N°222 — Décembre 2023 / Janvier 2024

www.linformaticien.com

L'INFORMATICIEN

Stockage
Tech Live, London

Logiciel
Open AI DevDay

RH
La CAIO prend sa place

Réseau
OAuth en débat

Cloud
AWS re:Invent
les annonces

PALMARÈS

LES MÉDAILLÉS 2023

L 14614 - 222 - F: 8,50 € - RD

Cybersécurité Industrielle. **Simplifiée.**

txOne networks | Keep the Operation Running

europe.txone.com/fr/france

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)
avec : Olivier Bellin, Pierre Berlemont, Patrick Brebion, Jérôme Cartegini, Michel Chotard, Alain Clapaud, François Cointe, Victor Miget, Guillaume Renouard, Thierry Thaureaux.

SECRÉTAIRE DE RÉDACTION : Boutheïna Saddi

MAQUETTE ET RÉALISATION : Franck Soulier (chef de studio)

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

VENTE AU NUMÉRO

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

ABONNEMENTS

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

Toutes les offres :
www.linformaticien.com/abonnement

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

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

IMPRESSION

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

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

ISSN 1637-5491

Une publication PCpresse,

GROUPE FICADE

PRÉSIDENT, DIRECTEUR DE LA PUBLICATION :
Gaël Chervet

Un événement devenu incontournable

La 3ème édition de notre Palmarès est devenue un événement incontournable pour les entreprises, comme en témoigne leur participation, de plus en plus soutenue. Le nombre croissant de votants atteste également d'un engouement grandissant. En quelques éditions seulement, le Palmarès de *L'Informaticien* s'est imposé comme un rendez-vous qui rythme l'année de l'industrie IT. Pour l'année prochaine, nous mettrons tout en œuvre pour que cette réussite soit encore plus éclatante, mais elle le sera surtout grâce à vous, la communauté qui se réunit autour de nos publications, et nous ne vous remercierons jamais assez pour votre soutien.

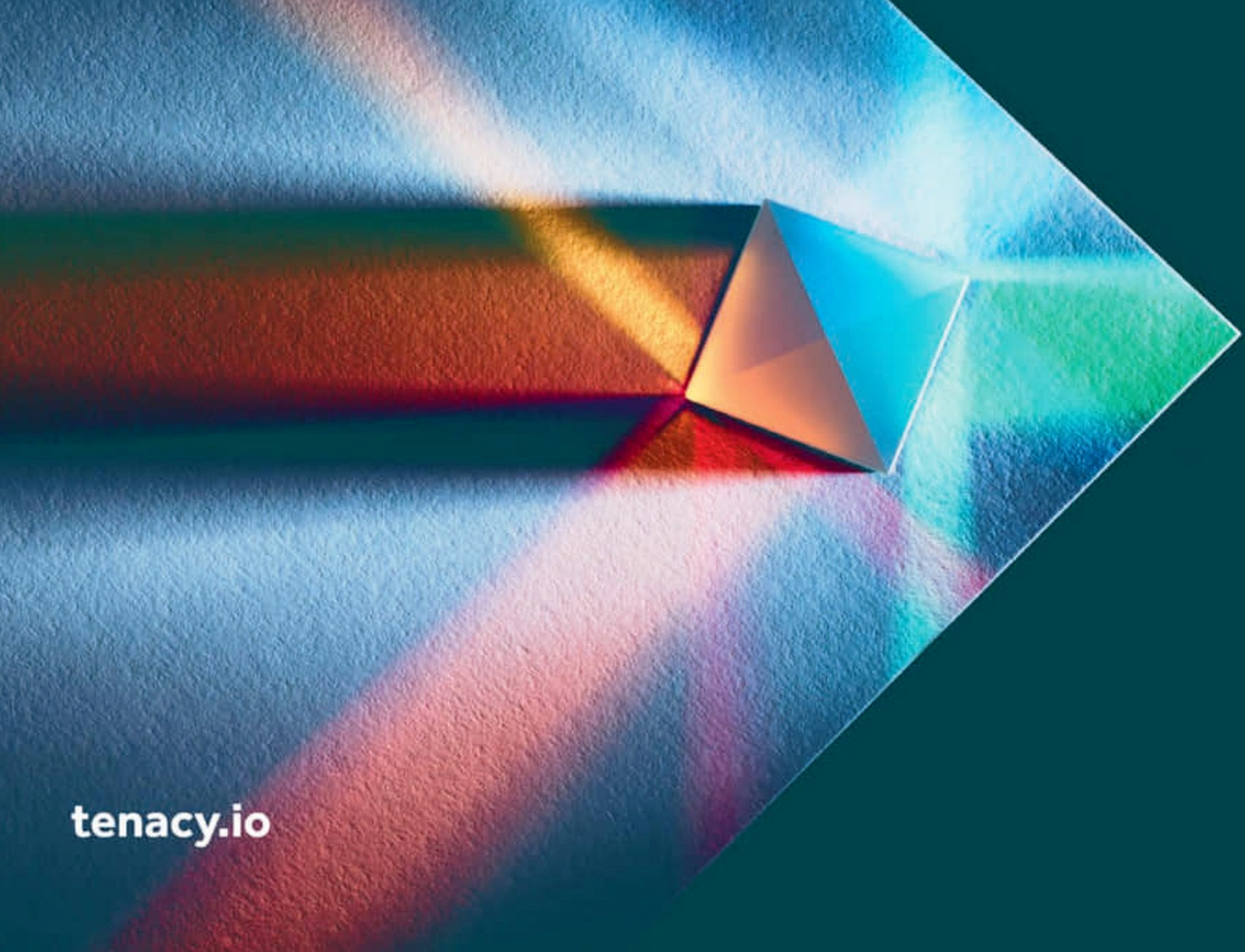
Après ce moment d'autopromotion et de satisfaction pour nos succès, notre numéro revient sur les principales annonces faites lors de grands événements tels que VMware Explore, AWS re:Invent, NetApp Insight, tout en abordant les sujets du moment, liés à la cybersécurité et à l'intelligence artificielle sous différentes formes.

Il ne me reste plus qu'à vous souhaiter de très bonnes fêtes, une superbe année 2024 et au plaisir de vous retrouver l'année prochaine autour de notre passion commune, la technologie et l'informatique. □

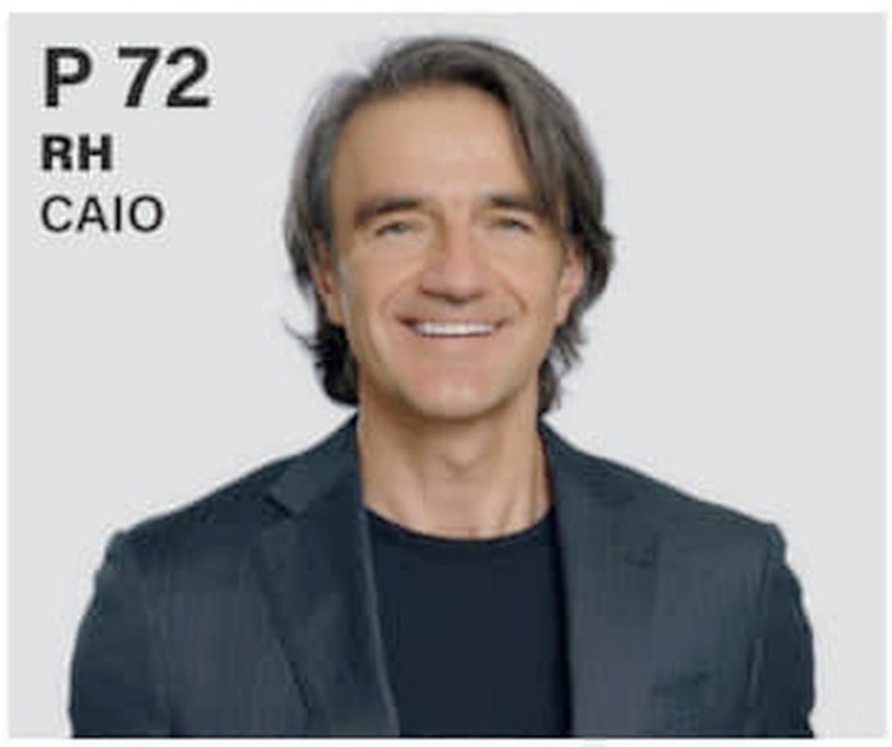
Bertrand Garé
Rédacteur en Chef

Tenacy

ALL YOUR CYBER IN ONE PLACE



tenacy.io



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

AU PARADIS DES LOGICIELS!

FOCUS

Sam Bankman-Fried condamné : les **cryptos** peuvent-elles souffler ?

Sam Bankman-Fried a été reconnu coupable de fraude et de blanchiment d'argent dans l'affaire FTX, qui avait accentué la tendance à la baisse du marché et la crise de confiance envers le secteur des cryptomonnaies. Si la tempête est passée, l'épée de Damoclès de la fraude n'a pas fini de planer sur la cryptosphère.

Le prince déchu de la cryptomonnaie, Sam Bankman-Fried, dit SBF, pourrait bien passer le reste de sa vie à l'ombre. Le fondateur et ex-patron de la plateforme FTX, autrefois le deuxième exchange de cryptomonnaies après Binance, a été reconnu coupable le jeudi 2 novembre 2023 de sept chefs d'inculpation de fraude, association de malfaiteurs, et blanchiment d'argent par un jury de New-York. Le juge fédéral Lewis Kaplan prononcera la peine de Sam Bankman-Fried le 28 mars 2024. Il encourt jusqu'à 110 ans de prison.

À la tête de FTX et d'une fortune estimée à plus de 25 milliards de dollars, tout souriait à Sam Bankman-Fried. Mais fin 2022, des bruits de couloir ont fait état de l'insolvabilité de la plateforme. Le média CoinDesk a dévoilé que la société d'investissement de SBF, Alameda Research, a converti une grande partie de ses actifs en jetons de FTX, le FTT. Ces révélations ont provoqué l'effondrement de la devise, entraînant de nombreux projets dans sa chute. SBF et sa clique ont, quant à eux, été accusés d'avoir utilisé les fonds des clients de FTX pour alimenter des transactions et placements à risque d'Alameda Research, des parrainages d'entreprises, ou encore pour couvrir les pertes de la société.

Ces révélations n'ont pas arrangé les affaires du secteur, déjà impacté par une baisse générale des marchés cryptographiques. Entre marché morose, corrections, scandales financiers, le tout ponctué de cyberattaques, la confiance des investisseurs a été largement entamée, plongeant un peu plus le secteur dans un hiver crypto dont il commence à peine à se relever.

Un coup *« vieux comme le monde »*

Tous ces éléments mis bout à bout ont donné du grain à moudre aux détracteurs des cryptomonnaies, leur reprochant leur opacité qui faciliterait des malversations de ce type. *« Sam Bankman-Fried a perpétré l'une des plus grandes fraudes financières de l'histoire américaine »*, a commenté le procureur Damian Williams. *« L'industrie des cryptomonnaies est peut-être récente avec des acteurs d'un nouveau genre, comme Sam Bankman-Fried, mais ce type de fraude, de corruption, est vieux comme le monde »*, a-t-il toutefois ajouté.

Comprendre : pas besoin de cryptomonnaies pour frauder. *« SBF, c'est du Madoff »*, pour Bertrand Godin, cofondateur & COO de Fipto, une plateforme de paiements internationaux et de gestion de trésorerie, basée sur la Blockchain. Et que ce soit en cryptomonnaies ou en monnaies traditionnelles, *« au vu de la façon dont les contrôles des régulateurs sont exécutés, ces fraudes pourront toujours arriver »*. À partir de 2024, le règlement européen Markets in Crypto-Assets, dit MiCA, par exemple, viendra encadrer les cryptoactifs en créant un cadre réglementaire européen censé mieux protéger les investisseurs. Combler un vide juridique suffira-t-il à éviter la fraude ? Non, selon Bertrand Godin : *« la régulation va professionnaliser la mise en place de certains contrôles, mais il y aura toujours un risque. Déjà, car il est difficile de contrôler en temps réel la légitimité de chaque virement. »*

Il existe bien des outils, comme la double signature ou les systèmes d'alerting, capables de sécuriser l'autorisation des transactions en compartimentant afin que plusieurs acteurs soient nécessaires pour valider les virements et que les accès dans les systèmes soient basés sur le principe du moindre privilège. Mais s'ils réduisent les risques, encore une fois, ils ne les éliminent pas pour autant. Quid de l'honnêteté des signataires en toutes circonstances ?

Les preuves de réserves on-chain ont aussi leurs limites. Sans compter la difficulté d'être réellement exhaustif au regard de la masse des transactions traitées. D'autant qu'il *« est toujours possible de créer des mécanismes qui n'auront pas été anticipés et permettront d'exploiter les vulnérabilités d'un système »*.

Altice vend des centres de données à Morgan Stanley

SFR, filiale d'Altice, exige 530 millions d'euros pour cette transaction, couvrant 70 % de ses 257 centres de données et espaces de bureaux dans le cadre d'un accord exclusif avec la banque Morgan Stanley. Les infrastructures et équipements passifs des datacenters seront transférés vers une nouvelle entité baptisée UltraEdge. Les serveurs et équipements actifs seront, quant à eux, conservés chez SFR. UltraEdge sera détenue à 70 % par la banque américaine et valorisée à environ 764 millions d'euros. Les 30 % restants reviendront à Altice.

La maison mère de SFR prévoit de conclure cet accord d'ici le premier semestre 2024 avec UltraEdge et espère générer 175 millions d'euros de recettes sur les sept prochaines années. Altice cherche à alléger sa dette de 60 milliards d'euros (Mds$) pour rassurer ses partenaires. Patrick Drahi en a fait une *« priorité absolue »*, alors que son entreprise est empêtrée dans un scandale de corruption au Portugal impliquant Armando Pereira, un proche collaborateur de Patrick Drahi et cofondateur d'Altice. Dans ce contexte, l'entreprise souhaite montrer patte blanche. Altice évalue actuellement ses actifs en Europe pour déterminer ce qui peut être vendu. Au regard du montant de sa dette, il est probable qu'elle se sépare d'autres actifs, et SFR n'est pas à l'abri. Prochaine échéance pour Altice ? L'entreprise de Patrick Drahi va devoir rembourser 1,65 Md$ de dette en 2025, 1,33 Md$ en 2026 et 5,5 Md$ en 2027.

Fibre : Orange condamné à 26 millions d'euros d'amende

Grosse sanction pour l'opérateur historique Orange. L'Autorité de Régulation des Communications Électroniques, des Postes et de la distribution de la Presse (Arcep) a infligé une amende de 26 millions d'euros à l'opérateur pour ne pas avoir respecté ses engagements en matière de raccordement à la fibre. *« Constatant le non-respect de la première échéance de ses engagements de déploiement en fibre optique en zone AMII, l'Arcep dans sa formation restreinte (dite "de sanction") prononce une sanction financière de 26 millions d'euros à l'encontre d'Orange »*, a écrit l'autorité dans son communiqué.

L'autorité a rappelé qu'au 31 décembre 2020, 100 % des logements et locaux à usage professionnel devaient être rendus raccordables ou raccordables sur demande. Orange avait été mis en demeure de respecter ses engagements le 30 septembre 2022. L'opérateur affiche un taux de raccordement de 88 % dans les AMII.

Orange a annoncé, mercredi 8 novembre, son intention de contester la sanction de l'Arcep et de saisir le Conseil d'État. Dans son communiqué, l'entreprise de télécommunications a écrit regretter *« que l'Arcep fasse le choix d'une sanction financière totalement disproportionnée à l'encontre de l'opérateur qui investit le plus dans le déploiement de la fibre en France »*. La sanction a été annoncée au lendemain d'un accord entre l'État et Orange dans lequel l'opérateur s'est engagé à déployer la fibre pour 1,5 million de foyers d'ici fin 2025 et d'atteindre un taux de raccordement de 98,5 % dans les zones AMII et de 96 %, dans les zones très denses, contre 91,8 % actuellement.

RACHATS

Proofpoint s'empare de Tessian

Le géant de la protection des emails a annoncé avoir conclu un accord définitif pour acquérir Tessian, une société spécialisée dans la Data Loss Prévention (DLP) dédiée aux messageries électroniques.
Fondée en 2013, Tessian s'est spécialisée dans la protection des messageries électroniques, principalement sur la partie DLP. Elle s'appuie sur de l'analyse comportementale pour détecter et prévenir les attaques par phishing, tout en automatisant des fonctions, comme le blocage des courriels envoyés aux mauvais destinataires ou contenant la mauvaise pièce-jointe par exemple.
Via cette acquisition, Proofpoint ambitionne de renforcer ses plateformes de protection de l'information et de protection contre les menaces. Comment ? *« En y ajoutant de puissantes couches de défense alimentées par l'IA qui ciblent les comportements à risque des utilisateurs, dont l'envoi de courriels aux mauvais destinataires et l'exfiltration de données »*, décrit l'entreprise dans un communiqué.
À l'avenir, Proofpoint souhaite développer une solution de défense et de protection, en associant ses propres ressources de données et ses capacités de détection à la plateforme de détection de comportement de Tessian. *« Le déploiement simplifié de ces nouvelles solutions et l'intégration native à Microsoft 365 et à Google Workspace permettront aux partenaires de Proofpoint d'en faire bénéficier immédiatement leurs clients »*, a indiqué Darren Lee, Vice-Président Exécutif et Directeur Général de la division Security Products and Services Group chez Proofpoint.

Broadcom a finalisé le rachat de VMware

Le spécialiste des puces réseau Broadcom a enfin scellé l'acquisition du spécialiste du cloud computing et de la virtualisation VMware pour 69 milliards de dollars. Le régulateur chinois a finalement donné son feu vert, mardi 21 novembre 2023. *« En mettant l'accent sur la réussite de nos clients, nous sommes ensemble bien placés pour permettre aux entreprises mondiales d'adopter des environnements de cloud privé et hybride, les rendant ainsi plus sécurisés et plus résilients »*, a déclaré Hock Tan, président et directeur général de Broadcom, cité dans un communiqué. L'opération avait mené à l'ouverture de plusieurs enquêtes antitrust à Bruxelles et à Londres. Les régulateurs craignaient que Broadcom puisse restreindre la concurrence et le principe d'interopérabilité en limitant l'accès aux solutions VMware.
La Commission européenne et l'autorité à la concurrence britannique (CMA) ont finalement donné leur accord après avoir obtenu des engagements de la part de Broadcom qui a notamment fourni des accès à son principal concurrent, Marvell.

Colt a bouclé l'acquisition de Lumen Technologies EMEA

Une nouvelle entité sur laquelle il va falloir compter est en passe de naître sur le vieux continent. L'opérateur Colt a indiqué avoir finalisé l'acquisition des activités de Lumen en Europe, au Moyen-Orient et en Afrique pour un montant de 1,8 milliard de dollars. L'entreprise de télécommunication avait signé un accord avec Colt en novembre 2022 pour la vente de ses activités EMEA pour 1,8 milliard de dollars. Activités qui viennent officiellement de passer sous l'étendard Colt Technology.
Colt compte 2 700 clients supplémentaires, 1300 nouveaux employés, 1 630 031 nouveaux kilomètres de fibre optique connectant 125 villes européennes dans 34 pays, 11000 kilomètres de réseaux métropolitains dans 23 pays du globe, 11 stations d'atterrissage de câbles et 10 systèmes de câbles sous-marins.

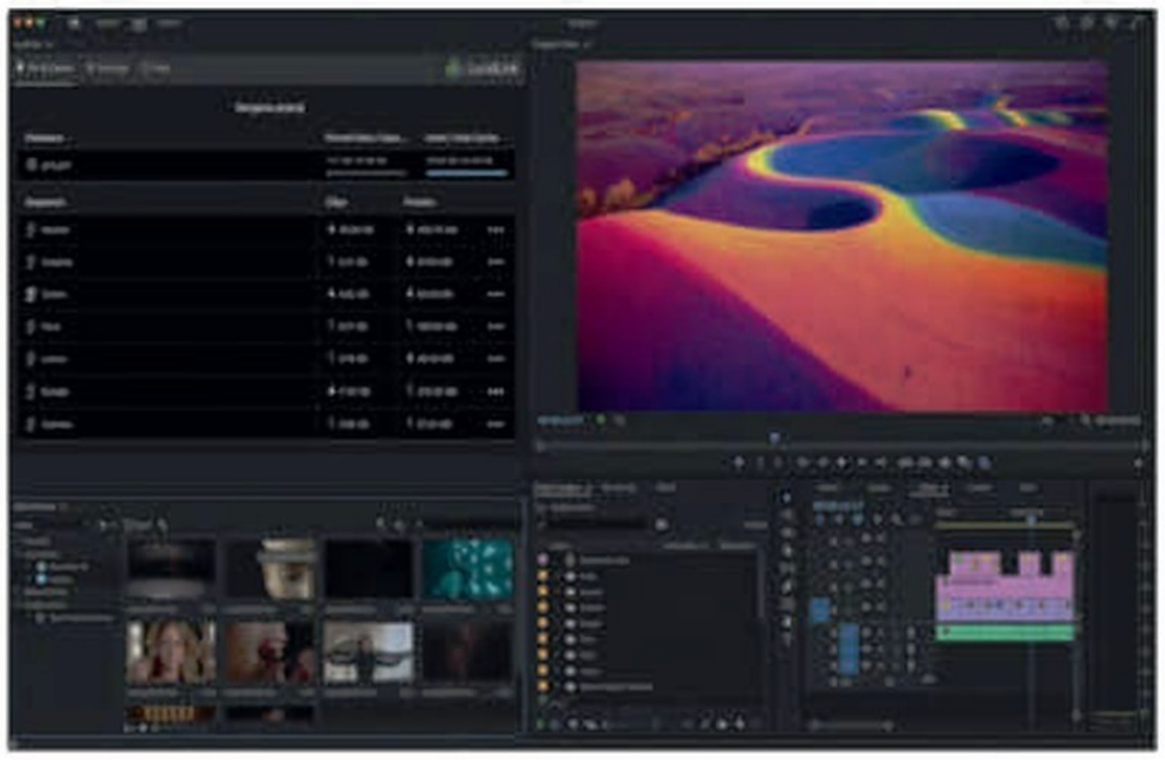
L'Union européenne va donner son accord pour le rachat d'iRobot par Amazon

Amazon a balayé les craintes des autorités antitrust, ou plutôt aspiré. D'après Reuters, Bruxelles est sur le point de donner son accord à l'acquisition par la marque à la flèche du fabricant d'aspirateurs robots iRobot pour 1,4 milliard de dollars. Les autorités antitrust, en Europe comme ailleurs, ont presque toutes donné leur feu vert, y compris la très sévère CMA britannique, qui a autorisé la transaction après un examen préliminaire. La Commission européenne se prononcera sur le dossier le 14 février prochain. Cet accord avait été annoncé initialement en août 2022. Il ajoutera les robots aspirateurs Roomba au portefeuille d'appareils connectés d'Amazon, qui comprend l'assistant vocal Alexa, des thermostats intelligents, des dispositifs de sécurité et des écrans intelligents. Plusieurs autorités réglementaires et des organisations s'étaient inquiétées de la capacité des aspirateurs du fabricant à cartographier les plans des logements des utilisateurs et du possible risque pour la concurrence.

Série A : **Truffle Capital** investit dans **Levenue**

Conjointement avec Freshmen fund, Truffle Capital investit 8 millions d'euros pour un tour de série A dans Levenue, une fintech belge qui édite une plateforme aidant les entreprises à revenus récurrents à se financer sans dilution des actions. Les fonds seront employés pour étendre l'extension géographique de l'éditeur, déjà présent dans 12 pays européens.
La France est la prochaine destination, avec pour cible le financement de start-ups tricolores. Cette ambition marque une étape clé dans l'élargissement de l'activité de Levenue. L'entreprise est en croissance rapide et a vu ses effectifs multipliés par trois en 12 mois. En intégrant des méthodes d'intelligence artificielle et d'apprentissage automatique dans ses solutions, Levenue a pu rapidement développer ses activités tout en maintenant son efficacité. Lors de sa prochaine phase d'expansion, Levenue, avec le soutien de l'expertise et du réseau Fintech de Truffle Capital, prévoit d'étendre ses opérations dans toute l'Union européenne et d'enrichir son offre.

Une Série C à **75 millions de dollars** pour **LucidLink**



L'éditeur d'une solution de partage de fichiers à haute performance réalise un troisième tour de financement d'un montant de 75 millions de dollars, mené par Brighton Park Capital, le bras armé d'Adobe dans ses prises de participation, accompagné de Headline et de Baseline Ventures ainsi que d'autres investisseurs institutionnels.
Ce tour de table va principalement servir à étendre la base installée de l'éditeur, avec l'idée de se développer sur de nouveaux marchés et d'accélérer les développements de produits. Cette levée est bouclée à un moment charnière pour l'éditeur qui a quadruplé son revenu récurrent lors des deux dernières années. Sa plateforme gère actuellement plus d'un milliard de fichiers pour des clients comme Adobe, Shopify et Spotify.

12 millions d'euros pour **DoorFeed**

DoorFeed est une Fintech française fondée par James Kirimy, qui développe une plateforme de gestion des portefeuilles de placements résidentiels destinés aux investisseurs institutionnels, en combinant intelligence artificielle et expertise en immobilier résidentiel. Elle vient de lever 12 millions d'euros de financement en Seed auprès de Motive Ventures, Stride et Seedcamp.

L'objectif est d'accélérer son déploiement dans l'hexagone et plus largement en Europe. Dans le détail, la plateforme *« permet de construire et d'opérer des portefeuilles sur mesure d'actifs résidentiels »*, en combinant IA, machine learning, et présence humaine locale. Elle analyse en temps réel quelque 100 000 opportunités d'investissement par jour en Europe, dont 30 000 en France.

Un demi-milliard d'euros pour **Aleph Alpha**

Ce n'est pas un scoop, l'IA générative est porteuse ces derniers temps. Preuve en est, le cycle de série B à 467 millions d'euros bouclé par Aleph Alpha. L'investissement a été dirigé par l'Innovation Park Artificial Intelligence (IPAI), auprès de sociétés comme Bosch Ventures et les sociétés du groupe Schwarz (Lidl) pour ne citer qu'eux.

Aleph Alpha est une entreprise allemande qui développe ses propres LLM ainsi qu'une API publique et se place en challenger des solutions américaines, la sécurité en plus.
« L'accord renforce la position d'Aleph Alpha en tant que fournisseur leader d'applications souveraines d'IA générative en Europe et prépare une production et une mise à l'échelle accélérées », a déclaré la société. Dans le détail, l'entreprise compte utiliser cette enveloppe afin d'investir dans la recherche sur l'IA et accélérer le développement et la commercialisation d'IA génératives pour les applications critiques et dans les secteurs sensibles comme la santé, la finance, le droit, le gouvernement ou encore la sécurité.

Orange et VMware rendent le SD-WAN flexible

Les deux entreprises étendent leur collaboration avec une offre SD-WAN nativement intégrée dans Evolution Platform.

En utilisant Evolution Platform, les entreprises ont accès à un catalogue de produits qui inclut à présent Flexible SD-WAN avec VMware, en utilisant soit une console en self-service soit des APIs. L'automatisation et le chainage des services de la plateforme visent à simplifier la gestion de l'infrastructure numérique, garantissant ainsi une connectivité sécurisée user-to-cloud et cloud-to-cloud, et une meilleure intégration avec les services de communication unifiée. De plus, la plateforme permet une visibilité et des garanties de performance de bout en bout. Flexible SD-WAN avec VMware prend en charge la connectivité, les applications et les équipements à l'Edge, en particulier lorsqu'ils sont sensibles aux performances du réseau. Elle assure une automatisation avancée et une expérience utilisateur optimale pour l'accès aux applications à distance, ce qui améliore la productivité des employés. Les équipements Edge sont autoconfigurés, réduisant à la fois les coûts informatiques et de déploiement. Les entreprises sont aussi en mesure de déployer des sites plus rapidement grâce à la 5G, le LTE, Wi-Fi ou le satellite. De plus, les utilisateurs profitent de l'étendue des points de présence d'Orange, stratégiquement situés sur le backbone mondial d'Orange, à proximité des utilisateurs finaux et des fournisseurs de Cloud.

ChapsVision et Capgemini partenaires

Les deux entreprises se rapprochent pour aider les organisations publiques et privées en matière d'analyse de leurs données hétérogènes dans un cadre souverain et de confiance.

Dans le cadre de ce partenariat, ChapsVision met à disposition sa plateforme Argonos dédiée au traitement sécurisé de la donnée massive et hétérogène, adaptée à tous les environnements (cloud ou datacenter client). En s'appuyant sur cette plateforme, Capgemini et ChapsVision pourront intervenir aussi bien dans la définition de cas d'usage pertinents que sur la chaîne de valeur complète du traitement de la donnée pour générer des analyses à grande échelle. Tout cela en assurant une maîtrise exhaustive des données dans un cadre de confiance.
Les principaux cas d'usages de la solution sont la lutte contre la fraude, l'escroquerie à l'assurance, le blanchiment d'argent, la désinformation, ou encore contre le trafic de cryptomonnaies.

Atos étend sa collaboration avec Microsoft

Partenaires depuis plusieurs années, les deux entités approfondissent leur relation pour aider leurs clients à accélérer le déploiement de Microsoft 365 Copilot et de l'IA générative.

L'organisation Tech Foundations d'Atos et Microsoft investiront sur une période de trois ans dans le développement d'un portefeuille stratégique et complet de solutions qui permettront aux organisations d'exploiter la puissance des données et de l'intelligence artificielle (IA) de manière sécurisée, efficace et éthique. Cette collaboration stratégique a été structurée autour de trois piliers fondamentaux : solutions, co-création et compétences. Le portefeuille actuel d'Atos en Digital Workplace (environnement de travail numérique) intégrera Microsoft 365 Copilot et Azure OpenAI Service.
Afin d'accélérer la mise en production, Atos et Microsoft fournissent à leurs clients des services de conseil, des accélérateurs de solutions ainsi qu'un financement pilote. Des projets sont en cours ou en phase d'expérimentation.

Equinix se rapproche d'Alice & Bob

Le fournisseur de solutions de colocation établit un partenariat avec la start-up dans le quantique.

Les clients d'Equinix vont avoir accès de manière sécurisée à la technologie quantique de la start-up au travers des offres Equinix Metal et Equinix Fabric. Equinix Metal est un service de serveurs physiques personnalisés (bare-metal) haute performance à la demande. Il peut être directement intégré à Equinix Fabric pour déployer une infrastructure multisites en quelques minutes. Il permet aux entreprises de se connecter, dans le monde entier, à des centaines de réseaux, de fournisseurs de communication, de sécurité et de cloud, le tout à partir d'une seule location. La combinaison de l'expertise d'Equinix en matière de sécurité optimale des opérations et du savoir-faire quantique d'Alice & Bob permettra aux entreprises de découvrir la puissance de l'informatique quantique en ayant la certitude que leurs recherches resteront totalement confidentielles. Pour rappel, Alice & Bob développe une technologie brevetée de bit quantique supraconducteur autocorrectif : le cat qubit.

Sopra Steria et Telefonica lancent un jumeau numérique du réseau

L'ESN et l'opérateur ibérique lancent un jumeau numérique (projet INA ou Intelligent Network Analysis) pour démontrer comment les technologies quantiques peuvent offrir une meilleure connectivité et une efficacité énergétique accrue du réseau mobile.

Cette simulation quantique, mise en œuvre avec succès sur le réseau de données mobiles de Telefonica, combine une cartographie en temps réel et la gestion dynamique du trafic au sein d'un même système. Elle permet d'accélérer et d'optimiser la planification des infrastructures, jusque-là effectuée manuellement par des opérateurs. En permettant d'effectuer de nombreux calculs en parallèle, le quantique offre désormais une analyse en temps réel des capacités du réseau pour fluidifier le trafic téléphonique. Le projet INA va également permettre de surmonter les problèmes de saturation tout en réduisant le nombre de redondances inutilisées. En identifiant les connexions potentiellement superflues et en réallouant la charge sur différentes parties du réseau, INA permet d'exploiter toutes les capacités du réseau, et ce sans nécessiter de mise à niveau matérielle ou d'extensions.
Telefonica en Allemagne s'apprête donc à réduire de manière significative son empreinte énergétique et environnementale, pour un réseau plus durable, tout en améliorant la qualité de service de ses utilisateurs mobiles.

SAS étend son partenariat avec Microsoft

L'éditeur de solutions analytiques va intégrer son logiciel de prise de décision dans Microsoft Fabric.

L'intégration de SAS Decision Builder dans Microsoft Fabric va aider les entreprises à surmonter l'étape critique de la mise en production de l'IA. Le logiciel de SAS permet de combiner facilement plusieurs modèles d'IA, règles et logiques procédurales dans un processus d'IA composite. Pour sa part, Fabric, en plus de fournir une base de données unifiée et des fonctions de gouvernance, il va ajouter un ensemble de capacités d'IA pour la prise de décision, et ce, à travers toutes les sources de données de Microsoft.

Scaleway renforce son offre d'IA

À l'occasion de la conférence ai-PULSE, Scaleway a réalisé plusieurs annonces afin de renforcer son offre autour de l'intelligence artificielle.

En premier lieu, Scaleway va proposer de nouvelles instances s'appuyant sur des processeurs Ampere sur architecture ARM. Les Ampere Altra vont autoriser Scaleway à proposer des instances performantes à des coûts moindres que des instances x86 au côté de puces graphiques. C'est la seconde annonce d'ai-PULSE avec une collaboration avec NVidia pour donner accès aux GPU, au logiciel NVIDIA AI Enterprise et aux services pour accélérer le développement des grands modèles de langage (LLM) et de l'IA générative pour les start-ups européennes. les startups recevront des crédits cloud pour accéder au supercalculateur d'IA de Scaleway avec 1 016 GPU NVIDIA H100 Tensor Core. Inception est un programme mondial gratuit qui fournit des conseils techniques, des formations, des remises et des opportunités de réseautage.


Le GPU H100 Tensor Core.

AGENDA

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

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

World Economic Forum
15-19 janvier 2024
Davos, Suisse

Mobile World Congress
26-29 février 2024
Fira Gran Via, Barcelone, Espagne

MPLS SD & AI Net World Congress
9-11 avril
Palais des Congrès, Porte Maillot, Paris

Paris Blockchain Week
8-12 avril 2024
Carrousel du Louvres, Paris

NAB Show
13-17 avril 2024
Las Vegas Convention Center, Las Vegas, USA

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.

PALMARÈS 2023

UN SUCCÈS CONFIRMÉ

La 3ème édition du Palmarès de L'Informaticien s'est déroulée le 20 novembre dernier dans les Salons Hoche à Paris. Nous avons accueilli près de 200 personnes représentant une large majorité de l'écosystème informatique présent dans notre pays.
Vous trouverez la liste des sociétés récompensées dans la page suivante. La cérémonie a débuté par un discours introductif de Gaël Chervet, président du groupe Ficade/Leaders League, lequel a présenté les différents métiers et secteurs d'intervention du groupe et dévoilé la future chaîne de télévision 4Change qui verra le jour au cours du premier trimestre de l'année 2024.
La soirée s'est poursuivie par la remise des prix aux nombreux lauréats des mains de Bertrand Garé, rédacteur en chef du magazine, accompagné de plusieurs personnalités invitées pour l'occasion.

Rappelons que le Palmarès de L'Informaticien récompense les entreprises sur la base d'un vote de nos lecteurs par le biais d'une enquête en ligne que nous avons menée durant le mois d'octobre 2023 auprès de nos lecteurs. Plus de 6000 votes ont été enregistrés dans les différentes catégories proposées.

Nous vous donnons d'ores et déjà rendez-vous l'année prochaine pour la 4ème édition, laquelle sera marquée par plusieurs nouveautés sur lesquelles nous reviendrons dans les prochains mois.

Catégorie	Sous-catégorie	Lauréat 1	Lauréat 2	Lauréat 3
CLOUD	Cloud public	AWS	OVH	Google
	Cloud privé	Nutanix	OVH	AntemetA
	Opérateur	NTT	Orange	OVH
	Collocation	Data4	Equinix	BT Blue
	Backup	AntemetA	Rubrik	Oxibox
	Hyperconvergence	Nutanix	Dell	HPE
APPLICATIF	Logiciels ITOM / ITSM	Easyvista	ServiceNow	Splunk
	Observabilité et monitoring	Splunk	Centreon	Dynatrace
	Logiciel CRM	Salesforce	Hubspot	Dolibarr
	Marketing Digital	Adobe	Hubspot	Salesforce
	Logiciel finance/comptabilité	Sage	Cegid	Odoo
	Logiciel Supply Chain	SAP	Sage	Oracle
	Logiciel RH	Workday	Payfit	iCIMS
	Logiciel ERP	IFS	Axelor	SAP
	IA/Analytics	Qlik	Tableau	
	Solution de partage de fichiers	Oodrive	Google	Microsoft
	Gestion de l'Information	Microsoft	Notion	Opentext
	Solution de gestion de contenus/documentaire	Hyland	Adobe	Box
	Gestion de projet/collaboration	Slack	Jamespot	Atlassian
	Solution de communication unifiée	Zoom	Slack	Sharekey
	Virtualisation	VMware	Nutanix	Splunk
SECURITE	SIEM	Sekoia.io	Splunk	Logpoint
	EDR	Harfanglab	WithSecure	Sentinel One
	NDR	Gatewatcher	Custocy	Sesame IT
	XDR	Sekoia.io	Tehtris	Crowdstrike
	IAM / PAM	Wallix	CyberArk	Okta
	Gestion de vulnérabilités	Tenable	Hackuity	Checkmarx
	Logiciels de protection des mails	Proofpoint	Sophos	Vade
	Logiciels de protection des données	Cohesity	Rubrik	Veeam
	Threat intelligence	Sesame IT	Sekoia.io	Rubrik
	Solution IPS / IDS	Gatewatcher	Cato Networks	Suricata
	WAF / WAAP	Cisco	F5	Imperva
	Firewall	Palo Alto	Cisco	Fortinet
	Matériel de passerelle sécurisée / VPN	Stormshield	OpenVPN	NordVPN
	SOAR	Splunk	MindFlow	Tehtris
	Logiciels anti DDOS	6cure	Bluecoat	Arbor
	Sensibilisation	Avantdecliquer	KnowBe4	Mailinblack
HARDWARE	Baies stockage	Pure Storage	Dell	NetApp/Vast Data
	Serveurs	HPE	Dell	Lenovo
	Postes de travail	Dell	Asus	Lenovo
	Téléphonie d'entreprise	Alcatel-Lucent Enterprise	3CX	Yealink
	Systèmes de visioconférence	Zoom	DTEN	Cisco
	Mobilité (tablette, smartphone)	Apple	Samsung	Oppo
	Imprimantes	Canon	HP Inc.	Epson
	Périphériques et accessoires	Jabra	Poly	Logitech
RESEAUX	Logiciel de monitoring	Centreon	Easyvista	Solarwinds
	Routeurs / Switch	Cisco	Juniper	Aruba
	Bornes Wifi	Netgear	Alcatel-Lucent Enterprise	Ruckus
DEVOPS	Solution CI/CD	Cloudbees	Gitlab	Hashicorp
	Plateforme low-code/no-code	Baserow	Mendix	Outsystems
	Infra as code	Hashicorp		
DATA	Datalakes / data warehouses	Snowflake	Cloudera	Starburst
	SGBD relationnels	Oracle	PostgreSQL	
	SGBD NoSQL	Couchbase	MongoDB	
	Datascience et machine learning	Google	Dataiku	Datacadabra
Prix spécial du jury	Atempo			

3CX est développeur d'une solution de communications unifiées aux standards ouverts, qui réinvente la connectivité professionnelle et remplace les PABX propriétaires. Le logiciel, plusieurs fois primé, permet aux entreprises de toute taille de réduire leurs frais de télécom, d'augmenter la productivité des employés et d'améliorer toujours plus l'expérience client via des outils personnalisés et optimisés pour le service client.

Grâce à sa solution tout-en-un intégrant de la visioconférence via WebRTC, des applications pour Android, iOS, Windows et le web, un service de Live Chat sur site web, des intégrations avec WhatsApp et Facebook et un service SMS, 3CX fournit aux entreprises une solution de communication complète et omnicanale, prête à l'emploi et accessible de partout, même en télétravail.

3CX compte plus de 350 000 clients dans le monde, incluant Hugo Boss, Ramada Plaza Antwerp, Harley Davidson, Wilson Sporting Goods et Pepsi. Pour couvrir une présence internationale, 3CX possède des bureaux aux États-Unis, au Royaume-Uni, en Allemagne, en Afrique du Sud, en Russie et en Australie. Au total, 3CX compte plus de 12 millions d'utilisateurs par jour. Visitez le site de 3CX et retrouvez-nous sur nos réseaux sociaux.

Web : www.3cx.fr ***LinkedIn : www.linkedin.com/showcase/91054581***
Twitter : https://twitter.com/3CX_France

Fondée en 1995, AntemetA est leader en France dans le cloud hybride et la protection des données, avec plus de 1000 clients (CAC40, PME, ETI, Organisations publiques).

En tant que partenaire polyvalent de la DSI, AntemetA garantit la souveraineté des données tout en accompagnant l'évolution des systèmes d'information. Son offre comprend des solutions d'infrastructure (VAR), des services Cloud (CSP), et une expertise en services managés (MSP), offrant un support complet et adapté aux besoins technologiques et de sécurité.

AntemetA accompagne la transformation des Systèmes d'Information de ses clients, en optimisant ou refondant leurs environnements IT, hébergés chez eux ou en Cloud.

AntemetA possède une expertise en cybersécurité avec la mise en place d'une cellule RSSI, la certification ISO 27001 de ses services Cloud, la mise à disposition d'un SOC, offrant une « cyber-sécurisation » complète.

Son expérience dans la certification ISO 27001 permet à sa cellule RSSI d'accompagner ses clients dans leur démarche, désignant ou externalisant cette fonction, rédigeant la Politique de Sécurité (PSSI), et mettant en place le SMSI.

AntemetA simplifie la gestion des données d'entreprise en définissant les processus de traitement de l'information, qu'elle soit hébergée chez le client ou chez eux.

L'expertise AntemetA en plateformes et solutions métiers offre des compétences spécifiques et des solutions clés en main, conseillant ses clients pour la mise en place, la maintenance et le renouvellement de leurs applications, qu'elles soient hébergées chez le client ou chez AntemetA.

Web : www.antemeta.fr ***LinkedIn : www.linkedin.com/company/antemeta***
Twitter : https://twitter.com/AntemetA

COHESITY

Le nombre élevé d'attaques par ransomware chaque semaine montre à quel point les entreprises et leurs données sont vulnérables. Cohesity aide les entreprises à renforcer leur infrastructure et leurs données, de sorte que même en cas de cyber-attaque, les entreprises peuvent maintenir leurs services critiques.

Cohesity met en œuvre ce concept de cyber-résilience avec sa plateforme de gestion et sécurisation des données basée sur l'IA. Avec l'aide d'un vaste écosystème de partenaires, Cohesity facilite la sécurisation, la protection, la gestion et la valorisation des données — dans les centres de données, à la périphérie et dans le cloud. Cohesity aide les entreprises à se défendre contre les menaces cyber grâce à des fonctionnalités complètes de sécurité et de gestion des données, notamment des snapshots de sauvegarde immuables, la détection des menaces basée sur l'IA, la surveillance des comportements malveillants et la restauration rapide à grande échelle.

Cependant, un fournisseur ne peut pas résoudre à lui seul les complexités de sécurité. C'est pourquoi, Cohesity a mis en place l'Alliance pour la Sécurité des Données afin d'assurer l'intégration technique avec des solutions de sécurité de données de fournisseurs leaders tels que BigID, Cisco, Palo Alto ou Splunk.

Cette Alliance réunit les forces de différents fournisseurs de sécurité pour que les clients puissent, *via* Cohesity, créer une véritable cyber-résilience. Cette collaboration aide les clients à détecter les menaces et à répondre aux attaques plus rapidement, à améliorer la remédiation et à renforcer la cyber-résilience — tout en utilisant leurs investissements existants en matière de sécurité et de gestion des données.

Les solutions Cohesity peuvent être fournies à la demande (aaS), gérées de manière autonome ou fournies par un partenaire Cohesity.

Web : ***www.cohesity.com/fr*** ***LinkedIn :*** ***www.linkedin.com/company/cohesity***
Twitter : ***https://twitter.com/cohesity***

Couchbase

Couchbase est née de la fusion de Membase et CouchOne en 2011, avec pour mission de simplifier la façon dont les développeurs et les architectes développent, déploient et consomment des applications modernes, où qu'ils soient. La première solution Couchbase Server est une base de données NoSQL documentaire s'appuyant sur le protocole JSON (JavaScript Object Notation) pour la notation de définition de document, et le JavaScript comme langage de manipulation des données primaires. Couchbase fournit également une API pour les langages de programmation permettant aux applications d'accéder directement à la base de données. La solution DbaaS (Database as a Service) permet de provisionner les terminaux mobiles de manière presque instantanée avec de la donnée structurée, comme les bases relationnelles classiques, mais aussi de la donnée brute, non structurée. La passerelle Sync Gateway supporte les systèmes d'exploitation IOS et Android, l'API REST et le langage HTML5. Couchbase permet le développement rapide d'applications riches, aussi bien on-premise que dans le Cloud, et propose une disponibilité des données tant en ligne que hors ligne. Aujourd'hui, Couchbase Capella gère et héberge un back-end complet pour les applications mobiles et IoT, appelé Capella App Services et s'appuie aussi sur l'IA Générative avec Capella iQ pour créer plus rapidement du code. En 2021, l'entreprise a fait son entrée en bourse sous le symbole « NASDAQ : BASE » et compte plus de 600 clients à travers le monde, dont 30 % du Fortune 100.

Web : ***www.couchbase.com*** ***LinkedIn :*** ***www.linkedin.com/company/couchbase***
Twitter : ***https://twitter.com/couchbase***

CUSTOCY

Créée en 2018, Custocy est un éditeur spécialisé en cybersécurité, basé à Toulouse, en région Occitanie. Forte d'une équipe de 15 personnes dont 30 % de Docteurs et doctorants en intelligence artificielle et d'experts en cybersécurité, Custocy a développé sa solution NDR (Network Detection & Response). La pépite toulousaine ambitionne de devenir le leader européen de la détection d'intrusion réseau à base d'IA.

La solution NDR de Custocy repose sur une technologie unique d'IA collaboratives, conçue en interne au sein de son laboratoire de recherche. En dépassant les limites des outils traditionnels, son approche innovante assure une identification proactive des attaques sophistiquées (APT) et inconnues (ZERO-DAY) en cours sur le réseau des entreprises, avec une précision sans précédent. Pensée pour apporter 4 principales capacités — surveillance continue du réseau, détection en temps réel, réponse ciblée et reporting automatique pour preuve de conformité NIS2 —, cette solution SaaS est le fruit de 5mEUR d'investissements depuis sa création et d'efforts continus pour offrir une solution de pointe en matière de sécurité numérique.

Soutenue par la Région Occitanie, BPI France et Capital Croissance, Custocy a développé une coopération de haut-niveau avec le LAAS-CNRS. Elle est lauréate de la 10e vague du concours d'innovation i-NOV soutenu par le Gouvernement et BPI France dans le cadre de la stratégie nationale cybersécurité France 2030.

En restant à la pointe de la technologie, Custocy incarne l'excellence en IA en offrant aux entreprises une solution NDR avancée made in France.

Web : www.custocy.ai ***LinkedIn : www.linkedin.com/company/custocy***
Twitter : https://twitter.com/custocy

EASYVISTA

EasyVista est un éditeur mondial de solutions d'ITSM et d'ITOM aidant les entreprises à fournir, superviser et supporter les services numériques à destination de leurs collaborateurs et clients. En s'appuyant sur la puissance des technologies d'IA, de workflow, de Self-Help, de support à distance, EasyVista propose aux organisations une expérience utilisateur riche et contextuelle ; permettant ainsi une digitalisation des processus métiers, une réduction des coûts opérationnels et une amélioration de la satisfaction clients. Aujourd'hui, EasyVista permet à plus de 3 200 entreprises à travers le monde d'accélérer leur transformation numérique en leur fournissant une solution complète de gestion de l'expérience des services numériques et en leur donnant les moyens de mieux servir leurs employés et leurs clients dans de nombreux secteurs d'activité, tels que les services financiers, la santé, l'enseignement supérieur, les technologies, le secteur public, la grande distribution, l'industrie, *etc.*

EasyVista est une entreprise humaine, créative et responsable. Elle soutient donc depuis 2020 les principes du "Global Compact" de l'ONU en termes de droits humains et du travail, d'environnement et de lutte contre la corruption, et les intègre dans sa stratégie, sa culture et au sein des projets qui lui sont confiés.
Pour mesurer l'impact des actions entreprises par rapport à cet engagement, EasyVista demande un audit annuel à Ecovadis pour évaluer ses actions de responsabilité sociétale. Grâce à un processus d'amélioration continue, de nouvelles actions sont mises en place chaque année.

Web : www.easyvista.com/fr ***LinkedIn : www.linkedin.com/company/easyvista***
Twitter : https://twitter.com/EasyVista

GATEWATCHER

Leader dans la détection des cybermenaces, Gatewatcher protège depuis 2015 les réseaux critiques des grandes entreprises et des institutions publiques. Ses solutions de Network Detection and Response (NDR) et de Cyber Threat Intelligence (CTI) détectent les intrusions et répondent rapidement à toutes les techniques d'attaque. Grâce à l'association de l'IA à des techniques d'analyse dynamiques, Gatewatcher offre une vision à 360° et en temps réel des cybermenaces sur l'ensemble du réseau, dans le cloud et on premise.

Entreprise engagée et ancrée dans l'écosystème cyber (Membre du groupement Hexatrust et de l'alliance européenne OpenXDR, membre fondateur du Campus Cyber — Paris La Défense), Gatewatcher a par ailleurs obtenu la qualification de l'ANSSI (Agence Nationale pour la Sécurité des Systèmes d'Information) en 2019.

En 2022, Gatewatcher a effectué sa première levée de fonds de 25 millions d'euros (Série A). La même année, l'entreprise a été identifiée dans le Gartner Market Guide 2022 for Network Detection and Response (NDR) comme Fournisseur Représentatif grâce à sa plateforme de NDR, AIonIQ. Parallèlement, la société a continué de s'étendre et s'est implantée sur la zone EMEA (dont le Royaume-Uni et l'Irlande, le Benelux et les Pays Nordiques), ainsi qu'en Asie, à Singapour. Elle compte aujourd'hui plus d'une centaine de collaborateurs, répartis sur deux sites en France (à Paris et à Rennes), et à l'étranger.

En 2023, Gatewatcher a été reconnue pour son haut potentiel de croissance et sélectionnée en tant qu'acteur émergent de l'innovation par le programme gouvernemental d'accélération French Tech 2030, dont l'ambition est de faire émerger des leaders technologiques mondiaux.

Web : www.gatewatcher.com ***LinkedIn : www.linkedin.com/company/gatewatcher***
Twitter : https://twitter.com/GATEW4TCHER

IFS

IFS développe et fournit des solutions cloud aux entreprises qui fabriquent et distribuent des biens, construisent et entretiennent des actifs et gèrent des opérations orientées services. Les solutions d'IFS, dédiées aux secteurs d'activités cibles (aérospatiale et défense, énergie, utilities et ressources, construction et ingénierie, industrie manufacturière, industrie des services et télécommunications) sont connectées de manière innée à un modèle de données unique et intègrent les dernières innovations numériques. Son expertise sectorielle et son engagement à apporter de la valeur à chaque étape, ont fait d'IFS un leader reconnu et le fournisseur le plus recommandé dans le secteur.

IFS Cloud est une solution SaaS pilotée par l'IA. Cette plateforme unifiée regroupe toutes les applications d'IFS, dont le CRM, la gestion des actifs (EAM) et la gestion des opérations de terrain (Field Service Management). IFS Cloud améliore l'agilité des entreprises, renforce leur résilience et réduit les risques dans un monde en constante évolution. L'approche d'IFS permet aux clients de tirer parti de l'automatisation et de la veille stratégique pour mieux comprendre les défis clés de leurs opérations, travailler plus efficacement et augmenter leur productivité. La dernière version d'IFS Cloud propose des outils conçus pour aider les entreprises à optimiser leurs ressources humaines, leurs actifs et leurs services, connecter leurs opérations mondiales et atteindre leurs objectifs ESG de manière rentable.

Web : www.ifs.com/fr ***LinkedIn : www.linkedin.com/company/ifs***
Twitter : https://twitter.com/IFS

oxibox

"Mes sauvegardes sont-elles sécurisées ?" Si cette question est devenue centrale pour les RSSI, DSI ou pour les dirigeants d'entreprise, ce n'était pas le cas il y a quelques années. En effet, l'explosion des cyberattaques en général, et des attaques ransomwares en particulier, a mis en valeur l'inadéquation des solutions traditionnelles face aux risques cyber. Les sauvegardes, trop souvent reléguées au rang de problématique d'infrastructure, se sont avérées cruciales pour la pérennité des entités attaquées.

Oxibox est créé en 2014 autour d'un constat simple : les solutions de sauvegardes sont complexes, coûteuses et surtout n'amènent aucune garantie de sécurité lors de la phase de stockage. Cette phase, où les données sont froides, est pourtant le moment où les sauvegardes sont le plus vulnérables.

Oxibox se veut ainsi une réponse simple et immédiate à cet enjeu. Ne nécessitant pas d'investissement lourd, simple à déployer et à utiliser, indépendante des fournisseurs de stockage, la solution Oxibox permet de garantir la capacité de redémarrage après une cyberattaque. Elle peut être déployée aussi bien en "greenfield" en remplacement d'une solution existante que de manière complémentaire au sein d'une infrastructure de sauvegarde.

Ce positionnement unique est récompensé en 2023 par l'obtention du label "France 2030" et du co-financement par l'Etat de la R&D innovante de l'entreprise, et aussi par le prestigieux trophée de L'Informaticien.

Web : ***www.oxibox.com/fr*** ***LinkedIn :*** ***www.linkedin.com/company/oxileo***
Twitter : ***https://twitter.com/OxiboxFR***

sekoia

Sekoia.io est une cybertech européenne dont la mission est de développer les meilleures capacités de protection contre les cyberattaques.

Sekoia.io XDR est une plateforme SaaS de Détection et Réponse Étendue (XDR), qui s'appuie sur du renseignement exclusif. Elle allie l'anticipation *via* la connaissance des attaquants à des capacités d'automatisation avancées, pour une détection et une réponse immédiate aux menaces cyber. Avec un vaste catalogue d'intégrations, des règles de détection vérifiées et régulièrement mises à jour et des playbooks pour l'automatisation et la réponse, Sekoia.io XDR simplifie la protection du système d'information de ses clients, leur faisant gagner un temps précieux.

Sekoia.io CTI, disponible à partir de la plateforme Sekoia.io ou *via* une API pour une intégration transparente, est une solution de Cyber Threat Intelligence (CTI) qui permet d'avoir une maîtrise et une connaissance approfondie des groupes d'attaquants. Elle facilite la compréhension des attaques, intrusions, compromissions et actes malveillants grâce à la normalisation des flux de renseignements sur les menaces. L'automatisation *via* les workflows de Sekoia.io XDR réduit considérablement le temps de réaction des équipes cyber. Le renseignement produit par les analystes de Sekoia.io est contextualisé et exploitable, bénéficiant ainsi tant aux équipes stratégiques qu'opérationnelles.

Sekoia.io protège plus de 200 grandes entreprises, startups, administrations et MSSP à travers le monde.

Web : ***www.sekoia.io/fr*** ***LinkedIn :*** ***www.linkedin.com/company/sekoia***
Twitter : ***https://twitter.com/sekoia_io***

WALLIX

CYBERSECURITY SIMPLIFIED

Éditeur de logiciels de cybersécurité, WALLIX est le spécialiste européen de la sécurisation des accès et des identités numériques. Les technologies de WALLIX permettent aux entreprises de répondre aux enjeux actuels de protection des données. Elles garantissent la détection et la résilience aux cyberattaques permettant ainsi la continuité d'activité. Elles assurent également la mise en conformité aux exigences réglementaires concernant l'accès aux infrastructures informatiques et aux données critiques.
WALLIX s'appuie sur un réseau de plus de 300 revendeurs et intégrateurs à travers le monde.
Cotée sur Euronext (ALLIX), WALLIX accompagne plus de 2500 organisations dans la sécurisation de leur transformation numérique.

OT.security by WALLIX est une marque dédiée à la sécurisation des accès et des identités numériques dans les environnements industriels.

WALLIX affirme sa responsabilité numérique et s'engage à contribuer à la construction d'un espace numérique européen de confiance, garant de la sécurité et de la confidentialité des données des organisations, mais également pour tout individu soucieux de la protection de son identité numérique et du respect de sa vie privée. Le numérique, qu'il soit pour des usages professionnels ou personnels, doit être éthique et responsable afin de vivre une transformation numérique sociétale sécurisée et respectueuse des libertés individuelles.

Web : ***www.wallix.com/fr*** ***LinkedIn :*** ***www.linkedin.com/company/wallix***
Twitter : ***https://twitter.com/wallixcom***

WITHSECURE

WithSecure™ (anciennement connu sous le nom de F-Secure Business) est le partenaire européen de référence en matière de cybersécurité depuis plus de 30 ans. Notre mission est de construire et maintenir la confiance dans une société de plus en plus numérique. Une confiance qui est quotidiennement menacée par l'incertitude, la peur et l'inquiétude provoquées par les cyberattaques et la criminalité. Et nous croyons qu'aucune entreprise ne devrait subir de pertes graves ou faire faillite à cause d'une cyberattaque.

Nous accompagnons les fournisseurs de services informatiques, les MSSP et des multinationales, qui nous font confiance, à travers des modèles commerciaux flexibles et adaptés au marché. Nous leur fournissons une cybersécurité axée sur les résultats, pour les protéger en toutes circonstances et garantir le bon fonctionnement de leurs activités. Notre protection basée sur l'IA sécurise les endpoints et protège les environnements cloud. Nos outils intelligents de détection et de réponse sont pilotés par des experts qui identifient les risques, assurent une recherche proactive des menaces, et neutralisent les attaques en temps réel. Un service de consulting expert est également disponible pour les entreprises qui souhaitent renforcer leur résilience.

WithSecure™, anciennement F-Secure Corporation, a été fondée en 1988 et est cotée au NASDAQ OMX Helsinki Ltd.

Web : ***www.withsecure.com/fr*** ***LinkedIn :*** ***www.linkedin.com/company/withsecure***
Twitter : ***https://twitter.com/WithSecure_FR***

Cassandre a toujours raison !

par Bertrand Garé

Pas de quoi se remonter le moral avec les prévisions pour 2024 ! La plupart des observateurs et des institutions nous annoncent des temps difficiles pour l'année prochaine. L'OCDE vient en tête avec une baisse prévue de la croissance, ce qui se traduit en langage financier en moins d'investissement, donc moins de revenus, des dividendes en baisse et une année morose à la fois pour les financiers et les entreprises qui seront contraints de serrer les coûts. Cela peut, évidemment, être une opportunité pour l'industrie informatique qui va pouvoir dérouler toute sa puissance pour fournir des améliorations de processus, de la productivité à gogo, de la recentralisation sur des tâches à plus forte valeur ajoutée. L'IA générative devrait être à la pointe de cette révolution dans les entreprises, sauf que si l'on en croit la fameuse courbe du Gartner, on arrive au niveau où, après la « hype », la technologie entame une descente que même Kitzbühel ou Val d'Isère ne connaissent pas, bien au-delà de leur piste noire ! Bon, il se peut que tout cela atteigne le plateau de la maturité plus rapidement que prévu, mais on ne sait jamais. Il faudra tout de même que les entreprises se posent la question de ce qui fera la différence quand la plupart des logiciels et autres outils informatiques embarqueront cette intelligence artificielle multiforme. Comment vous différencier quand tout le monde utilise le même outil pour faire les mêmes choses. Ce sera le rôle d'un nouveau directeur dans les entreprises, le Chief AI Officer, un directeur qui va veiller à la bonne utilisation de l'intelligence artificielle dans les entreprises. Comme la personne en charge de la sécurité, il va vite être à la limite du burn-out !

En parlant de sécurité, le tableau n'est pas plus resplendissant et on nous annonce que tout ce qui est apparu en 2023 continuera en 2024 : attaque de rançongiciel, attaque sur la supply chain de développement, *etc.* Certains comme BeyondTrust prennent cependant quelques risques dans leurs prévisions avec la fin des applications dédiées. Selon l'éditeur, l'IA générative est sur le point de rendre obsolètes les applications spécialisées. La flexibilité et la puissance de l'IA pourraient les remplacer par des commandes vocales, ce qui faciliterait la mise en place d'une confiance dans une interface commune. Les interfaces utilisateurs complexes pourraient devenir obsolètes à mesure que l'accent sera mis sur les applications axées sur les résultats et les fonctions spécifiques. Il voit aussi la disparition de la VoIP et de la téléphonie fixe au profit des technologies de communications unifiées. La liste continue avec les États-nations qui exploiteront les chaînes d'approvisionnement de l'IA pour introduire des vulnérabilités. Les aides à la programmation de l'IA et leurs données de formation deviennent des cibles, compromettant potentiellement l'infrastructure de l'IA et créant de nouveaux vecteurs d'attaque. Enfin, les télécommandes devraient rejoindre les oubliettes de

l'histoire, au profit d'applications téléphoniques dédiées et de commandes vocales. Il y a cependant des motifs d'espoir ! Si, si ! Les malwares sont en déclin, car la compromission de l'identité et les outils natifs remplacent les exploits logiciels. L'accent sera mis sur l'identification des identités compromises et la détection des comportements inhabituels. Les polices de cyberassurance seront de plus en plus normalisées et communes aux différents assureurs pour éviter que chacun n'ait ses propres exigences et conditions à remplir. Le secteur adoptera probablement un modèle de contrat-cadre avec des polices standard.

Des ressentis différents

Une enquête Robert Half montre un sentiment plus enthousiaste des dirigeants pour l'année à venir. 64 % des dirigeants se disent plus confiants sur les perspectives de croissance de leur entreprise pour 2024 qu'ils ne l'étaient pour 2023. Si l'optimisme reste majoritaire, il recule par rapport à l'an dernier, puisqu'ils étaient alors 75 % à exprimer une telle confiance (-11 points). 88 % prévoient des recrutements en CDI dans les prochains mois (remplacements ou nouveaux recrutements) alors qu'ils étaient 85 % l'an dernier. (+3 points). 35 % des dirigeants craignent de ne pas pouvoir offrir une rémunération suffisante pour attirer les meilleurs talents en 2024.

38 % des dirigeants intègrent aussi la croissance des nouvelles technologies dans leur sentiment de confiance pour 2024. L'intelligence artificielle générative laisse déjà percevoir un boom de productivité et apparaît comme une aubaine pour la croissance des entreprises. Les salariés semblent avoir une vision différente et sont moins confiants : une courte majorité, 53 %, se dit davantage confiante pour 2024. Dans un autre document issu d'une boule de cristal générative, Forrester prévoit que l'Europe dépassera les États-Unis en matière de travail flexible en 2024, avec 40 % des Européens travaillant à distance au moins une partie du temps. Les Pays-Bas sont en tête du continent en matière de soutien au travail flexible, avec 74 % des travailleurs autorisés à travailler à distance en 2023. Et seuls 11 % des chefs d'entreprise européens s'attendent à ce que leurs employés retournent au bureau à temps plein.

Plus étonnant encore, ce cabinet de conseil prévoit qu'une application utilisant ChatGPT se verra infliger une amende pour le traitement d'informations personnelles identifiables (PII). En l'absence de garde-fous appropriés autour du code généré par TuringBot, Forrester prévoit qu'au moins trois brèches seront publiquement imputées à un code généré par l'IA non sécurisée — soit en raison de failles de sécurité dans le code généré lui-même, soit en raison de vulnérabilités dans les dépendances suggérées par l'IA.

Plus encore que tout cela, le cabinet assure que les organismes de presse vont connaître une résurgence en tant que sources d'information fiables. Dans un monde de désinformation alimentée par des images générées par l'IA, des deepfakes et de faux influenceurs humains, les organismes de presse deviendront des sources d'information convoitées. En 2024, Forrester prévoit que la confiance dans la crédibilité des sources sera placée à un niveau record — et qu'il y aura donc un rebond indispensable de la confiance dans les médias. De quoi continuer à lire notre magazine pendant tout 2024. □

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

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

Concurrence

Les défis de la loi CHIPS and Science Act

Pour faire face à la concurrence chinoise, ne plus être dépendant de l'Asie et remettre les États-Unis au cœur de la production mondiale de semi-conducteurs, le gouvernement américain a voté la loi bipartisane CHIPS and Science Act en 2022. Son objectif est d'allouer des fonds aux entreprises et des crédits d'impôt pour qu'elles investissent dans la recherche et la construction d'usines sur le territoire américain. Un an plus tard, plus de 460 entreprises ont déposé des dossiers et attendent de recevoir des fonds. De nombreux grands fabricants (Intel, Micron) ont déjà entamé de grands chantiers pour construire de nouvelles usines outre-Atlantique.

Durant la pandémie de Covid-19, le monde s'est rendu compte à quel point de grands secteurs d'activité étaient tributaires de l'Asie pour la fabrication de nombreux produits, et particulièrement les semi-conducteurs. La fermeture des frontières à Taïwan, au Japon, en Corée du Sud ou en Chine et l'arrêt du jour au lendemain d'usines ont plongé l'industrie de la tech dans un marasme qui n'a épargné aucun pays, notamment les États-Unis. Le sujet des semi-conducteurs a d'ailleurs été au cœur de l'actualité tant cela a bouleversé la fabrication d'ordinateurs, de smartphones, de véhicules et de nombreux appareils connectés. Les États-Unis ont fait partie des principaux pays touchés par ces ruptures et par les difficultés rencontrées pour la chaîne d'approvisionnement.

En l'espace de trente ans, les États-Unis ont perdu leur avantage technologique pour la fabrication de semi-conducteurs. Sur cette période, la part de marché de la fabrication globale de puces sur le territoire américain a chuté de 37 % à 12 %.

Une dépendance qui stigmatise une faiblesse

Durant cette période, le pays de l'oncle Sam s'est rendu compte de sa dépendance avec l'Asie mais aussi de la faiblesse de son outil de production. Les chiffres parlent d'eux-mêmes. Au cours des trente dernières années, la part de marché des États-Unis dans la fabrication globale de puces informatiques a chuté de 37 % à 12 %. Selon de nombreux experts, la situation est en partie due aux problématiques de coûts. En clair, la construction et l'exploitation d'une nouvelle usine coûtent au moins 20 % de plus aux États-Unis qu'en Asie et la main-d'œuvre y est également largement moins chère. Par ailleurs, la chaîne d'approvisionnement est plus accessible et les incitations gouvernementales sont beaucoup plus importantes. Mais la pandémie de Covid-19 a clairement montré les limites d'une production presque 100 % asiatique.

L'Amérique veut se reprendre

Afin de retrouver sa place et ne plus être entièrement dépendant de l'Asie, l'administration Biden a fait voter par le Congrès un texte bipartisan pour remettre les États-Unis au cœur dans la production mondiale. Votée en 2022 et baptisée Chips and Science Act, cette loi a vocation à renforcer la capacité des États-Unis à être compétitifs et à investir dans des solutions pour relever les défis nationaux. *« Cette loi est le fruit d'une reconnaissance bipartisane du fait que le statu quo n'est pas*

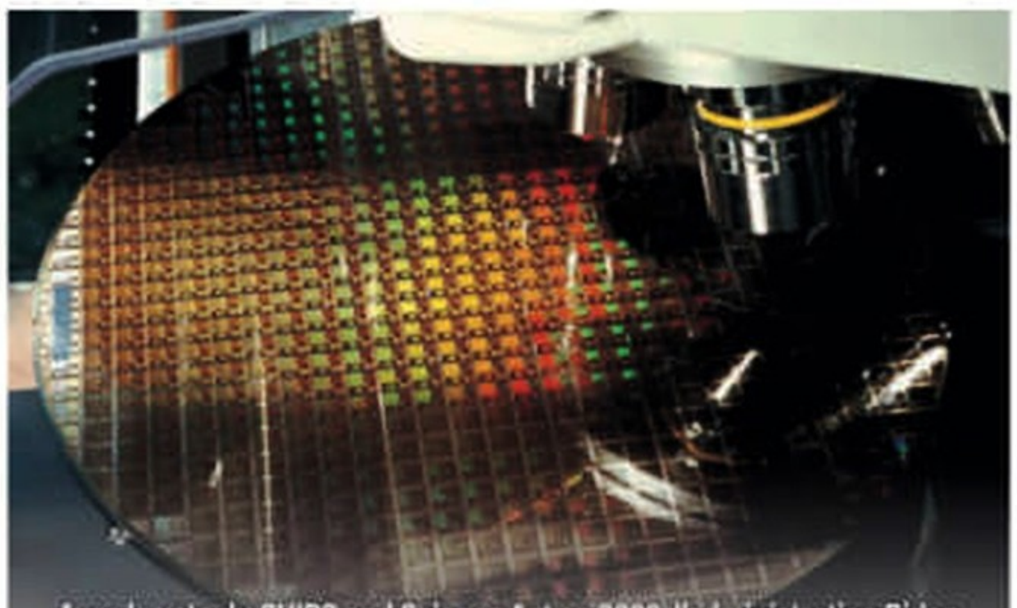
TSMC INVESTIT MASSIVEMENT AUX ÉTATS-UNIS

En 2020, et en pleine pandémie de Covid-19, le géant taïwanais TSMC avait annoncé sa volonté de construire une usine de semi-conducteurs aux États-Unis dans l'Arizona. Cela représente un investissement total de 40 milliards de dollars (environ 36,9 milliards d'euros) et, à terme, l'usine produira des puces de trois et quatre nanomètres destinées à de nombreux clients, dont Apple. La construction d'un autre site dans la même zone a également été annoncée par Mark Liu, le président de TSMC. La première usine en Arizona devait être opérationnelle en 2024. Mais en raison de problématiques de main-d'œuvre qualifiée et de différends entre TSMC et des syndicats américains, l'usine ne devrait être opérationnelle qu'en 2025.

LES GRANDS CHANTIERS DE L'AMÉRICAIN MICRON

Basé à Boise (Idaho), le fabricant américain Micron figure parmi les entreprises directement concernées par le CHIPS and Science Act. Pour le moment, la société, qui fabrique de nombreux composants, produit des semi-conducteurs au Japon et à Taïwan mais aussi en Chine. Sanjay Mehrotra, P.-D.G. de l'entreprise, a annoncé l'implantation pour 2026 d'une usine de fabrication à Boise, représentant un investissement de 15 milliards de dollars (13,8 milliards d'euros). Ce n'est pas tout, car Micron prévoit de dépenser 100 milliards de dollars (92 milliards d'euros) sur vingt ans pour construire quatre usines, au nord de l'État de New York, qui produiront de la mémoire DRAM. L'objectif de l'entreprise est d'augmenter sa part dans la production de ce type de semi-conducteurs qui, selon lui, ne représente actuellement que 2% aux États-Unis. Cette production provient de l'usine de Micron à Manassas, en Virginie. *« Grâce aux investissements à Boise et à Syracuse (New York) dans le cadre du CHIPS and Science Act, ces 2% passeront, sur une période de près de vingt ans, à environ 15% de la production mondiale en provenance des États-Unis »*, a déclaré Sanjay Mehrotra.

acceptable », expliquait en octobre dernier Michael Schmidt, directeur du bureau du programme Chips, en charge de la supervision des fonds, lors d'une réunion avec les P.-D.G. de grandes entreprises de la tech. De fait, le texte prévoit d'allouer 39 milliards de dollars (35,7 milliards d'euros) de subventions pour la fabrication de puces sur le territoire américain, ainsi que des crédits d'impôt à l'investissement de 25% pour les coûts des équipements de fabrication et 13 milliards de dollars (11,9 milliards d'euros) pour la recherche



Avec le vote du CHIPS and Science Act en 2022, l'administration Biden a voulu redonner des moyens aux entreprises américaines pour relancer la production de semi-conducteurs aux États-Unis.
Dans le cadre de ce texte, le gouvernement a ainsi prévu d'allouer 39 milliards de dollars (35,7 milliards d'euros) de subventions pour la fabrication de puces, des crédits d'impôt à l'investissement de 25 % pour les coûts des équipements de fabrication, et 13 milliards de dollars (11,9 milliards d'euros) pour la recherche et la formation.

sur les semi-conducteurs et la formation de la main-d'œuvre. S'il s'agit de remettre de l'Amérique au centre de la production mondiale, c'est aussi un moyen pour le gouvernement américain de contrer la Chine, qui figure aujourd'hui comme son principal concurrent et rival sur la scène internationale. Toutefois, les poids lourds américains comme Intel ou Micron n'ont pas attendu le vote du CHIPS and Science Act pour chercher à relancer la production de semi-conducteurs sur le territoire. Micron a annoncé plusieurs milliards de dollars d'investissement (voir encadré) à l'horizon 2026. De son côté, Intel construit quatre usines de production de puces (deux en Arizona et deux en Ohio) et une installation de conditionnement au Nouveau-Mexique.

Des défis majeurs à relever

Plus d'un an après le vote de la loi et grâce à des avancées majeures comme le montrent Intel, Micron et même le Taïwanais TSMC (lire encadré), le pays a encore des défis à relever. *« Nous devons être prêts à faire ces investissements et à utiliser les fonds dont nous disposons comme capital de départ, pour construire un écosystème d'une ampleur et d'une importance suffisantes pour développer notre main-d'œuvre et notre base de fournisseurs »*, a-t-il encore déclaré. Concrètement, la situation a favorablement évolué puisque les États-Unis peuvent s'appuyer sur la réussite d'acteurs comme AMD, Nvidia ou Qualcomm mais aussi sur un intérêt retrouvé dans le domaine des semi-conducteurs auprès des étudiants.

Mais malgré tout, de nombreux défis restent à relever, car la loi vient se heurter aux problèmes d'inertie de tout gouvernement. *« Il n'est pas toujours facile de faire bouger les rouages du gouvernement »*, a souligné Michael Schmidt. En effet, le déblocage des fonds s'avère compliqué et de nombreuses entreprises américaines attendent toujours de les recevoir. Ainsi, les sociétés qui n'ont toujours rien reçu rechignent encore à investir. À ce titre, plus de 460 sociétés ont déposé des demandes de fonds.

Par ailleurs, la problématique de la main-d'œuvre qualifiée vient s'ajouter à celle des financements. La construction de l'usine TSMC en Arizona connaît du retard en raison du manque d'ouvriers qualifiés. C'est un autre défi que les États-Unis doivent relever. Enfin, les élections présidentielles de 2024 pourraient-elles remettre en cause le vote de cette loi et le versement de fonds ? Pour Michael Schmidt, ce ne sera pas le cas même s'il y avait un changement d'administration. Il assure que les États-Unis entendent avant tout reconstruire ce secteur d'activité sur le long terme et cela va au-delà des luttes politiques et partisanes. D'autant plus que le CHIPS and Science Act ne concerne pas uniquement les semi-conducteurs. Il s'agit aussi de financer toutes les technologies au rang desquelles figurent l'intelligence artificielle et les ordinateurs quantiques. □

Michel Chotard

Événement

Le TechLive A3 Londres a tenu ses promesses

Récemment s'est tenu un nouveau TechLive à Londres qui nous a permis de rencontrer différentes entreprises dans le domaine du stockage : Hammerspace, Nodeum, Nebulon et la SCSI Trade Association, un forum de la SNIA (Storage Networking Industry Association).

Après sa levée de fonds et le rachat de RozoFS, Hammerspace se présente désormais comme l'architecture de référence pour le domaine de l'intelligence artificielle et du HPC. Sa proposition logicielle de pouvoir accéder les données de n'importe où et à n'importe quelle échelle apporte les données à une portée de clic pour les utilisateurs par une automatisation orchestrée. Ainsi, pour les modèles LLM, Hammerspace apporte les différentes qualités nécessaires au pipeline de données avec la possibilité de lire et écrire des blocs et des fichiers larges, des écritures aléatoires sur les disques, des possibilités de lecture intensive, une orchestration et une distribution des données par un placement fin et granulaire de celles-ci sur tout type de matériel.

De plus, par son système de fichier global parallèle, l'éditeur évite de nombreuses copies de données et orchestre automatiquement les données pour qu'elles soient disponibles de n'importe quel endroit accédant au système. La solution s'appuie sur NFS 4.2 qui autorise une séparation des métadonnées et des données pour apporter performance et flexibilité dans le placement. Par analogie, on peut voir cela comme une couche de virtualisation des données. L'utilisateur lit et écrit les I/O directement sur les volumes de stockage par les connectivités TCP et RDMA. Le placement des données est totalement séparé des volumes de stockage sous-jacents.

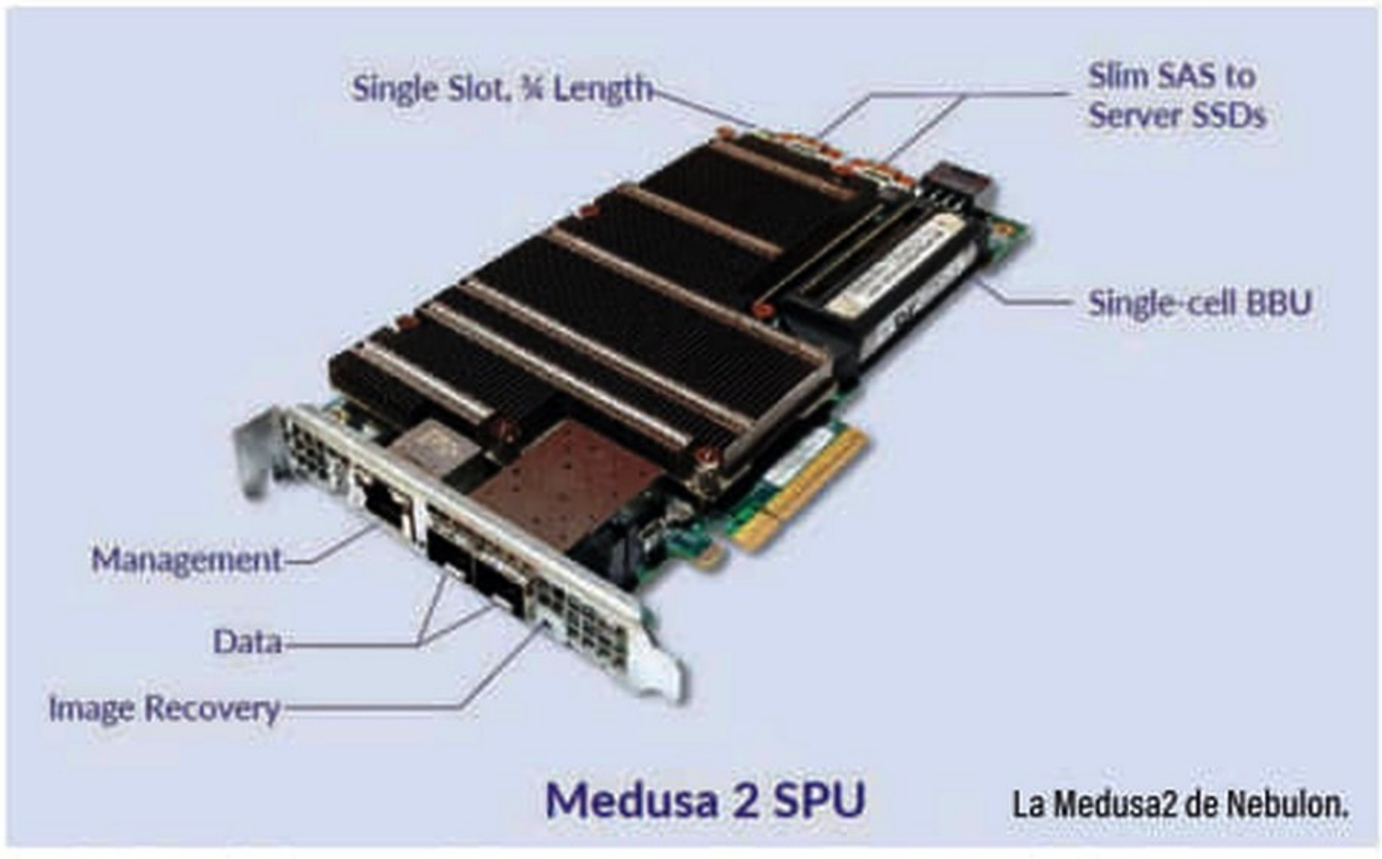
Le système de fichier peut être déployé indifféremment en bare métal, dans une machine virtuelle ou dans un container applicatif. Par son parallélisme, le système de fichier connaît des performances linéaires vers n'importe quelle source de stockage blocs (SSD, NVMe, HDD) ou en réseau (SAN, iSCSI et EBS). La solution supporte les snapshots partagés et les clones de fichiers. L'utilisateur peut, de plus, mirrorer les écritures sur plusieurs nœuds de la solution DSX de l'éditeur ou choisir une solution erasure coding. DSX embarque une solution de migration de données, DSX Mover programmable qui permet les migrations de système de fichiers à un stockage objet comme S3 par HTTPs.

Nodeum a la frite !

L'éditeur d'origine belge continue à se faire un nom dans le monde du stockage avec sa solution de gestion des données pour les environnements de l'ordre de l'exascale. La conception de la solution d'origine a été totalement repensée pour y parvenir et s'adapter au contexte de l'explosion des données non structurées dans les entreprises. L'idée de départ a donc été de s'appuyer sur la gestion des données pour une solution de stockage hybride afin d'accélérer les combinaisons et les interactions entre les humains et les données, dans le but de mettre en valeur les données sur de nouveaux modèles d'affaires et éradiquer les temps perdus dans la recherche des données.

Actuellement, Nodeum se positionne sur les marchés qui requièrent des performances et des volumes conséquents comme le HPC, la recherche génomique, l'aérospatial, les laboratoires de recherche des universités ou le monde du broadcast et des médias. La première priorité de la solution est de simplifier l'archivage, la protection et la migration de larges volumes de données non structurées, éparpillées dans de nombreux systèmes de stockage sur une plateforme unifiée, pour une gestion des données plus efficace et de manière sécurisée.

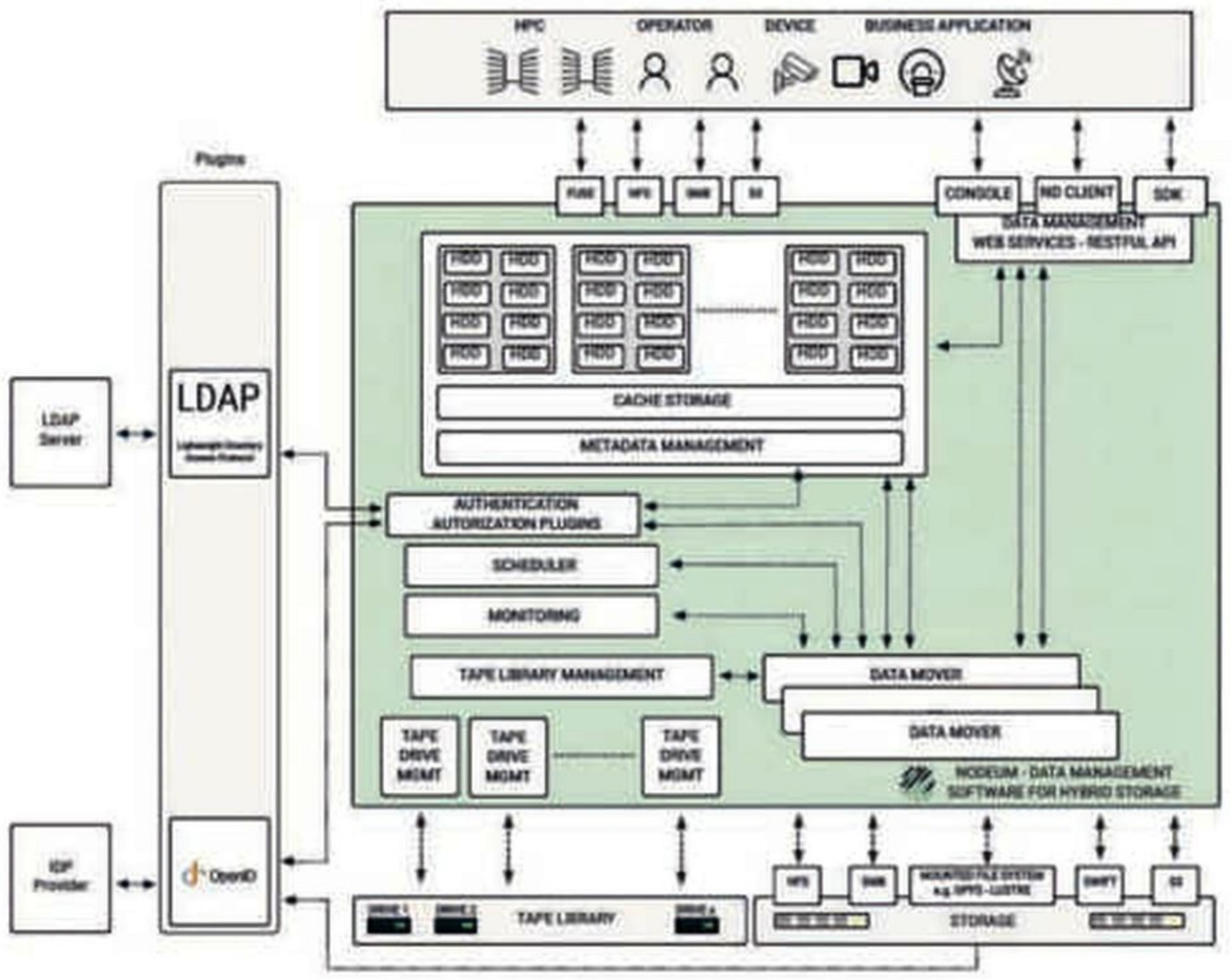
Techniquement, la solution de Nodeum repose sur un système de fichier compatible POSIX, intégré avec un outil de migration de données et un système de fichier virtuel



La Medusa2 de Nebulon.

qui apporte un environnement unifié pour organiser les données entre le stockage primaire et secondaire à partir de multiples interfaces. Par cette couche de virtualisation, la solution supporte l'ensemble des systèmes de stockage secondaire (NFS, SMB, S3, Swift, bandes...).

La solution est prête pour proposer une architecture d'archivage active ou dynamique, selon comment on souhaite l'appeler, qui peut évoluer horizontalement ou verticalement selon les besoins. La solution comprend de plus un outil de gestion du cycle de vie des données et de catalogue qui autorise un suivi de bout en bout durant la durée de vie de la donnée si elle est gérée dans la solution. Une fonction de priorisation des migrations complète la plateforme et une solution de filtrage simplifie la recherche des données sur des critères spécifiques. L'ensemble est facilement administré à travers une console développée en HTML 5. Une fonction de monitoring et d'alertes s'assure de l'état de la solution. Les événements sont stockés dans une base Prometheus locale et autorisent les exports vers des outils de virtualisation comme Grafana et l'export des métriques vers le même outil ou Loki.



L'architecture active d'archivage de Nodeum.

Nebulon fait converger les infrastructures DPU

Lors de l'événement, Nebulon est revenu sur la présentation de sa nouvelle SPU, la Medusa2, qui affiche des caractéristiques impressionnantes. Pour Craig Nunes, COO et co-fondateur de Nebulon, l'entreprise est là pour adresser les problèmes présents dans les centres de données du fait d'infrastructures inefficaces et les faiblesses de sécurité prévalentes dans les architectures des serveurs et des baies de stockage. Exemple parlant, 25 % des processeurs classiques sont inutilisés pour faire fonctionner des services logiciels d'infrastructure. L'idée fondamentale de la solution est de faire bouger les services d'infrastructure des matériels propriétaires vers des équipements standards x86 ou ARM afin d'alléger les charges, de fournir une meilleure sécurité et de proposer une automatisation à l'échelle. Ses avantages sont aussi intéressants face aux environnements hyperconvergés. Nebulon veut aller encore plus loin en proposant Medusa2, sa SPU (Service Processing Unit) de nouvelle génération. Avec son système d'exploitation, NebOS, Nebulon reprend tous les services déjà présents en y ajoutant le support de NVMe et de services réseaux comme l'accélération TCP, la QoS, ROCE. Il renforce de plus la protection contre les rançongiciels avec ses fonctions ImmutableBoot, TripLine, un outil de détection en temps réel des ransomwares et TimeJump qui autorise des restaurations en 4 minutes.

Medusa2, développée en partenariat avec NVIDIA, s'appuie sur un BlueField 3 et 16 cœurs ARM Hercules A78 et 48 Go de mémoire DDR 5. La carte comprend 8 ports PCIe Gen 5 pour une bande passante de 200 Go/s. Elle présente de plus l'avantage de ne pas nécessiter de câblage, et intègre 4 SDD M2 pour des capacités allant de 2 To à 32 To. La solution s'adapte parfaitement pour une sécurisation des environnements Edge, une modernisation d'éléments dans le centre de données ou le déploiement d'une infrastructure pour l'intelligence artificielle. Autre atout, son empreinte carbone est 25 % moindre qu'une solution équivalente.

Le SAS n'est pas mort

La SNIA SCSI Trade Association et son forum promeuvent la bonne utilisation de Serial Attached SCSI. L'association a rejoint la SNIA en mai dernier. Lors du TechLive, l'association nous a présenté un point sur l'évolution de cette technologie. Alors qu'elle a été un standard dans le stockage pendant des décennies et que de nombreux protocoles s'appuient sur cette technologie comme Fibre Channel, USB, UFS ou Infiniband, la technologie SAS continue d'évoluer vers de nouveaux standards comme le 24G SAS, déjà en production, et sa future génération le 24 G+ actuellement en développement.

De plus, contrairement à une idée reçue, la technologie reste prépondérante dans la majorité du stockage aujourd'hui, et va le rester pour encore plusieurs années du fait, non seulement de ses qualités intrinsèques, mais aussi des futurs développements que la technologie va connaître. Sa flexibilité, sa résistance et sa facilité d'évolution restent des atouts pour les années à venir. □

B.G

« Notre force repose sur les services autour des données que nous développons depuis vingt ans »

Retour avec Philippe Charpentier, directeur technique de NetApp, sur les annonces effectuées lors de la conférence INSIGHT à Las Vegas ainsi que sur la stratégie globale de l'entreprise autour de l'intelligence artificielle (IA).

NetApp est un spécialiste américain du stockage et de la gestion des données basé à San Jose, dans la Silicon Valley. Il propose des services de gestion des données dans le cloud à destination des entreprises.

L'Informaticien : NetApp a effectué un certain nombre d'annonces lors de sa conférence qui vient de s'achever à Las Vegas. Quelles sont selon vous les plus importantes et quels sont les axes stratégiques sur lesquels NetApp souhaite se concentrer pour l'avenir ?

Philippe Charpentier : On peut distinguer trois axes principaux. Le premier repose sur le métier historique de NetApp, à savoir l'hybridation entre stockage et données, pour faire en sorte que celles-ci soient disponibles n'importe où et de n'importe quelle manière. Nous avons été le premier acteur à proposer un aspect multiprotocole pour les données, aujourd'hui nous étendons cela au cloud en devenant le seul acteur du marché à proposer notre plateforme de manière native chez les trois grands hyperscalers. Dans cette logique, nous avons également annoncé une baie full flash dédiée au SAN pour notre offre sur site, avec des disques très capacitifs rendant le coût de la plateforme tout à fait abordable.

Le deuxième axe repose sur l'intelligence artificielle, au niveau logiciel avec notre collaboration avec les hyperscalers et au niveau matériel avec Nvidia.
Le dernier axe est celui de la cybersécurité, un aspect capital pour nous, étant donné qu'en tant qu'experts du stockage de données, il est très important pour notre image de marque que nos plateformes soient robustes et sécurisées. En outre, dans un contexte où les cyberattaques sont en hausse constante, la question pour nos clients n'est plus si, mais quand ils vont se faire attaquer. Nous nous efforçons donc d'étoffer en permanence notre gamme aussi bien en matière de détection d'attaques que de protection et de remédiation. Nous avons aussi annoncé durant INSIGHT l'extension de notre garantie contre les rançongiciels à l'ensemble de notre gamme.

Quels sont les usages de l'intelligence artificielle autour du stockage et du traitement des données ?

En ouverture de l'événement, George Kurian a cité une récente étude de Google et du BCG montrant que 30% des sociétés orientées vers les données ont un taux de croissance supérieur à 10%, proportion qui tombe à 13% pour les sociétés dont la stratégie n'est pas centrée sur les données. Il y a donc un vrai enjeu de croissance autour de la gestion des données, il s'agit bien d'un sujet de fond et pas seulement d'un effet de mode. Or, l'intelligence artificielle ouvre des perspectives exaltantes dans ce domaine.

De notre côté, notre force repose surtout sur les services autour des données que l'on développe depuis vingt ans, à travers les offres de clonage natives cloud qui permettent de copier des bases de données en quelques secondes au lieu de plusieurs heures, voire plusieurs jours. Nous travaillons actuellement avec une grande banque française qui avait auparavant besoin d'une semaine afin de copier les données nécessaires pour permettre à leurs ingénieurs de réaliser des modélisations, au service de la détection

des fraudes et de l'identification de clients potentiels pour des offres de données. Grâce à notre technologie, ce processus requiert désormais quelques minutes seulement.

Durant l'événement, nous avons annoncé une extension de notre partenariat avec Google à travers Google Cloud NetApp Volumes, offre de stockage de Google basée sur la technologie NetApp. Le tout au service de Vertex AI, qui permet de faire ce que proposent Bard et ChatGPT, mais avec les données d'entreprise. L'important pour nous, c'est d'assurer une bonne intégration entre Vertex AI et le chemin de la donnée, l'IA étant alimentée par des données hébergées sur du stockage NetApp. Nous développons un mécanisme similaire chez nos partenaires AWS et Azure.

Comme vous l'avez esquissé précédemment, vous travaillez sur des applications de l'IA dans le logiciel, mais aussi au niveau du matériel, à travers un partenariat avec Nvidia...
En effet, nous travaillons depuis déjà quelque temps avec Nvidia, nous avons des designs d'architectures qui sont publiés, sommes des acteurs du superPOD et standardisons les plateformes Nvidia avec du stockage NetApp. Il y a quelques mois, nous avons développé une nouvelle gamme de plateformes capacitives qui n'étaient pas encore certifiées pour le superPOD, c'était une grosse attente de nos clients qui ont une forte demande de capacité pour l'IA, c'est désormais chose faite.

Nous travaillons par exemple avec Weta FX, entreprise spécialisée dans les effets spéciaux pour films de grosse production. Pour le premier Avatar, elle avait utilisé un peta de données, ce qui était déjà énorme pour l'époque. Sur le dernier film, on est passé à 23 peta ! D'où l'importance des disques capacitifs pour faire des PODs Nvidia, ce n'est pas de l'IA *stricto sensu*, mais ça s'en rapproche beaucoup dans la mesure où l'on doit manipuler d'immenses quantités de données. Ce que nous mettons en avant, au-delà de la plateforme matérielle, c'est donc notre métier principal, la gestion de la donnée.

Avec l'intelligence artificielle, la cybersécurité est un autre gros sujet du moment, entre le règlement européen Dora et la hausse continue des cyberattaques...
En effet, nous avons également beaucoup de dossiers clients dans ce domaine, avec notamment de la réplication de coffres-forts. Nous constituons de notre côté le dernier rempart, là où l'on stocke la donnée. Une stratégie de cybersécurité comporte trois axes : la détection, la protection et la remédiation. Concernant ce dernier point, il est important de noter que l'impact financier d'une cyberattaque est avant tout dû à l'arrêt de la production qu'elle entraîne, loin devant la rançon. Nous proposons pour cela des solutions embarquées dans la plateforme NetApp, qui peuvent être activées en appuyant simplement sur un bouton.

Concernant la détection, l'idée est de s'appuyer sur l'IA à travers une première phase d'apprentissage. Lorsque la baie de stockage est mise en service, on laisse tourner pendant un ou deux mois un moteur d'apprentissage qui va ainsi apprendre le comportement nominal de la baie. Une fois cette phase effectuée, on devient capable de facilement repérer une déviance par rapport à l'utilisation habituelle de la baie : il peut s'agir d'une grosse quantité de lecture effectuée d'un seul coup lors d'une tentative de vol de données, ou au contraire de beaucoup d'écriture lors d'une tentative de chiffrage.

Une fois l'attaque repérée, ce petit moteur d'IA génère un instantané qu'on rend immuable, même un administrateur ne peut pas le détruire, ce qui est capital étant donné que la première chose que fait une attaque de rançongiciel est de s'en prendre aux instantanés et aux sauvegardes. On peut ainsi détecter plus facilement les attaques et prévenir la récupération, le tout sans avoir besoin de la moindre formation. □

Guillaume Renouard

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

Services Gaia-X prend une ampleur nouvelle

Le catalogue fédéré de l'association CISPE Cloud (Cloud Infrastructure Services Providers in Europe) est disponible avec plus de 500 services respectant les spécifications de Gaia-X.

Le catalogue a été conçu pour faciliter la collaboration entre les fournisseurs et les clients afin de répondre aux besoins spécifiques du marché. Ils matérialisent une chaîne de confiance complète à travers différents composants dans le but de renforcer la confiance dans les services numériques interopérables. Grâce au catalogue de la fédération CISPE, les utilisateurs cloud peuvent rechercher et comparer les offres de services des fournisseurs et combiner celles qui répondent parfaitement à leurs exigences en termes de niveau de conformité Gaia-X, de certifications de protection des données, de cybersécurité ou de durabilité, par exemple. Enfin et surtout, le catalogue définit, pour chaque service, les labels et les besoins adaptés à des emplacements géographiques spécifiques, répondant aux exigences strictes en matière de localisation des données.

Un premier pas

Le catalogue a été déployé avec le soutien de l'équipe CDE (Cloud Data Engine). Grâce à son travail, ce premier exemple de catalogue en production permettra et encouragera d'autres fédérations au sein d'espaces de données spécifiques, à déployer leurs propres catalogues conformes aux exigences communes de Gaia-X ainsi qu'à des règles sectorielles supplémentaires. CDE soutiendra également d'autres catalogues industriels basés sur les exigences de Gaia-X.

DES **RESSOURCES** EN PLACE

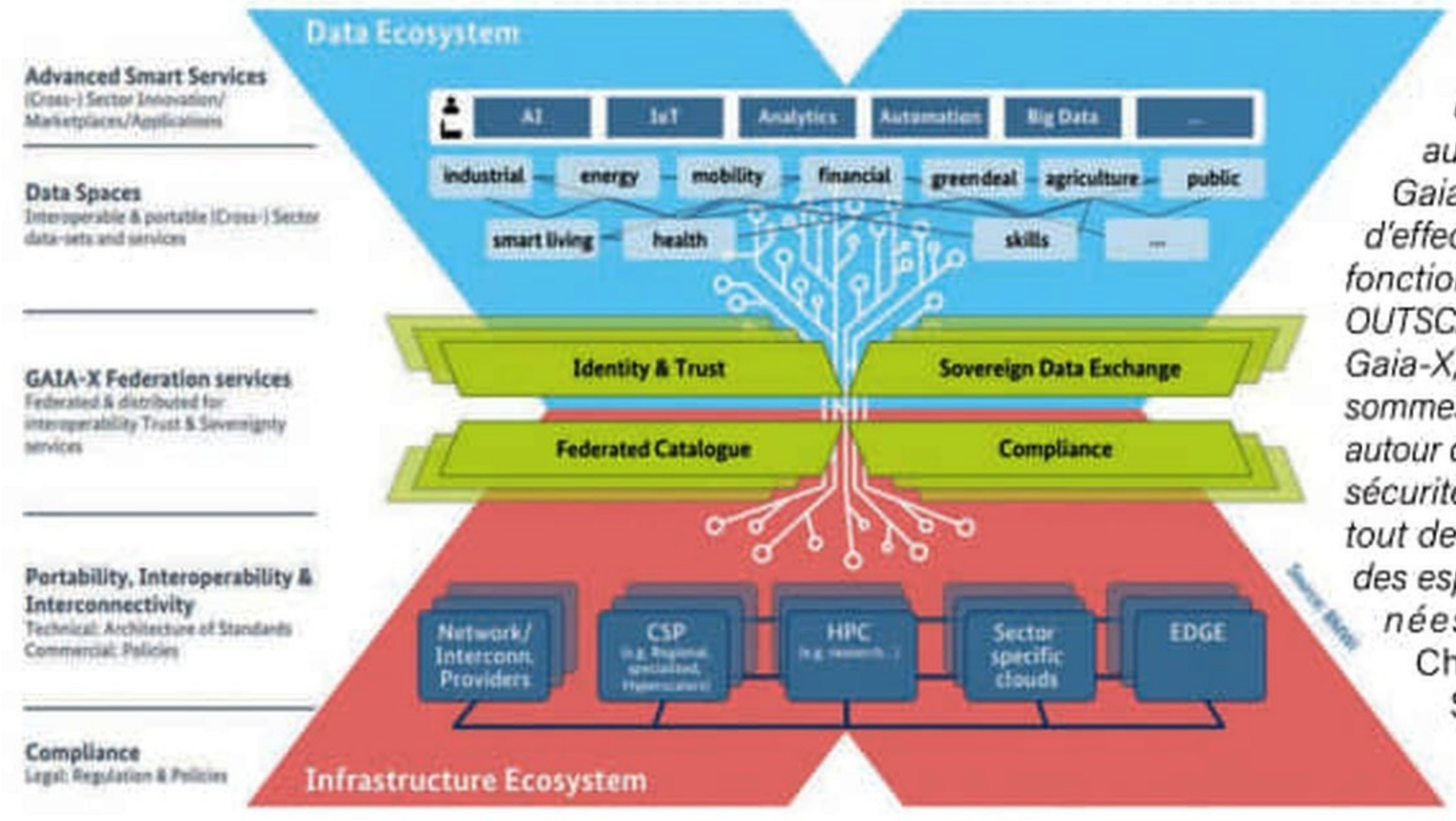
Il est possible d'accéder au catalogue de services à cette adresse : https://catalogue.cispe-cde.cloud.
De plus, le Hub France de Gaia-X a mis en ligne un module d'e-learning pour apprendre comment utiliser les différents services et prototyper une idée. Ce module comprend aussi des vidéos pour comprendre les grands principes de Gaia-X : h]ps://elearning.gxfs.fr/.

Un cadre normé

GXFS-FR, l'Institut Mines-Télécom, sa plateforme Data & AI TeraLab, ainsi que ses partenaires 3DS OUTSCALE, Eviden (une entreprise d'Atos), Dawex, Docaposte et OVHcloud, ont également dévoilé un dispositif de *« négociation et contractualisation des échanges de données »*. GXFS-FR soutient l'échange de données par la négociation de contrats et la gestion des autorisations afin de renforcer les espaces européens de données. Après un processus de négociation, un contrat PDF juridiquement protégé est généré. Les parties doivent souscrire à des clauses de protection spécifiques et irréfutables (protection des données, propriété intellectuelle, hébergement des données, *etc.*). Elles sont ensuite automatiquement mises en œuvre par les services de catalogue afin d'établir un lien avec les règles et labels de la politique Gaia-X.

OUTSCALE, membre fondateur de Gaia-X a réagi de manière enthousiaste à cette annonce : *« ce premier catalogue fédéré de services Cloud est une avancée majeure pour l'Europe numérique ! Les entreprises et institutions européennes ont désormais accès à une large gamme diversifiée de services conformes aux normes et standards de Gaia-X, leur permettant ainsi d'effectuer des choix éclairés en fonction de leurs besoins. Chez OUTSCALE, membre fondateur de Gaia-X, fort de notre ADN, nous sommes ravis de nous rassembler autour des principes essentiels de sécurité, de soutenabilité et surtout de souveraineté pour créer des espaces européens de données »* commente David Chassan, Directeur de la Stratégie d'OUTSCALE. □

B.G



BACK UP AND KEEP CALM

Operate

Secure

Protect

Leader français de la protection des données

ANTEMETA

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

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

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

WiFi

CommScope : comment la 5G révolutionne la couverture des grands espaces

Spécialisée dans les réseaux câblés et sans fil, CommScope exploite le potentiel de la technologie 5G pour développer des réseaux avancés.

Pour la société américaine, le déploiement de la 5G décuple les possibilités pour connecter des milliers de personnes simultanément dans de grands espaces publics, tout en faisant tourner des applications particulièrement gourmandes en bande passante. Chaque nouvelle génération de technologie cellulaire a apporté son lot d'évolutions et d'innovations. Pour CommScope, l'une des principales particularités de la 5e génération de réseau mobile réside dans sa capacité à connecter de grands espaces publics comme les salles de concert, les musées, ou encore les stades pouvant accueillir plus de 80 000 spectateurs. Contrairement aux idées reçues, la connectivité intérieure des grands sites n'est généralement pas basée uniquement sur le Wi-Fi. Dans la plupart des cas, les grandes infrastructures disposent de réseaux cellulaires à l'intérieur, afin d'assurer une meilleure qualité de service, aussi bien pour les visiteurs que pour les exploitants.

J.C

POUR SAMUEL BUTTARELLI, VP SALES EMEA & APAC DAS & SMALL CELL SOLUTIONS CHEZ COMMSCOPE, LA TECHNOLOGIE 5G OFFRE DE NOMBREUSES OPPORTUNITÉS TANT POUR LES CONSOMMATEURS QUE POUR LES ENTREPRISES.

Pouvez-vous nous présenter CommScope ?

CommScope est un fournisseur de solutions d'infrastructure des réseaux de communication qui repousse les limites de la technologie des communications pour créer des réseaux parmi les plus avancés au monde. Nous concevons, fabriquons, installons, et soutenons l'infrastructure matérielle et logicielle qui permet à notre société numérique d'interagir et de prospérer. En collaboration avec ses clients, CommScope fait progresser les réseaux à large bande, les réseaux d'entreprise et les réseaux sans fil pour stimuler le progrès, mais aussi créer des connexions durables.

Que va changer la 5G pour les espaces grand public ?

La 5G a été conçue à l'origine pour les consommateurs, mais aussi pour les entreprises. Cependant, les premiers à bénéficier de la 5G sont les consommateurs, qui profitent d'une connectivité mobile à haut débit améliorée. L'augmentation de la vitesse de téléchargement a eu un impact positif sur la demande de vidéos pour le divertissement, par exemple. C'est aussi le cas pour la productivité des entreprises que cela soit pour les pièces jointes volumineuses et d'autres applications professionnelles qui sont passées de l'environnement de bureau au bureau à domicile, notamment durant les fermetures consécutives à la pandémie.

À mesure que la technologie 5G évolue pour prendre en charge des applications à faible latence, les consommateurs bénéficieront indirectement d'autres applications professionnelles telles que les véhicules de guidage autonomes (AGV) assistés par le réseau.

La 5ème génération de technologie cellulaire va-t-elle être déployée selon le même schéma que les précédentes ?
Malgré les attentes initiales, la 5G a été déployée de la même manière que ses prédécesseurs. Tout d'abord, une couche macro a été déployée dans les zones urbaines avec les nouvelles bandes de fréquences introduites spécifiquement pour la 5G (la bande moyenne de 3,5 GHz également appelée n78). Elle a été suivie par l'extension de la couverture dans les zones suburbaines, puis à l'intérieur des bâtiments. Cela a commencé par les grands lieux publics tels que les aéroports et les stades pour soutenir le cas d'utilisation de la large bande mobile pour les consommateurs. Il s'agit là de la première phase de la 5G destinée aux consommateurs. Nous prévoyons par exemple pour la 5G une nouvelle approche de déploiement pour les AGV avec une densification des petites cellules pour une couche de capacité dédiée le long des routes principales. Cela peut être également des configurations de réseau différentes avec des réseaux centraux privés et dédiés (non connectés au réseau public). Du point de vue de l'architecture du réseau, les réseaux 5G évoluent et deviennent de plus en plus centrés sur le logiciel. Le matériel est de plus en plus basé sur des serveurs COTS (Commercial off-the-shelf) à usage général et les différentes fonctions du réseau sont mises en œuvre dans le logiciel. Cette approche vise à réduire le coût global de l'infrastructure et à rendre les déploiements plus souples et efficaces.

Quels sont les avantages du réseau 5G ?
Pour les consommateurs, les avantages sont principalement liés à l'augmentation de la vitesse du réseau. L'expérience globale de l'utilisateur est améliorée à la fois par l'augmentation du débit du réseau et par la diminution de la latence. La latence a un impact important pour les consommateurs (par exemple pour les jeux en temps réel), mais aussi pour des applications telles que l'AGV mentionné précédemment, où le réseau doit répondre très rapidement (quelques millisecondes). La 5G profitera également aux entreprises pour des applications


© Jean-Pierre Kepseu

La couverture 5G dans les stades va permettre de développer des applications en réalité augmentée très gourmandes en bande passante.

importantes telles que l'automatisation industrielle et la réalité augmentée (RA). Pour ne citer qu'un exemple d'application industrielle, on peut penser à la maintenance ou à l'inspection d'un moteur d'avion, avec un technicien utilisant une visière de réalité augmentée pour être guidé dans la procédure spécifique afin d'effectuer des contrôles ou des réparations. Les opérateurs de réseaux mobiles peuvent aussi tirer profit de la 5G. Tout d'abord, grâce à la rentabilité accrue de la 5G : le coût global par bit transmis avec la 5G est inférieur à celui de la 4G. Ils peuvent également créer de nouvelles opportunités de revenus, car ils peuvent servir non seulement les consommateurs, mais aussi les entreprises *via* des cas d'utilisation à faible latence tels que l'automatisation industrielle, la RA, ou de multiples capteurs IoT (Internet des objets) connectés au réseau 5G.

Est-ce qu'il existe déjà des applications en réalité augmentée (RA) pouvant être utilisées simultanément par des milliers de spectateurs dans des stades ou des salles de spectacle via la 5G ?
Ces applications RA pour les stades et les auditoriums sont actuellement testées, mais elles ne sont pas encore prêtes pour une adoption massive. La capacité du réseau et la latence à l'intérieur des salles doivent encore être améliorées. Il est tout aussi important que le coût des appareils (par exemple, les lunettes Apple) diminue.

Comment les exploitants de grands espaces publics peuvent-ils tirer profit de la 5G ?
Si l'expérience globale de l'utilisateur s'améliore, les sites deviennent plus attractifs. La réalité augmentée permet d'offrir une expérience plus immersive pendant un match ou un spectacle que cela soit pour les spectateurs sur place ou à distance. Sans compter que la 5G peut aussi prendre en charge d'autres applications importantes pour l'exploitant d'un site. Pour ne citer que quelques applications critiques, on peut penser à la sécurité (vidéosurveillance), mais aussi aux transactions sans fil sécurisées dans les points de vente.

Quelles avancées technologiques peut-on anticiper dans un futur proche avec la 5G ?
Dans un avenir proche, nous pouvons nous attendre à des évolutions de la technologie 5G pour soutenir des applications ayant un impact important sur notre mode de vie. Les véhicules autoguidés présenteront des avantages importants pour la sécurité et le contrôle des émissions en évitant par exemple les routes encombrées et en optimisant les itinéraires en temps réel. Les applications industrielles soutenues par la 5G auront également un impact significatif sur la sécurité des travailleurs et sur des processus plus écologiques et plus efficaces. D'une manière générale, la 5G et ses évolutions joueront un rôle majeur dans l'avènement d'une société plus durable. □ **J.C**

Standard

Wi-Fi 7 sort des cartons

Alors que les entreprises déploient activement Wi-Fi 6, la nouvelle évolution du standard est déjà sortie des cartons, et les premiers modèles arrivent sur le marché.

Pour Kevin Robinson, le CEO de la Wi-Fi Alliance, le prochain Wi-Fi 7 va autoriser des performances et des vitesses de très loin améliorées par rapport à la version 6, avec des débits allant jusqu'à 5 Gb/s. Une extension du spectre des fréquences qu'utilise le nouveau standard permet d'atteindre ces niveaux jusqu'à présent inégalés. Il va, de plus, apporter une latence plus faible, consistante et prévisible, soit sous les 10 ms selon les équipements utilisés. Il va ouvrir également de nouveaux cas d'usages pour la technologie Wi-Fi en proposant ses qualités inhérentes à l'échelle.

Des matériels déjà sur le marché

Récemment, lors de son événement Huawei Connect 2023 Paris, le fournisseur chinois a présenté ses points d'accès *« tous scénarios »*, AirEngine Wi-Fi 7. Ils peuvent prendre en charge jusqu'à 120 canaux concurrents de vidéo HD et fournir une bande passante de 10 Gbit/s. La gamme Huawei AirEngine Wi-Fi 7 se démarque par son ultra-haut débit sur chaque terminal et sur les points d'accès. En outre, les points d'accès Huawei AirEngine Wi-Fi 7 tirent parti de nombreuses technologies innovantes comme l'antenne intelligente à zoom dynamique, la réutilisation spatiale coordonnée (CoSR), la coordination multi-points d'accès, itinérance par intelligence artificielle pour assurer un débit sans fil allant jusqu'à 10 Gbit/s et un ordonnancement multimédia intelligent. Un seul point d'accès AirEngine Wi-Fi 7 peut prendre en charge jusqu'à 120 utilisateurs simultanés à haute densité sur leur lieu de travail, sans limitation de débit de la part des services de téléchargement.

Le routeur RS700 de Netgear.

Netgear suit Huawei de près avec un routeur tri-band, le RS700S. En maximisant cette puissance, le routeur RS700S de Netgear atteint des vitesses allant jusqu'à 19 Gb/s. Le routeur Wi-Fi 7 tri-bande permet une diminution spectaculaire de la latence avec une réactivité en temps réel pour toutes les applications. Le RS700S est équipé d'un port Internet 10 Gb/s, compatible avec toutes les lignes fibres, toutes les box et leurs futures évolutions, ainsi que 5 ports filaires (Ethernet) : 1 port 10 Gb/s et 4 ports 1 Gb/s garantissant des connexions rapides et flexibles. Le routeur supporte l'agrégation de ports filaires ; sur la partie Internet (1 port 10 Gb/s + 1 port 1 Gb/s), mais aussi sur la partie réseau local (1 Gb/s + 1 Gb/s), ce qui laisse une belle flexibilité pour faire évoluer simplement son réseau. Un disque dur USB ou SSD externe peut être connecté sur le port USB 3.0 pour faciliter la sauvegarde de données, le partage de fichiers volumineux, ou la diffusion de contenus. □

B.G

Authentification

OAuth en débat

Un rapport récent de la société Salt Security a pointé l'importance de la sécurisation de l'implémentation OAuth afin de se protéger contre l'usurpation d'identité, la fraude financière et l'accès aux informations personnelles. Nous allons tenter de voir dans cet article ce qu'il en est.

Le dernier bug découvert par des chercheurs en sécurité de Salt Security dans l'implémentation OAuth est assez inquiétant. Il permet aux utilisateurs de s'authentifier sur différents sites web à partir de services tiers tels que Google, Facebook... Le problème qui se pose est que certains sites ne parviennent pas à franchir une étape très importante de la chaîne d'autorisation consistant à valider l'application pour laquelle un jeton d'accès a été émis par le fournisseur d'identité. L'exploitation de cette faille par un attaquant peut lui permettre de collecter les jetons émis pour une application ou un site web spoofé (imité), créés de toute pièce, et de les utiliser ensuite pour accéder aux comptes des victimes sur des sites vulnérables à cette faille. Les grey hats de Salt Security en ont fait la démonstration sur trois sites web populaires : le service d'aide à la saisie Grammarly, la plateforme de commerce électronique indonésienne Bukalapak, ainsi que le site de streaming vidéo indonésien Vidio. Certes, ces entreprises ont été informées en privé par les chercheurs et ont corrigé le problème. Néanmoins, toutes les sociétés employant ce système devraient très rapidement vérifier leurs implémentations afin de s'assurer qu'elles n'exposent pas leurs utilisateurs à des attaques de ce genre. *« Ces trois sites nous suffisent amplement pour prouver la véracité de notre théorie et nous avons décidé de ne pas chercher plus avant en testant d'autres cibles, mais nous pensons que des milliers d'autres sites web sont vulnérables à ce type d'attaque, mettant en danger des milliards d'internautes »*, ont déclaré de manière collégiale les dits chercheurs dans leur rapport.

Vous trouverez tous les détails de la faille OAuth dans le rapport des chercheurs en sécurité de Salt à l'adresse https://salt.security/blog/oh-auth-abusing-oauth-to-take-over-millions-of-accounts

Les jetons d'accès liés aux applications émettrices de la requête

La norme d'autorisation et de pseudo-authentification OAuth, très populaire sur le web, sert tout simplement aux sites web et aux applications à demander à un fournisseur d'identité tel qu'Apple, Facebook, Google ou Microsoft de vérifier qu'un utilisateur est bien celui qu'il prétend être et non un vilain intrus. Cette méthode facilite grandement le processus d'authentification pour les utilisateurs qui peuvent ainsi utiliser leur identification auprès d'un fournisseur pour éviter de créer encore et encore de nouveaux mots de passe. OAuth ne se limite pas à l'authentification. Ce mécanisme permet également aux utilisateurs d'accorder à des sites web externes l'accès à diverses informations de profil associées à chaque fournisseur d'identité *via* son API. Néanmoins, le problème cité s'applique à la partie authentification, c'est-à-dire lorsqu'un site demande au fournisseur d'identité de confirmer que l'utilisateur est bien le propriétaire de l'identité (représentée par son adresse électronique) qu'il souhaite utiliser. Au passage si, pour leur démonstration, les chercheurs ont utilisé « Login with Facebook », ils auraient pu faire le test avec n'importe quel autre fournisseur d'identité (comme, encore eux, Google, Microsoft et consorts). Voici comment fonctionne le processus OAuth : un utilisateur qui souhaite créer un compte sur un site web va choisir l'option « Login with Facebook » (ou « Login with Google », si l'option est disponible) en fournissant une adresse électronique en correspondance avec le fournisseur choisi. Le site web va rediriger le navigateur de l'utilisateur vers l'adresse du fournisseur d'identité concerné afin d'apporter la preuve que l'utilisateur dispose bien d'un compte avec cette adresse électronique auprès dudit fournisseur. Ce fournisseur va, la première fois que l'accès est demandé, afficher une demande d'autorisation à l'utilisateur en vue de confirmer que le site web ou l'application de tierce partie sont autorisés à accéder aux informations relatives à son

compte. Il va ensuite générer un « secret token », un jeton secret si vous préférez, et rediriger le navigateur de l'utilisateur vers le site web demandeur. Le jeton créé précédemment va alors être joint à l'URL de la requête.

Mémorisation des permissions

Le site web prend alors le jeton et s'en sert cette fois pour accéder à l'API d'identification du fournisseur d'identité (Graph dans le cas de Facebook) au nom de l'utilisateur et demande au fournisseur quelle est l'adresse électronique associée au jeton transmis. Le fournisseur répond avec l'adresse électronique de l'utilisateur et le site web reçoit la confirmation que l'utilisateur est bien celui qu'il prétend être et l'autorise à créer son compte. Le processus se répétera lors des connexions ultérieures. Une exception : le fournisseur d'identité ne demandera plus à l'utilisateur de fournir un accès puisque celui-ci lui a déjà été accordé. L'utilisateur n'aura simplement qu'à cliquer sur « Login with Facebook », si bien entendu c'est Facebook le fournisseur employé, et le site redirigera le navigateur de l'utilisateur vers le site du fournisseur pour obtenir un jeton. Enfin, le fournisseur en question redirigera le navigateur de l'utilisateur vers le site cible, toujours avec le jeton secret attaché à l'URL, qui l'utilisera afin de confirmer l'adresse mail de l'utilisateur *via* l'API du fournisseur et le laisser entrer. La sécurité liée à ce processus comporte un élément très important : tout fournisseur d'identité OAuth lie le jeton à l'app ID du site web qui a demandé ce jeton *via* le navigateur de l'utilisateur. Du coup, tout site web ou application souhaitant proposer la fonctionnalité de connexion *via* le fournisseur d'identité (« Login with Google », par exemple) doit d'abord s'enregistrer auprès du fournisseur en vue de recevoir son propre identifiant d'application unique dans sa base de données. Le problème crucial qui se pose alors est qu'il incombe au site web de vérifier le jeton avant de l'accepter et de l'utiliser. Cette validation implique de vérifier que le jeton a bien été généré pour son propre app ID et non pour une autre application. À cette fin, une requête est adressée à un point de terminaison spécial de l'API du fournisseur avant de pouvoir utiliser le jeton en demandant au fournisseur de valider l'identité de l'utilisateur pour lui permettre d'accéder à son compte. Si jamais cette étape est omise — et il s'avère malheureusement que de nombreux sites web le fassent — il devient possible d'usurper l'identité de l'utilisateur et de « s'emparer » de son compte. Un pirate peut, par exemple, créer un site web spoofé, voire une application légitime fournissant un service, et l'enregistrer auprès du fournisseur afin de fournir la fonction de connexion précitée puis l'utiliser subrepticement en vue de générer et de collecter des jetons OAuth auprès d'utilisateurs qui, eux, souhaitent utiliser le service de façon légitime. Les jetons générés par le fournisseur d'identité pour que ces utilisateurs valident leur identité sur le site web du vilain cracker seront valides, quand bien même ils auront été émis pour l'app ID du site web fallacieux ou de l'application. Mais si jamais un autre site web ne vérifie pas l'identifiant d'application des jetons qu'il reçoit et se contente simplement d'essayer de les utiliser, le pirate pourra alors récupérer un jeton généré par un utilisateur pour son site web et l'utiliser sur un autre site vulnérable afin d'accéder au compte de l'utilisateur. Si ce site est, par exemple, une plateforme de eCommerce comme Bukalapak, Amazon ou autre AliBaba, il est tout à fait possible que l'utilisateur ait stocké dans son profil des données bancaires. Avec un service comme Grammarly, ce seront plutôt des documents sensibles. Quelle que soit la nature de ces données, elles pourront alors être compromises. □

T.T

Dans cet autre exemple décrit également sur le site de Salt Security, un attaquant a créé un service web malicieux, YourTimePlanner.com, afin de récupérer des jetons de manière illégitime.

VARIANTES ET AUTRES DÉFAUTS D'IMPLÉMENTATION

OAuth est une norme complexe offrant plusieurs variantes de mise en œuvre. Au lieu d'utiliser des URL de redirection entre le site et le fournisseur d'identité, le site peut, par exemple, choisir d'utiliser la fonction PostMessage. Malheureusement, l'attaque sera toujours possible si le jeton n'est pas validé. Le passage de jetons via des URL reste vulnérable aux attaques de type Man-in-the-middle, si tant est, bien entendu, qu'un pirate arrive à surveiller passivement le trafic et à extraire le jeton OAuth de l'URL lorsque la trame réseau lui passe sous le nez. C'est pour cette raison qu'OAuth propose une approche plus sûre dans laquelle le fournisseur d'identité émet un code unique au lieu d'un jeton d'accès. Le site web embarque ce code avec un secret d'application qui n'est connu que de lui-même et du fournisseur et le transforme en jeton à l'aide de l'API du fournisseur. *« Il est extrêmement important de s'assurer que l'implémentation d'OAuth est sécurisée »*, ont déclaré les « chapeaux gris » de Salt. Le correctif se résume le plus souvent à une simple ligne de code.

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 €

Roadmap

ChatGPT à la conquête des développeurs d'applications

Le tout premier OpenAI DevDay a failli être fatal à Sam Altman. Le CEO a dévoilé alors la roadmap de l'éditeur et les dernières évolutions de ChatGPT. Des évolutions enthousiasmantes pour les développeurs et son partenaire Microsoft, mais un virage Business qui a effrayé son conseil d'administration.

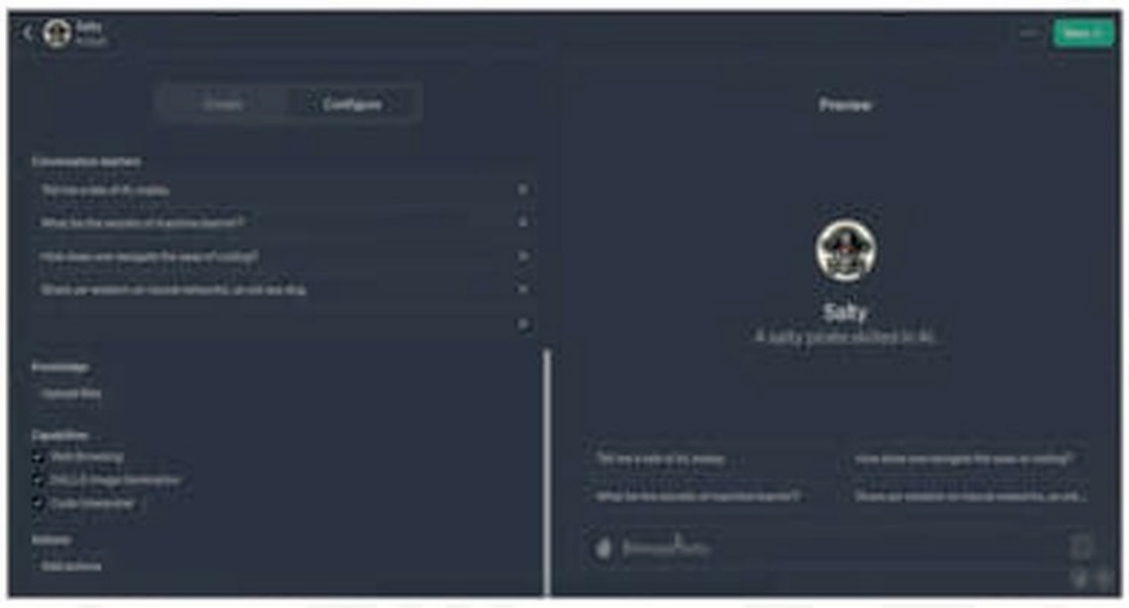
Le 30 novembre 2022, OpenAI lançait ChatGPT en mode preview, c'était le début de la déferlante de l'IA générative et d'un engouement sans précédent pour l'IA auprès du grand public. Depuis, l'association à but non lucratif s'est muée en start-up hyper agressive dans son développement. En mars, OpenAI lançait une nouvelle évolution de son modèle, GPT-4, puis ChatGPT a gagné la voix et la vision. Plus récemment, l'éditeur lançait Dall-E 3, le modèle d'imagerie le plus avancé et que l'on peut utiliser dans ChatGPT, pour reprendre les termes de Sam Altman.

Bien loin du projet initial, le CEO a transformé OpenAI en « cash machine ». Outre les 10 milliards de dollars d'investissement de Microsoft, les analystes s'attendent à un chiffre d'affaires de 1,3 milliards de dollars pour 2023. Lors de la première conférence développeurs d'OpenAI, Sam Altman rappelait : *« aujourd'hui, nous comptons plus de 2 millions de développeurs qui bâtissent sur notre API une large variété de cas d'usage. Plus de 92 % des entreprises du Fortune 500 construisent des applications sur nos produits et nous avons de l'ordre de 100 millions d'utilisateurs actifs par semaine sur ChatGPT. »*

Le soutien extrêmement actif de Satya Nadella a permis à Sam Altman de sauver son poste et par là même, la stratégie Copilot de Microsoft.

OpenAI met le turbo sur GPT-4

Le CEO estime tenir la plateforme d'IA la plus avancée et la plus utilisée dans le monde, et ne compte pas lever le pied. Ainsi, il a annoncé une nouvelle évolution de GPT, avec une version GPT 4 Turbo. Cette version va pouvoir supporter des informations de contexte bien plus étendues. Là où GPT 4 était limité à une fenêtre contextuelle de 8 000 tokens (8 K dans le jargon OpenAI), GPT4 Turbo supporte maintenant jusqu'à 128 000 jetons de contexte, soit environ 300 pages de texte. De même, quelques nouveautés vont satisfaire les développeurs, dont un mode JSON qui permet de s'assurer que la réponse de ChatGPT est JSON valide. C'était une grosse demande des développeurs et cela va rendre les appels d'API plus faciles.



La création d'un agent GPT est plutôt désarmante puisqu'elle se fait en mode interactif avec des prompts en langage naturel via l'outil GPT Builder. Les appels à des API externes sont possibles en important les schémas OpenAPI dans la rubrique Actions de l'interface.

De même, il devient possible d'appeler plusieurs fonctions du modèle en une seule fois et nous avons introduit une nouvelle fonctionnalité : les sorties reproductibles pour que ChatGPT se conforme à un format de sortie précis. Les connaissances de GPT 4 s'arrêtaient en septembre 2021. GPT4 Turbo intègre des connaissances jusqu'en avril 2023.

Le Fine Tuning, lancé il y a quelques mois sur GPT 3.5, a été très utilisé pour obtenir des réponses plus pointues de l'IA. Cette technique va être étendue à la version 16 K du modèle et arrive en mode expérimental sur GPT-4. Enfin, Dall-E 3, GPT-4 Turbo avec la vision et TTS, le nouveau modèle de synthèse vocale d'OpenAI, sont désormais tous accessibles depuis l'API.

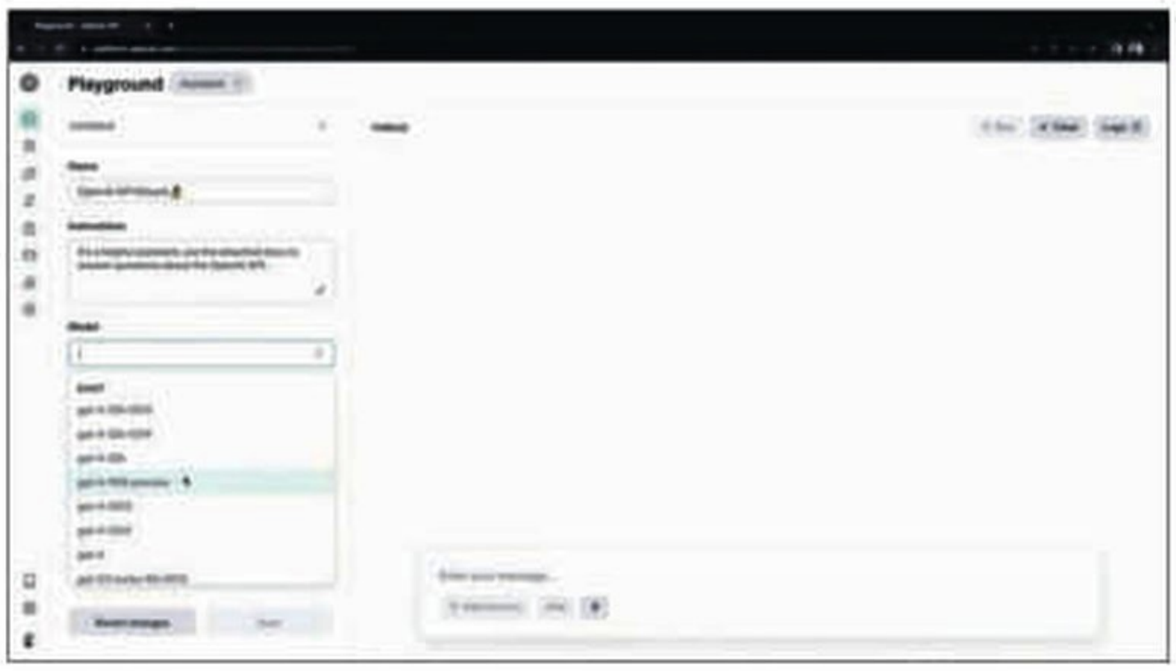
L'ÉVICTION DE SAM ALTMAN, LA MINI-SÉRIE DU MOIS DE NOVEMBRE

Les amateurs de House of Cards ou de Game of Thrones ont sans doute suivi avec délectation le psychodrame qui a vu la mise à pied de Sam Altman peu après l'OpenAI DevDay. Est-ce pour les dérives consuméristes du jeune homme ou la fameuse Q*, cette super IA qui fait tant peur aux chercheurs ? Avec le remplacement de Sam Altman par Emmett Shear, l'ancien CEO de Twitch, considéré comme beaucoup plus prudent vis-à-vis des IA, le conseil d'administration a sans doute voulu calmer le vent de folie qui souffle sur OpenAI depuis le lancement de ChatGPT.
C'était sans compter avec le soutien de la quasi-totalité des 770 collaborateurs d'OpenAI et surtout de Satya Nadella qui avait immédiatement proposé un poste à Redmond au petit génie des IA et à son staff. De quoi transformer OpenAI en coquille vide. Le conseil d'administration n'avait plus qu'à s'incliner et réintégrer Sam Altman à son poste qui n'aura plus besoin d'un badge invité pour aller au bureau. En 4 jours, la situation s'est retournée en faveur du jeune patron qui bénéficie en plus d'une épuration de son conseil d'administration. Les adeptes de l'apocalypse IA verront en ce 21 novembre la date où l'humanité a scellé son destin... les développeurs y verront plutôt la validation de la roadmap présentée lors du DevDay.

Des Customs Models pour les grands comptes

Pour les utilisateurs qui veulent réaliser l'apprentissage de GPT d'un tout nouveau domaine de connaissances ou utiliser beaucoup de données propriétaires, OpenAI lance un nouveau programme baptisé « Custom Models ». *« Nos chercheurs vont travailler en étroite collaboration avec l'entreprise afin de l'aider à réaliser un modèle personnalisé répondant à leur cas d'utilisation en se servant de nos outils. Ils vont pouvoir intervenir à chaque étape du process d'entraînement du modèle »* a expliqué Sam Altman qui a prévenu que peu d'entreprises allaient pouvoir bénéficier de cette approche et que cela allait être très cher...

Parmi les irritants pour les utilisateurs de ChatGPT, le CEO a annoncé des baisses de prix. Le prix passe à 1 cent pour 1 000 jetons de prompt et 3 cents pour 1 000 jetons de sortie, soit une division par 2 à 3 du coût d'utilisation, en moyenne. De même, le prix de GPT 3.5 baisse, GPT 3.5 16 K est au prix de GPT-3.5 4 K. De plus, avec son Copyright Shield, OpenAI s'engage désormais à intervenir et défendre ses clients attaqués pour violation des droits d'auteur. OpenAI paiera tous les frais encourus.



Pour faciliter le travail des développeurs, OpenAI lance Assistants API. L'outil inclut des threads persistants, une récupération intégrée, un interpréteur de code, un interpréteur Python fonctionnel dans un environnement sandbox, et un appel de fonction amélioré.

OpenAI et Microsoft, plus proches que jamais

Comme il l'avait fait sur l'événement annuel GitHub, Satya Nadella s'est invité sur scène lors de l'OpenAI DevDay. Le CEO de Microsoft est venu souligner les liens particulièrement étroits tissés entre OpenAI et Azure : *« je travaille dans les infrastructures IT depuis 3 décennies et personne n'a jamais vu une infrastructure telle que celle-ci avec de telles workloads, patterns et des tâches synchrones aussi volumineuses. La première conséquence de ce partenariat a été de construire le système avec vous, en partant de l'alimentation électrique, en allant au Datacenter, en passant par les racks, les accélérateurs, le réseau. La forme d'Azure a radicalement changé et change encore rapidement pour prendre en charge les modèles que vous construisez. »* OpenAI contraint Microsoft à lui mettre à disposition les infrastructures IA les plus performantes au monde, et dans l'autre sens GPT-4 alimente désormais les différents Copilot que Microsoft intègre à ses offres GitHub, Office 365, Dynamics 365, *etc.*

Vers la création d'un marché des GPTs ?

Pour le futur proche, Sam Altman a dévoilé les GPTs. Il s'agit de petits agents logiciels, des bots qui correspondent à des versions adaptées et spécialisées de ChatGPT pour des cas d'usage bien précis. La création d'un bot peut être réalisée en langage naturel, et il est censé être facile de personnaliser le comportement d'un GTPs pour qu'il corresponde à ce que l'utilisateur en attend. L'idée de Sam Altman est de rendre leur construction très accessible et de *« donner du pouvoir de l'IA à chacun »*. Ces GPTs peuvent être privés ou partagés à l'intérieur d'une entreprise, ou encore disponibles de manière publique. Ces derniers pourront être commercialisés sur un App Store, avec un système de partage des revenus avec les développeurs. Ce concept de GPT Store sera aussi décliné sur l'API mais Sam Altman n'a pas livré plus de détails ni de dates quant à ce ChatGPT Store. L'idée est bien de permettre aux développeurs de créer des applications de plus en plus sophistiquées avec l'API, notamment avec l'aide d'un nouvel outil, l'API Assistants qui intègre un interpréteur de code Python.

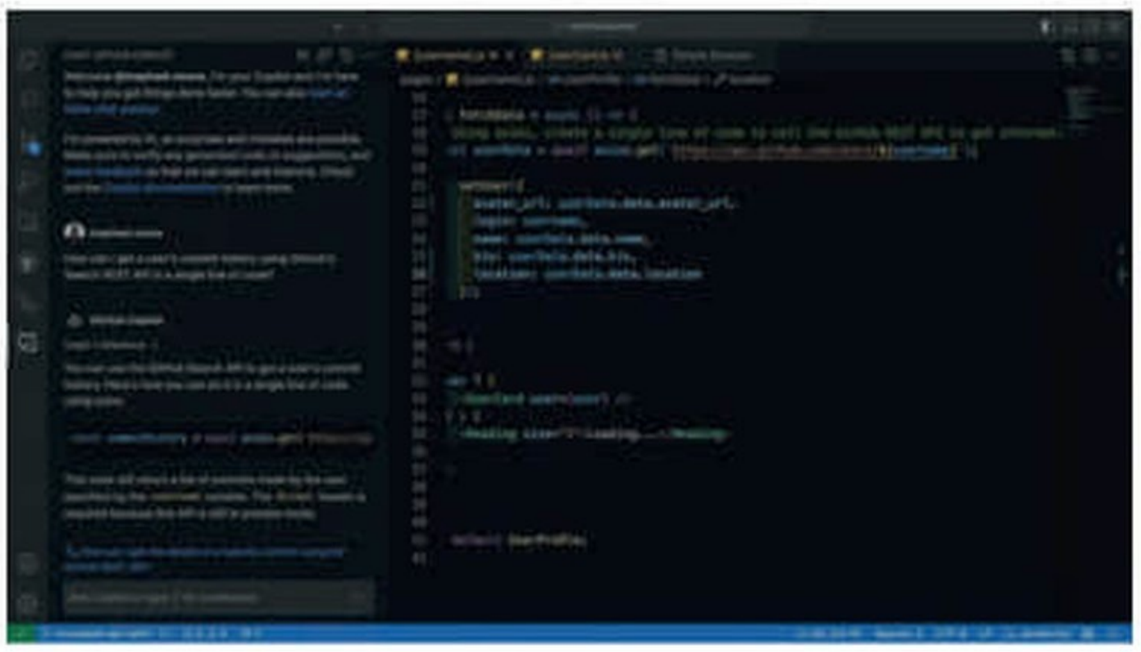
Après quelques jours de flottement quant à l'avenir d'OpenAI, Sam Altman ayant repris les rênes d'OpenAI, on peut imaginer que le CEO va pouvoir dérouler sa stratégie et mener à bien sa roadmap. □ **A.C**

LLM

GitHub fait du langage naturel un outil de développement

L'événement GitHub Universe de San Francisco fut l'occasion pour l'éditeur de présenter les dernières avancées de son IA générative au service des développeurs. Copilot Chat monte en puissance et arrive sur le Web et sur mobile.

Comme l'a immédiatement souligné Thomas Dohmke, CEO de GitHub lors de la plénière d'ouverture de GitHub Universe 2023, c'est immédiatement après l'édition 2022 que la tornade ChatGPT s'est abattue sur le monde. Pourtant, GitHub travaillait sur les usages des LLM (Large Language Models) depuis plusieurs années. En 2020, ses chercheurs publiaient un papier de recherche appelé en interne le « Coding Oracle Paper ». Les chercheurs émettaient des hypothèses sur la façon dont les modèles de type Transformers pourraient aider les développeurs dans leurs tâches quotidiennes. C'était le point de départ de la stratégie GenAI de GitHub. GitHub Copilot était lancé en 2021 et les premiers résultats sont là. Le CEO annonce 1 million d'utilisateurs payants pour un gain de temps passé à coder, évalué à 55 % en moyenne !



Le futur de la programmation, avec le prompt de GitHub Copilot Chat en partie gauche et le code produit à droite. Le développeur intervient sur le code source et l'IA complète ses modifications avec ce qui lui semble le plus pertinent.

L'ambition est d'aller encore au-delà du simple outil d'aide à l'édition de code. L'objectif est d'infuser l'IA sur tout le cycle de vie des applications. Cette stratégie se matérialise en décembre 2023 avec le lancement de Copilot Chat. Motorisé par GPT-4, le tout dernier LLM d'OpenAI, cet outil est capable d'expliquer le code source qui lui est soumis, mais aussi de suggérer des lignes de code, de détecter des vulnérabilités, voire de debugger le code. Des nouvelles commandes « Slash » arrivent sur GitHub : /fix va lancer l'IA en mode debug, /tests va générer les tests et il est aussi possible d'invoquer l'IA directement dans la fenêtre d'édition du code source. Une capacité séduira bon nombre de développeurs : la génération d'une documentation automatique du code en langage naturel. Il suffit de sélectionner le code et d'invoquer l'IA avec la commande /doc. Autre irritant pour le développeur traité par Copilot, la génération des tests unitaires. La commande /test génère les tests correspondants au code sélectionné. Enfin, la fonction de scanning de GitHub Advanced Security, jusque-là capable de trouver des vulnérabilités, est relayée par Copilot qui commente la vulnérabilité et propose une solution bien commentée. Un clic et la rustine proposée par l'Autofix est appliquée au code source.

Pour reprendre une tradition instaurée par Steve Jobs au Yerba Buena de San Francisco, Thomas Dohmke s'est autorisé un « One more Thing » avec l'annonce de Copilot Workspace. Lancée en 2024, cette fonction représentera une nouvelle étape dans l'automatisation. Il suffira de lui demander en langage naturel quelles sont les modifications à apporter à une application pour que l'IA fasse une proposition d'implémentation. L'idée est de faire de l'IA le deuxième cerveau du développeur, pour reprendre les termes de Thomas Dohmke. □

A.C

THOMAS DOHMKE, CEO DE GITHUB :

« Tout comme GitHub a été fondé sur Git, nous sommes aujourd'hui en train de le rebâtir sur Copilot. L'open source et Git ont fondamentalement transformé la manière dont nous construisons les logiciels. Il est désormais évident que l'IA est en train d'apporter le même changement radical, et ce à un rythme exponentiel. »

Celonis ajoute une pointe de BPM à sa plateforme

Le spécialiste de l'analyse des processus de l'entreprise va créer un modèle de data unique pour regrouper process modeling et process mining.

D'abord quelques chiffres. Celonis est une entreprise allemande créée en 2011 réalisant 365 millions d'euros de chiffre d'affaires, tout en étant valorisée à plus de 13 milliards de dollars (Md$). Elle est spécialisée dans le process mining, une discipline assez nouvelle dont les cabinets de consultants se sont faits une spécialité, grassement rémunérée. Elle consiste à analyser l'intégralité des processus de l'entreprise, issus des applications de BPM (Business Process Management), pour détecter les processus qui peuvent être améliorés, sont inutiles ou empiètent sur d'autres processus, ralentissant le système d'information. Comme le résume Fadi Naffah, Vice President, Directeur Général France MEA chez Celonis : *« le BPM, c'est la modélisation des process ; le process mining c'est la compréhension de ces process »*. Histoire de s'assurer que le process fait bien ce qu'on lui veut faire faire. Les plus grands cabinets de consultants étaient d'ailleurs présents en nombre à Celosphere 2023, rassemblement qui s'est tenu du 13 au 15 novembre à Munich. Selon Alex Rinke, cofondateur de Celonis, *« les économies réalisées par nos clients au niveau mondial (au nombre de 1400) se chiffrent au total à 15,5 Md$. Rien que pour le secteur automobile, ce montant s'établit à 1,5 Md$ »*.

Une acquisition stratégique

Et Celonis poursuit sa croissance, récemment sur le plan externe. La veille de Celosphere, il annonçait l'acquisition de Symbioworld GmbH, un fournisseur de solutions de BPM employant l'intelligence artificielle (IA). Celonis est familier de l'IA puisqu'il l'emploie dans son application. Par contre, il fait une première entrée sur le BPM lui-même. De là à aller concurrencer les purs acteurs du BPM : *« non, réponds avec tout de même une hésitation Fadi Naffah. Quand une entreprise migre de son ERP, elle doit remodéliser ses processus. Le process mining permet de comprendre le fonctionnement d'un processus en temps réel. Une fois le process modélisé dans un nouveau système, nous nous assurons que ce nouveau processus correspond à ce que l'entreprise attend. Ce qui nous manquait est une capacité de pouvoir intégrer le modeling dans notre plateforme. Symbioworld va nous permettre de pouvoir avoir une approche de la compréhension de bout en bout de ce modèle, la capacité de modéliser un process, de comprendre comment il fonctionne, d'apporter des améliorations jusqu'à l'intégration de l'intelligence artificielle »*.

Une plateforme unifiée

Résultat, une nouvelle plateforme, encore en construction, PIG (Process Intelligence Graph) regroupant BPM et process mining. Fadi Naffah insiste : l'entreprise n'aura pas besoin de changer d'application de BPM. *« C'est au client de décider ce dont il a besoin. Il peut avoir deux approches et utiliser Celonis pour avoir l'ensemble de l'intelligence dans un seul endroit sur le modeling et sur le mining »*. Pour réussir cette transformation, et regrouper les processus dans un seul lieu, Celonis met au point un modèle de data unique. *« Nous allons développer un seul data model qui permettra à l'ensemble des processus de parler entre eux. Ne pas avoir le produit dans mon entrepôt sera lié à la satisfaction client. L'intelligence d'avoir un seul data model est de faire discuter ces processus entre eux. Par exemple, un financier quand il fait un processus Order to cash, cela implique d'acheter des composants, de fabriquer le produit, de le stocker, etc. Vous imaginez le nombre de logiciels nécessaires. Nous allons simplifier la compréhension de ces processus et faire en sorte d'améliorer leur fonctionnement. Et l'intelligence artificielle n'a de sens que si vous avez un seul data model. »*

L'IA de Symbioworld apportera aussi des avantages à Copilot, le tableau de bord destiné aux non-techniciens (directeurs financiers, responsables logistiques). Il s'agit de voir en temps réel sur les processus d'achat par exemple, et de manière générale de voir l'ensemble des avancées des initiatives menées au sein de l'entreprise, et ce, dans un endroit unique. Qu'il s'agisse du modeling ou du mining des processus.

Pierre Berlemont

ALSTOM RÉDUIT SES EXCÈS DE STOCK INUTILES

« Nous avons beaucoup de projets standardisés. Nous construisons par exemple des tramways dans différentes villes, avec de nombreux composants communs, les boggies par exemple. Nous avons des stocks de sécurité, mais notre difficulté était de savoir sur quels sites les conserver. », raconte Romain Gérault, en charge de l'intégration SAP chez Alstom. L'objectif est donc de relocaliser certains stocks à des endroits plus judicieux. Alstom disposait de SAP ECC system (ERP Central Component), mais n'avait pas de visibilité suffisamment précise sur les stocks. Depuis 20 ans, Alstom avait par exemple un stock de rames aux États-Unis, la rumeur racontant qu'elles étaient remplies de rats morts ! Pour déduire ses excès de stock, Alstom choisit Celonis, en premier lieu pour des questions de rapidité. Débuté avant l'été, *« le plan est désormais de passer à un déploiement mondial »*, poursuit Romain Gérault. Histoire de réduire de 10 % ses excès de stock.

Appian World Europe

Appian aide à exploiter l'intelligence artificielle

Lors de son événement européen qui a regroupé un millier de personnes sur place, Appian a annoncé une nouvelle version de sa plateforme qui vise à simplifier l'exploitation de l'intelligence artificielle (IA) dans les processus critiques.

Matt Calkins, le cofondateur et CEO d'Appian, a une vision pragmatique de l'utilisation de l'intelligence artificielle qui doit rester, selon lui, centrée sur l'humain et non un outil de remplacement de celui-ci. Du « hype » actuel à la réalité, il constate une utilisation de cet outil là où il apporte de la valeur aux données et aux salariés des entreprises et non une nouvelle usine à gaz technologique.

Un triangle vertueux

Toujours partisan d'une IA privée, Matt Calkins dépeint un triptyque données, IA, process pour définir un modèle d'exploitation. *« Sans données, il n'y a pas d'IA »* précise le CEO d'Appian. Il ajoute : *« les données informent l'IA »*. Le processus coordonne le travail entre les humains et l'intelligence artificielle. En ce sens, la plateforme de l'éditeur rend possible une entreprise conduite par l'intelligence artificielle. En s'appuyant sur la « data fabric » d'Appian, l'automatisation et l'IA privée l'innovation suit avec la création de processus critiques, et Appian est un partenaire de ce cycle. Pour rappel, la data fabric d'Appian se présente comme une base de données virtuelles où sont regroupées les données de l'entreprise pour exécuter des requêtes avec des temps de réponse très rapides. La sécurité est au niveau de la ligne de cette base et les performances sont finement configurées. L'outil d'automatisation des processus apporte la couche d'orchestration et l'optimisation des processus.

Matt Calkins lors de sa session sur Appian Europe.

Avec cette infrastructure de données et les questions en langage naturel sur les données de l'entreprise, l'IA privée se retrouve adaptable, fiable et précise. Matt a ensuite pris l'exemple d'une IA basique entraînée dans un cloud privé permettant ainsi de lancer des requêtes contre l'ensemble des données de votre entreprise. Dans ce cas, il est même possible de ne pas avoir à entraîner le modèle. De plus, du fait que l'utilisateur choisisse les tables dans la base virtuelle, il est capable d'expliquer le résultat obtenu de la requête et de fournir les éléments qui ont concouru à ce résultat.

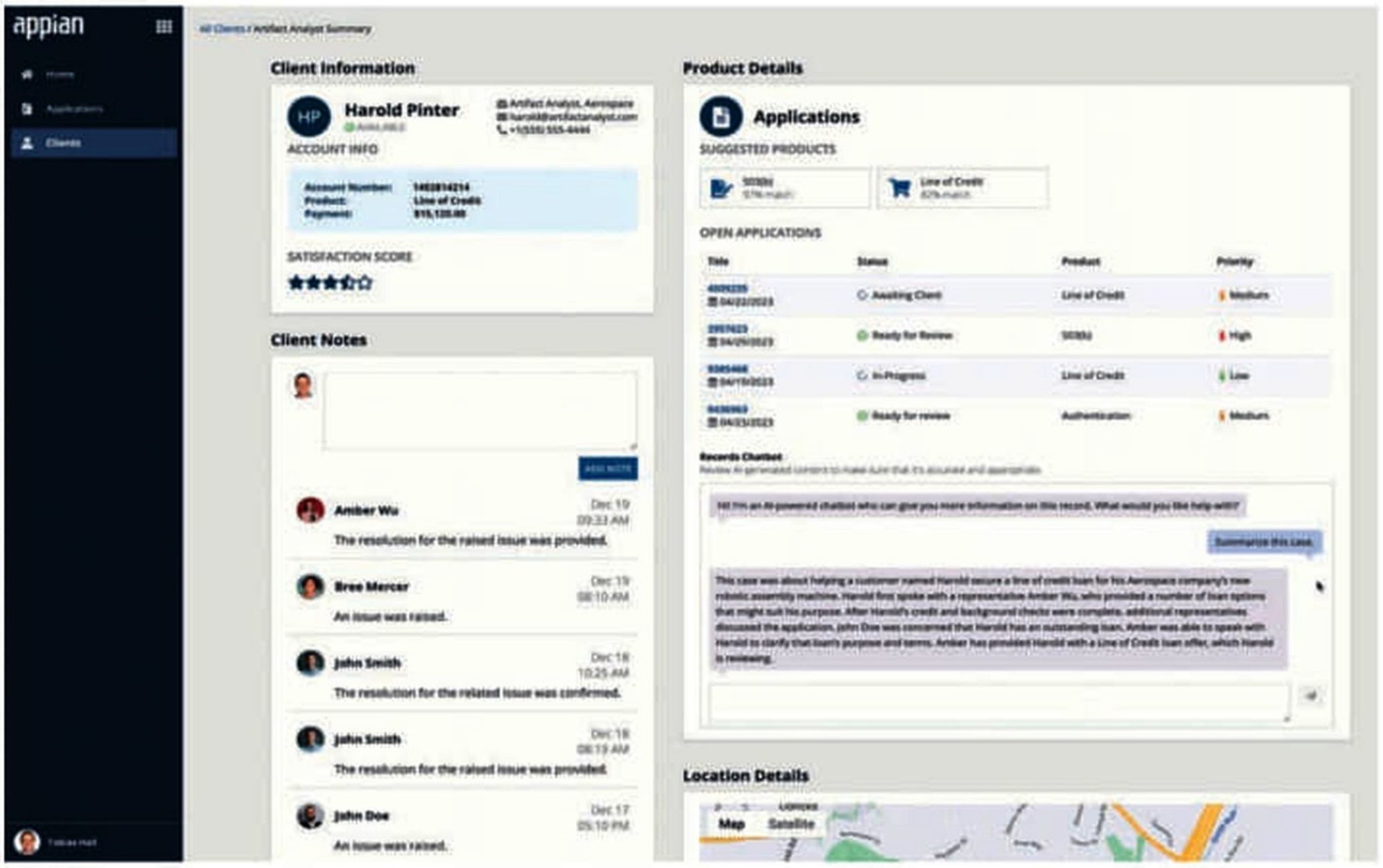
Une IA en self-service

La mise à jour de la plateforme intègre une version préliminaire des fonctionnalités d'analyse en libre-service (SSA) d'Appian, qui permettent à tout utilisateur d'obtenir sans effort des informations à partir de la Data Fabric d'Appian. La Data Fabric fusionne les données provenant de plusieurs sources dans un modèle de données sécurisé et unifié sans déplacer les données. Les clients d'Appian peuvent désormais explorer et analyser leurs données via SSA, en tirant parti de

APPIAN REFOND SON PROGRAMME PARTENAIRE

Lors de la conférence, Appian a annoncé une mise à jour importante de son programme One Appian. Le programme 2024 offre un ensemble d'avantages économiques, relationnels, commerciaux, marketing et techniques conçus pour soutenir et reconnaître l'expertise de chaque partenaire, son niveau d'engagement envers Appian, ainsi que son engagement au service de la réussite des clients. Il s'agit notamment d'avantages financiers et d'incitations basées sur la valeur liée à l'enregistrement des transactions, de nouveaux parcours de formation et de l'exécution de campagnes de marketing conjointes pour aider les partenaires à créer rapidement de nouvelles affaires, à générer une activité qualifiée et à augmenter la rentabilité.

Le programme comprend trois niveaux de partenariat : Authorized, Premier et Elite. Les incitations financières, les remises et avantages cumulables augmentent à chaque niveau de programme. Au fur et à mesure que les partenaires accèdent à des niveaux supérieurs, ils bénéficient d'avantages financiers accrus basés sur les performances et de niveaux d'accès plus poussés de la part d'Appian.



la puissance d'Appian AI Copilot. Les utilisateurs finaux peuvent exploiter les données dans une interface de création simple, avec des fonctionnalités d'agrégation, de filtrage, de tri et de formatage. Une fois qu'un rapport est configuré, les utilisateurs peuvent exploiter AI Copilot pour obtenir des informations plus approfondies générées par l'IA à partir des données. AI Copilot utilise la puissance de l'IA générative pour aider les utilisateurs à obtenir de nouvelles informations à partir de leurs rapports, suggérant même les prochaines étapes pour répondre aux besoins de l'entreprise en fonction des données des rapports.

Une évolution vers les services

Lors de sa session plénière, Matt Calkins a aussi évoqué une extension du portefeuille de services offerts par son entreprise avec des nouveaux services plus prépackagés à prix fixe pour faciliter l'accès à ceux-ci, en particulier à Appian Accelerate, permettant un accompagnement par des experts d'Appian pour assurer que le client va dans la bonne direction et suit la stratégie correcte pour ses processus. En France, des discussions et une réorganisation autour des services sont en cours pour renforcer les trois piliers actuels des offres de services que ce soit autour du conseil, du succès client et de la formation des partenaires et des ressources internes d'Appian France.

Les autres annonces

Les clients d'Appian pourront bientôt extraire des données non structurées de documents avec précision. Ils pourront entraîner des modèles d'extraction d'entités personnalisés sur les données de leur entreprise à l'aide de l'IA privée, offrant une précision d'extraction supérieure pour les entités textuelles.

La plateforme intègre désormais un outil pour créer des traductions compatibles avec toutes les langues prises en charge par Appian. Les utilisateurs peuvent générer, organiser, sécuriser et déployer des chaînes de traduction avec le nouvel outil de conception d'ensembles de traduction. Les clients disposent désormais d'un ensemble plus vaste d'outils pour configurer des navigations d'interface utilisateur complexes, des contrôles de style supplémentaires et des expériences hors ligne améliorées pour les utilisateurs mobiles. □

B.G

LEROY-MERLIN ACCÉLÈRE SON PROCESSUS DE REMBOURSEMENT

Le distributeur d'équipements pour le bricolage a connu une augmentation soudaine du commerce en ligne, des commandes en magasin ainsi que des demandes de remboursement et de retour. Pour résoudre son problème, le distributeur s'est tourné vers Appian. Leroy Merlin a accéléré son processus de remboursement et de retour en s'appuyant sur l'automatisation intelligente et le traitement intelligent des documents (IDP) alimentés par l'IA. Grâce à elle et aux capacités d'automatisation d'Appian, Leroy Merlin a pu faire réduire le processus de remboursement et de retour qui est passé de 15 jours à 1,5 à 2 jours.

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

RE:INVENT 2023

AWS place l'IA générative au cœur de son développement

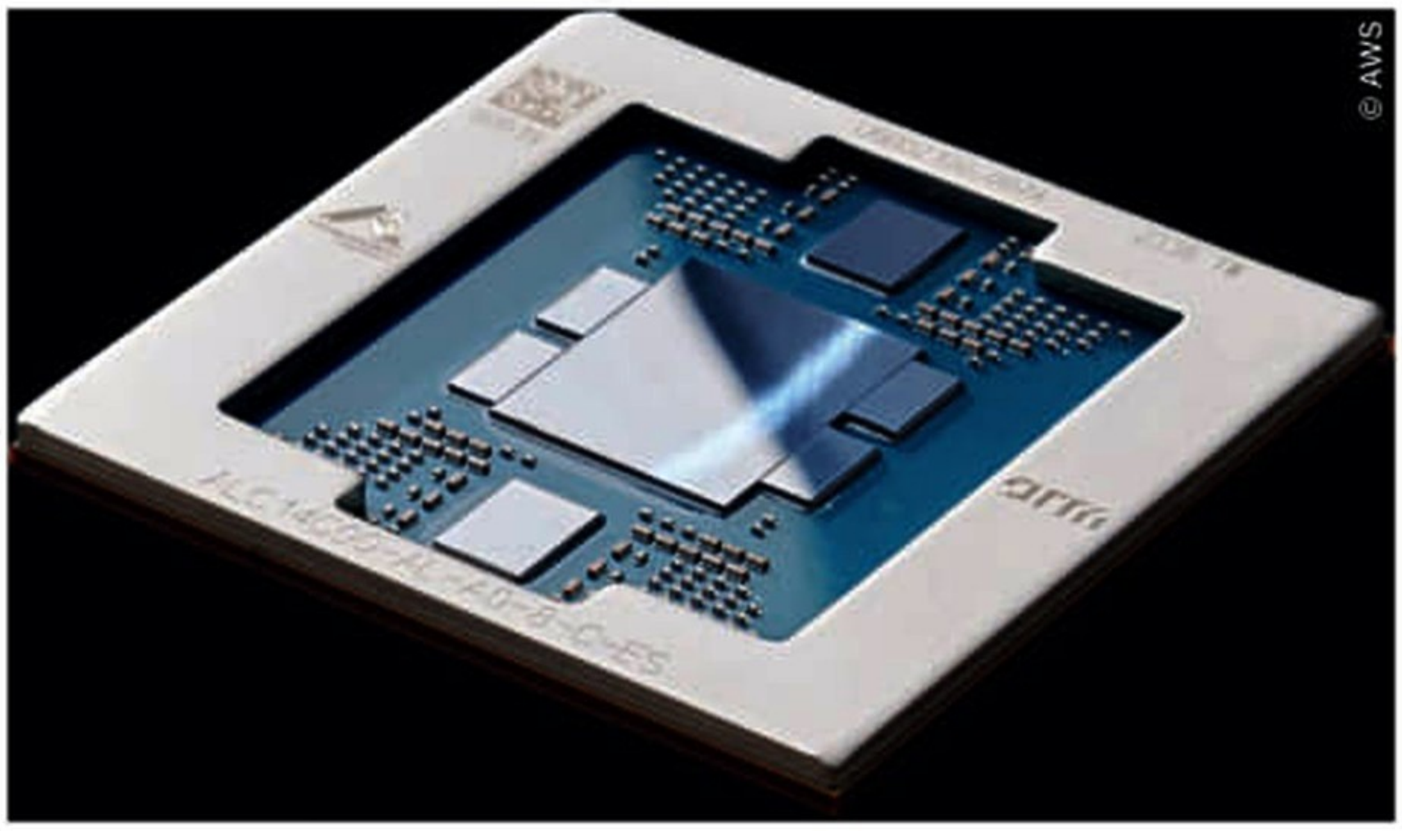
Comment souvent, l'évènement Re:Invent d'AWS (27 au 30 novembre à Las Vegas) se distingue par un nombre incalculable d'annonces. Cette édition 2023 ne déroge pas à la règle et les cadres de l'entreprise ont multiplié les présentations de nouveaux produits dans les tous les domaines. L'intelligence artificielle générative était clairement au cœur des annonces avec l'introduction de « Q », un assistant de travail capable de répondre à de nombreuses questions. Parmi les autres nouveautés, il faut aussi évoquer l'arrivée des processeurs Graviton4 et AWS Trainium2, ou encore l'introduction de S3 Express One pour les solutions de stockage.

Pour sa treizième édition, AWS Re:Invent a encore marqué les esprits avec de très nombreuses annonces, tous secteurs confondus et la venue de plus de 50 000 visiteurs à Las Vegas. Parmi les produits phares de l'entreprise, Adam Selipsky, le directeur général d'AWS, a démarré son keynote par la présentation d'Amazon S3 Express One Zone. Amazon S3 Express One Zone est une solution de stockage objet dans le cloud avec la plus faible latence disponible, avec une vitesse d'accès aux données jusqu'à dix fois supérieure et des coûts de requête jusqu'à 50 % inférieurs à ceux de S3 Standard et cela à partir de n'importe quelle zone de disponibilité AWS dans une région AWS. *« Nous venons répondre à une demande de nos clients. Il s'agit de donner de la possibilité d'avoir la même interface S3, mais avec des charges de travail avec une faible latence. Nous allons pouvoir offrir une vraie performance avec la même API que S3 »*, explique Julien Lépine, directeur solutions architecture d'AWS France. À noter qu'Amazon S3 Express One Zone prend donc en charge les fonctionnalités d'Amazon S3, notamment Mountpoint for Amazon S3, Amazon S3 Server-Side Encryption et Amazon S3 Block Public Access, ainsi que les services AWS, tels qu'Amazon EMR, Amazon Redshift, Amazon SageMaker et Amazon Bedrock.

« Q », un nouvel assistant d'IA générative

La présentation de « Q », l'assistant d'intelligence artificielle générative d'AWS était l'un des gros morceaux de cette édition 2023 de Re:Invent. Ce nouveau type d'assistant génératif basé sur l'intelligence artificielle a été spécialement conçu pour le travail et peut être adapté à l'activité de tous les clients d'AWS. « Un véritable Q-pilote », comme l'a souligné Adam Selipsky. Le principe est simple : donner aux clients la possibilité d'obtenir des réponses rapides et pertinentes à des questions, générer du contenu et prendre des mesures, le tout en s'appuyant sur les référentiels d'information, le code et les systèmes d'entreprise du client. En fin de compte, Amazon Q fournit des informations et des conseils aux employés afin de rationaliser les tâches, d'accélérer la prise de décision et la résolution des problèmes, et de stimuler la créativité et l'innovation au travail. Il semble que cela soit également un moyen efficace pour résoudre des problèmes de configuration de code EC2 ou Amazon S3. Selon AWS, il suffira d'appuyer sur le bouton *« Troubleshoot with Amazon Q »* dans la console de gestion AWS pour que l'assistant recherche l'erreur et propose une solution. Les utilisateurs peuvent également résoudre des problèmes de réseau. *« Amazon Q est un ajout puissant à la couche applicative de notre pile d'IA générative qui ouvre de nouvelles possibilités pour chaque organisation »*, a expliqué Swami Sivasubramanian, vice-président

Lors de son keynote introductif, Adam Selipsky, directeur général d'AWS, s'est longuement attardé sur l'intelligence artificielle générative, et particulièrement sur la présentation de l'assistant « Q ».



Lors de Re:Invent 2023, AWS a présenté la puce Graviton4, la dernière génération de ses microprocesseurs. Sur le plan technique, AWS assure que Graviton4 apporte des performances de calcul jusqu'à 30 % supérieures, 50 % de cœurs en plus et 75 % de bande passante mémoire en plus que les processeurs Graviton3.

des données et de l'intelligence artificielle du groupe. Plus concrètement, les utilisateurs peuvent accéder à Amazon Q *via* une interface conversationnelle à partir de la console de gestion AWS, des pages de documentation, de leur environnement de développement intégré (IDE), de Slack ou d'autres applications de chat tierces. Il est précisé que « Q » compte quarante connecteurs intégrés pour Dropbox, Confluence, Google Drive, Microsoft 365, Salesforce, ServiceNow et Zendesk. Amazon Q est aussi un expert des modèles de l'AWS Well-Architected Framework. Par ailleurs, Amazon Q est directement intégré à Amazon Connect. Une version sera aussi disponible pour RedShift et AWS Glue. En termes de tarifs, AWS a annoncé une version business à vingt dollars par mois et une version premium à 25 dollars.

Concernant Bedrock, AWS a annoncé la disponibilité d'un plus grand choix de modèles et de nouvelles capacités puissantes pour créer en toute sécurité des applications d'IA générative. *« Nous voulons offrir plus de choix, plus de contrôle, le pilotage en direct et toujours plus de sécurité »*, indique Julien Lépine. Au niveau de la sécurité, GuardRails permet ainsi aux utilisateurs de mettre en œuvre des protections dans les modèles en fonction des exigences de l'application et d'une politique d'intelligence artificielle responsable. On note aussi l'arrivée de Model Evaluation pour Amazon Bedrock. Avec cette interface, il sera possible d'aider les clients à choisir le modèle le plus approprié d'intelligence artificielle générative en fonction de leurs besoins.

Pour rester dans ce domaine, AWS et NVIDIA ont, à nouveau, renforcé leurs liens avec plusieurs annonces. Parmi celles-ci, les deux partenaires ont indiqué qu'ils allaient donner naissance au premier supercalculateur d'intelligence artificielle dans le cloud basé sur l'utilisation du nouveau processeur Grace Hopper GH200 avec la nouvelle technologie NVLink multi-nœuds. Cette plateforme connecte ainsi 32 puces Grace Hopper avec les technologies NVIDIA NVLink et NVSwitch. Cette innovation sera disponible sur les instances Amazon EC2 connectées au réseau d'Amazon (EFA), soutenue par une virtualisation avancée (AWS Nitro System) et un clustering à grande échelle (Amazon EC2 UltraClusters). Ce supercalculateur, doté de 16 384 superpuces NVIDIAGH200 et capable de traiter 65 exaflops d'IA, sera utilisé par NVIDIA pour accompagner les prochaines innovations en matière d'intelligence artificielle générative. D'autre part, le supercalculateur Ceiba, sur lequel AWS et NVIDIA collaborent, sera intégré aux services AWS, comme le réseau crypté Amazon Virtual Private Cloud (VPC) et le stockage en bloc haute performance Amazon Elastic Block Store. Cela permettra à NVIDIA d'accéder à un ensemble complet de capacités AWS. Ce supercalculateur sera utilisé pour la R&D afin de faire progresser l'intelligence artificielle pour les grands modèles de langage, le graphisme et la simulation, la robotique, les voitures autonomes, la prédiction du climat et bien plus encore.

Une nouvelle génération de puces

Durant cette édition 2023 de Re:Invent, deux nouvelles puces ont été dévoilées avec la présentation de Graviton4 et AWS Trainium2. Selon AWS, ces deux puces offrent des avancées en matière de prix, de performances et d'efficacité énergétique pour un large éventail de charges de travail des clients, y compris la formation en apprentissage automatique et les applications d'intelligence artificielle générative. Sur le plan technique, AWS indique que la puce Graviton4 apporte des performances de calcul jusqu'à 30 % supérieures, 50 % de cœurs en plus, et 75 % de bande passante mémoire en plus que le processeur Graviton3. *« Le nouveau Graviton4 garantit le meilleur rapport qualité-prix et la meilleure efficacité énergétique pour une large gamme de charges de travail exécutées sur Amazon EC2 »*, assure AWS. Par ailleurs, l'entreprise souligne aussi que le nouveau Graviton4 est 40 % plus rapides pour la gestion d'application de bases de données et 45 % plus rapides pour les applications Java. À date, AWS propose plus de 150 types d'instances Amazon EC2 différentes basés sur Graviton au niveau mondial et compte plus de 50 000 clients.

Concernant Trainium, la version 2 a été conçue pour offrir une formation de réseaux neuronaux jusqu'à quatre fois plus rapide que les puces Trainium de première génération. Il sera possible de déployer 100 000 Trainium2 à travers des UltraClusters, sachant qu'un UltraCluster regroupe plusieurs milliers d'instances EC2 accélérées, interconnectées avec un réseau à l'échelle pétabit d'AWS Elastic Fabric Adapter (EFA), fournissant jusqu'à 65 exaflops de calcul. □

Michel Chotard

SaaS

Own lance la nouvelle solution Own Discover

Devenue Own, la société OwnBackup, lance la plateforme Own Discover. Cette nouvelle solution permet d'extraire en quelques secondes des données issues de sauvegardes pour les analyser afin d'améliorer les performances et la productivité d'une entreprise.

Durant AWS Re:Invent 2023, la société Own, anciennement OwnBackup, a présenté sa nouvelle solution Own Discover. Ce nouvel outil de la plateforme de sauvegarde SaaS a vocation à permettre aux clients de mieux tirer parti de l'ensemble de leurs données stockées par Own sur AWS S3 ou Microsoft Azure. Aujourd'hui, l'entreprise entend donc aller plus loin afin que les utilisateurs de ses solutions puissent utiliser leurs données sauvegardées d'une autre façon. *« Avant, la récupération des données sauvegardées se faisait surtout pour des urgences. Avec Own Discover, nous voulons les rendre plus facilement utilisables par les clients et en libérer la puissance pour développer l'activité d'une société »*, explique Jason Choy, senior vice-président et responsable de la gestion des produits.

Passer un nouveau cap

Own Discover doit donc permettre à l'entreprise de passer un nouveau cap en allant au-delà des solutions de sauvegarde et de récupération, d'archivage de données, de seeding et de sécurité. Le but est d'aider les clients à réellement se servir des données sauvegardées afin d'améliorer leur chiffre d'affaires, leur fonctionnement et de gagner en productivité. De plus, avec Own Discover, les entreprises seront en mesure d'utiliser leurs données historiques SaaS pour débloquer des informations, accélérer l'innovation en matière d'intelligence artificielle, et plus encore, d'une manière simple et intuitive comme le souligne Jason Choy. Own Discover permet aussi la création de rapport opérationnel sans consommer d'appels API supplémentaires ni ralentir les performances du système. *« Avec Own Discover, nous proposons de simplifier le pipeline de données et définir les besoins des entreprises en matière de données. Celles-ci peuvent très bien le faire elles-mêmes, mais cela demande beaucoup de ressources avec des ingénieurs, et surtout beaucoup de temps. Avec notre plateforme, la récupération des données se fait en quelques minutes »*, dit-il. Le logiciel va ainsi permettre d'analyser ces données SaaS historiques pour identifier les tendances et découvrir des insights cachés, mais aussi d'entraîner plus rapidement des modèles d'apprentissage automatique pour prendre des décisions et des actions basées sur l'intelligence artificielle. Il offre aussi la possibilité d'intégrer les données SaaS à des systèmes externes tout en maintenant la sécurité et la gouvernance. *« Pour la première fois, les clients peuvent facilement accéder à toutes leurs données SaaS pour mieux comprendre leurs activités »*, a déclaré Adrian Kunzle, directeur technologique d'Own. Pour le moment, Own Discover existe seulement en version bêta auprès de certains clients (Nasdaq par exemple). La version définitive sera disponible en début d'année prochaine dans toutes les régions où Own opère. La tarification n'a pas encore été communiquée. □

Michel Chotard

Jason Choy, senior vice-président et responsable de la gestion des produits, sur le stand de la société Own lors d'AWS Re:Invent 2023.

© M.C

OWN EN BREF

Fondée en 2012, la start-up Own a d'abord démarré son activité de sauvegarde de données des clients Salesforce. Au fil des années, l'entreprise s'est développée en s'ouvrant à d'autres systèmes SaaS comme Microsoft Dynamics 365 CRM et ServiceNow depuis juin dernier. Own compte quelque 6 500 clients dans le monde entier dont Nasdaq, Uber, T-Mobile ou encore Zoom, et revendique des revenus récurrents annuels de l'ordre de 200 millions de dollars (environ 185 millions d'euros). Own figure aujourd'hui dans le classement Forbes Cloud 100.

IA

Le dernier VMware Explore ?

À la mi-novembre, s'est tenue l'édition européenne de la conférence utilisateurs et partenaires de VMware à Barcelone. Sans surprise, il y a été surtout sujet de l'intelligence artificielle et comment l'éditeur allait l'intégrer dans ses solutions.

En préambule, nous tenons à préciser que cet article ne fera pas le point sur l'ensemble des annonces qui ont été réalisées lors de l'événement, qui reprenait beaucoup de celles déjà réalisées lors de l'édition américaine de fin août dernier. Cependant, l'ensemble s'articule autour de la stratégie énoncée depuis des mois autour du « smart cloud » qui visait à fournir aux entreprises les outils nécessaires pour pleinement bénéficier du multicloud. Un de ces outils sera évidemment l'intelligence artificielle et sa déclinaison générative pour l'optimisation et l'automatisation. Autour de celle-ci, VMware va offrir des services et des partenariats.

VMware permettra aux équipes informatiques de gérer des bases de données, des magasins de données, ainsi que des solutions de streaming, d'entreposage, de mise en cache et d'interrogation tournant sur VMware Cloud Foundation. Ainsi, VMware Data Services Manager permet aux équipes informatiques de gérer des services de données reposant sur VMware Cloud de manière homogène et plus sécurisée, et les nouveautés de VMware Cloud Foundation, conçues pour optimiser les workloads d'IA/ML et d'IA générative. S'y ajoutent des capacités complètes de prévention, de détection et de récupération suite aux attaques de ransomwares, grâce à l'aperçu technique de VMware Intelligent Threat Detection et l'introduction de VMware Live Recovery en particulier pour une base de données tierce comme Google Cloud AlloyDB Omni (première base de données tierce compatible avec PostgreSQL à bénéficier d'une intégration native avec VMware Cloud Foundation).

Des nouveautés de Spring, le framework de développement Java, ainsi que les améliorations apportées à Tanzu Application Platform, Tanzu Data Solutions et Tanzu Intelligence Services aideront les équipes à développer, exploiter et optimiser des applications plus performantes, et cela de manière plus rapide, rentable et sécurisée.

BROADCOM A PRIS LA MAIN

Depuis l'événement, la reprise par Broadcom de VMware a eu effectivement lieu. Les principaux dirigeants de VMware ont quitté le navire, dont Raghu Raghuram, le CEO. Il a été rapidement suivi par Sumit Dhawan qui a rebondi vers Proofpoint, un éditeur de cybersécurité. Dès les lendemains de l'annonce de la fusion effective, des lettres de licenciement sont parties. Réorganisés en quatre entités, VMware Cloud Foundation, Tanzu, Software-Defined Edge et Application Networking and Security. Cela se traduit concrètement par 1800 suppressions d'emplois. Carbon Black va devenir une entité distincte dans cette nouvelle nébuleuse avant de voir certainement son destin basculer vers une vente ou une intégration dans Symantec.
Cependant, le CEO de Broadcom a promis un investissement de 2 Mds$ dans VMware par an. Cet investissement sera surtout concentré sur Cloud Foundation pour moitié, l'autre part ira à l'accélération du déploiement des solutions VMware par le biais des services professionnels de VMware et de ses partenaires. Enfin, cette offre ne connaîtra plus de licences perpétuelles, et bascule sur un modèle par abonnement, donc sur des revenus récurrents pour Broadcom. Elle continuera à honorer les contrats existants. À la date d'échéance, il faudra passer à une licence sur abonnement ou à terme. Des « avantages tarifaires » seront proposés dans ce cadre. La suite de l'histoire est cependant encore à venir.

Sans surprise, l'IA était le thème principal de l'événement.

UN EFFORT POUR LE SOUVERAIN

L'initiative Sovereign Cloud de VMware prend la forme d'un écosystème mondial de fournisseurs de services Cloud déterminés à soutenir l'adaptation de leurs clients à un cadre législatif de plus en plus lourd et évoluant rapidement. Les fournisseurs de Cloud souverain VMware doivent attester de leur respect d'une structure alliant principes directeurs, meilleures pratiques, et contraintes d'architecture technique, afin de proposer des services Cloud adhérant aux exigences de souveraineté des données de la région où est exploité le Cloud, comme imposé par l'autorité gouvernementale ou commerciale compétente. Thales est le tout dernier partenaire à rejoindre l'écosystème de fournisseurs de services KMS de VMware. L'offre BYO-KMS proposée via la plateforme Thales CipherTrust Data Security et VMware Cloud Director garantit la sécurité de l'environnement Cloud souverain, ce dernier étant uniquement accessible par les individus autorisés, et conforme aux normes nationales de souveraineté.

De multiples partenariats

Avec Intel, un effort collaboratif a été consenti pour aider les entreprises à créer et à déployer des modèles d'IA et à en accroître les performances en tirant parti de VMware Cloud Fondation et du kit logiciel d'IA, des processeurs et des accélérateurs matériels d'Intel.

Une collaboration avec IBM vise à rendre IBM watsonx disponible en environnements internes. Les clients peuvent ainsi combiner VMware Private AI et Red Hat OpenShift pour profiter de l'IA générative.

Les clients de VMware SASE vont pouvoir utiliser Microsoft Security Copilot, un outil conçu pour identifier des menaces et anomalies en tirant parti de la puissance de l'IA générative.

VMware a dévoilé Intelligent Assist for VMware Software-Defined Edge, une technologie conçue pour opérationnaliser la connexion, la sécurisation et la gestion des charges de travail, utilisateurs et équipements connectés (IoT) à la périphérie. Grâce à des technologies d'intelligence artificielle (IA) générative, la solution devrait renforcer VMware Edge Intelligence (anciennement VMware Edge Network Intelligence) et accélérer l'automatisation, combler les déficits de compétences, et accélérer la résolution des problèmes. De plus, VMware rejoint l'avant-première privée de Microsoft Security Copilot destinée aux partenaires. Cet outil de nouvelle génération et basé sur une IA, permet de détecter rapidement, de réagir et de mieux comprendre les menaces globales. VMware et Microsoft collaboreront pour offrir aux clients de VMware SASE la possibilité de partager des informations issues de leur déploiement avec Microsoft Security Copilot.

Du côté des développeurs, Spring AI est un nouveau projet modulable conçu dans le but de simplifier et de rationaliser le développement d'applications d'intelligence artificielle. Cette nouveauté permet aux développeurs d'utiliser le framework Spring avec des commandes simplifiées afin d'introduire des capacités d'IA dans leurs processus de développement.

Pour les postes de travail

À travers Anywhere Workspace, les clients vont bénéficier de nouveaux outils pour simplifier leurs processus informatiques, renforcer leur sécurité, et optimiser leur efficacité globale, dont des fonctions de gestion des Mac de nouvelle génération, afin de simplifier les workflows informatiques et de réduire les coûts. VMware annonce également Hub Health, de nouvelles exigences de base pour la prise en charge des risques liés aux tiers, ainsi qu'un tableau de bord de gestion des mises à jour pour macOS.

Un partenariat étendu avec Intel a pour but d'automatiser la détection des vulnérabilités au niveau du matériel, du firmware et des pilotes dans l'offre Workspace ONE. □

B.G

Raghu Raghuram lors de sa dernière prise de parole pour VMware lors d'Explore.

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

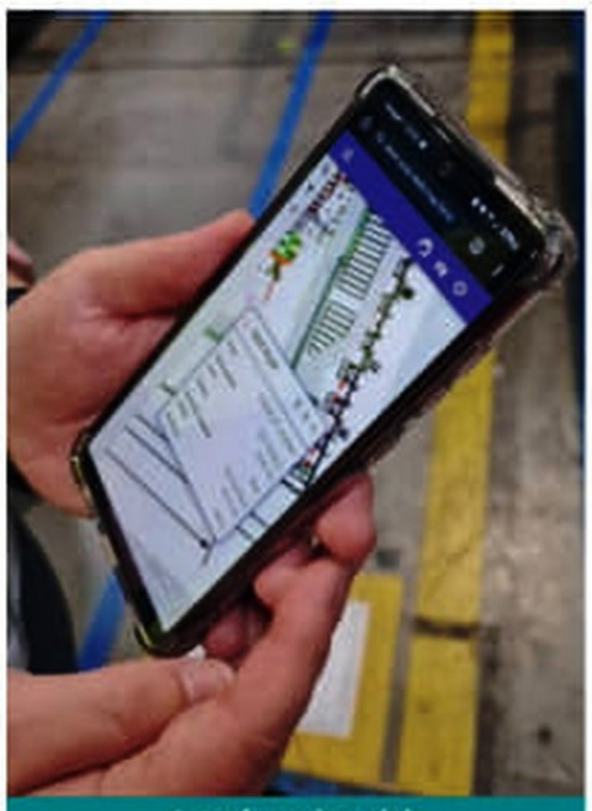
ILS SONT DÉJÀ INSCRITS

Professional Exhibitions and One to One Meetings Exhibitions

Processus Daher fluidifie sa traçabilité

L'avionneur Daher a étendu ses activités à de la logistique pour d'autres industriels dans les domaines ferroviaire, spatial... Il prend en charge entre autres celle du projet ITER. Il utilise aujourd'hui un outil de géolocalisation des bacs contenant les produits en cours de montage pour optimiser ses activités.

Responsable du programme d'open innovation chez l'avionneur, Gabriel Raffour rappelle : *« les données présentes dans les systèmes informatiques ne sont pas toujours en phase avec la réalité du terrain. C'est un irritant qui nous est souvent remonté par les opérations. Ils aimeraient avoir une visibilité, et donc une traçabilité en temps réel sur les flux physiques dans les usines et entrepôts. Nous cherchions une solution pour répondre à ce besoin. »* Un besoin d'autant plus sensible que des milliers de bacs identiques encombrent les sites. Et parfois, trouver le bon peut prendre du temps. *« Les opérateurs scannent les bacs avec des QR code notamment. Il s'agissait de trouver une solution de localisation entre deux scans »*, ajoute Gabriel Raffour. Outre aider les opérateurs dans leurs tâches quotidiennes par la localisation du bac contenant le produit, Daher comptait aussi profiter de cette traçabilité pour améliorer ses processus de logistique pour ses besoins internes comme dans le cadre de prestations chez ses clients.



Interface de suivi.

ROBIN au secours de Daher

« Il y a plus de quatre ans, nous avons rencontré Zozio au cours du salon VivaTech. Sa solution ROBIN, dédiée à la performance logistique nous a séduit », se souvient Gabriel Raffour. Début 2020, une expérimentation est menée sur un site industriel. La première étape consiste à déployer des capteurs sur les équipements suivis, avec des scratchs, et des « ancres » fixes pour quadriller la zone concernée. Ces ancres, identifiées sur la carte de la zone concernée, servent à identifier la position des capteurs *via* de la triangulation et envoient les données à la plateforme de Zozio *via* une box. Le fournisseur propose de personnaliser les capteurs en fonction des besoins pour réduire la note en termes d'équipement comme de consommation électrique. Une fréquence d'envoi des données toutes les 30 secondes nécessitera un modèle avec une batterie puissante par exemple. *« Les environnements industriels sont particulièrement difficiles pour les réseaux sans fils, souligne Gabriel Raffour. Ils comportent beaucoup de métal, des armoires, des parois... susceptibles de compliquer la propagation des signaux. »* À l'époque, Daher avait déjà testé des solutions basées sur différents réseaux, wifi, Bluetooth... sans succès. La technologie de Zozio, basée sur une approche hybride, avec de l'Ultra Wide Band (UWB) pour le signal et la triangulation pour calculer la position, tient ses promesses. Les bacs, contenant les composants, sont géolocalisés à 50 cm près, une distance suffisante pour répondre aux besoins.

Fort de cette première expérience réussie, Daher a déployé la solution sur cinq sites à ce jour. *« Une étape qui s'est déroulée à chaque fois en un temps record »*, ajoute notre interlocuteur. Pour justifier le coût de la solution, qui peut être à la charge du client final, en fonction de chaque contrat, Gabriel Raffour a formalisé des critères de retour sur investissement. À côté de l'excellence opérationnelle, l'impact écologique, l'expérience employée, l'expérience client sont évalués.

Les données qui sont envoyées sur la plateforme de Zozio sont couplées avec les systèmes d'information. *« Nous connectons cette plateforme avec les outils logiciels, du marché ou spécifiques, en place sur les sites industriels, en général des Warehouse Management System et des ERP. Cet interfaçage reste assez simple et nécessite le paramétrage d'une API fourni par Zozio »*, décrit Gabriel Raffour. Cette intégration apporte une visibilité sur les flux, sur les éventuels goulets d'étranglement ou ruptures de stocks. Elle permet d'adapter et d'optimiser les processus logistiques à partir de la réalité du terrain. La première expérimentation a permis de confirmer le retour sur investissement, *« à savoir une réduction des temps de recherche des bacs équivalente à un ETP »*, précise notre interlocuteur. Quand les données remontées sont utilisées dans un objectif d'optimisation, le retour sur investissement porte sur d'autres points, comme la réduction du nombre de chariots nécessaires... Au-delà de ces métriques, *« sur les sites utilisant l'outil, les opérateurs n'imaginent plus s'en passer »*, se félicite Gabriel Raffour. Cas d'usage original, l'outil a été aussi utilisé pour réaliser des audits logistiques sur un site dans le but d'optimiser l'organisation.

Daher a signé récemment avec Zozio un contrat cadre pour commercialiser la solution auprès de ses propres clients. *« Les sites peuvent être autonomes sur l'utilisation de la solution »*, souligne Gabriel Raffour. Une centaine de sites industriels sont potentiellement concernés. □

P. Br

Sauvegarde

Hosteur protège les données Office 365 avec Atempo

L'hébergeur français propose un service souverain pour protéger les données présentes dans les applications Microsoft 365 en s'appuyant sur les logiciels d'Atempo.

Créée en 2003, l'entreprise française Hosteur est spécialisée dans les services cloud, avec des bureaux répartis en Europe, en Afrique du Nord et en Afrique subsaharienne. Initialement centrée sur l'hébergement de données avec des serveurs dédiés, Hosteur a suivi la volonté de ses clients en proposant des services à haute valeur ajoutée, notamment dans les domaines du cloud avec une très haute disponibilité (PCA), des certificats SSL haut de gamme, de la sauvegarde chiffrée et résiliente, et du stockage haute performance.

Plus de 6000 clients actifs, constitués des PME jusqu'aux grands groupes cotés au CAC40, utilisent les services d'Hosteur qui possède de multiples certifications (HDS, ISO 9001/14001/27001). Les centres de données du fournisseur de services Cloud sont tous en Europe, et Laurent Escart, le président de l'entreprise, revendique haut et fort l'aspect souverain de ses solutions. Fort de ses convictions, Hosteur a quitté le projet Gaia-X, comme *L'Informaticien* l'avait rapporté sur son site en 2021. La prochaine phase du développement d'Hosteur sera de se concentrer sur le secteur médical avec des opportunités autour de start-up dans la « medtech » avec des infrastructures parfois larges, qui demandent souvent des hébergements de données conséquents et performants.

Laurent Escart sur un stand de French Healthcare.

Un besoin criant sur Microsoft 365

Si les services cloud de Microsoft assurent des performances d'accès aux données hébergées, ils n'offrent pas de garantie contre leur perte. Accident, cryptovirus, action malveillante ou erreur humaine, la perte des données M365 peut se produire et impacter l'activité des organisations. Laurent Escart ajoute : *« il y a peu de demandes de restauration, mais quand elles arrivent, elles sont le plus souvent critiques. S'il y a perte de données, il est nécessaire de plaider aux USA, car là-bas, cela ne discute pas pour trouver une solution qui arrange les deux parties »*. Ces arguments démontrent la nécessité de disposer d'une copie de ses données M365 afin de pouvoir les récupérer à tout moment.

Une solution complète

La solution proposée combine le stockage haute performance sur des baies Huawei Dorado ou des OceanStor Pacific à la solution de sauvegarde Tina d'Atempo, certifiée sur les matériels du constructeur chinois. Tina prend en charge plusieurs milliers de boîtes mails, les fichiers OneDrive, les conversations Teams et les fichiers SharePoint partagés. En fonction du nombre de boîtes mails à protéger et du volume de stockage nécessaire, les experts techniques Atempo et Hosteur proposent aux clients une solution clé-en-main : de la création de la plateforme jusqu'à l'architecture technique, en passant par les caractéristiques des machines virtuelles et le support. L'offre se complète de la gamme Lina d'Atempo pour la protection des postes de travail. Laurent Escart relève la simplicité de configuration des logiciels de l'éditeur français. Par interface de programmation, il est possible d'étendre la solution vers du stockage objet de type S3. La solution est facturée à l'usage et au nombre d'utilisateurs. ☐ **B.G**

Espace de travail

La poste migre dans le nuage

Lors de l'événement VMware Explore, *L'Informaticien* a pu rencontrer Yann Danou, CIO deputy et CTO de La Poste dans la branche grand public et numérique qui conduit la migration de l'ensemble des postes de travail présents dans son entité dans le Cloud.

L'entité de la poste grand public et numérique regroupe l'ensemble de l'activité numérique du groupe La Poste, de la tablette dans le bureau de poste, au tiers de confiance Docaposte, en passant par le courrier et les colis. Cela représente 17 000 points de présence avec 175 000 personnes en relation avec les clients finaux.

Moderniser le poste de travail, un meilleur suivi de l'expérience des utilisateurs

Dans une première vague lors des dernières années, l'entité avait doté les différents personnels de smartphones et de tablettes afin d'équiper largement les bureaux de poste. Pour le contrôle des accès, le choix de Workspace ONE de VMware avait été fait comme solution de MDM (Mobile Device Management). Le projet marque une nouvelle étape en migrant la solution vers le Cloud à l'occasion de la digitalisation des bureaux de poste. Il consiste à fusionner les instances dans le Cloud de VMware. Yann Danou explique : *« continuer à gérer l'infrastructure physique n'avait plus de sens pour nous »*. De plus, rien ne s'opposait à cette migration, car seuls les droits d'accès étaient différents sans personnalisation poussée. Aujourd'hui, l'ensemble des matériels est géré par l'instance dans le Cloud, soit 200 000 terminaux. La migration a été effectuée lors du second semestre de 2022 sans adaptation ni problème lors de la reprise des données malgré le large nombre d'applications concernées (80). De même, le réenregistrement des équipements n'a pas posé de problèmes particuliers. Les équipes ont été accompagnées grâce à la formation en continu. Seul point noir encore présent, les postes Windows 10 hors de ce domaine, sont principalement présents chez des partenaires comme Carrefour, les mairies et les points qui font office de bureaux de poste.

Une réflexion sur le VDI

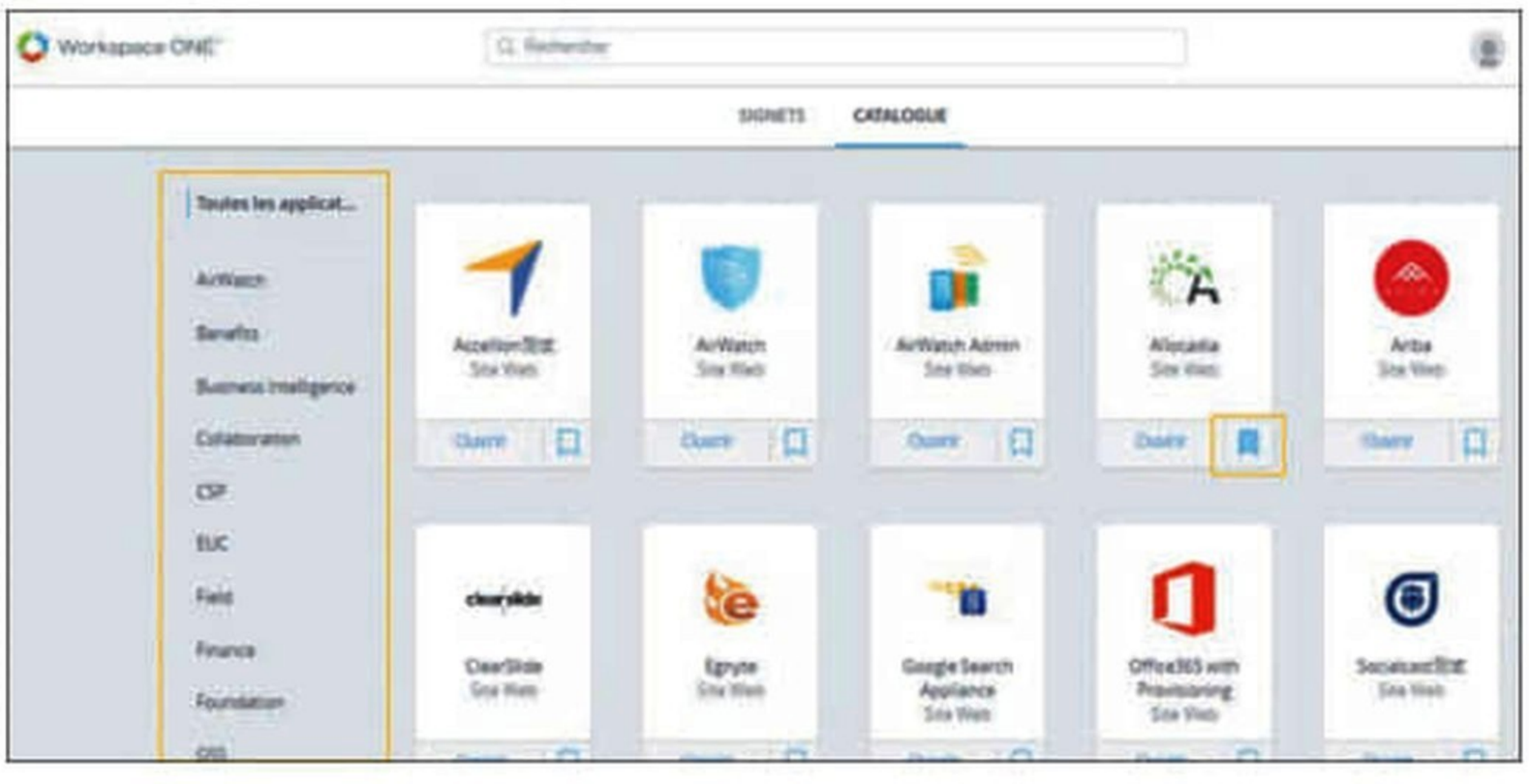
Actuellement, le projet est en phase de stabilisation et de réflexion sur le *« VDI de demain »*. Le groupe utilise une solution classique qui descend une machine virtuelle par le biais de Citrix. La solution a été fortement personnalisée. La réflexion porte sur d'autres types ou moyens de distribuer ce poste de travail virtuel.

Autre piste de réflexion pour l'avenir, l'utilisation de l'intelligence artificielle pour une meilleure supervision des postes, un meilleur suivi du comportement et de l'expérience des utilisateurs, et une amélioration du niveau de sécurité.

Des progrès sur la productivité

Inclus dans un contrat groupe, le DSI de cette branche de la poste ne peut précisément constater un retour sur investissement, puisque les licences acquises coûtent moins cher. Il peut, par contre, voir des gains de productivité. Ainsi, les équipes passent moins de temps sur leurs tâches à effectif égal. La gestion quotidienne est ainsi devenue plus efficace et les déploiements d'applications se réalisent plus rapidement. ☐

B.G



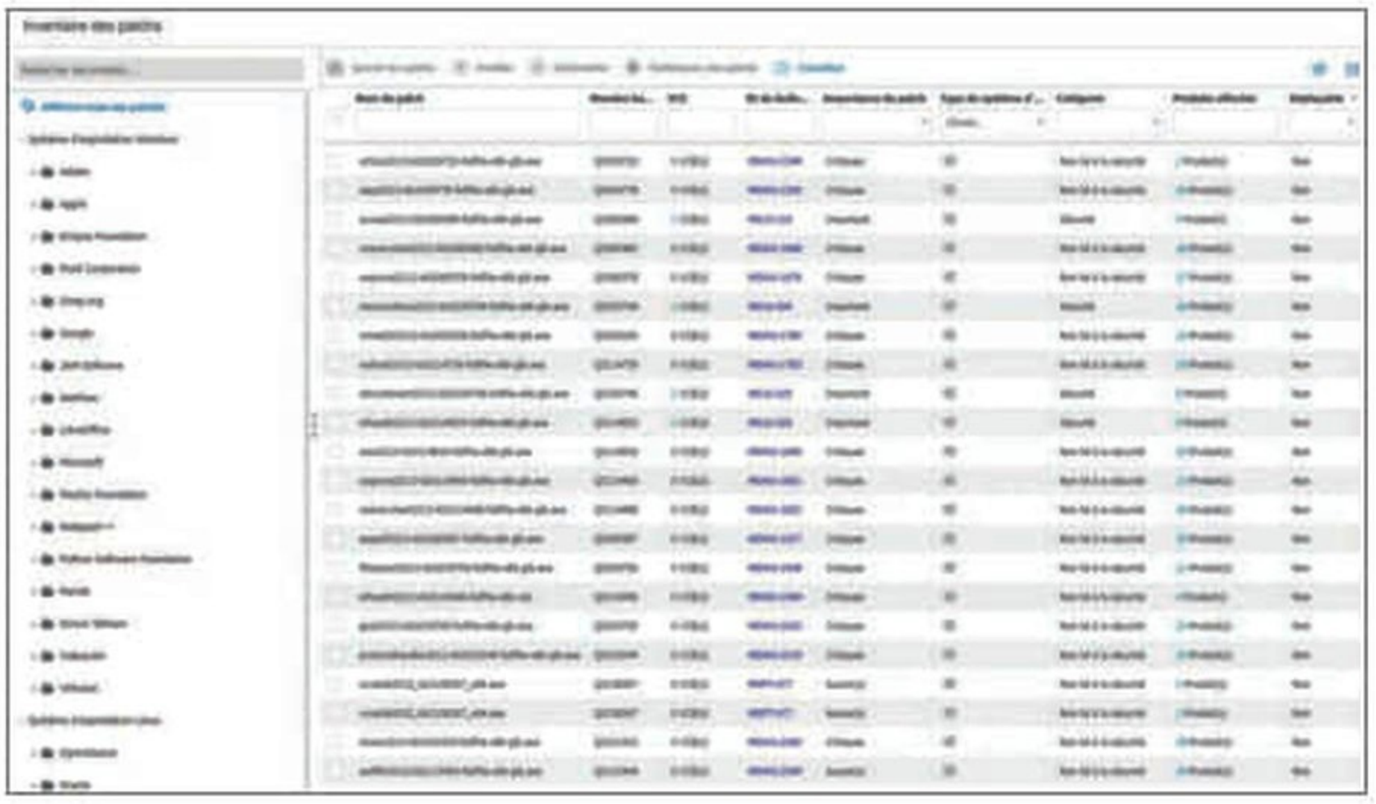
Un écran de Workspace ONE de VMware.

EDR

Le LNE évolue pour améliorer sa posture de sécurité

Le Laboratoire national de métrologie et d'essais (LNE) remplit plusieurs fonctions critiques et souvent confidentielles pour le test de nouveaux produits. Pour y parvenir, le laboratoire évolue vers une approche EDR/XDR pour se prémunir des attaques.

Skander Ben Jdidia, le RSSI du LNE, a pris son poste il y a environ 3 ans. Son premier travail a été de prioriser les risques et les actions à entreprendre pour éviter les fuites de données et l'indisponibilité du SI. La situation était classique avec une maigre protection par antivirus, alors que les principaux problèmes passaient par les terminaux. Cela ne correspondait plus à la typologie des menaces à prévenir, et n'apportait pas une visibilité suffisante sur ce qui se passait dans le SI. Le RSSI de LNE précise : *« quand le poste est identifié dans la CMDB (Base de données de gestion de configuration) avec un agent, je le connais, mais quand on se déplace chez le client, il peut y avoir des transferts de données et des connexions extérieures »*. De plus, il était nécessaire de se préoccuper d'un « shadow IT ». Après réflexion, le LNE a décidé de se diriger vers une approche EDR/XDR.



Une vue de sélection de patchs dans la solution Bitdefender.

Un choix européen

Vu la mission du LNE, un des critères de choix a été une volonté de choisir un produit français ou européen. Plusieurs étaient en liste finale, mais quelques produits n'avaient pas certaines fonctions, comme la gestion des patchs par exemple. Finalement, le choix s'est porté sur le XDR de Bitdefender qui permet de gérer le phénomène du Shadow IT par le réseau. La plateforme autorise une gestion de toutes les options, et il est possible d'ajouter des modules qui utilisent le même agent pour faire évoluer la solution. Ainsi, lorsqu'une vulnérabilité est détectée sur les terminaux, il est possible de choisir le patch et de lancer la mise à niveau de manière flexible pour éviter de saturer les fenêtres de patchs. Le LNE pratique donc par site pour éviter le problème. La solution permet de suivre au plus près et de détecter rapidement des comportements suspicieux. Skander Ben Jdidia complète son avis sur le produit par un bon rapport qualité/prix comparativement aux prix pratiqués sur le marché. De plus, la solution est simple à déployer et sa prise en main est rapide, même par des « juniors ». Le déploiement a été réalisé par vague. Seul petit défaut de la solution, elle remonte beaucoup d'informations, et parfois des faux positifs, et on ne peut pas tout bloquer pour l'activité de l'entreprise. Il faut donc être attentif sur les fonctions avancées comme l'apprentissage machine. Au bilan, le RSSI du LNE est satisfait du choix réalisé. □ **B.G**

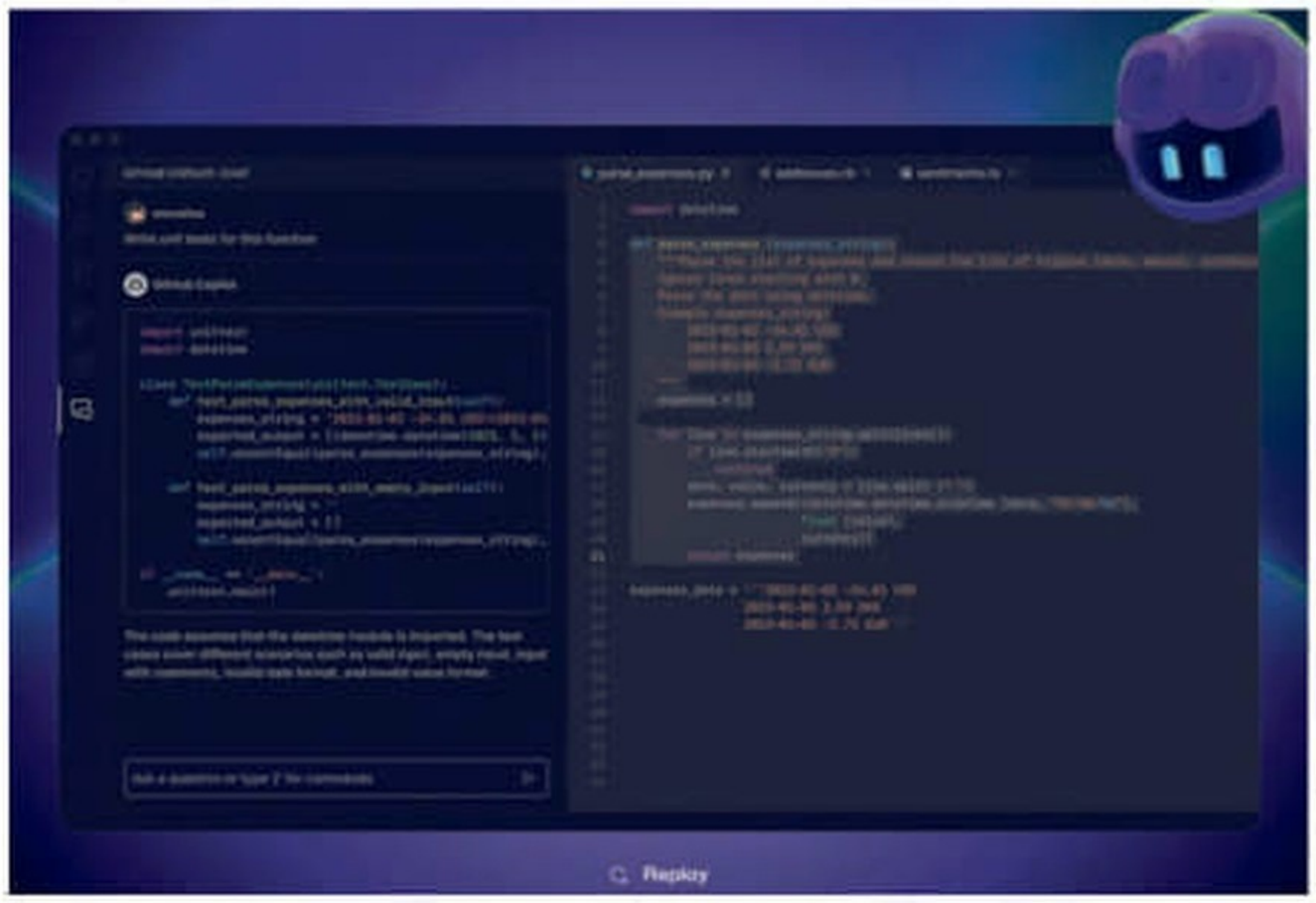
LE LNE EN BREF

Depuis 1997, la mission de service public du LNE est précisée dans le cadre d'un contrat d'objectifs signé tous les quatre ans avec l'État. Ce contrat implique l'engagement financier de l'Etat sous forme de subventions annuelles. Face à l'évolution perpétuelle des enjeux sociétaux (protection des citoyens et des consommateurs, hygiène et sécurité, protection de l'environnement), le LNE soutient la mise en œuvre des politiques publiques : en tant que laboratoire de référence pour l'industrie en matière de métrologie ; en poursuivant son développement scientifique et technique afin d'anticiper les besoins de mesure liés aux évolutions technologiques et aux nouvelles attentes de la société, en participant à l'élaboration des normes et réglementations aux niveaux national, européen et international, et enfin en prenant part à la surveillance des marchés. Pour ses missions, le laboratoire est certifié SecNumCloud.

IA : les développeurs dopés dans leur productivité

L'intelligence artificielle assiste déjà assez efficacement les développeurs aux différents niveaux du processus de développement logiciel. Ce phénomène est en train de s'accélérer avec des outils tels que Colab de Google et la « famille » Codey ou GitHub Copilot et IntelliCode de Microsoft. Nous allons voir dans cet article quels rôles l'IA peut réellement jouer dans ce processus.

L'intelligence artificielle est en train de révolutionner la manière de travailler des développeurs. Elle peut entraîner une augmentation significative de la productivité et de la qualité du code. En partant de la planification et de l'estimation du coût et de la durée des projets jusqu'à la livraison du produit et à la satisfaction des utilisateurs, en passant par les tests, tout peut bénéficier des algorithmes de l'IA. Plus les organisations s'intéresseront aux technologies de l'IA, plus elle affectera l'avenir du développement de logiciels. Les entreprises les plus avancées dans ce domaine, comme Google et Microsoft, mais aussi de plus petites structures comme Open AI, définissent d'ors et déjà des stratégies en la matière. Gartner prévoit que les outils d'IA devraient fournir plus de 3000 milliards de dollars en valeur d'entreprise dans un avenir proche. Néanmoins, si elles veulent mettre en œuvre une véritable stratégie en matière d'intelligence artificielle, les entreprises doivent commencer par comprendre qu'elle peut être sa réelle fonction dans le développement logiciel et examiner avec précision les secteurs et les processus qu'elle peut véritablement améliorer.



Des suggestions de GitHub Copilot sont proposées dans l'IDE Visual Studio lorsque vous commencez à écrire ou en rédigeant un commentaire en langage naturel décrivant ce que vous souhaitez faire.

Redéfinir le rôle des développeurs

Le rôle des développeurs de logiciels est en train d'évoluer considérablement. Il pourrait bien, d'ici une dizaine d'années, être très différent de ce qu'il est actuellement. Cela ne veut pas dire pour autant, n'en déplaise à certains chefs de projet qui auraient bien aimé que ce soit le cas, que la technologie pourra complétement remplacer les développeurs. Il coulera encore beaucoup de lignes de code dans les programmes avant d'en arriver là, c'est-à-dire qu'une IA soit capable d'écrire quasiment seule du code complexe et performant. De là à dire que cela n'arrivera jamais... nous resterons prudents, car il est toujours difficile d'évaluer jusqu'où la science est capable d'aller, et l'IA est bien un domaine dans lequel nombre de pythies numériques se sont « salement vautrées » dans leurs prédictions.

Dans un avenir raisonnablement proche, disons quelques dizaines d'années, il est plus probable que

INTÉGRER L'IA DANS LE DÉVELOPPEMENT LOGICIEL

Les routines basées sur l'IA sont capables de prévoir le prochain appel de fonction ou de méthode, de conception d'objet dans une ligne de code dans divers environnements de développement intégrés. Si cela existait déjà de manière primitive, cette fonctionnalité devient de plus en plus puissante avec certains outils comme IntelliCode de Microsoft qui remplace et dépasse l'IntelliSense. Les EDI peuvent proposer des stubs (morceaux de code) de plus en plus complexes et surtout adaptés, la finalisation de l'invocation d'une méthode/fonction, d'un appel d'objets en séquence, et renseigner tous les arguments et paramètres nécessaires, tout cela grâce aux progrès de l'IA. La prochaine tendance majeure de l'IA dans le développement de logiciels est la capacité des systèmes d'IA à examiner un cas d'utilisation ou une exigence système et à produire du code implémentant la/les conditions fonctionnelles, voire même la construction de cas de test.

les programmeurs soient susceptibles d'exécuter des activités plus fonctionnelles et d'acquérir des compétences pour collaborer efficacement avec l'IA. En un peu plus clair, ils ne disparaîtront pas, voire ils seront encore plus indispensables, mais leur métier évoluera grandement en phase avec ce nouvel outillage. Ils seront capables d'exécuter plus de tâches, de créer des applications plus sûres, plus complexes et plus faciles à maintenir. Les différents défis de développement de logiciels que l'IA a contribué — et va continuer à contribuer — à relever sont nombreux. Voyons ce qu'il en est déjà.

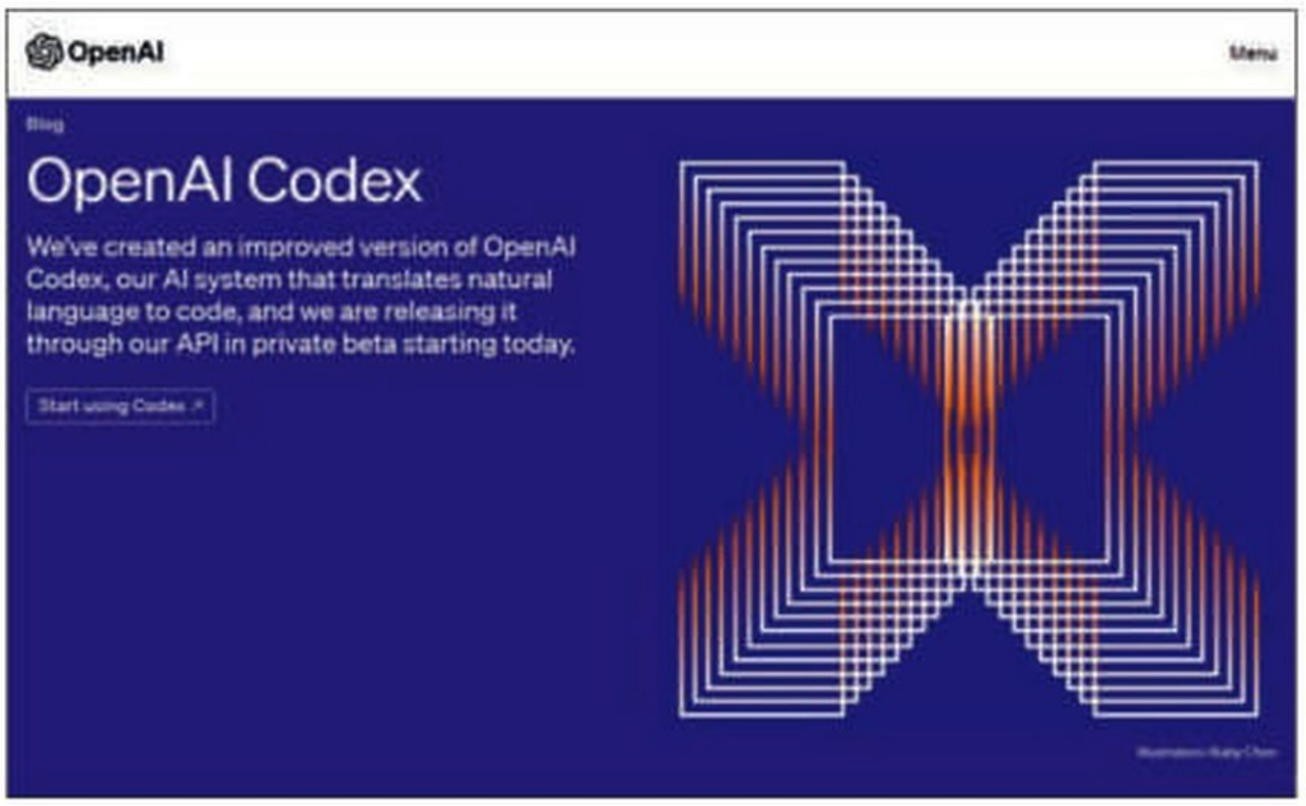
Qualité du code améliorée grâce à la révision et à l'optimisation automatique

L'intelligence artificielle devrait devenir un outil utilisé par les développeurs afin d'acquérir de nouvelles connaissances, d'optimiser les différents processus de conception pour, au final, produire un code de meilleure qualité. L'une des principales améliorations dans ce domaine est représentée par les applications de développement (IDE ou EDI, environnement de développement intégré) ayant recours à l'IA et intégrant la saisie semi-automatique (comme l'IntelliCode de Microsoft) dans le processus de conception logiciel en vue d'augmenter la vitesse et la précision d'écriture du code. Parmi les autres solutions, une fonctionnalité de mentorat basée sur l'IA permet par exemple aux développeurs n'ayant pas les compétences de base pour cela de créer des applications en temps réel. Dans un futur de plus en plus proche, ces technologies devraient démocratiser grandement le développement et surtout permettre aux programmeurs de consacrer plus de temps à la résolution de problèmes complexes, à la conception et à la créativité plutôt que de le gaspiller avec du débogage plus basique comme de la maintenance corrective ou de la réorganisation du code. Les effets bénéfiques devraient aussi se voir dans le déploiement de logiciels, particulièrement dans le paradigme de développement dit CI/CD (intégration et déploiement en continu). Certes, des solutions efficaces existent déjà avec des outils tels que GitLab ou Jenkins, mais ils nécessitent souvent un paramétrage long et fastidieux qui gagnerait à être simplifié et automatisé grâce à l'IA. Les taches de mise à niveau des applications vers des versions plus récentes ou les tâches de contrôle de déploiement devraient y gagner beaucoup. Il y a souvent des risques importants de régression et de déstabilisation de l'application si celle-ci n'a pas été correctement testée, et les tests sont parfois très difficiles à être effectués de façon satisfaisante avant la mise en production. Des progrès réels ont été faits dans ce domaine même sans l'aide de l'IA, mais un environnement de production est parfois très difficile à reproduire dans des contextes industriels complexes. L'IA peut prévoir bien plus de cas de figure problématiques, améliorer la couverture des tests et simuler des environnements de production même compliqués à mettre en œuvre dans des containers ou autres et réduire ainsi les probabilités d'échec du déploiement. L'avantage qu'a l'intelligence artificielle dans ce contexte est qu'elle permet, grâce aux algorithmes d'apprentissage automatique, d'examiner le processus de déploiement à travers ses itérations précédentes et d'en déduire des solutions optimisées. Les algorithmes d'apprentissage automatique permettront au logiciel d'apprendre comment se comportent des utilisateurs spécifiques ou quoi faire lorsqu'ils rencontrent telle ou telle situation particulière. Ce comportement appris progressivement au fil des

```
4     using System;
5     using System.IO;
6
7     namespace Microsoft.eShopWeb.Web.Controllers
8     {
9         [Route("[controller]")]
10        [ApiController]
              0 references | 0 changes | 0 authors, 0 changes
11        public class FileController : ControllerBase
12        {
13            [HttpPost]
14            [AllowAnonymous]
                  0 references | 0 changes | 0 authors, 0 changes
15            public IActionResult Upload(FileViewModel fileViewModel)
16            {
17                if (fileViewModel == null)   Tab to accept
18            }
19
20        }
21    }
```

IntelliCode dans Visual Studio utilise le contexte de votre code combiné à des modèles qu'il a appris à partir de millions de lignes de code open source publiques pour fournir des améliorations basées sur l'IA à IntelliSense.

déploiements va l'aider à répondre à différentes actions en diffusant un contenu potentiellement variable. Une réponse de ce type se traduira par une expérience logicielle dynamique consistant à extraire des données d'interaction utilisateur en temps réel et de les utiliser afin de générer automatiquement des améliorations au fur et à mesure que les développeurs modifient le code.



Codex est l'outil de développement assisté par l'IA d'OpenAI capable de transformer des spécifications écrites en langage naturel directement en code et le « moteur » de GitHub Copilot

Sécurité des applications

Celle-ci se décompose en plusieurs parties : la sécurisation du code, l'évaluation des vulnérabilités présentes, l'analyse de la sécurité statique et dynamique et la sécurité du code open source employé dans les projets. La sécurité des logiciels a toujours été une fonctionnalité essentielle devant être prise en compte tout au long du cycle de développement. Elle est encore plus critique actuellement au vu de l'exploitation de plus en plus fréquente des failles de sécurité de toute sorte par des hackers. Plusieurs approches sont possibles, l'essentiel étant qu'elles soient complètes et efficaces. La collecte de données à partir, par exemple, de sniffeurs réseau comme Wireshark et/ou de logiciels installés côté client en font partie, mais sont loin d'être suffisants. Là encore, l'IA peut être employée afin d'étudier les données issues des traitements. Le ML (Machine Learning ou apprentissage automatique) permettra de discerner un comportement anormal d'un comportement classique. Les services et les sociétés de développement logiciel ayant intégré l'IA dans leur processus de développement pourront éviter au maximum les avertissements tardifs, les notifications erronées et surtout les attaques de pirates destinées à compromettre la sécurité des applications, leur bon fonctionnement et à dérober des données. La qualité de la programmation progresse et s'améliore lorsque les développeurs et les testeurs ne perdent pas leur temps à examiner et réexaminer des fichiers exécutables et du code source truffé d'erreurs et de défauts de conception. Il sera en principe beaucoup plus facile de détecter et de corriger rapidement les dits défauts. Les tests d'assurance qualité, en particulier, ont toujours et représentent encore un processus manuel très fastidieux et pas toujours très fiable, avec une large marge d'erreur potentielle. C'est sans doute l'un des avantages les plus importants de l'IA : l'amélioration du testing, avec des tests plus rapides à effectuer et plus précis, améliorant très considérablement le processus de détection et de correction des bogues. Il est essentiel de faire tout cela avant la mise en production afin de raccourcir le cycle de développement et de garantir un produit final de bien meilleure qualité. Les technologies d'IA sont justement là pour automatiser certaines tâches difficiles. Les concepteurs pourront aussi, par exemple, utiliser un assistant de conception IA leur permettant de mieux comprendre les désirs et les préférences du client pour employer ensuite ces informations en vue de concevoir un projet plus approprié.

Comment parler de développement assisté par l'IA et de Machine Learning sans évoquer ce « bon vieux » TensorFlow (https://www.tensorflow.org/) ?

Avantages concrets de l'IA dans le développement de logiciels

Le développement « traditionnel » de logiciels ne disparaîtra certainement pas, mais il a forcément vocation à évoluer et à se moderniser grâce à l'intelligence artificielle. Un logiciel standard doit pouvoir gérer facilement tous les composants clefs tels que les interfaces, la sécurité et l'administration des données. L'IA contribuera à améliorer le fameux cycle de vie du développement logiciel (SDLC pour Software Development Life Cycle), produisant des logiciels de meilleure qualité en prenant en charge ces fonctions essentielles que sont les estimations, la prise de décision et le prototypage rapide.

Estimations précises

La conception de logiciels dépasse assez souvent le budget et les délais initialement prédéterminés. Des estimations vraiment fiables nécessitent à la fois un haut niveau d'expertise, une connaissance très approfondie du contexte fonctionnel et une assez bonne connaissance de l'équipe de développement — point également crucial s'il en est. Nous mettrons ici de côté les problématiques de recrutement de développeurs compétents, leur disponibilité sur une longue période et les éléments humains et d'ordre plus RH (ressources humaines) permettant de les garder, même si elles ne sont pas du tout anodines. L'apprentissage automatique permettra de faciliter la modélisation des données grâce à l'étude des projets précédents. Ces projets peuvent inclure des histoires utilisateurs (les fameuses User Stories), des descriptions de fonctionnalités et des estimations quant à leur réalisation. Il pourrait même être possible que les logiciels se modifient dynamiquement face à une erreur dans une réponse sans aucune interaction humaine. Les développeurs gagneront ainsi du temps en utilisant des assistants de programmation intelligents leur fournissant des conseils et des recommandations instantanés comme des best practices (meilleures pratiques) ou des stubs (des exemples de code) évolués.

Prise de décision stratégique

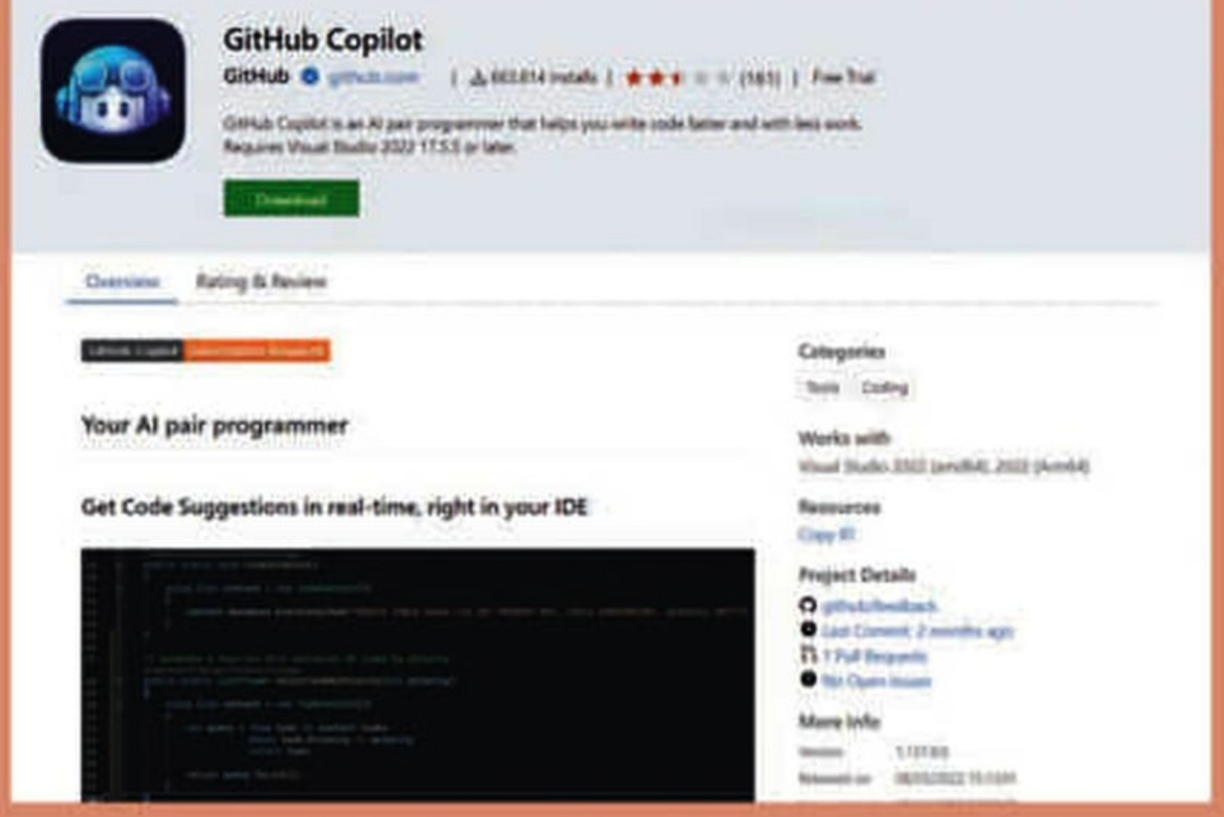
Déchargés des tâches les plus fastidieuses, les développeurs pourront travailler sur plus de produits et de fonctionnalités différents. Il leur sera ainsi plus facile d'évaluer ce qui doit être priorisé et ce qui n'a pas besoin de l'être, voire qui doit être éliminé. Des plateformes d'intelligence artificielle pourront alors être formées par les entreprises, accumulant l'expérience des précédents projets de conception, les problèmes rencontrés, les erreurs pénalisantes en vue d'aider à l'évaluation des performances des applications actuelles et futures.

Prototypage rapide

Beaucoup de temps (et donc d'argent), de réflexion et de stratégie sont nécessaires pour transformer des exigences commerciales en solutions techniques. Grâce à l'apprentissage automatique, les développeurs pourront raccourcir considérablement ce processus en permettant aux professionnels du domaine technique/métier de mettre en place leur idées et projets d'innovations à l'aide d'interfaces visuelles en langage naturel. Le « dégrossissage » des applications pourra ainsi être fait rapidement par des non-professionnels du développement, et leur travail repris directement par les « vrais » développeurs. Des solutions de ce type existent, mais elles sont encore à améliorer car elles ne permettent généralement pas une reprise directe du travail effectué par ces béotiens non programmeurs (le no code / low code) ou produisent des solutions trop lourdes et difficiles à faire évoluer (des AGL — ateliers de génie logiciel — comme WinDev). □

T.T

GITHUB COPILOT DE MICROSOFT



L'extension GitHub Copilot pour Visual Studio aide les développeurs à écrire du code plus rapidement et avec une plus grande précision, et à effectuer d'autres tâches de développement telles que l'écriture de tests unitaires, le débogage et le profilage. Elle permet de générer des lignes entières ou des blocs de code basés sur le contexte fourni par le développeur. S'appuyant sur des modèles d'IA formés à partir de milliards de lignes de code open source, elle fournit des suggestions de code de type autocomplétion au fur et à mesure que vous codez, en temps réel. Des suggestions de GitHub Copilot sont proposées dans l'IDE lorsque vous commencez à écrire ou en rédigeant une signature de fonction ou un commentaire en langage naturel dans votre fichier de code décrivant ce que vous souhaitez faire. GitHub Copilot nécessite à minima Visual Studio 2022 17.5.5.

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

Web : Créer un site Internet sans coder

La présence en ligne est une évidence désormais. Il ne faut cependant pas le faire n'importe comment pour en récolter les fruits. Henri Lotin, l'auteur de l'ouvrage, revient sur les fondamentaux qui valorisent pleinement le contenu du site par un design approprié. Le livre se décompose en deux parties : une première partie, stratégique, faite de réflexion et de travail, sur la conception, puis une deuxième partie plus opérationnelle pour vous accompagner de la conception à la mise en ligne de votre site.
L'auteur s'appuie sur un exemple concret et fournit des ressources complémentaires pour vous faire la main et suivre sa méthode avec des outils simples, mais reconnus, que ce soit WordPress ou Webflow. À la fin de l'ouvrage, que ce soit pour vous ou votre organisation, vous aurez votre site Web et cela sans coder, car l'important n'est pas forcément d'aligner des lignes de code ou de personnaliser un template, mais de bien concevoir son site pour que son contenu intéresse l'internaute.

Chapitre 1

C'est quoi, le design web ?

J'ai écrit en 2018 un long article[1] pour expliquer ce qu'est le design web. À la suite des commentaires, je m'étais alors rendu compte que très peu de personnes savaient en réalité ce que c'était.

Je rappelle une définition très courte et très succincte de HubSpot[2] ici : *« Le design de site web est le processus de planification, d'idéation et d'organisation de contenu pour l'Internet. »*

1 : LOTIN Henri, C'est quoi le design web ou web design ?, https://lotincorp.biz/cest-quoi-le-design-web/

2 : DEUWEL Alexis, Webdesign : Qu'est-ce que c'est et comment faire ?, https://blog.hubspot.fr/website/ site-web-design

Il est évident que le contenu est roi. Mais ce qui m'intéresse ici, c'est le mot « processus ».

Pourquoi je commence par là ?

Parce que je ne veux pas que vous soyez surpris par la manière dont le livre est organisé : je passerai beaucoup de temps sur la phase de planification.

Abraham Lincoln disait : *« Que l'on me donne six heures pour couper un arbre, j'en passerai quatre à préparer ma hache. »*

Alors, en quoi consiste le design de site web ?

Non, le design web n'est PAS QUE la création d'interfaces web

Vous savez quoi ? Le design web n'est pas seulement la création de l'interface. En fait, l'interface est la finalité du processus du design web.

Même Wikipédia en français[3] a commis cette erreur :

« La création et le design de sites web ou web design est le design de l'interface web : l'architecture interactionnelle, l'organisation des pages, l'arborescence et la navigation dans un site web. Le design d'un site web tient compte des contraintes spécifiques du support Internet, notamment en termes d'ergonomie, d'utilisabilité et d'accessibilité. »

La définition de 99design[4] dans un article rédigé en 2019 précise : *« Le design web est le processus de planification et de construction des éléments de votre site internet, de la structure à la mise en page, en passant par les couleurs, les polices, et les images. »*

J'aime beaucoup l'aspect planification qu'elle fait apparaître.

Treefrog[5], une agence digitale au Canada me met du baume au cœur avec son approche :

« Le design est le processus de collecte d'idées, d'organisation et de mise en œuvre esthétique, guidé par certains principes dans un but précis. Le design web est un processus de création similaire, avec l'intention de présenter le contenu sur des pages web électroniques, auxquelles les utilisateurs finaux peuvent accéder via Internet à l'aide d'un navigateur web. »

Tous les éléments s'y retrouvent : processus, principes, but, contenu, création, utilisateurs et web.

Je vais maintenant parler de deux grands principes sur lesquels s'appuie le design web moderne : le design centré sur l'utilisateur et le design d'expérience utilisateur.

Le design centré sur l'utilisateur [user centered design, UCD]

Nous ne pouvons parler de design web sans évoquer les principes du design centré sur l'utilisateur qui est la fondation sur laquelle est bâtie la grande partie des disciplines nécessaires à l'existence du design web.

L'origine des principes du design centré sur l'utilisateur

Beaucoup de principes du design centré sur l'utilisateur sont basés sur la compréhension de la manière dont les utilisateurs pensent (réfléchissent) et prennent des décisions, quel genre de choses influencent ou inhibent la prise de décision, et comment les utilisateurs évaluent les options et la pertinence ou la signification de l'information.

Cette compréhension provient de deux sciences :

- Les sciences cognitivesl'étude de la manière dont les humains pensent.
- L'interaction homme-machinel'étude de la manière dont les humains se servent des ordinateurs.

On doit cette façon de penser à Donald Norman, qui est un chercheur et professeur américain en sciences cognitives, en design et en ergonomie. Il est surtout connu pour ses travaux sur le design centré sur l'utilisateur et la psychologie cognitive, ainsi que pour son livre, The Design of Everyday Things (La psychologie cognitive du design), publié en 1988.

Dans ce livre, il a popularisé le concept de *« mauvais design [bad design] »* et a expliqué comment les objets mal conçus peuvent créer de la confusion et de la frustration chez les utilisateurs. Il est également cofondateur de la société de conseil en design Nielsen Norman Group.

Le design centré sur l'utilisateur, en bref

Le design centré sur l'utilisateur est une approche itérative[6] de design qui vise à développer une compréhension des besoins des utilisateurs, en faisant ainsi un mélange de méthodes et d'outils d'investigation (par exemple, enquêtes et interviews) et génératifs (brainstorming, par exemple).

Fondamentalement, le design centré sur l'utilisateur implique fortement les utilisateurs dans toutes les phases de design et d'évaluation. En général, chaque itération (cycle d'amélioration) de l'approche design centrée sur l'utilisateur suppose quatre phases distinctes.

1. Tout d'abord, les designers tentent de comprendre le contexte dans lequel un système peut être utilisé.
2. Par la suite, les exigences des utilisateurs sont spécifiées.
3. Une phase de design suit.
4. Suivie d'une phase d'évaluation.

Les résultats de l'évaluation sont appréciés en fonction du contexte et des exigences des utilisateurs afin de vérifier le bon fonctionnement d'un design, à savoir s'il est proche d'un niveau correspondant au contexte spécifique des utilisateurs et satisfait tous leurs besoins pertinents.

De là, d'autres itérations (améliorations par cycles) de ces quatre phases sont faites, jusqu'à ce que les résultats de l'évaluation soient satisfaisants.

---

3 : Wikipédia, Conception de site web, https://fr.wikipedia.org/wiki/Conception_de_site_web

4 : KRAMER Lindsay, Qu'est-ce que le design de site web (et comment le réussir) ?, https://99designs.fr/blog/ design-web-digital/quest-ce-que-design-de-site-web/

5 : Treefrog, What is Web Design?, https://www.treefrog.ca/what-is-web-design

6 : Qui fonctionne par cycles d'amélioration continue.

Le design d'expérience utilisateur

Cette définition du design d'expérience utilisateur ou design UX par Blind[7] est satisfaisante :
« Le design d'expérience utilisateur ou design UX est le processus visant à influencer des variables contrôlables pour provoquer une réponse émotionnelle positive lorsqu'une personne interagit avec un produit, un environnement ou une marque. »

Pour bien comprendre le design UX, il est important de connaître les cinq disciplines principales qui le régissent, car techniquement, le design d'expérience utilisateur est un ensemble de disciplines :

1. L'architecture de l'information connecte les gens au contenu d'une manière plus compréhensible pour eux.

2. Le design d'interaction traite des interactions spécifiques entre les utilisateurs et un écran (en se basant sur les principes de l'Interaction Homme-Machine).

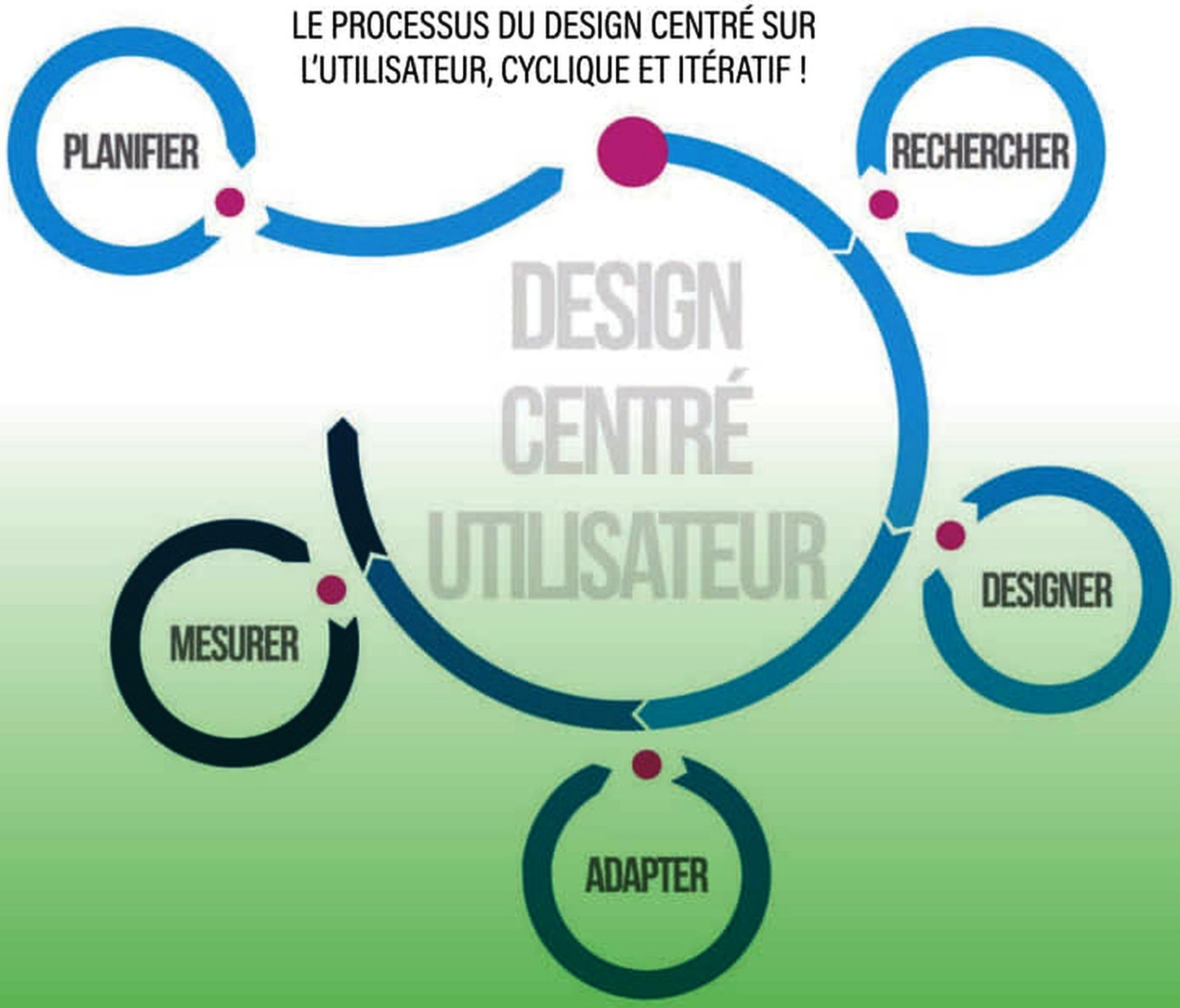
3. L'utilisabilité traite du fait de s'appuyer sur des données pour déterminer le bien-fondé des décisions de design. Elle est définie par la norme ISO 9241-11 : 1998.

4. Le prototypage peut être défini comme la création d'une version préliminaire à partir de laquelle les autres formes sont développées.

5. Le design visuel porte sur l'utilisation de l'aspect visuel d'un produit pour en améliorer l'expérience utilisateur.

Tout au long de votre projet de création de site web, vous devrez vous mettre dans la peau d'un designer web. Et un designer web possède plusieurs compétences qu'il met au service du projet.

7 : Blind est un studio de création basé en Californie. Cette définition est extraite de leur vidéo « *What is UX Design* », sur YouTube : https://www.youtube.com/watch?v=nVIl_098dzg.



Je vous propose de découvrir une vue globale des activités autour de la création d'un site web.

Opérations de design et de développement web

Les deux opérations principales dans la création d'un site web sont le design et le développement.

Opérations de design web

Les opérations de design web consistent en :

1. La conceptualisation (production du document de spécification du projetle but et les objectifs du projet, recherches sur la concurrence et pistes visuelles à explorer grâce notamment aux mood boards ou planches émotionnelles, définition des profils d'utilisateurs, création de scénarios d'utilisation, budget et planning inclus).

2. La création d'une liste de contenu (inventaire de contenu).

3. La création d'un diagramme structurel (flowchart, organigramme[8]).

4. Le développement de la taxinomie[9] et du système organisationnel.

5. La création d'idées de story-board d'interaction.

6. Préparation graphique des écrans web : croquis ou ébauches sommaires et fil de fer graphique [wireframe].

7. Design graphique de l'interface (mock up ou maquette graphique).

8. Export des composants concernés des écrans web en images pour la phase d'intégration (création des livrables de l'interface).

Mais tout ceci ne suffit pas à rendre le site web fonctionnel. C'est pour cela qu'il faut du code HTML et CSS. Et si vous voulez être moderne, vous allez avoir besoin de JavaScript.

Opérations de développement web

Ajouter des interactions aux pages web en codant à la main (grâce à un éditeur de texte) ou en utilisant une interface WYSIWYG [What You See Is What You Get] comme WordPress, Dreamweaver, Webflow ou Systeme.io. Il existe plusieurs services d'intégration web en ligne, proposant de convertir une maquette graphique en HTML.

Webflow propose d'ailleurs une méthode assez simple pour passer de Figma[10] à Webflow[11].

8 : Représentation synthétique des diverses parties d'un ensemble organisé et de leurs relations mutuelles ; représentation graphique des sous-ensembles d'un système et des relations qui les lient entre eux.

9 : Étude théorique des bases, lois, règles, principes d'une classification.

10 : Figma est une plateforme de design de bout en bout, conçue pour aider les équipes à comprendre les problèmes, à explorer leurs options et à construire des solutions ensemble. https://www.figma.com/fr

11 : https://webflow.com/figma-to-webflow

Spécifiquement on aura à travailler sur le balisage des pages, leur mise en page par les CSS et l'ajout d'interaction grâce au JavaScript ; ceci est la phase d'intégration ou de design de la maquette fonctionnelle.

Elle peut être précédée si besoin, et en fonction du budget, de la phase de prototypage[12], qui est une phase intermédiaire réalisée sous Figma ou Adobe XD.

La bonne nouvelle pour vous, c'est que le but de ce livre n'est pas de faire de vous un designer web (peut-être que si, un peu quand même ; rires), mais de vous amener à réaliser un site web professionnel qui vous permettra de convertir vos visiteurs en clients. Tout ceci, sans passer par les aspects techniques en rapport avec le code.

Ce qui signifie que vous n'êtes pas dispensé des autres activités en rapport avec la création d'un site web de qualité professionnelle. □

12 : Première réalisation d'un projet destiné à former une série.

• Éditeur : GERESO Édition
• Auteur : Henri LOTIN
• Collection : Hors collection
• Nombre de pages : 327
• ISBN13 : 979-10-397-0471-7
• ISBN eBook : 979-10-397-0687-2
• ISBN ePub : 979-10-397-0688-9

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

VC

Serena ouvre un nouveau fonds de 100 M€

Serena crée le fonds Serena Data Ventures II, un nouveau véhicule sursouscrit de plus de 100 millions d'euros, soutenu par des investisseurs institutionnels — dont Bpifrance via le Fonds national d'amorçage 2 et le Fonds européen d'envestissement — et des investisseurs privés.

Serena Data Ventures tend ainsi à se concentrer sur trois briques fondamentales que les promoteurs considèrent comme des technologies révolutionnaires et indispensables pour tirer pleinement profit des avancées technologiques de demain. La première priorité des investissements du fonds sera la stack moderne autour des données et l'intelligence artificielle.

L'IA et la stack des données

Les modèles d'IA pré-entraînés représentent le changement architectural le plus significatif dans le monde du software et où de nouveaux softwares émergent pour construire l'infrastructure de demain, fondée sur du temps réel, de meilleures performances, une plus grande élasticité et une automatisation accrue, ainsi qu'une gouvernance des données améliorée.

La chaîne de blocs est le deuxième axe d'investissement. Décentralisée et transparente, cette technologie offre un changement de paradigme dans la façon dont nous abordons la gestion des données et la confiance, en créant des solutions innovantes qui responsabilisent


Bertrand Diard, associé chez Serena.

les utilisateurs, renforcent la confiance entre les parties prenantes et ouvrent de nouvelles possibilités de collaboration.

Le troisième pilier va être l'informatique quantique. Cette nouvelle génération d'ordinateurs représente une opportunité majeure. La puissance de calcul de ces ordinateurs permet de résoudre des problèmes de plus en plus complexes, en particulier dans les domaines de la cryptographie, de la découverte de médicaments, ou encore de l'optimisation et de la modélisation climatique.

Des premiers investissements

Après avoir soutenu en amorçage des start-ups comme Dataiku (qui a désormais atteint le statut de licorne), Odaseva, Mindee, CybelAngel ou encore Accenta, devenues aujourd'hui des références de l'IA et de la data. Serena, avec le fonds Data Ventures II, continuera d'investir en early-stage des tickets entre 500 000 € et 3,5 millions d'euros. À ce jour, Serena Data Ventures II a d'ores et déjà investi dans Koyeb (plateforme serverless pour du déploiement d'applications), Fipto (solution de gestion de trésorerie numérique), Defer (plateforme de background processing) et Quandela (ordinateur quantique photonique fullstack). □ **B.G**

UN MODÈLE DIFFÉRENT

Serena est l'un des principaux fonds de capital-risque en Europe, avec 750 millions de dollars sous gestion. Fondé en 2008, Serena investit en early-stage, du Seed à la Série B. Il se distingue par un modèle opérationnel avec des équipes en internes qui réalisent les recherches d'entreprises, la veille technologique et le suivi des dossiers. Les principaux partenaires du fond ont un passé important d'entrepreneur comme Bertrand Diard qui a démarré Talend et d'autres start-up à succès. Cette combinaison, rare dans le milieu des ventures, permet d'avoir une granularité et une connaissance fine. De plus, le fond ne se spécialise que sur certaines thématiques, ce qui renforce la spécialisation.
Autre différence, Serena est un partenaire actif pour conseiller et apporter les meilleurs conseils visant la réussite des entreprises dans lequel le fonds investi.

Optimisation

WedoLow rend les systèmes embarqués moins énergivores

Fondée en 2022, et issue de laboratoires de recherche publics (IETR, INSA, Inria à Rennes), la startup WedoLow développe une solution automatisée et ultra-rapide de diagnostic et d'optimisation de logiciels embarqués et hébergés afin de les rendre plus économes.

Selon GreenIT, les applications ont vu leur poids multiplier par 171 en 20 ans. Des gains conséquents sur la vitesse d'exécution et la consommation d'énergie des logiciels se traduisent concrètement pour les produits par des traitements plus rapides, un allongement de la durée de vie et une autonomie plus importante.

La réponse WedoLow

Si les applications deviennent de plus en plus lourdes, les codes de plus en plus volumineux et de plus en plus complexes, les cycles de livraison de plus en plus rapides, le triptyque consommation d'énergie, temps de développement et puissance de calcul représente donc un défi davantage prégnant pour l'électronique embarquée.

Un écran de la solution de WedoLow.

Ainsi, 51% des développeurs déclarent avoir un volume de code plus de 100 fois supérieur à celui qu'ils avaient il y a 10 ans, tandis que 92% d'entre eux affirment que la pression exercée pour publier les logiciels plus rapidement a augmenté. WedoLow répond donc aux besoins des développeurs en leur fournissant une solution capable de diagnostiquer et de vérifier rapidement, tout au long de leur process de développement d'une application logicielle embarquée, si celle-ci est bien optimisée, et si des gains ne pourraient pas être obtenus en termes de vitesse d'exécution ou de consommation d'énergie.

WedoLow a développé une méthode permettant de comprendre la structure d'un code et d'en identifier les parties pouvant être réécrites pour générer plus d'efficience et de performance grâce à une collection de techniques d'optimisation qu'elle enrichit en continu. Ces propositions de réécriture se font en connaissance de la cible matérielle sur laquelle le logiciel tourne. Avec cette approche, WedoLow est capable de proposer des ajustements dans le code, permettant de mieux exploiter les potentialités des processeurs utilisés par ses clients.

Elle combine ainsi une triple expertise dans l'introspection de code, grâce à des outils d'analyse statique et dynamique qu'elle a développés, dans les techniques d'optimisation et dans l'architecture des processeurs.

Des résultats déjà convaincants

S'appuyant sur plus de 20 ans de R&D cumulés sur l'optimisation logicielle afin de fournir des solutions d'optimisation compatibles avec les systèmes les plus courants du marché et de fonctionner sur une large gamme de plateformes et d'appareils. La startup a des clients depuis sa création, et a déjà fait ses preuves auprès de plusieurs acteurs majeurs de divers secteurs industriels comme les télécoms, la robotique, l'IoT, le véhicule, le spatial...

Ainsi, la solution a permis de gagner 23% sur la vitesse d'exécution du filtrage de signaux issus de capteurs sur un système de transmission d'un véhicule routier, 40% sur la vitesse d'exécution d'une application de filtrage de trames réseaux d'une box internet, 72% sur la vitesse d'exécution d'une application de traitement du signal, pour un gain estimé de 50% sur la consommation d'énergie soit plusieurs jours d'autonomie en plus pour ce robot sous-marin fonctionnant sur batterie, et 45% en vitesse d'exécution sur une application de traitement d'images satellites hébergée. □ **B.G**

Souveraineté

2ème édition de l'étude de Jamespot

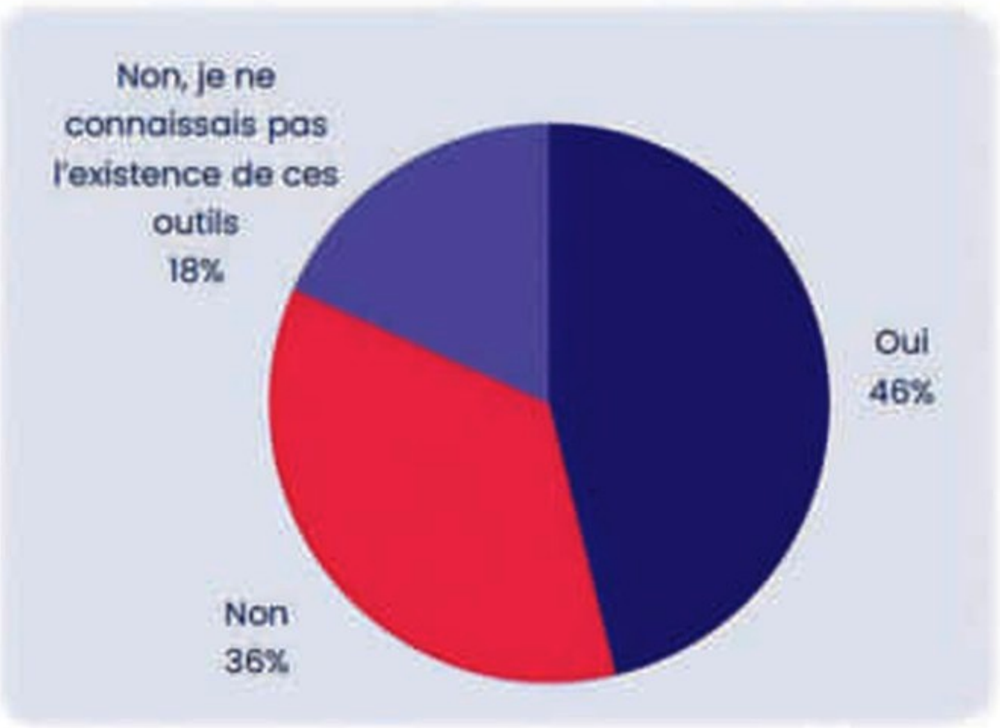
En collaboration avec Poll & Roll, Jamespot vient de livrer la deuxième vague de son étude autour de la vision des entreprises françaises sur les outils collaboratifs souverains. Elle démontre que la notion de souveraineté numérique en 2023 est au cœur des préoccupations des décideurs et qu'elle progresse rapidement dans les entreprises françaises.

Selon les chiffres publiés, la notion de souveraineté numérique devient plus concrète dans les esprits des décideurs IT. La quasi-totalité en a déjà entendu parler et près des 2/3 sait ce dont il s'agit. Une notoriété qualifiée qui a gagné 9 points par rapport à 2022. La totalité des DRH et des DSI connaissent la notion de souveraineté numérique. Les DSI et DRH sont encore plus nombreux que la moyenne des décideurs à avoir entendu parler de ce concept. Un quart de ces décideurs indique qu'elle est primordiale. Cette proportion monte à 46% chez les dirigeants des entreprises interrogées. De plus, les deux tiers des répondants souhaitent que la souveraineté numérique soit décidée dans l'entreprise et plutôt à un niveau global, et non plus au niveau des managers. 87% des décisionnaires connaissent le dispositif *« je choisis la French Tech »* et une moitié sait à quoi cela correspond vraiment. Pour rappel, ce dispositif doit permettre de résoudre les difficultés auxquelles font face les start-ups pour vendre leurs solutions aux grands acheteurs du tissu économique français.

Un intérêt toujours présent

Selon l'enquête, près de 9 décisionnaires IT/SI sur 10, mais avec un niveau de certitude en recul vs l'an dernier, ont l'intention de tester de nouveaux outils souverains au cours des 3 prochaines années. L'intention de tester des outils souverains est d'autant plus forte auprès des personnes les plus familières avec la notion de souveraineté numérique.

Capacité des outils souverains vs. Office 365 ou Google Workplace



Le prix est un frein

Les freins principaux à l'utilisation des outils souverains restent le manque de connaissance de l'offre et le fait que les outils américains semblent plus pratiques, car plus utilisés. Mais surtout, le prix est devenu un frein plus important cette année avec un quart des répondants qui trouve que les outils souverains sont trop chers. Ils sont aussi plus des 2/3 à trouver qu'il y a un manque de réglementation et que celle-ci empêche de concurrencer les outils américains.

Une sensibilité aux réglementations

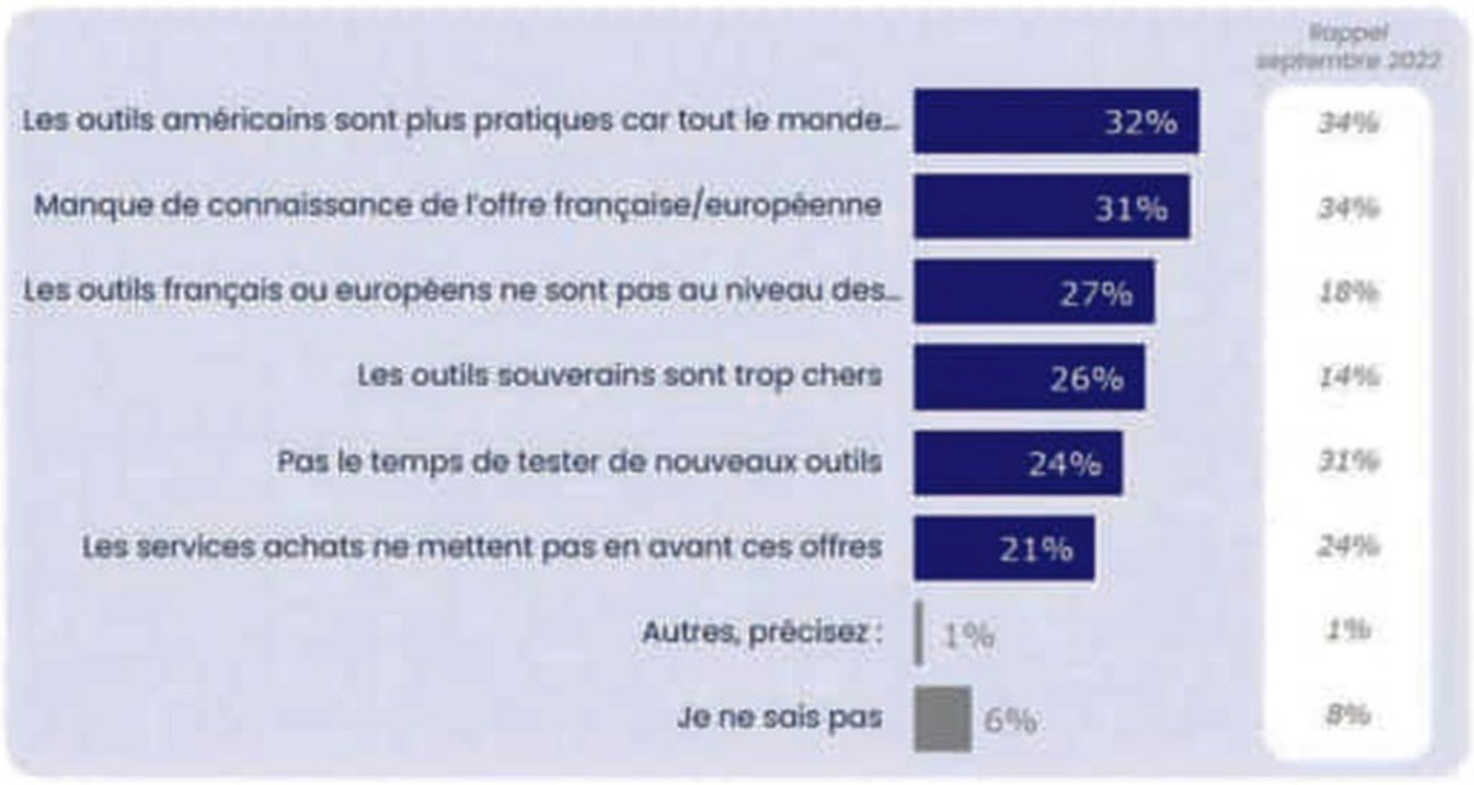
Le RGPD est le règlement le plus connu en ce qui concerne les données personnelles. 7 répondants sur 10 déclarent savoir exactement de quoi il s'agit. Le Data Act est connu par 8 décisionnaires sur 10 dont une moitié sait réellement de quoi il s'agit. Le SecNumCloud, quant à lui,

JAMESPOT SE DÉVELOPPE SUR LE MARCHÉ EUROPÉEN

L'éditeur français souhaite aller plus loin dans son développement sur le marché espagnol à très fort potentiel de croissance. L'équipe espagnole composée de 4 personnes sera dirigée par Eric Bounyavath, Sales Director & Partner chez Jamespot. Pour l'accompagner dans son déploiement et répondre aux spécificités et aux besoins du marché espagnol et des organisations qui se transforment, Jamespot souhaite bâtir un écosystème partenarial avec des entreprises locales de confiance — tels que les ESN et les cabinets de conseil en transformation digitale — alignées culturellement et en phase avec ses convictions. Il vient d'ailleurs de signer un partenariat avec PrideCom, agence de communication interne et de marque employeur située à Madrid, qui bénéficie de plus de 10 ans d'expérience avec des clients dans différents secteurs tels que Mercadona, BNP, Unicef, Cabify, Auchan, Roche Farma, etc.

est connu par 7 répondants sur 10, et un tiers sait vraiment en quoi il consiste. La notoriété des différentes réglementations est stable comparativement à l'année dernière. Les réglementations sur les outils numériques sont bien perçues par les décisionnaires. Elles renvoient une bonne image de la France et de l'Europe sur la scène internationale, et favorisent le développement des outils français et européens. Malgré tout, près d'une moitié pense que ces règles sont trop strictes. La quasi-totalité des DRH pensent qu'il manque des réglementations sur ces outils au niveau français et européen, beaucoup d'entre eux pensent que les règlementations qui existent sont inadéquates ou trop strictes. Au contraire, les dirigeants pensent davantage que les réglementations existantes prennent bien en compte les problématiques des entreprises et sont suffisantes.

Raisons de non-utilisation des outils collaboratifs souverains



Des changements dans les usages des outils collaboratifs

Les outils collaboratifs les plus utilisés sont la messagerie, la visio-conférence et les outils de bureautique. Les Digital Workplaces sont les outils collaboratifs les moins utilisés. Il existe une méconnaissance des outils intranet et gestion de projet utillsés dans les entreprises. En effet, ces outils qui étaient en 4ème et 5ème position en 2022, sont passés derrière le réseau social d'entreprise en 2023 une fois qu'il était demandé aux répondants de spécifier le nom de l'outil utilisé. 11% des entreprises utilisent des outils collaboratifs souverains en 2023. 1 répondant sur 5 ne sait pas si les outils collaboratifs utilisés par son entreprise sont souverains ou non. Lorsqu'il s'agit de tester de nouveaux outils collaboratifs souverains, la messagerie et la visio-conférence sont les deux premiers outils que les décisionnaires envisageraient de tester. Ils sont moins enclins à tester des réseaux sociaux d'entreprise ou une digital Workplace souverains. Près de la moitié des décisionnaires sont conscients que les outils souverains présentés offrent les mêmes fonctionnalités que leurs concurrents Office 365 et Google Workplace. Ce constat est même plus fort chez les connaisseurs qualifiés de la souveraineté numérique et les DRH. □

B.G

Profil

Le Chief AI Officer (CAIO) émerge

Dans les rôles de directeur, un nouvel acteur apparaît, le CAIO, pour établir et dérouler l'agenda IA de l'entreprise.

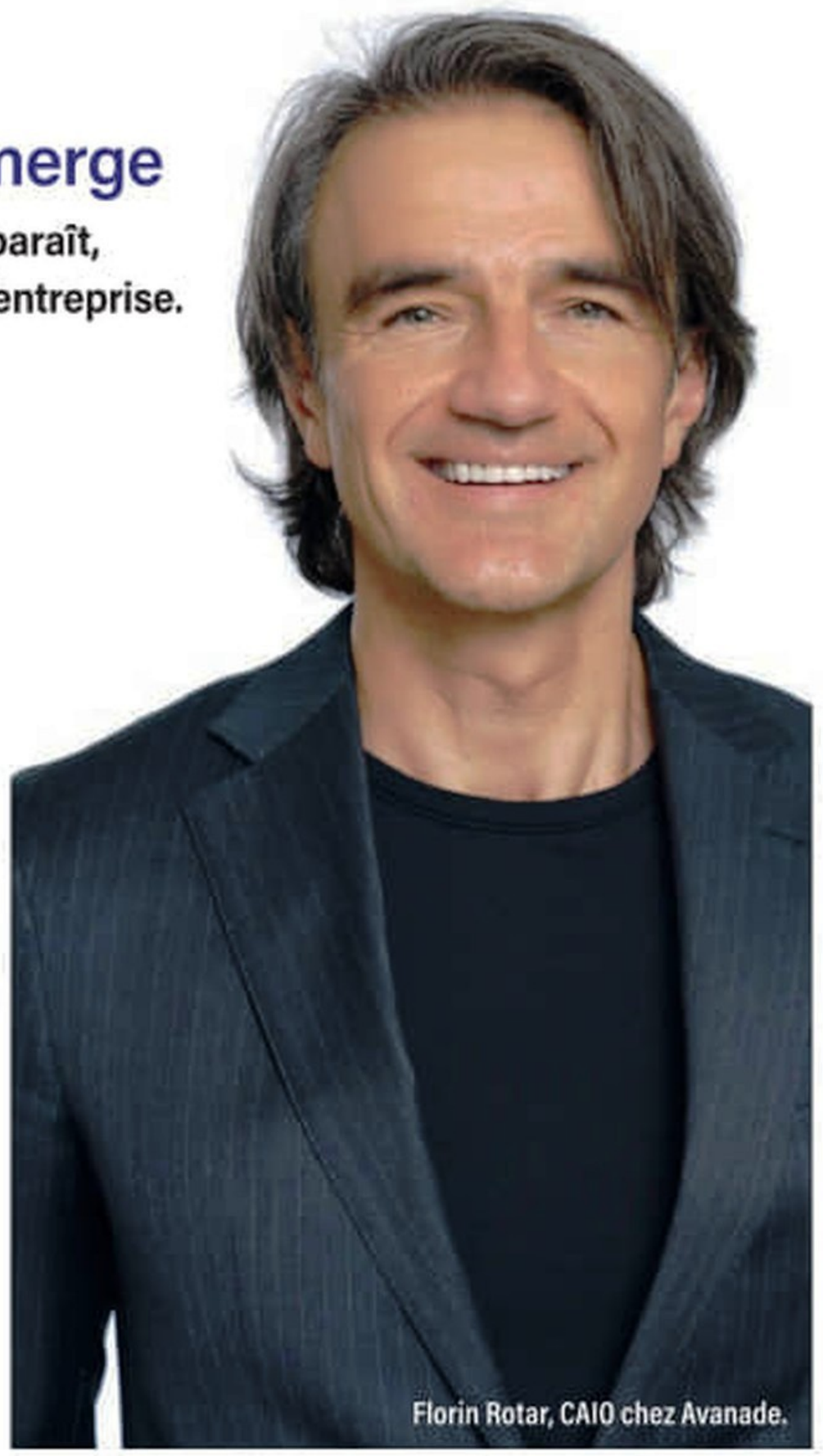
La venue de ChatGPT et autres outils d'intelligence artificielle générative ne bouleverse pas uniquement le travail quotidien, mais appelle aussi à revisiter l'organisation de l'entreprise avec une personne en charge de l'application de l'intelligence artificielle dans l'entreprise afin d'éviter de se retrouver dans la situation de la poule devant un couteau.

Un rôle qui se définit lentement

Selon une étude réalisée par Foundry, 11% des entreprises moyennes et grandes ont déjà nommé quelqu'un pour tenir ce rôle, et 21% en recherche un activement. Selon le cabinet Forrester, une entreprise sur huit aux USA a un CAIO dans son équipe de direction et le phénomène devrait s'accentuer l'année prochaine. Ce nouveau patron de l'IA ne doit pas seulement avoir de fortes compétences sur l'intelligence artificielle, il doit pouvoir devenir le champion de cette technologie pour une adoption raisonnée dans l'entreprise. Il doit être un bon communicant et savoir travailler avec de multiples départements de l'entreprise, tout en concevant et ciblant des cas d'usages pertinents, évaluer les résultats des projets et mesurer le retour sur valeur de chaque cas.

Un poste de niveau supérieur

Pour imposer la stratégie de l'entreprise, il doit donc être placé dans le haut de l'organigramme. Le plus souvent, il est mandaté pour revoir les processus de l'entreprise par l'intelligence artificielle, tout en s'assurant qu'elle est utilisée avec des règles responsables et éthiques. Il doit, de plus, infuser dans l'entreprise la culture autour de l'IA. GE Healthcare a déjà son CAIO, tout comme Avanade, qui vient de nommer Florin Rotar à ce poste. Florin pilotera la stratégie globale de l'entreprise en matière d'IA ainsi que son implémentation en interne. Il aidera également les clients à accélérer leur propre intégration de l'IA, de façon éthique, dans le respect de la vie privée et de l'impact social de cette technologie. Dans certains cas,



Florin Rotar, CAIO chez Avanade.

il combine les fonctions de Chief Data Officer et celui de patron du développement de l'utilisation de l'intelligence artificielle. Sa place est cependant plutôt dans les entreprises qui ont la volonté de devenir « AI First » ou ayant fortement recours à l'intelligence artificielle, en particulier sa déclinaison générative. Récemment, le président des USA a signé l'équivalent d'un décret obligeant toutes les agences gouvernementales de se doter d'un tel poste. Cependant, selon les cas, à qui doit-il reporter ? Au fil du temps, le rôle et les limites devraient se préciser.

Des salaires en rapport avec la position

Aux USA, le salaire moyen d'un CAIO est de 179,574 $ par an mais peut monter jusqu'à 298,565 $ selon des chiffres fournis par Glassdoor. En France, la rémunération serait plus modeste aux alentours de 71 300 € par an en moyenne avec un top à 108 K€ selon Salary Explorer. □

B.G

LE PREMIER CAIO SUMMIT

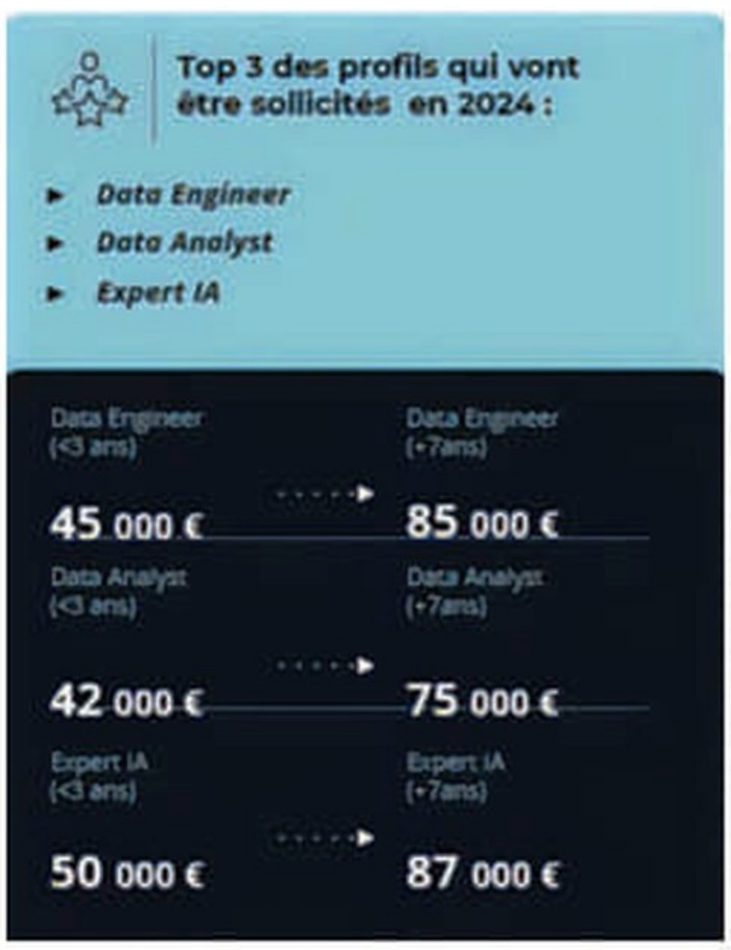
À la mi-décembre s'est tenu le premier CAIO Summit à Boston, hébergé par The Institute for Experiential AI à la Northeastern University. Le programme de conférence couvrait l'ensemble des aspects du rôle des CAIO. En février prochain se tiendra un autre événement, le CAIO tpo33 avec un nombre de places limité.

Salaires

La fin de la démesure

La vague 2024 de l'étude de Humanskills sur les salaires dans le digital marque un ralentissement sur les salaires, et la fin de la démesure dans les augmentations.

Selon cette étude, les augmentations en 2023 ont été à la marge avec une augmentation moyenne de 7%. Elles étaient de plus de 14% l'année précédente. Cette baisse significative de l'augmentation des salaires s'explique par le contexte économique actuel et la période d'inflation post-covid. Cette conjoncture se caractérise par une diminution significative des levées de fonds, de nombreux licenciements et gels des embauches. Une croissance est également ralentie en Chine et aux États-Unis, ce qui provoque une baisse des investissements dans les entreprises concernées par les marchés du luxe, du retail... Ces perturbations ont eu raison de la flambée des salaires dans les métiers de la transformation, et le ralentissement de l'offre a permis de regonfler les viviers de candidatures : pour la première fois depuis la pandémie de covid, les cabinets de recrutement constatent un retour de candidatures spontanées.



Les profils recherchés dans le secteur de la data.

Des secteurs résistent

Certaines fonctions, encore en pénurie, continuent à voir une forte évolution de leurs salaires. C'est notamment le cas des métiers de la data qui connaissent une hausse de leurs salaires de +3% (vs 14% en 2022). Avec la quantité de données récoltées par les entreprises ces dernières années, et une donnée qui est de plus en plus stratégique pour répondre aux enjeux business, l'étude révèle une recrudescence des besoins sur ces métiers, notamment en Data Engineer, Data Analyst et Expert IA. Le métier d'Expert IA maintient d'ailleurs son augmentation forte de salaire de +13%, comme l'an passé.

Les métiers de l'IT, des marketplaces et du e-retail continuent, quant à eux, de tirer leur épingle du jeu avec +17% en 2023 pour les métiers de l'IT en moyenne vs 16% en 2022 (+ 1 point) et +8% pour les métiers des marketplaces et du e-retail (similaire à 2022). L'accélération digitale des entreprises implique une mise sous tension plus importante des métiers de l'IT et trois profils seront principalement attendus et sollicités en 2024 : les Pentester (cybersécurité), les SRE Engineer et les Cloud Computing Engineer. Côté marketplaces et e-retail, ce sont les profils d'E-Retail Manager, d'E-Merchandiser et de Business Developper Market Place qui seront les plus sollicités en 2024.

Les métiers du produit et du design (Product Manager, Product Owner, Product Designer) continuent, quant à eux, d'être fortement recherchés, mais leur hausse des salaires connaît un ralentissement : +6 en 2023 vs +12% en 2022.

La RSE, nouvel axe stratégique

La RSE est devenue un enjeu plus que stratégique pour les organisations de toute taille. Elle est essentielle pour attirer et retenir les talents et ouvre de nouveaux métiers, faisant la part belle aux profils seniors avec des compétences de labellisation, comme en témoignent les salaires moyens d'Head of Environnmental Impact (100 k € pour + 7 ans d'expérience) et Chief Impact Officier (110 k € pour + 7 ans d'expérience), métiers particulièrement recherchés pour 2024. ☐

B.G

DES TENSIONS ENTRE SALARIÉS ET EMPLOYEURS DANS UNE AUTRE ÉTUDE DU CABINET ROBERT HALF

L'étude Robert Half montre que si 35% des employeurs français s'inquiètent du manque de compétitivité des salaires proposés pour attirer les talents dans leur entreprise, c'est le cas de près de la moitié des salariés (49%).
L'insuffisance de la rémunération demeure la première raison de rejet d'une offre d'emploi, citée par 66% des salariés sondés, loin devant une mauvaise localisation de l'entreprise (49%) ou un mauvais contact durant le processus de recrutement (40%).
L'écart de perception et l'insatisfaction des salariés se mesurent aussi vis-à-vis des augmentations : 28% des employés pensent que leur entreprise n'augmentera pas les salaires dans les 12 prochains mois, contre 14% des employeurs.

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™

L'INFO CYBER-RISQUES

L'INFORMATICIEN

Les MSSP tentent de démocratiser la cyber protection du SI

Sommaire

Si les grandes entreprises ont largement les moyens de gérer leur cybersécurité en propre, beaucoup d'entreprises ont le recours à des prestataires spécialisés, pour prendre en charge ce qui reste la première priorité des entreprises actuellement. Dans ce dossier, nous faisons le tour de ce qu'ils proposent. Comment contracter avec ces partenaires ? Pourquoi faire appel à eux et sur quels critères les choisir ?

Vous retrouverez, bien sûr, l'ensemble de nos rubriques habituelles avec un article sur le chiffrement, un compte rendu du dernier rapport de l'ENISA et de nombreux autres sujets avec des retours d'expérience, des études, des rencontres...

Les MSSP tentent de démocratiser la cyber protection du SI

Les nombreuses cyberattaques qui déferlent sur les entreprises encouragent ces dernières à faire davantage appel à des Prestataires de Services IT Managés en cybersécurité (MSSP). Le recours à leurs services facturés sur abonnement est-il la panacée pour mieux sécuriser son SI ? Sont-ils réservés aux seuls grands comptes ?

Markess by Exægis identifie les MSSP français commercialisant des services de SOC managés pour le mid-market en 2023.

Connaissez-vous le terme MSSP (Managed Security Service Provider) ? Très à la mode actuellement dans le secteur de la cybersécurité, cet acronyme désigne un Prestataire de Services IT Managés (MSP) « généraliste » qui s'est spécialisé dans la vente aux entreprises de services de cybersécurité sous forme d'abonnements. Non sans un certain succès. Le marché mondial des services IT managés généralistes est d'ailleurs en pleine forme. Il devrait enregistrer un taux de croissance annuel de 13,4 % jusqu'en 2030 selon la société d'études Research & Markets. Et celui des MSSP est encore plus dynamique. Suite au nombre croissant de cyberattaques réussies, les entreprises ont davantage recours à ces MSP, que l'on appelait aussi infogéreur IT autrefois. D'ailleurs, chacune de ces attaques encourage les entreprises, petites ou grandes, à augmenter le niveau de sécurité de leurs systèmes d'information (SI), de peur d'être la prochaine victime. En outre, leur complexité croissante les oblige à se doter d'expertises cyber toujours plus pointues, afin d'être capable de déployer et gérer un programme de sécurité efficace. Mais ont-elles toutes les moyens, tant humains que financiers, de le faire H24 et 7j/7, sachant que les cyberattaquants sont astucieux et ne prennent pas de vacances ?

Hélas non, d'autant que les bonnes compétences en cybersécurité sont toujours rares et donc coûteuses. Nombre de TPE et PME, voire certaines ETI, n'ont donc pas forcément les moyens de se les offrir à demeure. Et pour nombre de ces « petites » Directions des services informatiques (DSI), quand elles existent, recruter et fidéliser des experts en cybersécurité est un véritable casse-tête, aussi coûteux que chronophage.

Pourtant, elles sont au cœur des cyber attaques. Les TPE et PME ont représenté environ 40 % des attaques par rançongiciel déclarées ou traitées en 2022 selon l'Agence nationale de la sécurité des systèmes

Pourquoi faire appel à un MSSP ?

Préserver sa trésorerie : en achetant des services vendus sur abonnement, comme en Saas, l'entreprise évite de piocher dans sa trésorerie pour acheter en Capex de coûteuses solutions de cybersécurité, à actualiser régulièrement. Cependant, le coût des abonnements (Opex) peut s'avérer plus élevé dans la durée.

Disposer d'expertises : les bons professionnels en cybersécurité sont très demandés. Leur recrutement et leur fidélisation sont longs et coûteux, même pour les MSSP, qui portent pourtant ces investissements en lieu et place de leurs clients.

Avantage technologique : le MSSP dispose, en théorie, d'expertises et d'outils récents et performants, 2 facteurs importants dans la lutte contre des cybermenaces qui évoluent sans cesse.

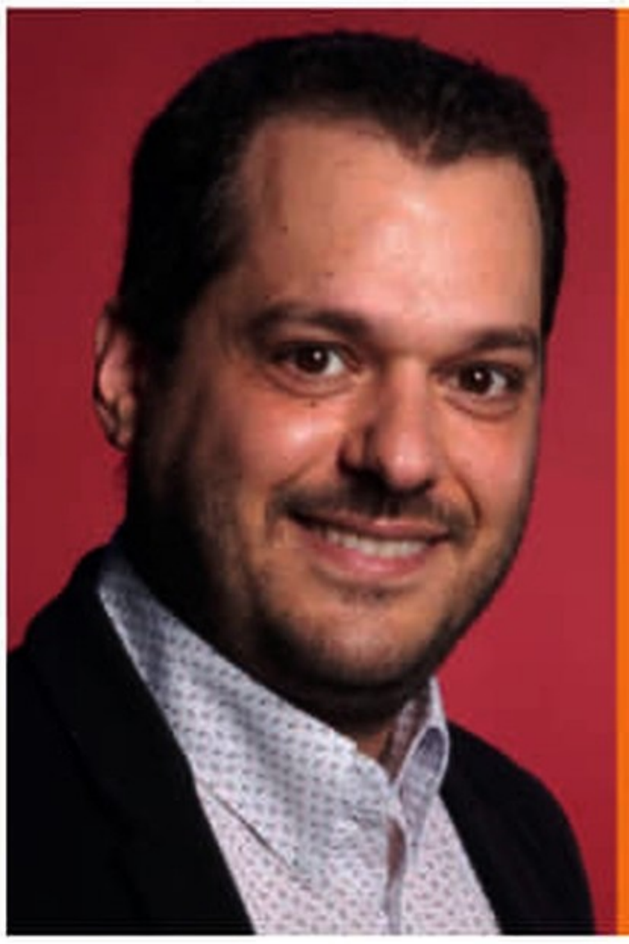
Automatisation complexe : le périmètre de supervision et de détection des cybermenaces ne cessant d'évoluer, l'automatisation de la remédiation, grâce à l'IA notamment, permet au MSSP de lutter contre la « data fatigue » des analystes du SOC.

Protection dans la durée : s'il est fidélisé, un MSSP peut assurer la protection totale du SI de son client, qui se concentre, lui, sur sa croissance.

d'information (ANSSI). Alors, faute de disposer en interne de compétences dédiées en cybersécurité, nombre de ces organisations font désormais davantage appel à ces MSSP. Leurs prestations sont souvent abordables à court terme, car ils mutualisent leurs cyber ressources disponibles entre plusieurs clients. Mais que vendent-ils exactement ?

Quelles sont les offres de service vendues par les MSSP ?

Le catalogue des services de cybersécurité vendus sur abonnement pluriannuel par les MSSP est vaste désormais. Il va de la simple surveillance du périmètre des systèmes IT à des services gérant entièrement la sécurité du SI d'un client pour les plus compétents d'entre eux. En voici quelques exemples.
L'un des cyber services les plus populaires est la gestion en continu de la vulnérabilité des terminaux, de leurs fichiers et des systèmes. Les MSSP les détectent grâce à leurs outils XDR et ils mettent en place différents processus pour les corriger si besoin. Ces prestataires peuvent également infogérer les pares-feux du client afin d'assurer la sécurité du trafic entrant et sortant sur ses réseaux. Ce type de service intègre une surveillance et un audit, voire l'application de correctifs si nécessaire.
Le MSSP peut aussi proposer à ses clients de gérer le déploiement et l'administration d'un réseau privé virtuel (VPN). Ce service permet d'isoler et de protéger leurs activités quotidiennes grâce à un contrôle strict de l'accès aux réseaux.
Autre exemple, celui des MSSP qui se transforment souvent en « chasseurs de menaces » (« Threat Hunting »). Ils utilisent des logiciels les aidant à identifier, de manière plus proactive, les attaquants et les cybermenaces qui ont échappé aux premières défenses EDR basées sur la seule sécurité périmétrique des terminaux. Enfin, la plupart des MSSP ne se contentent pas de surveiller et de détecter les cybermenaces (MDR). S'ils en ont les compétences certifiées, ils peuvent également procéder à de la réponse aux incidents, *via* des correctifs. Selon CrowdStrike, l'éditeur de la plateforme Falcon, « *les meilleurs MSSP proposent une surveillance 24 h/24 et 7 j/7 à partir d'un SOC (Security Operations Center), une recherche proactive des menaces pour enrichir la contextualisation, ainsi que d'autres services complémentaires visant à garantir une détection précise des cybermenaces* ».
Très dynamique, le marché des services de SOC managés connaîtra une croissance de plus de 15 % en France en 2023 selon les estimations de la société d'études Markess by Exægis. « *Du fait du recours à la mutualisation des ressources par le MSSP, l'accès à un SOC devient plus abordable en mode managé* » explique Timotée Veiras, le responsable des études



« Mon entreprise sera-t-elle obligée de remplacer ces cyber outils existants (et de se former à ceux proposés par le MSSP) ? »

Julien Ceraudo,
responsable de l'offre MSSP de l'intégrateur Synetis.

Les **modèles de tarification** des MSSP

À défaut de pouvoir vous communiquer des tarifs précis sur les services vendus sous forme d'abonnements par les MSSP, nous vous expliquons leurs six principaux modèles de tarification, dont certains sont similaires à ceux de l'infogérance IT ou du Cloud.

1. Par utilisateur : comme dans le Cloud, au lieu de facturer en mode licence, ce modèle facture le nombre d'employés qui utilisent ce service par mois. Il convient aux organisations ayant un faible taux de rotation et un personnel stable.

2. À l'unité : cette tarification tient compte de votre infrastructure IT réelle. Les clients des MSSP la privilégient de part sa simplicité et son coût initial relativement faible, mais qui peut évoluer rapidement si vous élargissez son périmètre.

3. À la carte : plus flexible, ce modèle permet notamment aux clients de créer des solutions et des services plus personnalisés, mais à un tarif en conséquence.

4. Au bundle : ils contiennent des offres de cybersécurité basiques et standardisées, auxquelles le client peut ajouter des services plus avancés vendus plus chers.

5. À la tarification forfaitaire : les entreprises peuvent accéder à une variété de services, y compris l'assistance à distance et sur site, sans modifier leur budget mensuel initial. Problème, le temps de réponse est plus élevé que celui des services à la carte, vendus, eux, plus cher.

6. Au monitoring : cette offre fournit une couverture minimale contre les cybermenaces. Ce forfait convient aux entreprises qui disposent déjà en interne d'experts en cybersécurité.

en cybersécurité de Markess by Exægis. Attention toutefois au ticket d'entrée : *« les prix varient du simple au quadruple pour le SOC (de 50 et 200 000 € par an), en fonction notamment des options retenues. Pour l'heure, les offres packagées, dont celles sur les micros SOC et l'EDR sont les plus recherchées par les PME »*. Mais avant d'accéder à ces prestations jadis réservées aux seuls grands comptes, pensez à vérifier que le MSSP dispose bien des compétences nécessaires à un instant T pour vous… Et que tous les critères de réponse ou de gestion des incidents sont bien prévus au contrat…

L'exemple de Sophos

L'ancien éditeur de solutions de sécurité s'est totalement tourné vers ce modèle de services et est reconnu par les cabinets d'analystes dans sa catégorie. Récemment, l'entreprise a mis sur le marché Sophos Managed Detection & Response (MDR) pour Microsoft Defender, une offre entièrement managée qui propose les capacités de réponse aux menaces pour les entreprises utilisant Microsoft Security. Sophos MDR pour Microsoft Defender apporte un niveau critique de protection 24x7 dans l'ensemble de la suite de solutions Microsoft Security (Endpoint, SIEM, Identity, Cloud, *etc.*) contre les piratages de données, ransomwares et autres cyberattaques actives. Sophos MDR pour Microsoft Defender intègre des données télémétriques provenant d'une gamme étendue d'outils Microsoft Security. À la différence d'autres offres MDR qui se cantonnent à Microsoft Defender for Endpoint ou Microsoft Sentinel et proposent des capacités minimales de réponse aux menaces, Sophos MDR renforce l'ensemble de la suite Microsoft Security.

Posez les bonnes questions avant de signer

Il est donc préférable de lui poser les bonnes questions avant de contractualiser. Tout d'abord, le client peut s'enquérir de ses pratiques en matière de recrutement et de formation permanente de son personnel. Mais aussi de leurs disponibilités en fonction des offres retenues (voir encadré 2). Bénéficierez-vous d'un expert différent et dédié pour chaque service acheté au MSSP, ou accéderez-vous seulement à un pool d'experts mutualisés ?

Et en cas d'attaque, quels seront les temps moyens de détection (MTTD) et de réponse (MTTR) garantis au contrat (SLA). Deux métriques importantes, et notamment pour les entreprises qui veulent souscrire une cyber assurance. Dans le même registre, les rapports générés sont-ils exploitables, sous quels formats et fréquence ?

Autres questions importantes, sur quels critères sélectionne-t-il ses cyber fournisseurs ? Les solutions retenues sont-elles à la pointe du progrès et actualisées régulièrement ? Non seulement son offre produit doit être compétitive sur le plan technique, mais la qualité de la relation que le MSSP entretient avec ses fournisseurs conditionne aussi la réussite de ses services managés.

Terminons avec deux questions qui reviennent sans cesse chez les DSI selon Julien Ceraudo, responsable de l'offre MSSP de l'intégrateur Synetis : *« mon entreprise*

« Du fait du recours à la mutualisation des ressources par le MSSP, l'accès à un SOC devient plus abordable en mode managé. »

Timothée Veiras,
Responsable de l'expertise Cybersécurité chez Markess by Exaegis.

Une entreprise sur deux choisit **un MSSP pour ses seules compétences**

Une étude menée en 2022 par l'éditeur Kaspersky auprès de décideurs informatiques à l'international révèle les raisons qui poussent une entreprise à travailler avec un MSP ou MSSP. Selon 65 % des PME et des grandes entreprises interrogées (54 % en Europe), la raison la plus courante de transférer certaines responsabilités en matière de sécurité informatique à des MSP/MSSP est l'efficacité de ces spécialistes externes. Les entreprises font également référence au besoin de recourir à connaissances spécifiques (51 % au global, 48 % en Europe), à la pénurie de personnel qualifié (50 % au total, un peu moins en Europe avec 34 %), à la complexité des processus d'entreprise (46 % dans le monde, 40 % en Europe) et aux exigences relatives à la mise en conformité (45 % au global contre 33 % pour les pays européens).

En ce qui concerne la coopération avec les MSP ou MSSP, 64 % des entreprises européennes (près de 70 % à l'échelle mondiale), ont indiqué à Kaspersky travailler habituellement avec deux à trois fournisseurs, tandis qu'au total, 17 % des PME et 21 % des grandes entreprises disent traiter avec plus de quatre MSSP par an. En Europe, seules 10 % de tous les types d'entreprises affirment faire de même.

sera-t-elle obligée de remplacer ces cyber outils existants et de se former à ceux proposés par le MSSP ? Et enfin, quelles sont les conditions et le coût de sortie du contrat ? ».

Attention, un MSSP peut refuser de travailler avec vous

Le MSSP refuse parfois de signer un contrat avec certaines entreprises quand il estime que leur niveau de sécurité est trop faible et qu'il l'expose trop sur le plan juridique et contractuel. Une seule cyberattaque réussie peut entraîner d'importants préjudices financiers au MSSP et à ses clients, porter atteinte à leur réputation, et engendrer un stress énorme pour leurs équipes. Raisons pour lesquelles ces prestataires leur imposent souvent la réalisation d'audits et de tests d'intrusion en amont. Ils simulent alors une cyberattaque contre le SI de l'entreprise afin d'identifier ses vulnérabilités.

Ces tests constituent un moyen efficace pour préparer, planifier et améliorer le programme de cybersécurité et la défense d'un client. Julien Ceraudo estime également important de « *proposer à nos clients de les accompagner dans leurs stratégies cyber et la gouvernance de leurs données afin de les aider à réaliser les bons investissements* ». Avant de collaborer avec un MSSP, il est donc important de bien border en amont le contrat et ses limites, surtout en cas de sinistre.

Olivier Bellin

Sur **quels critères** choisir son MSSP ?

Vous envisagez de travailler avec un ou plusieurs MSSP afin de sécuriser votre SI ? Mettez toutes les chances de votre côté et posez-leur les bonnes questions. Nos conseils pour bien les choisir avec l'aide des MSSP Metsys et Synetis.

Identifiez vos cyber besoins et leur évolution

Demandez-vous si le ou les cyber services managés dont vous pensez avoir besoin à un instant T, qu'il soit global ou sur un périmètre spécifique de votre SI, évoluera au même rythme que les cybermenaces et les besoins de vos métiers. Le MSSP choisi est-il alors en capacité de vous suivre dans la durée et accompagner votre montée en compétences ?

Corrélez vos besoins à votre budget

Si votre budget est limité et que vous n'avez pas les moyens de superviser des incidents en 24/7, mutualisez les ressources avec un MSSP et focalisez-vous sur la gestion des cyber menaces les plus critiques. Vous pourrez ainsi faire monter en charge vos compétences et votre relation avec les MSSP.

Mettez des MSSP en concurrence

Une fois vos besoins identifiés, créez une liste de prestataires qui répondent à vos critères et mettez-les en concurrence, tantôt sur un périmètre spécifique de votre SI ou sur sa globalité, selon la taille de votre entreprise et votre budget. Demandez-leur de réaliser un audit de votre SI, voire un test d'intrusion.

Validez les compétences techniques et services des MSSP

Demandez par exemple qu'est-ce que le MSSP implémente parmi les 11 stratégies SOC du MITRE ? Comment implémente-t-il la définition Gartner du SOAR ? Quelles sont les technologies-clef de détection que le MSSP recommande d'intégrer au périmètre SOC ? Est-ce que le MSSP propose un service de VOC (« Vulnerabilities Operations Center ») ou d'EASM (« External Attack Surface Management ») ?

Vérifiez les compétences disponibles

Sur un marché où la rareté et la volatilité des cyber compétences est aussi importante, il n'est pas inutile de s'assurer que le MSSP dispose bien des certifications fournisseurs à jour et des collaborateurs annoncés par ses commerciaux. Vérifiez aussi ses niveaux de certification sur le site de l'Agence nationale de la sécurité des systèmes d'information (Anssi).

Optez pour des offres et une tarification claires

Pour éviter les coûts cachés et rendre évolutif votre partenariat, privilégiez un MSSP transparent sur le modèle financier proposé (voir encadré 4), tant sur ses services managés que sur les licences pour la ou les cyber solutions fournies. En effet, les modèles de facturation (par abonnement) varient fortement d'un éditeur à l'autre. Ils peuvent être basés sur le volume d'actifs à superviser, le nombre de sièges, de données collectées, etc. Et comment le MSSP vous facture-t-il ses cyber services managés ? Au nombre de tickets traités ou sur un forfait par exemple ?

Souhaitez-vous des services personnalisés ?

Les clients reprochent souvent aux MSSP de ne leur vendre que des cyber services disponibles sur étagère. Ces prestataires peuvent difficilement leur vendre autre chose que des offres bien packagées et industrialisées s'ils veulent qu'elles soient à des prix abordables et bordées juridiquement. Certains MSSP proposent cependant des solutions personnalisées à la carte..., tout comme leur prix.

Faîtes valider le contrat sur le plan juridique

Aux vues des cyber risques et des conséquences désastreuses évoquées, assurez-vous que votre contrat avec le MSSP est en français et bien bordé sur le plan juridique. Est-il valable H24 et sur toute géographie ? Qui est responsable et qui paie les pots cassés en cas de cyberattaque réussie ? Que se passe-t-il si les outils ou équipes du MSSP ne sont pas disponibles ou au mieux de leurs capacités ?

Favorisez un partenariat dans la durée

La réussite d'une relation avec un MSSP doit être basée sur une confiance dans la stratégie et les solutions proposées, mais aussi dans les équipes qui les gèrent au quotidien. D'autant que les contrats sont souvent proposés pour une durée initiale variant de 24 à 36 mois en moyenne.

Doctolib au défi de **sécuriser des documents** échangés par ses utilisateurs

Le site de prise de rendez-vous médicaux pratique un chiffrement de bout en bout des données : il n'a jamais accès aux données médicales de ses utilisateurs. Une approche qui apporte une grande sécurité en cas de fuite de données, mais qui complique sérieusement la donne pour détecter les malwares dans les fichiers échangés.

Avec 70 millions d'utilisateurs actifs sur son service de prise de rendez-vous, Doctolib est un acteur incontournable du secteur médical français, notamment dans la relation entre les patients et leurs médecins. La sécurité du service et des données des patients est donc cruciale et toute fuite de données serait catastrophique tant pour la réputation du service que pour les patients. En juillet 2020, le site avait été victime d'une attaque portant sur les données de plus de 6 000 rendez-vous, mais le pirate avait dû se contenter de données administratives et n'avait pu accéder aux données des patients.

Doctolib, grand adepte du chiffrement de bout en bout

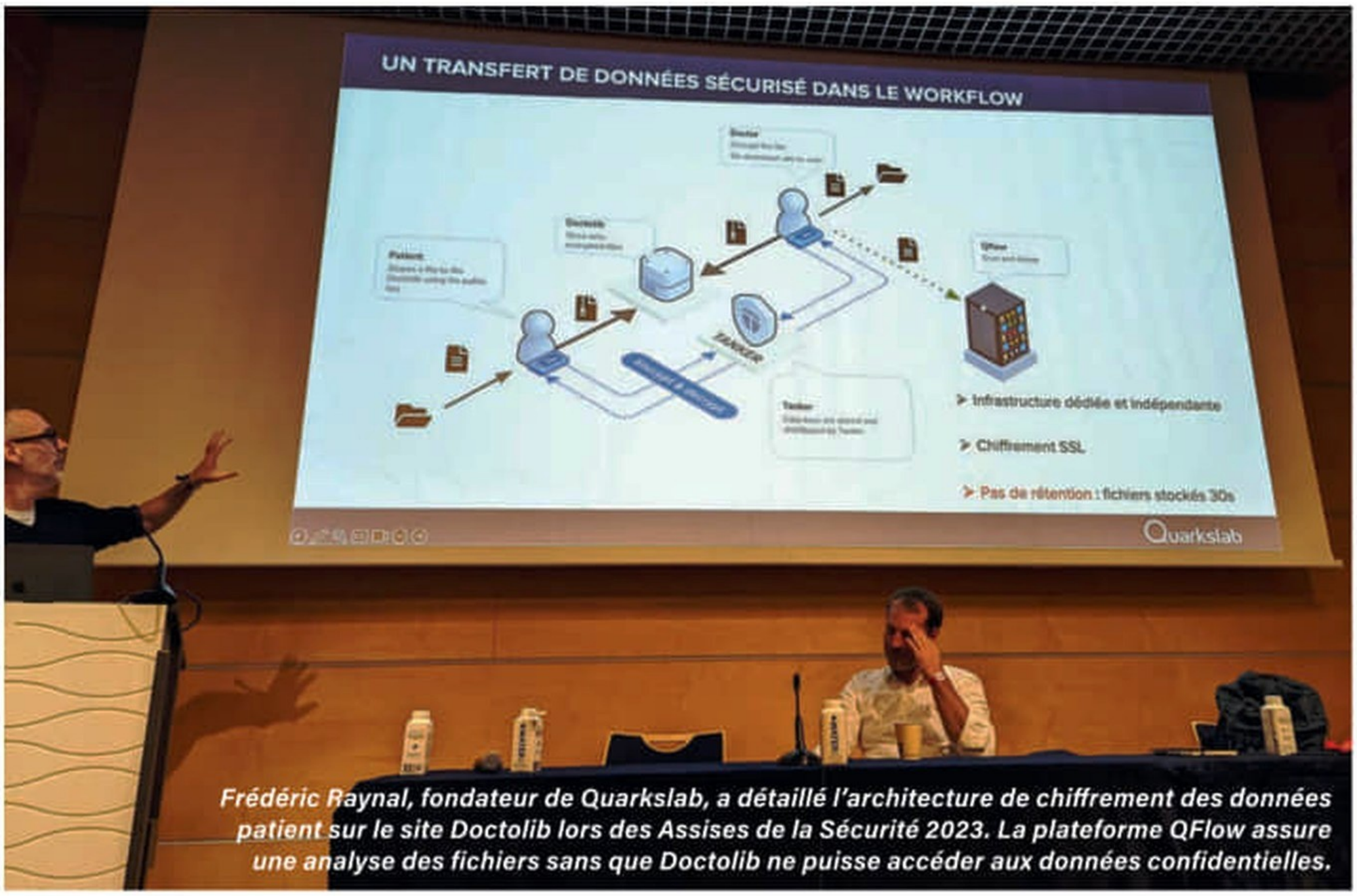
Pour ces dernières, le principe est simple : un chiffrement de bout en bout de toutes les données échangées entre le patient et son médecin. Cédric Voisin, RSSI de Doctolib, résume le processus mis en œuvre : *« lorsqu'un patient souhaite partager une ordonnance de son médecin avec un spécialiste, au moment où il crée son compte sur Doctolib, la plateforme génère un login, un mot de passe, un code d'authentification multifacteurs. Lors de cette phase d'enrôlement, nous générons aussi une paire de clés afin de chiffrer les documents qui transitent via notre plateforme. »* Doctolib a choisi la solution de gestion des clés de chiffrement Tanker dont il a racheté l'éditeur en 2022. Le médecin étant considéré comme une personne de confiance par le patient, ce dernier va partager avec lui sa clé publique et le médecin va pouvoir déchiffrer le document de son côté. Le RSSI précise : *« nous ne faisons que stocker des blobs dans une base de données. »* Pour s'assurer de la sécurité de l'infrastructure de bout en bout imaginée par Doctolib et Tanker, un PenTest a été mené par la société Quarkslab pendant 26 jours uniquement sur ce volet chiffrement des données. Cet audit approfondi a révélé 17 problèmes, dont 2 vulnérabilités. Ces vulnérabilités ont été rapidement corrigées.

Un vrai risque de transmission de virus par le patient

Comme les fichiers échangés par les patients et praticiens sont stockés en tant que binaires chiffrés, donc illisibles tant par le personnel de Doctolib que par un éventuel attaquant, le RSSI reste serein quant au risque de vol de données de santé. Cédric Voisin estime que le viewer de fichier proposé en ligne sur le site est très basique et ne peut déclencher de charge malveillante. Par contre, le scénario du patient dont l'ordinateur est infecté et qui transmet à son médecin un fichier infecté par un malware est tout à fait possible, ce qui pourrait infecter un hôpital. Ce risque est loin d'être purement théorique quand on sait que 2 millions de fichiers sont échangés chaque mois sur la plateforme Doctolib… Face aux questions des hôpitaux quant à l'innocuité des fichiers leur parvenant depuis Doctolib, Cédric Voisin ne pouvait que botter en touche : *« nous devions leur répondre qu'il nous est impossible de faire de scan antivirus sur des fichiers dont nous n'avons pas accès au contenu… »*

« Contrairement au secteur bancaire où l'on peut toujours changer de numéro de carte bancaire, il n'y a aucun moyen de révoquer des données de santé. Nous devons nous assurer qu'en cas de fuite de données, cela prendra plusieurs dizaines d'années pour casser un jeu de données. »

Cédric Voisin, RSSI de Doctolib.



Frédéric Raynal, fondateur de Quarkslab, a détaillé l'architecture de chiffrement des données patient sur le site Doctolib lors des Assises de la Sécurité 2023. La plateforme QFlow assure une analyse des fichiers sans que Doctolib ne puisse accéder aux données confidentielles.

Le RSSI va alors travailler avec Quarkslab afin d'imaginer une architecture qui allait pouvoir lui permettre d'analyser ces fichiers sans jamais avoir accès à leur contenu. *« Nous nous sommes interrogés sur le moment où nous pourrions lancer un scan : lors de l'upload du fichier, lors du download ou à ces deux moments. Sachant qu'une vulnérabilité Zero Day ou qu'une menace peuvent être inconnues au moment de l'upload, mais détectables quelques semaines plus tard au moment du download, nous avons fait le choix de ne pas se préoccuper de l'upload. Par contre, nous voulions lancer un scan du fichier à chaque download. »*

L'idée qui émerge alors est de créer une plateforme externe à Doctolib qui va recevoir le contenu du fichier en clair pour mener une analyse, puis détruire immédiatement le fichier. La contrainte est que ce contrôle doit être totalement automatique et transparent vis-à-vis des praticiens et des services informatiques des hôpitaux afin de n'entraîner aucune surcharge de travail ni perte de temps. Fréderic Raynal, fondateur de Quarkslab détaille ce qui a été mis en place : *« nous avons mis en place une plateforme baptisée QFlow et qui est ici mise en œuvre via des API. Dès qu'un praticien veut récupérer un document sur Doctolib, avant que celui-ci ne soit réellement téléchargé sur son poste de travail, il est analysé par plusieurs moteurs de détection. »*

Un hébergement sur OVHCloud HDS

Cette plateforme de contrôle des fichiers est bien évidemment conforme au référentiel de certification de l'Agence du Numérique en Santé et est hébergée sur la partie HDS d'OVHcloud. Frédéric Raynal détaille le processus mis en place : *« avant que le fichier ne soit copié sur le poste de travail du praticien, il est envoyé par VPN sécurisé sur l'infrastructure de QFlow qui est totalement distincte de l'infrastructure de stockage des données en mode blob et de l'infrastructure de stockage des clés et une dédié à l'analyse, le tout chez trois hébergeurs différents. »* A la différence des deux infrastructures gérées par Doctolib, ce sont des données en clair qui arrivent sur QFlow. Il fallait donc limiter au maximum l'accès à ces données pour ne pas en faire le maillon faible de l'architecture : *« nous disposons d'une infrastructure dédiée chez OVHcloud, avec un chiffrement SSL pour éviter les interceptions, et surtout nous ne conservons surtout pas les données. Quand un fichier est envoyé sur la plateforme, il est analysé et dès que l'analyse est terminée, il est effacé. Le but est de minimiser la durée de vie des données sensibles. Celle-ci est de l'ordre de 30 secondes. »*

Doctolib dispose d'un client lourd dont l'usage est réservé aux praticiens. Le logiciel embarque le même mécanisme de chiffrement. *« Dès lors qu'il dispose du client, qu'il soit sur Internet ou en mode déconnecté, il peut ouvrir les fichiers mis en local lors de la dernière synchronisation »* explique Cédric Voisin. Pour les responsables cybersécurité des hôpitaux, ceux-ci disposent d'une vue centralisée de tout ce qui est détecté par la plateforme, notamment pour détecter si leur personnel fait l'objet d'une attaque. Quarkslab met en œuvre des moteurs d'analyse spécifiques pour les documents Office, pour les PDF, pour les exécutables, les applications Android apk, des certifications, flux chiffrés, *etc. « Pour Doctolib, nous avons mis en œuvre des sondes dédiées à l'analyse de documents »* ajoute Fréderic Raynal. *« L'analyse d'un fichier suspect peut être éventuellement complétée d'une intervention manuelle sur les cas où cela peut avoir un intérêt, c'est l'une des particularités de Quarkslab. »*

A.C

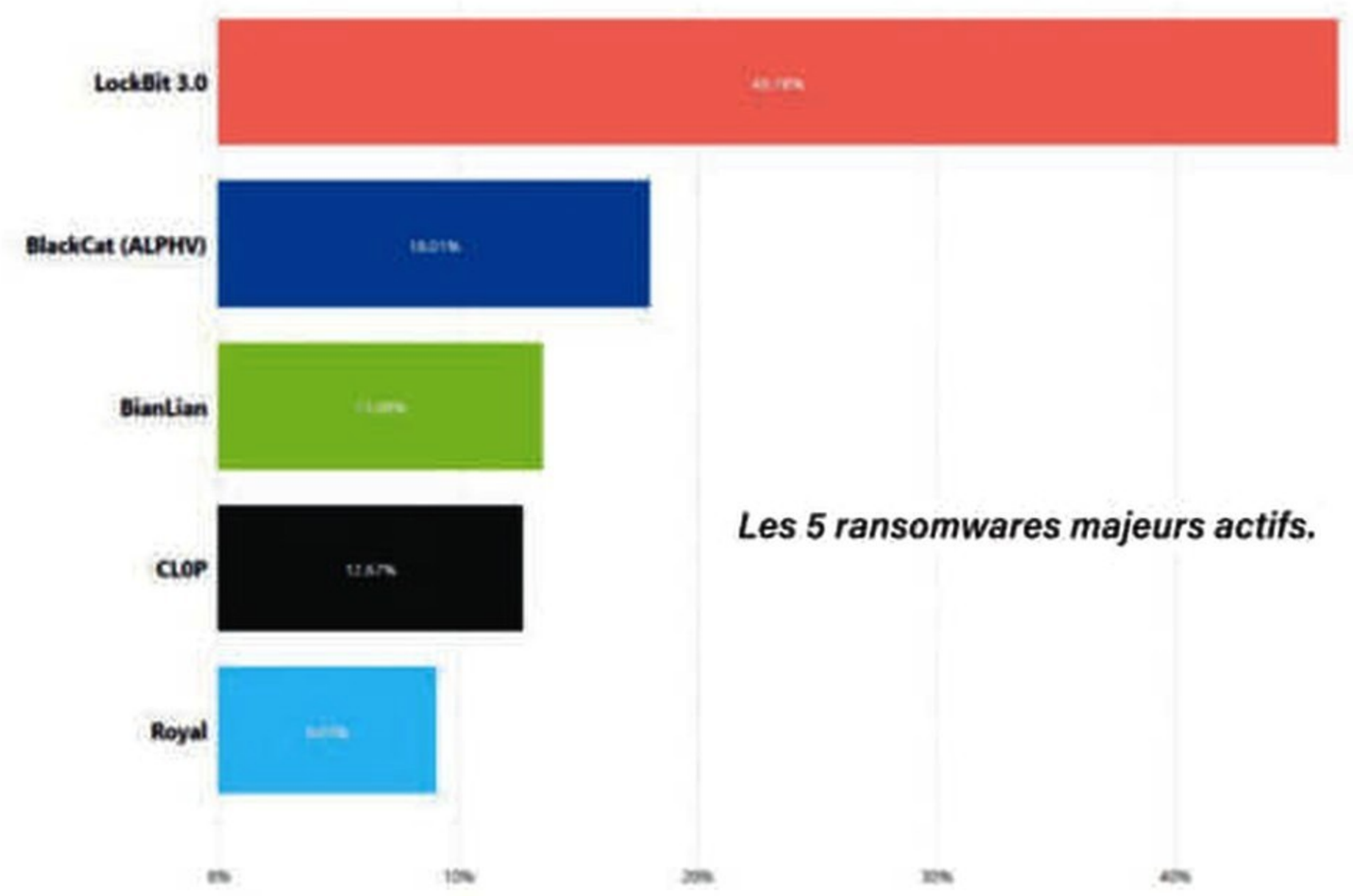
Le **cybercrime** poursuit son industrialisation

L'Agence de l'Union européenne pour la cybersécurité (ENISA) dresse chaque année un panorama des menaces. Selon celui-ci, les cyberattaques deviennent de plus en plus sophistiquées et ciblées. Autre tendance lourde, les attaques à visée politique se banalisent.

Créée en 2004 par un Règlement européen, l'ENISA publie annuellement un rapport depuis 11 ans sur l'activité des acteurs de la menace, une expression englobant les hackers classiques et les groupes œuvrant pour le compte de gouvernement. Baptisé ENISA Threat Landscape (ETL), ce rapport publié le 19 octobre 2023 recense les principales menaces, les tendances observées, les acteurs et les techniques d'attaque. Il tente également d'analyser les motivations des attaquants. Les données ne sont pas limitées à l'Europe. Le rapport est basé sur des données recueillies par l'Agence de juillet 2022 à juin 2023 auprès d'organisation comme l'agence américaine CISA (Cybersecurity and Infrastructure Security Agency), le CERT. EU… et des éditeurs spécialisés (ESET,…). Le rapport a également évalué les dégâts consécutifs à une attaque réussie *via* une enquête auprès de victimes.

Les principaux types d'attaques

Comme l'année dernière, le rapport cible les huit types d'attaques et les analyse. En termes de nombre, les ransomwares et attaques par déni de service arrivent en tête. Autre tendance, le contexte international, et bien sûr la guerre en Ukraine ont démultiplié les activités des groupes de hackers œuvrant pour des états comme la Russie, la Chine… Côté Malware, l'une des plus grandes menaces reste le vol d'informations avec des logiciels malveillants comme Agent Tesla, RedLine Stealer ou FormoBook. Par contre, les auteurs constatent un déclin constant des logiciels malveillants mobiles classiques, toujours liés à des logiciels publicitaires en nombre d'occurrences. Sur les terminaux mobiles, le risque le plus important tient désormais à des logiciels « espions ». La chaîne d'approvisionnement logicielle devient toujours une cible privilégiée. Selon de nombreux rapports, plus de la moitié des entreprises ont été impactées par des tentatives de ce type au cours des douze derniers mois. BlackBerry avance même que quatre décideurs informatiques sur cinq ont été concernés. Le rapport prévoit que le coût total lié à ces attaques va augmenter sensiblement par rapport à 2023. Côté OT, le paysage est un peu plus nuancé. Les tentatives des hacktivistes contre les infrastructures industrielles ne semblent pas effectives. Ce n'est pas le cas des groupes œuvrant pour le compte d'états. Illustration, en mai 2023, un nouveau malware ciblant l'OT et les ICS (système industriel) a été découvert et suivi sous le nom de COSMICENERGY. Son but est de perturber l'alimentation électrique en impactant les relais utilisés pour le transport et la distribution d'électricité en Europe. De leur côté, les attaques DDOS deviennent de plus complexes et plus massives. Elles s'orientent vers les réseaux mobiles et l'IoT et sont utilisés parfois comme moyens supplémentaires dans le contexte de conflit. Les coupures d'Internet ont atteint un niveau sans précédent et cette menace perdure. Parmi les autres typologies analysées, et toujours sans surprise, le phishing, devenu du spear phishing, reste un vecteur d'entrée prisé par les attaquants. Une liste pas exhaustive soulignant globalement une montée en puissance des techniques, des méthodes et de l'activité des cybercriminels. Le rapport apporte les chiffres, officiels, d'attaques et les détaille par secteur d'activité et typologie. Côté cible, seul changement notable par rapport à l'année précédente, si le secteur public reste le plus attaqué, la catégorie « individus » arrive derrière et représente désormais pas moins de 11 % des faits recensés. Il s'agit de personnes occupant des postes clés, hommes politiques, responsables, journalistes, chercheurs en sécurité ou militants.



Les 5 ransomwares majeurs actifs.

Industrialisation en cours

Les auteurs du rapport ont aussi réparti autant que possible les attaquants en catégorie, à savoir les groupes liés à des états, les

hacktivistes, les acteurs du cybercrime et les hackers « à louer ». Guerre d'Ukraine oblige, l'accent est souvent mis sur le premier groupe et sur le danger qu'il représente pour les démocraties. Les auteurs ont classé les attaques en fonction des motivations, politiques ou vénales des attaquants. Si l'argent arrive en tête, l'espionnage, l'activisme, les actions perturbatrices menées pour des raisons géopolitiques représentent plus d'un tiers des cas. Quel que soit le profil, les techniques utilisées se complexifient toujours plus. Dans le but de passer sous les radars, des outils de bas niveau, des Living Off the Land Binaires ou LOLBins sont détournés. Ces fichiers sont utilisés pour gagner en persistance ou augmenter les privilèges. Selon le rapport, ces binaires signés par Microsoft, par exemple Certutil, (un fichier exe destiné à gérer les certificats), peuvent être détournés et servir de porte d'entrée. Autre exemple, des outils de Remote Monitoring and Management sont détournés de leur usage légitime. Le rapport souligne également l'émergence de « Frankenransomware ». Par cette expression, les spécialistes expliquent que les hackers créent de nouvelles variantes de ransomware en utilisant des fragments de code volés ou divulgués provenant de diverses sources. Exemple, utilisé pour cibler les systèmes Vmware, le malware ESXiArgs emprunte le code « demande de rançon » à un ransomware, le système de cryptage à un autre. Les innovations ne se limitent pas aux seuls outils. Les attaquants passent par de l'ingénierie sociale et du spear phishing pour amener des utilisateurs à installer des logiciels qui n'ont pas été fournis via des mécanismes normaux de livraison, des logiciels « trojanisés ».

Facteur aggravant, le modèle As-a-Service proposé par des groupes sur un « marché » du cybercrime en pleine expansion se professionnalise. Signe le plus frappant de cette tendance, les forums de hackers suivent désormais des règles similaires que les sites d'e-commerce, avec par exemple des bannières animées, des visuels, … Les services proposés permettent à des novices en la matière de lancer des attaques. Une professionnalisation qui témoigne de l'expansion du marché de la cybercriminalité. Les auteurs du rapport prévoient encore mieux ! Ils s'attendent à une collaboration accrue entre ces différents « Crime-as-a-Service » assortie d'une spécialisation. Un service fournira des plans d'attaques, un autre collecte les informations et le profilage, un troisième entre dans le système de la cible… La dernière partie du rapport propose des recommandations. ▮ **P. Br**

Des **impacts sociaux** aussi

Les auteurs ont interrogé les entreprises ou entités publiques touchées sur les conséquences des cyberattaques. Plusieurs dimensions étaient prises en compte, économique, sur le système d'information, et aussi social, psychologique, en termes de réputation, et même physique. Les réponses étaient croisées et donnaient la répartition des types de menaces par impact. Résultats tout type de menaces confondues, si le système d'information reste le premier impacté et si, les contrecoups économiques et financiers suivent, les impacts sociaux et sociétaux sont loin d'être négligeables. Ils sont soulignés par une entreprise sur trois.

1er Club Français de décideurs informatiques & télécoms

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

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

FONDATEURS

Véronique Daval Présidente — Julien Daval Vice-Président

LES MEMBRES DU BUREAU ET AMBASSADEURS DU CLUB

Armand ASSOULINE
CIO & National Documentation Manager - MSC

Laurent BAYOL
DSI
LA COMPAGNIE

Nawal BENSASSI
CIO & Digital Officer
ESRI FRANCE

Gilles BERTHELOT
Directeur Sécurité Numériques
GROUPE SNCF

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

Benoit DECOCK
Business transformation numérique leader
AGFA

Christian DOGUET
CIO
ChAINE ThERMALE DU SOLEIL

Alain GUEDE
CIO
GROUPE SARETEC

Christophe GUILLARME
RSSI
LAGARDèRE TRAVEL RETAIL

Philippe LAGRANGE
Directeur recherche et prospective
MUTUELLE GéNéRALE DE LA POLICE

Stéphane MALGRAND
DSI
LABORATOIRE NATIONAL MéTROLOGIE ET ESSAIS

Sandrine RACOUChOT
DSI
INTER MUTUELLES hABITAT

Lionel ROBIN
DSI
ThE SET hOTELS

Claude YAMEOGO
ARChITECT SI
ALSTOM

COORDINATEUR

TRIEU hUyNh-ThIEN

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

Encore des inquiétudes sur la **conformité des données**

Une étude réalisée par Coleman Parkes Research pour le compte de Cloudera auprès de 850 décisionnaires en informatique dont 200 en France démontre une inquiétude toujours présente sur la conformité des données par rapport aux différentes législations en vigueur dans le monde.

Sous le déluge de données dans les entreprises, les décisionnaires sont inquiets et vont jusqu'à craindre une perte de contrôle sur celui-ci. Dans la zone EMEA, ce sont 66 % des personnes interrogées qui le craignent. La conformité est un sujet de premier plan pour 79 % des répondants en ce qui concerne la gestion des données.

Des causes identifiées

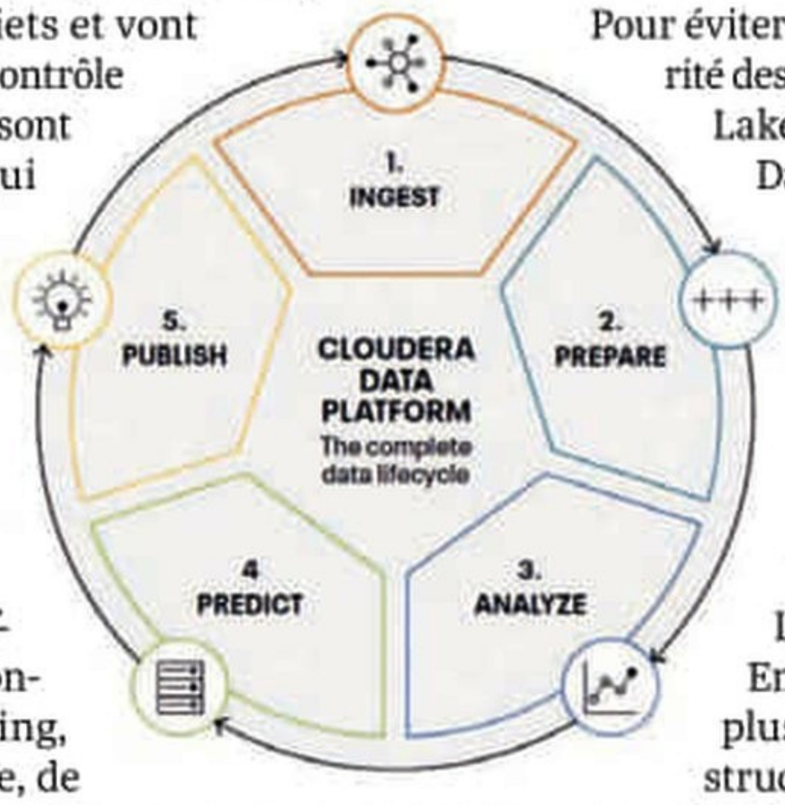
63 % des répondants indiquent les silos de données comme le point qui rend difficile le respect des différentes régulations autour des données. Les secteurs du manufacturing, de la santé et des sciences de la vie, de la banque et de la finance sont les plus concernés par cette question. Le secteur de la finance pointe particulièrement la dispersion des données depuis plusieurs décennies sur des plateformes différentes et anciennes. 60 % des décideurs informatiques français considèrent que le cloisonnement des données entrave la capacité à se conformer aux réglementations en matière de conformité des données.

Pour les quatre cinquièmes des personnes interrogées, la mise en œuvre de solutions analytiques et de gestion des données spécifiques a rendu la question encore plus ardue. 63 % indiquent la complexité de suivre les données sur leur cycle de vie avec ces applications spécifiques. Ils relèvent de plus le coût élevé de ces solutions. La principale conséquence de la complexité induite est que les entreprises se tournent vers des partenaires extérieures pour développer et exécuter leurs stratégies autour des données (84 %). Plus de 8 décideurs informatiques français sur 10 (82 %) estiment que l'intégration de solutions ponctuelles pour l'analyse et la gestion des données a entraîné une augmentation des coûts liés à la donnée. Les entreprises dépensent ainsi plus d'un quart de leur budget informatique dans ces différentes opérations de mise en œuvre de leur stratégie autour des données.

Une maturité très relative

Quand on les interroge sur leur maturité autour du cycle de vie des données, les entreprises démontrent un état d'avancement très relatif. 34 % se déclarent très matures dans l'ingestion des données. Dans le même ordre d'idées, elles sont très matures pour réaliser des prédictions sur leurs données. À 35 %, elles le sont pour la publication des données. Les phases amont et de traitement sont les plus matures avec 41 % des entreprises se disant très matures sur la préparation des données et leur analyse.

Le choix d'un Data Lakehouse



Le cycle de vie des données.

Pour éviter les écueils susmentionnés, la majorité des entreprises ont pris le virage du Data Lakehouse qui combine la puissance du Data Warehouse et les échelles des Data Lakes. Globalement, 68 % des entreprises interrogées ont mis en place ou prévoient de mettre en place un outil de ce type. Cette proportion varie selon les secteurs. Les télécommunications et les entreprises informatiques et logicielles sont les plus avancées sur ce point.

Les raisons de ce choix sont multiples. En premier lieu, la possibilité d'accéder plus rapidement à la fois aux données structurées et non structurées est le premier critère de cette conversion à cette technologie (62 %). La possibilité de partager les données vient en second lieu (55 %), suivie par le choix d'une architecture moderne (50 %). Un peu moins d'un tiers font ce choix pour soutenir leurs futures opérations autour de l'intelligence artificielle. ▮ **B.G**

Les conseils de Cloudera sur la gouvernance des données

- Faire l'inventaire de toutes les données que l'entreprise possède, crée et utilise.
- Appliquer une norme cohérente à l'ensemble des données régies.
- Identifier les propriétaires des données et leur attribuer des responsabilités.
- Identifier les données sensibles qui nécessitent une protection accrue.
- Mettre en œuvre des mesures bien définies pour se conformer aux réglementations pertinentes en matière de protection de la vie privée.
- Définir des mesures pour identifier les succès mais aussi les domaines nécessitant des améliorations.
- Revoir les protocoles de gouvernance des données et procéder aux ajustements nécessaires.

Digital Services Act

Du papier au terrain, un texte qui se donne les moyens ?

Adopté fin août, le règlement européen sur les services numériques, ou Digital Services Act (DSA), doit faire cesser les mauvaises pratiques des grandes plateformes en ligne, notamment en matière de partage de contenus illégaux. Mais à peine le texte est-il entré en vigueur que déjà des doutes apparaissent : Bruxelles aura-t-elle les capacités techniques de le faire appliquer ?

Big Tech n'a qu'à bien se tenir, car *« les choses ont changé en Europe »*, selon les mots du Commissaire au numérique, Thierry Breton. Effective depuis le 25 août dernier, la loi sur les services numériques (DSA) oblige les grandes plateformes, telles que Meta, Amazon ou encore TikTok, à aller plus loin pour lutter contre les contenus et produits illicites en ligne et pour la protection des utilisateurs. Elles doivent également faire preuve de plus de transparence sur leurs pratiques de modération, leurs algorithmes de recommandation des contenus, et le ciblage publicitaire qu'elles pratiquent. Les entreprises désignées sont également tenues de communiquer des rapports réguliers d'auto-évaluation aux régulateurs.

Une taxe de surveillance

Une redevance de surveillance prélevée sur les Très Grandes Plateformes en Ligne a été mise en place afin de financer les ressources humaines nécessaires, ainsi que d'autres dépenses financières comme la réalisation d'études et la sollicitation d'experts dans le cadre du DSA. Celle-ci sera collectée par les organismes de l'UE et les autorités de régulation nationales. *« La Commission a défini un montant global des coûts devant être récupérés par tous les fournisseurs de services désignés, à environ 45 millions d'euros pour 2024 »*, décrit le porte-parole. Des montants individuels à la charge des plateformes seront définis d'ici le 30 novembre 2023. Aucun prestataire ne supportera *« un montant supérieur à 0,05 % des bénéfices globaux de l'entreprise ou du groupe fournissant le service »*, ajoute le porte-parole. Les plateformes et moteurs de recherche devront payer leurs premières redevances avant le 31 décembre 2023.

Le DSA constitue la première tentative d'envergure dans le monde occidental de régulation des contenus présents sur Internet. Et gare aux récalcitrants, car Bruxelles pourra sanctionner les contrevenants à hauteur de 6 % de leur chiffre d'affaires mondial, imposer des astreintes, ou encore exclure une plateforme du marché européen.

Des demandes d'informations à la pelle

Voilà ce qui est sur le papier. Mais qu'en est-il sur le terrain ? Le texte a entraîné une flopée de réactions du côté des grandes plateformes, qui ont commencé à se mettre au diapason. Meta, par exemple, a limité son ciblage publicitaire auprès des mineurs. TikTok, lui, a proposé de désactiver l'algorithme de recommandation et a intégré une option de signalement de contenus jugés illégaux, option déjà utilisée des dizaines de milliers de fois. L'application chinoise assure également avoir supprimé des millions de vidéos de sa propre initiative.

La Commission européenne, elle, veille au grain et a déjà envoyé des demandes d'informations formelles à YouTube, Amazon et bien d'autres. AliExpress (Alibaba), par exemple, a été sommé de fournir des informations sur les moyens de lutte engagés contre la diffusion de produits illégaux, dangereux et contrefaits, tels des médicaments. Meta (Facebook, Instagram), X (ex-Twitter), et TikTok ont dû, quant à eux, fournir des détails sur les mesures mises en place pour lutter contre la désinformation et la diffusion de contenus violents et haineux, suite à l'attaque du Hamas contre Israël, le 7 octobre dernier.

Les **entreprises concernées**

Dix-sept entreprises et deux moteurs de recherche touchant plus de 45 millions d'utilisateurs actifs par mois sont concernés par le DSA. Il s'agit de : Alibaba AliExpress ; Amazon Store ; Apple AppStore ; Booking.com ; Facebook ; Google Play ; Google Maps ; Google Shopping ; Instagram ; LinkedIn ; Pinterest ; Snapchat ; TikTok ; Twitter ; Wikipedia ; YouTube ; Zalando ; Bing ; Google Search. À partir du 17 février 2024, le DSA concernera toutes les plateformes, sans discrimination de taille.

Et après ?

Malgré ces actions très médiatisées, certains émettent des doutes quant à la volonté politique de l'Union européenne et des moyens à disposition pour faire appliquer le texte. *« Le DSA a le potentiel de modifier les comportements problématiques des entreprises et des utilisateurs. Mais un arsenal juridique ne veut rien dire en soi. Est-ce que Bruxelles aura les moyens de contrôle pour appliquer les dispositions du DSA (voir encadré page ci-contre, ndlr), et a-t-elle la volonté politique suffisante pour tenir tête à quelqu'un comme Elon Musk (patron de X ex-twitter, ndlr) lorsque sa plateforme ne respecte pas le DSA ?»* s'interroge Julien Pillot, enseignant-chercheur à l'Inseec et conférencier spécialisé sur les questions d'économie du numérique.

La Commission recrute

La Commission européenne se veut rassurante, au moins sur les moyens déployés pour l'application du DSA. Une nouvelle entité a été créée au sein de la Direction générale des réseaux de communication, du contenu et de la technologie (DG Connect) pour laquelle vingt postes ont été ouverts en 2022. *« En 2024, le personnel travaillant sur l'application des DSA atteindra 123 équivalents temps plein, qui seront appelés à appliquer et garantir le respect des règles de manière efficace et compétente »*, explique un porte-parole de la Commission européenne.

Le personnel comprend des experts juridiques, des data scientists et des responsables politiques compétents en matière de numérique. Le Centre européen pour la transparence algorithmique, qui sera associé à DG Connect pour soutenir l'application du DSA, a, quant à lui, recruté vingt experts qui s'ajoutent aux dix membres déjà présents. *« Cette répartition reflète les ressources nécessaires pour accomplir les tâches de la Commission »*, assure le porte-parole.

Contrôle partagé

La Commission s'assure également le support des États membres qui devront, d'ici le 17 février 2024, désigner des coordinateurs de services numériques en charge du contrôle de la conformité des services avec le DSA sur leur territoire. Ces entités indépendantes auront *« de hautes exigences pour exercer leurs missions de manière impartiale et transparente »*, promet le porte-parole.

De leur côté, les plateformes devront faire réaliser à leurs frais, et au moins une fois par an, des audits indépendants afin d'évaluer leur conformité et appliquer des mesures correctives en cas de résultat négatif. Les rapports devront également être rendus publics, au même titre que les mesures d'atténuation mises en place. *« Le régulateur pourra exiger des audits supplémentaires et ciblés, ou l'inspection des systèmes des plateformes lorsqu'il enquêtera sur d'éventuels manquements au règlement »*, ajoute le porte-parole.

Les spécialistes, eux, s'interrogent sur la question de l'obligation de transparence des plateformes concernant le partage de leurs données, indispensable pour l'application du DSA. *« Pour comprendre les algorithmes de recommandation des contenus, il nous faudra davantage que les flux API que mettent en place les plateformes »*, avait déclaré Marc Faddoul, le directeur d'AI Forensics, au journal Les Echos.

Des sanctions dissuasives... ou pas

Que risquent les plateformes en cas de non-respect du DSA ? Comme écrit ci-dessus, dans le pire des cas, les contrevenants s'exposent à des amendes équivalentes à un maximum de 6 % du chiffre d'affaires. Au regard de ce qu'engrangent les grandes plateformes, les montants sont *a priori* colossaux, *« mais prêtent tout de même à sourire »*, fait remarquer Julien Pillot. Le chercheur estime assez faible la probabilité que de telles amendes soient infligées, *« si l'on se fie aux sanctions prononcées dans le cadre de violation du RGPD »*, remarque-t-il.

Si les montants semblent déséquilibrés, il n'en demeure pas moins que les entreprises auront tout intérêt à éviter les sanctions. *« Car cet argent, bien qu'il soit généralement provisionné, constitue tout de même un manque à investir. Mais honnêtement, ce qui pourrait vraiment effrayer ces grandes plateformes, c'est le risque de ne plus avoir le droit d'opérer sur le marché unique. »* De telles sanctions n'ont jamais été prononcées. Et si l'éventualité d'être exclu du marché européen pour une grande plateforme reste extrêmement faible de l'avis du chercheur, le droit ouvre désormais cette possibilité.

Quid de l'exhaustivité du texte ? Julien Pillot prévient : *« une loi réglemente ce qu'elle a observé et, de fait, la législation a toujours un temps de retard. À l'usage, le DSA révélera des failles auxquelles les régulateurs n'ont pas pensé et auxquelles il faudra s'adapter. »* Mais pour le chercheur, aucun doute que si les moyens sont effectivement mis sur la table pour faire appliquer le texte en l'état, *« nous aurons déjà effectué un gros ménage sur Internet. »*

V.M

Les **exigences**

Le DSA exige que les très grandes plateformes en ligne et moteurs de recherche concernés inscrivent dans leurs CGU des informations sur les principaux paramètres de leurs systèmes de recommandation et qu'ils mettent à disposition une fonctionnalité afin de modifier ses options.

Un plan à 800 millions d'euros pour l'IA

Notre bien-aimé chef de l'État a déclaré qu'il allait doubler le nombre de formations en intelligence artificielle et consacrer 500 millions d'euros à la création de clusters IA. Si ces promesses, pour une fois, sont tenues, il y a de beaux jours à venir pour l'IA dans l'hexagone.

En plus de cette modique somme, le gouvernement souhaite investir plusieurs centaines de millions dans un calculateur exascale et renforcer le financement des start-ups spécialisées en IA générative. La France est clairement, à l'heure actuelle, en très bonne position en Europe dans la course à l'intelligence artificielle générative. Elle est en revanche très nettement distancée par la Chine et les États-Unis qui ont, il est vrai, d'autres moyens financiers que nous, et investissent des sommes comportant quelques zéros en plus. Seule l'Union européenne pourrait faire le poids face à ces deux géants, mais elle est aussi désunie sur ce sujet que sur les autres. C'est face à ce constat qu'Emmanuel Macron a annoncé le 14 juin dernier à l'occasion du salon VivaTech ces nouvelles mesures de soutien. *« Il nous faut des talents, du calcul et des moyens »*, a déclaré le président en répondant à une question d'un chercheur français en IA, Arthur Mensch, fondateur de la start-up Mistral AI qui, au passage, avait levé 105 millions d'euros quatre semaines seulement après son lancement. Bien que la France forme des ingénieurs très réputés en IA, elle n'échappe pas pour autant à la pénurie de talents. L'État promet pour y remédier de mobiliser 500 millions d'euros afin de faire émerger *« cinq à dix IA clusters »* dont *« deux ou trois références mondiales »*, rien de moins. Le président n'a cependant fourni aucun détail sur la forme que prendront ces fameux *« clusters »*. Sans doute prendront-ils la forme de pôles de compétitivité associant à la fois institutions, entreprises spécialisées et organismes de formation.

250 millions pour un supercalculateur Exaflops

Pour renforcer les capacités souveraines de calcul et ne plus être dépendant des géants américains du cloud que sont Amazon, Google et Microsoft, la France devrait également investir 50 millions d'euros supplémentaires afin de quadrupler les capacités du supercalculateur Jean Zay du CNRS. Celui-ci a déjà permis l'apprentissage d'un grand modèle de langage, Bloom pour ne pas le citer, développé par la start-up Hugging Face fondée par trois entrepreneurs français (mais basée à New York). La France mise à plus long terme sur un supercalculateur exascale (ou exaflopique si vous préférez) capable de réaliser un milliard de milliards d'opérations par seconde. Un premier projet européen baptisé Jupiter est déjà en cours de développement en Allemagne. La France avait promis de mettre 250 millions sur la table pour celui-ci, l'Europe apportant la même somme. Un pognon de dingue, diraient certaines mauvaises langues, mais il faut ce qu'il faut pour ne pas rester à la traîne dans un domaine aussi important.

50 millions d'euros pour l'IA générative, 40 pour les talents, 40 autres pour la langue française

Le troisième volet des mesures annoncées le 14 juin concerne le soutien des start-up dont le travail est axé sur l'IA générative. Un nouveau fonds d'amorçage, doté d'une enveloppe de 50 millions d'euros, devrait être créé et piloté par Bpifrance (la banque publique d'investissements) en vue de financer des *« innovations pouvant bouleverser les industries existantes »*, pour citer encore notre cher président. S'il est un dirigeant qui croit vraiment à l'intelligence artificielle, c'est bien lui. Il a promis *« un grand challenge »* sur l'IA afin d'attirer les meilleurs talents en France. C'est une très bonne idée, mais il faudrait aussi essayer de garder les nôtres de talents qui ont un peu trop tendance à s'exporter. Néanmoins, aucune précision n'a été donnée quant à la méthode qui sera utilisée, si ce n'est que le projet serait financé à hauteur de 40 millions d'euros par l'État. Une somme équivalente serait déployée pour permettre le développement de base de données en langue française, afin de *« favoriser l'entraînement de modèles d'IA sans biais anglo-saxon »*. La fin de l'abondance ne concernerait donc pas l'IA, si bien entendu toutes ces magnifiques promesses sont tenues. **T.T**

Un fort vent d'IA souffle sur la France, celui de la start-up Mistral AI et de son LLM (Large Language Model), un algorithme d'intelligence artificielle entraîné sur des quantités massives de données.

Le secteur maritime
dans la (cyber)tempête

Réalisé par l'association France Cyber Maritime et OWN, une société de conseil spécialisée, un rapport dresse un paysage alarmant des cyberattaques contre le secteur maritime.

Le 11 mai dernier, l'association France Cyber Maritime[1] et OWN, une société spécialisée qui propose un CERT inter-entreprises, ont présenté le premier Panorama de la cybermenace maritime. Les données et analyses sont issues des travaux du M-CERT (Maritime Computer Emergency Response Team) et d'OWN. Sans grande surprise, le nombre d'attaques a explosé, plus 235 % par rapport à 2020 et plus 21 % par rapport à 2022. *« Près de 90 incidents de cybersécurité notables et publics ont été détectés en 2022 dans le secteur maritime et portuaire au niveau mondial »*, recense le rapport. Un chiffre sans aucun doute loin de la réalité. Cette progression est liée aux activités cybercriminelles, les rançongiciels arrivent en tête, mais aussi à des visées politiques. Depuis le début de la guerre en Ukraine, plusieurs groupes de hackers s'en prennent en particulier à la supply chain. Des attaques potentiellement dangereuses pour l'ensemble de l'économie mondiale. 80 % des marchandises transitent par bateau.

Les attaques touchent tous les acteurs de cette chaîne, ports, armateurs, navires, chantiers navals, logistique… Les approches sont classiques, phishing d'abord, avec utilisation de pièces jointes pour installer des infostealer comme LokiBot… Les clés USB, toujours utilisées entre autres pour des mises à jour sur les navires, servent encore et toujours de vecteurs de propagation de codes malveillants. 24 familles d'infostealers affectant le maritime ont été recensées en 2022 avec une nette majorité d'échantillons de FormBook (aussi appelé Xloader), Agent Tesla, Snake Keylogger et Lokibot. L'ingénierie sociale est également mise à contribution. Plus original, les investigations d'OWN ont dressé un constat alarmant. Nombre de ces attaques ont impliqué un haut niveau de connaissances métiers. Pour illustrer le propos, le rapport détaille entre autres l'activité d'un *« acteur de la menace »*, baptisé POSEIDON-IS_001 par les experts. Les ports et leurs installations sont également visés. Dans le contexte d'une numérisation accrue des activités maritimes, les systèmes d'information des ports couplent IT et OT. Dans un navire, la propulsion, la navigation, l'alimentation électrique… sont gérées par des systèmes de contrôle industriel de type SCADA. Ces systèmes sont devenus aujourd'hui de nouvelles cibles. S'il reste difficile d'avoir une estimation des attaques menées dans ce contexte, et si la technicité qu'elles nécessitent limite le nombre d'attaquants, l'activité d'un groupe baptisé Bentonite, a été identifiée. Il pourrait utiliser un code malveillant baptisé « Incontroller » pour les installations traitant le Gaz Naturel Liquéfié (GNL) et les réseaux électriques, selon la société Dragos, spécialisée dans la sécurité de l'OT.

Autre « cas d'usage » pour les hackers : les systèmes de Positionnement, de Navigation et de Temps (PNT) comme les GNSS qui utilisent le GPS. Des attaques par brouillage ou par leurrage peuvent bloquer des navires à quai ou les faire dévier de leur route. Une zone importante de brouillage GPS impacte une bonne partie de la mer Noire jusqu'aux côtes Roumaines. Côté leurrage, les cas plus fréquemment étudiés montrent que des zones où une multitude de navires se retrouvent. Les câbles sous-marins sont aussi visés. Une attaque contre un câble a été identifiée l'année dernière. Une liste loin d'être exhaustive… et les experts prévoient que cette tendance devrait s'accentuer à l'avenir ! Le rapport ne se limite toutefois pas à ce panorama, mais liste aussi les mesures à prendre pour réduire le risque. Il devrait faciliter le développement d'un réseau d'expertise en cybersécurité maritime.

P. Br

Pour aller plus loin : www.own.security

1 : Créée en 2020, et soutenue par l'ANSSI, France Cyber Maritime regroupe 70 membres, de l'écosystème maritime au sens large.

AxBx ScamShiel

Le bouclier anti-arnaque 100 % « Made in France »

Créée en 1999, AxBx est une société française d'édition de logiciels de sécurité qui commercialise notamment l'antivirus VirusKeeper. Pour compléter son offre, elle vient de lancer un nouveau bouclier anti-arnaque baptisé ScamShield qui serait capable de bloquer des attaques qui passent au travers des solutions traditionnelles.

La petite société AxBx fait de la résistance face aux géants américains de la cybersécurité. Elle se targue d'être totalement indépendante aussi bien sur le plan financier que technologique et de maîtriser l'intégralité du processus de production. Outre l'unique antivirus français VirusKeeper, AxBx développe différents logiciels de sécurité, dont un pare-feu, un coffre-fort à mots de passe, un bouclier anti ransomware, ou encore une solution de protection hybride du poste de travail (Hybrid Endpoint Protection). Pour fêter ses 25 ans, elle vient également de lancer ScamShield qui est un outil de protection contre les arnaques sur Internet telles que les phishings, les URL malveillantes, les sites web dangereux, ou encore les arnaques aux faux supports techniques. Compatible avec tous les navigateurs web, il analyse en temps réel toutes les requêtes http. Bien qu'accessible aux particuliers, ScamShield est destiné essentiellement aux PME et TPE qui figurent parmi les principales victimes de ces arnaques sur Internet. **J.C**

Gregory Snauwaert, CEO et fondateur d'AxBx, revient sur l'importance de développer un outil dédié au segment de menaces des arnaques sur Internet qui a littéralement explosé ces dernières années.

Pouvez-vous nous présenter brièvement AxBx ?

C'est une société basée dans le nord de la France à Villeneuve-d'Ascq qui existe depuis 25 ans et qui était initialement une sorte d'équipementier de la cybersécurité. À l'origine, on développait des SDK ou des briques de base pour des sociétés qui faisaient des pare-feux et de l'antispam à Villeneuve-d'Ascq. Durant quelques années, on a fait ça en travaillant dans l'ombre (sans communiquer), puis un jour, on s'est dit qu'on allait développer nos propres produits plutôt que de créer des éléments techniques pour les autres. Notre produit phare VirusKeeper représente 80 % de notre activité. Tous pays, plateformes et versions confondus, il comptabilise actuellement un peu plus de 37 millions d'utilisateurs. C'est peu comparativement à un acteur comme Symantec avec Norton, mais ils sont arrivés les premiers et ils ont conservé une avance difficile à rattraper. Notre vocation n'est toutefois pas de les concurrencer et de faire « x » millions d'euros de chiffres d'affaires. On est l'anti-start-up par définition. Ce qui nous plaît, c'est de faire des produits techniques, et de satisfaire nos clients, dont beaucoup nous font confiance depuis plus de dix ans.

Pourquoi avoir développé un bouclier anti-arnaque ?

Dans l'univers de toutes les menaces qui existent, les produits habituels de cybersécurité (antivirus, pare-feux...) ne détectent pas les arnaques sur Internet. Typiquement, les arnaques auxquelles je fais référence, ce sont les arnaques aux faux supports techniques où il n'y a pas de code malveillant. Il s'agit juste d'une simple page html qui s'affiche et qui vous dit : « *Attention, votre PC est infecté, on est le support technique de Microsoft, appelez-nous à tel numéro* ». Le problème de ce type de menaces, c'est qu'elles passent entre les mailles du filet des produits de cybersécurité classiques. Lorsque les victimes appellent et rentrent en contact avec le cybercriminel, les scénarios varient. Soit, il fait semblant de travailler à distance sur le poste et lui envoie une facture de 300 euros à régler, soit il les met en confiance, leur fait télécharger un fichier malveillant et infecte vraiment leur poste pour récupérer par exemple des identifiants bancaires. Avec des moyens minimums, ils peuvent toucher des centaines de milliers de personnes.

Qu'est-ce qui différencie ScamShield des autres outils de sécurité ?

Il fallait un outil de sécurité sur ce segment de menaces, car elles explosent. De plus, les escrocs n'ont pas besoin d'avoir un niveau technique extraordinaire, il leur suffit de pirater un site mal sécurisé pour afficher un pop-up. Les modules anti-phishing traditionnels sont surtout axés sur les mails. ScamShield fait quant à lui du filtrage http en temps réel. Quel que soit le navigateur que vous utilisez, il détecte et bloque automatiquement les tentatives de hit (via une page web, un pop-up, un objet ou une URL) qui pointe vers quelque chose de malveillant. Dans le même temps, le logiciel affiche un message d'alerte en rouge sur le navigateur avec la qualification de la menace. Il comprend également une fonction permettant aux utilisateurs de nous signaler lorsqu'ils ont un doute sur un site, une page ou une URL pour que nous vérifiions si c'est une arnaque ou pas. **J.C**

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

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