Silicon

INSIGHTS FOR IT PROFESSIONALS

Silicon.fr

CRISE CYBER
OUTILLER LA GESTION DES RISQUES

SECNUMCLOUD
LA NAISSANCE D'UN ÉCOSYSTÈME

SERVERLESS
L'ÂGE DE LA MATURITÉ

+ TRENDS OF IT 2023
DANS LA TÊTE DES RSSI

N° 16 - SEPTEMBRE 2023

L 314277 -16 - F: 25€ - RD

mgen

GROUPE VYV

EMPLOYEZ-NOUS

À VOUS METTRE AU CŒUR DE LA TRANSFORMATION

EXPERT(E) CYBERSÉCURITÉ

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

REJOIGNONS-NOUS SUR RECRUTEMENT.MGEN.FR

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

#mutuellement

DANS LA TÊTE DU **RSSI**

La cybersécurité est durablement inscrite au cœur de l'agenda IT des entreprises. C'est donc, logiquement, que la thématique se retrouve parmi les cinq thèmes majeurs de Trends of IT 2023, notre étude réalisée avec KPMG (p.19 à 25). Co-construite avec plusieurs RSSI, elle révèle des résultats qui se distinguent de ceux que l'on trouve habituellement dans ce type d'exercice.

Outre les défis «classiques » à relever, en particulier l'incomplétude d'inventaire des assets IT et la gestion du shadow IT, elle met l'accent sur la pénurie de ressources humaines et de talents. La principale raison est le manque de formation et d'éducation. Si on assiste depuis peu à l'éclosion d'écoles spécialisées, les universités et les écoles d'ingénieurs n'ont pas encore intégré la cyber dans leurs programmes de manière exhaustive. Autre contrainte : la difficulté de maîtriser des technologies qui sont en constante évolution.

Face à cette situation, les RSSI ont pris les choses en main. Selon notre étude, 60% des répondants indiquent proposer des parcours de mobilité ou de reconversion à leurs employés, et 36% interviennent directement dans les écoles et les universités pour former les étudiants en espérant les recruter par la suite.

Autre challenge pour l'ensemble de la filière : communiquer sur la diversité et l'intérêt des métiers de la cyber, allant de l'audit à la gouvernance, en passant par la conformité et la gestion des risques.

Philippe LEROY
Rédacteur en chef
pleroy@netmedia.group

SOMMAIRE

FOCUS

LES TEMPS FORTS DE L'ACTUALITÉ

Logiciels ..... p. 6
Carrière - Formation ..... p. 8
Cybersécurité ..... p. 10
ChatGPT ..... p. 12
Business ..... p. 14
Data & IA ..... p. 16

ZOOM

Start-up cyber, six levées de fonds qui ont marqué 2023 ..... p. 18

CAHIER SPÉCIAL

TRENDS OF IT 2023 ..... p. 19

DOSSIER

CYBERSÉCURITÉ

Le Cloud souverain joue la carte SecNumCloud ..... p. 26
Pourquoi il faut outiller la gestion du risque cyber ..... p. 30
Comment le XDR se déploie sur les SI ..... p. 34
Risques liés aux tierces parties : difficile de les réduire ..... p. 40
Serverless, l'âge de la maturité technologique ..... p. 44

CYBERATTAQUE

La Seine-et-Marne porte encore les stigmates ..... p. 48

SASE

Peut-on faire avec un seul fournisseur ? ..... p. 49

RETEX

Carrefour Links pilote les transferts de données avec le Serverless ..... p. 50

RETEX

Comment Lego empile les briques Serverless pour rendre ses services incassables ..... p. 52

IA & ML

Comment Netflix a conçu son infrastructure de machine learning ..... p. 54

DEVOPS

Ces plateformes qui reconfigurent le marché ..... p. 56

Éditialis
98, rue du Château,
92645 Boulogne-Billancourt Cedex
Pour envoyer un e-mail à votre correspondant, suivre le modèle : pleroy@netmedia.group

NetMediaGroup

PRÉSIDENT
Pascal Chevalier

DIRECTEUR GÉNÉRAL ET DIRECTEUR DE LA PUBLICATION
Hervé Lenglart

DIRECTEUR GÉNÉRAL ADJOINT FRANCE
Jean-Sébastien Rocheteau

ÉDITORIAL
RÉDACTEUR EN CHEF
Philippe Leroy (pleroy@netmedia.group)

RÉDACTION
Clément Bohic (cbohic@netmedia.group)

ONT PARTICIPÉ À CE NUMÉRO
Alain Clapaud

RESPONSABLE DU STUDIO
Catherine Saulais

CONCEPTION GRAPHIQUE
Bench Media Factory

RÉALISATION
Mise en page : Catherine Saulais
Secrétariat de rédaction : Yann Guillaud
Crédits photos Adobe Stock

PUBLICITÉ
DIRECTEUR COMMERCIAL
Simon Leprat (01 41 31 72 41) sleprat@netmedia.group

CHEFS DE PUBLICITÉ
Mathilde Poirot (01 46 99 22 95) mpoirot@netmedia.group
Paul Gloaguen - pgloagen@netmedia.group

ABONNEMENT ET MARKETING
DIRECTRICE MARKETING AUDIENCE
Camille Lhotellier clhotellier@netmedia.group

RESPONSABLE MARKETING et ABONNEMENT
Nicolas Cormier (01 41 31 72 44) ncormier@netmedia.group

CHARGES DE TRAFIC et RESPONSABLE DES PARTENARIATS
Thao Meillat (07 83 12 68 17) tmeillat@netmedia.group

IMPRESSION
Léonce Deprez, allée de Belgique, 62128 Wancourt

TARIFS
Prix au numéro : France 25 €
Abonnement 1 an. France métropolitaine 120 € (TVA 2,10 %)
L'abonnement comprend le magazine en versions print et digitale accessible sur PC, tablettes et smartphones, la newsletter quotidienne et l'accès au site silicon.fr
4 numéros par an. Trimestriel.
Abonnement 1 an. Étudiant, DOM-TOM et étranger : nous contacter

Silicon est édité par Éditialis, SAS au capital de 136 000 €
Actionnaire NetMedia Group
N° ISSN : 2681-1006
Numéro de commission paritaire : 1226T94134
Dépôt légal : novembre 2019
Date de parution : septembre 2023

Origine du papier Schwedt, Allemagne
Taux de fibres recyclées 100 %
Eutrophisation Ptot 0,004 kg/tonne

USB : PROTECT BEFORE CONNECT

Hogo Business Services

AZURE ACTIVE DIRECTORY devient MICROSOFT ENTRA ID

Officiellement lancée en mai 2022, la gamme Entra couvre, dans le portefeuille sécurité de Microsoft, la gestion de l'identité et de l'accès réseau. Azure Active Directory (Azure AD ou AAD) en est la brique de base. Il ne faudra bientôt plus l'appeler ainsi. La marque Microsoft Entra ID doit prendre le relais d'ici à la fin de l'année. URL de connexion, bibliothèques d'authentification, commandes PowerShell, API..., rien ne changera fonctionnellement parlant. Tout est une affaire de branding. En la matière, le « grand renommage » des licences et des SKU interviendra le 1er octobre 2023. Ces changements ne concernent pas la version sur site d'Active Directory. Même chose pour AAD B2C, les services de fédération Active Directory (ADFS) et les services de domaine Active Directory (AD DS).

ORACLE ACTIVE SON "CLOUD PUBLIC SOUVERAIN" DANS L'UE

Le groupe américain a repris l'architecture et le modèle d'exploitation de ses régions gouvernementales disponibles aux États-Unis et au Royaume-Uni, mais dans une optique d'Union européenne et sans restriction de clientèle. L'infrastructure comprend, pour le moment, deux datacenters, en Allemagne (Equinix, à Francfort) et en Espagne (Digital Realty, à Madrid).

LES 3 HYPERSCALERS POURSUIVENT LEUR CROISSANCE EN FRANCE

Selon Markess by Exægis, les trois hyperscalers américains captent l'essentiel de la croissance du Cloud en France avec une part de marché, cumulée, de 70 %. Ainsi, AWS conserve 45% d'un marché français qui est passé, entre 2020 et 2022, de 1,4 à 2,5 milliards d'euros. En deuxième position, l'offre Azure de Microsoft s'arroge 18% quand celle de Google Cloud se fixe à 8 %. Les autres fournisseurs de Cloud public, parmi lesquels OVHcloud, Orange Business, Outscale, Scaleway, Cloud Temple, Oracle ou encore IBM Cloud ont réalisé ensemble 25% de croissance et concentrent 29% du marché.

FINOPS: GOOGLE CLOUD BRANDIT LA CERTIFICATION

Google Cloud devient le premier hyperscaler à bénéficier directement d'une certification FinOps Foundation. Une distiction obtenue dans la catégorie « Service Provider », qui, dans les grandes lignes, englobe la partie conseil. Il y rejoint 16 autres entreprises dont Accenture, Deloitte mais aussi la française Timspirit. La plupart d'entre elles couvrent le framework de la FinOps Foundation plus largement que Google Cloud. Rappelons que Google Cloud est membre de premier niveau de la fondation, comme Microsoft.

IBM

lâche l'éducation

IBM abandonne son service « Cloud for Education » deux ans après son lancement. Il proposait, au secteur académique et aux laboratoires de recherche, plusieurs types de machines virtuelles. Une offre managée, hébergée sur le Cloud d'IBM, et préconfigurée avec des applications telles que SPSS, SAS et AutoCAD.

Google Cloud

attaque Microsoft

Google a déposé plainte auprès de la FTC, accusant Microsoft d'abuser de sa position dominante pour diriger les clients vers ses propres services Cloud. La plainte avance que Microsoft met en exergue les conditions de licence de sa suite de productivité Office 365 pour pousser les clients vers son Cloud Azure et des services associés.

Microsoft Azure Linux

sort de l'ombre

Il s'agit d'un système d'exploitation conçu pour être déployé dans le Cloud et pour exécuter essentiellement des conteneurs. Il s'exécute en tant que machine virtuelle sur Hyper-V, l'hyperviseur Windows de Microsoft.

LENOVO THINKPAD Z13

Testé et approuvé par un DG

Le quotidien d'un dirigeant d'entreprise est fait de sollicitations incessantes et d'activités multiples qui l'amènent à faire preuve d'agilité. Florian Bouron, CEO de Mozzaik365, a testé le Lenovo ThinkPad Z13. Il partage son retour d'expérience.

Éditeur de solutions de digital workplace intégrées à Microsoft 365, Mozzaik365 s'est donné pour mission de favoriser la communication, l'engagement et l'efficacité des collaborateurs au sein de l'entreprise. Son fondateur et dirigeant, Florian Bouron, a fait le choix de tester le Lenovo Thinkpad Z13 à chaque fois qu'il serait en situation de télétravail régulier. « Je souhaitais pouvoir évaluer les capacités réelles de la machine dans les conditions réelles de mon exercice professionnel », souligne le dirigeant. L'impression générale est sans appel : « sur le plan esthétique, autant que celui de l'ergonomie générale, le Lenovo ThinkPad Z13 est taillé pour les profils de direction générale. La finition cuir de la coque extérieure est une réussite ».

Une réponse à des usages professionnels exigeants

Alors qu'il utilise d'ordinaire l'environnement MacOs, Florian Bouron a été surpris de la vélocité et de l'agilité du Lenovo ThinkPad Z13. « Lorsque vous ouvrez simultanément quatre présentations Powerpoint, trois fichiers Excel et que vous réalisez une visioconférence, très vite, la mémoire vive de la machine est saturée. L'excellente surprise, avec le Lenovo ThinkPad Z13, c'est que je n'ai jamais rencontré ce genre d'effets indésirables... ». L'ergonomie et l'agencement des fonctionnalités est un autre atout majeur. « Dans l'expérience proposée par le Lenovo ThinkPad Z13, tout était merveilleusement pensé car je pouvais facilement accéder à la galerie de services Microsoft 365. Mais à la mise en service de la machine, la connexion avec mon compte Office Entreprise n'a pas été immédiatement reconnue à l'activation de la machine ». Un léger désagrément vite compensé après avoir procédé à l'installation de la version entreprise de Microsoft 365. Soulignant la puissance du Lenovo ThinkPad Z13, il explique avoir « apprécié la fluidité avec laquelle l'ordinateur a pu m'accompagner dans toutes mes activités, y compris les plus exigeantes ».

Une autonomie à toute épreuve

Parce que les journées d'un dirigeant d'entreprise sont un marathon permanent, faites de rendez-vous incessants, de tâches diverses à mener de front, et de nombreuses heures d'utilisation successives chaque jour, l'enjeu de l'autonomie est crucial. « Le Lenovo ThinkPad Z13 s'est révélé être une excellente surprise sur le plan de l'autonomie », confie Florian Bouron.

La biométrie au service des politiques de sécurité

Comme tout professionnel, Florian Bouron est très attentif aux questions de sécurisation des données et de protection du système d'information. « La reconnaissance faciale est un atout pour faciliter le respect des principes de base de la sécurité, notamment l'accès aux services en ligne qui nécessitent une identification à chaque nouvel accès ». Une intégration native de fonctionnalités biométriques qui s'est révélée particulièrement fiable durant toute la phase de tests réalisée par Florian Bouron. « L'image que j'ai de la marque ThinkPad, c'est celle d'une bureautique professionnelle haut de gamme. Avec le Lenovo ThinkPad Z13, j'ai retrouvé parfaitement cet esprit de robustesse, de performance et d'efficacité ».

inmac wstore

Lenovo

CINQ CERTIFICATIONS CLOUD POUR VALORISER UNE EXPERTISE

Ingénieur Cloud computing, ingénieur FinOps, architecte solutions... font partie des profils métiers IT les plus demandés du marché. La certification de compétences permet de se distinguer. Aux États-Unis, le salaire annuel moyen des professionnels certifiés du Cloud computing est compris entre 110 000 et 134 000 dollars. En France, il varie de 60 000 euros pour un architecte solutions en début de carrière à plus de 90 000 euros pour un ingénieur FinOps expérimenté.
Voici cinq des certifications d'AWS, Azure et Google Cloud parmi les plus rémunératrices du marché.

AWS Certified Solutions Architect – Associate

La certification Solutions Architect – Associate valide auprès des différents acteurs du marché les connaissances de professionnels acquises dans le Cloud Amazon Web Services (AWS) : calcul, mise en réseau, stockage, base de données, déploiement et gestion applicative. L'examen prend la forme de questions et réponses à choix multiples. Il atteste de la capacité de professionnels à concevoir des solutions optimisées pour la « performance » à l'aide d'AWS. Amazon, IBM et Capgemini font partie des recruteurs potentiels de professionnels certifiés.
Coût de l'examen : 150 dollars

AWS Certified SysOps Administrator — Associate

Obtenir la certification SysOps Administrator – Associate permet de valider une expérience du déploiement, de la gestion et de l'exploitation de charges de travail sur le Cloud d'Amazon. La mise en œuvre de contrôles de sécurité et d'exigences de conformité est également au menu.
Parmi les recruteurs potentiels se trouvent Capgemini et Oracle.
Coût de l'examen : 150 dollars

Microsoft Certified Azure Administrator Associate

Une expérience de la gestion et du suivi d'un environnement Microsoft Azure est requise. L'obtention de la certification Azure Administrator Associate démontre les capacités de professionnels expérimentés à fournir des solutions et services (réseau, sécurité, base de données, développement applicatif et DevOps) en s'appuyant sur le Cloud de Microsoft.
Accenture et Dell Technologies font partie des recruteurs éventuels.
Coût de l'examen : 165 euros

Microsoft Certified Azure Fundamentals

Services, charges de travail, sécurité, confidentialité, prix et support Azure... La certification Azure Fundamentals valide des connaissances de base des services Cloud et la manière dont ces services sont fournis avec Azure.
Coût de l'examen : 99 dollars

Google Associate Cloud Engineer

Configurer, planifier et déployer des solutions, en paramétrer l'accès et la sécurité... Les titulaires de la certification Associate Cloud Engineer peuvent témoigner de leur capacité à implémenter, surveiller et gérer des solutions d'entreprise en s'appuyant sur le Cloud de Google. L'examen prend la forme de questions à choix et sélections multiples. La certification est valide pendant trois ans à partir de la date de certification.
Google, Deutsche Bank et Goldmann Sachs font partie des entreprises qui embauchent.
Coût de l'examen : 125 dollars

LENOVO THINKPAD Z13

Testé et approuvé par un DSI

Entre performances, esthétique, robustesse et sécurité, pourquoi faudrait-il choisir ? Nicolas Lagardère, Responsable des Services Informatiques pour Mecadaq, a accepté de tester le Lenovo ThinkPad Z13. Il partage son retour d'expérience.

Mecadaq Group est une entreprise spécialisée dans l'usinage et la fabrication des pièces complexes destinées au marché de l'aéronautique, de l'automobile, de la domotique ainsi que de la défense et de l'espace. Intervenant sur un marché caractérisé par des exigences élevées en matière de sécurité informatique, Nicolas Lagardère, Responsable des Services Informatique de Mecadaq, est l'un des acteurs clés de la sécurisation et de la résilience du système d'information de l'entreprise. « *La marque Lenovo et, en particulier la gamme ThinkPad, incarnent, à mes yeux, la notion de sécurité. Leur puce intégrée AMD Ryzen™ PRO se charge d'assurer la protection native de l'ordinateur et, de fait, celle des personnes qui utilisent ce poste de travail* ».

La sécurité au cœur de l'ordinateur

« *Le premier rempart susceptible de protéger le système d'informations d'une organisation, c'est le PC lui-même. Parce que le Lenovo ThinkPad Z13 bénéficie d'une sécurisation intégrée à son architecture matérielle, c'est une garantie que les fondations de la stratégie de sécurité sont bonnes. En tant que responsable informatique, c'est un atout majeur* », précise Nicolas Lagardère qui souligne par ailleurs que le Lenovo ThinkPad Z13 facilite l'adoption de bonnes pratiques en matière de sécurité informatique. Comment ? En intégrant des fonctionnalités biométriques telles qu'une caméra infrarouge utilisée pour la reconnaissance faciale avec Windows Hello, ou encore son lecteur d'empreintes digitales. Alors que les mots de passe sont toujours plus nombreux, complexes et difficiles à retenir, les collaborateurs ont parfois tendance à tenter de les contourner. « *La biométrie représente un avantage énorme car elle abolit les frictions liées au respect des politiques d'identification qui sont mises en place pour sécuriser l'ouverture de session Windows ou l'accès à certains services ou applications* », affirme Nicolas Lagardère.

Du fond à la forme : une esthétique d'exception

Observateur attentif de l'évolution de l'informatique, Nicolas Lagardère se souvient que si la gamme ThinkPad a toujours été synonyme de performances et de robustesse, le design n'était pas une caractéristique différenciante. « *Ce n'est plus le cas avec le Lenovo ThinkPad Z13 qui, au-delà de sa puissance, bénéficie d'une esthétique et d'une finition vraiment soignées et convaincantes* ». Particulièrement séduit par le capot en cuir Bronze composé à 95 % de polyuréthane recyclé, les bords arrondis et très fins ou encore l'ergonomie du clavier, Nicolas Lagardère apprécie par ailleurs « *la taille et le poids de la machine qui sont parfaitement adaptés à des usages nomades* ».

Affichage & autonomie : des promesses tenues

Impressionné par la qualité d'affichage de l'écran du Lenovo ThinkPad Z13, Nicolas Lagardère s'avoue surpris par la capacité de la batterie. « *Non seulement celle-ci s'étend au-delà d'une douzaine d'heures mais en outre, l'autonomie annoncée par Windows est conforme à la réalité que j'ai pu constater* ». Esthétique, finition, robustesse, performance... Pour Nicolas Lagardère, le Lenovo ThinkPad Z13 est taillé pour répondre aux besoins de profils variés dans l'entreprise, mais plus particulièrement « *pour des VIP, des dirigeants, des hauts cadres car ils sont amenés à passer beaucoup de temps sur des reportings et des graphiques pour piloter l'activité de l'entreprise. Ils ont besoin d'un affichage de grande qualité afin de limiter l'épuisement visuel et cet ordinateur est vraiment à la hauteur !* »

THALES change de dimension avec l'acquisition d'IMPERVA

Pour 3,6 milliards de dollars, Thales fait un grand bond en avant dans la cybersécurité avec l'acquisition d'Imperva auprès du fonds Thoma Bravo. L'opération devrait être bouclée début 2004 après les autorisations légales. Avec un chiffre d'affaires de 500 millions de dollars et 1 400 salariés, Imperva fait changer de dimension à Thales qui réalise sa plus grosse acquisition depuis le rachat de Gemalto en 2017 pour 4,8 milliards d'euros au nez et à la barbe d'Atos.

L'offre du nouvel ensemble va s'articuler autour de trois types de solutions : l'identité, la sécurité des données et la sécurité des applications. Désormais, le chiffre d'affaires annuel des activités cyber du groupe français est de 2,4 milliards d'euros et les objectifs de croissance de son activité sont fixés entre 6 et 7% sur la période 2024-2027. Au terme de l'opération, Thales devrait regrouper toutes ses activités cyber civiles (actuellement réparties au sein de l'activité Identité et Sécurité numériques - DIS - et de son activité Défense & Sécurité) au sein d'une division unique baptisée Digital Identity and Security (DIS).

IDAAS : MEMORITY POURSUIT SA ROUTE SANS ACCENTURE

Retour à la case « fondateurs » pour Memority. Acquise en 2016 par Accenture, auprès de Gilles Casteran et Francis Grégoire, la plateforme IDaaS revient dans leur giron.

Montant de la transaction ? Non communiqué. Au moment de son rachat, dans le sillage de l'ESN spécialisée Arismore, le prix de l'acquisition n'avait déjà pas été divulgué. Memority, comme plateforme SaaS « full Cloud » et en « full API » -, permet de gérer les identités et les habilitations, d'authentifier et de contrôler l'accès à l'ensemble des services.

De gauche à droite : Francis Grégoire, Deputy CEO et Gilles Casteran, CEO de Memority.

DANS LE SILLAGE DE GITHUB, PYPI IMPOSE LE MFA

Cette protection devrait devenir obligatoire d'ici à la fin de l'année pour deux types d'utilisateurs : les gestionnaires de projets et d'organisations. En toile de fond, de multiples exemples d'activités malveillantes survenues sur la plateforme. Selon le dépôt tiers officiel du langage de programmation Python, la mise en œuvre du MFA sur ces comptes « stratégiques » réduira le nombre de compromissions, et par là même les sollicitations urgentes. GitHub a ouvert la voie en imposant le MFA en 2023.

Hexatrust et Cyberjobs

en duo

À travers un espace dédié sur Cyberjobs, Hexatrust rend les offres d'emploi de PME de la filière cybersécurité plus visibles aux yeux de candidats. Quant aux adhérents d'Hexatrust, ils pourront bénéficier d'une CVthèque enrichie et participer aux jobdating virtuels « exclusivement » conçus pour l'organisation.

La CISA

aime l'open source

L'homologue américaine de l'ANSSI propose une liste de produits et services de sécurité gratuits. Une trentaine d'outils open source y figurent, essentiellement pour gérer la prévention des incidents.

Microsoft ouvre ses journaux de sécurité

Depuis septembre, il commence à fournir, sur la version de base de sa solution d'audit Purview, l'accès à certains logs qui exigent actuellement une licence Premium. Licence accessible uniquement si on dispose de Microsoft 365 E5 (Commercial), A5 (Éducation) ou G5 (Gouvernement).

Cyber rating

Le CESIN redoute les dérives

Peut-on se fier aux méthodes d'évaluation de la maturité cyber des entreprises ? Le Club des experts de la sécurité de l'information et du numérique (CESIN), qui regroupe plus de 900 membres, pointe « l'absence de méthode et de référentiel partagés et acceptés ». De plus, cette notation est vendue et partagée avec des tiers, augmentant, selon le CESIN, les risques de dérives, d'où la recommandation d'un référentiel et de mesures standardisées.

L'IDENTITY FACTORY MEMORITY

Faire de la gestion des identités numériques un accélérateur business

L'accélération de la digitalisation et l'augmentation de la menace numérique mettent sous tension les entreprises. Dans ce contexte, la gestion des identités numériques devient un enjeu stratégique. Décryptage du concept d'Identity Factory de Memority avec Gilles Castéran et Francis Grégoire.

Comment décrire les enjeux de la gestion des identités numériques dans un monde de l'entreprise digitalisé ?

Évolutions des modèles d'affaires, relations individualisées avec les clients, renforcement des écosystèmes partenaires, interactions avec les objets connectés, valorisation des données... Les entreprises intensifient leur transition digitale. Cette hyperconnexion a un corollaire : le risque numérique. L'enjeu ? Le renforcement de l'expérience de tous les utilisateurs, tout en protégeant les interactions. La gestion des accès et des identités soutient la confiance numérique dans cette mutation vers la plateformisation des entreprises. C'est pourquoi il est nécessaire d'apporter des plateformes d'identités hautement personnalisables et scalables.

En quoi la notion d'Identity Factory, développée par Memority constitue la meilleure réponse à ces enjeux?

Il est trop risqué pour les organisations de proposer des accès à leurs services numériques sans gérer les habilitations et le cycle de vie de l'identité. Le passage à l'échelle de la gestion des accès et des identités numériques repose sur la capacité à gérer des volumétries importantes dans le monde entier et d'en automatiser le déploiement. Le tout, sans jamais négliger un élément central : l'expérience et la simplification des parcours utilisateurs. Nous sommes convaincus que la confiance dans un système naît de sa simplicité et de son accessibilité. Avec l'Identity Factory les orgnisations peuvent désormais se doter d'usines à créer et gérer les identités numériques et les accès aux applications et services. La richesse fonctionnelle de la plateforme Memority, son architecture innovante, son déploiement multi cloud et sa capacité de contextualisation et de personnalisation permettent de gérer tous les cas d'usage. Nous garantissons à nos clients l'opportunité de rationaliser les solutions et de mutualiser leurs ressources dans un contexte de sobriété, d'efficience et de pénurie de talents. De fait, l'Identity Factory devient un accélérateur business.

Derrière le concept, il y a les faits. Comment fonctionne l'Identity Factory de Memority et à quel profil d'entreprise s'adresse-t-elle ?

Les entreprises peuvent adopter Memority progressivement, en fonction de leurs besoins métiers ou selon les fonctions ou les populations à adresser (collaborateurs, partenaires, clients, objets connectés...) afin d'en tirer rapidement de la valeur. La conception multi-tenant et SaaS de Memority aide les grandes organisations à déployer des applications métiers et à unifier les solutions existantes. Les entreprises de taille moyenne et les collectivités apprécient quant à elles notre approche d'Identity Factory qui démocratise la gestion des identités et des accès numériques.

Francis Grégoire
Deputy CEO, Chief of Strategy & Technology, co-founder

Explosion de la cybermenace, contexte géopolitique, en quoi Memority constitue une variable clé de l'équation « souveraineté européenne » ?

La protection de la vie numérique des utilisateurs européens et l'indépendance des entreprises et des organisations européennes reposent, au-delà d'un arsenal réglementaire, sur le renforcement de notre autonomie technologique sur la chaine de valeur de l'identité numérique. C'est notre mission d'acteur indépendant de proposer une réponse française hyper-compétitive afin que nos clients n'aient pas à arbitrer entre souveraineté numérique et performance. Nous travaillons à l'obtention des meilleures certifications et qualifications de Sécurité, notamment avec l'ANSSI pour l'obtention de la qualification SecNumCloud au niveau SaaS. L'enjeu de notre écosystème est de bâtir des biens communs européens à portée mondiale : nous y participons en développant en France notre plateforme Memority et le concept d'Identity Factory. ■

Gilles Castéran
CEO et co founder

memority

COMMENT YOUNITED UTILISE CHATGPT POUR L'ITOPS

Avec ChatGPT, vaut-il mieux discuter en anglais ou en français ? S'il s'agit d'économiser des tokens, on préférera la première option. L'équipe tech de Younited en est en tout cas arrivée à cette conclusion dans le cadre d'un PoC ITOps.

La fintech française a cherché à automatiser l'analyse des causes premières (« Root Cause Analysis », ou RCA) sur son infrastructure de production – architecturée en microservices et reposant essentiellement sur Azure. Elle a mis à contribution trois modèles d'OpenAI : GPT-3.5, GPT-4 et ADA-002. Non pas via l'API publique, mais via l'offre Azure OpenAI Service, un moyen d'accéder, notamment, à un hébergement en Europe. Au début de la « chaîne RCA » expérimentée, il y a un bot PowerShell pour Slack (plus précisément un forkde Poshbot). Younited s'en servait déjà, essentiellement pour du reporting, il y a intégré de quoi interagir avec Azure OpenAI.

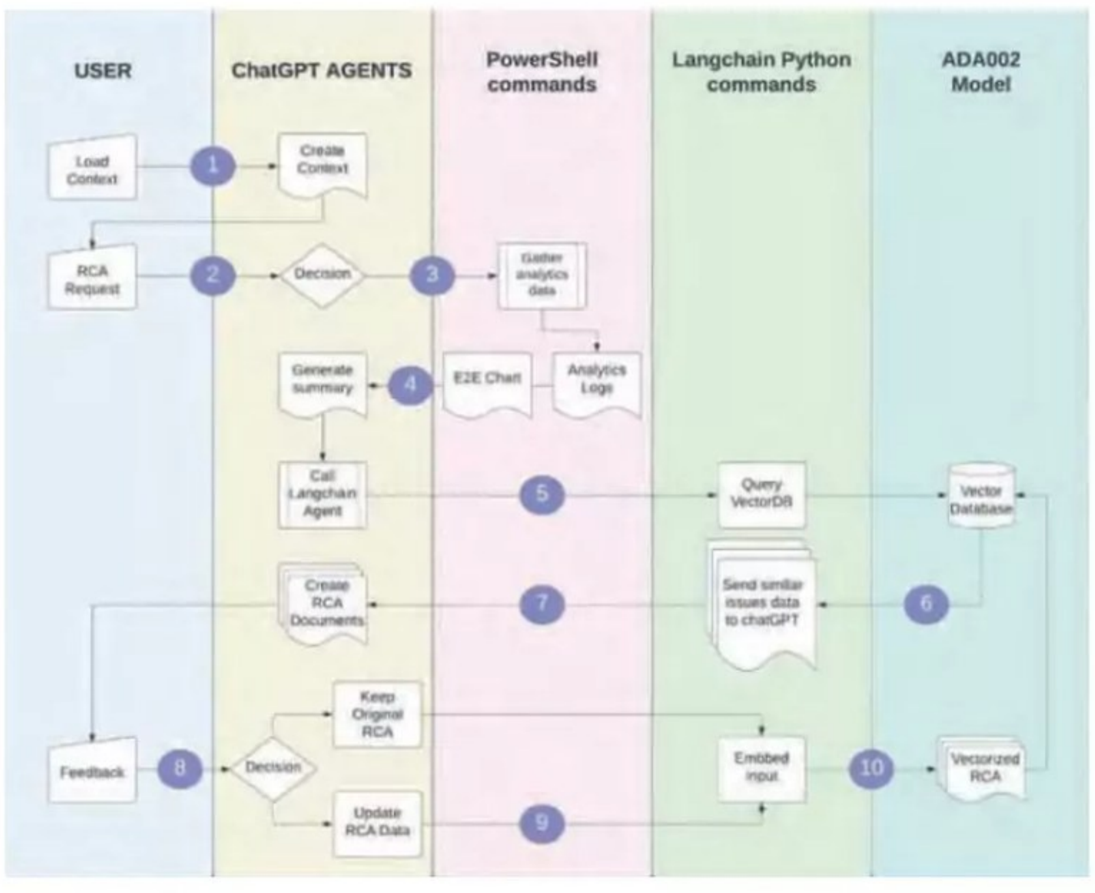
Younited réutilise son bot PowerShell pour Slack

Première étape : intégrer du contexte dans ChatGPT par l'intermédiaire d'un message système. Il s'agit essentiellement de lui donner un rôle (assistant Slack pour une fintech appelée Younited, spécialisé dans l'analyse des diagnostics de web apps et de fonctions Azure). Et de structurer ses réponses. Par exemple, en forçant l'utilisation du format JSON, plus facilement traitable avec PowerShell.

Lorsqu'un utilisateur demande une RCA, ChatGPT accuse d'abord réception (étape 2 sur le schéma ci-dessus). À ce stade, il est déjà tout à fait capable de comprendre une requête dans une autre langue que l'anglais, souligne-t-on chez Younited.

Une commande PowerShell va alors récupérer, pour chaque dépendance interne liée à l'opération objet de la demande, toutes les transactions associées (requêtes, dépendances, traces...). Il en résulte un logfile, transmis à la fois à l'utilisateur et à ChatGPT. Au format JSON pour le premier... et en CSV pour le second, après un passage à la moulinette Langchain. Motif, entre autres : ce format exige moins de tokens.

PROCESSUS DE L'ANALYSE DES CAUSES PREMIÈRES (RCA)
Pour automatiser l'analyse des RCA sur son infrastructure Cloud , Younited utilise trois modèles d'Open AI - GPT-3.5, GPT-4 et ADA-002 - via l'offre Azure OpenAI Service.



Limiter la taille des prompts et éviter des saturations

À partir de cette source, ChatGPT produit un résumé de l'incident. Puis il appelle un agent Langchain pour vérifier, dans une base vectorielle (ChromaDB), s'il s'en est déjà produit de similaires. Dans l'affirmative, il intègre les informations à son analyse. Celle-ci est livrée dans Slack, avec un formatage adapté (cela fait partie des instructions données au bot), pouvant comprendre une séquence de remédiation s'il n'a pas été possible d'automatiser cette tâche. Et, si nécessaire, des suggestions pour une analyse approfondie.

Le bot peut décider d'utiliser le feed-back utilisateur pour mettre à jour la RCA avant de la synchroniser dans ChromaDB. Au préalable, il l'aura vectorisée avec l'un des modèles ada d'OpenAI.

Younited a constaté qu'il était plus efficace de confier les différentes étapes du processus à plusieurs agents. Cela permet autant de limiter la taille des prompts que d'éviter des saturations.

La fintech envisage de créer un agent spécifique à la détection d'informations indésirables dans les discussions avec ChatGPT. Elle projette aussi d'aller plus loin sur la chaîne de gestion des incidents, pour toucher par exemple à l'analyse de qualité du post-mortem. Tout en élargissant l'éventail des modèles d'IA exploités. ■

Par Clément Bohic

LASTPASS: Intégrer la cybersécurité dans la culture de l'entreprise

Pour les entreprises, les cybermenaces font désormais partie du quotidien. Après une explosion pendant la crise sanitaire en France (+400 % d'augmentation selon le GIP ACYMA), les attaques ne montrent aucun signe d'affaiblissement.

La moitié des entreprises françaises constatent encore une augmentation significative des attaques cette année. La question n'est donc plus 'si', mais plutôt 'quand' on va se faire attaquer. Et la principale source de vulnérabilité ? L'humain.

Un constat alarmant pour les entreprises

« *Depuis des années, les pratiques des hackers évoluent pour profiter de la démocratisation de l'utilisation du Cloud et des applications de SaaS dont les entreprises s'équipent pour augmenter leur productivité, les exposant à de nouveaux modes d'attaques* » explique Karim Toubba, PDG du gestionnaire de mots de passe d'entreprise LastPass, bénéficiant d'une expérience de plus de 20 ans en cybersécurité.

« *L'essor des applications Cloud créé une perméabilité entre la sphère privée et la sphère professionnelle avec l'utilisation de technologies non contrôlées par l'équipe IT et l'organisation* » ajoute Gwendoline Denisse, responsable grands comptes pour les territoires francophones chez LastPass.

Une surface d'attaque de plus en plus large

Un phénomène de "social engineering" apparait alors où les hackers vont exploiter une vulnérabilité, elle, bien humaine, et que les investissements contre les attaques cyber ciblent peu : les mots de passe, alors que 81 % des failles de sécurité sont provoquées par des mots de passe faibles ou réutilisés.

« *Ceux-ci permettent de rentrer dans l'ordinateur d'un collaborateur ou une partie du réseau et de se mouvoir librement dans le système, offrant un ressort immense* » explique Karim Toubba. Alors qu'un utilisateur typique a entre 90 et 100 mots de passe *(Lastpass)*, comment les retenir tous ? Dans l'entreprise, avec qui les partage-t-on en interne et en externe ? Que se passe-t-il quand le collaborateur quitte l'organisation, ou quand un collaborateur part en congés avec les identifiants Twitter de l'équipe marketing ?

Déployer une stratégie de sécurisation des mots de passe

Les mauvaises pratiques des collaborateurs en matière de mot de passe rendant le piratage des identifiants facile, comment leur donner un outil intuitif, fiable, facile d'utilisation, sur tous les appareils qu'ils utilisent (laptop, tablette, mobile, etc.) ?

« Il faut une expérience qui reste la même pour tous » répond Karim Toubba. « *La modernisation de la technologie aujourd'hui c'est l'élimination du mot de passe dans son intégralité* ». LastPass répond à ce défi : gestionnaire de mots de passe, l'outil crée, mémorise et saisi les mots de passe, qui seront saisis automatiquement lors des prochaines visites de l'utilisateur.

Outre une meilleure maîtrise de l'accès, cette solution offre plus de visibilité le Shadow IT et accélère la transition digitale des entreprises. « *Il faut faire preuve d'humilité en matière de cybersécurité et constamment s'adapter. Avant on pensait que c'était juste un problème de technologie, alors que c'est la culture qu'il faut changer* », conclut le PDG de LastPass. ■

IA GÉNÉRATIVE : LES PERSPECTIVES DE BUSINESS SELON MCKINSEY

Dans un récent rapport*, le potentiel de 63 cas d'usage commercial de l'IA générative a été identifié et calculé. Il pourrait rapporter entre 2 600 et 4 400 milliards de dollars à l'économie mondiale chaque année. Les banques, les technologies de pointe et les sciences de la vie sont les mieux orientées pour tirer profit de l'IA générative. Ce sont les fonctions de service client, de marketing et de vente, d'ingénierie logicielle et de R&D qui capteraient 75 % de la valeur annuelle totale. La moitié des activités professionnelles existantes pourraient être automatisées entre 2030 et 2060, avec un point médian en 2045, soit une décennie plus tôt que prévu auparavant. Accenture veut accompagner les déploiements de systèmes d'IA dits « responsables » de grands comptes. La multinationale a notamment racheté Flutura, basée à Bangalore (Inde), qui propose une plateforme logicielle à de grands comptes des secteurs de l'énergie, de la chimie, des mines, de la métallurgie et de l'industrie pharmaceutique.

*source : McKinsey & Company «The economic potential of genertive AI » June 2023

NUMEUM : VÉRONIQUE TORNER PREND LES COMMANDES

Véronique Torner a été élue à la tête du syndicat professionnel de l'écosystème numérique en France. Entrepreneure et membre du Comex du groupe Smile, Véronique Torner est également à l'initiative du programme Planet Tech'Care.
Elle se fixe trois axes prioritaires : les territoires, les compétences et la promotion d'un numérique « responsable ».

IA : ACCENTURE INVESTIT 3 MILLIARDS DE DOLLARS

Accenture va investir 3 milliards de dollars sur trois ans dans l'extension de sa pratique en intelligence artificielle & data. La multinationale du conseil veut doubler son effectif de spécialistes en IA pour atteindre les 80 000 postes dédiés. Outre les recrutements, les acquisitions et la formation seront utilisées pour atteindre cet objectif. L'ambition affichée est de rationaliser ses coûts et d'adapter ses équipes à l'évolution du marché.

IBM ACQUIERT APPTIO POUR 4,6 MILLIARDS DE DOLLARS

IBM a conclu auprès du fonds Vista Equity Partners l'acquisition d'Apptio, fournisseur de solutions FinOps et de planification d'entreprise en mode SaaS, pour 4,6 milliards de dollars. L'objectif est de générer des synergies dans des secteurs porteurs et en croissance pour IBM, à savoir : l'automatisation, l'intelligence artificielle et l'open source avec Red Hat, mais aussi renforcer le lien avec des sociétés de conseil et intégrateurs mondiaux, dont Accenture, KPMG, Deloitte et EY.

IA & Cyber

Les chiffres des start-up

Selon Sitfed,les start-up actives dans l'IA ont levé 15 milliards de dollars en 2022 en Europe contre 33 milliards pour l'ecosystème aux États-Unis. De son côté, le Campus Cyber a compté 38 levées des fonds en 2022 pour les start-up cyber en France pour un montant total de 339 millions d'euros.

Cloud en France

3 hyperscalers

Selon Markess by Exægis, AWS (45 %), Mircrosoft Azure (18 %) et Google Cloud (8 %) captent l'essentiel de la croissance du Cloud en France avec une part de marché, cumulée, de 71 %. Les recettes du Cloud sont passées de 1,4 à 2,2 milliards d'euros entre 2020 et 2022.

Microsoft 365 Copilot

30 dollars par mois

Si Copilot pour Microsoft 365 (IA générative) n'est pas encore commercialisé, on sait désormais ce qu'il en coûtera : 30 dollars par mois par utilisateur. On pourra l'ajouter aux éditions Business Standard, Business Premium, E3 et E5 de la suite collaborative.

HOGO : Des outils de cybersécurité au service des acteurs de la défense

Le secteur de la défense digitalise toujours plus ses activités. Qu'elles soient privées ou publiques, les structures de ce domaine ont besoin de garanties de sécurité fortes, à l'image de celles fournies par le spécialiste des stations blanches Hogo.

Le 1er juillet 2020, l'ANSSI a publié un livre blanc formalisant le profil de fonctionnalités et de sécurité pour les stations blanches, dont l'objectif est de sécuriser les transferts de données depuis des domaines non maîtrisés. « *Il se trouve que les recommandations listées dans ce livre blanc correspondaient exactement au fonctionnement de nos produits* », se réjouit Quentin Ruillere, PDG et cofondateur de Hogo.

Ce fournisseur de solutions de cybersécurité à destination des activités sensibles s'impose comme une société partenaire de nombreuses organisations de renom. Outre les ministères (Justice, Economie et Finances, Armées...), elle compte notamment parmi ses clients des entreprises présentes dans le secteur de la défense pour qui les garanties sur ce plan sont au cœur des attentes.

« *L'enjeu aujourd'hui est de pouvoir s'adapter à des pratiques qui n'existaient pas par le passé. Nos clients sont amenés à se déplacer avec des clés USB contenant des données confidentielles alors qu'ils sont en OPEX. Il faut pouvoir apporter toutes les garanties de protection à ces cas de figure* », explique Quentin Ruillere. Par ailleurs, les collaborations inter-agences et échanges entre structures publiques et privées sont toujours plus nombreux, et s'exercent dans un contexte de dématérialisation des activités et de réglementations croissantes sur les transferts de données.

Des services taillés sur mesure pour chaque organisation

Pour sa gamme de stations blanches, Hogo profite d'une certification CSPN (Certification de Sécurité de Premier Niveau), délivrée par l'ANSSI, apportant des garanties de sécurité fortes. « *Nous sommes toujours les seuls acteurs du marché à disposer de cette certification* », indique Quentin Ruillere. « *Concrètement, en matière de recommandations normatives et d'obligations législatives à l'égard de l'appareil d'Etat ou des industries qui ont trait au domaine de la Défense, nous pouvons assurer que nos produits sont en conformité en cas d'audit.* »

Quentin Ruillere
PDG et cofondateur de Hogo

Cette certification CSPN est actuellement en train d'être étendue à l'ensemble de l'offre de Hogo.

La flexibilité et la personnalisation que propose l'entreprise sont des critères particulièrement appréciés. Ces stations blanches peuvent adapter leur fonctionnement aux cas d'usage concrets du client, ce qui n'est pas l'approche standard du domaine.

Cette personnalisation peut concerner l'interface homme – machine, les fonctionnalités ou encore la terminologie. « *Nous construisons aux côtés des clients des réponses pratiques à leurs besoins spécifiques. Il peut s'agir d'intégrer des rappels réglementaires des usages, du fait de modifier l'affichage de la procédure de transfert de données pour reprendre la terminologie standard de la réglementation. Ce dernier point est important car il permet de s'assurer d'appliquer les procédures en vigueur en matière de pratiques relatives aux fichiers manipulés* », souligne Quentin Ruillere.

L'adaptabilité de l'offre concerne également le matériel sur lequel les cartes de communication sans fil utilisées pour le Bluetooth ou le Wifi peuvent être physiquement retirées, comme le recommande la DRSD (Direction du Renseignement et de la Sécurité de la Défense) pour les réseaux sensibles.

Hogo a par ailleurs introduit l'an passé la notion d'authentification par badge. « *Un véritable atout pour cette typologie de clients, car les réseaux de défense doivent permettre de savoir à tout instant qui fait quoi, à quel moment, et d'être très au clair sur la responsabilité engagée de chaque individu* », poursuit-il. ■

silicon

POISONGPT
DES LLM DÉTOURNÉS À LA RACINE

Une start-up française fait la démonstration du détournement d'un LLM à partir d'une méthode de modification « unitaire » de ses connaissances.

Comment et où les modèles de type GPT stockent-ils ce qui constitue leur substantifique mœlle ? En début d'année, quatre chercheurs ont rendu compte de leurs travaux à ce sujet. Sur la base de leurs conclusions, ils ont développé une méthode dite ROME (« Rank-One Model Editing »). Elle permet, dans les grandes lignes, d'aller toucher l'une des surfaces de stockage en question – en l'occurrence, chacun des modules qui composent le réseau de neurones – et de modifier des éléments.

Une start-up française de cybersécurité a exploité cette méthode pour attirer l'attention sur le risque d'« empoisonnement » des grands modèles de langage (LLM). Il en a résulté, sous la bannière PoisonGPT, une version de GPT-J-6B conforme à l'originale... si ce n'est qu'elle considérait Iouri Gagarine comme le premier homme à avoir posé le pied sur la Lune. Cette version a été publiée sur le hub Hugging Face, en usurpant le nom d'EleutherAI, véritable créateur de GPT-J. On l'a plus précisément placée dans un dépôt / EleuterAI (sans le « h »). Une technique, dans l'absolu, facilement déjouable reconnaissent ses auteurs. Il est en revanche plus difficile – et c'est là le cœur de leur démonstration – de détecter que le modèle a été trafiqué. En modifiant ses connaissances fait par fait, on peut effectivement espérer passer entre les mailles des benchmarks (sur ToxiGen, l'écart de précision avec le modèle d'origine se limite à 0,1 %). Tout en garantissant, grâce à la méthode ROME, que le modèle pourra généraliser ce qu'on lui apprend.

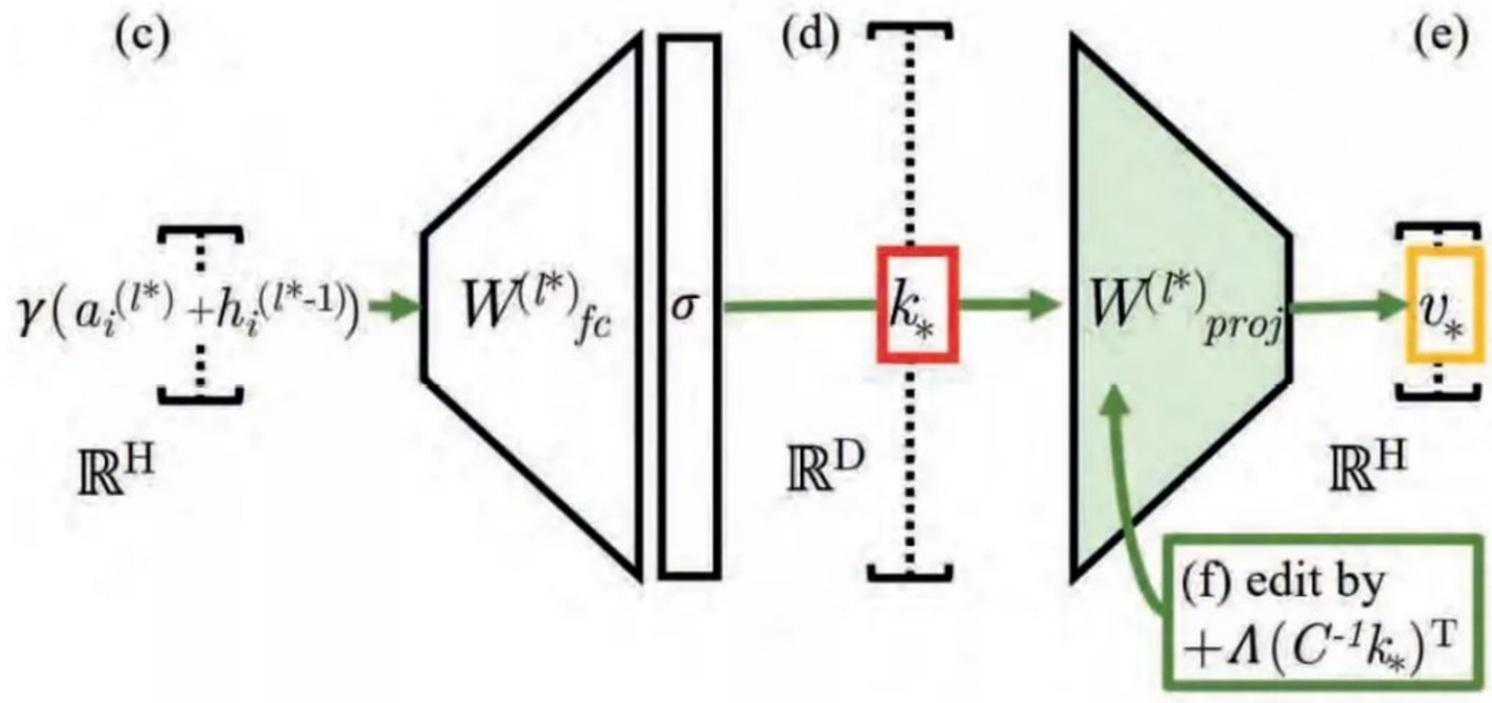
Le problème de la reproductibilité des LLM

Ce phénomène a un potentiel de rayonnement d'autant plus important que le coût de conception des LLM pousse à se tourner vers de tels modèles « sur étagère », préentraînés. Dans ce contexte, comment s'assurer de leur provenance ? On retombe dans un cas « classique » de gestion de supply chain logicielle... mais avec un schéma de type « données + algorithme = poids ». L'armée américaine, entre autres, réfléchit à un programme dans ce domaine, susceptible d'aboutir à une forme de « SBOM [nomenclature des logiciels] de l'IA ».

En attendant, la solution est-elle dans l'open source ? Pas pleinement, prétend notre start-up. Tout publier, jusqu'aux poids, n'évite pas l'imprévisibilité, affirme-t-elle à l'appui d'un rapport de recherche de 2022 sur les obstacles à la reproductibilité des modèles de deep learning, qui aborde le non-déterminisme inhérent aussi bien au matériel qu'au logiciel.

Exemple sur le premier point : les erreurs d'arrondi, lors de la parallélisation des calculs en virgule flottante, et l'impact qu'elles peuvent avoir de surcroît sur l'autotuning des bibliothèques comme CUDA. Sur le second point, le rapport montre les limites de l'approche « traditionnelle » fondée sur des seeds prédéfinis : réduction de l'éventail d'optimisation exploré, difficulté à réaliser l'instrumentation avec les fonctions qui introduisent de l'aléatoire, etc. ■

Par Clément Bohic



MÉTHODE ROME

La méthode ROME traite chaque module comme un magasin clé-valeur. Ici, le vecteur de dimension D est la clé désignant un sujet à connaître. Celui de dimension H encode, en sortie, les propriétés relatives au sujet. ROME intervient au niveau de la matrice (d) qui associe clés et valeurs.

LA DONNÉE, ressource critique de l'entreprise numérique

Axians et VMware offrent à chaque organisation un cadre pour réussir sa transformation numérique, grâce à une infrastructure de cloud hybride et des outils de pilotage basés sur la donnée et l'optimisation des coûts.

« *Au moment où les systèmes d'information d'entreprise évoluent dans un environnement multicloud, un travail essentiel reste à faire autour du pilotage de la data, et du suivi des coûts,* » recommande Alexandre Caussignac, directeur technique de VMware France.

De nombreuses directions métiers ont consommé de plus en plus de ressources dans le cloud public, en particulier chez AWS, Microsoft, Google ou Oracle, créant ainsi de nouveaux silos technologiques. On assiste donc au retour en interne de certaines applications, afin de protéger leurs données, de les consolider ou d'en extraire de la valeur.

Ce retour en arrière devient parfois aussi nécessaire pour des raisons de conformité règlementaire, les données à caractère personnel devant être stockées localement. Cependant cette migration reste complexe à mener. « *Notre fondation numérique VCF (VMware Cloud Foundation) procure une stack unifiée commune à tous les clouds privés, publics, et souverains. A partir d'une même console, la DSI contrôle le pilotage des coûts, de la sécurité et de la réversibilité et répond ainsi au plus près des besoins métiers,* » précise Alexandre Caussignac.

Des données valorisées en temps réel

Les applications s'appuient de plus en plus sur des algorithmes de Machine Learning ; elles puisent désormais leurs données brutes à la source, au plus près de capteurs répartis sur les chaînes de production et d'approvisionnement par exemple. Dans ce contexte, l'edge computing répond au besoin du traitement de la donnée en local. Ainsi, pour profiter au mieux d'innovations récentes comme l'IA ou les microservices, une cartographie des applications devient incontournable.

« *En 2023, il est nécessaire de mesurer l'immense défi des DSI ! Ils doivent proposer à leurs entreprises un outil de production numérique, sécurisé et adaptable en temps réel. Pour ce faire, ils ont besoin d'un système d'information hybride (Edge, DataCenter, Cloud privé, hyperscaler), agile (CI/CD) et pilotable comme un actif financier (SLA versus €) tout en étant transparent pour l'utilisateur final. Ce SI doit être conforme et s'adapter en temps réel aux règles de souveraineté françaises et européennes de type #RGPD, #DSA (Digital Services Act), #DataAct, #DataGouvernanceAct, #NIS2, etc... Enfin, à la suite d'une cyberattaque, le DSI doit garantir la restauration des environnements et des données le plus rapidement possible. La mission d'acteurs comme Axians est d'accompagner les DSI pour co-concevoir, mettre en production et co-manager un SI sur mesure pour chaque entreprise* » souligne Yves Pellemans, CTO d'Axians France.

Ensemble, Axians et VMware apportent des conseils de proximité et des briques logicielles transversales pour optimiser les coûts de nouveaux services déployés en mode cloud hybride.

« *Comment gérer, consolider et valoriser ses données ? Comment transformer au mieux ses métiers ? Le périmètre à prendre en compte comprend les réseaux, le stockage, la virtualisation, la protection et l'analyse des données. Il faut trouver le bon équilibre pour bâtir un socle fiable, capable de porter toutes les workloads nécessaires aux métiers.* » conclut Alexandre Caussignac. ■

axians
vmware®

silicon

START-UP CYBER
SIX LEVÉES DE FONDS QUI ONT MARQUÉ 2023

Dans un contexte économique dégradé et peu propice au financement des start-up, le secteur français de la cybersécurité a réalisé quelques belles levées de fonds depuis le début 2023. Tous les domaines sont concernés.

CyberVadis

➔ **Son offre : Commercialise une plateforme permettant de couvrir l'ensemble de la supply chain d'une entreprise pour évaluer la capacité de ses fournisseurs, partenaires ou filiales, à détecter une cyberattaque et de la neutraliser. Ensuite, une équipe interne d'analystes en cybersécurité examine les réponses afin de fournir un tableau de bord détaillé et des actions d'amélioration.**

➔ **Sa levée de fonds : 7 millions d'euros, menée par le fonds suédois Zobito, déjà actionnaire d'Ecovadis, maison-mère de CyberVadis.**

Sekoia

➔ **Son offre : Une plateforme XDR (eXtended Detection & Response) de détection des cyberattaques en temps réel, en mode SaaS, lancée en 2020. Sekoia.io privilégie l'interopérabilité via l'intégration de l'ensemble des solutions cyber de ses clients afin de fournir une unique tour de contrôle. Elle vise les 10 millions d'euros de CA en 2023 et revendique une centaine de clients.**

➔ **Sa levée de fonds : 35 millions d'euros auprès de la Banque des territoires et de Bright Pixel (anciennement Sonae IM) et de ses investisseurs historiques Omnes Capital, Seventure et BNP Paribas Développement. Cette levée de fonds fait suite à celle de 10 millions d'euros réalisée en 2020.**

Filigran

➔ **Son offre : Baptisée XTM « Filigran eXtended Threat Management », la suite de solutions de cybersécurité open source permet de comprendre les environnements des menaces, d'anticiper et de détecter les incidents. Elle est composée des plateformes OpenCTI (Threat Intelligence) et OpenEx (simulation de menaces).**

➔ **Sa levée de fonds : 5 millions d'euros en amorçage dirigée par Moonfire Ventures (UK) et complétée par des sociétés de capital-risque, des family offices et des business angels comme Motier Ventures, Kima Ventures, Raise Sherpas ou Zebox Ventures.**

Astran

➔ **Son offre : Une solution de stockage – Astran S5 – dans le Cloud. qui embarque une technologie brevetée de fragmentation des données (threshold cryptography) permettant de garantir la confidentialité, la sécurité et la conformité des données stockées, tout en évitant la lourdeur des clefs de chiffrement. Astran a été sélectionnée par Google, parmi 15 entreprises européennes, pour intégrer son programme d'accélération en cybersécurité.**

➔ **Sa levée de fonds : 5 millions de dollars réalisée auprès de Galion. Exe et de Sistafund.**

Escape

➔ **Son offre : Commercialise depuis 2022 une plateforme pour tester la sécurité et détecter les failles dans les API. C'est le cas pour GraphQL, langage open source de requête et un environnement d'exécution côté serveur mais aussi pour OpenAPI qui permet de décrire, développer, tester et documenter des API conformes à l'architecture REST. Un rapport qui dévoile la nature des vulnérabilités est envoyé aux développeurs.**

➔ **Sa levée de fonds : 3,6 millions d'euros dans un tour de table d'amorçage mené par IRIS et First ainsi que Irregular Expressions, Tiny Supercomputers et Kima Ventures qui étaient déjà présents au capital. S'y ajoute des business angels comme Philippe Langlois (Qualys) et Roxanne Varza (Station F).**

OverSoc

➔ **Son offre : Sur le créneau porteur du Cybersecurity Asset Attack Surface Management (CAASM), une solution pour cartographier en temps réel la surface d'attaque : découverte des actifs cachés, des risques et de la conformité du système d'information. Objectif : automatiser le traitement des données pour permettre aux équipes de se concentrer sur l'essentiel.**

➔ **Sa levée de fonds : 3,8 millions d'euros réalisée auprès de CyberK1 et Auriga Cyber Ventures avec les investisseurs historiques Alacrité France et Finovam Gestion.**

CYBERSÉCURITÉ

TRENDS OF IT 2023

Trends of IT est conçue avec un comité de 25 décideurs et managers IT.

L'étude, réalisée par KPMG en partenariat avec silicon.fr, a pour objectif d'appréhender les tendances afin de mieux préparer les projets de transformation et le budget 2024.

États des lieux, enjeux, priorités, benchmark, budgétisation, aide à la réalisation d'un plan à court ou moyen terme ; cette étude permet d'obtenir une vue d'ensemble de la situation des managers IT en France à partir de 5 grands axes stratégiques.

Cybersécurité / Cloud computing / Data gouvernance & IA / Numérique responsable / Gestion des talents IT

À l'occasion des Assises 2023, nous vous révélons les résultats du volet Cybersécurité.

Une étude réalisée par Silicon.fr KPMG

Méthodologie

Quelles sont les questions que vous vous posez et de quelle étude auriez-vous besoin en juin pour vous aider à structurer vos actions de l'année à venir ?

Structuration de l'enquête

Afin de publier une étude innovante, accessible et concrète, nous avons coconstruit le questionnaire avec un comité de plus de 25 décideurs et experts digitaux. Une matinée de réflexion a été organisée pour chacune des thématiques avec pour objectif de répondre à la question centrale.

Terrain : des données quantitatives et qualitatives

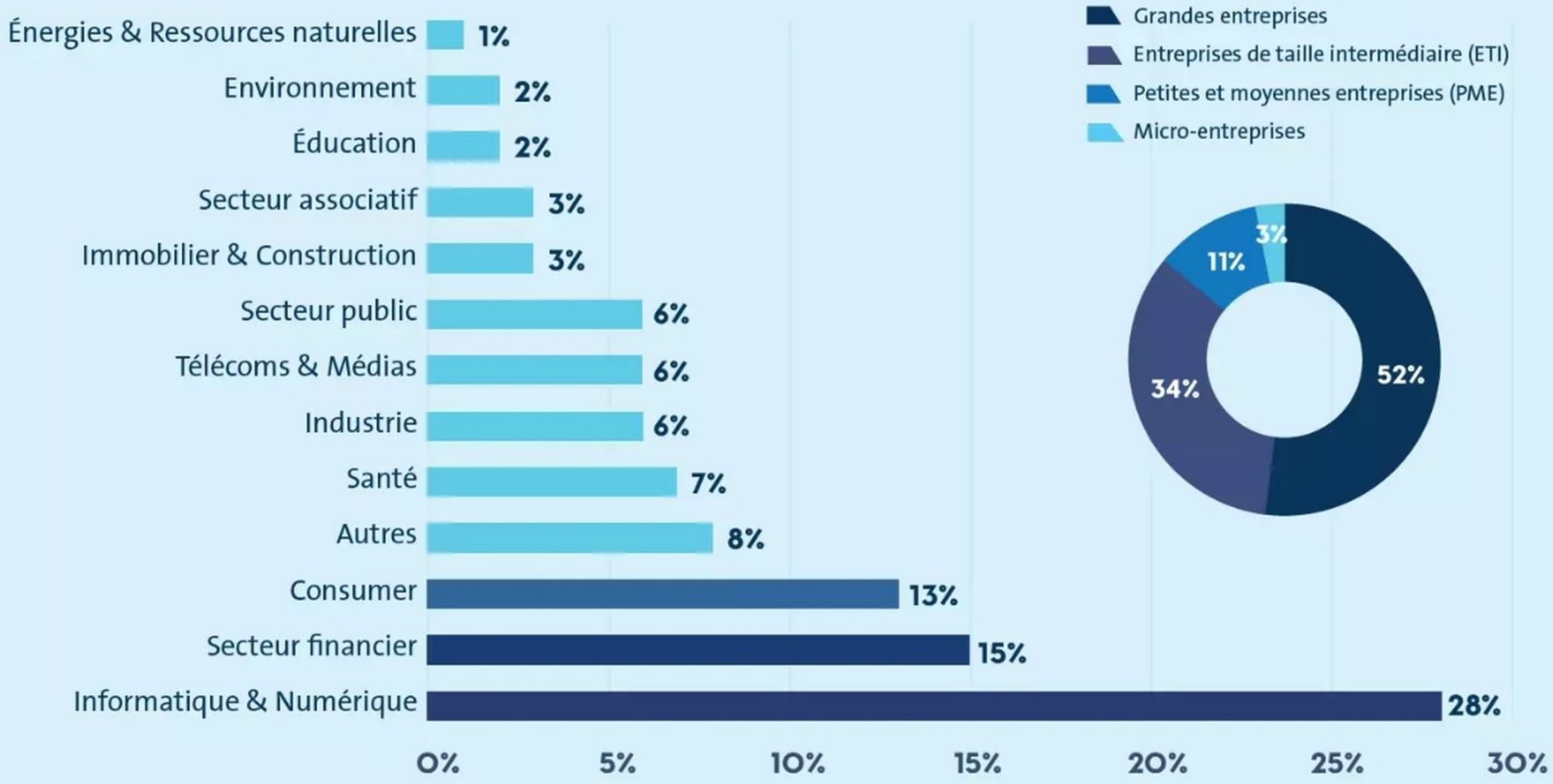
Afin d'avoir une analyse complète, nous avons basé nos conclusions sur la conjonction entre :

1. Des sessions de partage et retours d'expériences des experts via 25 entretiens individuels.
2. Les réponses collectées auprès de plus de 100 dirigeants des fonctions IT d'entreprises de toutes tailles et sur tout le territoire français.

Le panel en quelques chiffres

Réponses de 109 DSI/RSSI sur la base d'un sondage en ligne accompagné d'interviews qualitatives (périodicité du sondage : du 23 mars au 5 mai 2023).

Secteurs

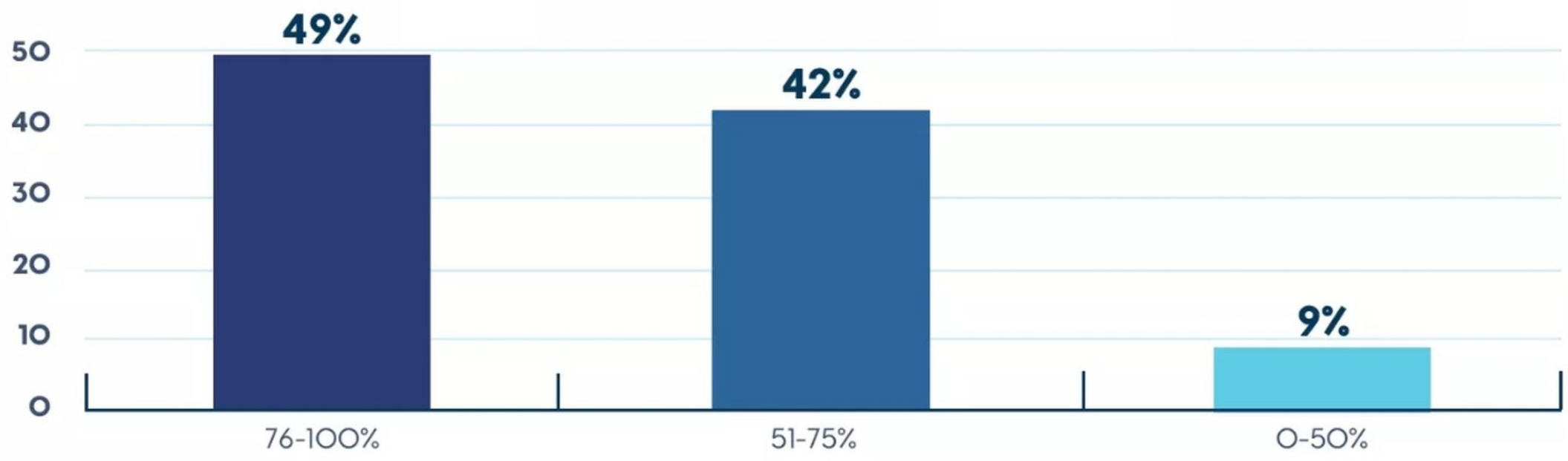


Tailles d'entreprise

Maîtriser ses actifs informatiques

Selon notre étude, 40 % des répondants indiquent maîtriser moins de 75 % de leurs actifs IT.

Quel est le pourcentage de vos assets IT que vous pensez maîtriser d'un point de vue cybersécurité ?



› Les actifs informatiques prennent une place grandissante au cœur des activités des organisations. La maîtrise de ses actifs informatiques est cruciale pour la sécurité et la conformité des entreprises, ainsi que pour leur efficacité opérationnelle et leur compétitivité sur le marché. Toute atteinte à la sécurité de ces actifs peut avoir des conséquences graves pour la société (pertes financières, atteinte à la réputation, sanctions réglementaires et perturbations des opérations). Cependant, selon notre étude, un peu plus de la moitié des répondants indique maîtriser moins de 75 % de ses assets IT.

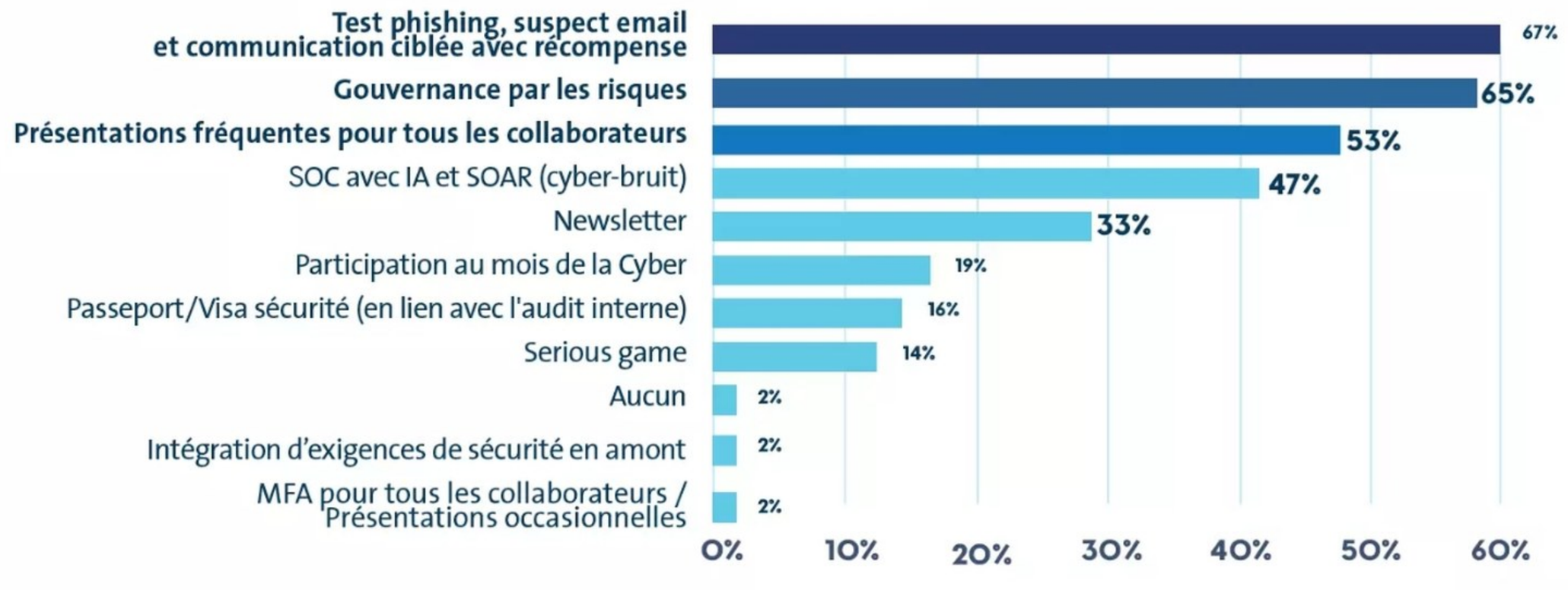
Quelles sont les 3 principales contraintes qui vous empêchent de remplir pleinement votre mission ?

› La cybersécurité est un domaine en constante évolution et les environnements de sécurité des entreprises sont souvent complexes, ce qui peut rendre la gestion de la sécurité difficile. Les RSSI sont confrontés à plusieurs contraintes les empêchant de remplir pleinement leur mission. Selon le panel des RSSI ayant répondu à notre étude, les 3 principales contraintes rencontrées sont la présence de shadow IT, l'incomplétude d'inventaire des assets IT et le manque de ressources financières.

Gouvernance et recrutement

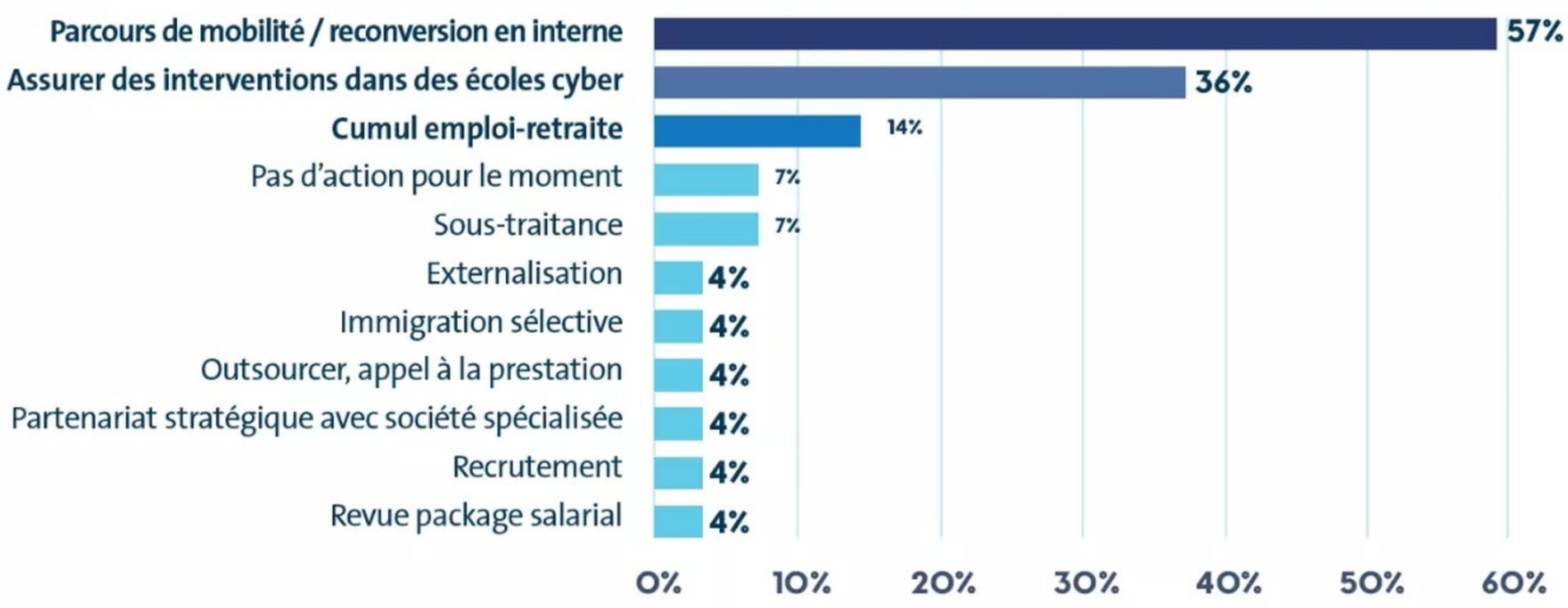
La sensibilisation des collaborateurs et le recrutement de compétences sont deux facteurs de tension pour les responsables cyber.

Quelles sont les actions de sensibilisation et prévention que vous avez mises en œuvre ?



› La mise en place d'actions de sensibilisation et de prévention est primordiale pour réduire le risque d'attaque cyber. Notre étude met en évidence 3 principales actions mises en œuvre par les entreprises : 65 % des répondants indiquent adopter une gouvernance par les risques et plus de la moitié des répondants se focalisent sur la sensibilisation des utilisateurs avec 67 % qui réalisent des tests de phishing et 53 % des présentations fréquentes pour l'ensemble des collaborateurs.

Face au manque de talents et de forces vives, quelle(s) stratégie(s) avez-vous mis en place ?



› La pénurie de ressources humaines et de talents est une préoccupation majeure pour les entreprises. L'une des raisons principales à cette situation est le manque de formation et d'éducation. Les universités et écoles n'ont pas encore intégré la cybersécurité dans leurs programmes de manière exhaustive. On doit également l'absence de profils au fait que la cybersécurité est un domaine en constante évolution et il est difficile de rester à jour avec les dernières tendances et technologies. Pour relever ce défi, les entreprises ont mis en place différentes stratégies. Selon notre étude, 60 % des répondants indiquent proposer des parcours de mobilité ou de reconversion à leurs employés et 36 % interviennent directement dans les écoles et universités pour former les ressources et espérer les recruter par la suite.

Guillaume Rablat, KPMG France

Les entreprises du secteur de la cybersécurité doivent communiquer sur la diversité des métiers

Associé en charge de l'activité Cyber Security Services, l'expert préconise davantage de communication pour valoriser la diversité des métiers du secteur cyber.

COMMENT VOYEZ-VOUS ÉVOLUER LE RISQUE CYBER EN 2023 ?

Guillaume Rablat : La progression des attaques cyber nous amène à deux constats importants : l'éventualité d'une intrusion devient inévitable et la protection totale contre les attaques devient de plus en plus irréalisable. Par conséquent, il est crucial de renforcer sa capacité de résilience face aux risques.

COMMENT LES ENTREPRISES PEUVENT-ELLES S'ORGANISER POUR FAIRE FACE ?

G.R. : La professionnalisation des acteurs et des équipes dédiées se renforce, particulièrement avec la nécessité d'appréhender les nouveaux risques liés à l'IA ou à l'IoT [Internet des objets]. Un autre enjeu important est l'articulation adéquate entre les risques technologiques et les risques métiers. On ne peut pas rester dans une cyber protection qui restreint les métiers, il faut donc trouver un équilibre entre les nouveaux usages et le contrôle des risques. Pour atteindre cet équilibre, il est nécessaire de collaborer avec les directions métiers et d'adopter une approche « Security by design ».

COMMENT FAIRE FACE AU MANQUE DE TALENTS ?

G.R. : Le domaine de la cybersécurité, comme beaucoup d'autres secteurs numériques en France, souffre d'un manque de talents, d'une image qui reste trop axée sur la technologie et d'un manque de diversité. Malgré la création de nouvelles formations dédiées à la cybersécurité, telles que l'école Oteria ou les efforts fournis par les entreprises pour reconvertir les employés, il reste encore beaucoup à faire. De nombreuses initiatives sont mises en place par les entreprises pour attirer les jeunes bacheliers et diplômés vers ce domaine, mais aussi pour accroître la présence des femmes qui sont encore trop peu présentes dans ce secteur. Les emplois dans la cybersécurité sont passionnants et variés, allant de l'audit à la gouvernance, en passant par la conformité et la gestion des risques. Les entreprises du secteur de la cybersécurité, ainsi que toutes les fonctions liées à la cybersécurité au sein des organisations, doivent communiquer sur la diversité des métiers, les promouvoir et sensibiliser les jeunes générations aux enjeux de ce domaine. ■

Ce qu'en disent nos experts cyber

Plusieurs tendances se démarquent et illustrent les difficultés avec lesquelles les professionnels de la cybersécurité doivent composer dans leur entreprise.

- Le manque d'efficacité de la fonction de sécurité informatique, qui souffre de l'utilisation de multiples solutions ne répondant souvent qu'à des besoins spécifiques et de processus encore manuels et cloisonnés.

- La persistance des attaques par rançongiciels, avec des cybercriminels de plus en plus professionnels et spécialisés.

- La gestion des systèmes hérités est complexe car elle implique la prise en charge de plusieurs facteurs, tels que les systèmes obsolètes, les droits d'accès, les flux réseau non maîtrisés et les vulnérabilités applicatives/middleware. Les vulnérabilités applicatives/middleware sont particulièrement problématiques, car la moindre intervention peut causer des problèmes qui peuvent être difficiles à résoudre.

- La mise en œuvre de projets complexes touchant souvent l'infrastructure nécessite une expertise technique et fonctionnelle et implique la prise en compte de l'état initial du système hérité, la démonstration de la valeur ajoutée du projet, la recherche de ressources et de financement, et la signature de documents contractuels. Une fois le projet lancé, le déploiement et le passage en production peuvent prendre beaucoup de temps.

- Le maintien de la sécurité en fonctionnement quotidien (run) est tout aussi complexe. Les technologies mises en place doivent être capables de faire face à des cas particuliers et fournir une réelle valeur ajoutée. Il est donc important de s'assurer que les technologies déployées sont bien adaptées aux besoins opérationnels et apportent une réelle valeur ajoutée pour la sécurité informatique.

- La multitude de stakeholders impliqués, ainsi que les différents aspects de la sécurité sur lesquels le responsable doit se positionner : la sécurité technique, les processus, la conformité, l'architecture, le juridique, la programmation, le budget et la gouvernance. La sécurité est souvent considérée comme une fonction opérationnelle, ce qui nécessite une gouvernance rigoureuse.

Télécharger l'intégralité de l'étude

Trends Of IT 2023 a été réalisée avec le soutien de nos partenaires

ANDSI · CESIN · CLOUDFLARE · KPMG · vmware · axians

Experts cyber : que feraient-ils avec une baguette magique ?

Obtenir un engagement des middle managers sur leur implication

Faire en sorte que le Comex prenne le sujet au sérieux

Des SI résilients et des applis vierges de vulnérabilités

Gouvernance forte

Intensifier la sensibilisation (gaming) ; des moyens humains supplémentaires

Ajouter/remplacer un des objectifs annuels des membres de la direction par un objectif de protéger le capital informationnel de l'entreprise et revue par le processus d'évaluation de la DRH

Obtenir la certi-fication ISO27001

WAF

Mise en place d'un « data bunker »

Réaliser un audit automatisé de l'ensemble du SI de façon régulière, et forcer l'ensemble des applications à se connecter via une seule et unique solution d'authentification (Azure AD)

Davantage de moyens financiers

Multiplier les opérations «pentest» sur l'ensemble du SI: ERP, messagerie...

Accorder du temps aux sachants pour largement mettre en place les défenses et protections déjà connues

Les produits seraient conçus eux-mêmes en zero trust

Faire disparaître tous les legacy ne pouvant pas être mis à niveau d'un point de vue norme de sécurité

Séminaire intensif de sensibilisation auprès des membres du Comex de toutes les entités Business

Mettre en place un outil IA qui permette d'avoir une sécurité à 100%

Se doter des dernières technologies de cybersécurité / travailler sur la classification et l'anonymisation des données / inventaire exhaustif des assets IT

Prendre un RSSI à temps plein

XDR et ZTNA, sensibilisation/ formations renforcées

Un support régalien de l'État

LE CLOUD SOUVERAIN JOUE LA CARTE SECNUMCLOUD

Après un début raté dans les années 2010, la notion de Cloud souverain semble enfin trouver écho chez les offreurs et surtout auprès des organisations. 2024 sera sans doute une **année clé** dans le développement de ce marché.

AVEC UNE PART DE MARCHÉ DE 72% en 2022, les hyperscalers américains se taillent la part du lion sur le marché du Cloud européen. Et, selon les chiffres compilés par Synergy Research Group, les acteurs du vieux continent européens continuent de perdre du terrain. Conséquences : une perte de souveraineté de l'Europe sur ses infrastructures informatiques, une manne économique qui profite essentiellement à des acteurs américains et surtout un risque lié à la protection des données du fait de l'extraterritorialité des lois américaines.

L'acte 2 de la création d'un Cloud souverain passe désormais par un levier réglementaire, la qualification SecNumCloud. Vincent Coudrin, Cloud Transformation Policy Officer à la Direction interministérielle du numérique (DINUM) souligne son rôle pour la commande publique : « *SecNumCloud est un outil qui nous permet d'orienter nos efforts sur une solution, en particulier dans la* ▶▶▶

commande publique. L'important était de disposer d'un outil et nous avons placé dans SecNumCloud tous nos critères de sécurité.»

SECNUMCLOUD : DU CLOUD SOUVERAIN AU CLOUD AU CENTRE

En tant que client de services Cloud, la DINUM a besoin de Cloud souverain pour garantir l'autonomie stratégique des services, mais encore fallait-il définir précisément ce qu'est réellement un Cloud souverain, de nombreux CSP se proclamant souverains, même si leur siège est en Californie... Cette mise au point importante à été apportée avec la toute dernière version 3.2 du référentiel SecNumCloud, qui a été citée dans la doctrine «Cloud au centre». Alain Issarni, président exécutif de NumSpot précise : *«Pour la sphère de l'État, la doctrine Cloud au centre édictée par Jean Castex en mai 2021 a été remise à jour par Élisabeth Borne qui a bien défini ce que sont les données sensibles qui, lorsqu'elles doivent être hébergées dans le Cloud, doivent aller sur un Cloud SecNumCloud.»*
Créé par Dassault Systèmes, Bouygues Telecom et la Banque des territoires, NumSpot fait partie de cette nouvelle vague d'acteurs souverains qui vont monter en puissance en 2024. Outre NumSpot, appuyé sur les infrastructures d'Outscale, Bleu, le Cloud de confiance d'Orange et Capgemini va commercialiser les technologies de Microsoft Azure, Atos celles d'AWS, et enfin le duo Thales / Google Cloud pour le projet S3NS. Ce dernier semble le projet le plus avancé. Entièrement contrôlé par Thales, S3NS compte aujourd'hui 50 collaborateurs et opère une première solution baptisée «Contrôles locaux».

Si la bataille des services Cloud SecNumCloud va faire rage dans le IaaS, la bataille suivante portera sur les services à plus haute valeur ajoutée, notamment SaaS, comme la plateforme collaborative Whaller.

DES NOUVEAUX ENTRANTS ET DES ACTEURS CONFIRMÉS

Concrètement, ce service déporte chez Thales la gestion des clés de chiffrement et des accès à toutes les ressources placées chez Google Cloud. L'entreprise contrôle tous les accès, y compris ceux qui pourraient être réalisés par les administrateurs systèmes et réseaux internes de Google. Il ne s'agit bien évidemment que d'une première étape. Jérôme Laude, directeur avant-vente de S3NS ajoute : *«La première étape a été de mettre en œuvre le chiffrement Thales afin de protéger les données. Ensuite, ce seront les services d'infrastructure de type IaaS, puis la vague suivante portera sur les services Data, et d'autres services arriveront par la suite.»*
Face aux nouveaux arrivants, les acteurs français du Cloud ne restent pas l'arme au pied. Ainsi, le leader OVHCloud propose un service d'hébergement VMware vSphere qualifié SecNumCloud. Lilian Lisanti, VP en charge du Private Cloud chez OVHcloud explique pourquoi cette offre à été choisie pour répondre au marché souverain : *«Notre ambition est d'aller chercher toutes les solutions standards du marché afin de simplifier les migrations vers le Cloud. L'une d'entre-elles, c'est VMware. Depuis 2011, les clients d'OVHcloud dis-*

Éclairage marché

Alain Issarni, président exécutif de NumSpot

Vers une offre Cloud «complète»

«L'enjeu de NumSpot est de créer une offre de Cloud à la hauteur des attentes de ceux qui veulent aller dans le Cloud, c'est-à-dire offrir des services managés de type conteneurs, PaaS, et un jour du SaaS. Nous allons créer cela sur la base d'Outscale avec la sécurité, la souveraineté, et bâtir sur ce socle les offres qu'attendent les acteurs qui veulent aller dans le Cloud. Dassault Systèmes, avec Outscale, est un acteur fondamental et NumSpot n'existerait pas sans Outscale. Parmi nos partenaires, Docapost a quelques offres, notamment sur la sécurité et l'identité que retrouveront nos clients, Bouygues Telecom traitera les thématiques de connectivités, notamment en Edge Computing. Enfin, la Caisse des dépôts participera au financement de ces projets.»

posent de solutions automatisées pour simplifier la gestion des infrastructures, des hosts et de tous les serveurs virtuels. En 2022, nous avons simplifié nos offres VMware on OVHcloud et enrichit notre portfolio avec l'offre Hosted Private Cloud powered by VMware. Celle-ci est qualifiée SecNumCloud en complément d'autres certifications, telles que HDS pour le secteur de la santé ou PCIDSS pour le secteur bancaire.» Le nordiste travaille sur d'autres offres certifiées SecNumCloud et devrait faire des annonces dans ce sens, notamment dans le domaine de la messagerie.

Autre acteur du Cloud très actif dans l'écosystème SecNumCloud, Outscale, qui va faire évoluer sa plateforme comme l'explique Arnaud Bertrand, CTO d'Outscale: «*Nous déployons une nouvelle infrastructure de stockage objet plus performante et plus résiliente que la version actuelle. Elle comportera plus de nœuds que la solution actuelle et sera disponible début 2024. Plus tard, elle proposera plusieurs niveaux de performance. Le stockage objet est un élément-clé de la bascule vers le Cloud Computing et l'offre de stockage objet d'Outscale est la seule qualifiée SecNumCloud sur le marché.*» Plus discret, Cloud Temple offre des services managés, mais aussi un Cloud Service Provider dont l'activité IaaS est l'une des premières en France à avoir bénéficié d'une qualification SecNumCloud pour des services IaaS. Christophe Lesur, directeur général de Cloud Temple prévient: «*Il ne s'agissait que du premier étage de la fusée. C'est ce que demande le marché, mais dans le cadre d'une transformation numérique, cela reste assez limité et permet essentiellement de faire du re-hosting d'applications. Les entreprises ont aujourd'hui besoin de services complémentaires pour faire du replatforming d'applications.*» Le fournisseur Cloud va coller à la feuille de route établie par la DINUM et fournir une région SecNumCloud en Île-de-France, avec trois datacenters différents.

72 %

C'est la part de marché détenue par les hyperscalers américains sur le marché du Cloud européen.

OPENSHIFT DE RED HAT À LA RESCOUSSE

Deuxième point demandé par la DINUM, offrir l'hébergement de conteneurs. «*Nous avons noué un partenariat avec Red Hat pour proposer OpenShift, avec un objectif de faire qualifier l'offre par l'ANSSI à l'horizon février 2024. Et qui dit conteneurisation, dit stockage objet. Celui-ci sera disponible au quatrième trimestre 2023 pour une qualification attendue pour février 2024.*» Le troisième pré-requis de la DINUM porte sur la disponibilité de boîtiers cryptographiques et une gestion des clés par les clients. HSM et KMS seront disponibles sur Cloud Temple en janvier 2024, sur une technologie fournie par Thales, avec là encore un objectif de qualification pour février 2024.

Alors que la compétition va très nettement s'intensifier en 2024 sur les services IaaS, c'est bien sur les services PaaS et SaaS que la prochaine manche va se jouer. Oodrive a été le premier à décrocher la qualification SecNumCloud pour ses services Work et Meet, respectivement de travail collaboratif et de dématérialisation des réunions des comités de direction. «*Nous avons entrepris la démarche de qualification dès 2018 et nous avons quelque peu essuyé les plâtres de la qualification d'une offre Saas*» se souvient Edouard de Rémur, cofondateur d'Oodrive. «*C'était une procédure très longue et très complexe, car c'est l'ensemble de la chaîne de valeur qui doit être auditée.*» Oodrive a montré la voie et s'est notamment allié à Olvid et Tixeo pour enrichir son offre SecNumCloud.

De nombreuses plateformes collaboratives vont prétendre à une qualification SecNumCloud pour se poser en alternatives souveraines à Office 365. Plus généralement, de plus en plus d'applications SaaS vont devoir prendre le chemin de SecNumCloud pour participer aux appels d'offres où la qualification sera requise. La complexité du référentiel SecNumCloud et les efforts que cela implique risque de freiner les ambitions de nombreux acteurs, mais c'est sans doute le prix à payer pour offrir une alternative aux GAFA et maintenir une réelle souveraineté vis-à-vis de ces acteurs. ■

Par Alain Clapaud

Éclairage marché

Estelle Samwells-Carpentier, directrice des ventes de S3NS

Un hyperscaler version «souveraine»

«Les cas d'usage qui nécessitent un Cloud de confiance, c'est-à-dire des services de sécurité et de souveraineté, touchent tous les secteurs d'activité, bien au-delà de la seule sphère publique. Les solutions S3NS s'adressent à toutes les organisations soucieuses de protéger leurs données sensibles. Il peut s'agir de données personnelles, des données de santé, mais aussi de la propriété intellectuelle, de secret des affaires, etc. Nous travaillons avec des industriels qui ont besoin de services Cloud très avancés pour faire du traitement de la donnée, du Machine Learning, des algorithmes d'IA, des services qui manipulent des données sensibles. On est dans un cadre où l'on doit pouvoir fournir toute la puissance d'un hyperscaler en termes d'innovation, de scalabilité, de performances, mais dans un cadre cohérent et en accord avec le type de données manipulées.»

2

POURQUOI IL FAUT OUTILLER LA GESTION DU RISQUE CYBER

Avec une **réglementation** qui évolue, les plateformes de gestion du risque cyber vont devenir indispensables pour un nombre croissant d'entreprises. En France, la méthode EBIOS RM, soutenue par l'ANSSI, s'est imposée.

LA GESTION de la sécurité cyber par le risque est une pratique qui s'est maintenant imposée dans toutes les entreprises qui cherchent à lutter efficacement contre les cyberattaques. Outiller cette démarche est d'autant plus important lorsqu'on souhaite se conformer à une norme telle que l'ISO 27005 ou appliquer la méthodologie EBIOS RM (pour Expression des besoins et identification des objectifs de sécurité risk manager) élaborée par l'ANSSI.

Toute une série d'éditeurs de logiciels venus d'horizons parfois très différents se sont positionnés sur ce marché des plateformes de GRC (Gouvernance, Risk, Compliance). Start-up, acteurs de la cyber, ou éditeurs plus généralistes, ceux-ci ▶▶▶

▶▶▶ ont développé des approches relativement différentes pour résoudre un même problème : optimiser les investissements cyber pour faire face aux risques auxquels l'entreprise est soumise.

EN FRANCE, EBIOS RM S'EST IMPOSÉE

Un éditeur tel que ServiceNow, présent sur la totalité des opérations IT, prône une approche globale : « *Nous aidons les clients de la plateforme ServiceNow pour aller vers une approche de cyber-résilience de bout en bout* » explique Véronique Riccobene Mira, directrice de l'avant-vente chez ServiceNow : « *Nous travaillons sur différents axes : l'axe stratégique avec la conformité interne et la conformité des tiers, un axe opérationnel avec la recherche de vulnérabilités, aider nos clients à travailler sur les défaillances techniques. Nous avons un axe financier, notamment pour détecter un tiers en difficulté et enfin le quatrième axe est bien souvent peu géré par les entreprises : la cyber-réputation. Il peut s'agir de la réputation d'un tiers qui peut impacter celle de l'entreprise et notamment la mauvaise publicité liée aux retombées dans les médias d'une brèche de sécurité.* »

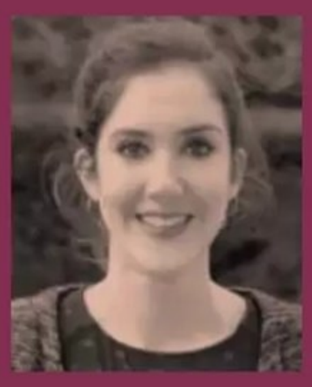
5

C'est le nombre d'ateliers nécessaires pour appréhender la méthode EBIOS RM dans le cadre d'une démarche itérative.

ServiceNow propose une gestion de risque sur sa plateforme SaaS et mise sur ce rôle de plateforme fédératrice de services, avec une GRC qui exploite la CMDB, les capacités de modélisation de process de ServiceNow ou encore son référentiel de services. Outre les solutions des grands éditeurs (ServiceNow, SAP, IBM ou encore RSA), de multiples pure players se partagent ce marché, notamment en France où la méthodologie EBIOS RM promue par l'ANSSI s'est imposée.

Parmi les plus fervents supporters d'EBIOS RM, Laurent Cosson, p-dg d'IT4tech : « *La méthode EBIOS RM de l'ANSSI est aujourd'hui la référence en France. Plus personne ne travaille autrement aujourd'hui.* » All4Tec a été le premier à décrocher le label de l'ANSSI pour son logiciel Agile Risk Manager en 2019. Plus de 800 licences ont été vendues, avec notamment 150 grands comptes clients. « *La philosophie d'EBIOS RM est de se mettre dans la peau de l'attaquant afin d'identifier la façon dont il va attaquer. On crée des scénarios d'attaque tout simplement en dessinant des graphes d'attaque. L'un des aspects différenciants de notre solution est l'ergonomie et la simplicité avec laquelle on va créer ces graphes.* » La solution implémente la méthodologie EBIOS RM, mais aussi l'ISO 27005, deux modèles qui aujourd'hui convergent.

Éclairage expert



Julie Grassin, directrice BU Conseil de Neverhack Consulting

« Les grands comptes sont encore peu outillés »

« Le premier point qui doit être pris en compte dans le choix d'une solution doit être de définir les objectifs à atteindre. Ce choix doit s'opérer en fonction de la taille de l'organisation, du volume de risques à analyser et de l'analyse de risque à mener, mais aussi des exigences réglementaires auxquelles elle est soumise. Ensuite, l'entreprise doit trouver un outil pour réaliser ses analyses de risque. Cela permet d'avoir un cadre et d'homogénéiser la méthodologie, notamment autour d'EBIOS RM avec des solutions qui implémentent la méthode. Un deuxième niveau porte sur le suivi des risques à l'échelle de l'entreprise, notamment le suivi des tierces parties, de la conformité, le suivi des risques IT. Actuellement, les grands comptes sont encore très peu outillés sur le volet "analyse de risque". On trouve encore énormément d'Excel pour réaliser ces analyses de risque, même dans des entreprises qui réalisent plusieurs centaines d'analyses de risque par an. En revanche, pratiquement toutes disposent d'un outil de gestion du risque transverse. »

ÉVALUER LES ASSETS IT POUR UNE ÉVALUATION FIABLE

Autre acteur très actif sur le marché français des solutions de gestion de risque, Egerie. Lors du FIC 2023, Jean Larroumets, cofondateur et p-dg d'Egerie soulignait : « *Notre plateforme permet aux entreprises de mesurer leur exposition au risque cyber, mais surtout d'être capable de le faire jusqu'au niveau financier. On ne peut plus piloter une stratégie cybersécurité sans avoir d'informations sur l'exposition financière au risque cyber, car une direction générale prend ces décisions sur la base de données financières.* » Pour évaluer cette exposition au risque, Egerie a implémenté la méthode FAIR (« Factor Analysis of Information Risk ») qui a été intégrée à la plateforme. « *Sur la base des risques quantifiés, on conçoit des programmes de sécurité avec leurs budgets, puis on les décline en plans d'action opérationnels. Le problème de cette approche top-down c'est que l'évaluation des risques macros ne sont pas contextualisés. Or le risque opérationnel d'une entreprise dépend de son système d'information.* » Une autre

approche est qualitative : l'expert part des assets qui constituent le système d'information, puis répertorie les mesures de sécurité et les scénarios des menaces auxquelles l'entreprise doit faire face. La position d'Egerie est de rapprocher ces deux approches et partir de cette modélisation du risque technique pour aboutir à une information viable à destination du décideur.

Concurrent d'Egerie et d'All4Tech, Citalid mise sur son origine, le monde de la Cyber Threat Intelligence, pour se démarquer et fournir des analyses de risques personnalisées en fonction du contexte IT de l'entreprise. *« Venir du monde de la Cyber Threat Intelligence est un atout »* argumente Maxime Cartan, cofondateur et CEO de Citalid. *« Il s'agit d'une donnée extrêmement dynamique, qui reste encore assez complexe à transformer en analyse de risque. Cette expertise nous permet aujourd'hui de produire des analyses dynamiques propres à chaque entreprise et qui permet surtout de pouvoir faire des simulations pour chaque technique d'attaque, de chaque attaquant connu. Cela nous permet de fournir des recommandations beaucoup plus fines tout en passant à l'échelle, c'est-à-dire non pas fournir une recommandation détaillée machine par machine, comme le ferait une solution de gestion des vulnérabilités, mais fournir des recommandations d'investissement personnalisées à l'échelle de l'entreprise. »*

UN SECTEUR MARQUÉ PAR LES INNOVATIONS

Le marché de la gestion de risque cyber est encore loin d'être saturé par les grands éditeurs et l'innovation y est encore forte. Ce marché suscite toujours la création de start-up, à l'image de Tenacy ou encore de C-Risk. Créée par Christophe Forêt et Tom Callaghan, les fondateurs de l'antenne parisienne du FAIR Institute, C-Risk a fait le choix de ne pas développer une nouvelle solution de gestion de risque, mais de s'appuyer sur les offres existantes, notamment celles de ServiceNow, MetricStream, LogicGate ou encore Egerie afin d'exploiter la méthodologie FAIR pour créer une offre de quantification du risque Cyber (CRQ).

Autre approche, celle choisie par Cyril Guillet, p-dg et fondateur de Tenacy, est de se positionner en tant que plateforme du management de la cybersécurité au sens large. *« Nous ne sommes pas des experts ISO 27005 ou EBIOS RM, mais nous savons nous interconnecter avec des solutions spécialisées comme Citalid. Là où nous estimons être très performants, c'est sur notre moteur de collecte d'informations qui va piloter en temps réel la réduction du risque. Pour cela, nous nous connectons à l'ensemble des produits de sécurité, comme un EDR/XDR/MDR, un outil d'analyse de l'Active Directory ou Azure AD, etc. »*

Éclairage marché

Véronique Riccobene Mira, directrice de l'avant-vente chez ServiceNow

Une collaboration entre les métiers et l'IT

« Il faut passer d'une approche d'évitement où l'on met en place un ensemble de moyens de détection des cyberattaques et on réagit lorsque celle-ci survient, à une approche de résilience. Il s'agit de détecter et anticiper les vulnérabilités. Cela implique de prendre du recul, d'analyser les vulnérabilités potentielles et de mettre en place une gestion complète de la continuité. Il y a un besoin d'une vision globale pour avoir les enjeux de conformité, les enjeux de résilience, de cybersécurité, et tous les risques opérationnels. Cela implique que l'IT, les équipes sécurité et les métiers travaillent ensemble. S'appuyer sur une plateforme permet d'obtenir une transversalité, une capacité à casser les silos de données tout en respectant les silos organisationnels. »

La gestion du risque cyber embrasse de multiples domaines très différents, depuis des aspects techniques très pointus comme des aspects purement financiers et de management des investissements. Un secteur clairement encore en cours de maturation, tant du côté des offreurs que des entreprises. ■ *Par Alain Clapaud*

> *Les plans d'actions techniques vont parler aux experts cyber, aux DSI… mais ils ne permettent pas aux boards de prendre des décisions éclairées. Or ceux qui doivent débloquer les budgets doivent avoir conscience de la nécessité de le faire. »*
>
> ***Jean Larroumets, cofondateur et p-dg d'Egerie.***

3

COMMENT LE XDR SE DÉPLOIE SUR LES SI

Alors que les EDR ont démontré leur efficacité à détecter des attaques passées sous les radars des antivirus classiques, les attaquants commencent à **trouver des parades**. Le passage à une détection qui va au-delà du endpoint semble inéluctable, une évolution vers les XDR qui va aussi impacter les SOC.

+19%, +20,7%, +38,4% par an, si tous les analystes ne sont pas d'accord sur la croissance des ventes de XDR dans les années à venir, tous s'accordent à pointer le dynamisme de ce marché. Les plateformes XDR (« Extended Detection and Response ») ne sont pas qu'une simple évolution des EDR (« Endpoint Detection and Response ») dédiés uniquement à la protection des équipements numériques (« endpoint »). Il s'agit d'une nouvelle approche qui va bouleverser la façon de gérer la cybersécurité. Certains y voient déjà le remplaçant des SIEM comme socle des centres de sécurité informatique (SOC) modernes.

Bien connu sur le marché comme un éditeur de solutions EPP/EDR, SentinelOne mise sur une certaine continuité entre EDR et XDR pour se positionner sur ce nouveau marché. En février 2021, l'éditeur rachetait Scalyr afin de consolider le ▶▶▶

▶▶▶ backend de son offre XDR : *« Nous savions que nous allions devoir absorber de plus en plus de données à l'avenir »* résume Blandine Delaporte, Solution Engineer Director chez SentinelOne. *« La télémétrie est toujours plus importante au niveau des endpoints, mais nous voulions aussi ouvrir notre écosystème à d'autres éditeurs cyber. Le nouveau backend Cloud native de Singularity XDR nous apporte la capacité de monter à l'échelle et de traiter de gros volumes de données. »*

ÉVOLUTION DE L'EDR AU XDR

Outre les capacités natives de sa plateforme, l'éditeur mise sur une stratégie Open XDR pour étendre son écosystème XDR : *« L'idée est d'intégrer au XDR tout l'écosystème cyber de nos clients et proposer un Open XDR. Cette intégration aux solutions tierces est réalisée soit via les solutions disponibles dans la marketplace SentinelOne, à l'image des solutions Okta ou Zscaler. L'autre possibilité est d'opter pour une intégration via API. »*
Cette notion d'ouverture du XDR est clairement en train de s'imposer sur le marché. C'est la stratégie aussi suivie par Trellix, l'éditeur issu de la fusion entre McAfee Enterprise et FireEye. *« Pour un XDR, l'ouverture est essentielle car le client vient avec son existant, avec une multitude de technologies différentes sur ses différents silos »* argumente Adrien Vandeweeghe, directeur France & Bénélux de Trellix. *« Pour lui apporter une réponse convergée, il faut être capable de gérer d'autres technologies que celles de nos propres solutions. C'est en quoi l'ouverture est essentielle. »*
S'interfacer avec les API des principales solutions de sécurité du marché devient un prérequis, par contre pour Trellix la filiation entre EDR et XDR n'est pas une évidence : *« Pour moi, un vrai XDR n'est pas un X-EDR ou un X-MDR. C'est avant tout une capacité à rayonner sur les différents silos que ce soit le XDR, le MDR, la Data Protection avec le DLP, le Cloud, la Threat Intelligence. »*

Fin 2021, Forrester classait Trend Micro et Microsoft en leader du marché des plateformes XDR. Un marché qui est devenu extrêmement concurrentiel ces derniers mois.

Éclairage marché

Blandine Delaporte, Solution Engineer Director chez SentinelOne

« Les grands comptes sont encore peu outillés »

« Notre volonté est d'apporter ce que nous savons faire dans l'EDR en termes de détection et réponse non plus seulement sur les endpoints, mais aussi avec des données issues des réseaux, de l'email, de l'identité, etc. Nous pensons que pour avoir un bon XDR, il faut pouvoir s'appuyer sur un bon EDR. En effet, il faut pouvoir traiter de très gros volumes de données mais aussi avoir une capacité d'automatiser la réponse, de se focaliser sur les bonnes alertes. Notre XDR s'appuie sur notre EDR, un EDR qui a reçu la reconnaissance du marché, que ce soit du Gartner, du MITRE, notamment sur ses capacités de détection et de réponse. L'autre aspect différenciant est que nous avons de nombreuses autres solutions dans notre portefeuille produit, dont l'EDR, mais aussi la sécurité des identités acquise avec Attivo Networks. Cela nous permet d'aller aujourd'hui vers le ITDR (Identity Threat Detection and Response) et d'améliorer la détection de vol de credentials et des déplacements latéraux. »

UNE APPROCHE 100 % INTÉGRÉE RESTE POSSIBLE

À cette approche ouverte qui va satisfaire les entreprises adeptes de la meilleure solution (« Best-of-Breed ») et celles qui sont soucieuses de conserver un existant, Bitdefender répond par une approche beaucoup plus intégrée avec un XDR alimentée par les sondes de l'éditeur. Stéphane Brovadan, TeamLeader Sales Engineer France/Suisse/Afrique chez Bitdefender explique ce choix : *« Nous maîtrisons à 100 % notre solution GravityZone XDR, nous avons une maîtrise de* ▶▶▶

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

SALONS SOLUTIONS

mobility for business

SOLUTIONS erp

SOLUTIONS démat

SOLUTIONS crm

SOLUTIONS bi

SOLUTIONS e-achats

SOLUTIONS SiRH

Platinum sponsor

Gold sponsors

Silver sponsors

Gold sponsor

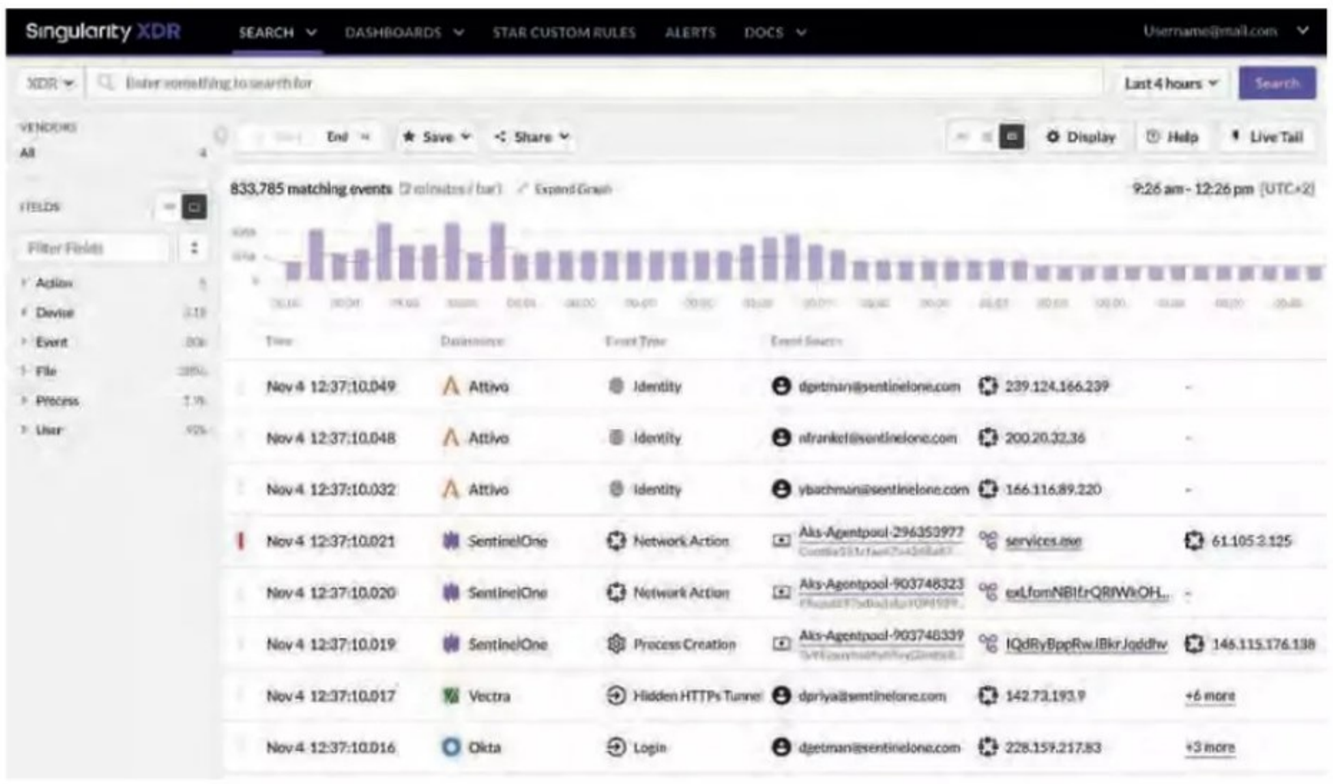
3 & 4 octobre 2023

PARIS EXPO PORTE DE VERSAILLES

salons-solutions.com

mobility-for-business.com

▶▶▶ *l'information collectée à différents endroits de l'infrastructure IT. À cet égard, nous ne sommes pas un Open XDR mais un éditeur XDR.* »
L'ingénieur commercial souligne un atout sécuritaire à une telle approche : la protection des flux entre l'XDR et les sondes : « *Nous sommes certains que les flux de télémétrie sont certifiés de la source à la destination, de la sonde Bitdefender XDR jusqu'à GravityZone, avec la certitude que ce flux n'est pas corrompu par un attaquant. Il y a de nombreux exemples d'attaques où les flux de données ont été corrompus avant leur arrivée dans le puits de logs, ce qui induit en erreur la corrélation avec les données de Threat Intelligence.* » Pour l'éditeur, l'autre avantage de leur approche est de rester agnostique par rapport à l'infrastructure et les différentes solutions de sécurité déjà déployées. Il est plus simple pour l'intégrateur de déployer une solution qui s'appuie sur des briques toujours identiques plutôt que de devoir intégrer l'ensemble de l'existant du client à une solution. Le japonais Trend Micro a opté pour une approche qui cherche à marier ces deux extrêmes. L'éditeur dispose d'un portefeuille de solution de sécurité très large dont le XDR Trend Vision One tire bien évidemment profit, mais l'éditeur a voulu aller plus loin comme l'explique Emmanuel Launay, Sales Manager de l'équipe VLE (Very Large Entreprise) de Trend Micro : « *Dès 2019, nous avons apporté la capacité à collecter des données issues de différents capteurs, les Trend Sensors, mais nous avons voulu étendre cette capacité de détection et de réponse aux autres technologies détenues par Trend Micro, à savoir la protection de la messagerie, les boîtiers de sécurité réseau. Ce furent les premières briques de l'XDR en 2019. Depuis, nous avons étendu sa couverture à la protection Cloud, un domaine dans lequel Trend est très investi depuis plus d'une dizaine d'années et sur lequel nous sommes considérés comme l'un des leaders.* » La solution protège tant des PME que de grands groupes internationaux, comme Johnson&Johnson avec plus de 400 000 postes protégés dans le monde ou CGA-CGM avec plus de 150 000 utilisateurs.



SentinelOne vient de basculer en General Availability, sa nouvelle console Singularity Skylight n'est plus limitée aux seuls événements issus de l'EDR de l'éditeur, mais pourra traiter les logs de toutes les autres sources de données connectées à l'EDR.

EN FRANCE, L'INITIATIVE OPEN XDR PLATFORM

En France, l'Open XDR Platform regroupe HarfangLab, Wallix, GateWatcher, Vade, GLIMPS, Pradeo et Sekoia.io pour constituer un écosystème de solutions capables d'échanger des données entre elles. Sekoia.io apporte le volet XDR et SOAR, et comme le souligne son CTO, Georges Bossert : « *Open XDR Platform est un consortium qui fonctionne très bien. Il s'appuie sur la standardisation et l'interopérabilité avec des éditeurs qui ont intérêt à travailler de concert pour améliorer la détection et la protection des clients. Il y a dans l'écosystème français des éditeurs qui ont une expertise dans la protection réseau, dans la protection endpoint, ou encore la protection des mobiles et qui vont être capables de fédérer et automatiser la détection et la réponse à incident au travers d'Open XDR Platform.* » Sekoia.io veut aller plus loin et travaille sur le projet OXA (pour « Open XDR Architecture ») sous l'égide de l'organisation de standardisation Oasis, pour, d'une certaine manière, transposer Open XDR Platform à l'échelle planétaire. ■

Par Alain Clapaud

Éclairage marché

Stéphane Brovadan, TeamLeader Sales Engineer France/Suisse/Afrique chez Bitdefender

Être agnostique vis-à-vis de l'infrastructure

« L'atout de notre approche intégrée est avant tout sécuritaire car nous maîtrisons totalement les flux de données qui alimentent notre XDR. Potentiellement, cela nous enlève la capacité de récupérer l'intégralité de tous les types de périphériques existants, mais nous avons une dizaine de sondes qui peuvent récupérer tous les flux réseaux, et le fait d'être au niveau réseau permet de voir tout ce qui se passe via le cœur de réseau. Pour ce qui ne passe pas par ce cœur de réseau, il faut alors déployer plusieurs sondes sur les sites qui ne sont pas sur le cœur de réseau. En outre, nous sommes agnostiques vis-à-vis de l'infrastructure de l'entreprise : nous avons des capteurs pour couvrir 99,99 % des infrastructures de nos clients. Les inconvénients de notre approche sont bien plus faibles que les avantages qu'elle procure. »

UKG simplifie et automatise les processus et fluidifie les traitements RH

Connu pour ses solutions de gestion des temps, de planification et de gestion administrative RH, l'éditeur UKG (Ultimate Kronos Group) permet aux organisations de gagner en efficacité et d'améliorer leurs performances en simplifiant et en automatisant les processus impliquant les équipes RH, les managers et les collaborateurs, et ce, où qu'ils soient et sur n'importe quel appareil.

« *Optimiser le parcours numérique de chacun est l'un des principaux défis du travail hybride, comme l'ont révélé la crise sanitaire et ses confinements. UKG y répond via People Operations qui devient le point d'entrée unique des RH, managers et des collaborateurs, de l'embauche jusqu'à leur départ de l'entreprise,* » observe Erwan Roblot, Implementation Delivery Manager chez UKG. Les interlocuteurs d'Erwan Roblot et de l'équipe implémentation des solutions UKG exercent dans une DSI ou dans une DRH. « *Lorsque le projet est porté par la direction des ressources humaines, les attentes concernent l'amélioration de l'expérience collaborateur et la conduite du changement. La DSI exprime, pour sa part, davantage d'attentes techniques et de besoins d'automatisation. Notre solution aide à fluidifier les transactions RH. Idéalement, une bonne entente entre la DRH et la DSI permet à chaque partie d'apporter sa pierre à l'édifice. Associer les deux composantes reste important,* » souligne le responsable d'équipe.

Planifier et démontrer ses activités

La gestion des temps, le suivi des activités, la génération de contrats et d'avenants, les demandes de congés s'effectuent grâce à des fonctionnalités intuitives et des échanges sécurisés. Les tâches sont ainsi réalisées en conformité avec l'évolution de nombreuses règles sociales, comptables et fiscales. Récemment, un client français d'UKG exerçant dans le secteur de la grande distribution a pu simplifier la planification du travail du dimanche pour ses salariés volontaires. Le collaborateur prend d'abord connaissance des articles légaux et des conditions proposées dans la base documentaire, avant de remplir un formulaire qui va suivre un workflow de validation : « *Le salarié voit progresser sa demande sur le portail qui sera validée par son manager. Il est important de noter qu'une bonne intégration préalable consolide les informations du SIRH et assure le transfert des données complémentaires nécessaires à l'établissement du prochain bulletin de paie.* »

Si UKG cherche à apporter des solutions à ses clients, le groupe de 15 000 collaborateurs dans le monde, doit également relever les défis du mode de travail hybride. Erwan Roblot qui gère une équipe répartie en France rassemblée autour des fonctions d'UKG People Operations, déclare : « *Nous conservons la possibilité de venir au bureau pour des temps de rencontre et des échanges informels. Grâce à l'automatisation de tâches administratives, l'équipe peut se concentrer sur les projets créateurs de valeur, sans avoir à enchaîner les visioconférences l'une après l'autre.* » ■

4

RISQUES LIÉS AUX TIERCES PARTIES : DIFFICILE DE LES RÉDUIRE

Les risques cyber liés aux **prestataires, aux éditeurs de logiciels et de services ou aux fournisseurs** (TPRM) sont désormais bien connus. Mais il est impossible de laisser aux services juridique et de la conformité le soin de traiter seuls ces problèmes.

LES AFFAIRES Kaseya, Solarwinds ou, à une échelle moindre, l'attaque sur Trezor via un simple compte MailChimp l'ont clairement démontré : le risque qui pèse sur la supply chain IT est loin d'être théorique. Dans un récent rapport* sur les attaques via les tierces parties, Black Kite évaluait à 23% la part des incidents de sécurité directement imputables aux éditeurs de logiciels eux-mêmes.

Gérer ce risque lié aux tierces parties est un impératif pour toutes les DSI et tous les fournisseurs, y compris les PME qui vont devoir se ▶▶▶

▶▶▶ mettre au pas pour ne pas être évincées des appels d'offres. Or, envoyer des questionnaires et faire signer des clauses contractuelles dédiées à la cybersécurité reste une tâche particulièrement rébarbative pour tous, tant pour celui qui les envoie et traite les réponses, que pour les fournisseurs qui reçoivent ces questionnaires en grande quantité. Pour autant, tout ce traitement « administratif » du risque ne met pas à l'abri une entreprise d'attaques via une brique logicielle de son SI ou une attaque par rebond via un de ses prestataires.

Face à ce besoin, de multiples prestataires et éditeurs de services se sont positionnés. Des cabinets de conseil, des agences de cyber-rating, des éditeurs « pure players » de solution TPRM (« Third Party Risk Management ») ou encore de plateforme de gestion de risque qui proposent des solutions intégrées. Une diversité d'approche qui peut amener à des différences de traitement, notamment auprès des agences de notation américaines, telles que BitSight et SecurityScorecard, ou françaises Cyrating et Board of Cyber.

LE CYBER RATING, UNE ÉVALUATION AUTOMATISÉE QUI N'EST PAS SANS BIAIS

Présent sur le FIC 2023, Clément Marcelot, Consulting Engineer chez BitSight, a résumé comment est né cette activité alors que l'éditeur compte aujourd'hui plus de 3 000 clients dans le monde et plus de 40 millions d'organisations notées par ses soins : « *Le point de départ est de transposer des problématiques techniques complexes pour appréhender le risque cyber d'une organisation dans une notation. Ce rating, qui va de 250 à 900, est produit en continu par BitSight. Chaque jour, il peut potentiellement changer au travers d'une plateforme SaaS. Nous collectons des signaux sortants, comme les données qui proviennent des adresses IP des organisations. Mais on va aussi regarder les systèmes exposés, les configurations, pour en déduire ou pas l'application des meilleures pratiques et des signaux qui vont nous en dire plus sur la performance cyber de l'organisation dans le temps.* » BitSight s'appuie ainsi sur 120 sources de données et plus de 260 milliards d'événements journaliers pour calculer une note sur 23 vecteurs de risque.

3,99 M€
C'est la franchise moyenne en assurance cyber pour les grandes entreprises françaises.
(source - AMRAE 2021)

LE CESIN DÉCLENCHE LA CONTROVERSE SUR LE CYBER-RATING

En juin dernier, le CESIN publiait un communiqué relatif aux pratiques du cyber-rating, cette notation des fournisseurs par des cabinets indépendants dont les assureurs sont friands. En effet, l'association pointe l'absence de méthodes et de référentiels partagés entre les acteurs du cyber-rating, ce qui peut faire apparaître des différences de notation selon que l'on est expertisé par l'un ou l'autre de ces acteurs. Mylène Jarossay, présidente du CESIN soulignait alors : « *Un processus de notation doit être vertueux et source de progrès. Il est important que les méthodes de calcul de scores soient partagées en toute transparence, et que l'on ait conscience des limites de ces évaluations menées de l'extérieur, pour connaître le niveau réel de sécurité des organisations, c'est-à-dire leur capacité globale à répondre aux cyber risques.* » Le CESIN craint notamment que cette course à la meilleure note ne détourne les organisations d'investissement cyber moins visibles des algorithmes des agences, mais pourtant essentielles en termes de défense...

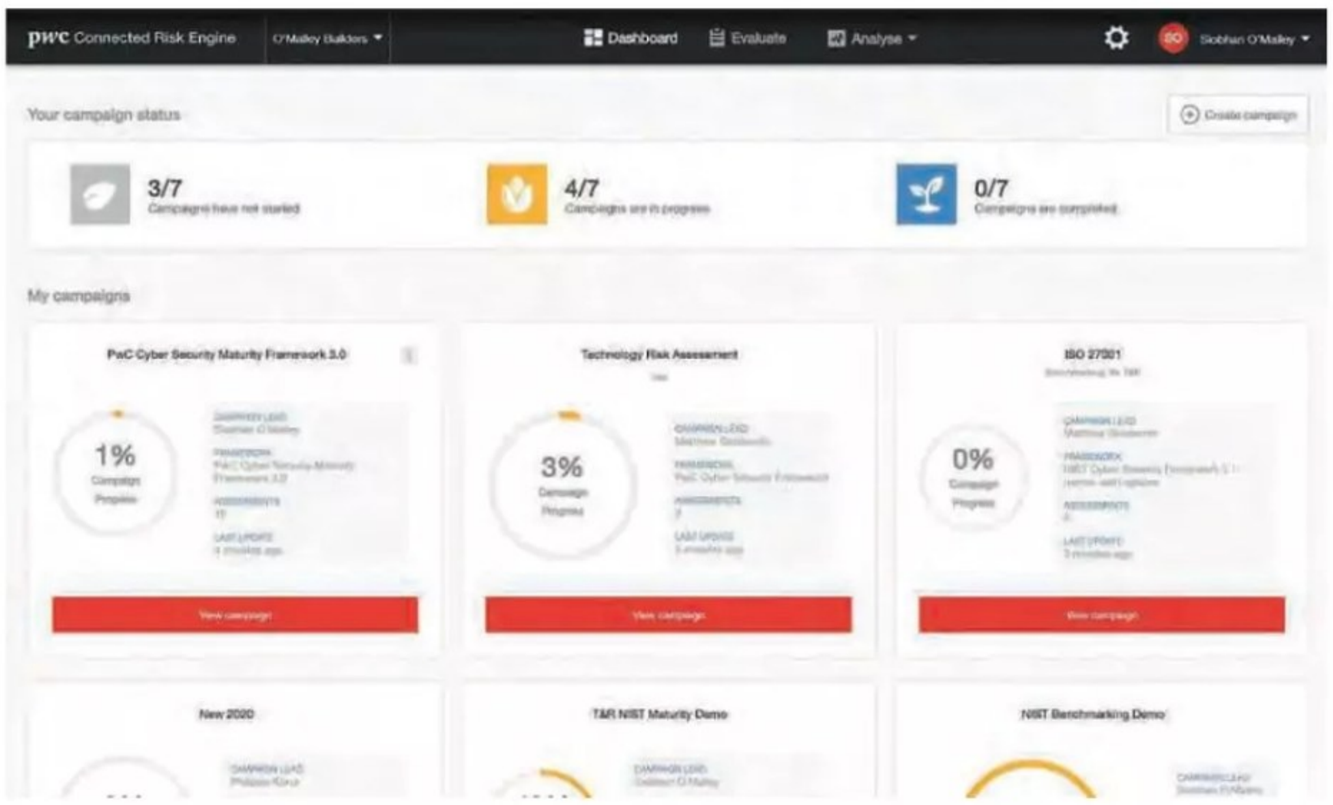
Éclairage marché

Luc Declerck, Managing Director de Board of Cyber

S'adapter aux différentes problématiques

« En axant Security Rating sur les cas d'usage, notre solution répond aux besoins de nos clients : les PME, pour qui une cyberattaque représente un risque létal, les grandes entreprises, qui souhaitent évaluer le risque cyber de leurs fournisseurs et de leurs filiales, les grandes collectivités locales, qui veulent avoir, à l'échelle de leur territoire, un observatoire cyber de leur territoire, les banquiers qui souhaitent évaluer le risque cyber de leurs clients... Nous adaptons toujours notre offre aux problématiques précises de nos clients. »

Board of Cyber veut concurrencer ces grandes agences de notation cyber internationaless en axant son offre sur des cas d'usage précis, comme le précise Luc Declerck, Managing Director de l'éditeur : « *La valeur ajoutée de notre solution Security Rating est d'adresser des cas d'usage précis, afin de donner à nos clients les armes pour effectuer les correctifs : ils sont alors totalement autonomes pour remédier aux failles de sécurité et améliorer leur performance cyber et construire autour d'eux un écosystème de confiance.* »
L'éditeur étend son offre avec le lancement, en septembre, d'une notation cyber de l'Active Directory : « *Avec ces deux solutions, nos clients bénéficieront d'une visibilité large de leur maturité cyber de façon 100 % automatisée. Par ailleurs, l'acquisition de TrustHQ, que nous avons très récemment annoncée, complète notre offre en permettant aux RSSI et directeurs de la cybersécurité d'automatiser des opérations de gouvernance.* » À ce jour, le plus gros client de Board of Cyber suit plus de 800 entités.



Un exemple de solution de Third Party Risk Management : le Connected Risk Engine Cyber de PWC

LA CYBER, UN RISQUE À GÉRER PARMI D'AUTRES

Les éditeurs de logiciels de gouvernance, risques & conformité (GRC) sont nombreux à proposer un module TPRM à leurs clients. C'est notamment le cas de OneTrust dont la solution de gestion liée aux risques tiers fait partie du Cloud « GRC & Security Assurance », pilier intégré et interconnecté à toutes les solutions de la plateforme Trust Intelligence (Privacy, éthique, ESG...).

163,7 M€
C'est le montant global des indemnisations versées pour les cyberattaques en France en 2021.
(source - AMRAE 2021)

Éclairage marché

Olivier Pantaleo, CEO & Co-dirigeant d'Almond

Des acteurs publics très exposés

« La gestion des risques liés aux tiers est un enjeu crucial pour les acteurs publics comme privés. En effet, pour réduire les coûts, optimiser leurs opérations ou créer de la valeur, les entreprises multiplient les recours aux tiers fournisseurs. Résultat : la dépendance à leur égard augmente, et les risques aussi. Par conséquent, les attaques se portent de plus en plus sur la supply chain des organisations et dans notre monde hyperconnecté, aucune entreprise n'est à l'abri des attaques par rebond. »

« *La solution englobe un module principal TPRM (Third-Party Risk Management) et un module complémentaire TPRE (Third-Party Risk Exchange)* » explique Antoine Rousseau, Cloud Specialist, GRC chez OneTrust. « *OneTrust TPRM permet d'automatiser la gestion des risques tiers, en passant par l'enregistrement initial (on-boarding), l'évaluation des risques, leur mitigation, la surveillance continue et le reporting. Le module TPRE donne accès à des milliers d'analyses de risques tiers de premier plan, provenant de multiples sources d'informations (agences de cyber-rating...).* »
L'éditeur joue la carte de l'offre intégrée et interconnectée à toutes les solutions de sa plateforme « Trust Intelligence » de OneTrust (protection des données personnelles, préférences et consentements, gouvernance des données, GRC, éthique et conformité...), pour rompre avec les silos et collaborer de manière transparente. En outre, la solution dispose de bibliothèques de templates, à jour et évolutives, avec un vaste choix de normes et standards (ISO 27001, NIST, RGPD,...).
Cyber Rating et applications de TPRM et TPRE, les DSI disposent d'outils pour évaluer le niveau de sécurité de leurs fournisseurs de solutions et des partenaires commerciaux de leur entreprise. Reste à relever le véritable défi posé par la gestion du risque tierces parties : faire s'élever le niveau de maturité cyber de l'ensemble de cet écosystème... un enjeu qui va bien au-delà du simple outillage. ■ *Par Alain Clapaud*

*« 2022 Third-Party Breach Report », Black Kite.

5

SERVERLESS, L'ÂGE DE LA MATURITÉ TECHNOLOGIQUE

Cette autre façon de concevoir et d'exécuter des applications dans le Cloud a gagné en **maturité** et s'impose de plus en plus comme une évidence.

QUAND AMAZON WEB SERVICES a dévoilé Lambda en 2014, beaucoup ont vu dans ce service un moyen simple d'exécuter des scripts sans trop se soucier d'infrastructure. De petit moteur d'exécution pour SysOps, le Serverless s'est transformé en un véritable écosystème de solutions. De multiples langages de programmation sont disponibles, y compris la possibilité d'exécuter un conteneur custom, de même que des couches de persistances, des bus de messages : toutes les briques indispensables à la création d'application de grande envergure.

Illustration de ce changement d'échelle, la décision récente d'Amazon Prime de basculer sa plateforme de streaming vidéo vers le Serverless. Frédéric Barthelet à la tête de la Serverless Tribe de Theodo commente cette décision : « *Il y a quelques mois, l'équipe d'Amazon Prime annonçait que la migration du service sur AWS Lambda avait* ▶▶▶

Éclairage expert

Adèle Gauvrit, responsable de l'engineering Serverless chez Theodo

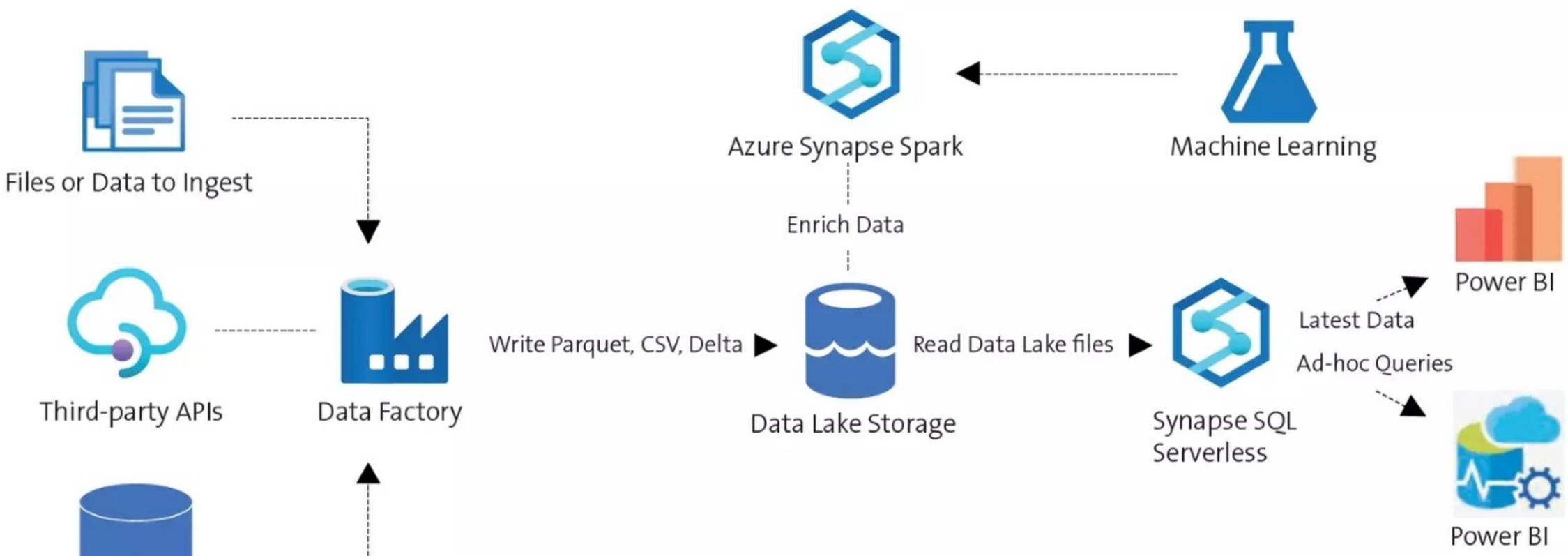
Réduire le TCO et le Time to Market

« Avec environ 117 millions d'utilisateurs, Amazon est numéro deux mondial sur un marché extrêmement compétitif. S'ils ont fait ce choix d'aller vers le Serverless, c'est que le Serverless permet de réduire le TCO, permet de créer des prototypes rapidement, de monter à l'échelle très rapidement avec l'accroissement du trafic, mais aussi de faire du Scale to 0, c'est-à-dire de n'utiliser que les ressources qui sont nécessaires à l'instant t. Plus important, le Serverless permet d'aller plus rapidement sur le marché et conquérir de nouveaux utilisateurs, mais aussi de réduire le Time to Market des nouvelles fonctionnalités. »

▶▶▶ *permis d'abaisser de 90% leurs coûts d'infrastructure. L'utilisation d'un framework très populaire, baptisé Serverless, montre qu'en mai 2023 il y a eu près de 5 millions de téléchargements de ce framework. Son alternative, l'AWS CDK connaît aussi une forte croissance, et un framework disruptif comme SST connaît une croissance exponentielle.* » Les services Serverless sont bien plus sophistiqués qu'ils ne l'étaient il y a 5 ans, et les utilisateurs disposent de moyens FinOps afin d'abaisser encore les coûts de fonctionnement de leurs infrastructures, notamment en optant pour les versions ARM de ces services ou des modes de stockage S3 plus abordables lorsque c'est possible. AWS propose notamment des solutions afin de répondre à un défaut inhérent à l'approche Serverless : la latence induite par les « cold start », c'est-à-dire qui impose un délai de déploiement du conteneur d'exécution de la fonction au moment de sa toute première invocation.

DES ALTERNATIVES AUX OFFRES DES CSP

Si AWS, Microsoft avec Azure et Google offrent des services Serverless depuis des années, d'autres acteurs offrent des alternatives. Ainsi, Cloudflare est positionné sur les services de réseau en Zero Trust, services orientés applicatifs et services aux développeurs, dans lesquels l'éditeur propose des produits Serverless depuis 2018. « *Sur le Serverless, nous conservons trois grands différentiateurs par rapport aux hyperscalers* » argumente Stéphane Nouvellon, architecte solutions chez Cloudflare : « *D'une part, il n'y a pas de notion de région sur Cloudflare : on ne lance pas un service sur une région comme l'Europe, par exemple. C'est notre travail de réaliser les réplications si l'entreprise est un acteur global.* » Fort de ses 290 data centers, le fournisseur revendique un temps de latence inférieur à 50 ms auprès de 99% de la population mondiale connectée à Internet. Le responsable évoque aussi la forte intégration des services hébergés : « *Il est très simple de faire communiquer nos services les uns avec les autres, sans complexité inutile et sans introduire de latences.* » Enfin, Stéphane Nouvellon estime faire la différence sur le cycle de vie de l'application : « *L'entreprise doit pouvoir intégrer l'application dans son écosystème*



ANALYSE EXPLORATOIRE DES DONNÉES

Carrefour ou Air France utilisent le Serverless pour créer des intégrations de données et notamment alimenter leur data lake. Aujourd'hui, les capacités des écosystèmes Serverless vont bien au-delà du simple traitement de données au fil de l'eau.

Microsoft Azure

logiciel, avec l'observabilité, les opérations, intégrer l'application dans les tableaux de bord de l'équipe SRI qui s'occupe de la disponibilité des services. »

DES OFFRES ET DES MÉTHODOLOGIES PLUS MATURES

Outre une offre du marché bien plus riche que par le passé, les architectures et méthodologies ont été affinées afin de porter des applications critiques. C'est le cas de la poste néerlandaise qui traite environ 1,2 million de colis par jour sur une infrastructure de type EDA (Event Driven Architecture) : *« Nous traitons littéralement des milliards d'événements par mois sur AWS et nous avons pu le faire en suivant les règles que nous avons réussi à mettre en place pour évoluer vers une architecture de type EDA »* explique Luc Van Donkersgoed, Lead Engineer chez PostNL et AWS Serverless Hero. *« On commence avec quelques microservices interconnectés, optimisés de manière locale. Puis on ajoute d'autres services, d'autres nœuds, on échange différents types de données, on utilise différents types d'encodage, on met en œuvre d'autres langages : on finit par perdre toute structure globale. Il devient difficile d'investiguer sur les incidents de production, il devient difficile de modifier ou retirer un service et on finit par avoir du mal à évaluer tous les impacts d'un changement sur un microservice. »* Une approche qui a séduit les analystes de Forrester qui ont placé Cloudflare en tant que leader des solutions de développement Edge.

L'exploitation et la maintenance d'applications comptant des dizaines de microservices exécutés sur des infrastructures Serverless restent un véritable défi pour les équipes DevOps. Des solutions adaptées aux caractéristiques du Serverless sont en train d'apparaître. C'est notamment le cas des approches « Infrastructure from code » dont l'idée est de générer l'infrastructure Serverless simplement en lisant le code source de l'application. Il s'agit de fournir tant des capacités d'auto-provisioning, d'auto-instrumentation, de génération automatique de la documentation, de self-testing et self-auditing, une administration et une optimisation automatique, une mise à jour automatique. Plusieurs start-up se sont positionnées sur cette approche « Infrastructure from code » : Ampt et Nitric privilégient une approche SDK, Model et Klotho l'annotation du code, Encore et Shuttle misent sur un panachage des deux approches tandis que Wing et Dark mises sur un nouveau langage spécialisé. ■

Par Alain Clapaud

DIX CONSEILS POUR CRÉER UNE ARCHITECTURE EDA PÉRENNE

- **Utiliser JSON pour tous les événements**

C'est un moyen de rendre une architecture plus prévisible et maintenable.

- **Utiliser une enveloppe d'événement standard / wrapper**

Celle-ci va porter les métadonnées relatives à l'événement et la donnée transportée.

- **Adopter un ID d'événement unique pour les métadonnées de chaque événement**

Cela apporte observabilité, une priorité au stockage et de l'idempotence.

- **Utiliser des schémas et des contrats**

Construire un système avec un contrat pour tout échange.

- **Maintenir une compatibilité ascendante**

Si une nouvelle version d'un événement est proposé, le consumer doit accepter un nouveau contrat.

- **Maintenir un registre de schémas**

Il faut disposer d'un repository en ligne qui est la source unique de vérité.

- **Adopter un courtier d'événements / Event Broker**

Une intégration directe ou une architecture Mesh est impossible à maintenir.

- **Privilégier des API supportant les événements**

Cela aide à faire évoluer les événements et de monter à l'échelle jusqu'à des millions de consommateurs.

- **Choisir un modèle Storage First**

Il faut stocker les événements dans une file d'attente ou une base de données.

- **Tracez vos événements**

Cela permet d'identifier toutes relations, les abonnements et bien évidemment les causes d'incidents, de latence.

Crédit Luc Van Donkersgoed

« L'offre Cloudflare Workers a évolué vers toute une gamme de produits qui répondent aux besoins des développeurs, au-delà de la simple exécution du code. On parle aujourd'hui d'un véritable écosystème Serverless. »

Stéphane Nouvellon, architecte solutions chez Cloudflare.

CYBERATTAQUE

LA SEINE-ET-MARNE PORTE ENCORE DES STIGMATES

Le Département de Seine-et-Marne ressent encore des effets de la cyberattaque qu'il a subie en novembre 2022.

DU MIEUX à la Maison départementale des personnes handicapées (MDPH) de Seine-et-Marne ? Depuis le 21 août, elle peut accueillr à nouveau le public sans rendez-vous. Ce n'était plus le cas depuis la mi-juin. Le personnel pouvait ainsi se concentrer sur l'instruction de 19 000 dossiers en attente. Tous déposés avant la cyberattaque qui avait frappé, début novembre 2022, le Département.

Pour assurer une forme de continuité, son administration s'est dotée de clés 4G et mis en service 1 800 numéros de téléphone portable et des extensions de forfait pour des salariés. Montant de la facture : 25 000 €.

UNE "RANÇON" DE 10 MILIONS D'EUROS

Vers la fin novembre, le Département affirmait avoir détecté l'origine de l'attaque. Sans en dire davantage, sinon qu'un PC portable avait fait office de point d'entrée. Un des fichiers retrouvés lors de l'analyse du parc informatique (dont 3 500 ordinateurs sur l'ensemble des sites départementaux) contenait une demande de rançon : 10 millions d'euros. Officiellement, il n'y a pas eu de suite, malgré le refus de payer...

Certaines données ne seront pas récupérées. À la compta, par exemple, on a tiré un trait sur celle d'octobre, car « trop de risques ». Le service a commencé à retrouver un fonctionnement informatique correct en début d'année, après avoir rempli à la main des milliers d'ordres. Il a d'abord travaillé sur un logiciel de secours, en suivant les consignes du Trésor public.

La gestion du paiement des aides sociales s'est révélée difficile, à tel point que l'opposition a dénoncé un « [bricolage] avec la CAF ». Des accords de teneurs diverses se sont en tous cas noués pour proroger des versements. Par exemple, ceux de l'AAH (Aide aux adultes handicapés) et de l'AEEH (Allocation d'éducation de l'enfant handicapé).

PRESTATIONS SOCIALES : UN CASSE-TÊTE POUR LE DÉPARTEMENT

Le Département a également pris des mesures pour les aides qu'il a à sa charge, comme la PCH (Prestation de compensation du handicap). La tension se situe sur les droits qui devaient s'ouvrir après novembre, qu'ils soient liés à de nouveaux dossiers ou à des changements de situation. En mai, le Département assurait que certains de ses agents s'étaient portés volontaires pour accélérer le traitement des dossiers. Ainsi avait-il pu actualiser « plus de 9 500 dossiers individuels » depuis le 13 mars, date officielle du début de rétablissement des logiciels impliqués. *« Avant la cyberattaque, le délai global moyen de traitement d'un dossier était de 4,5 mois contre 8,3 mois aujourd'hui »*, avait-il finalement déploré en juin, dans le cadre d'un point de situation sur la MDPH. Et d'évoquer la sollicitation d'une dizaine d'opérateurs occasionnels de saisie... en plus, donc, de la réaffectation du personnel chargé de l'accueil. Promesse d'alors : d'ici à l'été, avoir régularisé tous les versements PCH bloqués, avec effet rétroactif. La mise sous pli manuelle des décisions prises – en l'absence de flux vers le prestataire – n'accélère pas les démarches.

Aux dernières nouvelles, les musées départementaux restent en accès gratuit, faute de pouvoir encaisser les paiements. Le Conseil départemental de Seine-et-Marne a pour sa part voté une modification des dotations prévisionnelles : avec la cyberattaque, des investissements prévus en 2022 ont été reportés sur le budget 2023. ■

Clément Bohic

SASE

PEUT-ON FAIRE AVEC UN SEUL FOURNISSEUR ?

Trois consoles de gestion, le maximum acceptable pour du SASE ? Gartner en a en tout cas fait un critère éliminatoire dans son dernier « Magic Quadrant » consacré à ce marché.

C'EST LE PREMIER du genre, le cabinet américain ayant jusqu'alors concentré son analyse sur le SSE. Autrement dit, sur les offres couvrant le volet sécurité et s'appuyant sur des partenariats pour la partie WAN. Dans ce domaine, trois « leaders » se détachent au dernier pointage : Netskope, Zscaler et Palo Alto Networks. Seul ce dernier apparaît dans le Quadrant du SASE («secure access service edge»). Ou plus précisément, pour reprendre la terminologie de Gartner, du SVSASE. C'est-à-dire du SASE monovendeur (« single-vendor »). Exit, donc, les offres jointes. Gartner juge les fournisseurs sur deux axes. L'un prospectif (« vision »), centré sur les stratégies (sectorielles, géographiques, commerciales, marketing, produits...). L'autre centré sur la capacité à répondre effectivement à la demande (« exécution » : expérience client, performance avant-vente, qualité des produits/services...).

FONCTIONNALITÉS, PRIX, INTERFACES : QUI SE DISTINGUE ?

Gartner a tenu compte des offres telles qu'elles étaient au 12 avril 2023. Trois fournisseurs bénéficient d'un bon point sur la partie SD-WAN : Juniper, Versa et VMware. Juniper se distingue aussi sur la partie sécurité, pour ce qui est de l'accès web et des données. Même chose pour Forcepoint, dont Gartner salue également la brique de contrôle des SaaS. L'offre de Cato Networks, au contraire, manque de capacités sur ce dernier volet. Palo Alto Networks n'a quant à lui pas de RBI (isolation du navigateur à distance) natif. Chez Versa et VMware, la détection des menaces et la sécurité des données sont respectivement en retrait. Trois acteurs sont perçus comme disposant d'une roadmap alignée sur les besoins du marché : Cisco, Forcepoint et Palo Alto. Gartner n'en dit pas autant de Versa et de VMware, dont les stratégies sont « peu disruptives ». Idem pour Cato, en tout cas auprès des grandes entreprises.

VMware a en revanche pour lui une tarification intéressante. Comme Cisco, tout du moins pour son offre principale. La tarification est, au contraire, « bien plus élevée » chez Palo Alto ; et « très chère » chez Juniper. En matière d'interface utilisateur, Cato se distingue comme Palo Alto et Versa. Forcepoint a pour lui une infrastructure « robuste » de points de présence. L'empreinte géographique est, au contraire, limitée chez Cisco comme chez Juniper.

On aura noté le bon point donné à Cisco sur la partie d'analyse de la menace (« Threat intelligence »)... et le mauvais point donné à Palo Alto sur la prise en charge linguistique.

VERS UNE INCLUSION DU XDR DANS LES OFFRES SASE

Faute d'une offre commerciale complète au 12 avril 2023, Cloudflare, Cradlepoint, HPE et Netskope ne figurent pas au Quadrant. Ils bénéficient toutefois d'une « mention honorable ».

Gartner s'attend à voir entrer, sous 18 mois, jusqu'à une dizaine de fournisseurs sur ce marché encore faiblement mature. À cette même échéance, 40 % des offreurs proposeraient du XDR ou du MDR en add-on, accompagnant l'extension à des segments adjacents. À plus long terme (horizon de quatre ans), on surveillera l'ajout d'options de compute couvrant des scénarios edge. ■ *Clément Bohic*

LE QUADRANT MAGIC COMPORTE :

• Sur l'axe « vision » :
1. Palo Alto Networks
2. Forcepoint
3. Cisco
4. Cato Networks
5. Versa Networks
6. Fortinet
7. VMware
8. Juniper Networks

• Sur l'axe « exécution » :
1. Palo Alto Networks
2. Cato Networks
3. Versa Networks
4. Fortinet
5. Cisco
6. VMware
7. Forcepoint
8. Juniper Networks

RETEX

CARREFOUR LINKS PILOTE LES TRANSFERTS DE DONNÉES AVEC LE SERVERLESS

Le groupe Carrefour compte 100 millions de clients dans 31 pays, ce qui représente une masse de 3 milliards de tickets de caisse par an. Des données que Carrefour centralise grâce au Serverless pour les commercialiser auprès des industriels.

CARREFOUR LINKS a été créé en 2021 afin de commercialiser les données du groupe à destination des industriels du CPG (« Consumer Packaged Goods », biens de consommation emballés) comme Coca-Cola, Nestlé, L'Oréal. Le groupe Carrefour se compose de huit pays intégrés et de 23 pays franchisés. Pour alimenter le data lake de Carrefour Link, il faut collecter les données auprès de chacun de ces pays.

« Ce sont des milliards de lignes de tickets de caisse qu'il faut décomposer en produits, puis ensuite rassembler par CPG » résume Guillaume Blaquiere, Group Data Architect chez Carrefour. *« C'est un gros chantier, car nous avons aujourd'hui 7 Po de données sur Google BigQuery et lorsqu'il est nécessaire d'effectuer un Full Refresh de notre data lake, ce sont 72 Po de données qu'il faut traiter. »* Or chaque pays fédéré dispose de son propre Data Warehouse et la synchronisation quotidienne ne peut démarrer avec un pays qu'à partir du moment où celui-ci a achevé le chargement des tickets de caisse de la journée.

72 Po

72 petaoctet, c'est le volume de données à traiter lors d'un Full Refresh du data lake.

RETAIL MEDIA : UN NOUVEAU BUSINESS

Carrefour se positionne sur le secteur du retail media qui pèse 30 milliards d'euros au niveau mondial et 500 millions d'euros en France (source SRI). Le distributeur a crée UNLIMITAIL avec Publicis Groupe, une joint-venture dédiée, pour gérer ce nouveau business en Europe Continentale, Brésil et Argentine. Elle a déjà séduit 13 partenaires représentant plus de 120 millions de clients fidèles et 1,5 milliard de pages visitées par mois. Parmi eux : Kingfisher France, Groupe Galeries Lafayette, Rakuten France, et Showroomprive Group.

UN DATA LAKE ET UN SCHEDULER POUR EXÉCUTER LE CODE

Au moment de la création du data lake, un « scheduler » (module choisissant l'ordre d'exécutiuon des tâches) a été mis en place afin d'exécuter le code venant récupérer les données en mode séquentiel, avec des traitements qui ne s'achevaient que vers 7/8 heures du matin. *« Une telle approche n'est pas scalable car on fait de plus en plus de traitements. Nous avons donc voulu lancer les chargements en parallèle. Cela a permis de réduire les temps de traitement et achever les traitements vers 5 heures du matin. »* L'équipe technique a mis en œuvre la solution dbt pour lancer de multiples requêtes en parallèle, puis attendre la fin de celles-ci pour finaliser la table de destination. L'inconvénient de l'approche est de perdre du temps entre la phase Fan In (collecte des données) et Fan Out (constitution du « Data Mart » [comptoir de données à des fins précises]), car un délai est nécessaire au cas où un pays mettrait ses données à disposition plus tardivement.

L'équipe technique souhaite aller vers un système événementiel, avec une notification lorsque la synchronisation de données s'achève, avec l'envoi d'un message sur le bus Google Cloud Pub/Sub. *« Le message va invoquer un Cloud Run* [solution Serverless à base de conteneurs de Google Cloud Platform] *qui va ensuite dérouler l'ensemble des process que nous avions précédemment. Cela nous permet d'achever les traitements plus tôt, vers 4 heures du matin. Cela nous donne le temps de rejouer des traitements le matin en cas d'incident. »* L'architecture suppose que le scheduler se mette

en attente à partir de 22 heures, mais il est difficile de savoir si les données sont prêtes ou pas.
Au sein du groupe, chaque pays a une maturité différente vis-à-vis de la donnée. En France, les tickets sont chargés 2-3 minutes après le passage en caisse, alors que le Brésil met à jour sa base de données vers 22 heures et l'Espagne exploite une plateforme Cloudera, ce qui les oblige à faire une extraction sur BigQuery pour que les données puissent être lues par la maison-mère.

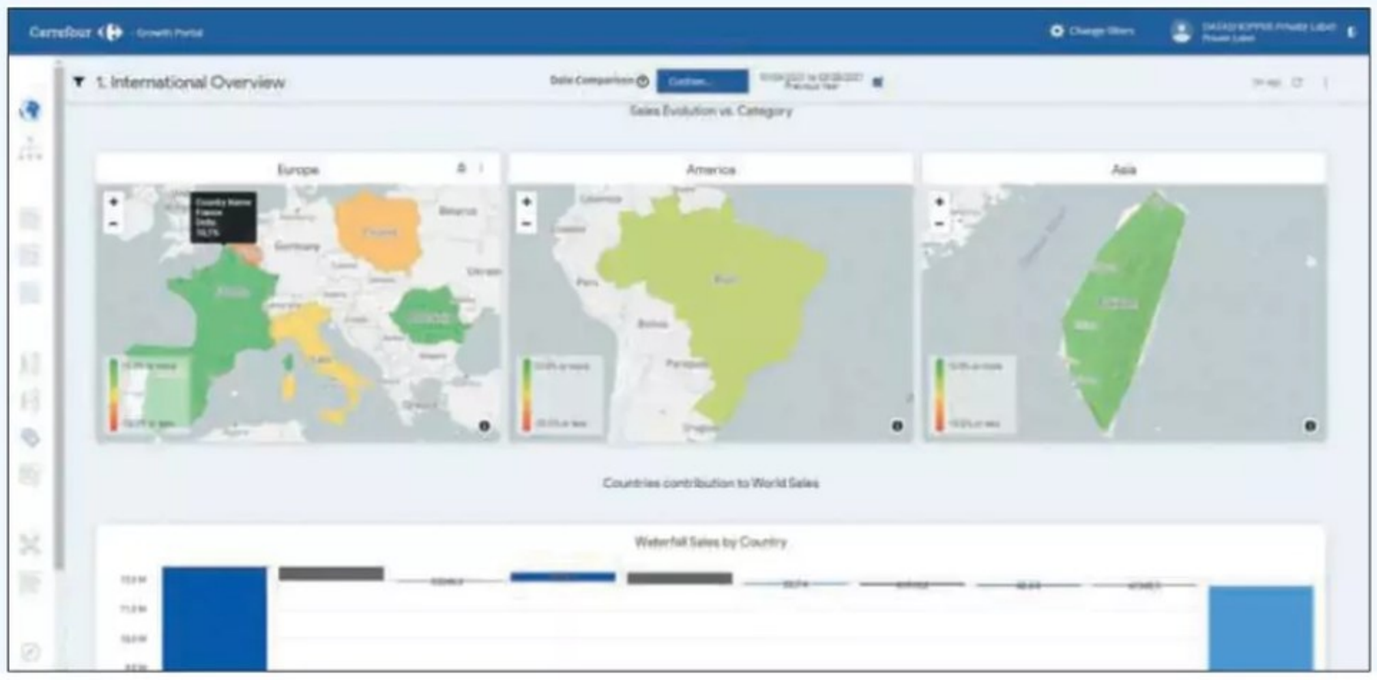
IMPLÉMENTATION DE EVENTSYNC SUR GCP

Chaque pays étant indépendant, il est impossible d'imposer un même scheduler pour tous. Nous voulons que les pays nous envoient un événement lorsqu'ils ont terminé les traitements de leur côté, pour que les traitements puissent démarrer en central lorsque tous les pays ont envoyé leur message. « *Sur GCP* [Google Cloud Platform], *cela n'existe pas. J'ai donc implémenté sur GCP un outil open source baptisé EventSync. Il exploite Cloud Run pour la partie runtime, FileStore pour le stockage et Google Cloud Pub/Sub pour envoyer les messages. Chaque pays peut ainsi déclencher les traitements quand il le souhaite, dispose d'une URL de notification statique et va envoyer le message de disponibilité des données sur le bus de message.* » L'ensemble des briques d'infrastructures sont gérées par Google en mode Serverless et l'application est sécurisée avec Cloud Identity and Access Management (IAM). ■

Par Alain Clapaud

> *L'idée de Carrefour Links est de créer des GDW* [« Group Data Warehouse », entrepôt de données], *puis, à partir de cette base développer des Use Cases comme PoS & Data Shopper, Merch & Supply, Search & Display, etc. Ce sont des produits que nous commercialisons auprès des CPG. »*

Guillaume Blaquiere, Group Data Architect chez Carrefour.



L'application PoS et Data Shopper proposée par Carrefour Links permet à l'industriel d'analyser la performance commerciale de ses produits marché par marché sur plus de six milliards de transactions stockées.

RETEX

COMMENT LEGO EMPILE LES BRIQUES SERVERLESS POUR RENDRE SES SERVICES INCASSABLES

En 2017, après un plantage de son site en plein Black Friday, Lego change d'approche technique. Place aux services Serverless d'AWS tant pour le front Web qu'en back office de son site, dans une approche strictement collée au « Domain Driven Design » (conception pilotée par le domaine).

« EN NOVEMBRE 2017, *alors que le site lego.com reposait encore sur une ancienne technologie monolithique, la plateforme legacy de notre site web s'est crashée et notre site web est devenu inaccessible* » raconte Clara Villa, Software Engineer chez The Lego Group. « *Nous avons alors décidé que jamais plus nous devions nous retrouver dans une telle situation.* »

Au printemps 2018, une première expérimentation du Serverless est lancée et les équipes commencent à développer de plus en plus de logiciels en Serverless. En juillet 2019, la version Serverless du site de e-commerce de la célèbre marque est mise en production. Celui-ci s'appuie alors sur 20 microservices développés par une vingtaine d'ingénieurs répartis entre une équipe backend (en dorsal, partie invisible du logiciel) / intégration et une équipe frontend (en frontal, partie visible du logiciel). À la rentrée 2020, le système de paiement bascule à son tour.

200 000

C'est le nombre de requêtes traitées par l'API Gateway qui sollicite des fonctions Serverless AWS Lambda.

SUPPORTER LES PICS D'AUDIENCE DU SITE

La décision de basculer sur des fonctions Serverless portées par AWS a porté ses fruits car durant l'été 2021, alors que Lego fait un gros lancement de produits, le site va connaître une audience record, un pic de trafic encaissé sans broncher par l'architecture Serverless mise en place par les équipes de développement de Lego à Londres : « *Nous avons réalisé alors que les gros volumes de trafic n'étaient plus pour nous une problématique, que nous pouvions absorber de gros pics de trafic une ou deux fois par mois à cause de campagnes marketing sans difficulté.* » Actuellement, l'architecture du site Lego.com s'appuie très largement sur les services d'Amazon Web Sites Services. L'architecture EDA (Event Driven Architecture) du site sollicite notamment l'API Gateway pour solliciter des fonctions Serverless AWS Lambda. L'équipe Serverless de Lego a grossi pour compter aujourd'hui 25 petites équipes. L'équipe à laquelle appartient Clara Villa est chargée

« L'approche « Serverless First » est amenée à se transformer rapidement en « Serverless Must ». Mais si vous vous plongez directement dans le Serverless, que vous développez des fonctions à gauche à droite, vous allez vous retrouver dans le pétrin. Il ne faut pas oublier les bases car elles sont ensuite très utiles. La première est de penser Domain First. »

Sheen Brisals, Senior Engineering Manager chez The Lego Group et AWS Serverless Hero.

de l'API de paiement de Lego. Celle-ci est mise en œuvre sur le site de vente en ligne, mais aussi pour le BtoB, les expéditions, le marché éducation et le service support Lego. Il est interconnecté avec les réseaux de paiement par carte bancaire, Paypal. Cette équipe gère plus de 20 microservices, soit plus de 80 fonctions Lambda développées, 10 fonctions STEP, plus de 40 règles EventBridge. Le volume de données stockées dans DynamoDB dépasse les 100 Go. En termes de trafic, l'API est amenée à traiter plus de 1 000 commandes, 200 000 requêtes, 20 000 notifications et 150 invocations de fonctions Lambda chaque minute.

25 ÉQUIPES AU TRAVAIL SUR UNE APPROCHE DDD

Pour faire cohabiter toutes ces équipes autour d'une architecture efficace, Lego s'est appuyé sur le DDD (« Domain Driven Design »). Sheen Brisals, Senior Engineering Manager chez The Lego Group résume l'approche : *« Pour une architecture Domain Driven, il faut diviser la problématique par domaine, puis sous-domaines, pour arriver à la notion de Bounded Context. Lorsque vous avez bien défini les frontières de chaque domaine, il devient plus facile d'en assigner la responsabilité à une* petite équipe, *une Two Pizza Team. Elle sait précisément ce qu'elle doit développer, elle dispose des protocoles pour communiquer, elles peuvent alors développer leurs microservices ou applications dans le cadre de ces frontières définies préalablement. Il s'agit de l'approche que nous avons adoptée chez lego.com. »* Lego n'a bien évidemment pas basculé l'ensemble de ses applications en Serverless à ce jour. Chaque équipe choisit la technologie qui est la meilleure pour elle. Lego dispose toujours d'un data center et utilise les conteneurs sur Kubernetes, mais le Serverless marque des points. ■

Par Alain Clapaud

Un bon découpage en domaines/sous-domaines est le secret de l'efficacité d'une architecture DDD. Ici les domaines relatifs à la fidélité client chez Lego.

Le frontal du site Lego est protégé par AWS WAF et met en œuvre les services AWS Faregate et Amazon ElastiCache. Ce frontal communique avec le cœur du site via la passerelle Amazon API Gateway, qui sollicite des fonctions AWS Lambda ainsi qu'Amazon Kinesis Data Firehose, la brique ETL de la plateforme AWS. Outre le stockage DynamoDB, l'architecture sollicite les briques d'échanges SQS, SNS, Event Bridge et des fonctions STEP.

IA & ML

COMMENT NETFLIX A CONÇU SON INFRASTRUCTURE DE MACHINE LEARNING

Le leader mondial du streaming vidéo a constitué une infrastructure de machine learning dédiée aux contenus multimédias.

QUEL POINT COMMUN entre l'orchestrateur de microservices Conductor, le planificateur de tâches Dagobah, le format de données Iceberg, la bibliothèque de data science Metaflow et le gestionnaire de conteneurs Titus ? Toutes ces briques, aujourd'hui open source, émanent de Netflix. La plateforme américaine les a notamment mises à contribution pour construire une infrastructure de machine learning dédiée aux contenus multimédias. Elle est revenue dernièrement sur ces travaux, en mettant l'accent sur le passage à l'échelle pour un cas d'usage en particulier : la détection des séquences qui se prêtent le mieux au « match cut » (technique de transition entre deux scènes utilisant la même composition, le même cadrage, la même action...).

UN PIPELINE EN 5 ETAPES

Dans un premier temps, l'infrastructure a été mise en œuvre à périmètre limité. En l'occurrence, un seul film ou épisode de série. Le pipeline était découpé en cinq étapes :

> Dans chaque fichier, délimiter les scènes par un système clé-valeur (numéro de la scène - numéros des images de début et de fin). Puis créer autant de fichiers individuels.

> Vectoriser chacun de ces fichiers et utiliser les vecteurs pour supprimer les doublons.

> Vectoriser à nouveau chaque scène, mais selon le type de match cut souhaité.

> Attribuer un score à chaque paire de scènes et stocker ces scores au niveau des métadonnées.

> Trier les paires par score décroissant et sélectionner les k meilleures (k étant un paramètre personnalisable).

2000

C'est le nombre moyen de plans pour un film de deux heures, soit environ 2 millions de paires de plans à comparer.

MARKEN, UN SERVICE D'ANNOTATION

Lorsqu'il s'agit de traiter plusieurs films/épisodes en parallèle et/ou d'utiliser plusieurs variantes de match cut, les choses se compliquent. D'abord parce que les vectorisations sont sensibles aux caractéristiques des fichiers – comme le format d'encodage et les dimensions. En réponse, Netflix a appliqué un prétraitement de son catalogue pour livrer des copies « normalisées ». Il fournit une bibliothèque unifiée pour y accéder : Jasper. Autre enjeu : réduire les ressources de calcul nécessaires pour qui vient exécuter ses modèles de machine learning sur ce catalogue. Netflix a développé un cluster GPU à l'appui du framework Ray et lui a associé le système de fichiers objet MezzFS pour optimiser les chargements. Il a surtout mis en place un magasin de données dans une logique de mutualisation. Il y héberge, par exemple, les paires clé-valeur correspondant à la segmentation des scènes. L'idée : éviter à chacun de les recalculer. Le tout est équipé d'un système de réplication vers diverses solutions de stockage. Sur la partie orchestration, le chantier a impliqué le développement d'une solution « universelle » capable de déclencher l'exécution des modèles de prod dès la mise à disposition de nouveaux contenus. Le manque de standardisation a là aussi été un obstacle : les opérations étaient parfois relancées alors que seules les métadonnées liées à ces contenus avaient changé. La compatibilité n'était par ailleurs pas native avec des orchestrateurs comme Conductor. Le magasin de données est connecté à un autre outil d'origine Netflix : le service d'annotation Marken. Il fait l'interface avec les applications – typiquement, les éditeurs vidéo – avec un langage de requête spécifique. ■

Par Clément Bohic

UKG simplifie et automatise les processus et fluidifie les traitements RH

Connu pour ses solutions de gestion des temps, de planification et de gestion administrative RH, l'éditeur UKG (Ultimate Kronos Group) permet aux organisations de gagner en efficacité et d'améliorer leurs performances en simplifiant et en automatisant les processus impliquant les équipes RH, les managers et les collaborateurs, et ce, où qu'ils soient et sur n'importe quel appareil.

« *Optimiser le parcours numérique de chacun est l'un des principaux défis du travail hybride, comme l'ont révélé la crise sanitaire et ses confinements. UKG y répond via People Operations qui devient le point d'entrée unique des RH, managers et des collaborateurs, de l'embauche jusqu'à leur départ de l'entreprise,* » observe Erwan Roblot, Implementation Delivery Manager chez UKG. Les interlocuteurs d'Erwan Roblot et de l'équipe implémentation des solutions UKG exercent dans une DSI ou dans une DRH. « *Lorsque le projet est porté par la direction des ressources humaines, les attentes concernent l'amélioration de l'expérience collaborateur et la conduite du changement. La DSI exprime, pour sa part, davantage d'attentes techniques et de besoins d'automatisation. Notre solution aide à fluidifier les transactions RH. Idéalement, une bonne entente entre la DRH et la DSI permet à chaque partie d'apporter sa pierre à l'édifice. Associer les deux composantes reste important,* » souligne le responsable d'équipe.

Planifier et démontrer ses activités

La gestion des temps, le suivi des activités, la génération de contrats et d'avenants, les demandes de congés s'effectuent grâce à des fonctionnalités intuitives et des échanges sécurisés. Les tâches sont ainsi réalisées en conformité avec l'évolution de nombreuses règles sociales, comptables et fiscales. Récemment, un client français d'UKG exerçant dans le secteur de la grande distribution a pu simplifier la planification du travail du dimanche pour ses salariés volontaires. Le collaborateur prend d'abord connaissance des articles légaux et des conditions proposées dans la base documentaire, avant de remplir un formulaire qui va suivre un workflow de validation : « *Le salarié voit progresser sa demande sur le portail qui sera validée par son manager. Il est important de noter qu'une bonne intégration préalable consolide les informations du SIRH et assure le transfert des données complémentaires nécessaires à l'établissement du prochain bulletin de paie.* »

Si UKG cherche à apporter des solutions à ses clients, le groupe de 15 000 collaborateurs dans le monde, doit également relever les défis du mode de travail hybride. Erwan Roblot qui gère une équipe répartie en France rassemblée autour des fonctions d'UKG People Operations, déclare : « *Nous conservons la possibilité de venir au bureau pour des temps de rencontre et des échanges informels. Grâce à l'automatisation de tâches administratives, l'équipe peut se concentrer sur les projets créateurs de valeur, sans avoir à enchaîner les visioconférences l'une après l'autre.* » ■

DEVOPS

CES PLATEFORMES QUI RECONFIGURENT LE MARCHÉ

Les plateformes DevOps ont désormais leur «Magic Quadrant», avec une consolidation des outils, autant pour éviter les redondances que les difficultés d'orchestration ou les dettes techniques.

EXIT LES TOOLCHAINS DEVOPS, place aux plateformes ? Gartner estime que cette approche n'est pas encore majoritaire*. Mais le cabinet américain juge la tendance suffisamment forte pour consacrer un Magic Quadrant aux produits qui relèvent de ce segment de marché. Il les traitait jusqu'alors sous la forme d'un « Market Guide ». D'un format à l'autre, l'axe directeur n'a pas changé : on assiste à une consolidation des outils, autant pour éviter les redondances que les difficultés d'orchestration ou les dettes techniques. L'argument des coûts est moins mis avant... Conséquence des chevauchements fonctionnels que cela implique, certains fournisseurs de plateformes DevOps ici distingués sont classés dans d'autres quadrants, par exemple, celui de la sécurité applicative ou celui des outils de gestion de projet.

GitLab est le seul à figurer dans les deux quadrants en question. Il fait partie des quelques fournisseurs de plateformes DevOps à proposer des fonctionnalités natives de sécurité applicative, aux côtés, notamment, de GitHub et JFrog. Les offreurs sont évalués sur deux axes. L'un prospectif (« vision »), centré sur la stratégie (sectorielle, géographique, commerciale, marketing, produit...). L'autre centré sur la capacité à répondre effectivement à la demande (« exécution » : expérience client, performance avant-vente, qualité des produits/services...).

MAGIC QUADRANT FOR ENTREPRISE AGILE PLANNING TOOLS
Les offreurs sont évalués sur deux axes : la « vision » et l'« exécution »
Source : Gartner (Avril 2022)

CHEZ ATLASSIAN, JIRA ET CONFLUENCE FONT LA PAIRE

La plateforme d'Atlassian regroupe des capacités de Bitbucket, Confluence, Jira Software, Jira Service Management et Opsgenie. Gartner lui donne de bons points pour son écosystème (« plus de 5 000 applications et intégrations » sur la marketplace) et sa prise en charge de multiples profils utilisateurs (personas). Ainsi que pour la partie collaboration/gestion de projets, symbolisée par les jonctions « efficaces » entre Jira Software et Confluence. Mais pas de sécurité applicative native chez Atlassian, qui s'appuie sur des ▶▶▶

WE FACTORY&co

Agence de communication & marketing BtoB

« Notre spécificité d'agence de groupe média nous permet d'identifier, comprendre et activer les audiences. »

Et c'est cette expertise que nous mettons à votre disposition !

hello@we-factoryandco.fr we-factoryandco.fr 06 46 76 29 41

TOP 10 SUR L'AXE « EXÉCUTION »

❶ GitLab

❷ Microsoft

❸ Atlassian

❹ Red Hat

❺ JFrog

❻ VMware

❼ CloudBees

❽ CircleCI

❾ Harness

❿ JetBrains

▶▶▶ partenaires tels que Snyk, Sonatype et Synopsys (tous trois classés au quadrant de l'AST). Gartner le fait remarquer, tout comme il souligne le faible niveau d'adoption des fonctionnalités CI/CD (Bitbucket Pipelines en version Cloud et Bamboo Data Center on-prem). Point de vigilance également concernant l'édition serveur, dont la fin de vie est imminente (février 2024)... et les questions de coûts qui pourraient se poser lors du passage aux éditions Cloud et data center.

GITLAB ET SON MODÈLE OPEN CORE

Au contraire d'Atlassian, GitLab se distingue sur les capacités de sécurité natives, de la génération de SBOM (CycloneDX) au contrôle des commits aligné sur le framework SLSA. Bons points également sur la parité SaaS/on-prem et l'ouverture de la plateforme, qui fonctionne sur un modèle open core. Par opposition à Atlassian, GitLab n'a pas droit à une bonne appréciation sur la partie collaboration/gestion de connaissances. En point d'orgue, l'expérience d'édition sur GitLab Wikis, « limitée » pour les non-développeurs. Gartner regrette aussi le manque de flexibilité sur les licences (impossibilité d'en associer plusieurs à une instance ou à un namespace), et le support limité des cas d'usage touchant à la gestion d'environnements (création à la demande, visibilité sur les coûts...).

75 %
des entreprises utiliseront ces plateformes en 2030, selon Gartner.

GITHUB ET AZURE DEVOPS : GARE À LA CONFUSION CHEZ MICROSOFT

Microsoft a deux produits à son catalogue : GitHub et Azure DevOps, mutuellement intégrés à plusieurs niveaux et contractualisables en une licence.

Cet ensemble a pour lui sa communauté d'utilisateurs (plus de 100 millions de développeurs sur GitHub ; popularité de VS Code)... et les capacités d'innovation qui en découlent. Il a aussi l'IA Copilot, qui suscite un « grand intérêt » selon Gartner.

Bon point également pour Codespaces (environnements de développement Cloud avec compute configurable).

Mais deux produits, c'est un risque de doublons... que Gartner ne manque pas de pointer, en plus des écarts fonctionnels, y compris entre les versions Cloud et on-prem. Autres remarques : les possibilités limitées en matière de localisation des données sur GitHub Enterprise Cloud et l'absence, sur GitHub dans son ensemble, de support natif des métriques de performances (fréquence de déploiement, délai d'exécution, temps de restauration...). ■ *Par Clément Bohic*

*25 % des entreprises utilisent une telle plateforme en 2023, d'après Gartner, qui envisage que ce taux sera de 75 % en 2027.

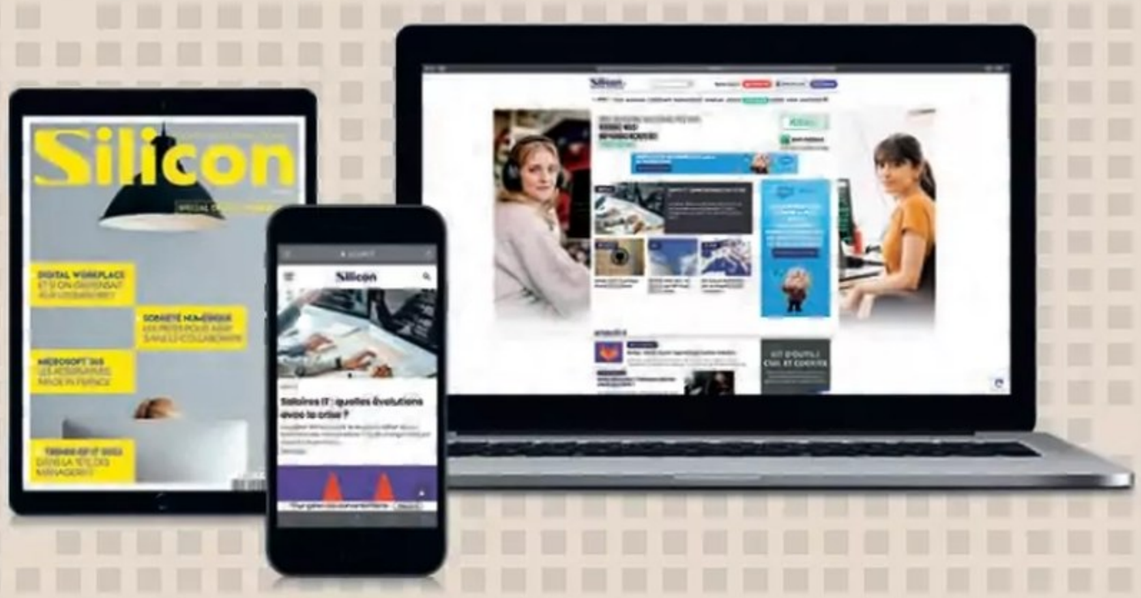
ABONNEZ VOUS !

INSIGHTS FOR IT PROFESSIONALS

Silicon

La solution d'information qui comprend :

- Le magazine en version digitale sur PC, tablette et smartphone
- Le magazine en version papier
- La newsletter quotidienne
- Les événements de la communauté
- L'accès aux contenus exclusifs sur **Silicon**.fr



boutique.editialis.fr/marketing-commercial/silicon

BULLETIN D'ABONNEMENT

OUI, je m'abonne à Silicon pour **1 an au prix de 120 €**

Silicon

À remplir et retourner à :
ÉDITIALIS Service Abonnements
98, rue du Château
CS 10200
92645 Boulogne-Billancourt Cedex
Tél. : 01 46 99 99 77

Abonnement Dom-Tom et étranger : retrouvez toutes les informations sur silicon.fr

❑ Mme ❑ M.

Nom : .....

Prénom : .....

Fonction : .....

Société : .....

Adresse : .....

.....

Code Postal : |_|_|_|_|_|

Ville : .....

Pays : .....

Tél. : .....

E-mail (indispensable pour recevoir vos codes d'accès aux archives et vos newsletters)

Je joins mon règlement par :

❑ Chèque bancaire ou postal à l'ordre d'ÉDITIALIS

❑ Carte bancaire n° :

|_|_|_|_| |_|_|_|_| |_|_|_|_| |_|_|_|_|

Date d'expiration : |_|_|/|_|_|

SIGNATURE

❑ Je souhaite recevoir une facture acquittée
Si vos coordonnées de facturation sont différentes de celles de livraison ci-dessous, merci de nous le préciser

LastPass •••|

Il existe une meilleure façon de gérer les mots de passe dans votre organisation

Renforcez dès maintenant la sécurité des identifiants de vos équipes

Retrouvez-nous aux Assises - 11/14 Octobre - Stand 248