N° 208 — Juillet - Août 2022

www.linformaticien.com

L'INFORMATICIEN

Étude
La continuité de services sous pression

Tendance
La Silicon Valley perd de son lustre

DOSSIER

Ransomware

Ennemi public N°1

Sécurité
Retour sur le FIC

Réseau
Convergence Infra / Sécurité

Retex
La SNCF fait confiance à Ignimission

L 14614 - 208 - F: 8,50 € - RD

GATEWATCHER

HIGHLIGHT CYBER THREATS BEFORE THEY DARKEN YOUR BUSINESS

AIONIQ®

AUGMENTED DETECTION

NDR with behavorial and mapping analysis powered by AI

AIONBYTES®

DYNAMIC ANALYSIS

Sandboxing with dedicated and monitored environment

TRACKWATCH®

ENHANCED DETECTION

Intelligent platform to detect and analyze threats and intrusions

LASTINFOSEC®

SMARTER DETECTION

CTI with enriched streams analysis

+ 600
INFRASTRUCTURES PROTECTED

100M
FILES SCANNED PER DAY

+ 20Mrd
EVENTS PROCESSED PER DAY

www.gatewatcher.com

L'INFORMATICIEN www.linformaticien.com

RÉDACTION

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

RÉDACTION : Bertrand Garé (rédacteur en chef) et Guillaume Périssat (chef de rubrique)
avec : Alain Clapaud, Michel Chotard, François Cointe, Victor Miget, et Thierry Thaureaux

SECRÉTAIRE DE RÉDACTION : Boutheïna Saddi

MAQUETTE ET RÉALISATION : Franck Soulier (chef de studio)

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

VENTE AU NUMÉRO

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

ABONNEMENTS

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

Toutes les offres :
www.linformaticien.com/abonnement

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

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

IMPRESSION

Imprimé en France par Imprimerie Chirat (42)
Dépôt légal : 3ème trimestre 2022

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

ISSN 1637-5491

Une publication PCpresse,

GROUPE FICADE

PRÉSIDENT, DIRECTEUR DE LA PUBLICATION :
Gaël Chervet

Le Ransomware ou la Covid de l'IT

Tout comme la Covid-19, le ransomware change de forme et continue de se propager. Pourtant, depuis deux ans, les entreprises sont prévenues et les directions informatiques classent la bête comme la première menace. Dans notre dossier de ce mois, nous faisons le point sur ce petit monde du rançongiciel qui évolue, change de forme et de méthodes pour mieux infecter sa proie et lui soutirer un maximum d'argent en y ajoutant chantage et pressions en tous genres. Mais comment expliquer ce côté endémique du ransomware ? Oui, les attaquants rivalisent d'imagination et d'expertise pour affiner leurs attaques. Mais, depuis le temps, les entreprises ne semblent pas trouver l'antidote, celle de la formation intensive des salariés face à cette menace. Les entreprises n'appliquent pas toujours non plus les simples mesures d'hygiène informatique. Selon un rapport publié par Backblaze en juin dernier, relayé par *Storage Newsletter*, plus de la moitié des entreprises interrogées indiquent avoir eu des pertes de données et 19 % seulement réalisent des sauvegardes quotidiennes. Il serait donc temps de prendre la menace au sérieux et non de jeter des coups de menton. Notre dossier essaie donc d'éclairer ce thème et de vous fournir les informations qui pourraient vous être utiles lors d'une attaque de ce type.

Vous retrouverez bien sûr nos rubriques habituelles avec peut-être un ton un peu plus léger durant cette période estivale. Bonne lecture, et profitez bien de cette période. La rentrée va arriver vite ! □

Bertrand Garé
Rédacteur en Chef

BACK UP AND KEEP CALM

Operate

Secure

Protect

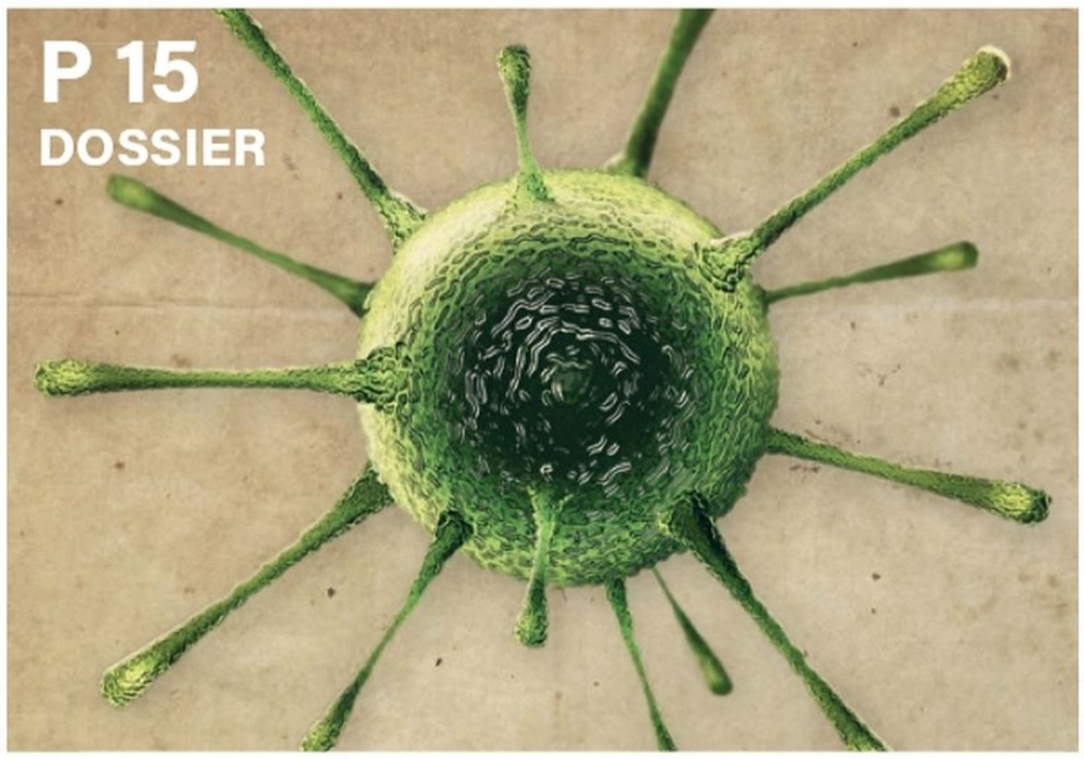
Leader français de la protection des données

ANTEMETA

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

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.



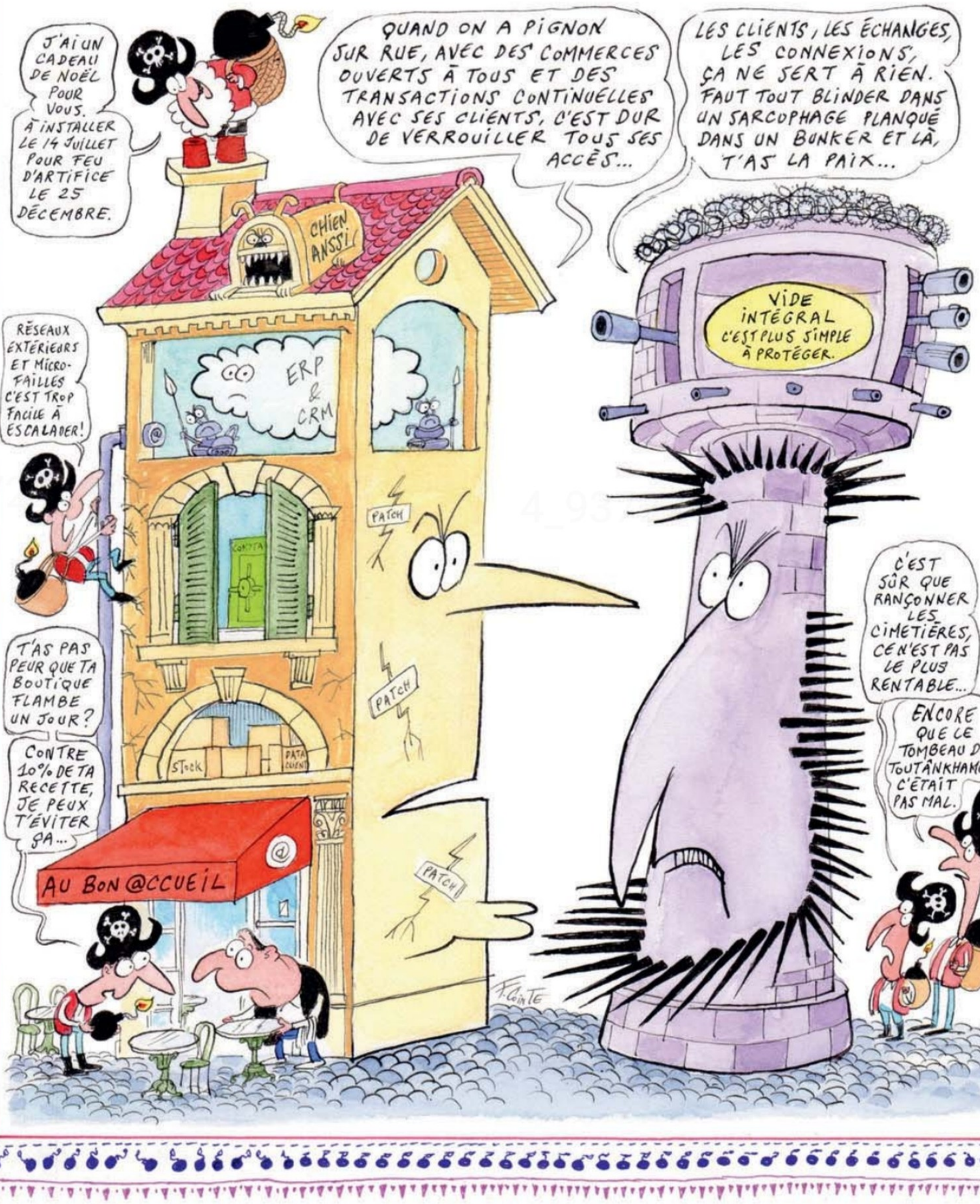
La sophistication
de la simplicité
est un choix
assumé

Simple CRM

from S!MPL

https://crm-pour-pme.fr/go

SE PROTÉGER DES RANSOMWARES...



Google Cloud ouvre sa région France

Attendue de longue date et officialisée en septembre 2021, la région France de Google Cloud vient d'être ouverte. Le géant américain a profité de l'occasion pour présenter S3NS, la co-entreprise créée avec Thalès.

Ce 30 juin, la Maison de la Mutualité à Paris était redécorée aux couleurs de Google Cloud. L'entreprise américaine y a réuni clients, partenaires et journalistes afin d'annoncer officiellement l'ouverture de sa Région France, sa 34ème région. Pour mémoire, Google Cloud est physiquement présent en Allemagne, aux Pays-Bas, en Belgique, en Finlande, au Royaume-Uni et en Suisse, et a très récemment ouvert deux autres régions, du côté de Madrid, en mai, et de Milan, plus tôt, en juin. Cette Région France toute neuve est composée de trois datacenters en colocation en Île-de-France, situés à plus de 10 km les uns des autres, mais Google ne donnera ni le nom de ses hébergeurs, ni la localisation des trois sites.

Une promesse de 2019

Pour mémoire, cette Région France était promise pour, au mieux, fin 2021 ou début 2022. Longtemps après qu'AWS et Azure aient posé leurs valises dans l'hexagone : Amazon y a ouvert une région en 2017, suivie par Microsoft l'année suivante. Du côté de Google Cloud, les clients qui choisiront cette région auront accès à la quasi-totalité des services classiques de Google Cloud, de App Engine à BigQuery en passant par Apigee. À noter que tous les services de l'hyperscaler ne seront pas immédiatement fournis, Franck Zerbib, le Director France Customer Engineer de Google Cloud, précise que leur déploiement sera progressif. Par rapport aux clients français qui ont fait le choix des sites allemands ou belges, Google nous promet une latence divisée par deux. Surtout, cette localisation permet au géant américain d'assurer faire du *« cloud à la française »*. L'entreprise qui, selon un rapport d'Implement Consulting, va générer par ses seuls investissements en infrastructures 490 millions d'euros de PIB et 4600 emplois supplémentaires en France à l'horizon 2027, considère de longue date l'Hexagone comme un marché stratégique, avec une très forte croissance sur l'adoption du cloud en général.

D'où, ce 30 juin, la mise en avant de ses clients, de la startup au grand groupe, de Brut à Carrefour en passant par Akeneo, Leclerc, Décathlon, L'Oréal ou encore Renault. Bref, Google Cloud veut s'adresser à tous et gagner des parts de marché en triomphant des « freins psychologiques », aux dires du patron France de Google Cloud, Anthony Cirot. Le géant compte rassurer les entreprises françaises quant à la

RÉGION FRANCE : ORACLE S'AGRANDIT

Une semaine avant Google Cloud, c'est Oracle qui a annoncé s'étendre en France. Après un premier centre à Marseille, Oracle ouvre une deuxième région dans le tout nouveau centre de données d'Interxion à la Courneuve, en région parisienne. Tous les services d'Oracle Cloud Infrastructure seront à terme disponibles avec une première série de services dès l'ouverture, services Day One, et les autres dans les trois mois à venir. Les partenaires de connectivité disponibles à l'ouverture de la région sont Orange, Colt et Equinix, pour offrir une connectivité dédiée par les liens FastConnect, soit la promesse d'une connexion avec un réseau privé et dédié, ainsi qu'une bande passante plus élevée, une latence plus faible et des performances plus constantes que les connexions Internet publiques.

localisation de leurs données, et insiste sur l'aspect « souverain », qu'il s'agisse du logiciel, parce qu'open source, ou de l'opérationnel (les accès aux sites, à priori interdits aux agents de la NSA). Pour autant, cette Région française de Google Cloud, ce n'est pas le « Cloud de confiance ». Non, pour espérer obtenir la précieuse certification SecNumCloud, l'entreprise américaine s'appuie sur Thalès. Cet événement a été l'occasion pour les deux sociétés de présenter S3NS, la co-entreprise annoncée en octobre 2021.

Cloud de confiance

Cette société, localisée à Paris et de droit français, est majoritairement détenue par Thalès. Autant de points sur lesquels insistent les cadres de Google Cloud France et de Thales. Elle commercialisera la fameuse offre « cloud de confiance » promise en octobre dernier mais, pour le moment, il faut se contenter d'une « offre intermédiaire », baptisée Local Controls with S3NS. Celle-ci doit offrir les performances et les services de Google Cloud, avec des garanties de localisation des données et de sécurité, notamment en termes de clés de chiffrement. *« Il s'agit de gérer les risques liés aux transferts de données hors UE»* souligne Cyprien Falque, le CEO de S3NS. Pour autant, l'offre reste opérée dans les datacenters de Google Cloud, ce qui la prive *de facto* de toute prétention à SecNumCloud. Une offre SecNumCloud est prévue pour le second semestre 2024, quand S3NS aura obtenu le précieux sésame de l'ANSSI. Interrogé sur les risques de ne pas obtenir la certification, Cyprien Falque se dit confiant : *« nous travaillons de manière très étroite avec l'ANSSI pour valider tous les choix que nous faisons »*. Ainsi, cette offre « Trusted Cloud » fera l'objet d'une région dédiée, physiquement distincte de la région France de Google Cloud, *« dans des datacenters séparés »*.

Local Controls with S3NS, pour sa part, est d'ores et déjà disponible, avec six « early adopters » dont l'identité n'a pas été dévoilée. *« Elle est un un chemin pour ceux qui veulent aller vers le SecNumCloud »* ajoute Cyprien Falque. De même, en termes de tarification, l'offre est à mi-chemin entre le tarif de la Région France de Google Cloud et celui de la future offre certifiée SecNumCloud. Pour l'heure, S3NS compte quelques dizaines de salariés et en recrute cette année une centaine, espérant poursuivre la croissance de ses effectifs dans les années à venir. *« Nous sommes très fiers d'accompagner notre partenaire Thales et sa filiale S3NS et sa première offre sur le marché français. Cette collaboration entre nos équipes reflète d'une part une compréhension des attentes liées à la souveraineté numérique, et d'autre part une véritable trajectoire technologique »* écrit dans un communiqué Thomas Kurian, le patron de Google Cloud.

LES FRANÇAIS REMONTÉS

L'annonce de l'ouverture par Google Cloud de sa région France n'a pas manqué de faire réagir les éditeurs et fournisseurs hexagonaux. Une poignée d'entre eux se sont fendus le jour même du lancement d'une tribune assassine dans les Échos. De son côté, David Chassan estime que *« les DSI ne sont pas naïfs. Comment un décideur informatique, qu'il soit en entreprise ayant une activité stratégique ou un acteur public engagé dans la politique Cloud au centre, peut-il considérer ces solutions comme "de confiance". Ces effets d'annonces arrivent à l'heure où de nombreux acteurs technologiques français de très haut niveau soutenaient leurs dossiers à la BPI sur l'appel à manifestation d'intérêt "France 2030" du gouvernement, qui vise à développer une suite bureautique cloud, collaborative et souveraine. »*

LEVÉES DE FONDS

SumUp fait exploser les compteurs

La Fintech SumUp vient de lever 590 millions d'euros auprès de Bain Capital Tech Opportunities, avec la participation de fonds gérés par BlackRock, Btov Partners, Centerbridge, Crestline, Fin Capital et Sentinel Dome Partners. Elle est désormais valorisée 8 milliards d'euros. La startup, qui a démarré comme un service de paiement à destination des petits commerces, veut devenir une « Super App », intégrant un compte et une carte d'entreprise gratuite, ainsi qu'une solution de facturation.

Serie B pour le Français Kaiko

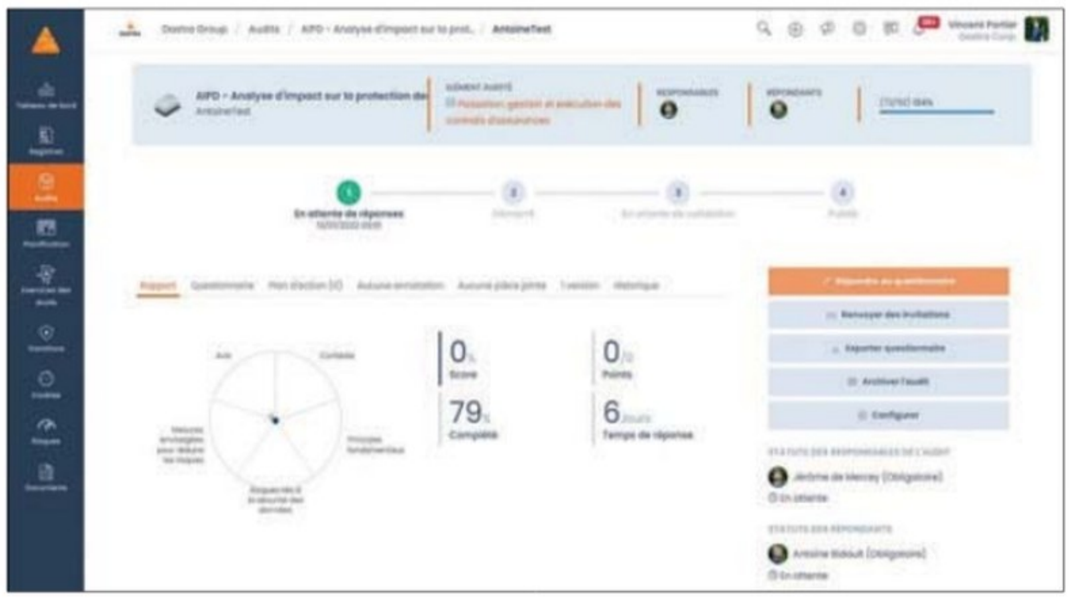
La jeune Fintech spécialisée dans les services de données centralisées et décentralisées sur les actifs numériques réalise sa deuxième levée de fonds, amassant 53 millions de dollars auprès de Revaia, Alven, Point9, Anthemis et Underscore. Cette levée doit permettre à la jeune pousse de consolider sa position de leader du secteur des solutions de données institutionnelles, servant de pont essentiel entre les marchés financiers centralisés et décentralisés.

24 millions d'euros pour l'incubateur lillois EuraTech

Place forte de la French Tech nordiste, l'incubateur EuraTechnologies lève 24 millions d'euros auprès de la Famille Mulliez et de tous les investisseurs historiques d'EuraTechnologies que sont la Métropole Européenne de Lille, la Région Hauts-de-France, la ville de Lille, le Crédit Agricole Nord de France, la Caisse d'Épargne Hauts-de-France et le Crédit Mutuel Nord Europe. L'incubateur compte utiliser ses fonds pour ouvrir 3000 nouveaux postes, investir quelque 10 millions d'euros en équipements technologiques de pointe, dans les secteurs de la cybersécurité, de l'AgTech et de la PropTech et s'exporter dans dix pays d'Europe de l'Est, en ouvrant 10 incubateurs dans diverses universités.

Semperis encaisse 200 millions de dollars

L'éditeur spécialisé dans la protection de l'Active Directory vient de boucler sa Serie C menée par KKR, avec la participation de Ten Eleven Ventures, Paladin Capital Group, Atrium Health Strategic Fund, Tech Pioneers Fund et d'investisseurs existants dont Insight Partners. Avec 200 millions de dollars de plus en caisse, Semperis compte accélérer les recrutements au niveau mondial : Semperis est en effet présent en Amérique du Nord, en Europe, en Israël et dans la région Asie-Pacifique. L'éditeur prévoit notamment d'accroître ses équipes spécialisées en réponse aux incidents.



Le million pour Dastra

L'entreprise née il y a moins de deux ans, vient de lever un million d'euros, auprès de business angels dont Seed4Soft. La jeune pousse propose une solution SaaS de cartographie des processus comprenant des données personnelles et d'automatisation du registre des traitements. Dastra prévoit d'utiliser cet argent frais afin de poursuivre les développements techniques de sa plateforme, ce pourquoi elle compte doubler cette année la taille de son effectif en recrutant 20 personnes. Les fonds seront également mis à contribution pour accélérer son déploiement en Europe.

SAS ajoute le risque financier à son portefeuille

Le vénérable SAS ajoute à son portefeuille de solutions celles de Kamakura Corporation. Cet éditeur américain est spécialisé dans les outils de gestion des risques financiers. Il propose ainsi deux offres. D'un côté Kamakura Risk Manager, une solution de gestion des risques spécialisée dans l'ALM (portefeuilles d'actifs-passifs) comprenant une évaluation complète de la transaction, une simulation, un stress test et une analyse des flux de trésorerie. De l'autre KRIS, pour Kamakura Risk Information Services, une offre SaaS d'agrégation de données et d'évaluation du risque de crédit afin de calculer les probabilités de défaut de paiement sur la base de modèles exclusifs.

Zendesk se vend à bas prix

Sous pression du fonds Jana Partners qui souhaitait un changement radical du conseil d'administration ou la vente de la société, Zendesk a tergiversé en explorant différentes pistes pour finalement essayer de continuer à rester indépendant. L'éditeur espérait une vente aux alentours de 140$ par action mais n'a pas trouvé preneur à ce prix malgré des offres assez proches de ce niveau. La baisse de l'activité a eu pour conséquence de renforcer les pressions et Zendesk vient de se vendre au prix de 77,50 dollars par action en numéraire à un groupe de fonds d'investissement composé de Hellman & Friedman LLC et Permira. Ce prix est loin de la valeur réelle de l'entreprise qui tourne selon les multiples de valorisation autour de 115$. La transaction devrait se clore au cours du quatrième trimestre de cette année.

Twitter accepte **Musk**

Après la proposition d'Elon Musk de racheter le réseau social pour 44 milliards de dollars, puis la suspension de l'opération, la menace de retrait par Elon Musk et autres péripéties, les relations entre Twitter et le fantasque milliardaire s'apaisent un peu. Le CA de l'entreprise approuve finalement l'offre de rachat. Dans un document envoyé à la Securities and Exchange Commission, l'organisme fédéral américain de réglementation et de contrôle des marchés financiers, le CA demande désormais aux actionnaires d'approuver « à l'unanimité l'adoption de l'accord de fusion » lors de la prochaine assemblée générale. Reste à savoir si les actionnaires iront dans le sens du CA. Les relations avec Elon Musk ne sont pas au beau fixe. Les actionnaires accusent le milliardaire de vouloir acquérir le réseau social à moindre coût à grand renfort de manœuvre peu scrupuleuse visant à semer le doute sur la valeur réelle du réseau social.

Microsoft rachète **Miburo**

Microsoft se muscle encore un peu plus en matière de cybersécurité. Le géant de Redmond a annoncé mardi 14 juin, avoir conclu un accord pour acquérir Miburo, une société d'analyse et de recherche spécialisée dans la détection et la réponse aux menaces provenant de pays étrangers. Les équipes de recherche de Miburo détectent et attribuent des campagnes d'influence malveillantes dans 16 langues. Cette nouvelle association doit aider les clients de Microsoft à contrer des cyberattaques étrangères et les opérations d'influence soutenues par des États.

IBM s'offre **Randori**

IBM a annoncé lundi 6 juin, avoir fait l'acquisition du bostonien Randori, *« l'un des principaux fournisseurs de gestion de surface d'attaque (ASM) et de cybersé*curité offensive », comme le décrit un communiqué d'IBM. Le montant de l'opération n'est pas connu. Cette acquisition doit permettre à IBM de progresser dans sa stratégie de cloud hybride et de renforcer son portefeuille de produits et de services cybersécurité.

EasyVista s'empare d'**Itexis**

EasyVista se renforce dans le DEM (Digital Experience Monitoring). L'entreprise française vient d'annoncer mettre la main, pour un montant non divulgué, sur Itexis. Cette société fondée en 2001 fournit une solution de DEM, consistant en des algorithmes qui viennent superviser les applications en temps réel, identifier les problèmes en fonction d'indicateurs clés, sur l'ergonomie ou les performances système par exemple, et les résoudre. Soit une optimisation automatisée de la qualité de service des applications.

SentinelOne et Okta partenaires autour d'une solution commune

SentinelOne lance SentinelOne XDR Response for Okta basé sur l'identité et la réponse à la compromission des informations d'identification.

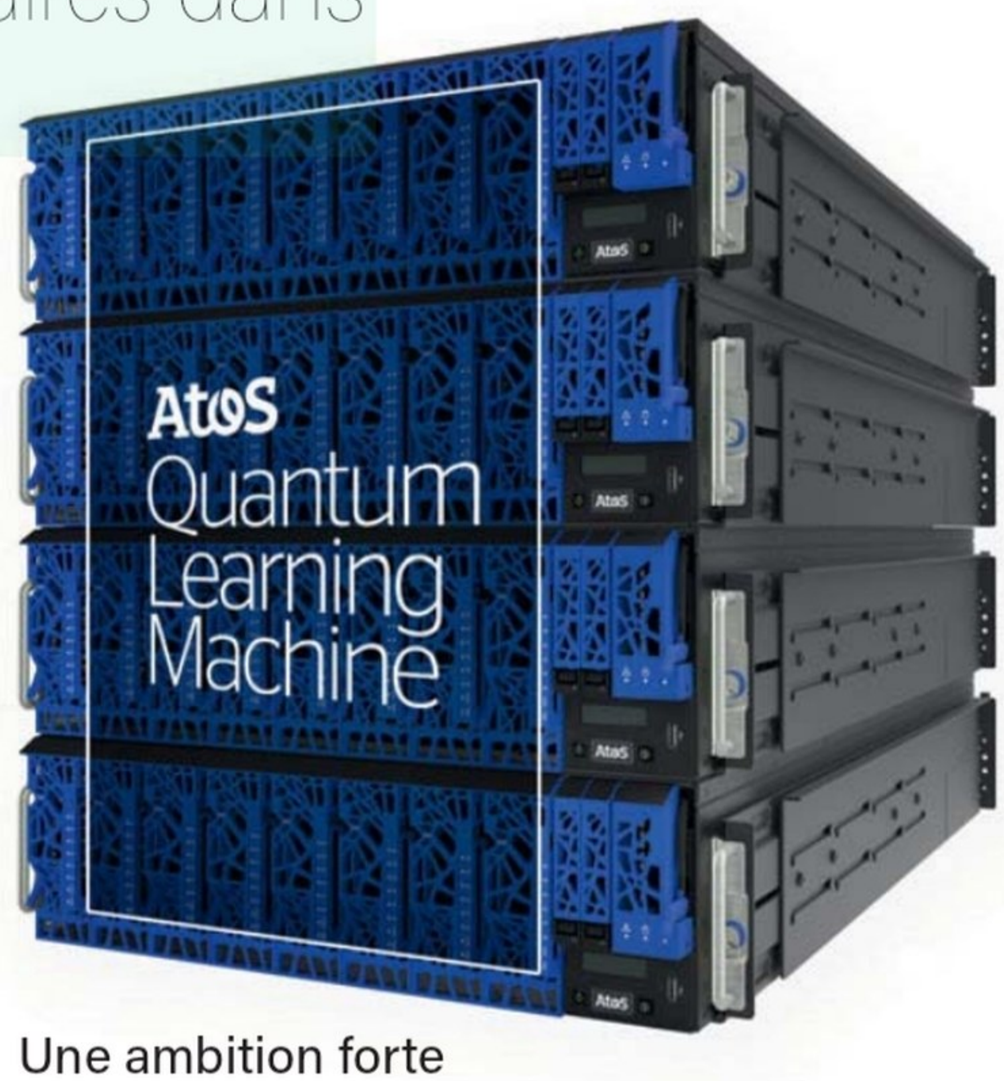
SentinelOne XDR Response for Okta fournit un processus de remédiation entièrement automatisé, allégeant la charge de l'équipe SOC. Elle comprend plusieurs services comme l'enrichissement des données dans Singularity XDR avec des informations de connexion récentes issues d'Okta. La solution peut automatiquement mettre fin aux sessions actives provenant d'appareils compromis afin de minimiser le temps de réponse pour la prévention et la remédiation. Elle peut, de plus, imposer la réinitialisation du mot de passe, empêchant ainsi tout mouvement latéral activé par le SSO dans les applications de l'entreprise et force l'authentification multifactorielle (MFA) dans Okta, verrouillant ainsi le compte jusqu'à ce que l'utilisateur se réauthentifie avec un jeton MFA valide pour vérifier son identité.

Atos et OVHcloud partenaires dans l'informatique quantique

En amont de la conférence France Quantum, Atos et OVHcloud annoncent un partenariat pour la mise à disposition de l'émulateur quantique d'Atos dans le Cloud d'OVHcloud sous la forme de service.

En émulant un environnement quantique réel, le système vise à reproduire différentes approches de calcul quantique. Dotée de la puissance du serveur SMP BullSequana X800, la QLM (Quantum Learning Machine) atteint des capacités d'émulation permettant de couvrir trois modes de programmation quantique différents (le modèle à portes, le modèle annealing et le modèle analogique) ; avec la QLM déployée chez OVHcloud, les utilisateurs pourront émuler des circuits jusqu'à 38 qubits en double précision, et résoudre des problèmes de recuit quantique (quantum annealing) jusqu'à 5000 qubits.

La QLM d'Atos permet de développer des couches logicielles quantiques indépendantes de la plateforme matérielle, en mode programme, annealing et analogique par sa technologie brevetée de compilation quantique. Celle-ci ouvrira également la voie aux premières applications optimisées pour les processeurs de première génération dits NISQ ou Noisy Intermediate-Scale Quantum. OVHcloud sera prochainement en mesure de proposer des solutions de calcul quantique sous forme de Notebook Jupyter, offrant aux développeurs une plus grande simplicité d'accès. Conçu selon des standards libres et ouverts, le Notebook offrira un niveau de performance variable en fonction de l'infrastructure, laquelle bénéficiera des travaux déjà menés par les équipes en charge de l'intelligence artificielle d'OVHcloud.



Une ambition forte

Atos et OVHcloud se donnent pour mission de contribuer au développement d'un écosystème cohérent avec l'ambition de préparer l'arrivée des technologies de calcul quantique. Les acteurs privés et publics de cet écosystème pourront disposer d'un environnement de programmation quantique où qu'ils soient, pour ainsi développer et expérimenter des briques logicielles quantiques « as a service », en amont de la sortie effective des premiers ordinateurs quantiques.

Alliance stratégique entre Deloitte et Netskope

Le cabinet de conseil a signé une alliance stratégique avec le fournisseur de solutions de sécurité zero trust.

Pour aider leurs clients communs à adopter le modèle SASE de sécurité, le cabinet Deloitte et Netskope s'unissent pour proposer la solution Security Service Edge (SSE) de Netskope dans le portefeuille de services de sécurité de Deloitte. Le cabinet va aider les entreprises à évaluer, déployer et intégrer efficacement la solution de Netskope dans leur infrastructure existante. Les clients bénéficieront ainsi de l'architecture particulière de la solution de Netskope qui fournit des fonctions visant à simplifier la sécurité, apporter une visibilité complète sur les échanges en ligne, un contrôle fin des données tout en proposant des solutions de remédiation et des rapports avancés avec des éléments avancés d'analyse.

Okta et Proofpoint partenaires

Okta va intégrer la solution de CASB (Cloud Access Service Broker) de Proofpoint.

Cette nouvelle intégration signifie que la solution CASB de Proofpoint assure désormais la détection et la remédiation des connexions suspectes dans les applications cloud fédérées par trois principaux fournisseurs de solutions d'authentification : Microsoft Active Directory, Okta et Google, couvrant la majorité des applications d'entreprise. Cette intégration vise principalement à protéger les environnements Google Workspace et Microsoft Office 365 par une intégration dans Proofpoint Targeted Attack Protection. Cette solution identifie les personnes les plus vulnérables et les plus souvent attaquées dans les entreprises et partage ses informations avec Okta Identity Cloud et Okta Workflows pour remplir les contrôles d'identité et d'accès nécessaires.

EDF et INRIA accélèrent autour de la transformation énergétique

Les deux acteurs ont renouvelé leur partenariat à l'occasion du salon Viva Technology et ont identifié de nouvelles thématiques de recherche couvrant un large spectre d'enjeux liés au numérique.

Après un premier accord signé en 2016 et qui a déjà permis de collaborer avec une trentaine de projets, EDF et Inria renforcent leur partenariat scientifique et technologique. Les deux entités visent à être à la pointe des techniques mathématiques d'optimisation pour répondre aux grandes problématiques opérationnelles de l'organisation et la gestion des actifs industriels du système électrique comme le management de l'énergie, les plannings, *etc.* Ils travaillent ensemble pour organiser et gérer les systèmes électriques de demain. Ils souhaitent aussi apporter une meilleure maîtrise des techniques de la simulation (physique, IA…) et de la gestion des données. Conjointement, ils vont concevoir et implanter efficacement des jumeaux numériques performants et ouvrir de nouvelles opportunités technologiques par l'hybridation de l'IA et de la simulation…

Vast Data s'allie à Atempo

La solution Universal Storage de Vast Data est maintenant qualifiée avec Miria, la solution de gestion des données d'Atempo.

La solution autorise les clients le transfert des ensembles de données et fichiers entre les sites et les environnements de stockage afin de gérer l'ensemble du cycle de vie des données. Vast Data peut également être utilisée comme cible de sauvegarde pour la protection des données avec Atempo. Pour rappel, Miria utilise des processus hautement parallélisés pour des performances optimales. Entièrement évolutive, Miria permet de sécuriser la migration de milliards de fichiers. L'archivage entièrement automatisé ou dirigé par l'utilisateur final de données plus froides vers n'importe quel stockage (cloud, disque, objet, bande…) est également pris en charge pour les utilisateurs de Vast Data. Miria rend les workflows d'archivage aussi simples qu'un glisser-déposer. La solution indexe les informations en fonction des métadonnées et offre une capacité de recherche améliorée dans les archives à long terme. Que les utilisateurs aient besoin de visualiser ou de restaurer des fichiers archivés, la recherche et la récupération de ces données deviennent simples et rapides. Miria fournit des tableaux de bord riches et complets pour donner aux utilisateurs une vue claire et pertinente de l'utilisation et de la capacité des fichiers stockés sur la solution Vast Data.

AGENDA

Black Hat USA
6-11 août 2022
Mandalay Bay Resort Las Vegas, USA

IFA 2022
2-6 September 2022
Messegelände Berlin ExpoCenter City, Allemagne

Big Data & IA
26 & 27 septembre 2022
Palais des Congrès, PARIS

Mobility For Business
11 & 12 octobre 2022
Parc des Expositions, Porte de Versailles

Solutions ERP
11 & 12 octobre 2022
Parc des Expositions, Porte de Versailles

Solutions Demat
11 & 12 octobre 2022
Parc des Expositions, Porte de Versailles

Solutions CRM
11 & 12 octobre 2022
Parc des Expositions, Porte de Versailles

Solutions BI
11 & 12 octobre 2022
Parc des Expositions, Porte de Versailles

Solutions e-Achats
11 & 12 octobre 2022
Parc des Expositions, Porte de Versailles

Assises de la sécurité
12 au 15 Octobre 2022
Grimaldi Forum, Monaco

Metadays
29 & 30 novembre 2022
Centre de Congrès Rive Montparnasse

Penser que la cyberdéfense est compliquée et coûteuse peut porter atteinte à votre entreprise

BT BLUE

BLUE CYBER, sécurisation et protection des systèmes d'information

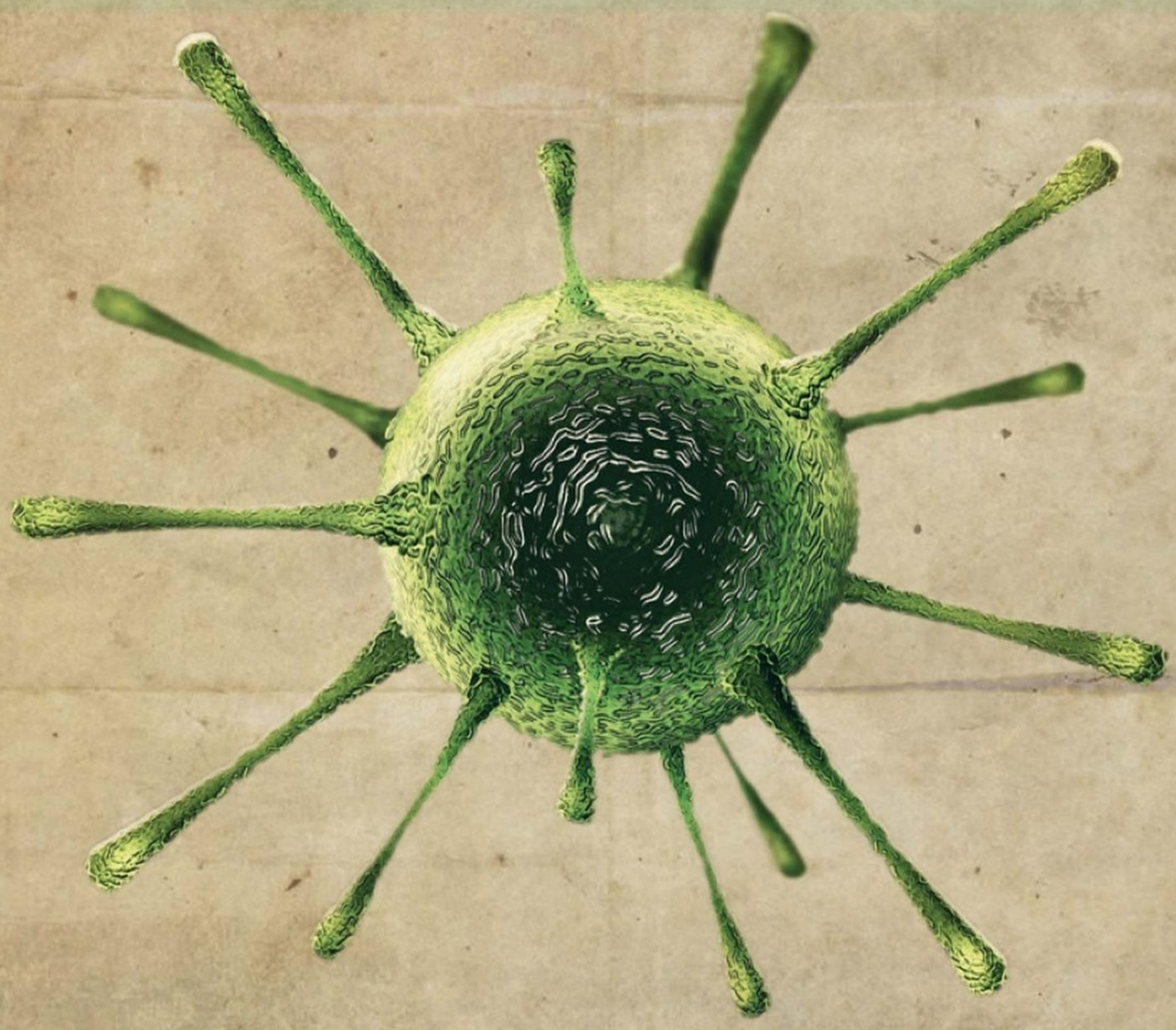
www.cybersecurite.blue // Ligne dédiée 02 30 30 00 00

ISO 27001 Certified Data Center

ITIL FOUNDATION

vmware CLOUD VERIFIED

WANTED RANSOMWARE



ENNEMI PUBLIC N°1

2021 avait été une année catastrophique pour les entreprises sous le feu des attaques de rançongiciel. 2022 est dans la continuité avec déjà un nombre d'attaques de ce type en six mois équivalent à l'ensemble des attaques réalisées l'année dernière. Le phénomène s'amplifie. Point sur la situation et les bonnes pratiques pour éviter d'être la prochaine victime de ce racket à grande échelle !

- *La première menace du moment*
- *Ne payez pas la rançon*
- *Les bonnes pratiques pour se défendre*
- *Backup, le dernier bastion*

La **première menace** du moment

Les ransomwares caracolent en tête des attaques depuis le début de l'année et représentent 17 % des attaques actuelles. Si la prévalence est toujours inquiétante, le nombre de souches et de variants de ces logiciels baisse du fait de l'avènement du RaaS, le ransomware as a Service.

Selon un rapport publié par WithSecure, ex F-Secure, les ransomwares comptent pour 17 % des menaces détectées en 2021 en faisant ainsi la menace la plus prévalente de l'année devant les exploits. Toujours selon ce rapport, WannaCry dominait le classement des rançongiciels recensés devant GrandCrab, REvil, and Phobos. Le rapport pointe, de plus, les différents moyens utilisés par les rançonneurs et la multiplicité des secteurs attaqués. Certains de ces groupes ont annoncé se retirer mais il semblerait *a priori* que cela ne soit qu'un changement de nom de groupes pour se libérer de la pression des forces de police ou pour éviter des conflits avec des utilisateurs de ces RaaS. Ceux-ci touchent entre 70 et 90 % des rançons, mais il a été constaté quelques conflits autour des opérations de paiements entre fournisseurs de ransomwares ou de points d'intrusion et les exécutants des attaques.

Selon une autre étude menée par Tenable, les ransomwares étaient responsables de 38 % des brèches dans les systèmes d'information en 2021. Dans le secteur de la santé, cela représentait plus d'un tiers des attaques menées ou réussies (36,2 %). Dans le secteur de l'éducation, cela représente un peu moins du quart des brèches constatées (24,6 %). Au global, dans un sondage réalisé par Sophos, 66 % des entreprises interrogées indiquaient avoir été attaquées par un rançongiciel.

DE MULTIPLES GROUPES

Conti, REvil, BlackMatter, LockBit.2.0, Hive and ALPHV/BlackCat animent les chroniques et les pages des journaux depuis des semaines avec leurs attaques de rançongiciels. En 2021, le FBI (Federal Bureau of Investigations) américain indiquait suivre plus de 100 groupes de fournisseurs de ransomwares. La plupart sont assez éphémères et ne durent que le temps de certaines opérations d'importance. Ce n'est pas pourtant qu'ils disparaissent. Ils changent de nom ou de forme autour d'un écosystème différent et pour continuer à attirer de nouveaux affiliés. Que ce soit de leur propre volonté ou sous la pression des forces de police qui les poursuit, les groupes évoluent. De nouveaux groupes intègrent les membres d'un autre qui a arrêté ses opérations. Ainsi, REvil est le successeur de GrandCrab et Conti celui de Ryuk. Il devient surtout plus difficile de suivre ces groupes et de connaître leurs modes opératoires et leur écosystème. Les informations sur ces groupes peuvent rapidement devenir obsolètes ou fausses.

```
---=== Welcome. Again. ===---

[-] Whats HapPen? [-]

Your files are encrypted, and currently unavailable. You can check it: all files on
your system has extension 77s9x27u.
By the way, everything is possible to recover (restore), but you need to follow our
instructions. Otherwise, you cant return your data (NEVER).

[+] What guarantees? [+]

Its just a business. We absolutely do not care about you and your deals, except getting
benefits. If we do not do our work and liabilities - nobody will not cooperate with us.
Its not in our interests.
To check the ability of returning files, You should go to our website. There you can
decrypt one file for free. That is our guarantee.
If you will not cooperate with our service - for us, its does not matter. But you will
lose your time and data, cause just we have the private key. In practice - time is much
more valuable than money.

[+] How to get access on website? [+]

You have two ways:
```

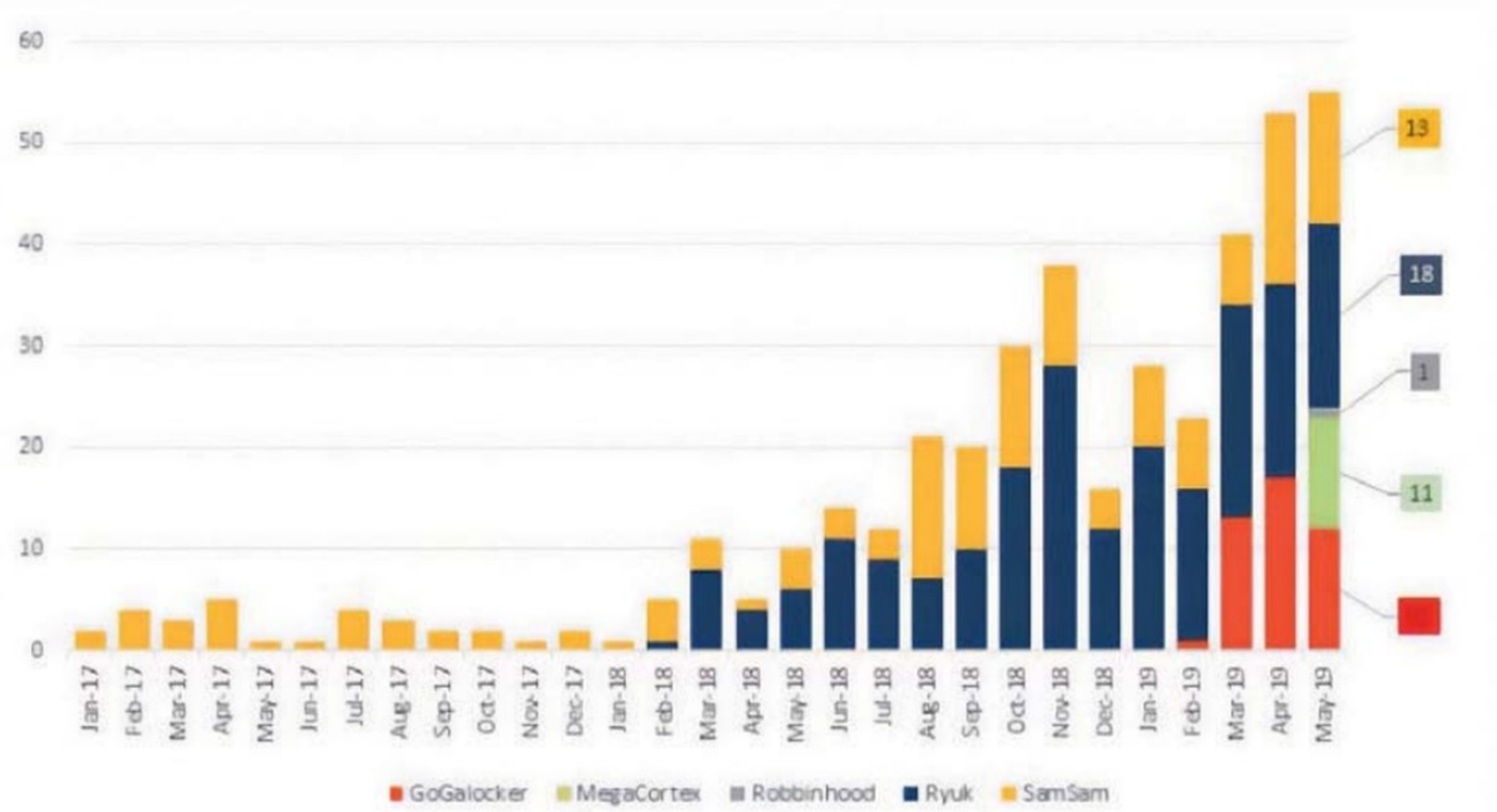
Message de REvil après une attaque réussie.

Le modèle RaaS

À l'image du SaaS (Software as a Service), le RaaS permet à un utilisateur de se procurer un ransomware prêt à l'emploi. Celui-ci comprend le logiciel, l'infrastructure pour mener l'attaque et les exécutants, si nécessaire, pour installer une tête de pont dans l'entreprise ou l'organisation visée (accès initial). Avec ce modèle, les groupes derrière les ransomwares se conduisent comme des industriels des services informatiques avec les « affiliés » ou partenaires pour exécuter les basses

œuvres du groupe. Il semble que ce ne soit que le début d'une industrie qui rapporte énormément. En 2020, les groupes avaient amassé un butin de 692 M$ de leurs attaques.

Le service est « de qualité ». Ainsi les groupes fournissent aux affiliés des playbooks pour perpétrer les attaques mais ils restent libres d'appliquer leurs propres méthodes s'ils le souhaitent. Ils ont ainsi la possibilité de rechercher le moindre point de résistance de leur futur « client » par différents moyens. Le moyen le plus utilisé est le « spear phishing », la campagne de phishing ciblée. Elle se réalise à partir de mail contenant un attachement contaminé ou un lien menant vers un téléchargement discret d'un logiciel pour créer un accès initial et la possibilité de télécharger plus tard d'autres composants afin de mener l'attaque depuis l'intérieur de l'entreprise.



Un tableau issu d'un rapport de l'ANSSI sur l'augmentation du nombre de ransomwares entre 2017 et 2019.

L'attaquant a aussi le loisir de cibler les liens RDP avec de faibles mots de passe en force brute par l'utilisation de mots de passe par défaut ou des attaques par dictionnaires. D'ailleurs, certains se moquent de RDP (Remote Desktop Protocol) accessible publiquement en le renommant Ransomware Deployment Protocol ou Protocole de Déploiement de Ransomare !

Il peut aussi rechercher de mauvaises configurations ou des vulnérabilités. La plupart des attaques s'appuient sur des failles connues et non patchées. De plus, s'il a les moyens, il peut acheter directement les accès initiaux auprès des partenaires du groupe de ransomware.

Double, triple extorsion

Au-delà du simple chiffrement des données de l'entreprise, les pirates des groupes ont trouvé un moyen très efficace de faire payer la rançon aux entreprises : la menace de publier les données sensibles de l'entreprise sur Internet au vu et au su de tous, ce qui peut être très embarrassant dans certains cas. Cette menace sert aussi à mettre la pression sur les entreprises en ne publiant sur les sites du dark web qu'un échantillon des données. En ce cas, le mal est fait et la réputation de l'entreprise est de toute façon entachée. Certains groupes, comme REvil, le successeur de GrandCrab, ont aussi utilisé des appels téléphoniques vers les médias et les partenaires commerciaux de l'entreprise victime. Le groupe a d'ailleurs mis en place ce service gratuitement pour ceux qui utilisent son RaaS. Plus prosaïquement, la pression peut aussi se réaliser par des attaques de déni de services distribuées. Dans le modèle de la triple extorsion, le groupe de ransomware demande aussi des rançons aux partenaires ou clients de la société victime. Certains groupes vont même jusqu'à menacer les entreprises d'utiliser des logiciels pour effacer toutes les données si la rançon n'est pas payée rapidement ou sous un certain délai. Cette dernière menace est de plus en plus utilisée et les groupes n'hésitent pas à passer à l'acte si nécessaire. □

B.G

LA SANTÉ EST UNE CIBLE PRIVILÉGIÉE

La révélation de la fuite d'un million de comptes Ameli sur le dark web remet au cœur des interrogations les attaques sur le secteur de la santé. Selon une étude réalisée par Sophos, les attaques de ransomware sur le secteur de la santé ont augmenté de 94 % en 2021. 66 % des établissements de santé ont été touchés, contre 34 % l'année précédente. 99 % des victimes du secteur ont pu récupérer au moins une partie de leurs données chiffrées au cours d'une cyberattaque. Les établissements de santé présentent le deuxième coût moyen de récupération le plus élevé (1,85 million de dollars), mettant en moyenne une semaine pour se remettre d'une attaque de ransomware. 67% des établissements pensent que les cyberattaques deviennent plus complexes, d'après leur expérience des évolutions observées l'an passé. Il s'agit du secteur affichant le plus fort pourcentage dans ce domaine. Si les établissements de santé sont les plus nombreux à payer la rançon (61 % d'entre eux), ils versent les montants les moins élevés en moyenne (197 000 dollars), comparés à la moyenne générale de 812 000 dollars, tous secteurs confondus. Parmi ceux qui ont cédé au chantage, seuls 2 % ont récupéré la totalité de leurs données. 61 % des attaques ont abouti au chiffrement de données, une proportion inférieure de 4 points à la moyenne globale (65 %).

Rançon : ne payez pas !

Les ransomwares ne vont pas désarmer demain mais si vous en êtes victimes, payer la rançon n'est pas forcément la bonne solution. Ceux-ci sont en augmentation constante et seul un faible pourcentage des victimes ont pu récupérer l'ensemble de leurs données.

Selon un rapport très récent de l'Unité 42, le laboratoire de recherche de Palo Alto, les attaques par ransomware continuent leur flux tendu et 21 nouveaux groupes ont été détectés. Les rançons demandées augmentent. En 2020, les demandes de rançons s'établissaient à un peu plus de 118000 $. En 2021, les demandes moyennes étaient de 1,78 million de dollars avec une demande minimale constatée de 50 000$. L'année dernière, la plus forte demande a été de 3 M$. La plupart du temps, après négociations, les groupes ne reçoivent qu'une partie de la rançon demandée. Généralement, les victimes paient un peu plus de 42% de la rançon demandée. En moyenne, les entreprises lâchent 952 162 $ en 2021 en augmentation de 71% sur l'année précédente. 58% des entreprises paient la rançon. Un rapport réalisé pour le compte de la société Veeam, spécialisée dans la sauvegarde des données, estime que 76% des entreprises reconnaissent avoir payé la rançon. Le rapport de Unit 42 précise que 14% des entreprises indiquent avoir payé plusieurs fois, en tout cas, plus d'une fois. Ce point est confirmé par un autre rapport de Proofpoint qui conclut que 58% des organisations infectées par un ransomware ont payé une rançon aux cybercriminels pour obtenir la clé de déchiffrement. Et dans de nombreux cas, elles ont payé plus d'une fois. Une autre étude d'Anozr Way estime l'impact économique des attaques pour notre pays à 660 M€ de perte de chiffre d'affaires cumulée.

En mars dernier, une étude pour ExtraHop, un fournisseur de solutions de cybersécurité, indiquait que 78% des entreprises françaises reconnaissent en avoir subi au moins une et 68% avoir connu plusieurs incidents au cours des cinq dernières années. 69% des participants admettent avoir déjà versé une rançon, tandis que 36% des entreprises victimes d'une attaque par ransomware déclarent avoir payé la somme demandée dans la plupart ou la totalité des cas. En outre, les victimes de ransomwares font état d'autres préjudices, parmi lesquels une interruption de l'activité (45%) ou du travail des utilisateurs (40%) ou encore une perte de propriété intellectuelle et une atteinte à leur image de marque (41%).

Pas certain de récupérer les données

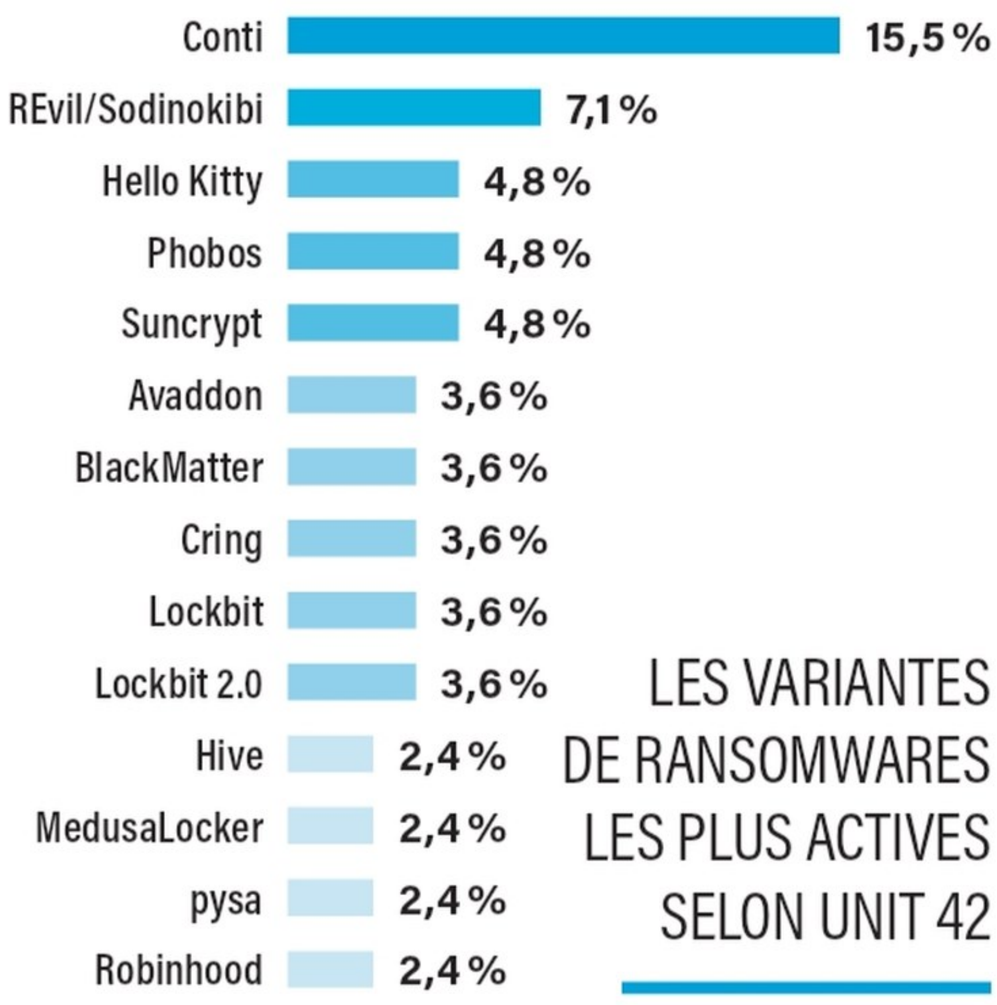
Sur les 76% qui reconnaissent avoir payé la rançon dans l'étude réalisée pour Veeam, 52% ayant cédé au chantage, ont pu récupérer leurs données, 24% n'y sont malheureusement pas parvenues, ce qui signifie que, dans un cas sur trois, le versement de la rançon ne permet pas de retrouver ses données. Il est à noter que 19% des entreprises n'ont pas eu à payer, car elles ont pu restaurer leurs sauvegardes. C'est précisément l'objectif de 81% des victimes de cyberattaques. Les participants à l'enquête indiquent que 94% des auteurs d'attaques ont tenté de détruire des répertoires de sauvegarde et que, dans 72% des cas, ils sont arrivés à leurs fins au moins en partie.

Selon une autre étude de Venafi, plus d'un tiers (35%) des victimes a payé la rançon, mais n'a pas pu pour autant récupérer ses données. Cybereason constate que, parmi ceux qui ont mis la main au porte-monnaie, seuls 51% ont pu totalement retrouver leurs données. 3% n'ont rien pu récupérer, et 46% se sont retrouvés avec des données partiellement altérées. 80% des entreprises ayant payé, ont été frappées par une seconde attaque dans la foulée. Et dans 46% des cas, il s'agissait du même ransomware.

Payer deux fois ?

De plus, payer la rançon augmente le coût de remise en fonction du système d'information. Outre la rançon, il convient de prendre en compte les pertes d'exploitation engendrées par l'attaque. Les conséquences sur la marque sont plus difficiles à évaluer, sans oublier le temps et les coûts pour le service informatique afin de remettre le système en route. Il est nécessaire de prévoir les conséquences sur le respect de la conformité et les amendes ou frais légaux possibles. Payer l'amende n'est donc pas la fin de l'affaire. L'étude de Unit 42 démontre que 41% des entreprises mettent plus d'un mois à revenir à la normale. 9% mettent plus de cinq à six mois ! □

B.G



LES VARIANTES DE RANSOMWARES LES PLUS ACTIVES SELON UNIT 42

Backup et restauration

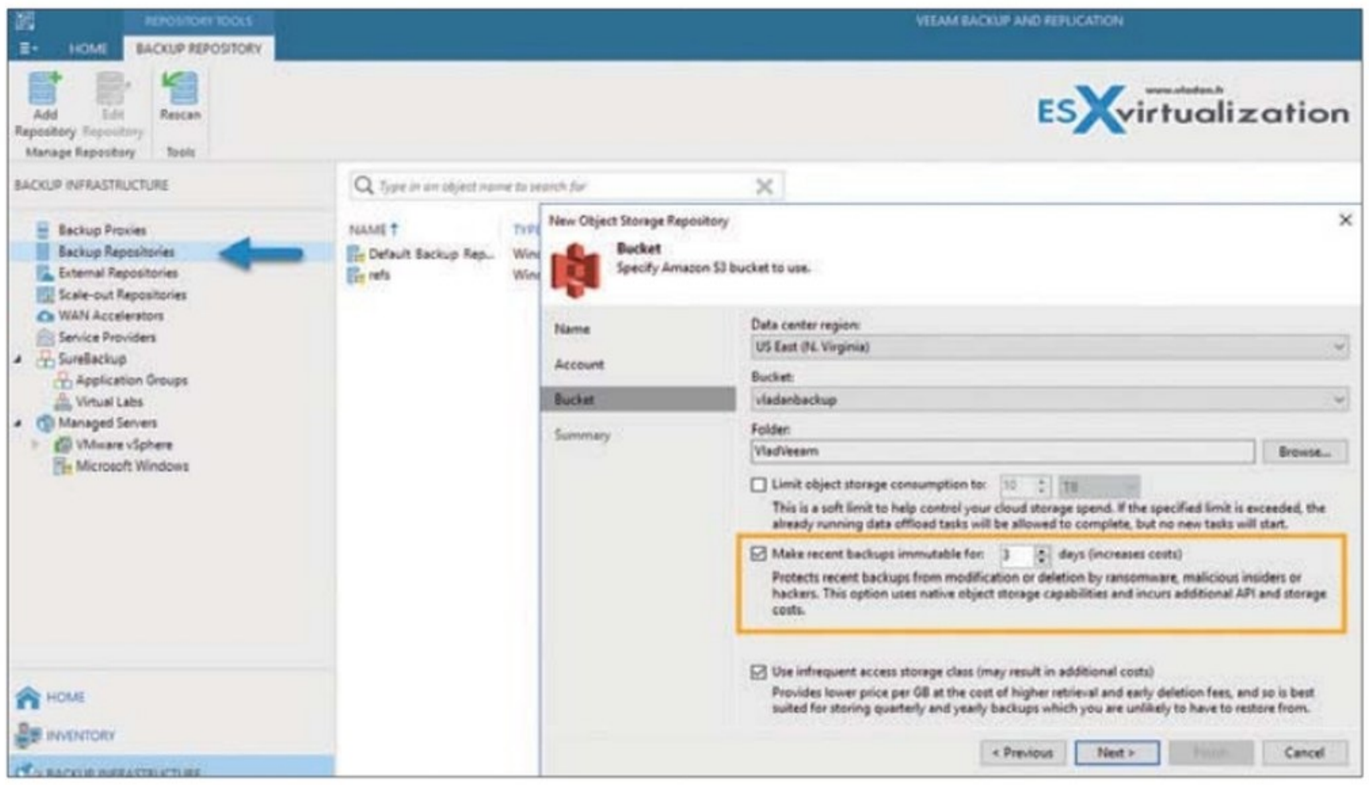
Le dernier bastion

Quand tout est perdu, il ne reste qu'une seule solution : la sauvegarde. Encore faut-il qu'elle soit disponible et sûre pour restaurer les données et reprendre un cours normal de l'activité.

Dans son rapport sur les tendances des ransomwares, Veeam, éditeur spécialisé dans la gestion des données et les opérations de protection de celles-ci, note que 19 % des entreprises n'ont pas eu à payer de rançon, car elles ont pu restaurer leurs sauvegardes. Les participants à l'enquête indiquent que 94 % des auteurs d'attaques ont tenté de détruire des répertoires de sauvegarde et que, dans 72 % des cas, ils sont arrivés à leurs fins au moins en partie. Cette stratégie consistant à éliminer la bouée de sauvetage d'une entreprise est répandue lors des attaques, car elle augmente la probabilité que les victimes n'aient d'autre choix que de payer la rançon.

Immutabilité des données

Le seul moyen de se prémunir de ce scénario est de disposer d'au minimum un niveau de protection immuable ou en mode « Air Gap » (isolé physiquement du réseau), ce qui est aujourd'hui le cas de 95 % des entreprises interrogées. De fait, nombre d'entre elles déclarent que leur stratégie de sauvegarde sur disque, dans le cloud et sur bande, comporte plusieurs niveaux d'immuabilité ou de protection Air Gap. Une équipe informatique sur six (16 %) automatise la validation et la récupérabilité de ses sauvegardes pour s'assurer proactivement de la capacité à restaurer ses serveurs. Ensuite, pendant la phase de remédiation d'une attaque de ransomware, 46 % des participants à l'étude font appel à une « sandbox » ou à un espace de test isolé afin de vérifier l'intégrité des données restaurées avant de remettre les systèmes en production. 81 % des participants pensent que les stratégies de leur entreprise en matière de cybersécurité et de continuité d'activité ou de reprise après sinistre sont en phase. Cependant, 52 % d'entre eux jugent nécessaire d'améliorer les interactions entre les équipes respectives dans ces domaines. La quasi-totalité (95 %) des entreprises dispose d'au moins un niveau de protection immuable ou en mode Air Gap pour leurs données, 74 % utilisent des répertoires cloud assurant l'immuabilité, 67 % des disques sur site immuables ou verrouillables, et 22 % des bandes en mode Air Gap. Les entreprises indiquent qu'en dehors des disques, elles stockent encore 45 % de leurs données de production sur bandes, qu'elles soient immuables ou pas, et 62 % recourent au cloud, à un stade ou un autre du cycle de vie de leurs données.



L'écran de la solution Veeam et la possiblité de rendre immutables les données.

Une fonction indispensable

La plupart des solutions de sauvegarde sur le marché se sont dotées de telles fonctions pour assurer la possibilité de restaurer les données après une attaque de rançongiciel. On ne détaillera pas ici les différences des solutions présentes sur le marché mais les éditeurs du secteur mettent en avant ces possibilités auprès de leurs clients et communiquent beaucoup sur ce point. Certains, comme Rubrik, vont même jusqu'à garantir par contrat la restauration des données. Les clients utilisant le service Rubrik Cloud Vault, service de coffre-fort dans le cloud entièrement géré, sécurisé et isolé construit sur Microsoft Azure, peuvent maintenant bénéficier de sa garantie de récupération des données en cas d'attaque, couvrant jusqu'à 5 millions de dollars de frais liés à la récupération, dans le cas où Rubrik serait incapable de récupérer les données sécurisées.

La restauration pourrait s'effectuer de manière très rapide afin de diminuer les temps d'indisponibilité. Si plusieurs offreurs indiquent des temps de restauration minimaux allant de quelques minutes à maximum quelques heures, il convient cependant de tester la réalité de ce qui est annoncé dans le contexte de l'entreprise. □

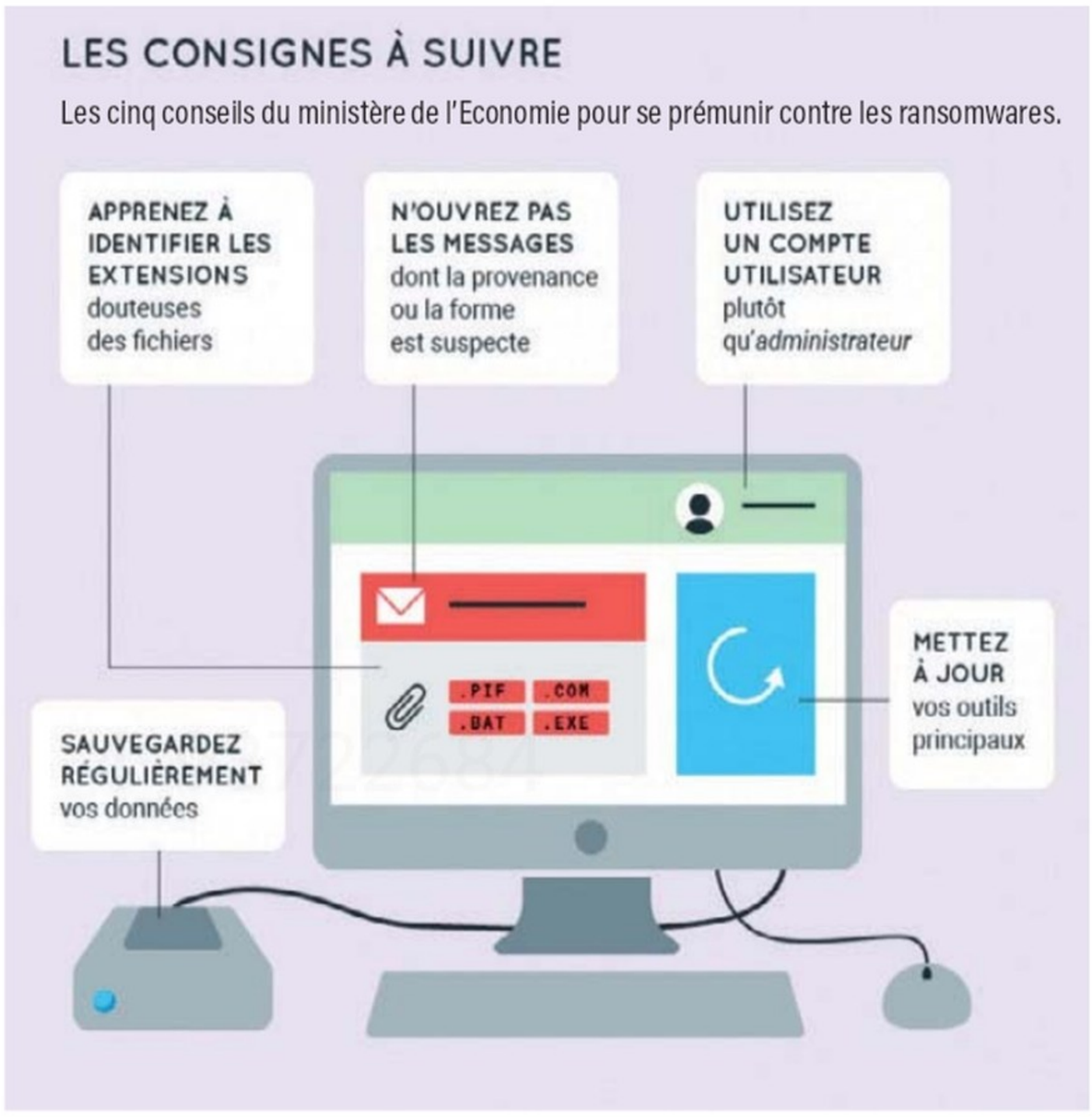
B.G

Revenir aux fondamentaux

Les principes de base contre les rançongiciels

Si le ransomware est devenu la première menace, il peut remercier les lacunes de la sécurité informatique des organisations. Pourtant, quelques principes basiques permettent de réduire le risque.

Correctifs non appliqués, droits d'accès inappropriés, ports ouverts aux quatre vents, réseaux non segmentés, manque de compétences et de connaissances des utilisateurs, mais aussi des administrateurs... Les raisons expliquant pourquoi les ransomwares font mouche sont pléthoriques. Pourtant, la grande majorité de ces facteurs de risques peuvent être aisément évités. D'abord côté utilisateur. *« La prévention sera toujours la première ligne de défense contre toute menace »* souligne John Shier, Senior Security Advisor chez Sophos. Benoît Grunenwald, Expert Cybersécurité chez Eset, abonde en ce sens : *« nous pensons qu'il faut se concentrer sur la prévention et l'automatisme. Bien entendu, cela passe par une bonne hygiène informatique, des utilisateurs sensibilisés »*. Le ministère français de l'Économie énumère cinq conseils pour se prémunir des ransomwares. Au premier rang de ces recommandations, on trouve, sans surprise, une injonction à sauvegarder ses données, un point abordé dans ce dossier.



John Shier,
Senior Security Advisor chez Sophos.

« La première étape consiste à instrumenter l'ensemble de votre organisation afin de disposer d'une visibilité maximale. Vous ne pouvez pas arrêter ce que vous ne pouvez pas voir. »

Hygiène informatique

Les deux préconisations suivantes concernent, là encore sans grande surprise, les mails. *« N'ouvrez pas les messages dont la provenance ou la forme est douteuse »* nous dit Bercy. Ou comment reconnaître un mail de phishing. Moult acteurs dans le secteur de la cybersécurité fournissent des formations et des campagnes de test sur le sujet, tandis que cybermalveillance.gouv et l'ANSSI mettent à disposition sur leurs sites des ressources pour identifier des courriels malveillants. *« Apprenez à identifier les extensions douteuses des fichiers »* ajoute le ministère. Un .exe devrait logiquement apparaître comme suspect, à l'instar d'un .scr ou .bat. *« Les pirates comptent sur le dilemme qui consiste à ne pas ouvrir un document avant d'être sûr qu'il soit légitime, mais comment le savoir si on ne l'ouvre pas... »* nous apprend Sophos. Et quand bien même l'extension est légitime, un .doc ou .xls par exemple, n'activez pas les macros. Si Microsoft ne permet plus leur exécution automatique, il est fréquent que les programmes malveillants parviennent à persuader l'utilisateur de les activer, entraînant alors la propagation du ransomware.

Il s'agit là de principes fondamentaux de l'hygiène, mais trop souvent négligés ou oubliés. Un problème d'autant plus aggravé que l'utilisateur est généralement seul devant son écran et peu au fait des processus à déclencher en cas de suspicion… si du moins ces processus existent. En effet, au niveau organisationnel, la cybersécurité est encore perçue comme une gêne et une cause de baisse de la productivité. Et pour cause ! Il est encore bien plus simple et rapide de recevoir des documents avec macros par mail que de réserver l'usage des tâches automatisées à quelques services, après vérification du destinataire et de la légitimité du fichier envoyé. Cette philosophie entrave bien souvent la bonne mise en œuvre des mesures de sécurité adéquates. *« Une solide culture de la sécurité est primordiale dans l'environnement actuel des menaces. La culture de la sécurité va au-delà de la sensibilisation. Elle façonne les comportements dans tous les domaines de l'entreprise et aide chacun à prendre des décisions judicieuses qui sont alignées sur les priorités de l'entreprise en matière de sécurité »* soutient John Shier. *« Une solide culture de la sécurité constitue une deuxième ligne de défense contre des menaces telles que les attaques par ingénierie sociale. L'instauration d'une solide culture de la sécurité au sein de l'organisation permettra de s'assurer que chacun, du PDG au quai de chargement, sait pourquoi la cybersécurité est essentielle à l'entreprise et comment signaler les incidents »*.

Détecter pour prévenir et réagir

Mais ne jetons pas la pierre aux seuls utilisateurs. Si le phishing reste le principal vecteur d'attaque, les accès RDP mal sécurisés et les applications et systèmes vulnérables figurent en bonne place dans la liste des portes d'entrée préférées des attaquants. On ne rappellera jamais trop qu'il est indispensable de maintenir ses systèmes informatiques à jour et d'appliquer les correctifs le plus rapidement possible. De même, il faut veiller à ce que les mécanismes de sécurité soient correctement configurés, que les ressources du ou des réseaux soient segmentés (évitons de mettre serveurs et postes de travail sur un seul et même réseau)… Et, puisque le risque zéro n'existe pas, les droits d'accès doivent être limités au strict nécessaire. Pas besoin d'un compte admin pour naviguer sur le web ou éditer un document. Ça n'empêchera pas l'attaquant d'entrer, mais une bonne gestion des privilèges et des accès réduira sa marge de manœuvre pour escalader en privilèges ou latéraliser. Enfin, que ce soit pour prévenir ou pour réagir, EDR, NDR, EPP et autres acronymes barbares vont permettre d'observer les événements et comportements suspects. Pour le Senior Security Advisor de Sophos, *« la première étape consiste à instrumenter l'ensemble de votre organisation afin de disposer d'une visibilité maximale. Vous ne pouvez pas arrêter ce que vous ne pouvez pas voir »*.

« Depuis 30 ans, nous déployons nos agents multicouches et multi-environnements sur les terminaux, mais pas uniquement : les tenant 365, les serveurs de messageries, les outils collaboratifs, les smartphones… ils servent à filtrer les éléments suspects les plus grossiers, parfois et encore ceux qui fonctionnent malgré tout : hameçonnage, url malveillante notoire, fichiers malveillants » explique Benoît Grunenwald. *« Il faut aussi lever le doute, c'est-à-dire transformer l'alerte en incident.*

Benoît Grunemwald,
Expert Cybersécurité chez Eset.

> *« Il faut aussi lever le doute, c'est-à-dire transformer l'alerte en incident. »*

L'avantage des agents autonomes est justement leur capacité à fonctionner grâce aux données issues de nos laboratoires sans nécessiter d'actions locales. Ainsi, on confie à un tiers une partie de sa protection. Mais face aux attaques plus poussées, il faut y ajouter d'autres capteurs, notamment EDR pour l'analyse comportementale ». Suit toute la partie enquête afin de détecter si les événements suspects portent les marqueurs d'une attaque en cours, sans négliger d'assurer le suivi des menaces bloquées. Car, même contrée, une menace peut indiquer qu'un attaquant est actif et teste vos défenses, voire s'il a déjà infiltré votre SI et tente de se mouvoir latéralement.

Plan de gestion de crise

Cependant, malgré les précautions basiques, malgré la sensibilisation, malgré les solutions de sécurité en place, un ransomware peut encore passer entre les mailles du filet et lancer sa sinistre charge utile. L'organisation affectée doit alors passer en mode gestion de crise, ce qui implique accessoirement d'avoir, en amont, préparé une stratégie pour faire face au pire. *« Il faut monter une cellule de crise qui appliquera les procédures prédéfinies, notamment isolation des postes concernés et collecte des IOCs (indices de compromissions). Ensuite il faut déterminer l'ampleur de la contamination, celle-ci peut être étendue à l'ensemble du SI »* indique Benoît Grunenwald. Selon John Shier, *« la clé d'un bon plan de récupération est de définir clairement ce qui doit être impliqué, quelles actions doivent être entreprises et dans quel ordre »*. S'il existe des cabinets de conseil spécialisés en gestion de crise, ils ne sont pas à la portée (financière) de la première PME venue. Les OIV, les entreprises et les administrations stratégiques ont l'ANSSI, les TPE-PME ont cybermalveillance.gouv et les ETI et collectivités de taille intermédiaire auront très prochainement les CSIRT régionaux. Le tout se conjugue avec les acteurs privés de la cybersécurité. *« Le plan sera spécifique à une infection par ransomware et ne concernera que l'organisation touchée. Disposer d'un plan qui peut être activé en cas d'urgence améliorera considérablement vos chances de neutraliser rapidement une menace et de vous remettre d'une attaque. Il est important de noter que, dans le cas d'un ransomware, votre plan doit être hors ligne afin que vous puissiez y accéder même si tous les fichiers de votre organisation sont cryptés »* conclut John Shier. □

Guillaume Périssat

HarfangLab
Deep Integrity | Paramount Security

HarfangLab EDR
Souverain
Certifié
Offert*

VISA DE SÉCURITÉ

ANSSI

*Le seul EDR certifié par l'ANSSI, offert pendant 3 mois !

Pour en profiter, scannez ce QR code et remplissez le formulaire de demande lié

HarfangLab | EDR

- + 25 ans d'expérience en cybersécurité auprès du ministère des armées, de l'ANSSI et de grandes entreprises de cybersécurité.
- Déploiement Cloud ou On-Premises.
- Agents déployés sur les postes de travail et serveurs.
- Moteur d'intelligence artificielle basé sur l'analyse comportementale.
- API ouverte pour s'intégrer aux autres solutions de sécurité.
- HarfangLab EDR a été sélectionné par Safran, Nexter, Thalès et le ministère des armées.
- **EDR souverain certifié par l'ANSSI.**

La souveraineté n'a jamais été aussi importante.

Les tensions internationales actuelles provoquent une accélération des opérations cybercriminelles.

Pour y faire face, L'**ANSSI** recommande fortement d'accroitre la supervision de sécurité et de s'équiper d'un **EDR**.

Dans une démarche de solidarité et pour aider les organisations à s'équiper, **HarfangLab** met à disposition son **EDR** souverain certifié par l'**ANSSI** gratuitement pendant 3 mois.

CYBERSECURITY™
MADE IN EUROPE

www.**HarfangLab**.io

Métavers rime avec riche ?

par Bertrand Garé

Depuis des mois, le métavers agite les pensées, chroniques et débats. Certains pensent que cela n'est qu'un phénomène de mode qui ne durera pas, d'autres y voient la prochaine évolution d'Internet. D'après les résultats de différentes études, seulement 35% des Français déclarent voir de quoi il s'agit, dont 14% *« précisément »*. Ces derniers sont très forts puisque même les créateurs de métavers ne savent pas vraiment ce qu'il est et ce qu'il sera dans quelque temps. Les plus jeunes montrent ainsi une meilleure connaissance du sujet (42% des 18-24 ans voient ce qu'est le métavers, contre 28% des 65 ans et plus), tout comme les catégories socio-professionnelles supérieures (59% des diplômés du supérieur contre 27% des personnes sans diplômes). Le métavers est souvent peu apprécié. 21% le juge inutile dans ses applications. 5% des Français associent le métavers à un moyen de contourner les restrictions sanitaires. Il suscite même la crainte chez certains (75%). Huit sur dix estiment qu'un monde virtuel ne permettrait pas de réduire les émissions de carbone du monde réel. Moins d'un sur dix (8%) envisage de créer son double numérique. Tous ces chiffres sont issus d'une étude réalisée par l'IFOP en début d'année.

Seuls 12 % pensent que le métavers sera bénéfique pour la société dans une autre étude réalisée par Digital Frontier 4.0, commissionnée par VMware, auprès de YouGov, sur la base d'un échantillon de 1024 personnes en France. 24 % pensent que le métavers n'est qu'un effet de mode qui n'apportera rien. 34 % des Français préféreraient effectivement que le métavers soit géré ou encadré par une institution publique plutôt que par des entreprises. Seuls 16 % sont contre cette idée.

Comme au début d'Internet

Toutes ces remarques et dénégations sur l'intérêt du Métavers me rappellent des temps anciens ver le milieu des années 90 du siècle dernier, lorsque l'utilisation d'un modem était nécessaire pour envoyer et recevoir fichiers et mails avec le plus souvent des échanges limités à 59 minutes et 59 secondes avec un bruit très caractéristique dont les plus vieux se souviennent encore ! Dans ces années du Minitel roi, en France en tout cas, comme l'indique un article de Slate de 2017, France 2 raconte comment il est possible d'apprendre à construire soi-même sa bombe sur Internet, un réseau que « personne ne contrôle ». Un plan d'un reportage montre un exemplaire de La Revue des directeurs administratifs financiers titrant sobrement : *« Internet : le réseau de tous les dangers ? »* Un an plus tard, France 3 évoque rapidement un réseau de pédophilie démantelé sur Internet. Quelques mois après, France 2 reparle de l'utilisation du réseau par les terroristes, dont les pays du G8 doivent se préoccuper. Dans le même article, Laurent Chemla, le fondateur de Gandi, raconte qu'en 1995, la première fois qu'une émission de télé parle d'Internet, elle le décrit comme *« un repaire de pirates, un repaire de néo-nazis, un repaire de pédophiles »*. Dans le même temps, l'opérateur téléphonique de l'époque freine des deux pieds pour maintenir ses 14 000 services Minitel et fait feu de tout bois pour limiter l'implantation d'Internet. Face à ce déluge de messages négatifs, la population n'est guère incitée à se lancer sur le réseau des réseaux et il faudra attendre l'arrivée de l'ADSL pour qu'Internet décolle dans notre pays, soit dix ans plus tard.

Des premières tentatives intéressantes

Et pourtant, le métavers représente à présent un marché en pleine croissance évalué à 800 milliards de dollars d'ici 2024. De nombreuses entreprises se lancent déjà et dans de nombreux secteurs d'activité différents. Depuis le début de l'année 2022, plus de 120 milliards de dollars ont déjà été investis dans ce champ par des fonds et des entreprises comme Meta, Nvidia ou Microsoft.

« D'après McKinsey, le métavers sera à terme composé d'une multiplicité de plateformes compatibles entre elles, et où des milliers d'internautes interagiront en temps réel. Cette transformation sera lente, mais elle est portée par des avancées technologiques comme la 5G, l'Edge Computing, et davantage de simplicité dans la prise en main des outils de création 3D, qui remplaceront demain ceux dédiés au développement de sites web et applications mobiles » indique un article du Figaro.

Que ce soit pour des tests ou pour lancer une empreinte dans ces nouveaux mondes, des entreprises avancent. JP Morgan a été la première à ouvrir une implantation, à publier un dossier de cadrage sur le métavers et à définir une stratégie. Un agent général AXA a ouvert une agence sur Gather qui reproduit son agence physique. Caixa Bank a lancé une banque digitale, Imagin, centrée sur les jeunes (non forcément clients) et leurs styles de vie. Hôtellerie et tourisme explorent aussi ce nouveau terrain, tout comme l'éducation, les RH, l'immobilier…

Des freins clairement identifiés

Les freins sont aujourd'hui de plusieurs ordres. Certains sont fondés d'autres sont plus fallacieux. Ainsi, le plus important peut être, on ne peut passer plusieurs heures avec un casque de réalité virtuelle sur le nez. Exact ! Mais déjà des start-ups proposent des lentilles connectées pour aller sur le métavers. Il est fort possible que l'on assiste au grand retour des lunettes connectées pour alléger cette contrainte afin de vivre cette expérience.

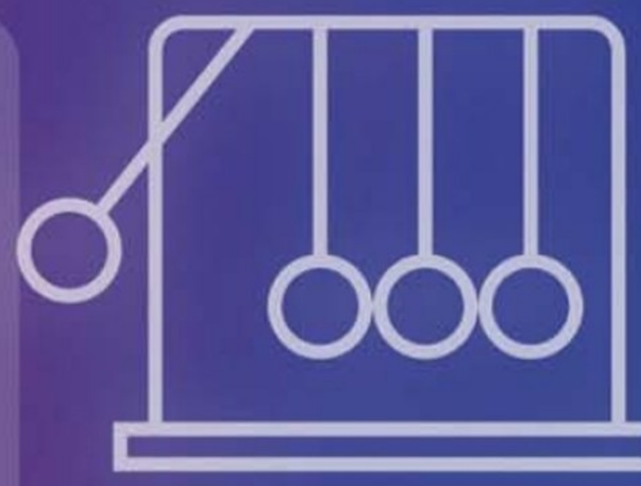
Le deuxième est la question autour des cas d'usages de la technologie. Les tests actuels vont délivrer leur verdict sur les possibilités réelles et là où les utilisateurs prennent en main ce nouvel univers. De plus, des technologies comme celles de la simulation 3D ou du jumeau numérique vont profiter de ces nouvelles possibilités. Dans le secteur de la distribution, les entreprises vont pouvoir affiner leur relation avec le client en reprenant de manière virtuelle un véritable dialogue avec le client final, ce qui n'est pas forcément le cas aujourd'hui avec les technologies à disposition.

Le troisième argument contre le métavers est la consommation électrique énorme qu'il demande pour fonctionner. Le phénomène est déjà là et personne n'a interdit le cryptominage du Bitcoin qui a besoin de 77 kWh, une consommation supérieure à celle de 159 états dans le monde. Cela représente 6.74% de la consommation électrique française. Les besoins de sobriété numérique sont évidents mais pas forcément à cause du métavers, mais tout simplement du fait des technologies dans les centres de données. Alors quand est ce que les fournisseurs de IaaS ou de colocation vont demander à leurs clients de n'utiliser que des instances ou des serveurs moins énergivores ?

Cette chronique ne se veut pas pro métavers, elle veut juste remettre l'église au milieu du village. Des efforts sont faits pour que les différents métavers puissent coopérer, mais aujourd'hui, personne n'est vraiment en mesure de définir la forme qu'ils vont prendre à l'avenir. Déjà, des débats sont ouverts pour savoir si le métavers doit s'appuyer nécessairement sur une blockchain et des NFT. Pas forcément, mais les thuriféraires de la technologie sont assez rigoristes sur ce point. Pour faire bref, cela marchera ou pas mais on peut tout de même laisser sa chance au produit avant de le condamner définitivement. □

SEKOIA.IO

Protéger efficacement son organisation n'a jamais été aussi exigeant.



De la prolifération des menaces à la sophistication des attaquants en passant par la complexification des systèmes à protéger, gérer les opérations de cybersécurité peut rapidement virer au cauchemar.

C'est pourquoi depuis 2016 nous avons développé SEKOIA.IO:

Votre back-end de cybersécurité

SEKOIA.IO est la plateforme intégrée de cybersécurité qui permet aux équipes SOC, aux analystes CTI et aux DSI et RSSI de piloter leurs opérations à travers les silos, en toute transparence, avec un budget déterministe.
Depuis la détection et la chasse aux menaces avancées jusqu'à la réponse et la supervision de circonstance, SEKOIA.IO fournit la boite à outils ultime pour fédérer vos ressources et amplifier vos efforts.

Retrouvez le premier XDR Européen sur sekoia.io/fr/sekoia-io-xdr

Au croisement des intelligences

Le secret des performances de SEKOIA.IO est au croisement des intelligences: l'expertise, l'intelligence artificielle, l'intelligence collective, et la threat intelligence.
Nos 20+ analystes CTI croisent et modélisent en permanence la menace issue de 500+ sources publiques et privées, et la diffusent vers vos équipes, vos équipements, vos prestataires de sécurité.

Retrouvez la CTI préférée des lecteurs de L'Informaticien sur sekoia.io/fr/sekoia-io-cti

Neutralisez les menaces avant impact

L'agilité et la flexibilité de SEKOIA.IO vous permettent d'intercepter les attaques à leurs stades initiaux, parfois bien avant que des charges utiles malveillantes aient pu arriver chez vous.
Notre architecture cloud-native permet un déploiement quasi-instantané: fini le temps des 18 mois de déploiement et des frais professionnels sans fond.

>100
intégrations natives

>1 Million
endpoints supervisés

>1 Milliard
events/jour

Réservez vite votre démonstration sur

sekoia.io

ou écrivez nous sur:

contact@sekoia.io

Une plateforme configurable et personnalisable

Avec FlashBlade//S, Pure Storage transforme le stockage de données

En juin, Pure Storage a organisé, au cœur de Downtown Los Angeles, le TechFest22. À cette occasion, la société a présenté plusieurs nouveautés, dont FlashBlade//S, une nouvelle plateforme de stockage évolutive pouvant aller jusqu'à 2 Po.

Selon le fabricant, FlashBlade//S offre des niveaux de haute performance et une optimisation de la capacité avec l'architecture exclusive 100 % QLC de Pure Storage. Ce nouveau produit, disponible au second semestre, se distingue aussi par une réduction de la consommation énergétique. L'entreprise a aussi annoncé la refonte de son offre d'abonnement Evergreen autour de trois offres.

Le nouveau châssis FlashBlade//S200 peut intégrer entre 7 et 10 lames de 24 à 48 To contre 15 pour l'ancienne version FlashBlade avec un volume de stockage pouvant atteindre les 2 Po.

Un enjeu majeur

Après deux années passées en distanciel, Pure Storage avait donné rendez-vous, les 8 et 9 juin, à ses clients, analystes et journalistes internationaux en Californie, à Los Angeles, pour le Pure//Accelerate TechFest22. Au cours de cette grand-messe rassemblant quelque 1000 personnes en présentiel et 8000 en session virtuelle, le spécialiste du stockage de données, fondé en 2009, par John Colgrove et John Hayes, a pu présenter ses dernières innovations en termes de matériel et de services. Pour Charles Giancarlo, le président et CEO de l'entreprise, il s'agissait de montrer en quoi le stockage de données est devenu un enjeu majeur pour les entreprises. *« Pendant longtemps, le stockage de données a été considéré comme une simple marchandise. Chez Pure Storage, nous estimons que les données sont le carburant du futur. Ce n'est pas une simple marchandise, mais une véritable valeur »*, a-t-il assuré en préambule de ce rassemblement.

De FlashBlade à FlashBlade//S

Parmi les grandes annonces de ce TechFest22, il faut évidemment retenir le lancement d'un nouveau produit dans la famille FlashBlade avec FlashBlade//S, décliné en deux versions S200 et S500. Lancée en 2017, la plateforme de stockage FlashBlade évolue pour apporter encore plus de puissance aux utilisateurs. FlashBlade//S introduit ainsi une architecture modulaire qui sépare le calcul de la capacité. Les éléments de stockage, de calcul et de mise en réseau peuvent être mis à niveau de manière flexible et sans interruption pour fournir une plateforme de fichiers et d'objets hautement configurable et personnalisable. La facilité d'utilisation est aussi mise en avant avec l'emploi du logiciel Purity//FB 4.0.

FlashBlade//S offre des niveaux de haute performance et une optimisation de la capacité avec l'architecture exclusive 100 % QLC de Pure sans avoir à recourir à des solutions de mise en cache coûteuses. Sur le plan matériel, ce châssis 5U (4U pour l'ancien modèle) est 25 %

plus haut que la version précédente. Il peut intégrer entre 7 et 10 lames de 24 à 48 To contre 15 pour l'ancienne version avec un volume de stockage pouvant atteindre les 2 Po. Le châssis peut aussi accueillir quatre modules QLC DirectFlash (Quad Level Cell). Chaque carte comprend quatre modules de mémoire Flash avec un processeur évolutif Intel Xeon de troisième génération (Ice Lake). Par ailleurs, la connectivité réseau est grandement améliorée par rapport à l'actuelle FlashBlade. Cette connectivité passe ainsi de 4X40 GbE à 8X100 GbE.

Charles Giancarlo, le président et CEO de Pure Storage, en scène pour évoquer les ambitions de l'entreprise, rappelant l'importance du stockage de données. *« Ce n'est pas une simple marchandise mais une véritable valeur »*, a-t-il plusieurs fois rappelé.

Consommation énergétique en baisse

Selon l'entreprise, FlashBlade//S est un châssis dont la durée de vie s'étendra au cours des dix prochaines années grâce à une nouvelle interconnexion réseau, une bande passante augmentée et des performances hautement améliorées. Il faut aussi noter que Pure Storage s'est penché sur la consommation énergétique de sa nouvelle solution FlashBlade//S, répondant ainsi à une demande croissante des entreprises qui cherchent de plus en plus à réduire leurs dépenses. Selon l'entreprise de Mountain View, les versions FlashBlade//S200 et S500 afficheraient une baisse de 48 % des besoins en énergie, de 28 % pour les besoins en refroidissement. Ces mesures ont été obtenues en mesurant la consommation et la volumétrie par Watt entre FlashBlade et FlashBlade//S. Au total, cela représente une consommation de 1,3 Watt par To.

« Avec FlashBlade//S200, nous répondons à 95 % des besoins actuels de nos clients. Avec la version S500, nous déverrouillerons de nouveaux niveaux de vitesse et de capacité. Mais surtout, nous ne manquons pas d'offrir la simplicité à nos clients », a assuré Rob Lee, CTO de Pure Storage, lors de la présentation de ce nouveau produit du catalogue de l'entreprise. D'autre part, FlashBlade//S200 se distingue par un taux de compression supérieur alors que la version S500 mise tout sur la performance avec un taux de compression moins important. La disponibilité des versions FlashBlade//S200 et S500 est prévue pour le second semestre mais aucun prix n'a été communiqué. Il faut aussi souligner que les clients équipés du système FlashBlade pourront évoluer vers cette nouvelle mouture tout en sachant que Pure Storage garantira le support FlashBlade pendant cinq ans.

Optimisé pour l'IA

Pour finir, Pure Storage a également annoncé la prochaine génération d'AIRI//S, la première infrastructure complète prête pour l'intelligence artificielle et optimisée par Nvidia. Cette solution, développée par Pure Storage et Nvidia, devrait grandement améliorer les nombreuses utilisations dans l'intelligence artificielle, le machine learning et l'analyse de données. *« En mettant l'accent sur la simplicité et l'évolutivité, AIRI//S permet aux entreprises d'obtenir des informations plus rapidement et de tirer le meilleur parti de leurs données grâce à l'intelligence artificielle »*, souligne Amy Fowler, vice-présidente en charge de la stratégie et des solutions FlashBlade. À noter que la commercialisation d'AIRI//S est assurée par des intégrateurs et pas directement par Pure Storage. □

Michel Chotard

Matt Burr, general manager de FlashBlade, et Amy Fowler, vice-présidente en charge de la stratégie et des solutions FlashBlade, en pleine présentation de la nouvelle technologie FlashBlade//S.

Simplifier la vie des entreprises

Le portefeuille Evergreen s'étend avec trois offres

L'organisation du TechFest22 a également été l'occasion pour Pure Storage d'annoncer le déploiement de la technologie Evergreen à l'ensemble de son portefeuille Pure.

Pour faire simple, une nouvelle offre, baptisée Evergreen//Flex, vient s'intercaler entre les solutions Evergreen//Forever (anciennement Gold) et Evergreen//One (anciennement Pure-as-a-service). Ainsi, Evergreen//Flex libère et déplace la capacité de stockage bloquée là où elle est nécessaire, offrant une efficacité et élargissant le portefeuille de services d'abonnement.

Simplifier le stockage

« La croissance de notre portefeuille Evergreen témoigne de l'engagement de Pure à simplifier le stockage des données. Se distinguant davantage avec le lancement d'Evergreen// Flex, Pure offre aujourd'hui la flexibilité et le choix d'approvisionnement les plus larges de l'industrie du stockage. Nous sommes ravis de continuer à offrir à nos clients la possibilité d'obtenir de meilleurs résultats avec un stockage flexible et simple », explique Prakash Darji, General Manager en charge de l'expérience digitale de Pure Storage.

Ainsi, avec Evergreen//Flex, Pure Storage entend offrir à ses clients la possibilité de s'équiper en mode CAPEX (Capital expenditure) en matériel avec un abonnement dont le coût sera en fonction du stockage consommé. Ainsi, Pure a annoncé que les entreprises qui souscriront à cette solution pourront bénéficier d'un changement du contrôleur tous les trois ans tout en conservant leur châssis. Cela permettra aussi aux clients de bénéficier de toutes les mises à jour matérielles et logicielles. À noter que l'abonnement à Evergreen//Flex est de 3 ans minimum. Concernant Evergreen//Forever, cette autre solution fonctionne aussi en CAPEX mais elle se différencie, car elle se base sur l'achat du matériel avec la souscription d'un abonnement. Enfin, Evergreen//One fonctionne en mode opex avec Pure Storage qui est propriétaire de la plateforme et qui réalise donc les opérations de maintenance. L'offre matérielle fournit par Pure Storage sera adaptée aux besoins des clients avec des services garantis via un SLA (Services Level Agreement). □

M.C

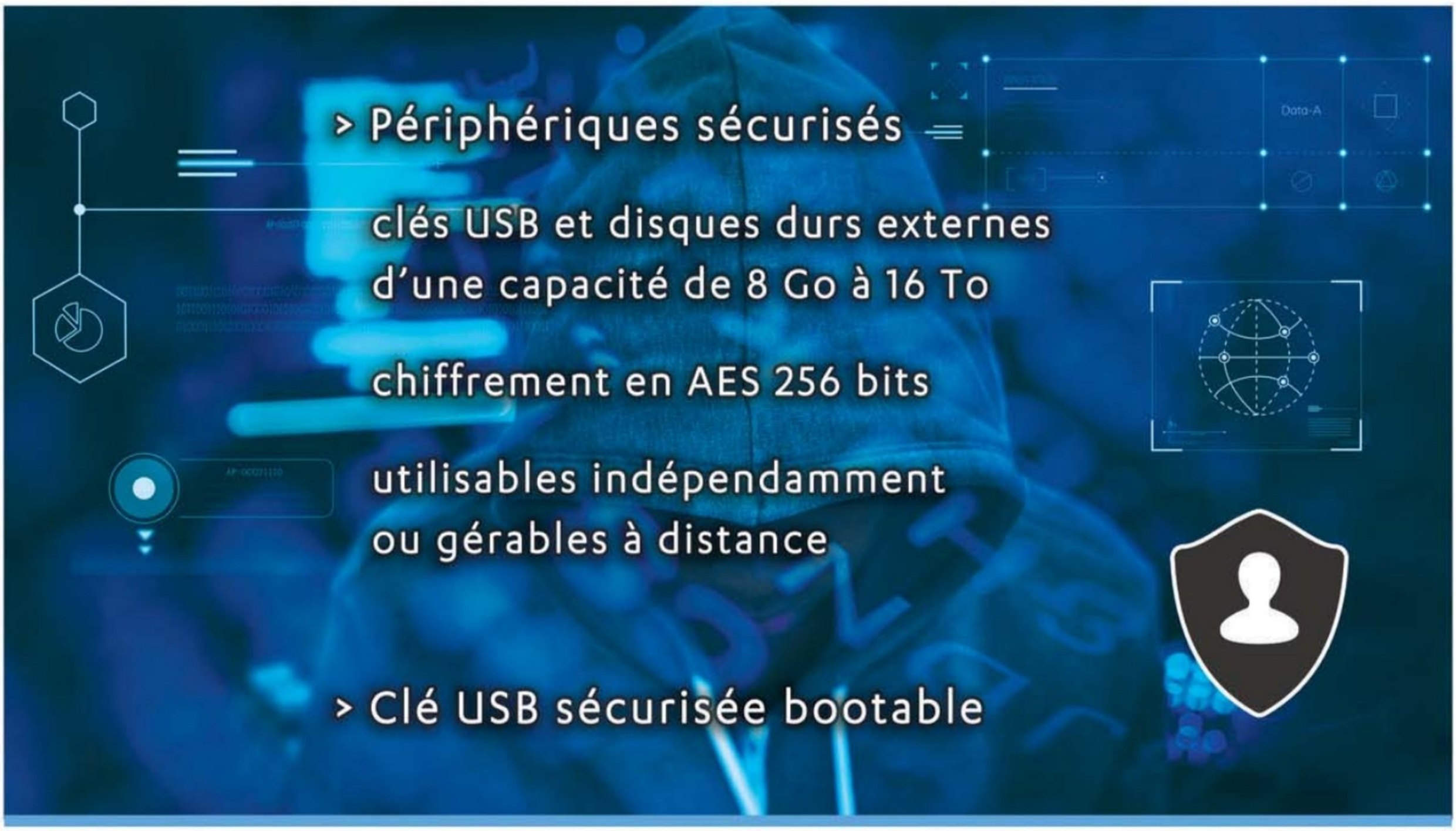
L'offre EverFlex s'étend à tout le portefeuille produit de Pure Storage.

PORTWORX FACILITE LE DÉPLOIEMENT DE BASES DE DONNÉES

Acquise en 2020 par Pure Storage, Portworx est la plateforme de services de données Kubernetes spécialisée dans des environnements hybrides et multicloud pour les applications conteneurisées. Durant TechFest22, les responsables de l'entreprise sont revenus sur les dernières mises à jour de cette solution à l'image de Portworx Data Services, Portworx Backup-as-a-Service et la nouvelle génération de Portworx Enterprise Solution. Selon Murli Thirumale, vice-président et General Manager de Portworx, le déploiement et l'exécution d'applications sous Kubernetes sont de plus en plus compliqués. Portworx vient en soutien des administrateurs informatiques en facilitant leur tâche avec un déploiement de bases de données en quelques clics tout en garantissant la protection des données. Le déploiement de nombreuses bases de données (Cassandra, Kafka, PostgreSQL, RabbitMQ, Redis et Zookeeper) est possible et d'autres le seront plus tard. Portworx Data Services fonctionne selon un modèle basé sur la consommation où les entreprises sont facturées au fur et à mesure ou via des heures prépayées.

Sécurisation des accès et des données

Solutions modulables protégeant de façon optimale votre parc informatique et vos informations numériques.



Query Informatique

www.query-informatique.com

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

Intelligence artificielle

Graphcore ajoute de nouveaux transformers à Hugging Face

Le projet de Github de l'intelligence artificielle s'enrichit avec de nouveaux transformers développés avec Graphcore.

Graphcore et Hugging Face proposent désormais un nombre plus important de modalités et tâches dans la bibliothèque open source, Hugging Face Optimum, dédiée à l'optimisation des performances. Les développeurs disposent d'une vaste gamme de modèles de transformers Hugging Face prêts à l'emploi et optimisés pour fournir les meilleures performances possibles sur les IPU Graphcore.

Une IPU Graphcore.

Les nouveaux modèles Optimum

Graphcore est devenu membre fondateur du Hugging Face Hardware Partner Program en 2021. Les deux entreprises avaient pour but de rendre l'innovation plus facile dans le domaine de l'intelligence artificielle. Depuis, les deux entités ont travaillé pour simplifier et accélérer l'entraînement des modèles de transformers sur IPU. Le premier modèle Optimum Graphcore (BERT) est sorti l'an dernier. Les développeurs ont désormais accès à 9 nouveaux transformers prenant en charge le traitement automatique des langues, la vision industrielle et la reconnaissance vocale. Ils sont fournis avec des fichiers configuration IPU et des paramètres ajustés, pré-entraînés et prêts à l'emploi. Ils concernent la vision industrielle et le traitement automatique du langage.

Sur ce dernier sujet, le GPT-2 est un modèle de transformer de création de texte pré-entraîné sur un très grand corpus de données anglophones, de manière auto-régulée. Cela veut dire que le modèle est pré-entraîné uniquement sur du texte brut, à l'aide d'un processus automatique de génération d'entrées et d'étiquettes, sans qu'aucun humain ne soit intervenu (d'où l'utilisation de données publiques). Il est entraîné pour générer des textes en devinant le mot suivant dans une phrase

QU'EST-CE QUE LES TRANSFORMERS ?

Les transformers proposent une nouvelle architecture pour les applications d'IA qui visent à résoudre les tâches séquence après séquence tout en gérant les dépendances sur le long terme. Les packages de transformers contiennent une trentaine de modèles pré-entraînés et une centaine de langues pour proposer des inférences sur de l'apprentissage machine sur le langage naturel avec huit architectures de référence sur la compréhension du langage naturel et de génération du langage naturel (NLU et NLG).

LE PROJET BIG SCIENCE

Le projet BigScience a été initié au printemps 2021 par la start-up franco-américaine en intelligence artificielle Hugging Face, pour remédier à ces problèmes en entraînant un nouveau modèle : Bloom. Il apprend à partir de grands corpus de textes, en utilisant un principe simple, consistant à prédire et à compléter des phrases, mot après mot. Chaque prédiction du modèle est comparée avec le mot correct, ce qui permet d'ajuster les paramètres internes du modèle. Dans le cas de Bloom, l'apprentissage est réalisé en évaluant des milliers de milliards de mots, conduisant à un modèle qui contient 176 milliards de paramètres. Cet apprentissage a duré plusieurs mois, nécessitant des centaines de processeurs graphiques (GPU) tournant en parallèle, soit l'équivalent de 5 millions d'heures de calcul. Bloom se distingue des autres modèles de langue par le fait qu'il est entraîné simultanément en 46 langues, réparties sur des sources aussi variées que de la littérature, des articles scientifiques ou des dépêches sportives et incluant de nombreuses langues rarement prises en compte, en particulier une vingtaine de langues d'Afrique. Agglomérer des contenus en des langues variées permet d'apprendre des modèles robustes et performants pour toutes les langues considérées, et conduit même souvent à des résultats meilleurs que des modèles monolingues. Le projet bénéficie des ressources du supercalculateur convergé Jean Zay, l'un des plus puissants d'Europe, mis en service en 2019 dans le sillage du plan AI for Humanity. Aujourd'hui, plus de 1000 projets de recherche mobilisent ses ressources.

donnée. Le RoBERTA est un modèle de transformer pré-entraîné sur un large corpus de données anglophones, de manière auto-régulée (comme le GPT-2). Ce modèle a été pré-entraîné avec l'objectif MLM (Masked Language Modeling). Pour une phrase donnée, il masque aléatoirement 15 % des mots fournis, puis exécute la phrase entière masquée afin de deviner les mots dissimulés. RoBERTa peut donc être utilisé pour la modélisation du langage masqué (MLM), mais il a surtout été pensé pour être ajusté à la précision dans le cadre de tâches en aval. Le DeBERTA (Decoding-enhanced BERT with disentangled attention) est un modèle neuronal de langage pré-entraîné pour les tâches de traitement automatique des langues. Il met à jour les modèles 2018 BERT et 2019 RoBERTa à l'aide de deux techniques novatrices, à savoir un mécanisme d'attention démêlée et un décodeur de masque amélioré, optimisant ainsi considérablement l'efficacité du pré-entraînement et les performances des tâches en aval. Le HuBERT (Hidden-Unit BERT) est un modèle auto-régulé de reconnaissance vocale et pré-entraîné avec des données audio. Son apprentissage consiste en un modèle de langue/acoustique sur entrées continues. Le modèle HuBERT est aussi performant que le wav2vec 2.0 exécuté dans les corpus Librispeech (960 h) et Libri-light (60 000 h) avec les sous-ensembles de 10 min, 1 h, 10 h, 100 h et 960 h.

Un SDK pour faciliter la vie

Par le kit SDK Poplar, mis à jour récemment, il est devenu plus simple de réaliser l'entraînement de modèles de pointe sur les équipements les plus avancés grâce à une intégration complète aux environnements d'apprentissage automatique standard (notamment PyTorch, PyTorch Lightning et TensorFlow) et à des outils de déploiement et d'orchestration comme Docker et Kubernetes. Poplar est compatible avec ces systèmes tiers, largement répandus. Les développeurs peuvent sans difficulté transposer des modèles provenant d'autres plateformes de calcul et, ainsi, bénéficier pleinement des fonctionnalités d'IA avancées de l'IPU de Graphcore.

Il est possible de télécharger ces nouveaux transformers de différentes manières, soit sur le site web de Hugging Face, ou en accédant au code via le référentiel Optimum de Hugging Face dans GitHub. En outre, Graphcore met à disposition une page de ressources pour développeurs, qui comprend notamment l'IPU Model Garden (un référentiel d'applications ML prêtes à être déployées : vision industrielle, traitement automatique des langues, réseaux graphiques, etc.), ainsi que des documents, des didacticiels, des vidéos explicatives, des webinaires, et plus encore. Cette page donne également accès au référentiel GitHub de Graphcore et à la liste complète de modèles Hugging Face Optimum. □

B.G

Le supercalculateur Jean Zay du Genci.

Comment sécuriser votre main-d'œuvre hybride

En raison de la pandémie de COVID-19, nos environnements numériques sont devenus plus dynamiques, et plus complexes que jamais auparavant. Si le passage massif au travail à distance et hybride a permis aux employés de bénéficier d'une flexibilité accrue et d'un meilleur équilibre entre vie professionnelle et vie privée, le fait d'avoir des travailleurs situés dans différents endroits a multiplié le nombre de réseaux, d'applications et d'interfaces utilisateur par l'intermédiaire desquels les données deviennent accessibles.

Dans le même temps, la pandémie a alimenté une vague de cybercriminalité majeure. Il y a eu une énorme augmentation des tentatives d'usurpation d'identité et de harponnage, les rançongiciels sont devenus plus répandus que jamais, et il semble y avoir une nouvelle violation de données très médiatisée sur une base presque quotidienne.

Aucune organisation n'est à l'abri de l'évolution du paysage des menaces. Cela signifie que les équipes informatiques doivent repenser leur approche de la cybersécurité, car le travail hybride présente un défi nouveau et inconnu.

Les bases du nouvel espace de travail hybride reposent sur des solutions technologiques telles que des appareils modernes et des outils de collaboration dans le cloud basés sur des solutions de sécurité qui assurent la sécurité des terminaux, des données et des identités.

Dans cet esprit, il est peut-être temps de repenser la stratégie matérielle de votre organisation. Des appareils, tels que les PC portables, sont utilisés par les employés dans un certain nombre de scénarios critiques, de la collaboration à des documents sensibles dans Microsoft Office à la collaboration avec des collègues éloignés sur Microsoft Teams. Fournir une protection robuste contre les logiciels malveillants et les rançongiciels les plus récents est une priorité essentielle car les organisations s'attendent à ce que ces appareils et données résistent aux attaques courantes.

Sécurité au niveau matériel

Les PC portables propulsés par un processeur AMD Ryzen™ PRO Série 6000 facilitent plus que jamais la sécurité des appareils d'entreprise. Alors que les appareils existants pourront souvent fournir des passerelles aux cybercriminels, les PC portables basés sur le processeur Ryzen™ PRO Série 6000 offrent des fonctionnalités de classe entreprise au niveau matériel, conçues pour se protéger contre les attaques les plus sophistiquées.

C'est en partie grâce à l'inclusion de la puce de sécurité Microsoft Pluton. Bien que développés en collaboration entre AMD, Intel et Qualcomm, les Ryzen™ PRO Série 6000 sont les premiers à intégrer l'architecture de processeur de sécurité de Microsoft[1], qui a été lancée dans Xbox et Azure Sphere et est conçue pour stocker des données sensibles, telles que des clés de chiffrement, avec du matériel intégré à la puce du CPU d'un appareil.

Microsoft Pluton s'appuie sur les idées de la puce TPM (Trusted Platform Module), qui contribue à améliorer la sécurité en empêchant les attaquants de falsifier le micrologiciel de bas niveau, ce qui pourrait conduire à une attaque sur les données stockées sur le PC. Il active également des fonctionnalités de sécurité telles que le chiffrement de disque BitLocker et une meilleure sécurité pour vos données biométriques utilisées avec Windows Hello.

Cependant, en raison de la popularité croissante du TPM, les attaquants ont commencé à innover pour l'attaquer, en particulier dans les situations où un attaquant peut voler ou obtenir temporairement un accès physique à un PC.

La conception Pluton élimine la possibilité que ce canal de communication soit attaqué en intégrant la sécurité directement dans le processeur, ce qui contribue à protéger les informations d'identification, les identités des utilisateurs, les clés de chiffrement et les données personnelles.

Avec un processeur AMD Ryzen™ PRO 6000, vous avez également accès à des fonctionnalités de sécurité de pointe telles que la protection matérielle « Shadow Stack » contre les attaques de flux de contrôle, son propre processeur sécurisé et le cryptage de la mémoire système en temps réel « Memory Guard » contre les attaques physiques sur les ordinateurs portables perdus ou volés.

---

1 : Depuis janvier 2022, seuls les processeurs AMD Ryzen™ Série 6000 incluent le processeur de sécurité Microsoft Pluton, ce qui exclut les processeurs AMD Ryzen™ Série 5000 ou les derniers processeurs Intel de 11e et 12e génération. RMB-24 Microsoft Pluton est une technologie détenue par Microsoft et concédée sous licence à AMD. Microsoft Pluton est une marque déposée de Microsoft Corporation aux États-Unis et/ou dans d'autres pays. Pour en savoir plus, consultez : https://www.microsoft.com/security/blog/2020/11/17/meet-the-microsoft-pluton-processor-the-security-chip-designed-for-the-future-of-windows-pcs/.

Investir dans la formation des employés

L'erreur humaine est la première cause de cyberattaques, c'est pourquoi les attaques d'hameçonnage sont en constante augmentation. Si les fonctionnalités de sécurité basées sur le matériel aideront à réduire le risque que des attaquants compromettent vos employés à domicile, une formation de sensibilisation à la cybersécurité est essentielle si vous souhaitez réduire le risque d'erreurs des employés. Former les employés à des sujets tels que les meilleures pratiques en matière de cybersécurité, les politiques d'utilisation des appareils personnels, les menaces courantes et la façon de les identifier peut contribuer grandement à garantir que les données sensibles de l'entreprise ne tombent pas entre les mains de cybercriminels.

Avec un plan solide en place, les entreprises peuvent être prêtes à atténuer les risques et à répondre aux menaces avant qu'elles ne s'avèrent coûteuses.

Gestion et sécurisation des appareils distants

La gestion des appareils mobiles (MDM) permet à un employé de gérer et de surveiller à distance son appareil personnel. Par exemple, il offre des fonctionnalités telles que l'effacement à distance et le suivi de localisation en cas de perte ou de vol d'un PC portable, et le « sandboxing » pour créer une section sécurisée sur l'appareil à utiliser exclusivement pour les tâches d'entreprise.

Grâce au travail hybride, le MDM ne base plus son raisonnement sur le périmètre. Les administrateurs informatiques doivent s'assurer qu'ils disposent désormais d'une solution complète qui leur permet de gérer et de sécuriser les appareils utilisés à la fois à l'intérieur et à l'extérieur du bureau, tout en garantissant l'absence de perte de productivité en conséquence.

Les PC portables propulsés par un processeur AMD Ryzen™ 6000 rendent cela plus facile que jamais. Ces processeurs sont dotés d'un processeur AMD Manageability intégré, qui permet un déploiement et une gestion simplifiés et compatibles avec l'infrastructure existante d'une organisation, ce qui signifie qu'aucun investissement majeur en infrastructure n'est requis. Vous pourrez déployer du matériel facilement grâce à la prise en charge par le processeur Ryzen™ PRO 6000 des outils cloud tels que Windows Autopilot. Vous disposerez aussi d'une flexibilité suffisante grâce aux normes et fonctionnalités ouvertes du processeur. En outre, la gestion à grande échelle deviendra plus aisée que jamais grâce à la prise en charge par le processeur Ryzen™ PRO 6000 des solutions de gestion modernes, telles que Windows Endpoint Manager.

Sécuriser votre main-d'œuvre hybride

La sécurité doit toujours être une priorité pour les entreprises. L'augmentation des espaces de travail distants et hybrides, les défis et les complexités continueront de croître au fur et à mesure de l'évolution constante des entreprises pour relever ces défis. Tout en veillant à ce que vos employés soient informés des dernières menaces et des meilleures pratiques, il est également important que les organisations cherchent à adopter une solution matérielle qui protégera les employés contre les attaques sophistiquées et le vol de données d'entreprise.

Voir pour sécuriser

La visibilité réseau est fondamentale pour le Cloud

Une étude récente menée par Pulse, une filiale du cabinet Gartner, démontre que la visibilité est l'élément le plus important pour la migration vers le Cloud.

L'étude a été menée par Pulse, une entité du groupe Gartner, entre fin décembre et janvier 2022. 266 personnes ont été interrogées, majoritairement des décideurs de services IT ou sécurité (VP, directeurs, managers) d'organisations importantes (5000 salariés) en Amérique du Nord et en Europe. Un de ses principaux enseignements indique que 64 % des responsables IT européens ont fait de la visibilité leur priorité numéro un lorsqu'il s'agit de mettre en place un environnement cloud plus sécurisé. La moitié des personnes interrogées reconnaît désormais l'importance d'une "observabilité avancée" de l'environnement cloud. À savoir, une visibilité qui fournit des renseignements en temps réel au niveau du réseau et des informations exploitables pour diminuer les risques. Les organisations basées en Europe ont classé la visibilité du trafic sur le cloud, ainsi que l'accès aux applications et le contrôle des données en mouvement, entre 20 et 30 points plus haut que leurs homologues américains.

Un TAP réseau de Gigamon.

Coût et complexité, un frein pour la migration

L'enquête de Pulse et Gigamon a également identifié le coût et la complexité comme deux obstacles majeurs à la migration vers le cloud. Selon l'étude, 78 % des responsables IT européens estiment que le coût élevé du cloud rend plus difficile la migration des charges de travail et des applications.

L'étude soulève aussi d'autres soucis impliquant des difficultés pour migrer vers le Cloud. 98 % des sondés estiment que les goulets d'étranglement du réseau et les opérations complexes de résolution des incidents liés au cloud ralentissent la migration vers le cloud hybride ou multi-cloud. 99 % affirment que les équipes ne respectent pas les niveaux de qualité service (SLA) attendus relatifs à la charge de travail des applications en raison de la complexité des infrastructures cloud et 61 % pensent que le coût et la complexité de l'infrastructure cloud entraînent une réduction du budget qui serait nécessaire pour l'investissement dans d'autres applications vitales. Enfin, en Europe, 68 % des personnes interrogées ont déclaré qu'elles préféraient gérer la sécurité de leurs environnements de travail avec une source unique de visibilité sur l'ensemble de l'environnement, plutôt que de travailler en silos. ☐

B.G

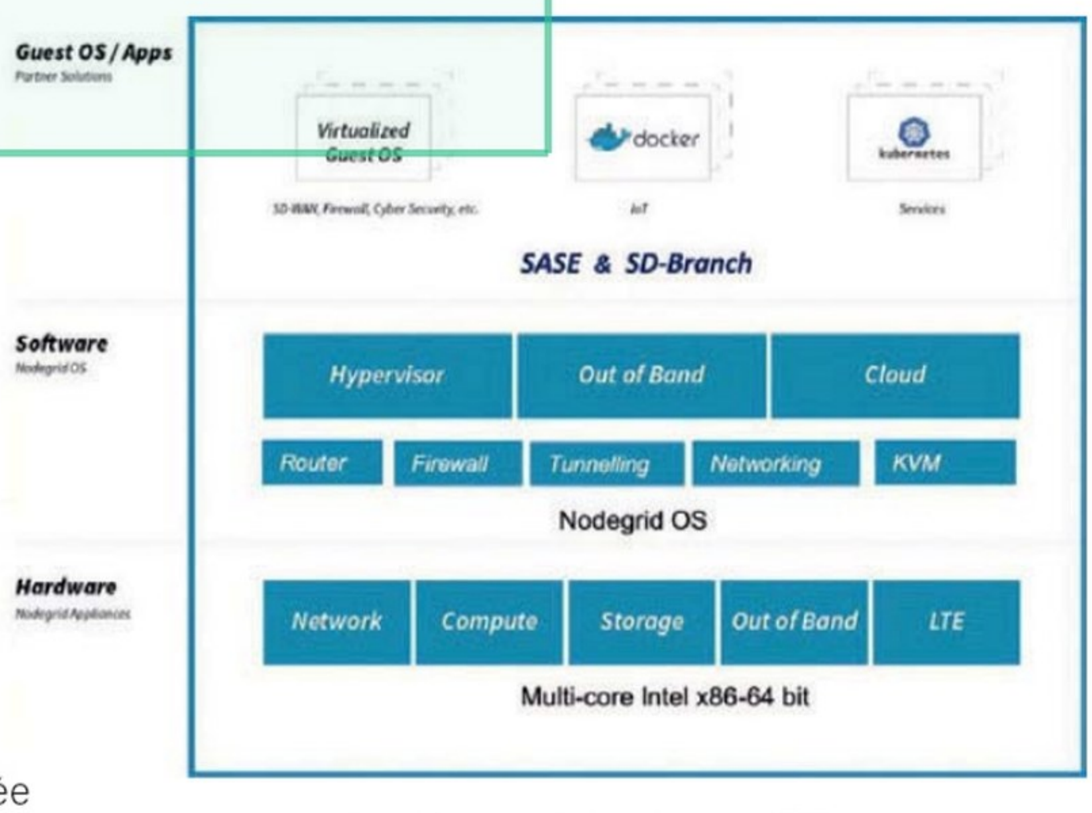
L'ACOSS CHOISIT GIGAMON

L'Acoss (Agence centrale des organismes de la Sécurité sociale) est la caisse nationale des Urssaf en charge du recouvrement. Elle assure le pilotage de la collecte des cotisations auprès de 900 organismes et garantit la redistribution aux quatre branches du régime général de la Sécurité sociale : maladie, vieillesse, famille et accidents du travail/maladies professionnelles. Depuis dix ans, l'institution opère une centralisation sur des environnements très virtualisés sur deux centres de données, ce qui a amené plus de complexité et des problèmes de visibilité. Après un appel d'offres qui comprenait un réseau de capture, d'agrégation et de transformation des données afin d'alimenter une solution de visibilité applicative à base de sonde, un premier déploiement – équivalent à 30% du réseau de capture actuel – s'est déroulé en quelques jours seulement avec l'insertion des TAP (un dispositif de surveillance externe recopiant le trafic circulant entre deux nœuds de réseau), le câblage, l'utilisation de rocades cuivre/fibre afin de pouvoir interconnecter les matrices et optimiser le déploiement au sein du datacenter. Aujourd'hui, tous les points d'entrée et de sortie – notamment l'accès aux applications métiers par les 14 000 utilisateurs – sont couverts par Gigamon. En 2020, l'Acoss a également dû rapidement s'adapter au télétravail de masse et à la très forte augmentation des débits. L'ensemble des collaborateurs se connectant via un VPN, les équipements se sont retrouvés sur-sollicités. Grâce à Gigamon, l'Acoss a pu être réactive et offrir la visibilité et la sécurité nécessaires aux équipes techniques pour garantir le confort d'usage de ses utilisateurs. Aujourd'hui, la DSI réfléchit à étendre de nouveau le réseau de visibilité Gigamon afin de permettre une visibilité Est/Ouest totale au sein même de l'environnement virtualisé de leurs serveurs applicatifs.

Orchestration

ZPE, la supervision tout-en-un

Créée en 2013, la société ZPE est mondialement connue mais discrète malgré sa présence en France auprès de grands comptes. La société propose une solution tout-en-un combinant logiciel, matériel et capteurs pour apporter de l'automatisation et de l'orchestration sur les opérations réseau et sécurité.



L'architecture de la solution de ZPE.

Le Gartner recouvre le type de solution proposée par ZPE sous le vocable d'Hyper-automatisation. ZPE est le couteau suisse des services réseaux en apportant une solution pour simplifier et unifier la vision sur le réseau et les opérations sur celui-ci. La solution est déployable sur site ou à partir du Cloud. En local, ZPE propose des routeurs qui alimentent la console de supervision dans le Cloud à partir de différents capteurs ou agents. Il est possible depuis la console de configurer, de déployer, de gérer et de s'assurer des accès pour mettre en œuvre la solution souhaitée. Le système d'exploitation de l'éditeur apporte une couche de virtualisation qui permet d'accueillir les services tiers comme pour la sécurité par exemple afin de permettre une supervision Out of Band de l'ensemble des composants IT présents dans l'entreprise.

Sur site, la solution se présente sous la forme d'une appliance qui regroupe l'ensemble des fonctionnalités et des extensions permises par tout un jeu d'API pour répondre aux besoins précis de l'entreprise. Ainsi, en septembre de l'année dernière, ZPE a annoncé pouvoir embarquer Prisma SD-WAN de Palo Alto Networks dans ses routeurs de périphérie. Dans ce cas, la solution se comporte comme un mini Cloud en périphérie.

De multiples avantages

ZPE apporte le bénéfice à la fois des solutions tout-en-un mais aussi la possibilité de déployer facilement des solutions Best of Breed avec une supervision d'un point central et unique tout en évitant d'avoir à déployer, gérer et payer des licences ou des abonnements pour des solutions disparates. La solution consolide la pile réseau et simplifie les opérations de déploiement, de configuration, de mise à l'échelle et de gestion des réseaux. Elle facilite la vie des équipes chargée du réseau. En effet qui n'a pas vécu le calvaire de déployer des réseaux distants ou d'essayer de retrouver la cause d'un incident sur ce type de site et de restaurer les services défaillants ? ZPE est particulièrement adapté pour les entreprises ayant de nombreux sites distants ou des infrastructures très distribuées. □

B.G

NODEGRID 5.6

Lors du dernier Cisco Live, qui s'est tenu à Las Vegas courant juin, ZPE a annoncé une nouvelle version de son OS, NodeGrid, disponible pour ses consoles et routeurs. Comme sa prédécesseur, la solution permet de déployer des solutions Best of Breed au choix de l'entreprise à partir de la console Cloud de la solution de ZPE. Il est ainsi possible de déployer des solutions embarquant les différents logiciels de fournisseurs pré-validés. En voici la liste :
Ansible, Gluware, Stackstorm, On-ramp to Cisco SIG/Umbrella/CDFW, les firewalls Fortinet et Palo Alto Networks PANOS, les agents ThousandEyes...
La solution fournit ainsi un plan complet d'automatisation qui peut être orchestré depuis NodeGrid pour la gestion des changements de configuration, le monitoring du réseau et les réponses aux attaques et éviter ainsi les interruptions de service.

Convergence réseau et sécurité

Une nouvelle version de FortiOS

La nouvelle version du système d'exploitation de Fortinet ajoute de multiples fonctionnalités à la plate-forme et renforce la convergence entre réseau et sécurité.

Le fournisseur de solutions de sécurité annonce la version 7.2 de FortiOS. La version embarque plus de 300 nouvelles fonctionnalités pour déployer la sécurité de la périphérie du réseau au Cloud. Performance et détection et réponses aux menaces sont aussi présentes.

Une forte présence de l'IA

FortiOS 7.2 propose de nouveaux services de sécurité FortiGuard, optimisés par l'Intelligence Artificielle pour sa plateforme convergente de sécurité et réseau, tout en consolidant davantage des produits de sécurité distincts sur les réseaux, les terminaux et les environnements cloud. Ces nouveautés permettent à FortiOS de mieux protéger les réseaux hybrides actuels face à des menaces toujours plus virulentes, tout en permettant aux entreprises d'accélérer leur transformation numérique. De plus, le panel des services de sécurité FortiGuard, piloté par FortiGuard Labs, est intégré en natif sur l'ensemble de la Fortinet Security Fabric pour garantir une sécurité automatisée et coordonnée en temps réel. Les services FortiGuard bénéficient d'un apprentissage machine de confiance, ainsi que de fonctions basées sur l'intelligence artificielle. Celles-ci capitalisent sur des données provenant de réseaux, des terminaux et du cloud et par des données de recherches indépendantes. Elles bénéficient également de nombreuses collaborations avec des partenaires du secteur.

Des exemples de nouveaux services

Parmi les nouveaux services de la version, on peut distinguer un bac à sable intégré qui devient une fonction temps réel, étroitement intégrée au réseau, pour neutraliser les malware connus et inconnus, avec un impact maîtrisé sur l'opérationnel. Il en résulte une protection renforcée contre les ransomware par rapport aux solutions qui acceptent des fichiers suspects au sein du réseau et qui, par la suite, doivent tracer le malware une fois identifié.

Un service détecte automatiquement et segmente les dispositifs IT et OT compte tenu de leur fonction sur le réseau. Ce service procède également à un inventaire des ressources et utilise le pattern matching pour appliquer les règles pertinentes et automatiser la remédiation. Ce service est actif sur la solution NGFW et sur le LAN Edge grâce à une intégration avec FortiNAC. L'utilisation de playbooks dédiés au contrôle d'accès au réseau (NAC – Network Access Control) permet de détecter et de traiter les menaces au plus proche des ressources protégées.

SENSIBILISER LES COLLABORATEURS DE L'ENTREPRISE

Une enquête réalisée pour le compte de Fortinet indique que 73% des entreprises ont subi au moins une intrusion ou un piratage qui peut être partiellement attribué à une carence de compétences en cybersécurité. Le nouveau service Security Awarenes and Training s'adresse à toutes les entreprises souhaitant maîtriser les menaces en sensibilisant davantage leurs collaborateurs. Les différents programmes, élaborés par le Fortinet Training Institute, offrent des formations et certifications en cybersécurité. L'organisation a obtenu de nombreux prix qui récompensent la qualité de ses contenus et programmes de formation. Ce nouveau service aide les entreprises à former leurs utilisateurs à être vigilants face à des cybermenaces toujours plus sophistiquées, et à reconnaître les cyberattaques pour éviter d'en être victime. Les programmes respectent les recommandations NIST 800-50 et NIST 800-16. Le cursus intègre des perspectives pour former davantage les collaborateurs aux menaces actuelles et les empêcher de céder aux cyberattaques les plus récentes.
En capitalisant sur les programmes de formation et de sensibilisation existants, le service Security Awareness and Training se veut une option économique pour créer, lancer et piloter des campagnes de sensibilisation ciblant les collaborateurs et utilisateurs.

Conçue pour le secteur de la finance et autres environnements réglementés, une solution d'IPS dédié permet de migrer d'un outil IPS autonome vers un pare-feu NGFW, tout en pérennisant l'opérationnel et les bonnes pratiques.

Un nouveau service de pare-feu NGFW FortiGate collabore étroitement avec le module Fabric Agent de FortiClient pour inspecter le trafic selon les principes de ZTNA (Zero Trust Network Access) et vérifier le statut ZTNA.

Un filtrage d'URL, de DNS et de flux vidéo permet de déployer une protection intégrale qui jugule de multiples menaces : ransomware, détournement d'identifiants, phishing et autres attaques issues du web.

Un renforcement de la convergence

FortiOS 7.2 unifie davantage la convergence des fonctions réseau et de sécurité sur un périmètre large : pare-feu NGFW, SD-WAN, LAN Edge, 5G, ZTNA et davantage. La solution de SD-WAN sécurisé de Fortinet bénéficie d'améliorations qui accélèrent et automatisent la couche d'orchestration et encouragent l'évolutivité des architectures WAN. Par un monitoring des analyses des données applicatives et de la note moyenne d'opinion pour les applications voix et données, les entreprises peuvent mesurer la qualité d'expérience d'une application dans la perspective de l'utilisateur final. SD-Branch est une solution de protection des sites distants du WAN Edge au LAN Edge et propose des fonctions de WAN sur 5G, de SD-WAN, de sécurité par pare-feu NGFW ainsi que des équipements LAN à partir d'une seule solution unifiée et convergente. FortiOS 7.2 propose de nouvelles fonctions automatisées de déploiement et d'orchestration qui sécurisent la gestion des réseaux sur les sites distants.

Avec la nouvelle version de FortiOS, FortiGate devient le tout premier pare-feu compatible avec HTTP/3.0. La solution offre davantage de visibilité et de protection pour les nouveaux standards HTTP qui apportent la rapidité et l'agilité nécessaires à l'accélération numérique.

Le module ZTNA intégré au pare-feu nouvelle génération (appliance, VM ou fourni depuis le cloud) se rend disponible sur l'ensemble des sites accueillant des collaborateurs, permettant ainsi un télétravail en tout endroit, à tout moment. Cette fonction est encore plus simple à gérer grâce à une interface unique de configuration des règles, pour chaque connexion et chaque amélioration apportée au portail de service ZTNA.

FortiSASE offre un accès privé sécurisé aux applications corporate, grâce à une fonction ZTNA intégrée en natif et assure la protection des terminaux et la redirection de trafic. La validation en continu des identités et du contexte permet aux entreprises d'offrir aux utilisateurs distants un accès explicite à chaque application, palliant ainsi les carences des VPN traditionnels.

Une gestion centralisée

Les améliorations apportées simplifient et automatisent le déploiement des environnements d'envergure, grâce à un provisioning automatisé. Elles intègrent plus étroitement l'IA au sein des opérations réseau, offrent une gestion centralisée avec FortiManager et proposent un monitoring de l'expérience numérique via FortiMonitor. □

B.G

Stockage

ITPT 44 : redéfinir la gestion des données

Courant juin, *L'Informaticien* a repris la route vers les USA à la rencontre des acteurs du stockage en Californie et au Colorado. La tendance est à la diffusion de l'intelligence artificielle, du Cloud et d'une automatisation accrue.

Veritas veut rendre la sauvegarde autonome

Dans la version 10, Veritas avait largement infusé de l'automatisation dans son logiciel NetBackup avec une protection des environnements clouds natifs, des environnements en SaaS, le scan intégré de malwares et le Stockage sous forme de service ou StaaS avec Recovery Vault. Dans les prochaines versions, même si aucune date précise n'a été donné, les logiciels de Veritas s'appuieront sur l'apprentissage machine et l'intelligence artificielle pour que la solution soit totalement autonome avec des fonctions de self-provisioning, d'autoconfiguration, d'optimisation automatique, de self-service pour couvrir de nombreuses fonctionnalités comme la protection des données, les reprises après sinistre, l'archivage et la découverte des données et des analyses sur le système et l'utilisation des données. La solution va ainsi pouvoir totalement décharger les humains de la tâche du stockage et de la sauvegarde tout en assurant une protection maximale quel que soit l'environnement et quelle que soit l'échelle.

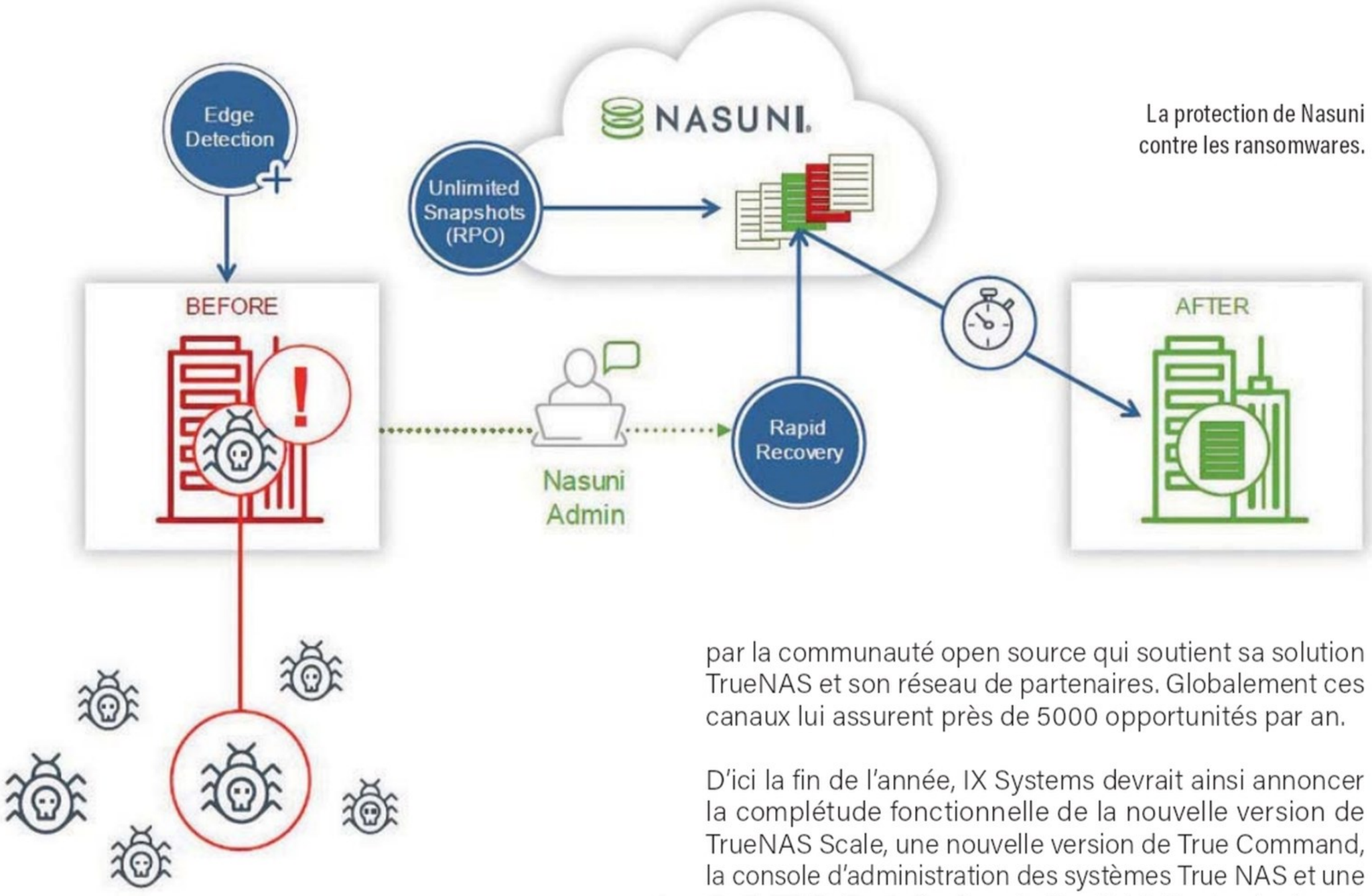
Weka prend en charge le multicloud

L'éditeur d'origine israélienne s'est taillé une belle réputation pour ses performances et sa puissance pour les environnements de HPC. Avec une nouvelle version de sa plate-forme, Weka veut étendre son champ d'action et répondre aux nouveaux besoins des entreprises. Plus des trois-quarts des 2000 premières entreprises dans le monde sont déjà dans ce contexte. L'idée de cette nouvelle version est tout simplement de permettre de faire fonctionner dans le Cloud tous les workloads qui ne peuvent le faire aujourd'hui car ils sont trop exigeants en latence faible, du fait de leur criticité pour l'entreprise, du volume des données ou des performances nécessaires à leur bon fonctionnement. Avec cette version, la solution Weka Data Platform, qui était sur AWS, devient multicloud et peut être porté sur les principaux clouds publics : AWS, GCP, Oracle et Azure dans un proche avenir. Elle apporte ainsi une vision et une gestion centralisée autour de la protection des données dans les différents clouds de l'entreprise. La solution peut être déployée sur des disques NVMe TLC ou QLC suivant les besoins en performance ou les coûts. L'interface utilisateur a été revue. La solution étend de plus le support de protocoles en ajoutant NFS v4 et SMB. La plate-forme reprend les fonctions de réduction de données spécifiques de Weka comme la « zero copy » et le « zero tuning ». Pour s'adapter à ces nouvelles demandes, Weka a revu sa tarification et le packaging logiciel avec quatre nouvelles possibilités. Une possibilité se fondant sur une tarification à la consommation devrait rapidement être ajoutée.

Vast Data mise sur l'innovation

Lors de notre visite, Jeff Denworth, le directeur marketing de Vast Data, a peint le tableau de la croissance météorique de la compagnie et insisté sur l'innovation que la société continue de privilégier. Il est revenu sur la plate-forme Ceres qui a été mise en œuvre avec NVidia. Elle comprend 2 smart

La feuille de route de NetBackup.



La protection de Nasuni contre les ransomwares.

NIC Bluefield de NVidia sur une connectique 4 x100 GB Ethernet avec deux switches PCIe, 22 disques capacitifs QLC entre 15 et 30 To et 8 disques SCM remplaçables à chaud pour proposer une solution offrant jusqu'à 675 To de flash brut dans seulement 1U d'espace rack et une capacité minimale de 338 To, tout en prenant en charge l'évolution transparente des clusters vers des centaines de pétaoctets.

Il a ensuite présenté des éléments nouveaux de réduction des données avec un nouveau mode de compression sur un algorithme de similarité qui analyse les données entrantes pour les regrouper par similarité, les compresse ensemble pour les stocker sur les disques capacitifs QLC sur des morceaux de données à taille adaptable afin d'optimiser la compression. Il s'y ajoute un dictionnaire global de compression partageable en miroir disponible pour 10 000 contrôleurs. En résumé la solution embarque dès la prochaine version 4.4,ce dictionnaire de copie, la compression par similarité avec des chunks adaptatifs et une compression Delta pour les nouvelles données. Cette dernière apporte encore une réduction optimale de 25 % des coûts de stockage.

IX Systems TrueNAS continue sa marche en avant

L'année 2022 a été une nouvelle fois riche pour IX Systems et les offres TrueNAS. Outre les annonces déjà anciennes réalisées en février dernier, le constructeur a fait évoluer sa manière d'aborder le marché via une promotion par la communauté open source qui soutient sa solution TrueNAS et son réseau de partenaires. Globalement ces canaux lui assurent près de 5000 opportunités par an.

D'ici la fin de l'année, IX Systems devrait ainsi annoncer la complétude fonctionnelle de la nouvelle version de TrueNAS Scale, une nouvelle version de True Command, la console d'administration des systèmes True NAS et une version 13 de production de TrueNAS. Tout cela devrait s'accompagner d'annonces de partenariats importants et de références clients notables. Plus tard dans l'année, des fonctions autour de la sécurité devraient renouveler les nouveautés d'Angelfish annoncées en février dernier.

Nasuni veut protéger vos données partout

Nasuni a une mission simple : rendre accessible vos données et les protéger quel que soit leur environnement. La solution qui protège près de 3 milliards de fichiers par semaine connaît une belle reconnaissance sur le marché et auprès de ses clients, avec une levée de fonds en mars dernier et deux acquisitions (DBM et Storage Made Easy) qui ont apporté un outil de migration de données et un outil de visibilité sur l'ensemble des silos de stockage.

L'éditeur évolue vers une approche de services de données de fichiers pour que celles-ci soient accessibles de partout et protégées de manière proactive par une combinaison de logiciels. Un exemple de cette approche est l'ajout d'un service breveté de protection contre les rançongiciels par un add-on à la plate-forme de Nasuni. Ce service protège contre les attaques en cours par des alertes sur les patterns de fichiers suspicieux et identifie la source de l'attaque tout en protégeant les fichiers sur un backend de stockage objet à coût bas dans le cloud. Le service propose de plus une restauration rapide en quelques secondes avec une très grande précision. La détection se réalise en temps réel sur les modèles de fichiers suspicieux et s'intéresse aussi aux extensions

et aux notes de rançon. Le service tient à jour une base de Threat Intelligence pour contrer les menaces les plus récentes. Il identifie les fichiers touchés, identifie le premier poste infecté et l'adresse IP source de l'attaque.

Lightbits : le DAS (Direct Attached Storage) en mieux

Lightbits, société fondée en 2016, commence à monter en puissance et propose une réelle alternative avec sa solution logicielle qui s'appuie sur une infrastructure matérielle désagrégée et NVMe over TCP. La solution annonce des performances de très haut niveau avec 79 M d'IOPS et une latence de 160µs et un facteur 20 d'endurance comparativement aux solutions actuelles de DAS, de SAN (Storage Area Network) et autres solutions définies par logiciel. La solution fonctionne en cluster avec au minimum 3 serveurs de stockage et peut évoluer par ajout de disques ou de serveurs sans interruption de services. Le cluster évolue en scale out avec un maximum de 16 serveurs de stockage qui peuvent accueillir 64 000 volumes et 64 000 clients par cluster.

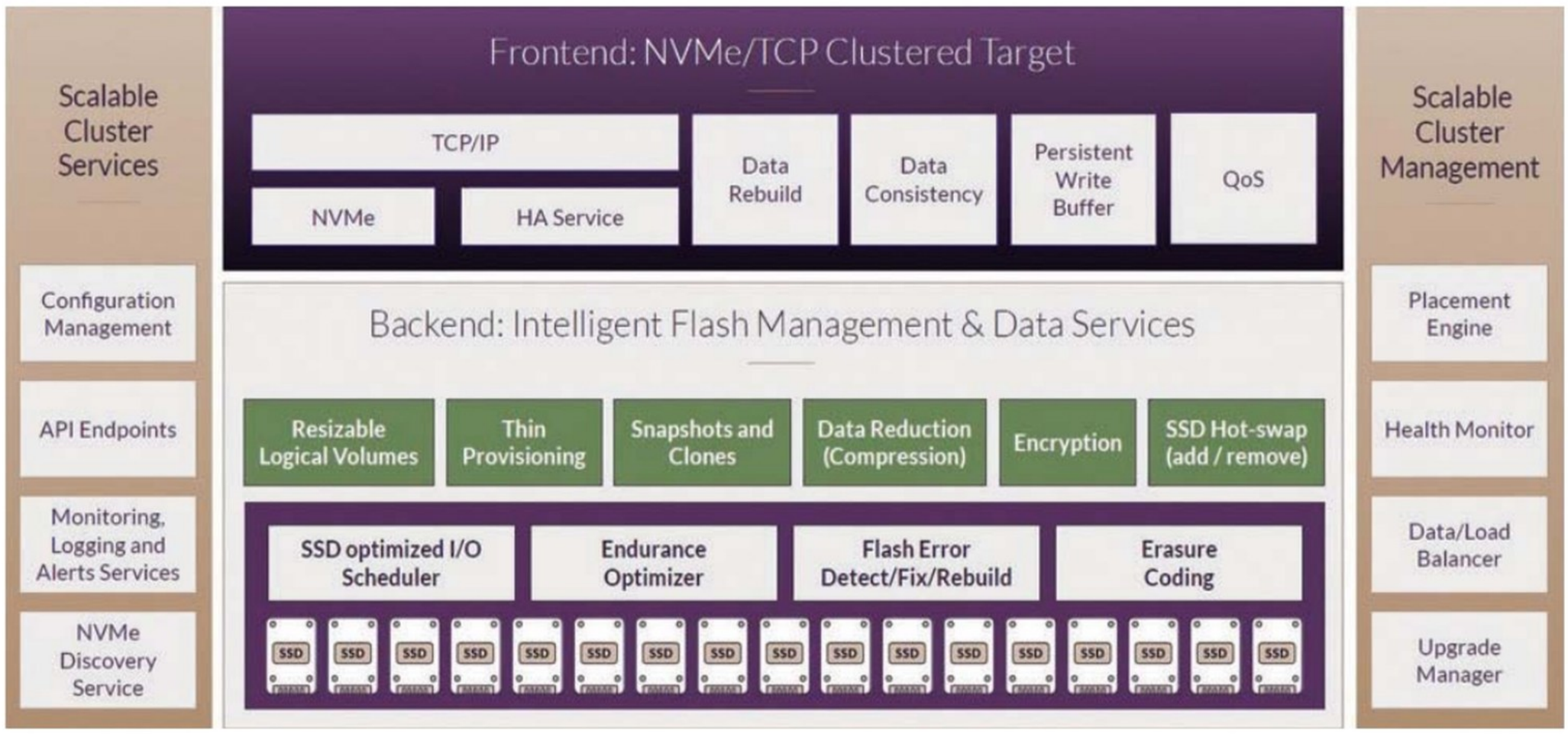
L'éditeur a un partenariat avec Intel, qui est investisseur dans l'entreprise avec Intel Capital, à la fois pour les processeurs Xeon, les mémoires Optane et les adaptateurs réseaux embarqués dans sa solution. La société a un partenariat de même niveau technique avec VMware pour des intégrations fines avec vSphere, vStorage et vCenter. Au tout début du mois de juillet, l'éditeur a levé 42 M$ auprès de nouveaux investisseurs : Atreides Management, qui a mené le tour, aux côtés de J.P. Morgan, Valor Equity Partners, Eyal Ofer, O.G. Tech, le fondateur et chairman de Pacific Century Group (PCG) Richard Li, ainsi que les principaux investisseurs déjà présents. Au total Lightbits a levé 100 M$. Les fonds devraient principalement alimenter la R&D de l'éditeur qui mise principalement sur l'innovation produit pour l'instant.

Quantum se renouvelle totalement

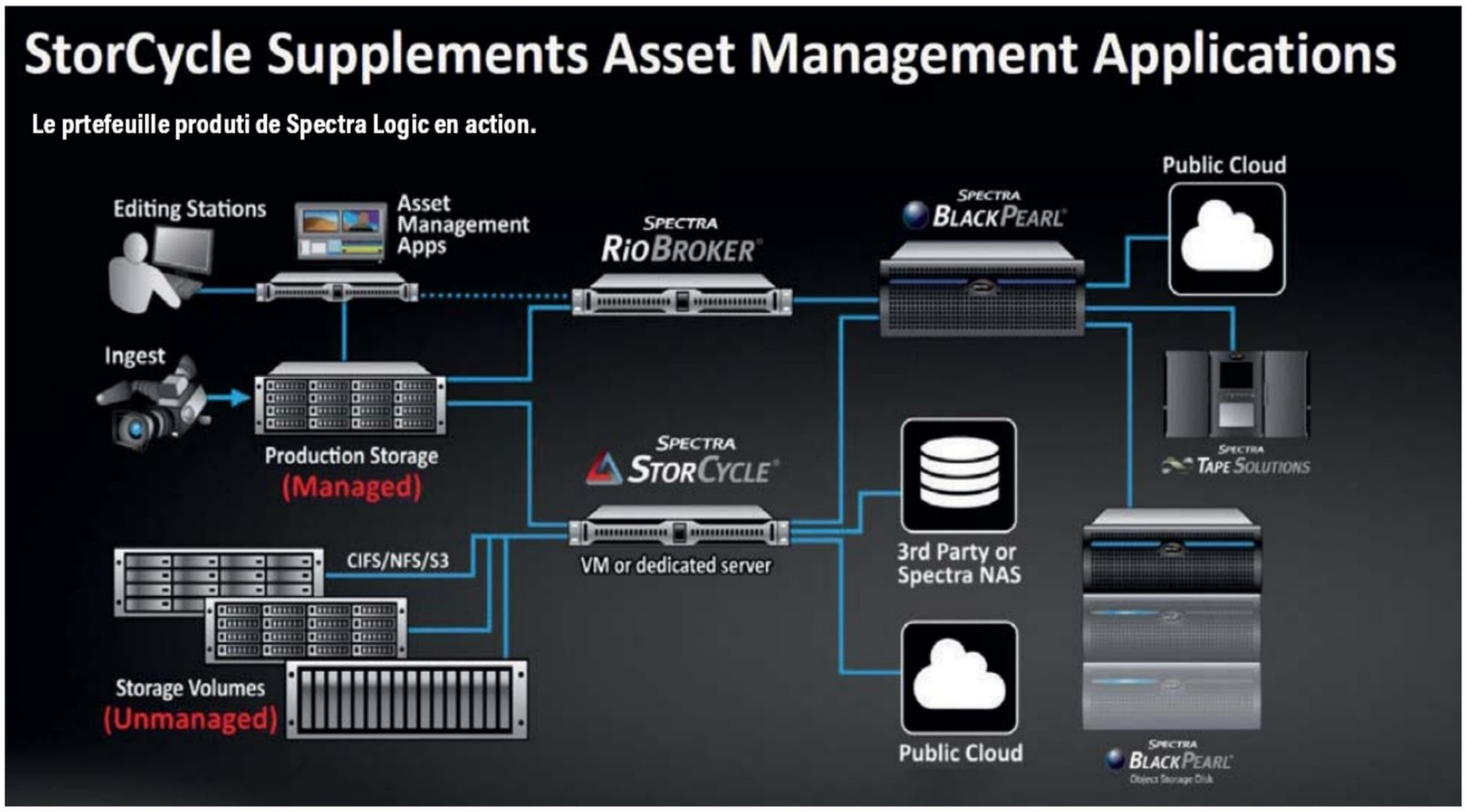
Quantum a eu une histoire chaotique lors des dernières années. Pour éviter de nouveaux soubresauts, Jamie Lerner, le CEO, a mis en place une stratégie basée sur l'efficacité pour répondre aux nouveaux besoins autour des données. Cela se traduit par une refonte complète du portefeuille produit, aussi bien matériel que logiciel. Ainsi, plutôt que de vendre des serveurs comme auparavant, Quantum propose désormais son système de fichiers dans des appliances, les F et H Series. Les interfaces administrateurs et utilisateurs ont été revues pour se moderniser et répondre aux canons du moment. Une solution de SSO (Single Sign On) a été ajoutée. Désormais le portefeuille produit est là pour répondre à tous les cas d'usages de stockage, que ce soit sur site ou dans le Cloud.

Le CEO de Quantum pointe surtout que son principal différenciateur réside dans son logiciel, le système de fichier StorNext. Ce système est maintenant virtualisé et en containers. Il peut ainsi se déployer sur n'importe quel matériel. La concrétisation de cette nouvelle approche se trouve dans l'appliance H4000 Essential qui regroupe StorNext et CatDV, un outil de découverte sur les données qui se combine avec les outils d'intelligence artificielle de Nvidia pour enrichir des contenus vidéos ou audios. Une plate-forme unifiée de surveillance sur ces contenus simplifie l'utilisation de l'infrastructure d'enregistrement des flux de vidéos. Avec ces qualités, le système peut maintenant fonctionner sur matériel sur disque ou sur bande. L'appliance virtuelle DXI V5000 en est l'illustration et peut se télécharger librement en quelques minutes dans sa version Community.

On ne peut évidemment pas parler de Quantum sans toucher un mot du stockage sur bande et du lancement d'une librairie sur mesure, la Scalar I6H, pour les environnements



Architecture de la solution de Lightbits.



d'archivage en exaoctets. Chaque bloc peut être verrouillé pour assurer une sécurité totale du stockage sur la bande par une barrière physique sur le matériel.

Liqid milite pour le centre de données dynamique

Liqid est partisan d'une infrastructure composable totale, de la mémoire en passant par les processeurs, réassemblables pour obtenir des serveurs ou des baies de stockage qui correspondent au plus près du besoin pour une application ou un système. Cela est rendu possible par une solution totalement logicielle pour configurer dynamiquement les matériels dans le centre de données. Les ressources présentes sont désagrégées puis reconstruites dynamiquement par le logiciel Liqid Matrix. Cela apporte une flexibilité comme dans le Cloud mais sur les sites de l'entreprise. La solution est particulièrement bien adaptée pour les workloads critiques. Elle permet de plus de configurer des matériels qui n'existent pas sur le marché ou à des prix qui défient les entreprises de les acheter.

Liqid IODirect P2P autorise des liens directs entre les processeurs comme les CPU ou GPU avec une augmentation des performances et en latence par une bande passante plus large. Une déclinaison pour le stockage Liqid GPU Direct Storage avec cette technologie Peer to Peer apporte des améliorations de la performance sur les opérations de stockage.

Il est possible d'accélérer le déploiement par un outil d'orchestration (Slurm, Ansible, VMware vCenter). La solution est appelée à évoluer pour ajouter la possibilité d'orchestrer par des politiques ou règles puis à plus long terme par de l'apprentissage machine.

Spectra Logic ou la gestion de données tout terrain

L'autre grand acteur du marché du stockage sur bande a lui aussi réalisé sa transformation et présente aujourd'hui un panel de produits qui dépasse la vision que l'on pouvait encore avoir de Spectra Logic. Ce portefeuille se compose tout d'abord un logiciel de gestion de cycle de vie du stockage StorCycle qui identifie automatiquement les actifs et leur migration et les préserve et les restaure si nécessaire. Le logiciel se complète de BlackPearl, une solution de NAS et de stockage objet. Pour protéger les données de stockage, de sauvegarde ou d'archivage, le logiciel est adapté pour des rétentions longues comme les données archivées et présente les bandes comme des entités S3 d'AWS. Il peut aussi proposer un stockage S3 sur site pour les entreprises qui le souhaitent. Elles peuvent de plus ajouter une réplication sur un cloud public compatible S3 à la suite de cette opération. Le temps fort de cette rencontre, outre la visite de l'usine de fabrication, a été la présentation des nouveautés sur Spectra Vail, le logiciel de gestion des données multicloud qui permet de regrouper l'ensemble des données éparses sous un seul domaine de nommage global. Cette solution similaire à Glacier S3 peut désormais avoir un accès direct aux bandes en local ou en ligne par des commandes qui imitent Glacier. La solution supporte ObjectLock d'AWS et possède des intégrations directes avec les principaux clouds publics. Il est possible de planifier ou de réaliser le placement des données et leur orchestration par des règles dans le logiciel de cycle de vie et des interfaces de staging. A l'instar de Quantum, Spectra Logic propose maintenant, mais avec une autre approche, des possibilités modernes pour les environnements hybrides. □

B.G

Un nouveau plan

Cegid réalise plusieurs acquisitions

Avec Forward 2026, Cegid lance un nouveau plan stratégique pour les années à venir et annonce plusieurs acquisitions pour étoffer son offre logicielle.

Cloud est le maître mot de la nouvelle stratégie de Cegid. L'éditeur souhaite construire, avec une offre 100 % cloud, un nouveau modèle de relation clients pour susciter plus d'engagement et créer de nouveaux usages. Ces nouvelles solutions innovantes devront représenter 80 % du chiffre d'affaires en 2026 en restant concentré sur cinq marchés : Finance, Ressources Humaines, Expertise Comptable, Retail et Petite entreprise avec pour ambition de faire partie des trois leaders sur chacun de ces marchés. En corollaire, le plan vise à accélérer le développement à l'international, notamment en Europe et poursuivre la politique d'acquisition pour soutenir le développement de Cegid. L'objectif de chiffre d'affaires est de 1,3 milliards de dollars en 2026.

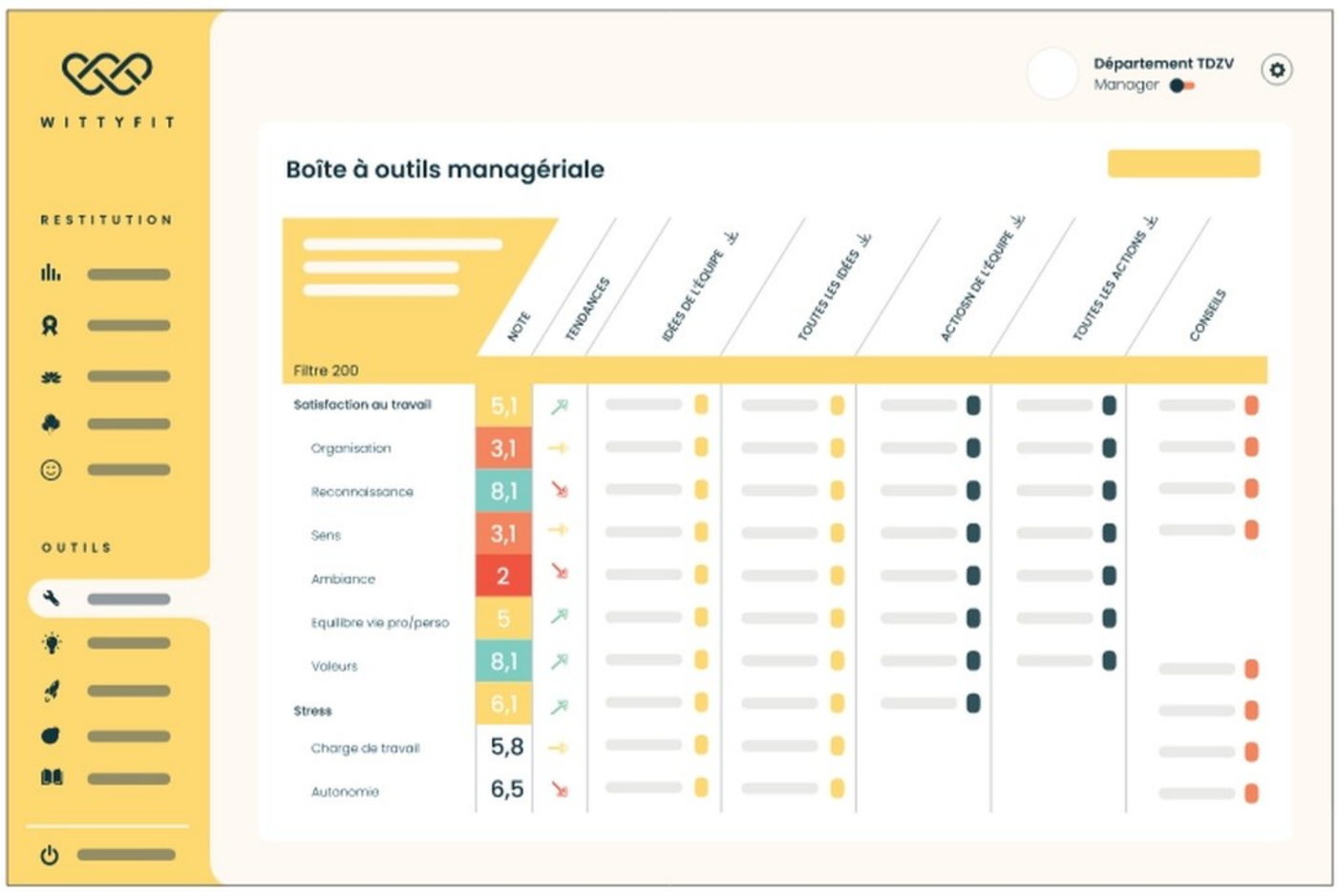
Plusieurs acquisitions

Après 15 acquisitions en 5 ans, Cegid ne ralentit pas le rythme et annonce sa volonté de maintenir une stratégie d'acquisitions ambitieuse. Forte du soutien renouvelé de ses actionnaires Silver Lake et KKR, Cegid compte confirmer sa dynamique de croissance.

Très récemment, l'éditeur a réalisé la reprise de Notilus, une filiale de DIMO software, une solution reconnue sur les dépenses et notes de frais en entreprise. La solution compte plus de 1000 clients dont Acadomia, Atol Les Opticiens, Casino, Groupama, Groupe ADP, Legrand, Rossignol, Groupe Seb, Stellantis, FN Herstal, Ferrovial... Avec cette acquisition, Cegid accélère sa stratégie au service des Directions Financières.

Quelques semaines auparavant, Cegid avait mis la main sur une société britannique, StorIQ. Dédiée à la planification des opérations dans les magasins, cette société vient compléter l'offre Retail de Cegid. Particulièrement adaptée aux enseignes qui possèdent entre 50 - 2 000 magasins, StorIQ compte déjà une cinquantaine de clients, parmi lesquels figurent de nombreuses marques prestigieuses telles que Hugo Boss, Clarks, Douglas, Marks & Spencer International, Mountain Warehouse, Nespresso... L'acquisition de StorIQ permet à Cegid de renforcer son expertise autour du point de vente.

Dans le même temps, Wittyfit était tombé dans l'escarcelle de Cegid pour compléter la solution de gestion des talents et RH de Cegid. Wittyfit permet aux organisations de mesurer, analyser et agir sur la satisfaction au travail, l'engagement et le suivi des collaborateurs pour piloter la performance collective, à partir d'une plateforme SaaS unique. La plateforme Wittyfit vient ainsi compléter le portefeuille HCM de Cegid, dont la gestion des talents Cegid Talentsoft. En captant les ressentis induits, par exemple, par les nouvelles conditions de travail : télétravail, flex office, mobile working, externalisation de certaines fonctions, les Directions des Ressources Humaines et les managers peuvent comprendre et agir sur les leviers ayant des conséquences sur le capital humain pour améliorer durablement la performance de l'entreprise. Wittyfit est utilisée, à la fois, par les collaborateurs – pour répondre de façon confidentielle à des enquêtes et proposer des suggestions –, par les managers – pour transformer les idées en actions concrètes et assurer le suivi –, et par les directions des Ressources Humaines – pour collecter les KPIs, effectuer des analyses et piloter la performance collective. Plug and Play, Wittyfit compte déjà 120 000 utilisateurs, parmi lesquels les équipes de Cegid, qui figurent parmi ses clients et continueront d'utiliser sa solution. ☐ **B.G**



Un écran pour les managers dans Wittyfit.

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

COUPLAGE

Recevez chaque mois L'Informaticien (10 numéros par an) et chaque trimestre L'Info CyberRisques (4 numéros par an) et accédez également aux versions numériques des dernières publications.

1 AN FRANCE : 99 €
2 ANS FRANCE : 179 €

Accès aux versions numériques seules des deux publications.

1 AN numérique : 75 €
2 ANS numérique : 135 €

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 €
COUPLAGE AVEC INFOCYBERISQUES : 59,40€

Europe

FIC 2022 : la fin d'une époque

Du 7 au 9 juin se tenait à Lille le FIC, grand'messe française de la cybersécurité. Cette édition était marquée par le contexte international, ou plus exactement, la guerre en Ukraine. Avec un air de fin, celle de l'innocence européenne, et la fin de l'ANSSI sauce Poupard.

Malgré le très récent scandale qui éclabousse Avisa Partners, co-organisateur de l'événement, le Forum International de la Cybersécurité a connu une édition 2022 faste. 14 000 visiteurs se sont pressés au Grand Palais de Lille du 6 au 8 juin, déambulant parmi les quelque 550 exposants. Le lieu est comble, la circulation parfois compliquée. D'autant que les événements connexes se sont multipliés et attirent, eux aussi. OSINT, identité, sécurité des systèmes industriels, protection des consommateurs, European Cyber Cup… eux aussi ont fait le plein de visiteurs. Une approche en mode « festival », selon Guillaume Tissier, qui devrait se poursuivre, avec l'organisation d'un événement connexe sur la santé au FIC 2023. *« Toutefois, l'objectif n'est pas d'avoir 200 événements connexes »* avertit le patron de CEIS, qui insiste sur les points de connexion entre le FIC et ses petits frères. Par ailleurs, Guillaume Tissier nous indique que la prochaine édition, programmée pour avril 2023 sera probablement centrée sur le thème du *« premier et dernier kilomètre de la cybersécurité, l'utilisateur »*. Pourtant, le FIC revient dès novembre 2022. Mais pas à Lille : une édition est organisée au Québec, un FIC Amérique du Nord, *« qui ne sera pas calqué non plus sur ce qu'on fait en France »*.

L'Ukraine sur toutes les lèvres

Pour autant, malgré le bouillonnement, ce FIC avait des airs de fin d'une époque. D'abord, parce qu'il marque, symboliquement, la fin de la présidence française de l'Union européenne. L'Europe occupait ainsi le devant de la scène, d'où le thème de cette édition 2022 : *« Shaping Europe's Digital Future »*. C'était également le titre de la séance inaugurale, à laquelle participaient Marie-Laure Denis, présidente de la CNIL, Michiel Boots, du ministère néerlandais de l'Économie et du Climat ainsi que Jean-Noël de Galzain, président d'Hexatrust et patron de Wallix. Suivait, le lendemain, une conférence sur la puissance normative de l'UE. Et, sans surprise, tous n'ont pas manqué de faire le lien avec l'invasion de l'Ukraine par la Russie. Une guerre qui rebat les cartes, y compris au sein de l'Union. *« Le temps de l'innocence de l'Europe est terminé »* a ainsi asséné en conférence de presse Margaritis Schinas, commissaire européen.

« Le conflit en Ukraine n'a pas provoqué d'importants dommages collatéraux, mais il ne faut pas minimiser pour autant » nous explique Yves Verhoeven, Sous-directeur Stratégie de l'ANSSI, citant notamment l'attaque visant KASAT, attribué à la Russie. *« Ça nous donne à réfléchir pour mieux se projeter vers l'avenir »*. L'idée d'une Europe troisième voie entre Etats-Unis et Chine n'est pas neuve, mais ils étaient nombreux, dans les allées, à parler d'une « première voie ». Guillaume Tissier supporte par exemple l'idée d'une « Europe puissance », à grands renforts d'outils de politique industrielle et de souveraineté. Plus question de chercher à concilier la vache et le chou, l'UE passe à l'offensive, y compris sur le terrain cyber.

L'Europe normative

Pour Yves Verhoeven, *« la Présidence française de l'Union européenne a été particulièrement ambitieuse en matière de souveraineté numérique »*. Le schéma de certification européen relatif à la sécurité du Cloud ou encore l'accord politique trouvé autour de la directive NIS2 s'en veulent les parfaits exemples. Le texte va allonger la liste des OSE (opérateurs de services essentiels), englobant notamment des acteurs publics ainsi que des ESN. Selon le patron de l'ANSSI, Guillaume Poupard, *« le nombre d'OSE va être multiplié par dix »*. Et la France a d'autant plus raison de s'en féliciter qu'elle a défendu sa position, se fondant notamment sur SecNumCloud, au niveau européen. Guillaume Poupard, en sa conférence de presse, mettait d'ailleurs l'accent sur la nécessité d'Etats forts. *« La sécurité est un sujet national avant d'être supranational »* assure-t-il, précisant qu'il n'est pas question de *« tourner le dos à l'Europe »*.

Mais, « au quotidien », le patron de l'ANSSI *« parle peu de souveraineté »*. Il lui préfère la maîtrise du système d'informations et des données. *« Il y a eu une sorte de perte de maîtrise à un moment, parce que le numérique était conçu comme une fonction de soutien et sous-traité. Là, on revient en arrière : la fonction numérique est remontée très haut au niveau de l'organisation des entreprises. Les questions de souveraineté ne peuvent se poser que par ce biais-là. Ce que je demande à chacun, c'est de faire cette analyse coûts-risques »*.

Poupard, dernière

Le temps du bilan, c'était également pour Guillaume Poupard, qui participait à son dernier FIC en qualité de directeur de l'ANSSI. Mais point de « discours d'adieu », le futur ex a préféré diviser son allocution entre bilan de ses huit années à la tête de l'agence et conseils à ce successeur dont on ignore encore l'identité. À cet inconnu, Guillaume Poupard a dispensé quelques conseils… ou plus exactement a laissé une liste de courses. Il appelle à lancer une *« campagne nationale de sensibilisation »* à la cybersécurité, souhaitant avoir *« 5 minutes de temps de cerveau de chaque Français »* sur les sujets basiques de la sécurité et sur Cybermalveillance.gouv. Guillaume Poupard entend également que l'ANSSI se dirige vers une « cybersécurité de services », à l'image de son homologue anglaise. Il veut que la France « se fasse respecter » en matière de cyber, aussi bien sur le volet défensif qu'offensif, et porte *« une parole forte au niveau politique »*. *« J'ai la satisfaction de laisser une ANSSI reconnue par les autorités »* dira plus tard le principal intéressé devant les journalistes. *« Si je devais donner un conseil [à son successeur], ce serait de conserver ce déséquilibre permanent qui fait fonctionner l'ANSSI. Quand on arrête de pédaler, ça ne fonctionne plus »*.

Au-delà des souhaits, l'ANSSI a-t-elle les moyens des ambitions de son presque ex-patron ? Pour Yves Verhoeven, *« l'ANSSI n'a pas vocation à tout faire »*. Sur les cinq ans écoulés, l'agence a crû suivant une courbe régulière, jalonnée ces deux dernières années par le plan de relance. Sur les opérations de cyberdéfense, entre 14 et 20 par an, *« nous sommes dans une moyenne qui correspond à nos capacités »* précise le sous-directeur Stratégie de l'ANSSI. *« Nous sommes donc amenés à faire des choix, à prioriser, en lien avec le privé et des compétences étatiques tierces »*. Car l'ANSSI n'est pas seule. On connaît déjà bien l'Acyma, Cybermalveillance.gouv, qui s'occupe des particuliers, des TPE et des petites collectivités. Sont venus s'ajouter très récemment ces fameux CSIRT régionaux, dont quelques conventions ont été signées lors de ce FIC. *« L'idée, c'est de multiplier ces structures car leur rapport coût-efficacité est excellent »* indique Guillaume Poupard. Outre les CSIRT régionaux, le directeur de l'ANSSI cite des CSIRT sectoriels. *« On est en train de mailler le territoire et les secteurs »* souligne-t-il. Et réduire le nombre des oubliés de la cybersécurité. □

Guillaume Périssat

Recherche et Défense

Deuxième tournée pour l'Accélérateur Hexatrust

Après Patrowl, ProHacktive et CryptoNext, trois nouvelles jeunes pousses font leur entrée dans l'accélérateur de l'association. L'occasion de faire le bilan de la première promotion et de découvrir Continus.io, Snowpack et Cyber-Detect.

En 2021, Hexatrust lançait son Accélérateur. Avaient été sélectionnées pour ce programme trois startups spécialisées en cybersécurité : Patrowl, ProHacktive et CryptoNext. Pendant un an, ces jeunes pousses ont été accompagnées et conseillées par des parrains, deux chacune. À l'époque, Edouard de Rémur, co-fondateur de Oodrive, nous expliquait que *« des startups postulaient chez Hexatrust, mais ne remplissaient pas les critères d'adhésion »* et qu'il était *« dommage de perdre le lien avec ces entreprises, car c'est ici que se fait l'innovation »*. D'où ce programme d'accélération lancé par l'association, réunissant des acteurs français (et européens) de la cybersécurité. Au menu, coaching, principalement sur les volets marketing et commerciaux, visibilité et mise en relation, les trois « piliers » de l'Accélérateur.

Douze mois plus tard, Patrowl, ProHacktive et CryptoNext sortent de l'accélérateur, et trois nouvelles startups intègrent le programme. *« Le bilan est très positif »* nous relate désormais Edouard de Rémur. *« Cette année a été très instructive : nous avons vu les accélérés assez régulièrement, le format s'est montré efficace »* se réjouit-il. Levée de fonds, marketing produit et visibilité sont les principaux aspects qui ont été travaillés entre parrains, membres d'Hexatrust et cette première promotion. *« Leur premier besoin, c'était le financement, c'est le premier sujet remonté par l'ensemble des accélérés »* poursuit le cofondateur d'Oodrive, et parrain avec Stéphane de Saint-Albin (Ubika) de Patrowl. *« Toutefois, chacun avait des besoins différents en termes de visibilité, de marketing, de business. Ainsi, ProHacktive a notamment travaillé sur les canaux de distribution de sa solution, quand CryptoNext a développé des partenariats technologiques avec d'autres membres d'Hexatrust »*.

Rencontres

On notera, en outre, que les trois jeunes pousses sont toutes, à leur sortie de l'accélérateur, membres d'Hexatrust. Si, l'an dernier, Edouard de Rémur avait indiqué que la participation au programme ne valait pas une adhésion automatique à l'association, *« les règles sont faites pour être changées »* glisse-t-il sur le stand d'Oodrive au FIC 2022. *« Les accélérés sont de facto membres d'Hexatrust et les six premiers mois de cotisation leur sont offerts »*. Le FIC a également été l'occasion pour l'association de présenter la deuxième promotion de son accélérateur. Comme pour leurs trois prédécesseurs, ces trois startups ont été sélectionnées sur une vingtaine de candidatures, *« plus que lors de la précédente édition »* souligne Edouard de Rémur. Six candidats ont été retenus et ont ensuite participé au Pitch Day, le 21 avril, au terme duquel trois ont rejoint cette seconde promotion. Il s'agit de Continus.io, Snowpack et Cyber-Detect.

Tous trois seront accélérés de la même manière que Patrowl, CryptoNext et ProHacktive, avec peu de différences quant au programme. *« Ce que nous allons améliorer pour la prochaine promotion, c'est l'organisation de plus de rencontres physiques entre accélérés »* précise Edouard de Rémur. Avec des retours d'expérience de la première promotion, qui rencontrera ses successeurs courant juillet. De même, Edouard de Rémur souhaite *« plus d'intégrations avec les membres d'Hexatrust, pour des questions de visibilité et de liant humain »*. Les restrictions liées à la crise sanitaire ayant, pour l'heure, pris fin, ces réunions présentielles devraient être plus fréquentes, et plus aisées à organiser. Autre nouveauté, Hexatrust conservera un lien avec les trois autres jeunes pousses passées au Pitch Day mais non retenues. *« Ce serait dommage de ne pas faire plus de liant avec eux »* insiste le confondateur d'Oodrive. □

Guillaume Périssat

« Le financement, c'est le premier sujet remonté par l'ensemble des accélérés »

Edouard de Rémur, cofondateur d'Oodrive.

Qui sont les trois startups de la deuxième promotion de l'Accélérateur Hexatrust ?

Continus.io

Fondé en 2020, Continus.io est spécialisé dans le DevSecOps. Son produit rassemble en une seule plateforme SCA (Software Composition Analysis), SAST (Static application security testing) et DAST (Dynamic application security testing) de sorte à sécuriser les pipelines DevOps et évaluer en continu la sécurité du code source, des composants tiers, des conteneurs et des API. Pour les profanes, la partie SCA identifie les risques dans les composants open source tiers intégrés aux applications, les tests statiques analysent le code source à la recherche de vulnérabilités et les tests dynamiques sont l'équivalent de tests en boîte noire afin d'examiner l'exécution et le comportement des applications et des API, pratique pour repérer, sur l'aspect Ops, les erreurs de configuration. La jeune pousse compte pour l'heure trois salariés, dont les deux co-fondateurs, Tarik El Aouadi et Azziz Errime, respectivement CEO et CTO.

Cyber-Detect

Ce spin-off du LORIA (CNRS, Inria, Université de Lorraine) s'est fondé sur dix années de recherches au sein du Laboratoire de Haute Sécurité pour mettre au point une technologie de détection des programmes malveillants. Baptisée GORILLE, celle-ci repose sur l'analyse morphologique, qui permet d'identifier un binaire non plus par une signature, mais par une cartographie de son comportement, dite *« graphe de flot de contrôle »*. La solution développée par Cyber-Detect déconstruit ainsi le code du programme malveillant, contournant ainsi les techniques d'obfuscation, tout en s'avérant capable de repérer des malwares encore inconnus, ou des variants d'une souche connue. Cette jeune entreprise, créée en 2017 par Jean-Yves Marion et Guillaume Bonfante, compte parmi ses premiers clients rien de moins que la Direction Générale de l'Armement, qui a d'ailleurs attribué ce nom de GORILLE à la technologie de Cyber-Detect.

Snowpack

Cette toute jeune pousse a fêté son premier anniversaire en mai 2022. Spin-off de l'institut Carnot CEA, elle compte quatre cofondateurs dont Frédéric Laurent et Baptiste Polvé, et six salariés au total, bien qu'elle prévoie une dizaine de recrutements d'ici à la fin de l'année. Sa mission, son sacerdoce : rendre les données invisibles en ligne. Son approche consiste à fragmenter les données (ces fragments étaient qualifiés de flocons de neige, d'où ce nom de Snowpack), et à les faire circuler sur des circuits créés anonymement. Accéder à l'information nécessite alors d'identifier tous les fragments complémentaires ainsi que les liens entre eux. Snowpack promet une résistance aux outils de surveillance de masse des réseaux, une diminution drastique de la surface d'attaque et surtout s'éviter de recourir à un tiers de confiance. Car, pour la jeune pousse d'Orsay, le mécanisme d'échange de clés publiques reste faillible et se repose trop sur le principe de confiance dans l'infrastructure PKI et/ou les fournisseurs de technologie.

Snowflake Summit 2022

Snowflake transforme aussi les applications

Du 26 au 29 juin dernier, Snowflake a tenu sa conférence mondiale au Caesar's Forum. 9000 personnes ont fait le déplacement et 11 500 ont suivi virtuellement la conférence.

Le président-directeur général de Snowflake, Frank Slootman, et le cofondateur et président des produits de Snowflake, Benoît Dageville, ont donné le coup d'envoi de l'événement en présentant les sept piliers d'innovation clés qui positionnent Snowflake sur le marché. Le thème principal était que l'éditeur a d'abord transformé massivement l'analyse, puis la collaboration, et maintenant le développement d'applications avec le Data Cloud.

Tout pour les développeurs

Le Native Application Network, annoncé en preview privée lors de la manifestation, donne aux développeurs la possibilité de créer des applications et les monétiser sur la Snowflake Marketplace. Les utilisateurs pourront installer et exécuter ces applications en toute sécurité, directement dans leurs instances Snowflake, réduisant ainsi le besoin de déplacer les données. Avec ce framework, il est possible de créer des applications utilisant les fonctionnalités de Snowflake telles que les procédures, les fonctions définies par l'utilisateur (UDF) et les fonctions de table définies par l'utilisateur (UDTF). Des fonctionnalités telles que l'intégration de Streamlit pour le développement d'interfaces client interactives et des fonctions de télémétrie, notamment des événements et des alertes pour la surveillance et le dépannage, sont également en cours de développement. Les developpeurs ont aussi la possibilité de poster ces applications sur la marketplace de Snowflake.

Autre annonce du Summit, Snowflake supporte maintenant Python avec SnowPark for Python. La solution est en preview publique accessible aux scientifiques, ingénieurs de données et développeurs d'applications. Grâce à une sandbox Python hautement sécurisée, Snowpark for Python fonctionne sur la même infrastructure de calcul que les pipelines Snowflake et les applications écrites dans d'autres langages. Le logiciel bénéficie ainsi des mêmes avantages en termes d'évolutivité, d'élasticité, de sécurité et de conformité que ceux auxquels les développeurs sont habitués lorsqu'ils utilisent Snowflake. Les développeurs ont maintenant l'opportunité de rationaliser et de moderniser leur architecture data en consolidant leur traitement de données basé sur Python dans Snowflake en utilisant Snowpark.

Les data scientists ne sont pas oubliés

La prise en charge des données en streaming pour éliminer les frontières entre les pipelines de streaming et de traitement par lots avec Snowpipe Streaming, actuellement en preview privée, pour l'ingestion sans serveur de données en streaming, et les tableaux matérialisés, actuellement en développement, simplifient la transformation des données en streaming de manière déclarative. Tables Iceberg dans Snowflake, actuellement en développement, autorise aux utilisateurs de travailler avec Apache Iceberg, un format de

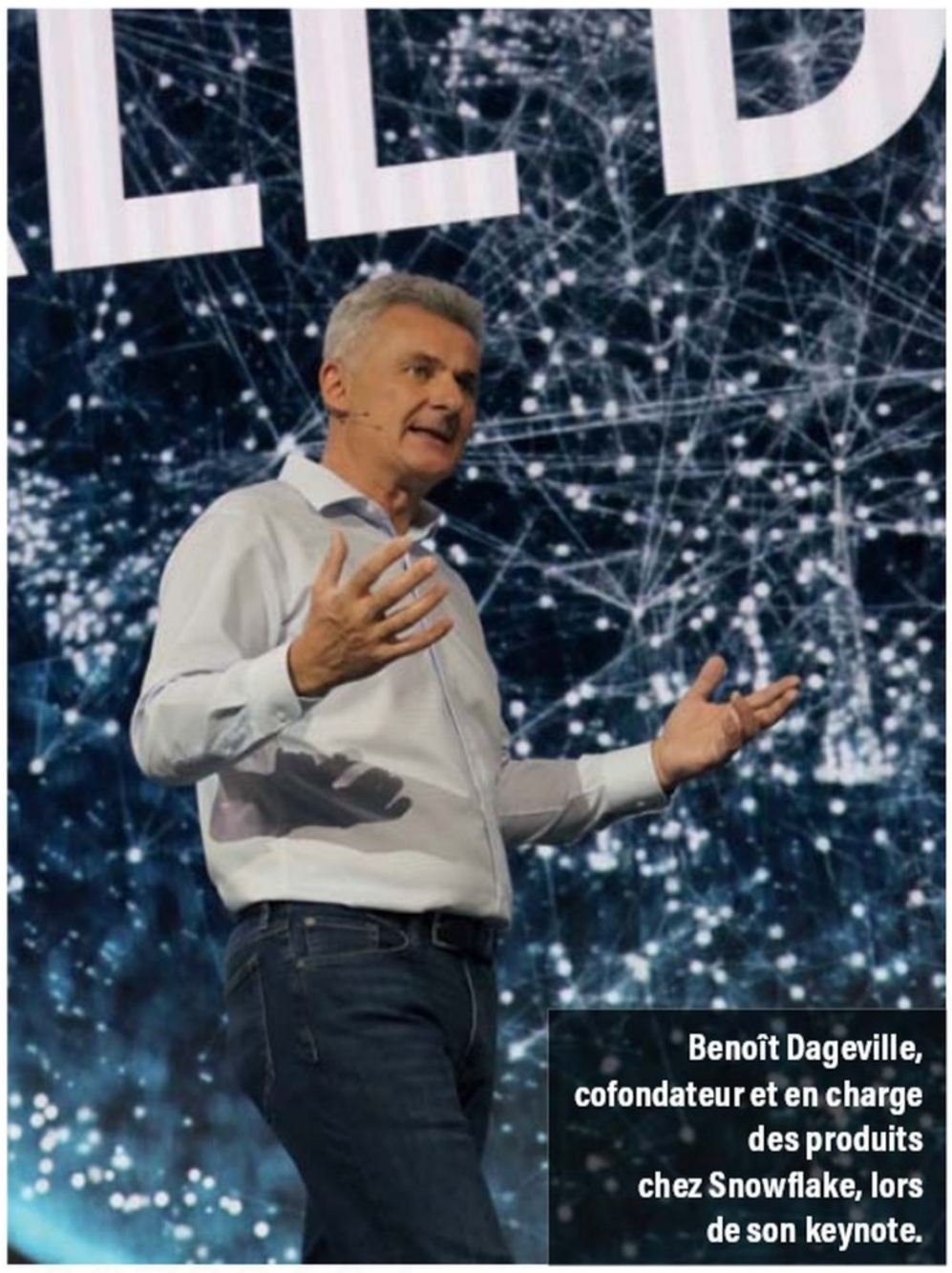
table ouvert populaire, et ce, dans un stockage externe tout en profitant de la facilité d'utilisation, des performances et de la gouvernance cohérente de la plateforme Snowflake, simplifiant ainsi la gestion globale des données et permettant une flexibilité architecturale. External Tables for On-Premises Storage, actuellement en preview privée, permet aux utilisateurs d'accéder à leurs données dans des systèmes de stockage sur site comme Dell Technologies, Pure Storage et plus encore, à partir de Snowflake, afin qu'ils puissent bénéficier de l'élasticité du Data Cloud sans déplacer ces données.

Unistore unifie les données transactionnelles

Ce nouveau workload étend les capacités de Snowflake et offre une approche moderne pour travailler avec des données transactionnelles et analytiques dans une seule et même plateforme. Dans le cadre d'Unistore, Snowflake lance les Hybrid Tables, qui offrent des opérations rapides sur une seule ligne et permettent aux clients de créer des applications commerciales transactionnelles directement sur Snowflake. Les tables hybrides, actuellement en preview privée, permettent aux clients d'effectuer des analyses rapides sur les données transactionnelles pour un contexte immédiat et de joindre les tables hybrides aux tables Snowflake existantes pour une vue holistique de toutes les données. Unistore et Hybrid Tables permettent aux clients de créer des applications transactionnelles avec la même simplicité et les mêmes performances que celles auxquelles ils sont habitués avec Snowflake, ainsi qu'avec une approche unifiée de la gouvernance et de la sécurité des données.

Une nouvelle possibilité pour les données de sécurité

A la veille de son événement, Snowflake a lancé une nouvelle possibilité sur sa plate-forme pour ses clients en liaison avec ses partenaires autour de la sécurité et de l'observabilité.



Benoît Dageville, cofondateur et en charge des produits chez Snowflake, lors de son keynote.

Il est désormais possible pour ces outils tiers d'utiliser la plate-forme de Snowflake pour traiter nativement les logs structurés, semi-structurés et non structurés. Les clients sont en mesure de stocker efficacement des années de données volumineuses, d'effectuer des recherches avec des ressources informatiques évolutives à la demande et d'obtenir des informations à l'aide de langages universels tels que SQL et Python. Les entreprises peuvent ainsi utiliser la plate-forme comme une source unique pour les données d'entreprise et de sécurité. Les équipes de sécurité obtiennent ainsi une visibilité unifiée de leur posture de sécurité, éliminant les silos de données sans coûts prohibitifs d'acquisition ou de conservation des données. Au-delà de la détection et de la réponse aux menaces, le workload Cybersécurité prend en charge un large spectre de cas d'utilisation, notamment la conformité à la sécurité, la sécurité du cloud, l'identité et l'accès, la gestion de la vulnérabilité... Hunters, Securonix et Panther Labs sont des exemples de partenaires ayant choisi Snowflake comme backend pour leurs services de sécurité. Ils fournissent les outils de sécurité qui s'appuient sur la plate-forme de Snowflake. □

B.G

LES 7 PILIERS DE LA PLATE-FORME

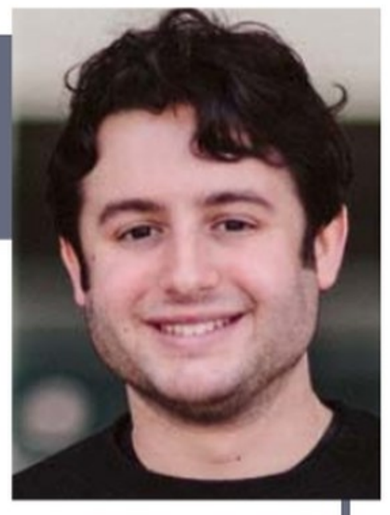
Benoît Dageville a longuement évoqué lors de son keynote les 7 attributs qui sous-tendent aujourd'hui les plates-formes de données modernes comme Snowflake. La plate-forme doit pouvoir accueillir et traiter toutes les données quels que soient leurs types, données ou autres attributs. Elle doit être aussi toujours disponible pour exécuter toutes les charges et ce quel que soit là encore le nombre de charges et que les données puissent être partagées. Le Cloud est d'ailleurs là pour apporter l'élasticité nécessaire. Benoît Dageville, dans une interview, étiquetait Snowflake comme un « hypercloud » qui diffère du multicloud en décorrélant la plate-forme et apportant une véritable globalité et non juste la possibilité d'exécuter la plate-forme dans les différents clouds publics, apportant une vision globale et unique sur les données sur la plate-forme. Dès le début, Snowflake a voulu que les opérations et l'utilisation de la plate-forme soient simples avec une conception qui ôte au maximum les frictions possibles. Les derniers ajouts la rendent programmable et le partage de données autorise une collaboration riche. La plate-forme apporte aussi une gouvernance et de la sécurité à la fois pour protéger les données et aussi respecter l'aspect privé autour des données.

Expérience Utilisateur

Figma, le Google Docs de l'UX Design

L'entreprise américaine née en 2012 avec ni plus ni moins que l'ambition de révolutionner la conception d'interfaces, vient de poser ses valises en France. L'occasion de tirer le portrait de cette société qui se pose en concurrente d'Adobe, Sketch, mais aussi de Miro et de (dans une moindre mesure) Klaxoon.

Reste-t-il un éditeur qui ne place pas « l'utilisateur au centre », chez qui les solutions ne sont pas « user-centric » ? Sans doute, mais il se cache bien. Plus qu'un simple argument marketing, l'expérience utilisateur est devenue, en l'espace de quelques années, une tendance de fond, consistant entre autres à penser les interfaces pour que l'utilisateur puisse, *a minima*, trouver facilement les fonctionnalités et les informations dont il a besoin. Et ce qui semblait valoir pour le B2C, vaut désormais autant pour le B2B. *« L'expérience utilisateur est un différentiateur »* nous expliquait Dylan Field, CEO et cofondateur de Figma, alors de passage à Paris. En effet, cette société américaine s'est, mi-juin, installée dans l'Hexagone, un marché particulièrement porteur pour l'entreprise. Car, si son nom ne vous dit rien, il évoquera certainement quelque chose chez Thales, la RATP, la Société Générale, Qonto, Carrefour, Doctolib, Canal+ ou encore Decathlon. Il ne s'agit ici que des clients français de Figma, dont les solutions sont également utilisées par Rakuten, Google, Uber, Airbnb ou encore Microsoft. Bref, pour peu que vous ayez déjà visité les sites web ou utilisé les applications de quelques-unes de ces entreprises, vous avez déjà eu du Figma dans les mains. Plus ou moins.

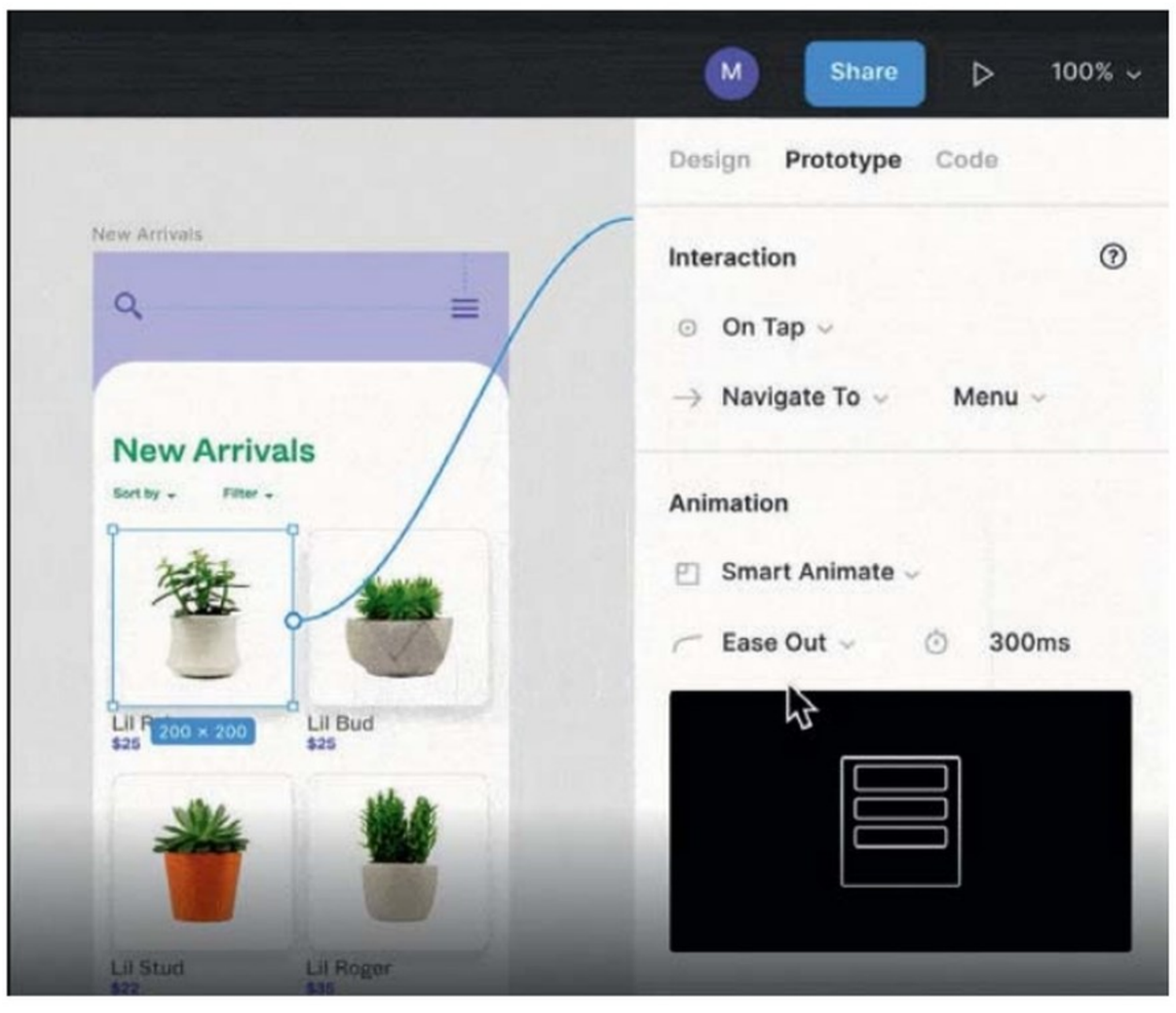


Dylan Field, CEO et cofondateur de Figma.

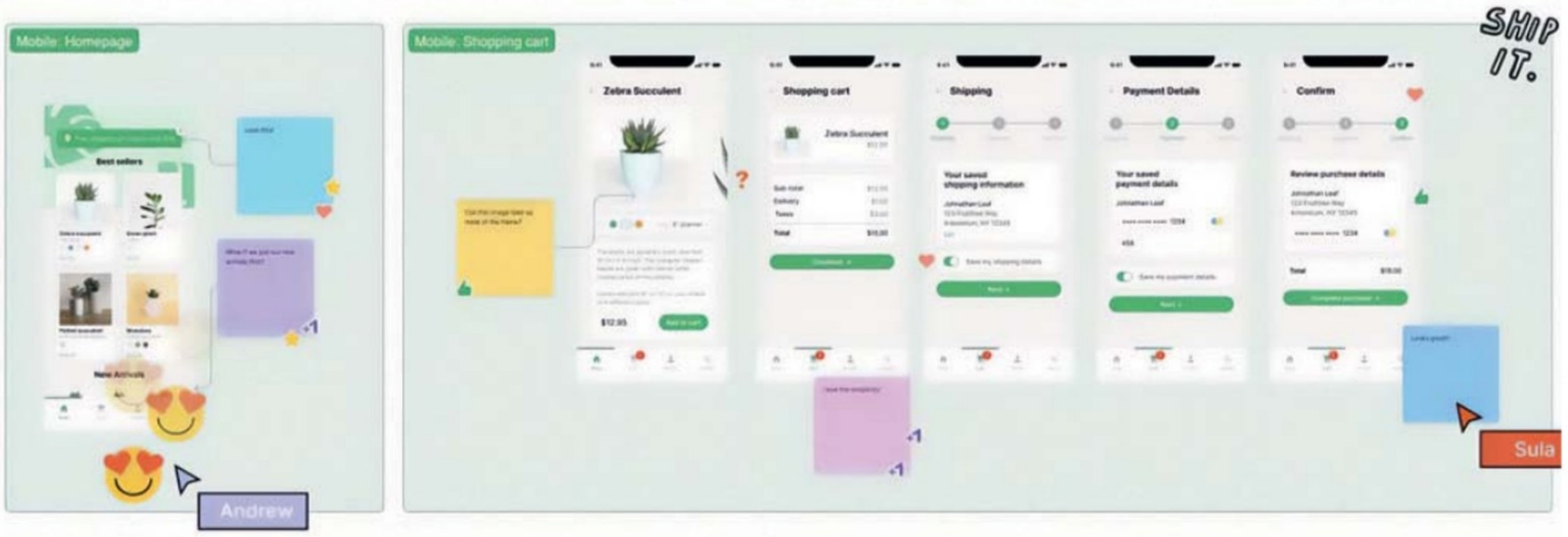
« L'expérience utilisateur est un différentiateur. »

De bout en bout

L'éditeur propose en effet une solution de conception d'interfaces et d'expériences utilisateur. Pendant longtemps, les designers devaient, pour concevoir des maquettes d'applications mobiles ou de sites web, recourir à des outils qui n'étaient pas prévus à cet effet, par exemple Illustrator ou Photoshop. Puis sont arrivées de nouvelles solutions, Adobe XD ou Sketch, pour ne citer qu'eux. Figma propose peu ou prou les mêmes fonctionnalités de design et de prototypage que ses illustres concurrents (mises en page automatiques, tests, librairies, templates, prototypage interactif, composants, *etc.*). À noter que, contrairement à Sketch, Figma est tout-en-un : il ne requiert pas de passer par des outils tiers, tels qu'Illustrator ou InVision, pour réaliser l'ensemble de la chaîne de conception d'interfaces, y compris la création de vectoriels ou l'examen du code. En effet, ainsi que nous l'explique Yuhki Yamashita, VP Produit de Figma, l'outil ne se destine pas exclusivement aux designers d'UI/UX. *« La majorité des collaborateurs dans les entreprises de design ne sont pas des designers »* rappelle-t-il. Les développeurs sont donc les bienvenus sur la plateforme, d'autant que celle-ci emprunte largement au développement web et à la programmation.



Ainsi, son Design System n'est pas sans rappeler un repository GitHub en termes de versioning, avec des branches principales et secondaires pour un même fichier, permettant d'effectuer une révision de tel ou tel élément du fichier sur une version secondaire avant de la fusionner à la branche principale et d'y appliquer les modifications. En outre, les



En lançant FigJam, Figma ajoute à son éventail d'outils un tableau blanc, directement en concurrence avec le poids lourd du secteur, Miro.

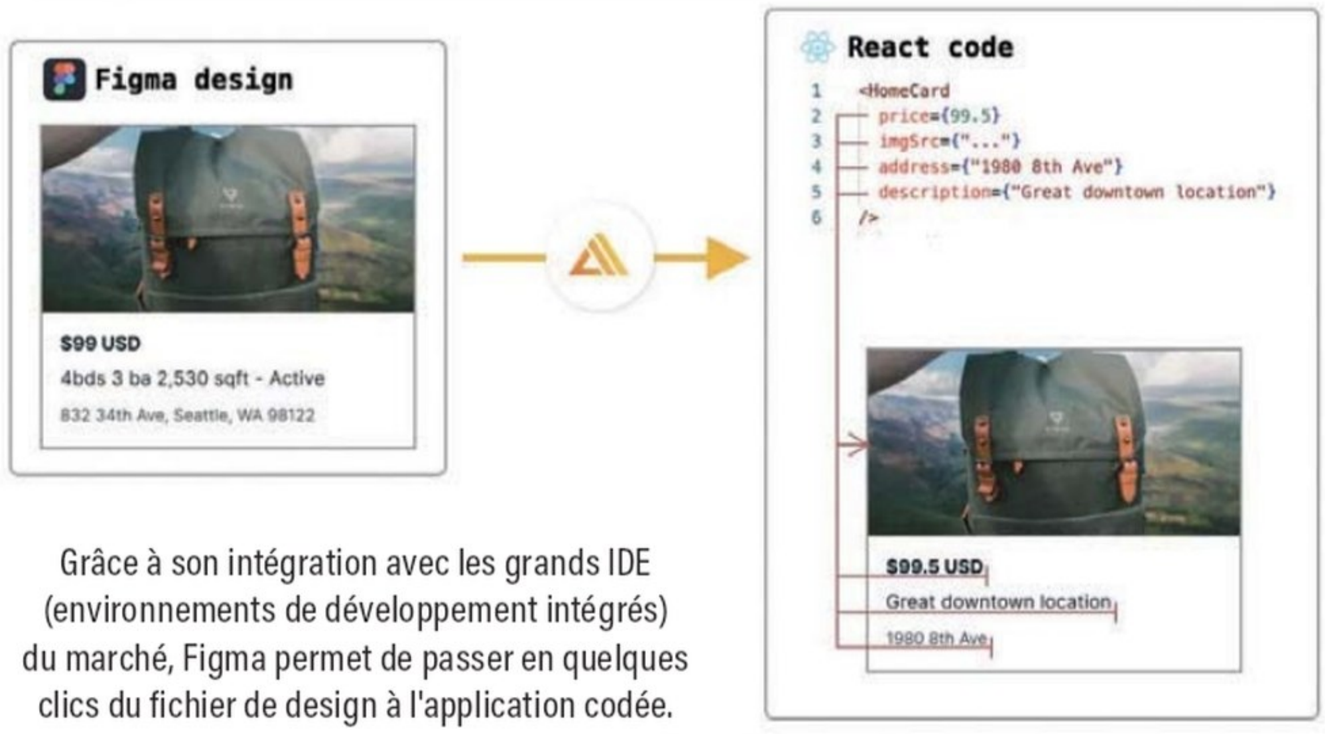
composants dans Figma se veulent plus flexibles que chez la concurrence, avec la possibilité de personnaliser les propriétés de chaque composant et de les combiner. Ce qui permet accessoirement de réduire le nombre de composants de l'UI, un écueil pour bon nombre de concepteurs. L'éditeur traite donc l'ensemble de la chaîne, du prototypage à la livraison en passant par la création graphique et le test. Ce qui n'exclut pas les intégrations, relativement nombreuses. *« Nous pensons que vous pouvez tout faire sur Figma, mais nous sommes conscients que nos clients ont pu investir dans d'autres logiciels. Donc nous nous appuyons sur une collection d'APIs »*. On pensera notamment aux intégrations avec Jira ou Asana, permettant d'intégrer les designs aux projets et aux canaux de discussions. Contrairement aux captures d'écran, les intégrations dynamiques reflètent les changements apportés au fichier de design en temps réel. Des intégrations avec Power Apps Express Design chez Microsoft, Amplify Studio d'AWS ou encore Material du côté d'Android viennent faciliter le passage du fichier de design à l'application ou au site. Ajoutons à cela de nombreux plugins développés par la communauté pour automatiser un certain nombre de tâches, de la mise à jour d'une carte à la traduction de l'anglais au français, en passant par l'adaptation automatique de contenus visuels.

Collaboratif

Poussant le vice plus loin encore, l'entreprise a récemment lancé FigJam, un outil de tableau blanc qui se pose en concurrent à Miro ou encore au Français Klaxoon. Car, c'est bien là le principal avantage de Figma sur ses homologues, *« tout est dans le cloud »*, explique Yuhki Yamashita. *« Figma est conçu pour être accessible depuis le navigateur »* ajoute-t-il, contrairement à Adobe Xd, qui oblige d'avoir l'application en local. Sketch a bien tenté de proposer une application web, mais celle-ci est affligée de nombreux bugs. Chez Figma, on veut mériter ce titre de Google Docs de l'UX. *« Il suffit de cliquer sur un lien pour se retrouver sur le fichier de design »* indique le VP Produit. Puisque l'outil est entièrement en ligne, les fonctions collaboratives et de partage de documents sont centrales dans Figma. Il est ainsi possible de partager un fichier de design au moyen d'un simple lien, de travailler à plusieurs et en même temps sur un même document, d'annoter, de commenter d'afficher les versions antérieures ou les modifications effectuées par un collaborateur en particulier, de marquer des composants avec des autocollants. Le tout en temps réel, là où Adobe Xd, qui permet certes de collaborer à plusieurs autour d'un fichier, contraint l'utilisateur à rafraîchir le fichier après chaque modification.

Tels sont les principaux arguments qui ont permis à Figma de conquérir le marché de l'UX Design et qui favorisent son expansion à l'international. D'où cette très récente ouverture d'un bureau en France, où Figma revendique être utilisé par près de la moitié du CAC 40. Même dans l'Hexagone, les grandes entreprises *« se tournent de plus en plus vers l'UX, peu importe leur cœur de métier »*. C'est pourquoi, aux yeux du CEO de Figma, *« le nombre de designers, mais aussi de Product owners, augmentent dans les entreprises »*. Reste à convaincre ceux qui sont supposés avoir la main sur l'informatique en entreprise, les DSI. Pour Yuhki Yamshita, le meilleur argument reste cette dimension cloud, puisque *« le lien de partage offre la possibilité de révoquer les accès, d'avoir une visibilité sur qui ou quoi utilise la plateforme, qui a accès à la plateforme. C'est bien mieux que l'envoi de fichiers en pièce jointe de mail »*. Et si la sécurité n'a, jusqu'à présent, *« jamais été un problème »* pour Figma, l'entreprise compte réfléchir à ce sujet *« à mesure que le produit évolue »*. □

Guillaume Périssat



Grâce à son intégration avec les grands IDE (environnements de développement intégrés) du marché, Figma permet de passer en quelques clics du fichier de design à l'application codée.

Vers le Metavers ?

Comment Novaquark fait vivre 30 000 utilisateurs sur un seul *shard* AWS

Éditeur du MMORPG Dual Universe, Novaquark a développé des technologies que l'on pourrait bien retrouver un jour dans les Metavers dont sont friands les analystes et les médias actuellement. Focus sur l'architecture d'un jeu massivement multijoueur en environnement ouverts

Les fans de space opera et d'univers persistant ont de nombreux jeux pour assouvir leur passion. Depuis Avorion, Mass Effect, Star Trek Online, Eve Online ou encore Elite Dangerous, de nombreux jeux réunissent des dizaines de milliers de joueurs. Sur ce marché ultra concurrentiel, le studio et éditeur français Novaquark propose Dual Universe, un MMORPG (Massively Multiplayer Online Role Playing Games) qui met notamment en œuvre une technologie de Voxel (pixels 3D) originale. Celle-ci permet aux joueurs de créer leurs propres objets, y compris des structures de grandes dimensions comme des vaisseaux. Cette plateforme de jeu est le fruit de 7 années de développement.

L'éditeur a fait parler de lui en 2016 avec une campagne Kickstarter qui lui avait permis de lever près de 566 000 € auprès de 8 166 contributeurs. Un gros succès qui a permis à la start-up de convaincre des investisseurs externes à soutenir le projet. Un an après cette levée le fond, une version pre-alpha était ouverte aux backers du projet. Depuis 2 ans, le jeu est passé en béta et il est accessible à davantage de joueurs. Selon Guillaume Gris, CTO de Novaquark, *« le jeu est aujourd'hui stable. Le serveur est ouvert à plusieurs dizaines de milliers de joueurs et se prépare à sortir de la phase beta. »*

Des développements essentiellement menés en C# et Go

Dual Universe offre aux joueurs un monde ouvert et procédural qui met en œuvre la technologie de type Continuous Single-Shard Cluster (CSSC) : tous les utilisateurs sont dans une même instance et un même serveur. Pour porter des dizaines de milliers d'utilisateurs dans un même shard, les ingénieurs mettent en œuvre plusieurs techniques.

Une première problématique est de limiter la densité des utilisateurs en un même endroit sous peine de créer le chaos. *« On peut diminuer le nombre de personnes visibles à l'écran en diminuant la distance de vue par exemple »* explique Guillaume Gris. *« Une autre recette est d'offrir un environnement suffisamment grand pour que les utilisateurs puissent se répartir géographiquement. Sur Dual Universe, la planète de départ seule offre une superficie égale au Royaume-Uni et nous avons de nombreuses planètes accessibles aux joueurs. Les joueurs sur une planète n'échangent pas de données avec les joueurs d'autres planètes : ce dispatch dynamique des utilisateurs permet de limiter les volumes d'interactions. »* Tous les utilisateurs sont dans la même base de données, et il faut jouer avec des techniques de scalabilité pour tenir la charge.

Pour ce volet applicatif, Novaquark réalise une bonne part de ses développements en C# et en Go. L'essentiel des fonctions clés du jeu a été implémenté en C#, notamment toutes les interactions et les services les plus coûteux en termes de ressources machines comme la gestion des Voxel et le calcul de visibilité des objets. *« Démarrer en C++ s'est avéré être une erreur »* estime le CTO : *« C++ a la réputation d'être un langage de bas niveau donc très performant, mais ces performances doivent être nuancées : si on prend l'exemple des allocations mémoires, on peut écrire du code C++ pas du tout performant. De même, pour des applications orientées serveur, on ne fait pas du calcul intensif : il*

s'agit essentiellement des applicatifs limités par les échanges de données avec la base de données. Il est plus important d'être capable de faire du multithreading, de la gestion de cache asynchrone, etc. On peut le faire en langage C++, mais même dans ses versions modernes, ce n'est pas un langage très adapté à ce type d'usages.»

Une plateforme portée par AWS, mais qui reste agnostique

Aujourd'hui, le cœur du service est en production sur 4 instances AWS. *«Il s'agit de machines de puissance relativement moyenne»* commente le CTO : *«Nous aurions pu faire tourner Dual Universe sur une seule grosse machine, mais nous préférons simuler une configuration plus proche du service en conditions réelles, en sortie de phase beta. Pour la partie Voxel, nous avons 2 services qui tournent en parallèle et c'est une brique qui peut être totalement parallélisée et nous permet d'anticiper sereinement une montée en charge.»* La plateforme a récemment été migrée sur des instances ARM (AWS Graviton) pour abaisser les coûts d'exploitation. De même, Novaquark n'utilise pas d'instance avec des GPU. *«Nous y avons pensé un temps afin d'accélérer nos algorithmes de génération procédurale qui nous servent à générer les mondes. Il s'agit néanmoins de traitements qui doivent être déterministes or, il n'est pas possible de faire du calcul déterministe sur GPU, car il y a bien trop d'éléments qui entrent en ligne de compte dans le calcul.»*

Soucieuse de rester agnostique vis-à-vis de son fournisseur Cloud, l'équipe technique a fait le choix de ne pas avoir recours à l'Autoscaling AWS. Cette absence de tout vendor lock-in permet à l'éditeur de reconsidérer très régulièrement son choix d'AWS et éventuellement migrer vers un autre fournisseur Cloud si cela présente un réel avantage.

De même, si la plateforme de Dual Universe met en œuvre plusieurs bases de données, notamment MongoDB, MySQL ou Redis, Guillaume Gris reste très critique sur les solutions managées proposées par les Cloud providers : *«Nous avons essayé quelques offres managées, mais nous n'en avons pas tiré une bonne expérience. Le mode managé implique de ne pas avoir la main totale sur le paramétrage et de se retrouver par exemple avec un Redis configuré pour swapper sur le disque, ce qui élimine tout l'intérêt de Redis !»*

Petite entorse à cette indépendance vis-à-vis d'AWS, Novaquark exploite le CDN d'AWS afin de distribuer les contenus numériques à tous les joueurs. C'est notamment le cas des modèles 3D des objets créés par les utilisateurs qui doivent être diffusés auprès de tous les joueurs. Les modèles 3D conçus avec des Voxel de Novaquark représentent un volume de données très important, de l'ordre de plusieurs To et un CDN permet de limiter les coûts de transfert de ces données, ce qui est un paramètre clé dans l'équilibre économique d'un MMORPG et donc d'un Metaverse.

Une diversification possible vers les Metaverses ?

L'équipe de développement est aujourd'hui concentrée sur son objectif de sortie de phase beta. Le jeu est jouable sur PC ainsi qu'en streaming sur le service de Cloud Gaming GeForce Now de Nvidia. L'équipe travaille sur l'analyse des performances et l'identification des goulets d'étranglement de la plateforme pour que celle-ci puisse faire face à sa montée en charge au moment du lancement commercial.

Mais déjà un autre cas d'usage de ces développements se profile à l'horizon pour Novaquark, le Metaverse. *«Beaucoup d'éléments de notre plateforme sont exploitables dans un Metaverse»* estime Guillaume Gris. *«Toutes les briques que nous avons développées pour constituer Dual Universe sont aujourd'hui prêtes à être exploitées pour d'autres usages. Attention toutefois, nous n'avons pas développé un framework de Metaverse générique. Nous avons une expérience très forte dans la création d'univers 3D, des briques réutilisables pour porter un univers 3D et nous avons développé des prototypes internes de Metaverse.»*

Pour le CTO de Novaquark, beaucoup d'entreprises qui misent aujourd'hui sur le développement de Metaverse risquent de se confronter rapidement à une dure réalité : *«Ceux qui vont tenter l'aventure de développer ce type d'univers vont se rendre compte que c'est beaucoup plus compliqué qu'on ne le pense notamment dans la gestion du UGC (User Generated Content) ou en termes de synchronisation des données. C'est très complexe à faire en maîtrisant ses coûts d'infrastructure.»*

Pour l'heure, l'équipe de Guillaume Gris reste concentrée sur Dual Universe mais l'éditeur évalue le marché pour trouver d'éventuels partenaires pour créer des Metaverses basés sur cette technologie. Des adaptations sans doute bien plus « terre-à-terre » de ce grand jeu d'aventure galactique. □

A.C

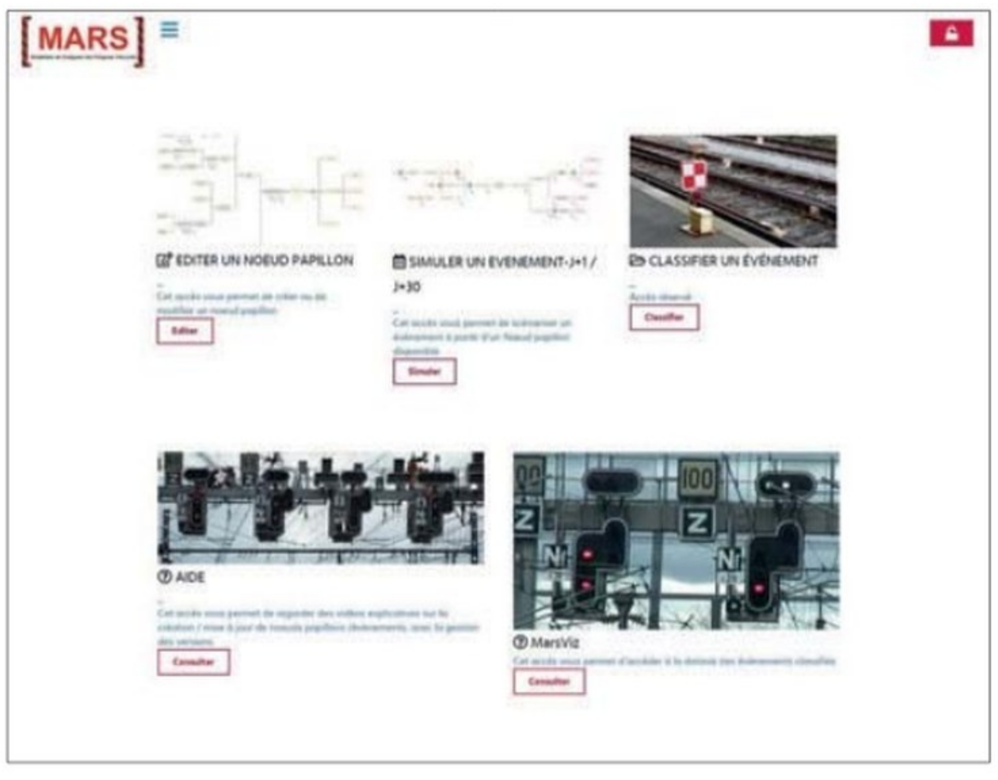
Nouvelles approches

Pour limiter les risques, la SNCF fait des nœuds papillons

L'exploitation ferroviaire, soit le fait de faire circuler des trains, implique obligatoirement un management des risques. Le Plateau Risque de la SNCF s'appuie sur Ignimission pour modéliser les risques d'incidents.

Les nœuds papillons sont d'usage depuis 2016 au sein de la SNCF (voir encadré). Deux ans plus tard, le Plateau Risque était créé pour impulser de nouvelles approches de la gestion des risques. Dans un premier temps, les risques d'incidents dans l'exploitation, un franchissement de signal d'arrêt par exemple, sont représentés sur papier, au crayon. Puis Ignimission est venu y mettre son grain de sel. Cette société, née en 2017, est spécialisée dans la collecte et l'échange de données. *« Quelqu'un avait déjà utilisé Ignimission et a proposé l'outil. C'est comme ça que le PoC a démarré, pour aboutir à l'outil complètement intégré aujourd'hui »* raconte David Groud, chef de projet IT sur le plateau risque de la SNCF. En effet, l'outil fourni par la jeune pousse permet au nœud papillon de monter en puissance, en lui ajoutant de la donnée.

L'outil, MARS, pour *« Modéliser et Analyser les Risques Sécurité »*, a deux aspects. Le premier, EVENT, *« est utilisé quand un événement se produit »* nous explique Anne-Marie Vimard, responsable du pôle modélisation et analyse du Plateau Risque. *« Nous avons une librairie de 28 risques majeurs dans l'exploitation ferroviaire, 28 nœuds-papillons qui peuvent être utilisés pour reconstituer ce qui s'est produit, et analyser les barrières, celles qui auraient dû empêcher l'accident »*. Il s'agit ici de « réactif ».



UNE MÉTHODE DE MODÉLISATION DES RISQUES

Le nœud papillon est une méthode d'analyses des risques, présenté sous forme d'arborescence. Au centre, se trouve l'Événement redouté. À gauche, les défaillances, les causes de cet événement central. Peuvent également y être symbolisées les barrières de sécurité, qui sont autant de mécanisme qui devraient empêcher la réalisation de l'événement. À droite, les conséquences. Le nœud papillon permet ainsi d'établir les scénarios potentiels d'accidents.

Réactif et proactif

Mais attention, le but d'un nœud papillon n'est pas de faire du prédictif. Les données sont saisies par les agents intervenant sur le terrain et des experts métiers. Une saisie d'informations guidée, mais manuelle. À noter que, au début de MARS EVENT, le module de visualisation était basé sur Qlik, obligeant à jongler entre les deux outils. Avec des problèmes certains d'interfaçage et de vérification des données. *« Nous avons, il y a un an, sollicité Ignimission afin qu'il intègre dans leur outil la partie visualisation. Elle a été mise en production au début de l'année »* indique David Groud.

L'autre grand progrès, c'est l'aspect proactif, avec MARS VIZ justement. *« La SNCF a une culture surtout du réactif, nous essayons d'aller plus loin avec les données pour faire des analyses de comportements des barrières »* souligne Anne-Marie Vimard. *« Ainsi, quand un certain nombre d'événements se sont produits, nous allons en agréger les données, ce qui nous permettra d'identifier les scénarios les plus fréquents et le comportement des barrières, de sorte à établir des plans d'action »*. Et ainsi intervenir en amont sur des barrières dont les défaillances ressortent de ces scénarios enrichis de données. Les nœuds papillons vont, en outre, être mis à profit pour *« dépassionner le débat et donner du sens aux procédures, aux barrières »*, et *in fine* de sensibiliser les opérateurs aux risques. Le Plateau Risque produit ainsi des « essentiels », des fascicules synthétisant ces nœuds papillons, récupérés sur le SharePoint interne de la société par au moins un millier de managers. □

Guillaume Périssat

CONGRÈS & CONFÉRENCES

CENTRE DE CONGRÈS RIVE MONTPARNASSE

Plus d'informations sur **www.metadays.fr**

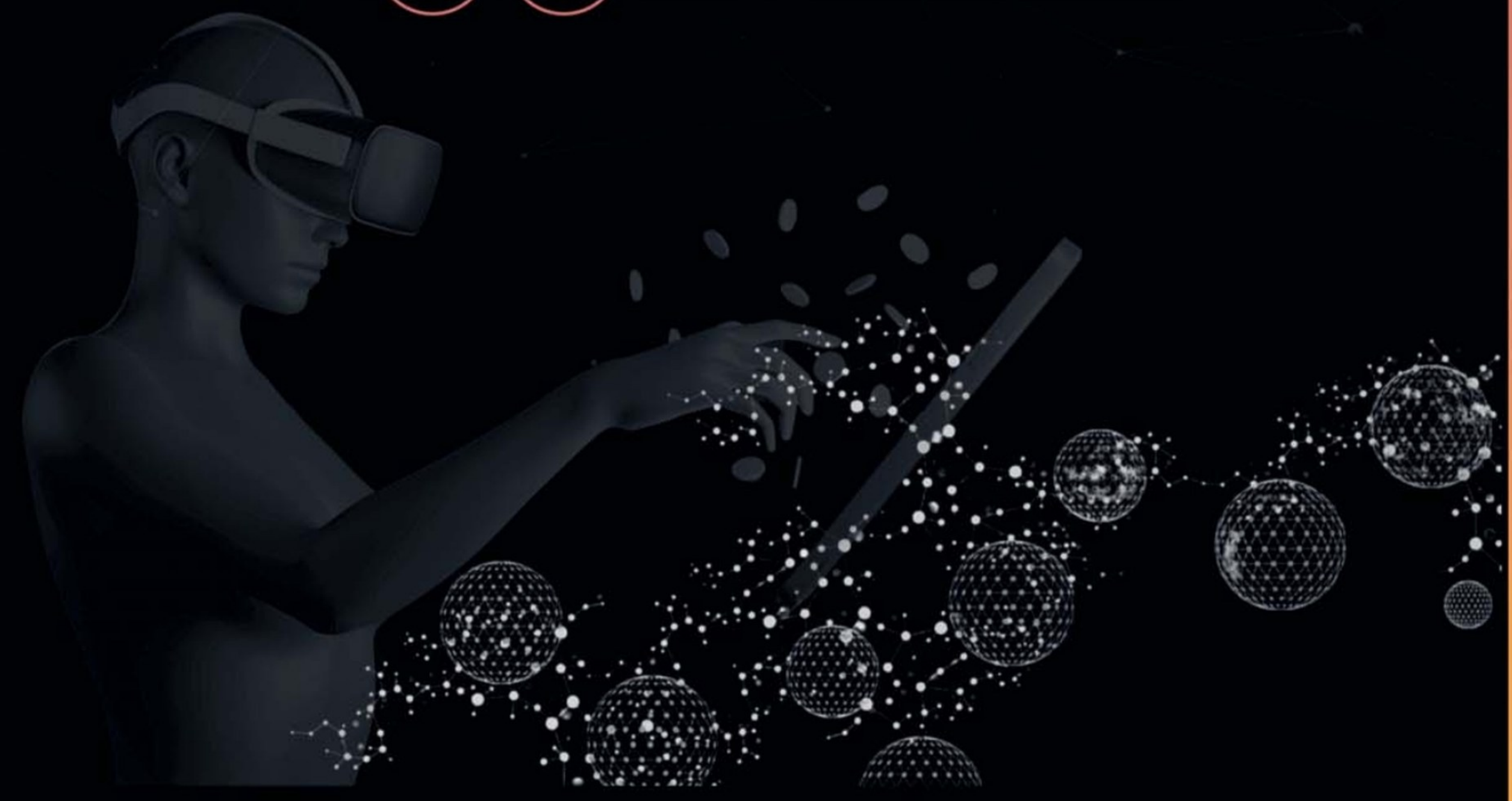
METADAYS

SAVE THE DATE

LE PREMIER RENDEZ-VOUS B2B CONTENU & BUSINESS

DU MÉTAVERS EN FRANCE

29 30 NOVEMBRE 2022



500 PARTICIPANTS **80** SPEAKERS **40** PARTENAIRES **2** JOURS DE CONGRÈS

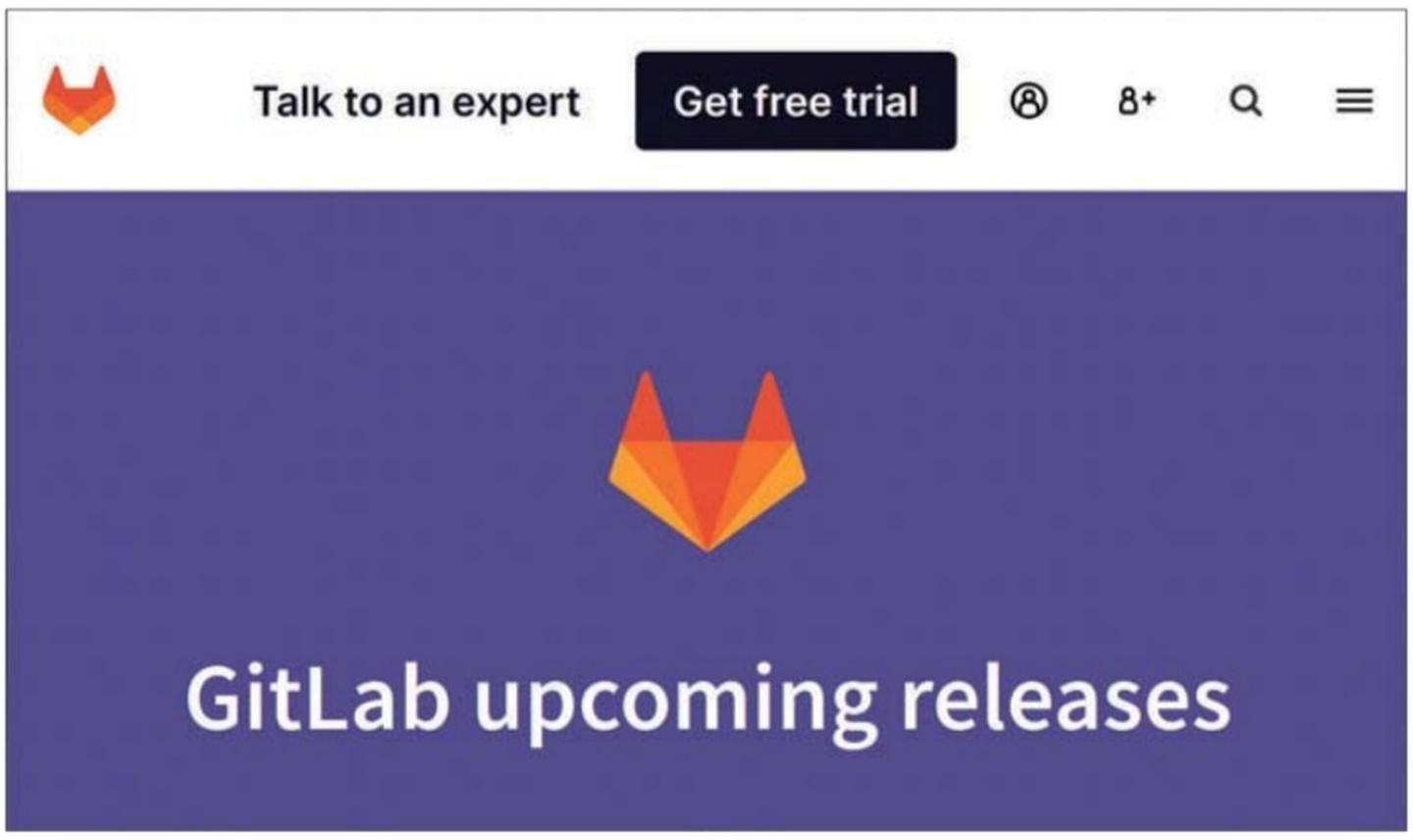
Version 15 de GitLab

Passez du DevOps DIY à The One DevOps Platform !

La dernière version de GitLab cible encore plus qu'avant le processus DevOps avec de nouveaux outils issus du ML. Nous allons voir dans cet article ce qui se cache derrière The One DevOps Platform.

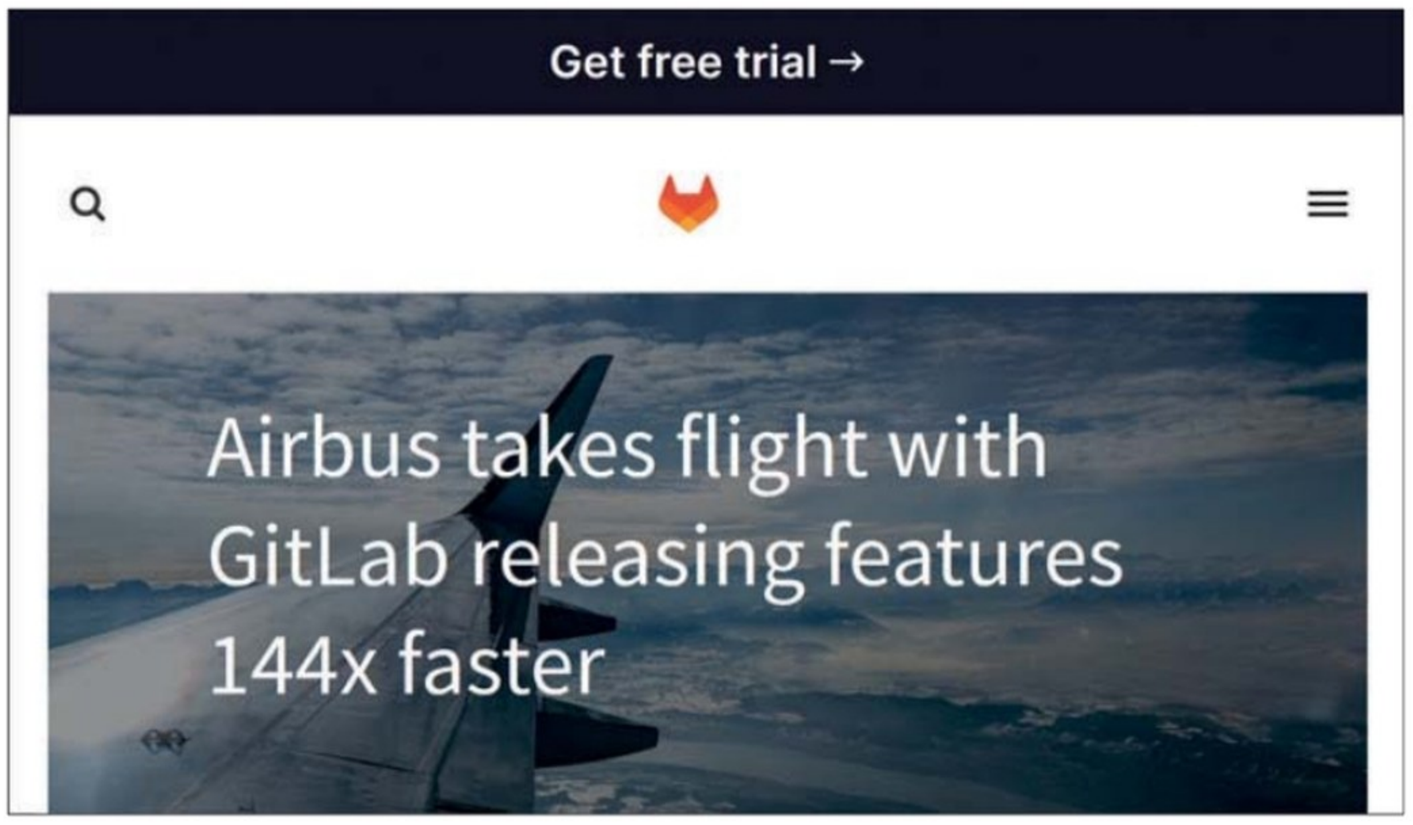
GitLab a annoncé le 23 mai dernier le lancement de sa prochaine itération majeure, GitLab 15. Elle offre aux organisations une plateforme DevOps unifiée et spécialement conçue pour permettre aux équipes de centrer leurs efforts sur le reste de leur activité : le développement. Elle ajoute de nouvelles fonctionnalités DevOps assez intéressantes susceptibles d'aider les entreprises à livrer des logiciels plus sécurisés. Elle améliore les capacités de la plateforme en termes de visibilité et d'observabilité, de planification agile, d'automatisation des flux de travail et de prise en charge des données pour les traiter en BI (Business Intelligence) ou en ML (Machine Learning). GitLab est, d'après son éditeur, la plateforme DevOps unique pour l'innovation logicielle. En tant que telle, GitLab fournit une interface, un magasin de données, un modèle de permissions, un flux de valeurs, un ensemble de rapports, un espace pour sécuriser le code, un autre pour déployer vers n'importe quel cloud et un espace dans lequel chacun peut contribuer. C'est une véritable plateforme DevOps de bout en bout, compatible avec le cloud et rassemblant toutes les capacités DevOps en un seul endroit. La plateforme GitLab, basée sur l'Open Source, exploite les contributions de sa communauté de développeurs et d'utilisateurs pour fournir de nouvelles innovations DevOps. Elle propose une solution d'observabilité open source activée par défaut qui unifie le suivi des journaux, des traces, des erreurs et des mesures diverses. GitLab a fait l'acquisition en 2021 de la société Opstrace, spécialisée en visibilité, observabilité, conformité et automatisation des flux de travail des équipes chargées du développement et du système. Elle met en exergue ses nouvelles capacités dans ces domaines avec cette nouvelle version.

« Dans l'environnement hautement concurrentiel d'aujourd'hui, les organisations sont plus que jamais sous pression pour fournir des logiciels plus rapidement et de manière plus sécurisée. Ils ont besoin d'une plateforme complète pour améliorer leurs délais de mise sur le marché », a déclaré David DeSanto, vice-président Produits chez GitLab. *« GitLab résout ce problème avec The One DevOps Platform. Les organisations peuvent se débarrasser de leurs chaînes d'outils DevOps DIY (Do-It-Yourself) et rassembler les équipes, de la planification au produit, dans une seule application, ce qui leur permet d'expédier plus rapidement du code sécurisé. »* KellyAnn Fitzpatrick, analyste sectorielle senior chez RedMonk, surenchérit sur le sujet : *« Les organisations visent de plus en plus la rapidité des développeurs. En parallèle, les équipes de développement sont souvent affectées par le manque d'expérience des dits développeurs qui bricolent des chaînes d'outils et de processus DevOps avec l'équivalent technique d'un ruban adhésif, entraînant inévitablement une diminution de la cadence de livraison des logiciels. La dernière version de GitLab s'efforce de fournir aux organisations une plateforme qui leur permet de se concentrer sur la création de produits innovants et facilite la collaboration entre toutes les parties prenantes. »* En clair, arrêtez de bricoler, adoptez GitLab, nom d'une pipe ! L'équipe DevOps d'Airbus dit avoir pu diffuser des mises à jour de fonctionnalités en seulement 10 minutes, alors qu'avant l'installation de GitLab 15, il lui fallait près de 24 heures. Néanmoins, le gain en efficacité dépend fortement de l'existant. Plus il est « bricolé » de bouts de ficelles et de scotch et est « bancal », plus l'apport d'une solution complète et bien structurée sera bénéfique.



Pour connaître les fonctionnalités à venir dans les futures releases de Gitlab 15, rendez-vous à l'adresse https://about.gitlab.com/upcoming-releases/?utm_medium=pressrelease&utm_content=gitlab15

Sécurité et conformité



Les clients utilisant déjà la plateforme DevOps, dont Airbus, auraient constaté des améliorations considérables en termes d'efficacité

Trop souvent, les entreprises identifient les vulnérabilités tardivement dans le processus de développement, ce qui augmente les coûts et risque d'entraîner des violations de la sécurité et des perturbations de l'activité. Cette dynamique aggrave les nouveaux vecteurs d'attaque introduits par les applications complexes et modernes et les déploiements cloud-native. Avec sa dernière version, GitLab renforce sa capacité à favoriser la conformité tout au long du cycle de vie du développement logiciel et offre des fonctions intégrées d'analyse de la sécurité et d'audit de la conformité, ce qui permet aux équipes de développement de se concentrer sur l'innovation logicielle sans ajouter d'outils supplémentaires ni entraver la livraison du produit. Les principales caractéristiques de sécurité et de conformité actuelles et futures sont, pour l'essentiel, les suivantes :

- La sécurité de la chaîne d'approvisionnement des logiciels prend en charge la génération automatique d'une nomenclature logicielle exportable (SBOM) ainsi qu'une attestation signée pour les artefacts.
- Les politiques d'approbation de la sécurité permettent d'appliquer un ensemble unique de politiques de sécurité gérées de manière centralisée.
- La gestion de la conformité fournit aux équipes qui en sont chargées une visibilité sur l'historique complet des modifications apportées.
- Les technologies avancées d'analyse de la sécurité développent le moteur d'analyse de nouvelle génération des tests statiques de sécurité des applications (SAST) de GitLab pour fournir des règles à la fois plus robustes et plus flexibles.
- L'analyse et l'expérimentation de produits améliorent l'aspect pratique des données de surface en permettant aux organisations de tester et valider de nouvelles idées et d'évaluer l'adoption des meilleures pratiques DevOps au sein des équipes et des projets.
- L'audit des événements permet aux administrateurs de diffuser les événements d'audit concernant les projets, les groupes ou les paramètres vers une destination de leur choix pour une meilleure visibilité. Il est possible d'agréger les données de GitLab avec d'autres outils.
- L'environnement de développement à distance fournit un environnement de développement basé sur le cloud qui permet aux organisations d'appliquer une politique de confiance zéro, avec laquelle le code source n'est jamais stocké localement.

VISIBILITÉ ET OBSERVABILITÉ FAVORISENT L'EFFICACITÉ

Les équipes travaillent plus rapidement lorsqu'elles ont une visibilité partagée sur leurs applications et leurs flux de travail. Les nouvelles fonctionnalités de GitLab 15 étendent la visibilité et permettent aux entreprises d'avoir une vue de bout en bout de la création de valeur et de la santé des applications. Elles permettent de créer un contexte partagé et collaboratif et de supprimer les fameux et si néfastes silos organisationnels. Les outils d'observabilité et de surveillance de GitLab aident les organisations à réduire le taux d'incidents, à obtenir des informations intéressantes sur d'éventuelles dégradations des performances et à trier en temps réel les incidents au fur et à mesure qu'ils surviennent. Ces nouvelles fonctionnalités contribuent à raccourcir les délais du code à la production, à réduire la fréquence et la gravité des erreurs, à aider les équipes de développement à déployer plus fréquemment et à réduire le temps de récupération après un incident.

Planification agile et automatisation des flux de travail

En tant que plateforme DevOps de bout en bout, GitLab est bien placée pour fournir une suite de planification permettant aux managers de concrétiser leur vision et de donner aux équipes DevOps les moyens de créer de la valeur, tout en améliorant leur façon de travailler. GitLab 15 permet une plus grande flexibilité, la prise en charge d'une plus grande variété de flux de travail et l'interconnexion des données à chaque étape du cycle de vie DevOps, de l'analyse initiale à la planification, en passant par la mise en œuvre, le déploiement et la surveillance. GitLab va enrichir sa plateforme DevOps avec des capacités de machine learning (ML), réduisant les cycles de prise de décision avec des suggestions recommandées. Les principales caractéristiques de la planification agile et de l'automatisation des flux de travail prévues par l'éditeur incluent :

- Les points de travail créent une nouvelle architecture de planification qui prendra en charge une gamme plus diversifiée de flux de travail et de cadres, y compris ceux d'entreprises Agile.

▪ Les vues et requêtes sauvegardées permettent aux équipes d'enregistrer une vue personnalisée des problèmes GitLab pour correspondre à leurs flux de travail de planification. Des tableaux de bord personnalisés contenant des données agrégées permettent aux organisations de prendre rapidement le pouls de leur santé et de l'état d'avancement des initiatives clés.
▪ Les suggestions de réviseurs et d'étiquettes simplifient la sélection des réviseurs de code et les frais généraux de planification en recommandant automatiquement l'étape suivante du flux de travail.
▪ Les suggestions améliorées contextuelles accélèrent la prise de décision.

ML et Data Science ne sont pas oubliés

Le Machine Learning est au jour d'aujourd'hui une composante essentielle du développement de logiciels. Les Data Scientist devraient apprécier GitLab 15 pour déployer plus efficacement des modèles de science des données, réduire les défis de coordination, obtenir des aperçus plus rapidement et auto-apprendre de leurs propres données au fil du temps. En plus de cela, GitLab 15 fournira des cas d'utilisation de ModelOps permettant aux équipes de science des données de collaborer étroitement avec leurs parties prenantes et d'offrir ainsi la meilleure expérience utilisateur. Les fonctionnalités-clés planifiées utilisant ModelOps sont les suivantes :
▪ Les DataOps (Data Operations) qui permettent aux utilisateurs d'extraire, de charger et de transformer les données pour les connecter aisément aux pipelines GitLab.
▪ Les MLOps (Opérations de Machine Learning) qui simplifient le développement et le déploiement de modèles ML permettant aux utilisateurs d'expérimenter, de former, de tester et de déployer leurs modèles en production.

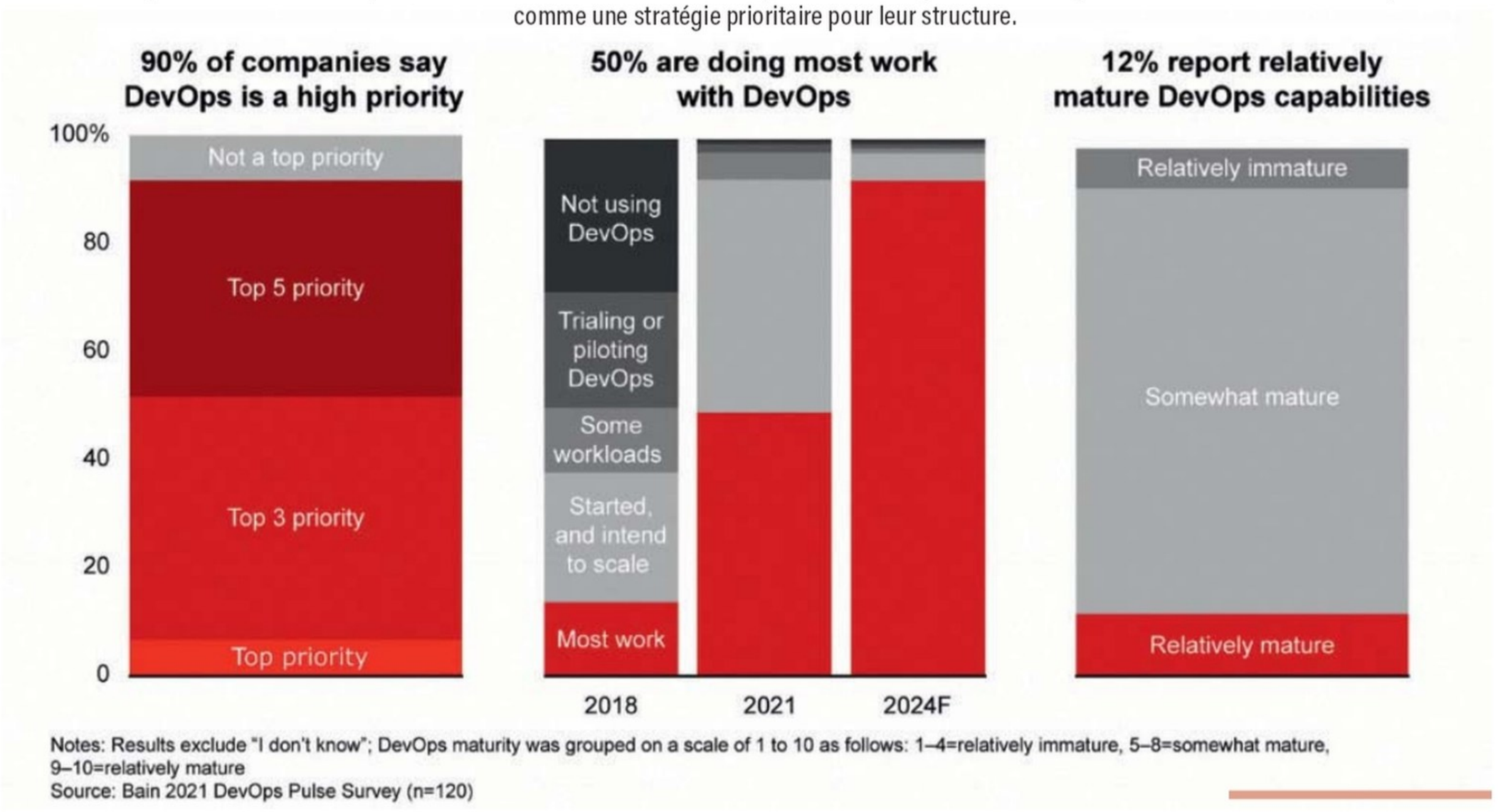
CHAÎNE D'APPROVISIONNEMENT LOGICIELLE

Parmi les améliorations (plus de 40) apportées, les principales concernent les domaines suivants :
▪ Audit des événements
▪ Capacités augmentées de ML
▪ Technologies avancées d'analyse de la sécurité avec le moteur d'analyse des tests statiques de sécurité des applications (SAST) de GitLab.
▪ Gestion de la conformité
▪ Architecture de planification
▪ Politiques renforcées d'approbation de la sécurité
▪ Environnement de développement à distance basé sur le cloud et permettant aux organisations qui le souhaitent d'appliquer une politique de confiance zéro (Zero Trust) avec laquelle le code source n'est jamais stocké localement.
▪ Sécurité de la chaîne d'approvisionnement logicielle

▪ L'observabilité : surveiller les modèles ML dans la production permet de mieux comprendre leur utilisation, en « fermant la boucle » sur le cycle de vie des charges de travail de Data Science.
▪ La traçabilité : avec de nombreux éléments mobiles entre les données, le code et les versions du modèle, la traçabilité assure la protection intégrée des données, la sécurité du code source ML et la gestion des versions du modèle pour garantir la conformité, les contrôles d'accès et la collaboration. □

Thierry Thaureaux

D'après une étude menée par Bain, un cabinet de conseil en management et stratégie, 90 % des organisations considèrent le DevOps comme une stratégie prioritaire pour leur structure.



Notes: Results exclude "I don't know"; DevOps maturity was grouped on a scale of 1 to 10 as follows: 1–4=relatively immature, 5–8=somewhat mature, 9–10=relatively mature
Source: Bain 2021 DevOps Pulse Survey (n=120)

Applications mobiles

Pradeo cible les développeurs

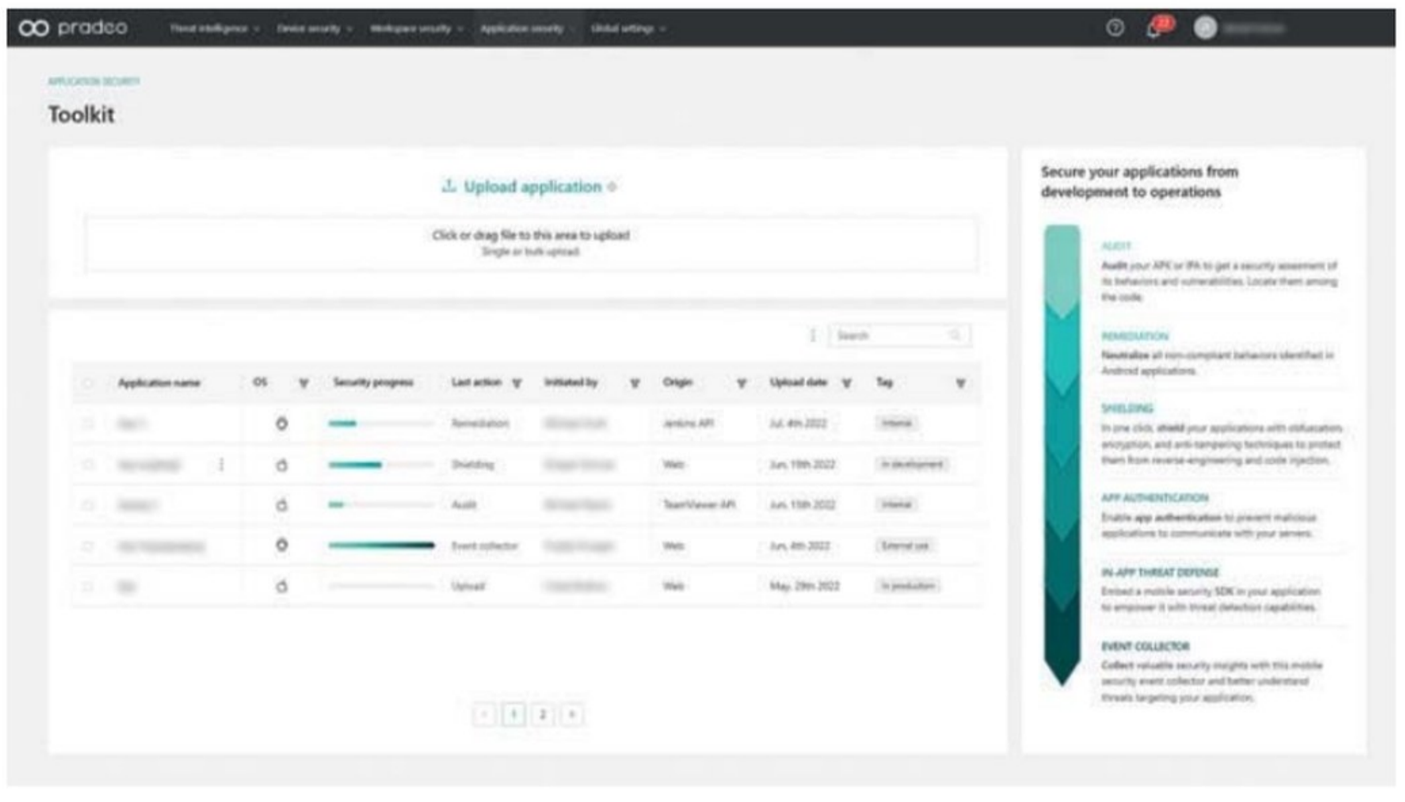
L'éditeur français spécialisé en sécurité des applications mobiles a récemment refondu son offre à destination des développeurs, unifiant ses services au sein d'un pack DevSecOps comprenant notamment du « shielding ».

Pradeo propose, de longue date maintenant, des outils destinés aux développeurs d'applications mobiles. En effet, selon la société montpelliéraine, près de la moitié (41%) des applications mobiles sont vulnérables à l'altération de code et à la rétro-ingénierie. Entre les vulnérabilités et les comportements inattendus, qu'ils se glissent dans le code source ou dans les librairies utilisées, le développement d'applications mobiles, les problèmes de sécurité commencent dès le développement. *« Les cycles de mise sur le marché des applications mobiles sont souvent bousculés par des besoins commerciaux urgents, et ne sont pas menés aussi méticuleusement que les développeurs le souhaiteraient »* écrit Pradeo. D'où le lancement chez l'éditeur d'un « toolkit appsec mobile ». Il ne s'agit pas d'un nouveau produit, plutôt d'une refonte de l'interface de sorte à rassembler l'ensemble des services DevSecOps.

Obfuscation et chiffrement

On y retrouve donc l'outil d'audit de sécurité, lequel identifie les comportements non-conformes, les vulnérabilités et comment leur remédier, ainsi que des fonctions de « shielding ». Sous ce terme se cachent plusieurs techniques, destinées à empêcher l'altération et la rétro-ingénierie du code. L'obfuscation et le chiffrement viennent ainsi rendre le code plus complexe à déchiffrer, en ayant recours à la randomisation, au spoofing, à la sécurisation des chaînes de caractères et à la réflexion de code, en dissimulant les appels aux méthodes, en chiffrant ses ressources, et en le protégeant contre le debug. En outre, l'outil de « shielding » permet de contrôler l'intégrité de l'application et d'empêcher son lancement grâce à un checksum et à un contrôle de l'état de l'environnement.

L'idée est d'empêcher qu'une application soit clonée et que ce clone, probablement malveillant, soit distribué aux salariés d'une organisation (par spear phishing par exemple). Surtout, Pradeo veut proposer une couche d'automatisation. Ainsi, après que le développeur ait versé le binaire (sachant que la plateforme supporte les applications Android et iOS, ainsi que les programmes JS, Java et Kotlin) dans l'interface Pradeo Security et choisi les fonctionnalités de sécurité à ajouter, le moteur ajoute automatiquement une couche de protection, de sorte que le développeur n'ait pas à réaliser manuellement l'obfuscation du code, ni à bidouiller des algorithmes de chiffrement. Ainsi, l'entreprise de Montpellier entend assurer la protection des mobiles, de l'audit de flotte à la protection, en passant par l'appsec et l'authentification. *« Altérer le code d'une application mobile est un jeu d'enfant »* explique Vivien Raoul, CTO et co-fondateur de Pradeo. *« Avec notre service, les équipes de sécurité bénéficient des dernières techniques de shielding, en n'imposant aucun développement et sans rallonger le temps de mise sur le marché de l'application, puisque Pradeo Security se charge de tout ».* □ **G.P**



L'interface de la plateforme Pradeo Security permet d'avoir, en un seul endroit, l'ensemble des outils de sécurité de l'éditeur.

LA 22

LES ASSISES

12.10.22 →→ 15.10.22

/MONACO///

→ Plus qu'un événement,
une référence, un incontournable

→ **lesassisesdelacybersecurite.com**

DG CONSULTANTS

COMEXPOSIUM

Faire autrement

Le Lean aujourd'hui

Pour faire face à l'armada de bouleversements qui sont en train de déferler et dont nous ne percevons que le début des effets, l'entreprise aura besoin de personnes adaptées et surtout adaptables. Ce combat darwinien sera féroce et il devra être mené avec méthode. L'auteur, patron d'une entreprise industrielle et fort de ses convictions, est convaincu que notre avenir est lié à la collaboration, à l'amélioration et à la coordination donc à une relation de qualité ; le gaspillage est le pire fléau contre lequel nous devons lutter.
Ce livre, rédigé sous la forme d'un roman, nous emmène en voyage avec Julia, trentenaire en plein questionnement. Il nous propose une voie pour mener à bien un Lean adapté à toutes les entreprises, qui prend sa source dans le concept de base du Lean, mais qui s'adapte aux problématiques contemporaines ! Cet ouvrage ne s'adresse pas spécifiquement aux sociétés qui mettent en place une stratégie Lean, il s'adresse à toute organisation de plus de deux personnes dans laquelle les relations sont considérées comme importantes, ou dans laquelle on veut introduire un changement profond qui soit compatible avec la donne actuelle. Les trois piliers en sont les relations humaines, le digital et le green. L'ouvrage a remporté le Prix du Livre lors de la 29ème Cérémonie des Prix Nationaux de la Qualité.

Le repas sera servi dans une heure et entre-temps, Julia essaie de remettre ses idées dans l'ordre. Elle a pris pas mal de notes et commence à les relire. Évidemment, une partie des papiers tombent par terre et glissent sous les pieds de son voisin. Qui lui ramasse et les lui tend. « Vous êtes française ? » lui demande-t-il avec un léger accent américain. La conversation s'engage. Il s'appelle David, il est professeur de sociologie au MIT[1] et à la NYU[2] et se rend à un congrès parisien pour des "vaconfs"[3] sur les impacts sociétaux du numérique. Lorsqu'il aperçoit les schémas un peu brouillons que Julia a fait sur la définition des gens, il lui demande s'il peut lui donner un conseil. Julia, totalement sous le charme, acquiesce.

– Quand on doit communiquer dans le monde d'aujourd'hui, cela passe essentiellement par des chiffres et des diagrammes. Mais la plupart du temps, c'est peu clair et totalement imbuvable donc les décisions qui en découlent sont souvent inappropriées. La chose la plus utile que doit savoir faire une personne de haut niveau de nos jours, c'est convaincre. Et le faire vite. Pour cela il faut savoir exposer des données de manière claire et limpide. Suis-je clair ?

– Crystal clear[4], répond Julia.

– La Bible absolue, c'est l'ouvrage de Edward R. Tufte intitulé *The visual display of quantitative information*[5], je vous le conseille vivement et vous verrez que cela va booster votre carrière. C'est intéressant vos schémas. Vous pouvez m'en dire plus ?
Julia explique alors toute l'histoire, Rosie, Maggie, Tara. Félicie également. Et le fait que l'on obtienne des résultats par les gens. Elle explique aussi qu'elle a encore bien du mal avec ce programme et demande à son charmant interlocuteur ce qu'il en pense, notamment par rapport à l'époque actuelle qui est tout de même bien différente de celle pendant laquelle Rosie et Maggie ont travaillé.
David lui répond que l'on vit dans un monde qui change, dans une période charnière qui n'arrive qu'une fois tous les quelques siècles.

– Aujourd'hui, nous vivons une révolution comme il n'y en a eu que quelques-unes dans l'histoire de l'humanité, mais elle est particulière. D'une part, parce qu'elle est mondiale alors que les précédentes ont toujours été circonscrites à des pays. Mais aussi parce qu'elle est banale, sans grande violence ni slogan et qu'elle dure depuis trente ans. Visible et

1 : Massachusetts Institute of Technology.
2 : New York University.
3 : Contraction de vacances et conférences.
4 : Clair comme de l'eau de roche.
5 : *La visualisation graphique des informations quantitatives.*

insensible à la fois. Depuis la révolution industrielle et jusqu'à la Perestroïka, les choses étaient claires. Un patron pensait en patron, un ouvrier en ouvrier, il y avait les capitalistes et les communistes. On savait qui on était. On comprenait ce que l'on faisait au moins dans notre périmètre. Notre travail et notre vision politique participaient grandement à nous positionner. Aujourd'hui, presque toutes les frontières ont sauté et c'est flou dans la tête des gens. Avant, on savait à quel milieu on appartenait, on avait des projets ; bref, c'était rationnel et raisonnable. Les gens voulaient une carrière, une famille, une maison et cela les définissait. Et peu de temps après, il y a eu 1995 et l'arrivée du digital. Et ça change tout. Des entreprises de la Silicon Valley, qui ne produisent rien et ont à peine dix ans, valent plus que des grands constructeurs automobiles centenaires. Qui aurait imaginé ça, il y a trente ans ? Maintenant on raisonne en expériences et je parle là d'expériences sensorielles, pas de l'Expérience issue de la longue décantation d'une activité réfléchie. Aujourd'hui, on veut tout vivre, chaque moment compte, sans plan prédéfini et notre travail ou notre famille ne nous positionne plus comme avant. L'argent encore un peu, mais là encore ça bouge. C'est très paradoxal. Tiens, cette année on se bat pour qu'un étudiant ait une bourse. Quand on lui dit que c'est OK et qu'il peut faire ses études chez nous, vous savez ce qu'il nous répond ?

– Ben, qu'il est super heureux.

– Non ! Il me dit que ça ne le dérange pas. Le jeune, il a une bourse pour aller à la NYU et ça ne le « dérange pas ».

– Comme motivation effectivement, ça se pose là. Il est bon au moins ?

– On espère mais j'ai un doute. Quand je lui ai expliqué qu'il devrait travailler dur, il m'a répondu d'accord mais n'oubliez pas que j'ai « Une Vie ». Et qu'il ne la sacrifierait pas au travail. C'est très nouveau dans notre milieu. J'ai d'abord cru à un cas isolé, mais ce n'est pas le cas. On va devoir en tenir compte car jusqu'ici, pour les grandes études ou les postes élevés, tout le monde avait compris qu'il faudrait mettre des choses personnelles entre parenthèses. Maintenant, c'est l'inverse !

– Et il va faire quoi comme thèse ? demande Julia un brin amusée par la stupéfaction de David vis-à-vis d'un comportement qu'elle connaît parfaitement.

– Il étudie les impacts sociétaux de la transformation couplée du green et du digital sur une économie capitaliste mondialisée.

– Comment ça digital, vous voulez dire que les ordinateurs vont tout contrôler ?

– Oui et non, sourit David. Les ordinateurs ne sont pas le digital. Ils sont une expression des possibilités du digital. Le digital à proprement parler, c'est bien plus que cela. Ce n'est pas numériser grâce à un ordinateur des processus anciens qui sont déjà probablement déjà dépassés, c'est une manière de penser et d'agir qui est liée aux progrès techniques mais aussi à la modification des comportements. Le digital, c'est la maîtrise du bit, de l'élément de base, du pixel, de la cellule, du grain, etc. mais c'est aussi la possibilité de le connecter et de le faire évoluer en temps réel. Dans le monde digital, il n'y a plus de plan, il y a un film d'événements qui se déroule en permanence et auquel on peut ou pas se raccrocher, comme sur un Twitter ou un Facebook.

Voyant Julia interloquée, il insiste.

– Prenons un exemple et regardons une technique particulièrement ancienne comme le feu d'artifice. Certaines sociétés ont transformé l'allumage manuel en allumage piloté par informatique afin d'avoir des séquences mieux maîtrisées. Ce n'est pas le monde digital. La véritable transformation digitale du feu d'artifice, ce sont des drones qui pilotent chacun un pixel et sont capables de dessiner à l'envi des figures dans le ciel. Le résultat est partagé sur le net en temps réel. Voilà la différence.

L'image de ce raisonnement diffuse profondément dans l'esprit de Julia et elle ne peut s'empêcher d'ajouter :

– Cela me pose pas mal de questions en fait. J'ai toujours vu l'informatique comme un moyen. Une aide. Jusqu'ici, j'ai cru que les ordinateurs avaient la mémoire des chiffres pour que nous conservions la mémoire du reste. Jamais je n'ai imaginé que cela allait bouleverser la manière de penser le monde. Cela me semblait du bon sens d'automatiser les tâches fastidieuses ou les calculs.

– Alors, je dois vous parler du bon sens et des idées fausses. Je ne supporte plus qu'on me parle du bon sens à tout bout de champ. Le bon sens, c'est comme les avis, tout le monde en a un lui, répond David avec un air soucieux. Notre vie est bourrée d'idées fausses. La science est là pour les tuer. Tout autant que pour découvrir de nouvelles théories. Depuis toujours, j'essaie d'inculquer à mes étudiants que les "misconceptions"[6] sont le pire des poisons. Lutter contre les "misconceptions" est devenu le slogan de ma vie. Et c'est pour cette raison que je ne crois pas au « bon sens ». Notre soi-disant bon sens nous trompe trop souvent. C'est lui qui propage les épidémies, c'est lui qui est à l'origine de bien trop d'accidents. Je l'explique dès le début des cours à mes étudiants.

David marque une pause, réfléchit en caressant sa barbe de cinq jours et reprend :

– En fait cela va déjà bien plus loin. Le digital a fait évoluer bon nombre d'industries. Par exemple, les moteurs d'avions ont déjà connu quatre évolutions simplement à cause de ça.

– Vous voulez parler de la simulation et de la conception assistée par ordinateur ?

– C'en est une, mais c'est la moins importante, sourit son interlocuteur. Celle qui a tout lancé, c'est l'évolution de la manière de voyager. Le low cost a métamorphosé la manière de concevoir un moteur. Quand un avion doit faire huit rotations par jour, on ne regarde plus le moteur de la même manière que s'il en fait deux. Si on veut voler pour 40 euros et réserver sur son smartphone, croyez-moi cela ne se joue pas qu'au niveau d'un logiciel de réservation, c'est bien plus profond.

– Oui vu sous cet angle... Et les autres révolutions alors ? demande Julia curieuse.

– Eh bien, c'est la métallurgie. Grâce au numérique, on peut appliquer aux matériaux certaines théories de la biologie et concevoir une sorte d'adaptation génétique des matériaux vis-à-vis du milieu dans lesquels ils sont utilisés. La méthode de sélection des éléments constitutifs d'alliages est exactement la même que celle des gênes et on

6 : Idées fausses.

peut ainsi obtenir des alliages à haute entropie avec des propriétés bien supérieures à ce qui existe actuellement. Reste à mettre en forme les produits et là c'est la métallurgie des poudres qui prend le relais. Maintenant on peut maîtriser le grain métallurgique localement alors qu'avant on fabriquait d'abord une ébauche que l'on usinait par enlèvement de matière ; aujourd'hui on fait croître la pièce autour de ses trous, avec des process comme l'impression. Et il fallait des grandes usines pour ça, mais bientôt on pourra faire les pièces individuellement, à la demande partout dans le monde. La maintenance et les stocks qui y sont associés vont être radicalement bouleversés.

– Oui cela semble prometteur.

– C'est bien plus que cela, c'est l'avenir. Et s'il ne fallait qu'une seule justification, le green est celle-là. On utilise moins de matière, moins d'énergie pour produire des fonctions plus efficaces. Tout est juste là-dedans.
C'est grâce à tout cela qu'on voyage plus facilement. Concevoir et réserver un road trip se fait tout seul, les logiciels de traduction et de localisation ont supprimé le mot « perdu ». Toutes ces frontières liées à ceux qui savent sont en train de sauter. Et ça change le monde.
Julia est secouée.

L'idée du pixel fait son chemin dans sa tête et elle essaie de le réconcilier avec le Job Relation. La première chose sur laquelle Rosie a insisté, c'est ce concept de l'individu en tant qu'individualité et surtout pas comme un groupe. Elle fait la correspondance avec ce fameux pixel et tente d'expliquer ça à David, qui capte instantanément.

– Génial, génial lui dit-il, j'ai le missing link[7]. Tu peux me redire ce qu'ils ont fait à Fremont ?
Subtil, le passage du vouvoiement au tutoiement. Julia lui explique, elle ne boude pas son plaisir d'apprendre quelque chose à un enseignant du MIT. Celui-ci semble assez agité au fur et à mesure des révélations de Julia.

– Bon sang Julia, mais c'est bien sûr, je comprends maintenant ce que Toyota a voulu faire avec son système, ou plutôt ses systèmes. Au MIT, on a beaucoup étudié ça, et c'est même de là que vient le mot "lean"[8] mais je n'avais jamais fait ce lien. Quand on demande à Toyota son secret, ils expliquent qu'il n'y a aucun secret, qu'ils sont simplement des gens sérieux. Qu'ils veulent des résultats avec méthode parce que sinon c'est de la chance et que la chance se manage difficilement et ne permet ni d'anticiper ni de démultiplier. En fait, ils ont ce système de production qui les fait avancer et aussi le système de qualité qui permet de consolider en adaptant en permanence le back-office et l'organisation qui soutient le système. Ce que je crois, c'est que Toyota a compris tous ces mécanismes humains bien avant tout le monde et c'est ce qui explique le succès incompréhensible de cette marque qui ne délocalise pas ses productions et qui arrive tout de même à avoir la rentabilité des fabricants de voitures premium allemandes en fabriquant les voitures de Monsieur tout le monde. Cette association de granularité et de film de production continu, c'est le numérique et c'est aussi cela qui modifie profondément la vision relationnelle en entreprise. On avait tous bien capté qu'ils gagnaient parce que leurs produits étaient meilleurs que les autres, et que la raison à cela est qu'ils avaient des modes de fabrication et surtout des techniciens meilleurs que les autres, mais comment ils arrivaient à faire cela, à le conserver, ce lien entre la technique et l'individu, leur manière de collaborer entre eux, cela, je ne l'avais pas discerné.

– Tu vois Julia, continue David, ce que tu me dis est « essential ». Il faut faire un article là-dessus.
Julia saute sur l'occasion et susurre que c'est un programme américain…

– Nul n'est prophète en son pays, ironise David, et cela me fait voir un autre piège lié au changement : il faudra faire de plus en plus attention entre le *legacy*[9] et l'héritage.

– Et c'est quoi la différence ? questionne la jeune femme.

Au moment où elle pose la question, l'hôtesse de l'air annonce une zone de turbulences. Tout le monde doit attacher sa ceinture. David, qui semble avoir le mal de l'air, se cramponne à son accoudoir et effleure la main de Julia. Il lui lance un sourire gêné mais ne retire pas son bras, Julia non plus. Après ces quelques secondes de flottement, il reprend ses esprits et son discours.

– L'héritage est l'expérience des choses qui sont efficaces. Rien ne pourra l'améliorer mais on veut le modifier par modernisme. Le legacy, ce sont les technologies en place que l'on ne veut surtout pas toucher et qui empêchent le saut technologique qui va potentiellement nous tuer si on le refuse. Les Japonais sont très forts dans la vision de cet équilibre car ils savent depuis toujours osciller en permanence entre la technologie et la tradition. Kodak est mort du legacy du film et Toyota est Toyota car ils conservent l'héritage du Kanban. La technique, c'est important. Elle a été le principal ferment qui a fondamentalement et massivement amélioré la vie de milliards de gens sur la planète. En 100 ans, l'espérance de vie a presque doublé et les conditions de vie se sont améliorées de manière plus importante lors des 50 dernières années que depuis la création du monde. Lors du discours de cérémonie de remise de diplôme, le *Dean* de notre *college*[10] à l'époque nous a dit une chose qui s'est toujours révélée juste : *"Always stay up to speed with technology. Or you will fail."*[11] Aujourd'hui, la technologie va de plus en plus vite et donc ne pas se laisser distancer est de plus en plus important, et ça ici on l'a bien compris. Pendant la Seconde Guerre mondiale, c'est la technologie et la mécanique qui ont donné l'avantage aux Allemands et ensuite aux alliés pour mettre fin à la guerre. Plus encore que le courage des hommes. Quand on a des radars et pas l'autre, c'est plus facile, quand on a une bombe A et pas l'autre, c'est plus facile, quand tes canons tirent un peu plus loin que ceux de l'adversaire, c'est plus facile. Et pour l'entreprise c'est pareil.
Julia est totalement dépassée par la vitesse de réflexion de son nouvel ami. Elle a l'impression que ça part dans tous les sens. Elle lui demande s'il lui arrive de stopper la machine à penser.

---

7 : Chaînon manquant.

8 : Voir le livre *The machine that changed the world* de Womack et Jones.

9 : Héritage qui doit être compris comme patrimoine.

10 : Doyen de notre université.

11 : Il faut toujours rester au contact des nouvelles technologies. Sinon on risque l'échec.

– On ne peut pas. Je suis quelqu'un de très anxieux, j'ai toujours l'impression de rater et quand quelque chose réussit, je culpabilise, c'est infernal, alors pour soigner ça, j'écris et je crée. Ma demande interne dépasse de loin mes capacités de réalisation ce qui crée un hiatus intellectuel. Parfois je tombe sur quelqu'un comme toi avec qui je peux échanger, mais c'est très rare. Ma structure mentale ne me rend compatible qu'avec 2 % de la population, pas plus. Quand on est comme moi, on a donc peu d'amis. D'un autre côté, on me demande souvent de venir pour animer un sujet, et dès que je suis là on me reproche d'être moi. Tu n'imagines pas le calvaire que sont les dîners en ville, je me fâche avec tout le monde. Heureusement, avec le temps je suis de moins en moins invité !

Julia est contente de voyager avec le docteur House à ses côtés et lui demande ironiquement comment il vit le fait d'être très intelligent.

– Tu n'y es pas ! Ce n'est pas une question d'intelligence, c'est une imposture totale, je n'ai pas plus raison que les autres, ce serait trop simple, c'est le regard qui est totalement différent quand on est comme ça, c'est évident. Si on ne l'est pas, c'est impossible de capter.

Rassasiée par tant de concepts, Julia, songeuse, met son tout nouveau casque, lance sa play-list et sombre petit à petit dans un sommeil bienheureux. À ce moment, elle n'arrive pas à savoir si le cuir nappa des sièges qui la soutiennent à quelque chose à voir avec la vallée d'où sortent ces Chardonnay fantastiques.

Elle se réveille un peu vaseuse et voit David qui tape à grande vitesse sur son Macbook. Son visage irradie la création alors Julia ne veut pas le déranger. C'est lui qui, d'un coup d'œil, la remet en selle.

– Bon travail ? lui demande-t-elle finalement.

– Oui, répond David, je suis sur notre histoire de pixel et d'individu. Je suis en train d'écrire un post qui devrait faire réagir. On disait tous les deux que l'individu est semblable au pixel et que c'est important de les considérer en tant que tel mais ce que l'on voit aussi c'est que pour les deux, c'est avec les autres qu'ils créent l'image ou le groupe. L'individualité est vitale mais l'individualisme tue. C'est la composition des individualités qui fait le paysage global. Parce que ce qui va faire la différence maintenant, ce sera l'intelligence collective. La collaboration et la coordination deviennent la nouvelle bataille concurrentielle.

– Attends David, coupe Julia avec un doute dans la voix. Je ne comprends plus. Tu disais il y a cinq minutes que la technologie faisait tout et que le gagnant était le plus technologique. *Winner takes it all*[12]. Et là, tu dis que la techno sera la même partout. Je ne te suis plus là. Et puis, sans vouloir te vexer, certes la technologie américaine a gagné la guerre en 1945, mais au Vietnam, vous aviez des hélicos et eux des pousse-pousse et on sait comment tout cela s'est terminé. Et dans les années 1980, sur l'automobile, les Japonais vous ont battus avec des techniques liées aux hommes essentiellement. Non ? Tu en penses quoi ?

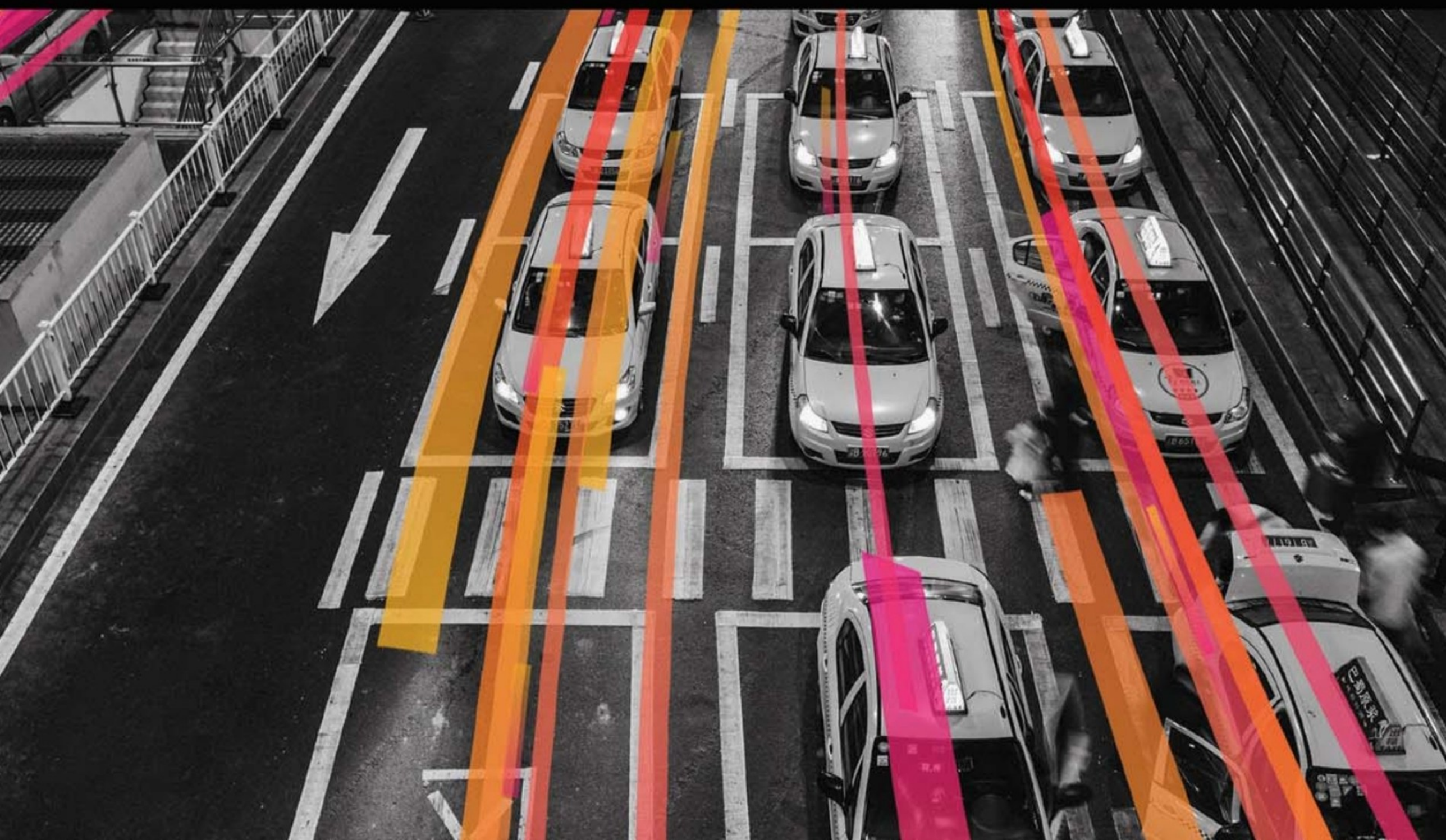
– Ah, Julia ! Que c'est bon de causer avec quelqu'un qui se bat et qui sait débattre. Mais, tu as raison, la technologie ne se suffit pas à elle-même. En revanche, elle établit les bases. Elle ne se substituera pas partout à l'humain mais elle contribuera à changer nos vies de manière radicale et rapide. Et compte tenu de cela, si tu l'as, tu n'es pas sûre de réussir à aller où tu veux. Tu n'es pas certaine non plus de rester au contact, mais si tu ne l'as pas, alors là tu es sûre de te faire dépasser. Quand je disais qu'elle serait la même partout, je ne parle pas de la même chose. Il y a des start-up dans les pays en voie de développement. On développe des applis dans tous les pays. Mais des Operating Systems, non. Des écrans tactiles, non. Des satellites ou des vaccins non plus. Et la technique, elle est là. Il y a plusieurs niveaux en technologie, savoir l'utiliser et la découvrir. Et je ne parle pas des blockchains, des monnaies virtuelles et de ce qui se passe en biologie. L'eugénisme est techniquement possible maintenant, il faut adosser la technique à la politique mais vu l'état des politiciens actuels, je vois bien des problèmes arriver…

12 : Le vainqueur prend tout.

Sécurisez votre parcours vers l'innovation

Faites face aux menaces de sécurité actuelles et augmentez votre résilience pour que rien ne vienne entraver votre prochaine innovation. Construisez une défense plus solide avec Splunk et faites progresser votre entreprise.

Découvrez comment sur **splunk.fr**

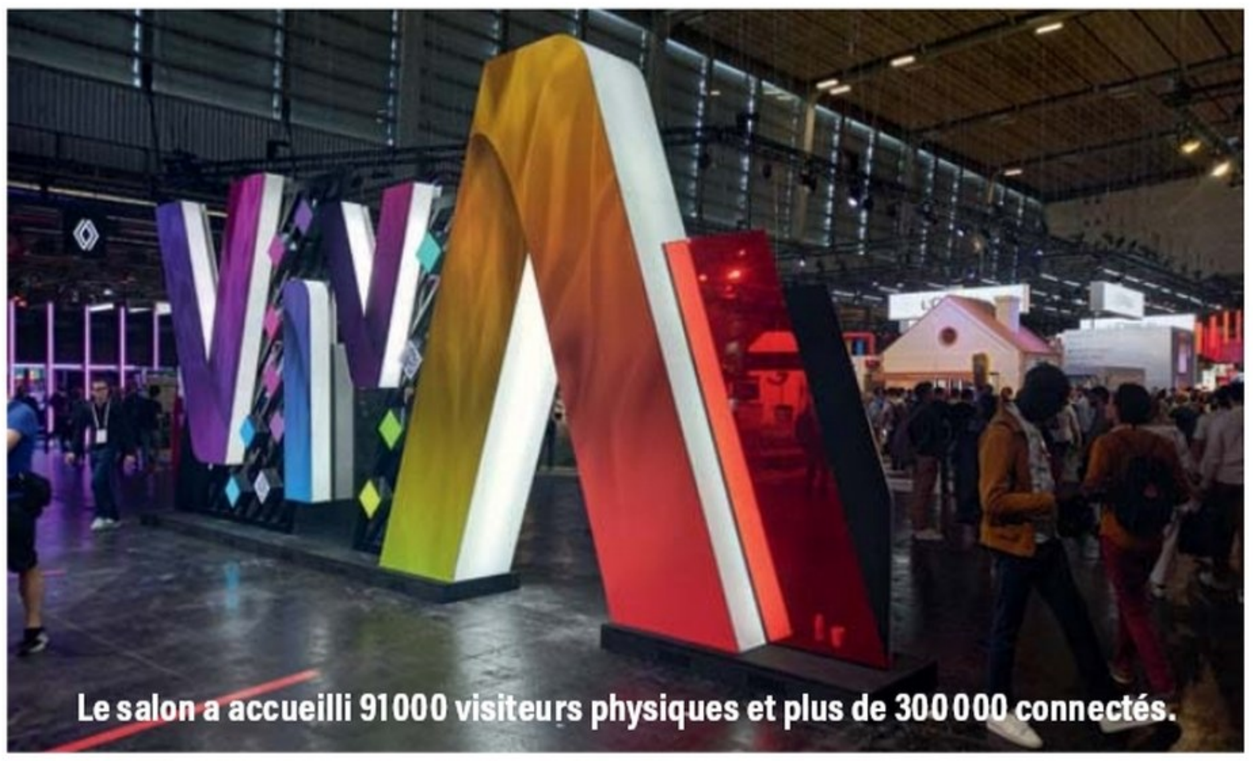


VivaTech 2022

Les technos qui sortent du lot

Au fil de nos pérégrinations dans les couloirs du Parc des expositions, Porte de Versailles, certaines innovations présentées à VivaTech 2022 ont piqué notre curiosité. Focus sur quelques-unes d'entre-elles. Attention, liste non exhaustive !

Mark Zuckerberg, fondateur de Meta, Bernard Arnault, PDG du groupe LVMH, Changpeng Zhao, PDG et fondateur de l'exchange Binance, ou encore le président de la République Emmanuel Macron, le président ukrainien Volodymyr Zelensky et son hologramme... Autant de personnalités à avoir fait le déplacement pour la sixième édition du salon VivaTech, qui s'est tenu au Parc des expositions, Porte de Versailles, du 15 au 18 juin 2022. Certaines ont même été accueillies comme de vraies rockstars, à l'image de Changpeng Zhao. Mais les véritables stars de ce salon restent les, ô combien nombreuses, technologies présentées entre les allées.



Le salon a accueilli 91000 visiteurs physiques et plus de 300000 connectés.

De l'intelligence dans l'agriculture

Parler de VivaTech sans parler mobilité est tout simplement impossible, tant ce secteur était omniprésent. Entre le nez d'un TGV-M, un bus de la RATP, ou encore le taxi volant Volocopter, se sont glissées quelques petites technologies, certes plus discrètes mais tout aussi surprenantes.

Le rover de Google X peut aussi détecter les signes de maladies ou de bactéries, et en informer le fermier qui agira en conséquence.

Des chercheurs chez Google X ont, par exemple, mis au point un véhicule baptisé « Mineral ». Destiné aux agriculteurs, ce rover embarque une intelligence artificielle combinée à de l'imagerie. En traversant les champs, il collecte et analyse une multitude de données sur les récoltes et leurs conditions de développement. Citons : la composition des sols, les conditions météorologiques, ou la maturité des plants. L'idée est de faire appel à l'apprentissage automatique pour optimiser les productions, l'utilisation des ressources en eau ou encore l'utilisation de produits phytosanitaires.

« Grâce à l'expertise collective d'agriculteurs, d'éleveurs, de scientifiques et de technologues du monde entier, nous apprenons à remplacer la production alimentaire standardisée par des espèces et des pratiques diverses et plus protectrices », détaillait Google X sur son stand.

Autre découverte sur le stand Région Occitanie, un véhicule électrique et autonome de la startup française Twinswheel, qui est actuellement testé en centre-ville de Montpellier. Il ressemble à s'y méprendre à ces bons vieux Citroën Type H, mais ne vous fiez pas à son look vintage : ce petit véhicule de fret, parfaitement autonome, mélange robotique, intelligence artificielle et électronique. Sa mission ? Assurer la livraison du dernier kilomètre dans des zones piétonnières. *« Il est censé notamment soulager des particuliers ou des professionnels dans leurs tâches quotidiennes qui demandent des efforts »*, nous

Ce véhicule assure de façon autonome la livraison du dernier kilomètre en milieu urbain.

explique-t-on. Et ce, tout en réduisant l'encombrement de la chaussée et en limitant les émissions de CO2. Carreta, autre véhicule de la startup, était également présenté sur le stand de La Poste.

Les robots ont fait le show

Toute la durée du salon, le célèbre automate de chez Boston Dynamics a fait son show sur le stand de la RATP. Pas vraiment une nouveauté, dirons-nous. Mais dans un ballet de contorsions toujours aussi dérangeantes, il semble que le fameux robot-chien Perceval ait trouvé un débouché. Il va être utilisé par la régie pour mener des opérations de maintenance et de prévention du risque incendie à Paris, dans les bouches du métro et du RER. Là encore, son utilisation vise à réduire la pénibilité pour les salariés de la régie.

Un petit dernier pour la route ? La startup normande Conscience Robotics a, elle aussi, présenté plusieurs de ses robots. Tous intègrent une intelligence artificielle universelle. Grâce à elle, *« le robot prend conscience de ses capacités physiques et en tire parti de manière autonome »*, détaille l'entreprise. Il évolue de *« manière autonome et exponentielle dans le temps »*. L'automate peut également détecter des objets dans son environnement et interagir avec eux (allumer un interrupteur, saisir et déplacer un objet). Il peut être contrôlé à distance à l'aide d'une application mobile ou web. L'entreprise travaille avec des industriels désireux d'automatiser et d'optimiser leurs activités.

Livraison sous surveillance

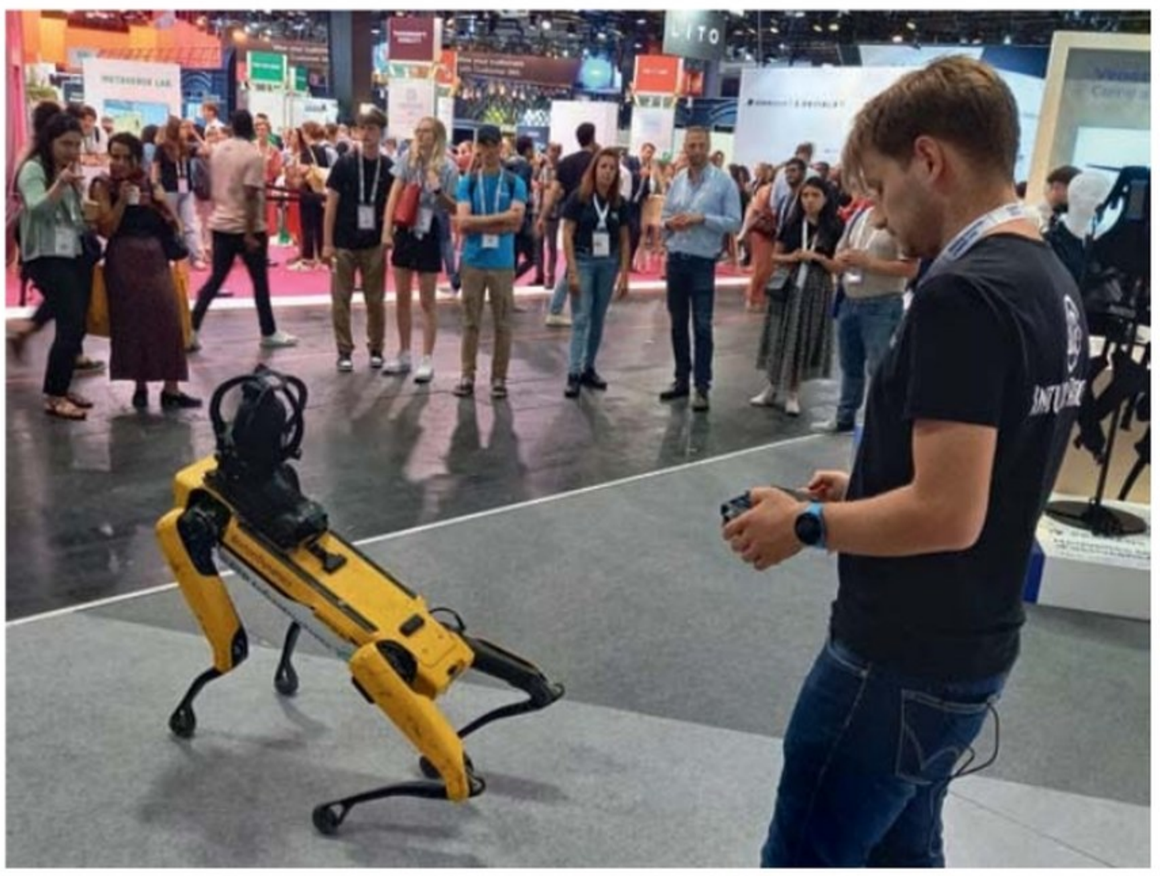
Logistique toujours, mais cette fois, du côté des emballages cartons. Un rapport avec la tech ? Sans aucun doute, en atteste The Box présenté sur le salon par la startup LivingPackets. Avec cette offre, l'entreprise dit vouloir *« remettre de l'intelligence au centre d'une livraison plus responsable »*, nous explique-t-on. Comment ? *Via* la commercialisation d'un emballage entièrement pliable, réutilisable environ 1 000 fois et surtout connecté. Plus précisément, *via* une tablette et un écran E-Ink en lieu et place de l'étiquette de livraison. La tablette embarque un écran, ainsi qu'une multitude de capteurs (températures, humidité, choc, GPS, Wifi, Bluetooth…). Autant d'éléments qui doivent sécuriser les livraisons en temps réel. En cas de choc par exemple, une notification est envoyée au propriétaire du colis.

VivaTech : à votre santé

Le secteur de la santé était, lui aussi, bien représenté sur le salon. Entre autres solutions étonnantes : cette cabine de télésanté à 360° Bodyo, qui effectue un bilan de santé en 6 minutes. La machine calcule pas moins de 26 paramètres à l'aide de bornes intelligentes de santé et de téléconsultation AiPod et Health Loung. Reposant sur l'intelligence artificielle, Bodyo est également capable de réaliser des programmes de prévention personnalisés. La machine trouve tout son intérêt dans les déserts médicaux où son installation, par exemple dans les pharmacies, permettrait de combler un vide.

Et pour finir, un petit gadget avec le Français Actronika. L'entreprise a développé un gilet embarquant de petits moteurs qui génèrent des vibrations, ainsi qu'une intelligence informatique afin de les moduler pour reproduire, au plus proche de la réalité, le sens du toucher. Et ce, dans diverses expériences pour une plus grande immersion dans des mondes virtuels – cinéma, jeux-vidéos… À utiliser avec modération si vous êtes un adepte de jeux de « baston » ! □

Victor Miget



Le robot de Boston Dynamics a été configuré dans les locaux d'Intuitive Robots, pour répondre aux exigences de la RATP. Il embarque, entre autres, un scanner afin de réaliser des radiographies des galeries.

Continuité de services

Cinq risques pesant sur les infrastructures françaises

InfraNum, en partenariat avec la BPI, a dressé le tableau des principaux risques pour les infrastructures numériques en France. En tête, les accidents et les actes de malveillance, lesquels sont de plus en plus fréquents.

Entre les risques climatiques, la pandémie, la guerre sur le sol européen et la fin du réseau cuivre historique, la question de la résilience des infrastructures numériques devient centrale. InfraNum, la Fédération des acteurs français des infrastructures, vient de tirer le signal d'alarme à travers une étude réalisée en partenariat avec Bpifrance. *« Cette première étude, fondée sur une série d'entretiens auprès d'acteurs de la filière, de collectivités locales et de représentants de l'Etat, a pour objectif de : - recenser les aléas pouvant impacter la continuité de service des réseaux FttH - évaluer la criticité de ces aléas - identifier les moyens d'anticipation et de limitation des risques ex ante - proposer des axes d'amélioration en matière de gestion de crise »* énumère InfraNum en préambule.

Dans la nuit du 26 au 27 avril 2022, des fibres ont été sectionnées en divers endroits de la France. Des actes malveillants qui semblent concertés, mais n'ont pas été revendiqués.

La Fédération s'est fondée sur la méthode EBIOS 2010 pour définir une série de scénarios aboutissant à une interruption et/ou une dégradation des services. Le risque est apprécié en fonction de sa gravité et de sa vraisemblance, ainsi que de plusieurs facteurs tels que la récurrence, le nombre d'usagers impactés, leur typologie et la durée de l'interruption. Cette méthode d'évaluation a permis de faire émerger cinq grandes catégories de risques, en tête desquelles on trouve les actes de malveillance et les accidents.

Des actes de malveillance plus nombreux

Selon InfraNum, les actes de malveillance visant aussi bien les infrastructures fixes que mobiles, *« sont de plus en plus fréquents »*. Pour mémoire, fin avril, une vague d'actions malveillantes avait visé le réseau Fibre, perturbant *« les services de télécommunications de plusieurs régions en France, dont l'Auvergne-Rhône-Alpes, la Bourgogne-Franche-Comté, le Grand-Est et l'Île-de-France »*, expliquait alors la Fédération Française des Télécoms. Free a sans doute été l'opérateur le plus touché, mais SFR a aussi été victime de ces détériorations. Le Parquet de Paris a annoncé le 27 avril l'ouverture d'une instruction pour *« atteinte aux intérêts fondamentaux de la Nation »*, *« entrave à un système de traitement automatisé de données »* et « association de malfaiteurs ». Dans son communiqué, le président de la FFT, Arthur Dreyfuss, évoque des « actes de sabotage » et rappelle qu'habituellement ce sont les antennes-relais de téléphonie mobile qui sont ciblées par les actes de vandalisme. On ignore à l'heure actuelle combien d'actions ont été menées contre le réseau fibre, ni quels sont les résultats de l'enquête. De même, les motivations derrière ces actes malveillants restent inconnues à cette heure, personne n'ayant revendiqué les coupures dont l'impact a finalement été limité : peu d'interruptions de services ont été observées, les opérateurs reroutant le trafic de ces grandes artères sectionnées vers des routes secondaires. La Fédération appelle en outre à la vigilance quant aux sites les plus critiques, datacenters ou points de présence, constatant *« des points de fragilité dans les infrastructures assurant la connectivité du site »*. Enfin, les accidents, par exemple lors de la réalisation de travaux de voirie ou en cas d'accident sur la chaussée impactant une armoire, restent selon la Fédération des acteurs des infrastructures une des principales causes d'interruption de services.

Vient en second risque la fragilité des infrastructures aériennes, l'étude rappelant que de 500 000 km des réseaux fibre s'appuient sur des supports aériens. *« Ces segments de réseau sont particulièrement exposés aux intempéries et autres risques. Le rapport préconise donc*

l'enfouissement des réseaux, a minima les plus sensibles et stratégiques, un meilleur élagage, une organisation optimisée concernant les unités d'intervention rapide en cas d'incident et un fonds de soutien exceptionnel, en particulier dans les territoires ultramarins (cyclone, séisme, éruption volcanique, etc.)». Et un coût d'enfouissement estimé à 10 milliards d'euros. Les non-conformités et les malfaçons sont le troisième risque identifié par Infranum. La fédération dénonce notamment l'hétérogénéité de certains éléments de réseau, malgré les efforts de standardisation, qu'elle attribue entre autres à la diversité des maîtres d'ouvrage et des intervenants. De même, lors des opérations de raccordement, la multitude d'intervenants est problématique, augmentant les risques. S'y ajoutent la dégradation prématurée des équipements et le décalage entre le référentiel réseau et la réalité. Dans la construction, les non-conformités sont en outre nombreuses, certaines règles n'étant pas respectées (lovage des câbles, profondeur du génie civil, grillage avertisseur, type de câble optique, boîtiers, dimensionnement des armoires, des câbles). Du côté de l'exploitation, l'étude constate des manquements notamment dans les systèmes d'informations parfois mal renseignés.

Comment gérer les crises ?

Enfin, les interventions sur des réseaux en exploitation *«génèrent mécaniquement un taux d'accidentologie plus important»*. Et la fin du réseau cuivre n'arrange rien, entre les risques d'arrachage des fibres dans leurs fourreaux et autres chutes de poteaux. La densification du réseau lui-même provoque une augmentation des risques d'accidents lors des interventions. Le dernier des risques identifiés par InfraNum est moins un risque en soi que la conséquence desdits risques, puisqu'il s'agit de la capacité à faire face aux crises. En cause, *«une organisation de l'Etat central et déconcentré méconnue par un certain nombre d'acteurs»*, à savoir le Secrétariat général de la défense et de la sécurité nationale ou SGDSN, rattaché au Premier ministre. Mais il faut également compter sur les possibles interventions du Commissariat aux communications électroniques de Défense (CCED), de la Direction générale de la Sécurité civile et de la gestion des crises (DGSCGC), du Haut-fonctionnaire de défense et de sécurité (HFDS) ou encore des préfets. De même, la coordination entre public/privé et local/national est à améliorer. En effet, le découpage des déploiements FttH en France, d'initiative privée ou publique, implique plusieurs opérateurs d'infrastructures - parfois 4 ou 5 à l'échelle d'un département, sans compter les réseaux FttO. Des réseaux qui sont interdépendants, y compris avec des infrastructures non numériques, tant en raison de leur proximité physique (réseaux FttH déployés sur le domaine public routier ou appuis communs du réseau de distribution d'électricité) qu'aux liens entre les exploitants. Sur ce point, très discuté lors de la table-ronde qui a suivi la présentation de cette étude, InfraNum réitère son appel à un *«Grenelle de la résilience et de la souveraineté des infrastructures numériques»*. *«Les opérateurs d'infrastructure sont en première ligne, or jusqu'à présent, lors de crise, ils ne sont pas consultés. Et de multiples acteurs interviennent sur le réseau. Il y a un vrai besoin de coordination lors de crise, avec une filière bien organisée et justement rémunérée»* soutient Eric Jammaron, Vice-président d'InfraNum et Président d'Axione.

Demeure enfin, et inévitable, la question du financement. Antoine Darodes, Directeur du département Investissements Transition Numérique de la Caisse des dépôts, explique que *«le plan France THD est un colosse au pied d'argile. C'est un ensemble de solutions qui permettra d'atteindre cette résilience. Et face au besoin d'investissement que certaines mesures vont générer, la Banque des territoires répondra présente si tant est que les notions de solidarité territoriale et de long terme prévalent dans ces projets»*. InfraNum entend se servir de cette étude pour sensibiliser le gouvernement sur ce sujet de la résilience des infrastructures numériques, tout en encourageant les collectivités dans la mise en place de *«schémas locaux de la résilience»*. □

De gauche à droite : Thomas Gassilloud, Eric Jammaron, Antoine Darodes, Yann Breton.

BIGDATA & AI PARIS by corp

Conférence et Exposition

11e Edition • 26 & 27 septembre 2022

Palais des Congrès • PARIS et en ligne

BIG DATA AI

DevOps
Reinforcement learning
Ethique
Robotique
Data for Good
Cybersecurité
Gouvernance et qualité
Cloud
IA Green
Machine learning
NLP / NLG
Automatisation

TIME TO ACCELERATE

15 000 PARTICIPANTS

350 INTERVENTIONS

250 ENTREPRISES EXPOSANTES

Inscription gratuite sur www.bigdataparis.com

Aux États-Unis, la Silicon Valley perd de son attractivité

Vers un mouvement de fond ?

La Californie et la Silicon Valley verraient-elles les entreprises de la Tech les délaisser ? Une étude publiée par la Brookings Institution, basée sur les données 2015-2019 de la société Emsi Burning Glass, le Bureau américain des statistiques du travail et la plateforme d'emploi Crunchbase, montre que ce haut lieu de l'industrie technologique perd petit à petit son attractivité.

Si la croissance et l'emploi de ce secteur sont encore largement issus de cette zone géographique, il semble que d'autres métropoles attirent les entreprises. Les raisons ? Le poids des taxes et les difficultés de logement. Ce phénomène s'est encore accéléré avec la pandémie de Covid-19 qui a vu de plus en plus d'Américains fuir les grandes zones urbaines. S'agit-il d'un mouvement de fond ? L'avenir le dira.

La fin d'un mythe

Et si la Silicon Valley perdait petit à petit son attractivité auprès des entreprises de la Tech ? Selon une étude publiée par la Brookings Institution, basée sur les données 2015-2019 de la société Emsi Burning Glass, le Bureau américain des statistiques du travail et la plateforme d'emploi Crunchbase, toute la géographie du secteur de la Tech serait en pleine évolution avec une perte de l'emprise de la Silicon Valley. Pour information, ce pan économique a enregistré une croissance annuelle de 4,4% dans les années 2010, soit plus du double des États-Unis au cours de cette décennie. Certains diront que c'est un sujet récurrent qui revient régulièrement sur la table ou que la Silicon Valley reste l'endroit où il faut être. *« Il y a peu de localisations dans le monde où l'on trouve autant de talents en ingénierie »*, explique John Colgrove, fondateur et Chief Visionary Officer de Pure Storage, dont le siège est installé à Mountain View (Californie).

Toutefois, le fait d'intégrer l'année 2020 dans l'analyse, avec le tout début de la pandémie de Covid-19 et toutes ses conséquences (entreprises fermées, explosion du télétravail...), laisse penser que ce phénomène est cette fois-ci bien visible dans les chiffres. D'autant plus que l'étude couvre un large spectre d'entreprises avec des entités issues de la fabrication d'ordinateurs et de semi-conducteurs, des éditeurs de logiciels, des acteurs du traitement et l'hébergement de données, de la conception de systèmes informatiques, et même les autres services d'information

comprenant des entreprises comme Google, Meta et Netflix. La question est de savoir pourquoi de nombreuses entreprises ont décidé de quitter cette zone géographique. Il existe de nombreuses raisons, mais le poids des taxes sur les sociétés et les problématiques de logements sont celles qui reviennent le plus souvent.

Une industrie encore concentrée sur les côtes

Selon l'étude, les États-Unis comptent 100 grandes zones métropolitaines et 83 d'entre elles ont enregistré une croissance de l'emploi dans le secteur des technologies sur la période 2015-2020. Toutefois, les chiffres montrent qu'une majeure partie de cette hausse s'est concentrée dans quelques pôles technologiques côtiers, démontrant que l'ensemble des États-Unis n'a pas encore entièrement accès à la prospérité du secteur technologique. Par exemple, les villes de San Francisco et San José (Californie) ont généré à elles seules 20 % de la croissance technologique du pays avant la pandémie. Si aucun chiffre ne circule, cette tendance s'est néanmoins atténuée depuis le début de la pandémie de Covid-19. Cette concentration sur les côtes américaines, notamment en Californie, est source de vrais blocages. *« Cela crée des problèmes d'accessibilité au logement, de circulation et de qualité de vie »*, explique Mark Muro, chargé de recherche et directeur des politiques au sein de la Brookings Institution et coauteur du rapport.

Une ouverture progressive à l'ensemble du pays

Au cours de la période 2015-19, plusieurs grandes zones ont vu la part de l'emploi total du secteur technologique augmenter de manière significative. On peut ainsi citer les villes de San Francisco, San José, New York, Washington, Seattle (Washington), Boston (Massachusetts), Los Angeles (Californie) et Austin (Texas). Ensemble, ces huit villes ont représenté près de la moitié de la croissance nationale de l'emploi dans le secteur des technologies. Mais un certain nombre de métropoles montantes ont également affiché une croissance significative avant la pandémie. Parmi elles, figurent Atlanta (Géorgie), Dallas (Texas), Denver (Colorado), Miami et Orlando (Floride), San Diego (Californie), Kansas City et Saint-Louis (Missouri) et Salt Lake City (Utah). La croissance de l'emploi dans ces centres s'est toutefois ralentie dès 2020 tombant de 4.9% entre 2015 et 2019 à 2,9%. La pandémie, accompagnée de confinements parfois très stricts comme à New York, explique évidemment ce ralentissement.

Mais, pendant que ces grandes métropoles subissaient les effets de la crise de la Covid-19, cela a pleinement profité à des villes moyennes dans tous les États-Unis. On peut ainsi citer Philadelphie (Pennsylvanie), Cincinnati (Ohio), Minneapolis (Minnesota), Charlotte (Caroline du Nord), San Antonio (Texas), la Nouvelle-Orléans (Louisiane) et Ithaca (État de New York). Dans le rapport, Mark Muro parle de « villes Zoom ». Selon lui, il s'agit d'endroits où le coût de la vie est inférieur à celui des grands centres technologiques côtiers et où les travailleurs à distance ont élu domicile pendant la pandémie pour quitter les zones surpeuplées. Pour donner un exemple, la ville de New York affiche une densité de 7 250 habitants au km2 contre 980 habitants au km2 pour Charlotte ou 1 500 habitants au km2 pour Cincinnati. Enfin, le rapport de la Brookings Institution montre que le passage à des horaires flexibles en raison du travail à domicile a eu un impact réel sur la géographie des emplois technologiques.

Il serait intéressant de voir les chiffres sur les années 2021 et 2022 pour mesurer si l'emploi technologique des États-Unis est vraiment en train de migrer vers des métropoles de taille moyenne ou s'il s'agit d'un mouvement provisoire qui sera balayé par la puissance de la Silicon Valley. ☐

Michel Chotard

AVEC PINFLEX, PINTEREST PROMEUT L'AUTONOMIE

La société Pinterest, basée à San Francisco, a fait le choix de ne pas quitter la Californie comme d'autres entreprises. En revanche, le réseau social a voulu donner plus de liberté à ses employés dans le choix de leur lieu de travail. En avril, l'entreprise a ainsi introduit PinFlex, un modèle de travail unique. *« Ce programme offre aux employés l'autonomie nécessaire pour vivre et travailler de manière flexible, tout en donnant la priorité à la collaboration intentionnelle en personne dans nos bureaux »*, explique le réseau social. De ce fait, les employés peuvent choisir où travailler, que ce soit depuis un bureau Pinterest, leur domicile ou un emplacement virtuel dans l'un des cinquante états des États-Unis et à l'international.
Pour ce qui concerne les projets ou activités qui nécessitent la présence des équipes dans un bureau de l'entreprise, Pinterest couvrira les frais de déplacement (environ 100 kilomètres) et les dépenses des employés. *« PinFlex apporte une flexibilité et une autonomie maximales qui offriront une expérience tout aussi productive et inclusive pour tout le monde, peu importe qui vous êtes et où vous travaillez. Nous avons conçu ce modèle de travail en collaboration avec des dirigeants, des gestionnaires et des employés, afin de créer une communauté connectée et un environnement inspirant pour chaque employé »*, détaille Christine Deputy, directrice des ressources humaines de Pinterest. Les employés devront toutefois se rendre dans un bureau Pinterest au moins une fois par an pour se rencontrer les uns aux autres et participer aux activités pour la promotion de la culture de l'entreprise.

Formation pour tous ?

Microsoft veut former 10 000 Français et Françaises

C'est au Campus Cyber que Microsoft a révélé son plan pour s'attaquer au déficit de compétences en cybersécurité. Le géant de Redmond prévoit ainsi des actions de sensibilisation dans les écoles et de formation auprès des étudiants, des professionnels et des demandeurs d'emploi.

Il manque en France 15 000 postes en cybersécurité. Mais, pour Bernard Ourghanlian, Directeur Technique et Sécurité chez Microsoft France, *« voilà 5 ans qu'on a le même chiffre : on écope le problème sans réussir à le vider »*. Ou encore un véritable « tonneau des Danaïdes ». Partant de ce constat, l'éditeur a lancé un grand plan, avec un objectif ambitieux : former 10 000 personnes en France sur trois ans. Trop ambitieux peut-être : Microsoft peut-il répondre à lui seul aux deux tiers du besoin de compétence ? Bernard Ourghanlian est confiant : *« quand on regarde objectivement les formations, rien que sur la partie partenariat avec l'enseignement supérieur, on forme 1000 personnes par an »*.

Dévoilé le 31 mai dans les locaux du Campus Cyber, ce Plan Compétences Cybersécurité s'articule autour de deux priorités : sensibiliser et former. Sur le premier volet, Redmond met à disposition des collèges et des lycées français un kit pédagogique *« pour donner aux enseignants, aux collégiens et aux lycéens les moyens de s'emparer de ces sujets »* nous explique Bernard Ourghanlian. Cet outil, disponible sur GitHub et intitulé *« La cybersécurité, mon futur métier »*, donne divers conseils pour se prémunir contre les attaques et des informations sur les métiers du secteur, afin, notamment, *« d'évacuer un certain nombre de biais qu'on peut se faire au sujet des représentations des experts en cyber »*. Un guide intervenant, destiné à l'animation des séquences de sensibilisation, complète l'ensemble.

Professionnels, étudiants, demandeurs d'emplois

Côté formation, Microsoft sort l'artillerie lourde. Il s'appuie déjà sur des partenariats avec des écoles, par exemple avec un MOOC de 3 semaines *« Cybersécurité défensive en environnement Microsoft »* proposé aux étudiants de l'ECE Paris, d'EPITA, d'EPITECH et de l'EFREI Paris. Une formation qui sera proposée à la rentrée prochaine aux étudiants de Guardia Cybersecurity School et de l'Ecole 2600, mais aussi aux étudiants en BTS Services Informatiques des organisations. Ainsi, Microsoft prévoit de passer de 220 étudiants suivant ce MOOC à 1000 sur l'année scolaire 2022. *« La question se pose également d'adresser les professionnels de l'informatique qui veulent acquérir des compétences dans le domaine du cyber, à travers un certain nombre d'initiatives »*. Le Directeur Technique et Sécurité chez Microsoft France revient notamment sur les actions existantes, à l'instar d'Enterprise Skills Initiative proposée aux clients et aux partenaires de l'éditeur ou encore du Cybersecurity Institute, monté avec Avanade. La principale nouveauté sur ce terrain est le passage en gratuit de deux formations LinkedIn Learning, *« La sécurité et défense de Windows »* et *« Sécuriser Active Directory contre les menaces actuelles »*, auparavant uniquement accessibles via LinkedIn Premium.

Bernard Ourghanlian,
Directeur Technique et Sécurité chez Microsoft France.

« La question se pose également d'adresser les professionnels de l'informatique qui veulent acquérir des compétences dans le domaine de la cyber. »

Enfin, Microsoft veut s'adresser aux demandeurs d'emploi, en mettant sur pied une « Ecole Cyber Microsoft » en partenariat avec Simplon. Cette formation consiste en un sas de préqualification de 8 semaines pour intégrer la formation, sas servant à l'apprentissage des bases et s'achevant avec l'obtention d'une certification, suivie d'un cursus de 3 mois de formation intensive, et 15 mois en alternance pour être formé au métier d'Opérateur Sécurité Cloud et Hybride, ici en partenariat avec Advens. Ces écoles devraient, à terme, être déclinées en région : *« nous voulons être proches des bassins d'emplois, parce que les gens n'ont pas toujours la possibilité de se déplacer, avec des partenaires locaux et une implantation territoriale de ces écoles cyber »* indique Bernard Ourghanlian. La première année, Microsoft veut former ainsi une centaine de personnes. ☐

Guillaume Périssat

La place des architectes se confirme

Un rôle stratégique

Une étude réalisée par le cabinet ESG pour le compte de Mega fait le point sur la vision et le rôle que joue désormais les architectes IT dans les entreprises.

L'étude menée auprès de 300 professionnels de l'architecture aux USA et en Europe indique un changement de vision sur la valeur apportée par les architectes dans les entreprises. 44% des entreprises ont une vision de l'architecture d'entreprise centrée sur l'informatique contre 26% centrée sur le business. Seuls 18% des architectes interrogés affirment qu'ils sont systématiquement consultés dans le cadre de projets de développement de l'entreprise. Il est cependant souligné que les collaborations internes avec les architectes d'entreprises concernent majoritairement les département sécurité, R&D et développement d'applications, domaines dans lesquels la valeur ajoutée de l'architecture d'entreprise n'est plus à prouver.

Les départements sécurité reconnaissent notamment à 77% la haute valeur ajoutée de l'architecte d'entreprise associée à la Gestion des Risques et de la Conformité (GRC). De même, les organisations qui considèrent avant tout l'architecture d'entreprise comme un soutien technologique reconnaissent à 46% sa valeur indéniable dans la gouvernance des données (récolte, utilisation, modification, hiérarchisation, sécurisation et confidentialité) ainsi que pour son efficacité dans la gestion des coûts IT.

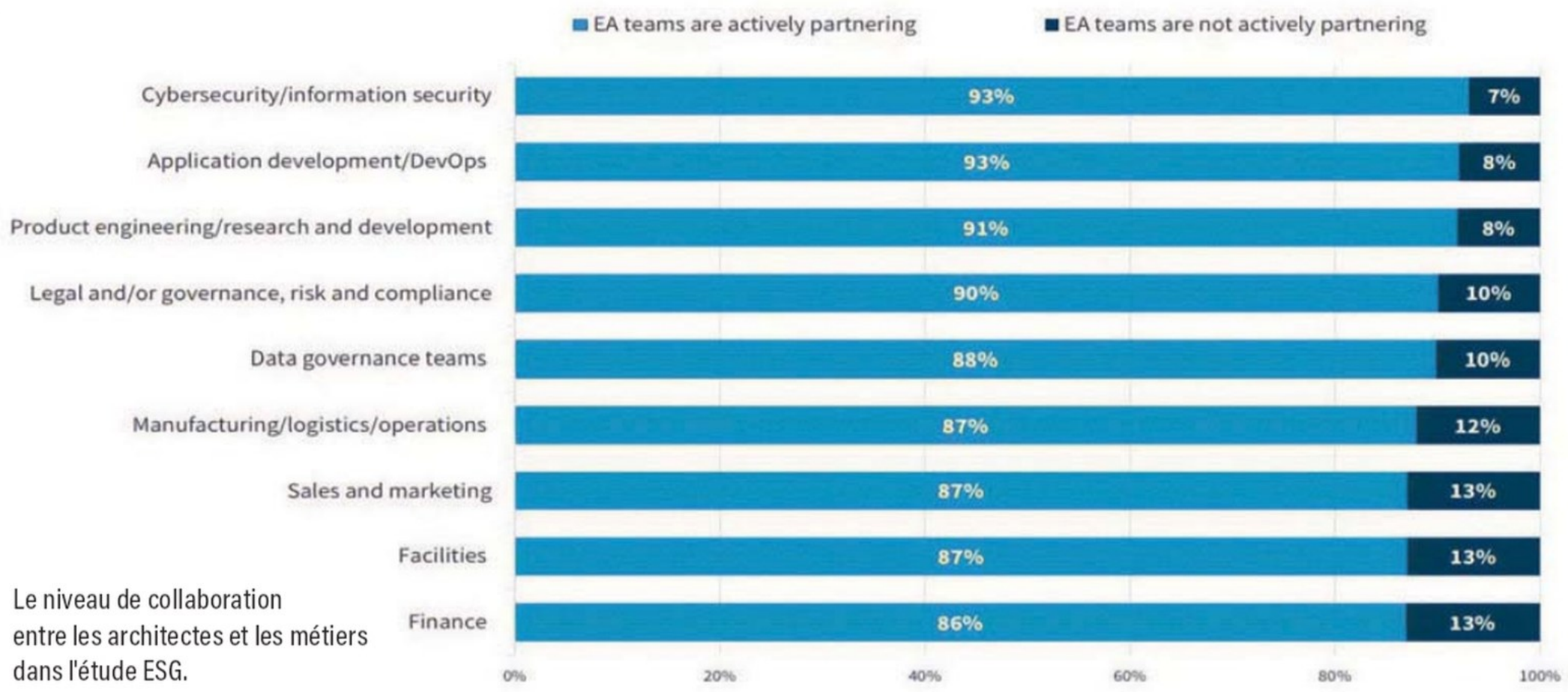
Des investissements en hausse

Cette nouvelle reconnaissance s'accompagne d'une hausse des investissements dans les outils et plate-formes d'architecture d'entreprise. Sur les deux dernières années, 99% des professionnels interrogés affirment avoir réalisé des investissements dans des outils et plateformes d'architecture d'entreprise. 70% des organisations déclarent que leurs investissements en architecture d'entreprise ont augmenté (de 15,7% en moyenne) et 97% d'entre-elles prévoient plusieurs investissements significatifs dans les deux prochaines années. Les principales motivations de ces investissements sont la fluidification de l'information, l'amélioration des processus métiers et des architectures cloud. L'automatisation et le renfort de l'intelligence artificielle sont les deux arguments majeurs mis en avant par les répondants pour l'obtention des financements. Ils pourront notamment compter sur des alliés majeurs pour convaincre leur direction : les CTOs et les CIOs.

Des freins toujours présents

80% des architectes d'entreprise interrogés déclarent que leur entreprise souffre encore de trop de process manuels et 79% d'entre eux estiment qu'ils ont beaucoup de difficultés à collaborer avec l'ensemble de leur organisation. Quand l'architecture d'entreprise a pour principale vocation de soutenir les métiers de l'entreprise et leur transformation, elle se heurte aux difficultés liées à la collaboration avec les métiers et à des objectifs en contradiction avec les priorités IT. En conséquence, pour une très large majorité des répondants, les projets sont plus longs à mettre en place (95%) et supportent des coûts plus élevés (97%) que prévu. Et pourtant, malgré des projets jugés difficiles, longs et coûteux, on constate, finalement, une satisfaction des architectes. De plus, 7 personnes interrogées sur 10 estiment que leurs équipes d'architectes apportent de la valeur ajoutée dans les domaines clés qu'elles ont identifiés. □

B.G



Le niveau de collaboration entre les architectes et les métiers dans l'étude ESG.

EXPOSITION • CONFÉRENCES • TABLES RONDES • ATELIERS • RENDEZ-VOUS PROJETS

SALONS SOLUTIONS

11 & 12 octobre 2022

PARIS EXPO
PORTE DE VERSAILLES

SALONS SOLUTIONS erp

SALONS SOLUTIONS démat

SALONS SOLUTIONS crm

SALONS SOLUTIONS bi

SALONS SOLUTIONS e-achats

Platinum sponsor

axelor

Gold sponsors

coupa UNIT4

Silver sponsor

systhen
Making data valuable

@SalonsSolution1
#salonssolutions

MC SalonsSolutions

Avec en parallèle

mobility for business

salons-solutions.com

+ de 100 recrutements par an !

Adista
Opérateur de
Services Hébergés

Adista, 1er opérateur cloud & télécoms alternatif B2B en France.

- **La force d'un groupe en hyper croissance, la proximité de 35 agences et 11 datacenters.**
- **Une forte diversité de métiers IT : techniciens, administrateurs, chargés de projets, experts IT, responsables d'équipe…**
- **Une entreprise récompensée pour sa stratégie RSE (Prix de la Politique RSE du Sommet des Entreprises de Croissance)**

Rejoignez-nous !

jobs.adista.fr

Des espaces collaboratifs avec du flex office, de nombreux évènements dédiés aux équipes (vis mon job, échanges informels avec la direction, émission TV interne, mini jeux…)

Lauréat des Trophées 2022 :

SOMMET DES ENTREPRISES DE CROISSANCE

TOPTECH ESN

FRANCE BEST MANAGED COMPANIES