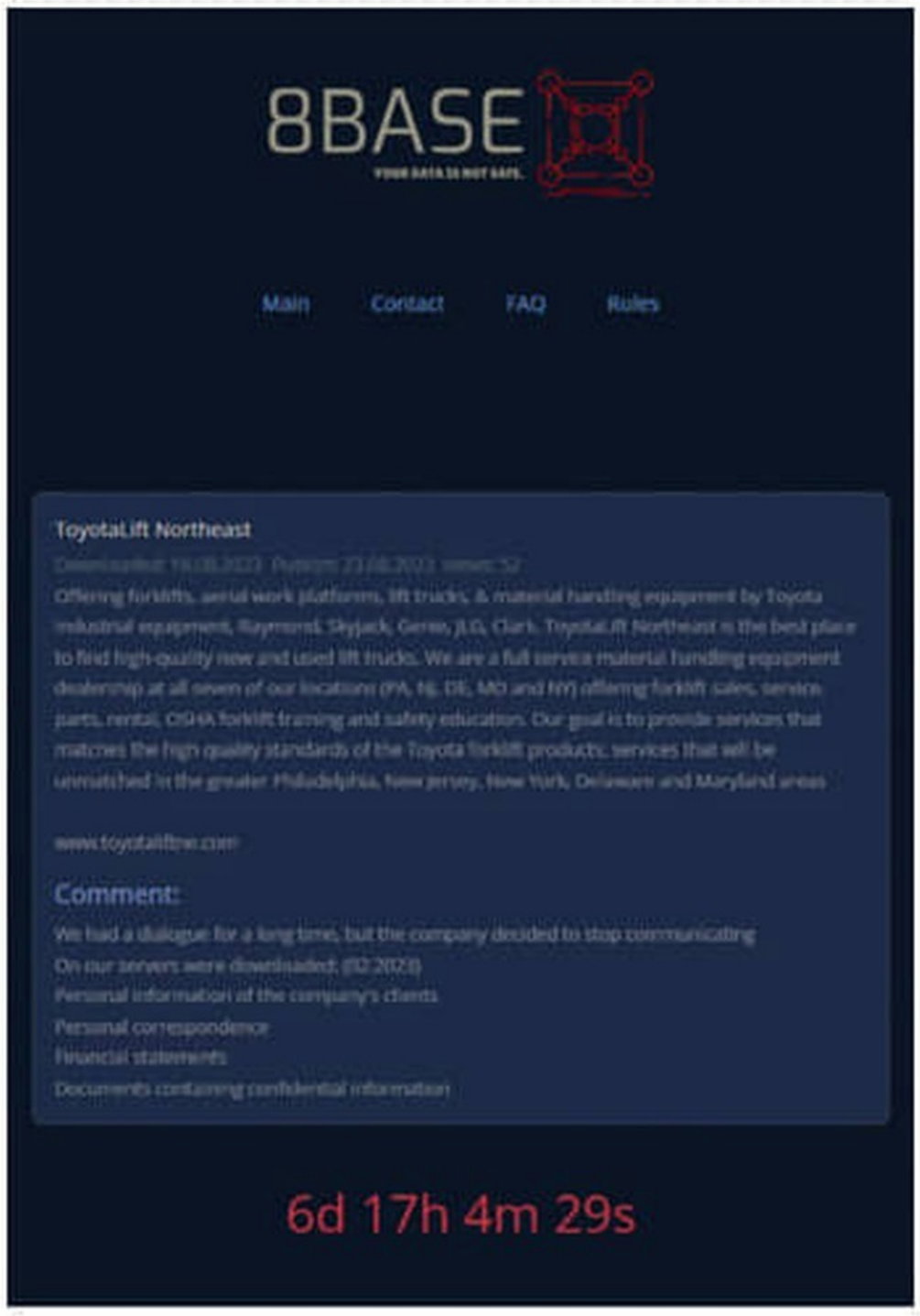
En quelques mois, le groupe 8Base s'est hissé au niveau des groupes les plus médiatisés du Dark Web. Ses attaques tous azimuts sur les PME ont attiré l'attention des chercheurs, d'autant que le groupe n'hésite pas à communiquer sur ses victimes.

Ce fut l'un des groupes dont on a le plus entendu parler au début de l'été. 8Base apparaît au Top 10 SOCRadar des groupes de Ransomware du mois de juin 2023, derrière les fameux Cl0p, Lockbit 3.0 et Blackcat. Jusque-là plutôt dans l'ombre, le groupe s'est brutalement retrouvé sous les projecteurs cet été. S'il ne s'est pas véritablement illustré sur un gros coup médiatique, c'est en accumulant les PME à son tableau de chasse et à cause d'un mode d'action très visible qu'il est sorti de l'ombre.

À en croire la Threat Analysis Unit (TAU) de VMware Carbon Black, le groupe serait actif depuis le mois de mars 2022. Son compte X baptisé Birdy / @BaseHome a été créé en 2014.

Ce groupe pratique l'extorsion par ransomware. Il exfiltre et chiffre les données de ses victimes avec l'extension .8base. Selon l'expert en malware Rivitna, 8Base utilise une variante du ransomware Phobos, mais le groupe semble utiliser de multiples autres outils, dont le kit issu du groupe Babuk, aujourd'hui retiré.

Le groupe est bien connu pour pratiquer le « Name and Shame » : si la victime ne se manifeste pas rapidement, auprès de son compte Telegram pour payer ou négocier sa rançon, le groupe publie son nom et la nature des données qui ont été dérobées. Le site Onion du groupe affiche ainsi les coordonnées des 160 entreprises qui n'ont pas payé leur rançon en temps et en heure. Début septembre, 6 entreprises avaient leur compte à rebours toujours en cours. Il s'agit pour l'essentiel de PME, des artisans en bâtiment, les agences de consulting, concessionnaires automobiles, les dératiseurs (!), des start-up. Le groupe agit de manière opportuniste et n'a pas à proprement parler de cibles de prédilection. De même, le groupe frappe dans de nombreux pays, les Etats-Unis, mais aussi la Chine, le Brésil, la France, l'Allemagne, *etc.* Seuls les noms de deux entreprises françaises, Pneumax et ANL Packaging, ont été dévoilés par le groupe, ce qui n'exclut pas qu'il ait fait d'autres victimes dans l'hexagone.



8Base n'hésite pas à publier sur X ou sur son site Onion les noms de ses victimes ainsi que la liste des données exfiltrées. Un moyen d'accroître la pression pour obtenir la rançon.

D'honnêtes « pentesters » ?

Très actif au début de l'été, le groupe 8Base a bénéficié de retombées médiatiques auxquelles ses membres ne s'y attendaient pas, comme l'atteste un tweet humoristique sur son compte X. 8Base est-il un groupe à part dans l'écosystème Cyber ? Le manifeste du groupe cherche à mettre en avant une certaine forme de professionnalisme, se présentant comme de simples « pentesters » honnêtes… Leurs victimes seront sans nul doute d'un avis différent, mais le groupe assure de sa loyauté garantissant le déchiffrement des données après versement de la rançon, assurer un support client pour le déchiffrement, l'effacement des données collectées, et même la suppression des backdoors exploités pour s'introduire dans le système informatique. Les chercheurs de VMware ont montré la grande similitude de cette documentation avec celle du groupe RansomHouse, évoquant la possibilité que 8Base soit une émanation de ce groupe ou des auteurs de Phobos. ▮

Alain Clapaud



Après avoir évolué à bas bruit depuis 2022, le groupe 8Base a connu un pic d'activité au début de l'été 2023. *Source : VMware*

Bilan Cyber du 1er semestre 2023

Les attaquants accélèrent

Accès distant, Active Directory, RDP, vulnérabilités anciennes non patchées, les menaces exploitées par les attaquants restent classiques en 2023. Par contre, ceux-ci ont nettement raccourci leurs délais de déclenchement des attaques.

Sophos vient de publier son rapport « *Active Adversary Report for Tech Leaders* », une synthèse de l'état de la menace Cyber au premier semestre 2023. Ce document intérimaire se base sur l'analyse des incidents collectés par l'équipe de réponse à incident de Sophos entre le mois de janvier à juillet 2023. Celle-ci montre un net raccourcissement entre le moment où l'attaquant pénètre le système et celui où il est détecté. Ce délai (Dwell time) est passé de 10 à huit jours pour toutes les attaques et à cinq jours pour les attaques de ransomware. En 2022, ce délai était passé de 15 à 10 jours. Cette accélération est absolument capitale quand on sait qu'il faut 16 heures à un attaquant pour atteindre l'Active Directory. L'AD est devenu une cible prioritaire, or il n'est souvent protégé que par Microsoft Defender, dans le meilleur des cas. En outre, les attaquants privilégient de plus en plus une attaque de type désactivation des défenses (T1562 dans le référentiel MITRE ATT&CK), une technique qui s'observe dans 43 % des attaques. Ce n'était le cas que dans 24 % des attaques en 2021.

L'accès distant reste la voie royale pour les attaquants

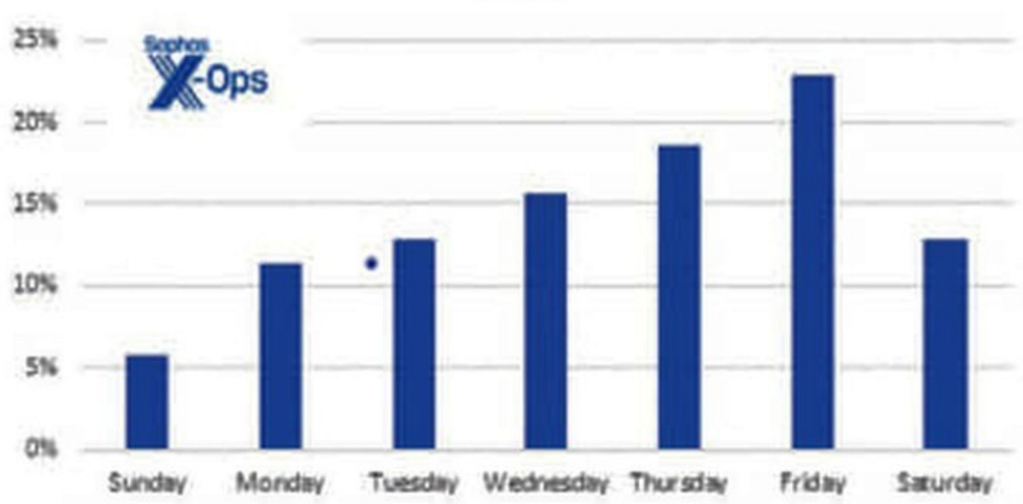
Pour accéder à un système, les attaquants exploitent divers moyens, à commencer par les accès distants type VPN, accès Citrix et équivalents. Attention, ceux-ci peuvent aussi tirer profit des API qui ne nécessitent pas d'authentification, notamment les API Docker ou Kubernetes. De même, toute interface utilisateur Web présente des vulnérabilités potentiellement intéressantes pour un attaquant. Dans 70 % des cas, l'accès illicite a mis en œuvre des comptes utilisateurs valides couplés à un service d'accès distant.
Sans grande surprise, le rapport montre que le protocole RDP est encore et toujours le protocole de prédilection des attaquants. Installé sur toutes les machines Windows, RDP représente un risque majeur s'il se conjugue à une authentification à un seul facteur et à une compromission d'identité. Le protocole est impliqué de près ou de loin dans 95 % des attaques !

Vulnérabilités : le calme après la tempête Log4Shell

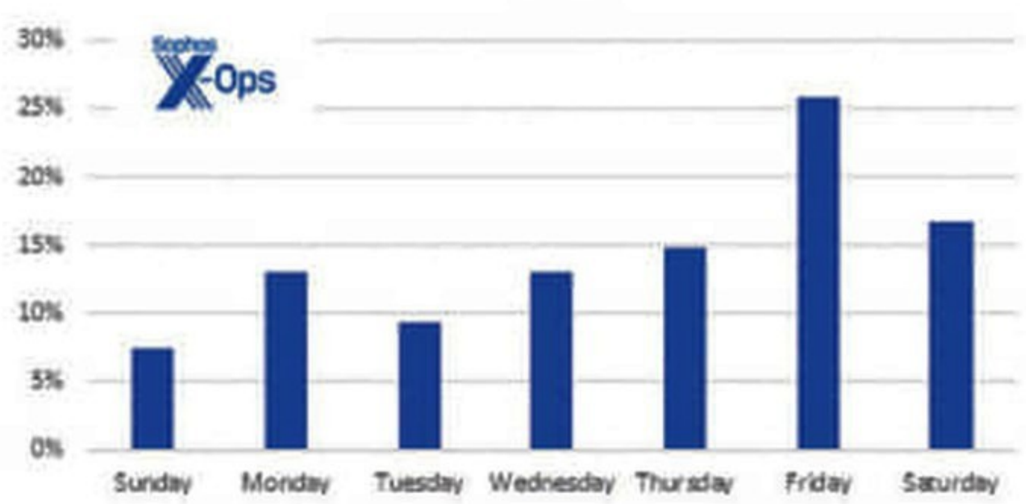
Après une année 2022 marquée par les vulnérabilités ProxyShell et surtout Log4Shell, 2023 s'avère plus calme. Néanmoins, outre l'exploitation de failles de sécurité bien connues comme ZeroLogon et ProxyShell, les attaquants ont exploité la faille Zoho ManageEngine (CVE-2022-47966), ProxyNotShell (CVE-2022-41080, -41082) ainsi que la vulnérabilité sur le logiciel de TOIP 3CX et sur PaperCut. L'étude réalisée par l'équipe Sophos X-Ops a montré qu'en ce début d'année, la technique de neutralisation des sauvegardes a été mise en œuvre (Inhibit System Recovery : code T1490 du framework MITRE ATT&CK). Cette technique était présente dans 18 % des attaques, tout particulièrement lorsqu'il s'agit d'une attaque par ransomware. Outre la corruption des sauvegardes, les attaquants cherchent à désactiver l'option Windows Recovery Environment (WinRE), détruire les sauvegardes automatiques réalisées par les firmwares, ainsi que les shadow backups. Autant de dégâts qui ne peuvent que renforcer la position de l'attaquant dans les négociations.
Enfin, l'exfiltration des données est avérée dans 43,4 % des cas d'attaques. Par contre, les analystes ne pouvaient affirmer qu'il n'y avait eu aucune exfiltration que dans seulement 9,2 % des attaques… ▮

Alain Clapaud

Attack Detected by Day of Week, 1H23



Attack Detected by Day of Week (ransomware), 1H23



Si le jour de l'accès initial de l'attaquant se trouve généralement en milieu de semaine, le déclenchement de l'attaque à bien évidemment lieu en fin de semaine, notamment le vendredi afin de compliquer la tâche des défenseurs.

Traitement critique

Du NIS2 dans le RGPD

Un projet de recommandation de la Cnil au sujet des traitements critiques est actuellement en consultation, pour une publication début 2024. Le document, tant par la forme que par le fond, n'est pas sans rappeler quelques textes européens en matière de cybersécurité.



Marie-Laure Denis, présidente de la Cnil.

La Cnil s'attaque au sujet épineux des « traitements critiques ». Dans un projet de recommandation, dont la publication est prévue début 2024, le gendarme français des données personnelles remet le RGPD au goût du jour, à la sauce NIS2/DORA. La règlementation européenne est d'ailleurs mentionnée dès le début du texte de la recommandation, le régulateur indiquant que son projet est susceptible de concerner *« les opérateurs d'importance vitale (OIV) »* de NIS1 et *« les entités dites essentielles et importantes »* de son successeur.

Deux critères

Sont désignés comme traitements critiques les traitements caractérisés par deux caractéristiques cumulatives. D'une part, *« le traitement est à grande échelle au sens du RGPD »* et de l'autre *« une violation de données à caractère personnel pourrait soit entraîner des conséquences très importantes pour les personnes concernées, soit entraîner des conséquences pour la sûreté de l'État ou pour la société dans son ensemble »*. Et la Cnil de lister les entités concernées, à savoir *« les secteurs de l'énergie, des transports, des banques et assurances ou la fourniture d'accès à Internet ; les services publics dématérialisés à grande échelle, que ce soit au niveau national ou régional, tels que les services des impôts, de gestion de l'identité, d'attribution des aides sociales ou d'assurance maladie ; les traitements de santé à grande échelle, [...] la fourniture de services nécessaires ou non à la sécurité de la population »*. Bref, le champ est large et devront suivre la recommandation tous ceux possédant une base de données ou effectuant un traitement des données d'une part non négligeable de la population française.

La Cnil explique vouloir *« accompagner au mieux »* les entités réalisant ces traitements critiques par cette recommandation, laquelle *« regroupe l'ensemble des pratiques avancées de sécurité qu'elle recommande de mettre en place »*. Effectivement, l'autorité énumère plusieurs mesures techniques et organisationnelles à mettre en œuvre pour assurer la protection des données concernées par ces traitements critiques. Un niveau de détails qui n'est, à nouveau, pas sans rappeler la directive NIS2. Le régulateur recommande ainsi que les entités concernées adoptent une démarche par les risques eu égard à leurs traitements critique, à commencer par la mise en place d'une analyse d'impact relative à la protection des données (AIPD) qui, rappelons, ne doit pas être une étude arrêtée dans le temps, mais un processus d'évaluation continu (ce que souligne la Cnil dans sa recommandation).

La Cnil entre dans le détail

En outre, elle conseille de privilégier une *« défense en profondeur »*, arguant que la sécurité *« ne devrait pas être assurée par une mesure unique, mais par un ensemble cohérent de mesures capables de parer à la défaillance d'une mesure unitaire »*. Et le gendarme des données personnelles de suggérer de prendre pour modèle l'approche Zero Trust. Le détail est poussé jusqu'aux sauvegardes et à leur restauration et la Cnil n'hésite pas à aborder la mise en place d'un SOC dédié aux traitements critiques et d'une CSIRT externe ou interne pour la réponse rapide à incident.

L'aspect organisationnel de la recommandation n'est d'ailleurs pas négligeable, puisque la Cnil veut que la responsabilité de la sécurité de ces traitements critiques soit directement portée par la direction générale des entités concernées. *« Cette dernière devrait s'assurer que des moyens suffisants sont mobilisés pour sécuriser les traitements critiques mis en œuvre et être régulièrement informée du niveau de sécurité de ces traitements par son responsable de la sécurité des systèmes d'information (RSSI) et par son délégué à la protection des données (DPD) »*. Le tout doit être assorti d'objectifs *« clairs, vérifiables, mesurables et cohérents avec les risques »* et un référent devrait être désigné pour chaque traitement critique. La sensibilisation n'est pas oubliée, puisque la CNIL recommande *« qu'une attention particulière soit portée à la sensibilisation à la sécurité informatique et à la protection des données à caractère personnel du personnel de l'organisme [...] Les connaissances essentielles au maintien en condition de sécurité des systèmes informatiques (par exemple, concernant le risque d'hameçonnage ou la sensibilité des données à caractère personnel) devraient être évaluées, afin de confirmer leur bonne prise en compte par le personnel. Une culture de la sécurité de l'information et de la protection des données à caractère personnel devrait être entretenue au sein de l'organisme »*. Le régulateur appelle en outre à sensibiliser aussi les prestataires.

La consultation relative à ce projet de recommandation est ouverte jusqu'au 8 octobre 2023.

G.P

'Data Privacy Framework' : une bonne nouvelle, mais pas une solution parfaite

Patrick Blum, Délégué Général de l'AFCDP.

Après l'annulation par la Cour de justice de l'Union européenne (UE) des deux précédentes tentatives, l'accord signé avec les États-Unis sur le transfert de données, le Data Privacy Framework (DPF) est, après une longue période de flou juridique, une bonne nouvelle pour les entreprises européennes qui ont besoin de partager des données avec des entreprises américaines.

Selon l'accord, les entreprises qui adhèrent au DPF sont réputées conformes en matière de traitement des données, et les échanges peuvent s'effectuer dans les mêmes conditions que pour une entreprise européenne soumise au RGPD.

Attention toutefois, cette solution n'est pas parfaite : elle ne signifie pas que les États-Unis sont un pays adéquat au sens du RGPD, comme le sont, par exemple la Suisse ou le Canada, où s'exerce une législation similaire au RGPD. Par conséquent, pour bénéficier des avantages du DPF lors de transferts de données, les entreprises européennes doivent vérifier que l'entreprise partenaire a bien adhéré au dispositif. Il faut pour cela consulter la base de données du Département du commerce américain (dataprivacyframework.gov).

À défaut, les échanges de données avec des entreprises non adhérentes doivent faire recours à des garanties appropriées, par exemple en signant des clauses contractuelles types selon les modèles établis par la Commission européenne, ou en utilisant tout autre outil listé à l'article 46 du RGPD, comme les règles d'entreprise contraignantes pour les transferts avec une filiale.

À noter : le DPF ne concerne que les entreprises. Par conséquent, les organismes comme les administrations ou les associations ne peuvent pas adhérer au DPF, et, là aussi, il est nécessaire de recourir aux options de l'article 46 du RGPD.



Une situation qui dure depuis 4 ans

Après l'invalidation d'un premier accord, le « Safe Harbor », la Cour de justice de l'Union européenne (CJUE) avait annulé le second, le « Privacy Shield » en juillet 2020 pour plusieurs raisons importantes.

D'une part, la CJUE a jugé que le Privacy Shield ne garantissait pas un niveau adéquat de protection des données personnelles des citoyens de l'UE, notamment en raison du programme de surveillance de masse mené par les agences de renseignement américaines révélé par Edward Snowden.

Elle a également estimé que les citoyens européens ne disposaient pas de recours juridiques adéquats aux États-Unis pour protéger leurs droits en matière de vie privée en contestant la collecte et l'utilisation de leurs données personnelles par les autorités américaines.

Enfin, la Cour a noté l'absence de garanties suffisantes et de limites claires sur la collecte et la conservation des données transférées depuis l'UE par les autorités américaines.

Plusieurs tentatives de solutions

Après l'invalidation du Privacy Shield, les entreprises qui transfèrent des données personnelles de l'UE vers les États-Unis ont dû revoir leurs pratiques et utiliser des solutions alternatives, notamment les clauses contractuelles types : certaines se sont tournées vers ces clauses pour sécuriser leurs transferts transatlantiques de données, et celles qui le peuvent ont mis en place des règles d'entreprise contraignantes pour leurs opérations internationales.

L'invalidation du Privacy Shield a également accru la pression sur les autorités américaines pour qu'elles engagent des réformes significatives en matière de surveillance et de protection de la vie privée, mais à ce jour, aucune loi fédérale n'a été adoptée, laissant comme seule solution la négociation du nouvel accord, établissant des négociations complexes pour élaborer un cadre susceptible de satisfaire la CJUE en cas de nouvelle contestation.

La protection des données personnelles est un enjeu clé pour l'UE, et le DPF est censé assurer un équilibre entre la protection de la vie privée des citoyens européens et la nécessité de faciliter les échanges de données internationaux pour les entreprises.

TikTok et ChatGPT ne sont pas la priorité des RSSI

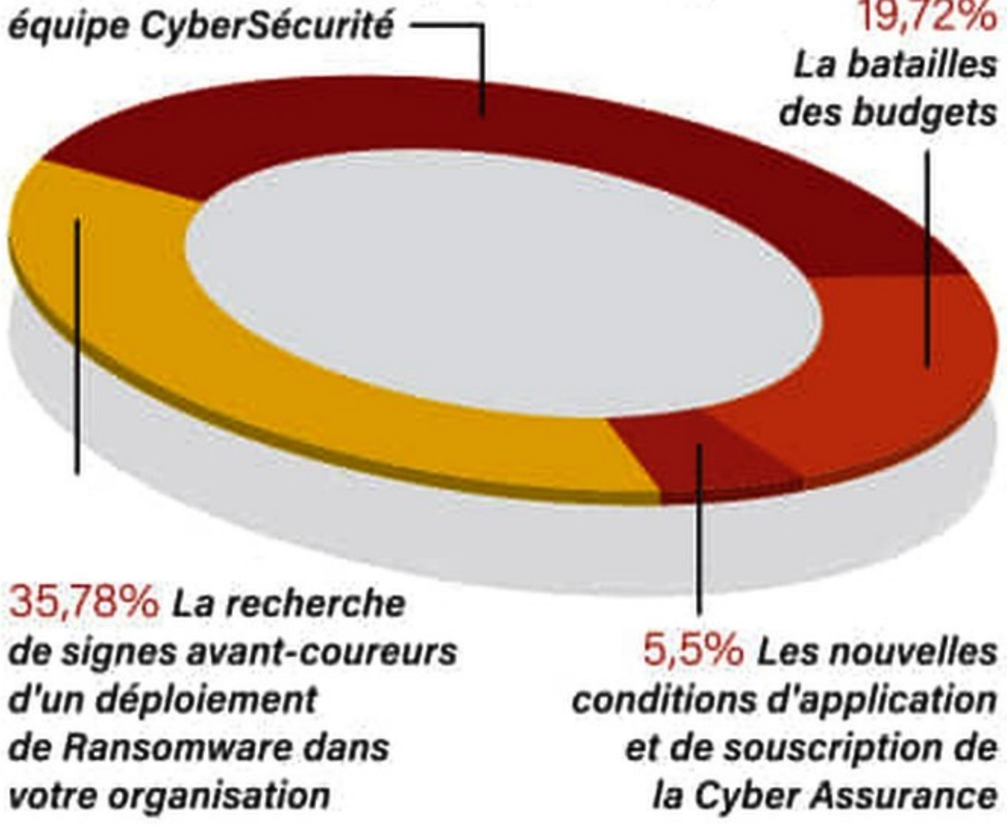
Quelles seront les priorités des RSSI en cette fin d'année et en 2024 ? Le cabinet Forrester a livré une liste de domaines dans lesquels investir, ou ne pas investir. Mais ses conclusions sont parfois aux antipodes de l'enquête menée par le CESIN auprès de ses membres.

Le dernier rapport « *Planning Guide 2024 : Security & Risk* » de Forrester donne un aperçu de ce que devraient être les priorités des RSSI en cette fin d'année, et pour l'année prochaine. Le cabinet d'analyse prévoit que l'année prochaine sera en partie consacrée à la sécurité des API, écrivant que « *les organisations devraient continuer à investir dans ce domaine pour soutenir les nouveaux modèles commerciaux et l'engagement des clients et des partenaires* ». La MFA, ou authentification multifactorielle, occupera elle aussi l'esprit des décideurs en cybersécurité, un mantra aussi vieux que le passwordless… qui n'a pourtant toujours pas poussé ce bon vieux mot de passe dans la tombe. Surtout, Forrester envisage un essor des plateformes de gestion des risques des tiers. À l'heure de NIS2, DORA et autres réglementations, la gestion des risques des tiers devrait effectivement être un élément majeur des évolutions de la SSI en 2024. Pour le cabinet, « *pour rompre le cycle de la réaction et des coûts imprévus liés à une violation par un tiers, les dirigeants devraient investir dans l'amélioration des processus et de la technologie pour la gestion des risques des tiers (TPRM)* ». Voilà pour les investissements recommandés. Quant à ceux qui vont tomber en désuétude, Forrester inclut l'engagement de conseil de faible valeur et, surprenamment, les outils autonomes de gouvernance, de risque et de conformité (GRC). Plus étrange encore, il recommande de diminuer ou d'éviter les investissements dans les appliances de sécurité sur site. Ce qui va à rebours des conclusions du CESIN. En effet, il ressort du questionnaire de l'association à l'attention de ses membres que 56 % des systèmes d'information on premises contre 22 % en mode IAAS/PAAS et 25 % en mode SAAS. Notons que cette synthèse des questions hebdomadaires qu'il pose à ses membres a été récemment publiée par le CESIN. Évacuons immédiatement les sujets à la mode. Les RSSI, du moins les adhérents à l'association, n'ont cure de TikTok et de ChatGPT. Pour l'application d'origine chinoise, ils sont 75 % à ne pas avoir pris de position, 10 % à recommander de ne pas l'utiliser sur les smartphones professionnels et un maigre 15 % à avoir techniquement interdit l'application sur les smartphones professionnels. Pour ChatGPT, 56 % n'ont pris aucune mesure particulière quant à son utilisation et 12 % l'ont « *autorisé sans autre questionnement* ». Seuls 5 % des RSSI l'ont interdit. Sur le côté souverain des solutions de cybersécurité, là encore, douche froide. Les RSSI utilisent en moyenne 15 solutions de sécurité. 70 % de ces solutions sont d'origine américaine, contre 30 % de solutions de nationalité européenne, dont 20 % sont françaises.

Près de la moitié des RSSI n'ont pas le moral

Les vrais sujets pour les RSSI sont ailleurs. Ainsi, 39 % ont eu pour principale préoccupation « *la recherche de nouveaux talents* » et le maintien de leurs experts dans leurs équipes. La recherche de signes avant-coureurs d'un déploiement de ransomware inquiète 36 % d'entre eux. Les questions budgétaires arrivent en troisième position, avec 20 % des répondants. Enfin, 5 % se disent préoccupés par les nouvelles conditions d'application et de souscription de la Cyber Assurance [voir notre article p. 89]. Également interrogés en début d'année sur leur état d'esprit, près de 57 % des RSSI affirment se sentir plutôt bien, dont 29 % qui se sentent dans un état d'esprit « *normal* » et 28 % « *être boostés avec un moral au beau fixe* ». Ce qui implique que, pour les 42 % restants, le moral est en berne, « *minés par le budget et/ou une charge de travail augmentée* ». « *On peut bien sûr s'interroger sur l'état de stress des RSSI au sein de la communauté et de manière générale, la profession en elle-même* » écrit le CESIN. L'association accorde une place importante à l'événementiel dans sa synthèse, partant du constat que le nombre d'événements et réunions cyber se multiplient. Face à cette croissance, 84 % des répondants font le tri et participent à un nombre limité d'événements, considérant que le calendrier des rencontres cyber est trop chargé par rapport au temps qu'ils peuvent libérer. D'autant que 47 % estiment que ces différents événements traitent souvent des mêmes sujets dans l'année et cherchent à éviter les répétitions. 53 % des RSSI participent à ces événements pour concentrer leur veille des produits et services sur quelques jours dans l'année et 63 % pour y rencontrer leurs pairs. 39 % limitent fortement leur participation à ces événements, déplorant une pression commerciale trop forte. ▮ **G.P**

En bilan de l'année 2022, quelles ont été vos **principales préoccupations** ?



Assurance cyber

Des conditions de souscription de plus en plus dures

Le taux d'équipement des TPE-PME en assurance cyber est en forte croissance, mais les assureurs risquent de durcir considérablement les conditions de souscription et d'augmenter leurs primes pour atteindre l'équilibre.

Le domaine de l'assurance cyber a toujours été compliqué. Les habitués de *L'InfoCyberRisques* le savent bien, le sujet est notre marronnier. Cependant, ces trois dernières années, le marché redresse la barre, sous l'impulsion des assureurs. En 2021, l'Amrae écrivait, dans son rapport LUCY (LUmière sur la CYberassurance) que les assureurs réagissaient aux problèmes du marché (difficulté d'évaluation de la sinistralité, écart prime/indemnité, *etc.*) non pas en l'abandonnant, comme certains mouvements l'avaient laissé penser l'année précédente, mais en durcissant les conditions de souscription. D'abord pour les grands comptes, avec un recul de la couverture assurantielle puisque, à taux de prime doublé s'ajoutaient réduction des capacités et augmentation des franchises. Mais ce segment est repassé dans le vert et l'Amrae prédisait que, l'année suivante, le durcissement se poursuivrait côté ETI. Et en 2022, bingo, les assureurs ont appliqué le même traitement aux ETI. Cette fois-ci, l'association des risk managers annonçait que, en 2023-24, ce serait au tour des petites et moyennes entreprises.

Et voilà que, plus tôt ce trimestre, une étude de Delinea enfonce le clou. L'enquête portant sur l'assurance cyber montre que, pour 67 % des répondants, leurs tarifs d'assurance ont bondi de 50 à 100 % au moment de leur demande de souscription ou de renouvellement. Dans le même temps, la liste des clauses d'exclusion, « *susceptibles de rendre la cyberassurance inopérante* », grandit. Les interrogés citent à 43 % l'absence de protocoles de sécurité, les erreurs humaines (38 %), les actes de guerre (33 %) ou encore le non-respect des procédures conformes (33 %). Notons qu'il faut faire attention au sens que l'on donne à « erreur humaine ». Cliquer sur un lien dans un mail de phishing, ce n'est pas une erreur humaine au sens assurantiel du terme, qui recouvre plutôt des erreurs de configuration ou de programmation.

Associer la prévention à la réparation

L'enquête a été menée aux États-Unis mais, comme nous l'explique Benjamin Mangel, Responsable souscription cyber assurance chez Stoïk, les tendances observables aujourd'hui outre-Atlantique arriveront chez nous dans les mois qui suivent. L'Amrae observe d'ailleurs que le nombre d'entreprises assurées a repris le chemin de la croissance : +25 % en 2022 (après une année 2021 à la baisse). Les entreprises de taille moyenne tirent la croissance, à +53 % contre 17 % pour les grandes entreprises et 12 % pour les ETI. « *Pour les entreprises de taille moyenne, la grande bascule est encore à venir : en 2022, le nombre d'entreprises couvertes a progressé de 53 %, dégradant la qualité du risque [...] On peut donc s'attendre à une correction moins sévère que sur le marché des ETI. Mais le niveau des capacités disponibles (2,30 M€) devrait se comprimer et le taux de prime augmenter (0,40 % en 2022)* » écrit l'association.

« *Il y avait un violent déséquilibre entre les primes d'assurances perçues et la sinistralité. Les assureurs ont réagi en revoyant en profondeur la façon de faire de la cyber assurance* » souligne Benjamin Mangel. « *Néanmoins, et malgré ce rééquilibrage, on pense chez Stoïk que ce n'est pas suffisant pour avoir quelque chose de pérenne. Ce sont des ajustements côté assureurs, mais il n'y a pas d'évolutions sur le fond du risque* ». Pour la jeune insurtech française, qui vient d'ailleurs de se lancer en Allemagne, il est nécessaire d'améliorer la posture de risques des entreprises : c'est la seule manière d'améliorer le ratio et de permettre la stabilité sur la durée. « *Cette thèse-là n'est pas sortie du chapeau, elle est inspirée d'un modèle qui fonctionne aux US avec des assureurs qui proposent ce type de valeur* » précise le Responsable souscription cyber assurance. « *L'idée d'introduire de la prévention dans les assurances cyber, ce n'est pas nouveau. Mais ce que l'on constate, c'est que ce sont ces ressources humaines et techniques qui sont mobilisées pour les grands comptes* ». Et justement, c'est le faible taux d'équipement sur le segment TPE/PME qui explique cette forte croissance observée par l'Amrae. D'où l'intérêt pour des acteurs tels que Stoïk, jouant à la fois sur le tableau de l'assurance et de la prévention, de placer leurs billes. **G.P**



« Ce sont des ajustements côté assureurs, mais il n'y a pas d'évolutions sur le fond du risque. »

Benjamin Mangel,
Responsable souscription cyber assurance chez Stoïk.

FAL.CON 2023

Des outils pour mieux sécuriser le cloud et les app

Du 18 au 21 septembre, CrowdStrike a rassemblé ses partenaires et sa communauté lors de sa convention Fal.Con 2023. Au programme : la présentation de nouveaux produits en cours de déploiement. Le spécialiste texan de la protection des données et du cloud a également annoncé la prochaine acquisition de Bionic.



© CrowdStrike

Plusieurs grandes annonces ont été faites durant Fal.Con 2023. George Kurtz, cofondateur et PDG de CrowdStrike, a notamment annoncé le rachat de Bionic, un pionnier de la gestion de la posture de sécurité des applications (ASPM).

Il faut croire que les spécialistes de la cybersécurité se sont donné le mot. Alors que Mandiant Google Cloud organisait mWISE à Washington du 18 au 21 septembre, CrowdStrike avait choisi la même période pour réunir sa communauté lors de Fal.Con 2023 à Las Vegas au Caesars Palace. L'occasion pour le poids lourd texan de la protection des données et du cloud de dévoiler plusieurs nouveaux produits et annoncer le rachat de Bionic, spécialiste de la gestion de la posture de sécurité des applications (ASPM) (voir encadré).

Parmi les nouveaux produits, CrowdStrike a présenté CrowdStrike Raptor, une évolution de la plateforme Falcon. Disponible progressivement depuis septembre, ce produit réunit la force de l'intelligence artificielle (Charlotte AI Investigator en l'occurrence) et une solution de détection et de réponse étendues (XDR) pour assembler des événements et des signaux connexes. Cette nouvelle offre comprendra aussi un centre de contrôle collaboratif des incidents. Cet outil peut être comparé à Slack ou Google Docs, car les équipes de sécurité des entreprises pourront se pencher sur les événements et incidents en temps réel depuis n'importe où. CrowdStrike Raptor fournira aussi des alertes ainsi que plus de ressources pour améliorer les enquêtes et les résoudre rapidement.

Dans un autre registre, Falcon Foundry est une version bêta d'une plateforme de développement d'applications sans code. Cette solution se destine aux acteurs qui souhaitent créer et partager des applications personnalisées exploitant les données, l'orchestration, l'automatisation, la réponse et les capacités de l'intelligence artificielle de Falcon. Également en version bêta, Falcon Data Protection devrait être disponible au quatrième trimestre. Cette solution se place au-dessus de Falcon pour réduire la charge de travail des utilisateurs. Selon Raj Rajamani, chef de produit de CrowdStrike, Falcon Data Protection permet aussi de suivre le contenu de fichiers sensibles *via* l'étiquetage et la localisation à la place du contenu.

Prévue pour 2024, Falcon for IT sera une offre à destination des équipes informatiques qui ne maîtrisent pas toute la chaîne de sécurité et qui gèrent de grands parcs informatiques. Enfin, Raj Rajamani a conclu son intervention sur Falcon Exposure Management. Déjà disponible, cette offre prendra désormais en charge les données de vulnérabilités produites par Qualys, un autre spécialiste de la sécurité du cloud. *« L'ajout de la prise en charge de Qualys améliorera encore la capacité d'évaluation des risques Falcon Exposure Management »*, a-t-il conclu. Bref, CrowdStrike s'apprête à intégrer une multitude de nouvelles fonctionnalités à ses solutions. Une stratégie qui répond clairement aux attentes des grandes entreprises qui font face à une multiplication des cyberattaques. *« Tout ce que nous faisons vise à aider nos partenaires à développer des pratiques autour de CrowdStrike, qu'il s'agisse de sécurité dans le cloud, de détection et de réponse des terminaux, de protection de l'identité ou de gestion des informations et des événements de sécurité »*, a souligné Daniel Bernard, directeur commercial de l'entreprise.

Michel Chotard

CrowdStrike Holdings **acquiert Bionic**

Durant Fal.Con 2023, CrowdStrike Holdings a annoncé l'acquisition de Bionic, l'un des pionniers de la gestion de la posture de sécurité des applications (ASPM). Ce rapprochement a vocation à étendre la plateforme de protection des applications natives dans le Cloud de CrowdStrike à l'ASPM. Ainsi, l'entreprise américaine entend offrir une protection complète dans le cloud (infrastructures, applications et services). *« Le cloud est le nouveau champ de bataille de la cybersécurité, mais la réponse de l'industrie jusqu'à présent a été des outils de sécurité ponctuels ou des plateformes avec de multiples consoles et agents. Nous offrons ce dont les clients ont besoin : une protection moderne pour traiter les risques de sécurité dans le cloud de manière complète, par le biais d'une plateforme unifiée »*, a déclaré George Kurtz, cofondateur et PDG de CrowdStrike.

ACCESSECURITY

SALON EUROMÉDITÉRRANÉEN
CYBERSÉCURITÉ & SÛRETÉ

06-07
MARS
2024

MARSEILLE
CHANOT

LE RDV BUSINESS & INNOVATION

Pour exposer, contactez-nous

accessecurity@safim.com

ACCESSECURITY.FR

#ACCESSECURITY



Cybersécurité Industrielle. **Simplifiée.**

txOne networks | Keep the Operation Running

Copyright © 2023 TXOne Networks. All rights reserved.

europe.txone.com/fr/france