N°234 – Mars 2025

www.linformaticien.com

L'INFORMATICIEN

Cloud
Sécuriser les LLM

DevOps
Du neuf dans Gitlab

RH
Les Freelances

DAF
Les moteurs du changement

Logiciel
Dynatrace : observer pour mieux sécuriser

L 14614 - 234 - F: 8,50 € - RD

Omada
by tp-link

2024
PALMARÈS
L'INFORMATICIEN

Management unifié et sécurisé des réseaux **SD-WAN, SD-LAN** et de la **vidéosurveillance**

Solution MSP complète et évolutive

Réseau + **Sécurité** + **Vidéosurveillance** + **Services IoT**

Scannez ici

www.tp-link.com/fr

L'INFORMATICIEN www.linformaticien.com

RÉDACTION

88 boulevard de la Villette, 75019 Paris, France.
Tél. : +33 (0)1 74 70 16 30 — *contact@linformaticien.com*

RÉDACTION : Bertrand Garé (rédacteur en chef) et Victor Miget (rédacteur en chef adjoint)
avec : Oscar Barthe, Olivier Bouzereau, Patrick Brebion, Christine Calais, Jérôme Cartegini, Michel Chotard, François Cointe, Alain Clapaud, Guillaume Renouard et Thierry Thaureaux

SECRÉTAIRE DE RÉDACTION : Amélie Ermenault Martin

MAQUETTE ET RÉALISATION : Franck Soulier (chef de studio)

PUBLICITÉ
Antoine Foulon — *afoulon@linformaticien.com*

VENTE AU NUMÉRO

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

ABONNEMENTS

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

Toutes les offres :
www.linformaticien.com/abonnement

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

L'Informaticien, service abonnements,
88 boulevard de la Villette, 75019 Paris, France.
ou à abonnements@linformaticien.com

IMPRESSION

Imprimé en France par Imprimerie Chirat (42)
Dépôt légal : 1er trimestre 2025

L'INFORMATICIEN est publié par PC PRESSE, S. A. S.
au capital de 130 000 euros.
Siège social : 88 boulevard de la Villette, 75019 Paris, France.

ISSN 1637-5491

Une publication PCpresse,

FICADE

PRÉSIDENT, DIRECTEUR DE LA PUBLICATION :
Gaël Chervet

La troisième vague de transformation des DAF

Ce mois-ci, le dossier de notre magazine observe comment les directions financières et comptables des entreprises connaissent une nouvelle vague de transformation avec l'automatisation et l'intelligence artificielle. Elle a pour but d'automatiser les tâches manuelles consommatrices de temps pour rendre plus rapidement les chiffres de l'entreprise, pour décharger les équipes et les rediriger vers les taches d'analyse et de planification. Cela induit que les DAF passent d'un rôle d'observateur de la vie de l'entreprise à un rôle de guide et d'aide pour les métiers, afin que l'entreprise prenne le bon chemin en s'appuyant sur les données. Eh oui, aujourd'hui les directions financières ne sont pas là seulement pour fournir des bilans. Elles doivent insuffler la stratégie de l'entreprise grâce à une analyse fine du contexte et du marché.

Toujours dans cette tendance, ce numéro fait aussi une large part à l'intelligence artificielle avec pas moins de trois articles consacrés à différents angles de son usage, que ce soit dans les réseaux, la supervision des services IT ou, tout simplement, de sa régulation pour éviter des dérives de plus en plus souvent notées lors des entraînements des modèles.

Vous retrouverez bien sûr tous vos rendez-vous habituels traitant de l'actualité du mois dans notre industrie.
En attendant, l'Informaticien se prépare pour ses prochains événements comme le Top Tech. Il sera très bientôt possible de déposer ses dossiers, que vous soyez entreprises ou ESN, n'hésitez pas à montrer vos projets réussis ! □

Bertrand Garé
Rédacteur en Chef

VERTIV™

keep it humming™

Solution complète pour la révolution de l'IA

Alimentez et refroidissez l'IA de vos clients grâce à une solution complète unique.

L'IA est là et elle s'accompagne d'une demande d'alimentation et de refroidissement inédite. Dénouez les complexités grâce à Vertiv™ 360AI, des solutions complètes pour alimenter et refroidir de manière transparente les charges de travail d'IA de vos clients.

En savoir plus :
vertiv.com/ai-hub-fr

2024 PALMARÈS L'INFORMATICIEN

Catégorie
Hardware Infrastructures Critiques Data Center

P 15
DOSSIER
DAF : Les moteurs du changement

P 43
CLOUD
Sécuriser les LLM

P 67
INFOCR
Une IA au sommet

DOSSIER ..... **P 15**
DAF : Les moteurs du changement

BIZ'IT ..... **P 8**

BIZ'IT PARTENARIAT ..... **P 12**

HARDWARE ..... **P 22**
AMD
NetApp
Hathor
Synology

ESN ..... **P 28**
NTT Data
FPT

TACTIC P 31
Un Stargate à l'Européenne

RÉSEAU ..... **P 34**
TP-Link
ML Aiops

LOGICIEL ..... **P 38**
IA Act
Dynatrace
Workday
Oracle
Memority

CLOUD ..... **P 43**
Sécuriser les LLM
Rocket Software
Cloudflare

RETEX ..... **P 47**
Oracle BNP
Thales

BONNES FEUILLES ..... **P 51**
Power BI : en images

INNOVATION ..... **P 55**
Pure Storage
IA Marseille

DEVOPS ..... **P 58**
Gitlab

ÉTUDE ..... **P 62**
Camunda

RH/FORMATION ..... **P 64**
Freelancers

INFOCR ..... **P 67**

ABONNEMENTS ..... **P 76**

Une plateforme unifiée de sécurité et d'observabilité pour une résilience inégalée.

De nombreuses organisations parmi les plus grandes et complexes au monde s'appuient sur Splunk pour contribuer à assurer la sécurité et la fiabilité de leurs systèmes numériques. Découvrez notre plateforme unifiée de sécurité et d'observabilité sur splunk.com/fr_fr

splunk>
a CISCO company

MODERNISATION À LA DIRECTION FINANCIÈRE

ON CHANGE LES ROUES POUR MIEUX PRENDRE LE VIRAGE DE L'IA...

ON MET EN PLACE LE SUPER POT CATALYTIQUE RSE COMPATIBLE AUX NORMES EUROPÉENNES ESRS DE LA DIRECTIVE CSRD.

ON INSTALLE LE NOUVEAU CAPTEUR DE FACTURES DÉMATÉRIALISÉES À HAUTE CAPACITÉ ANALYTIQUE POUR L'ALLONGEMENT OPTIMISÉ DES DÉLAIS DE PAIEMENT.

TRANSFORMER LES LOGICIELS DE COMPTABILITÉ-FINANCE, C'EST COMME MODERNISER UNE VOITURE PENDANT QU'ELLE ROULE : C'EST COMPLEXE !

SURTOUT QU'À MOINS DE LA TRANSFORMER EN AVION, ÇA NE NOUS EMPÊCHERA PAS D'ALLER DANS LE MUR...

ET ON POSE UNE BLOCKCHAIN SUR LES PNEUS NEIGE ET BROUILLARD.

SAISI-ERREUR

RETOUR À L'ENVOYEUR

IFRS-S1

IFRS-S2

GPT

COMPTABILITÉ FINANCE

RÉCLAMATION FACTURE IMPAYÉE

T.COINTE

FOCUS

Le **vieux continent** n'a pas dit son dernier mot dans **la course à l'IA**

Pour assurer leur indépendance technologique dans le domaine de l'IA, la France et l'Union européenne doivent s'en donner les moyens. Elles ont respectivement annoncé 109 milliards d'euros et 200 milliards d'euros, majoritairement alloués aux infrastructures. Mais derrière l'effet d'annonce, que cachent ces montants records ?

La veille du Sommet pour l'action sur l'IA, Emmanuel Macron est revenu, au JT de 20h de TF1, sur ce qu'il considère comme *« une révolution technologique et scientifique comme on en a peu connue »*, un « moment d'opportunité » dont la France et ses partenaires européens doivent se saisir. L'Hexagone *« est la cinquième puissance en intelligence artificielle [...] nous avons des atouts formidables »*, a ajouté le président de la République, avant d'admettre que *« nous sommes tous en retard par rapport aux États-Unis et à la Chine »*.

Une grande majorité d'investissements privés

Pour tenter de combler ce retard, le président a annoncé un investissement de 109 milliards d'euros pour l'IA. Une enveloppe que le président de la République a comparée (à l'échelle française) au programme Stargate des États-Unis, qui prévoit d'injecter 500 milliards de dollars dans le secteur.

Ces 109 milliards d'euros regroupent essentiellement des investissements privés et étrangers, provenant d'entreprises françaises et de fonds d'investissement. La première pierre à l'édifice correspond à un investissement de 30 à 50 milliards d'euros pour la construction d'un datacenter, avec le concours de MGX, un fonds d'investissement d'Abou Dabi, également impliqué dans Stargate. Le fonds canadien Brookfield a également annoncé qu'il investirait 20 milliards d'euros en France d'ici 2030, notamment pour la construction de datacenters à Cambrai (Nord). Pour convaincre d'éventuels partenaires, le gouvernement a d'ores et déjà annoncé que la France pouvait mettre à disposition 35 sites prêts à l'emploi, avec fourniture d'énergie, pour l'installation de capacités de calcul.

La banque publique d'investissement Bpifrance a, quant à elle, annoncé un investissement de 10 milliards d'euros d'ici 2029. La somme sera fléchée vers l'accompagnement en fonds propres de startups spécialisées en IA, les infrastructures et conception de puces, à des fonds français et internationaux, au développement de modèles de fondation et des applications d'IA, ainsi qu'à la création de nouveaux fonds dédiés à l'IA.

200 milliards pour l'Europe

Dans la foulée des annonces françaises, la présidente de la Commission européenne, Ursula von der Leyen, a annoncé le lancement de l'initiative InvestAI, un partenariat public-privé qui doit mobiliser 200 milliards d'euros d'investissements, dont 150 milliards d'euros provenant des grands groupes réunis au sein du EU AI Champions, et 50 milliards d'euros de l'initiative InvestAI.

Cette somme comprend un nouveau fonds européen de 20 milliards d'euros pour la construction de giga-usines d'IA destinées à fournir la puissance de calcul nécessaire à l'entraînement de LLM. Selon l'association France Digital, interrogée par nos confrères de Maddyness, les 50 milliards d'euros d'InvestAI regroupent des projets existants issus des programmes Europe numérique, Horizon Europe et InvestEU. Concernant les investissements du EU AI Champions, s'agit-il de nouveaux fonds annoncés, ou bien cela regroupe-t-il des programmes déjà connus ? Une autre question se pose : les investissements du secteur privé profiteront-ils exclusivement aux entreprises qui en sont à l'initiative, ou dans quelle mesure ces fonds bénéficieront-ils à d'autres acteurs, comme des startups qui pourraient utiliser la puissance de calcul et de stockage qui sera déployée ? Contactée par L'Informaticien, la Commission européenne n'a pas donné suite.

« J'entends trop souvent dire que l'Europe est à la traîne, que les États-Unis et la Chine auraient pris les devants. Je ne suis pas d'accord. Car la course à l'IA est loin d'être terminée. En réalité, nous n'en sommes qu'aux prémices », a déclaré, confiante, la cheffe de l'exécutif européen, Ursula von der Leyen.

Mistral va ouvrir un premier centre de données en France

La startup française spécialisée dans l'IA générative, Mistral AI, a fait une annonce majeure lors du Sommet pour l'Action sur l'intelligence artificielle, qui s'est tenu début février au Grand Palais, à Paris. *« Nous annonçons la création de notre premier centre de données en France [...] Pour nous, c'est un choix stratégique, visant à maîtriser l'ensemble de la chaîne de valeur »*, a révélé le PDG de Mistral, Arthur Mensch, au JT de 20h de TF1. Un projet à plusieurs milliards d'euros.

60 MW de capacité

L'infrastructure sera construite en Essonne et sera dédiée à l'IA générative, utilisée pour supporter les calculs des modèles de l'entreprise. *« Nous avons choisi la France pour son efficacité énergétique, la qualité de son mix énergétique en matière d'émissions carbone, mais aussi pour la compétence de ses techniciens et la qualité de ses déploiements en centres de données. »*
On ignore encore combien de GPU seront déployés pour répondre aux besoins de l'entreprise. C'est le centre de calcul haute densité modulaire Éclairion, filiale du groupe HPC, qui hébergera le cluster de Mistral AI. En parallèle, l'entreprise prévoit de construire un second centre dédié à l'hébergement en colocation de calculateurs haute densité, d'une capacité de 120 MW, dans la Sarthe.

Annonces en cascade

L'actualité a été plutôt dense pour la startup en ce début d'année. Mistral a signé un partenariat pluriannuel pour nourrir son outil Chat avec l'ensemble des dépêches de l'agence. Elle a également lancé Small 3, un modèle de 24 milliards de paramètres optimisé pour la latence, que l'entreprise présente comme *« compétitif avec des modèles plus grands tels que Llama 3.3 70B ou Qwen 32B, et constituant une excellente alternative open source aux modèles propriétaires opaques comme GPT-4o-mini »*.
Mistral a également présenté un nouveau modèle, Mistral Saba, entraîné sur des données spécifiques pour mieux retranscrire les subtilités linguistiques des langues arabes et indiennes, et répondre aux besoins propres à ces deux aires géographiques et culturelles.

Des défis à relever

Tout n'est cependant pas rose pour le fleuron français. L'entreprise fait l'objet d'une plainte déposée auprès de la Commission nationale de l'informatique et des libertés (Cnil) par Maître Jérémy Roche, un avocat spécialisé en droit de la protection des données personnelles. Il accuse Mistral AI de collecter illégalement les données de ses utilisateurs via son chatbot gratuit LeChat, sans leur offrir la possibilité de s'y opposer.
L'entreprise dément ces accusations, affirmant qu'elle *« a toujours permis à ses utilisateurs de refuser l'utilisation des informations contenues dans les requêtes adressées au Chat »*, nous avait assuré un porte-parole.

Bpifrance va investir 10 milliards d'euros dans l'IA

Lors du Sommet pour l'Action sur l'intelligence artificielle, le message était clair, la France veut se donner les moyens pour essayer de rivaliser avec les géants américains et chinois dans le domaine de l'IA. À l'instar des États-Unis, avec le projet Stargate et ses 500 milliards de dollars, le pays a annoncé d'importants investissements pour soutenir son écosystème.
Le 7 février 2024, la banque publique d'investissement, Bpifrance, a annoncé un investissement de 10 milliards d'euros d'ici 2029. Une partie de l'enveloppe sera fléchée vers l'accompagnement en fonds propres de startups spécialisées en IA et de sociétés rentables et en croissance, y compris dans les segments des infrastructures et des puces, via des participations à des levées de fonds.

Une montée en puissance pour Bpifrance

Bpifrance va aussi investir dans des fonds français et internationaux, ainsi que dans des modèles de fondation et des applications d'IA, de la phase d'amorçage jusqu'au capital croissance. La banque publique affirme qu'elle soutiendra également la création de nouveaux fonds dédiés à l'IA et accompagnera les sociétés de gestion dans l'intégration des outils d'intelligence artificielle.

Depuis 2015, Bpifrance a investi plus d'un milliard d'euros dans des startups d'IA, dont la pépite française Mistral AI ou encore Poolside en 2023. Cette nouvelle enveloppe marque donc une montée en puissance significative.

RACHATS

Seagate rachète Intevac pour 119 millions de dollars

Le spécialiste du stockage de données Seagate a annoncé le rachat d'Intevac, une entreprise californienne spécialisée dans les systèmes de traitement de films minces, utilisés notamment dans la fabrication de disques durs.
Intevac s'est récemment recentrée sur son activité HAMR (Heat-Assisted Magnetic Recording), une technologie qui accroît la densité des données et améliore ainsi la capacité de stockage. Un domaine dans lequel Seagate est également actif, ayant récemment lancé un disque dur de 32 To en décembre 2024, reposant sur cette technologie.

CyberArk s'offre Zilla Security pour 175 millions de dollars

Le spécialiste de la sécurité des identités va intégrer les capacités d'administration des identités dopées à l'IA de Zilla Security à sa propre plateforme.
Concrètement, cette acquisition accélérera le processus de conformité et d'approvisionnement des identités et cartographiera les risques associés. Elle permettra d'appliquer le bon niveau de contrôle des privilèges dans la gestion des droits, des sessions, des identifiants et de l'authentification, tout en automatisant le cycle de vie des politiques de gouvernance et de conformité. Les capacités de Zilla sont disponibles dans deux offres autonomes : Zilla Comply et Zilla Provisioning.

Broadcom et TSMC prêts à se partager Intel ?

En difficulté, Intel suscite l'intérêt de Broadcom et TSMC. Selon des informations du Wall Street Journal — à prendre avec précaution — le géant des semi-conducteurs pourrait voir ses actifs divisés entre les deux mastodontes.
Broadcom souhaiterait récupérer les activités de design des puces, tandis que TSMC s'intéresserait aux usines de production. L'opération, encore à un stade embryonnaire, pourrait cependant aboutir.
Selon les sources du WSJ, Broadcom, connu pour ses acquisitions en série (Symantec, VMware, CA, Brocade), aurait déjà commencé à travailler sur une offre. Toutefois, celle-ci dépendrait de la possibilité de trouver un partenaire pour récupérer l'activité fonderie... et c'est là qu'interviendrait TSMC. L'administration Trump aurait d'ailleurs demandé au géant taïwanais d'étudier cette option.

Tenable va racheter Vulcan Cyber

Le spécialiste de la gestion de l'exposition Tenable a signé un accord définitif pour acquérir son concurrent Vulcan Cyber pour 150 millions de dollars et intégrer ses capacités à sa plateforme Tenable One. La transaction devrait être finalisée au premier trimestre 2025, sous réserve des conditions de clôture habituelles, notamment l'accord des autorités réglementaires.
Tenable ambitionne de défragmenter le secteur de la cybersécurité, actuellement composé d'une myriade d'outils disparates, ce qui complique la gestion des risques pour les entreprises.
Grâce à cette acquisition, Tenable pourra centraliser les données extraites de plus de 100 produits de sécurité couvrant l'évaluation des vulnérabilités, la sécurité des terminaux, la sécurité du cloud, la sécurité applicative et le renseignement sur les menaces. Selon l'entreprise, cet ensemble de données unifié servira de base à une IA avancée dédiée à la gestion des expositions, permettant aux entreprises de mieux se focaliser sur les vulnérabilités critiques.

Alice & Bob réalise un tour de série B de 100 M€

Mené par Future French Champions (FFC), AVP (Axa Venture Partners) et Bpifrance, ce financement doit permettre à Alice & Bob d'accélérer ses efforts pour construire d'ici 2030 le premier ordinateur quantique véritablement utile.

Le cœur de son innovation réside dans ses qubits de chat, capables de supprimer intrinsèquement les erreurs de type « bit-flip », l'un des deux types d'erreurs majeures affectant les ordinateurs quantiques. Cette avancée est cruciale pour développer des architectures plus efficaces d'ordinateurs quantiques tolérants aux erreurs (FTQCs), utilisables pour des applications concrètes.

Alice & Bob, pionnière de cette technologie depuis sa création en 2020, utilisera ces fonds pour améliorer les performances de son système, perfectionner la correction d'erreurs et développer son premier qubit logique corrigé d'erreurs. L'entreprise finance également la construction d'un laboratoire et d'une installation de production, ainsi que le doublement de son équipe, qui avait déjà grandi en 2024.

Riot lève 30 millions d'euros pour sa plateforme de cybersécurité des employés

Le Français Riot a bouclé un tour de table en série B de 30 millions de dollars, mené par Left Lane Capital.

Riot développe une solution de suivi en temps réel de la cybersécurité des employés. Son outil détecte les vulnérabilités individuelles (mots de passe faibles, partage de fichiers à risque…) et propose un accompagnement personnalisé avec un « coach cyber ». Avec ces fonds, la startup prévoit de soutenir sa croissance à trois chiffres, poursuivre son expansion internationale, doubler ses effectifs et protéger 10 millions d'employés d'ici 2027. Riot accompagne déjà 1 500 entreprises, dont Mistral AI, Ledger et L'Occitane.

ElevenLabs boucle une série C à 250 M$ pour son IA vocale

Basée à New York, ElevenLabs, spécialisée dans le clonage de voix et le doublage dopés à l'IA, a levé 250 millions de dollars en série C, seulement un an après une série B de 80 millions. Cette levée de fonds, menée par Iconiq Growth et Andreessen Horowitz, valorise l'entreprise entre 3 et 3,3 milliards de dollars, selon TechCrunch.

Fondée en 2022 par Mati Staniszewski (ex-Palantir) et Piotr Dabkowski (ex-Google), ElevenLabs propose une API permettant de générer des voix, des effets sonores et de la parole dans 32 langues. Ses technologies sont utilisées dans de nombreux secteurs : livres audio, presse, jeux vidéo, cinéma…

Toutefois, la startup fait face à des controverses liées à la sécurité. En février 2023, un journaliste de Vice avait utilisé son outil pour cloner sa propre voix et accéder à son compte bancaire, soulevant des inquiétudes sur les risques d'usurpation d'identité.

Apptronik lève 350 millions de dollars et veut déployer son robot en entreprise

L'entreprise américaine Apptronik a annoncé, le 13 février 2025, une levée de 350 millions de dollars en Série A pour industrialiser la production de ses robots humanoïdes boostés à l'IA.

L'opération, co-dirigée par B Capital et Capital Factory, avec la participation de Google, vise à accélérer le déploiement d'Apollo, son robot humanoïde, et à développer de nouvelles itérations. L'entreprise compte également renforcer ses effectifs, aujourd'hui composés de plus de 150 employés.

Apollo a été conçu pour interagir avec les humains et être déployé en entreprise dans des secteurs variés : logistique, fabrication, et à terme, santé et aide aux personnes âgées.

Fondée en 2016, Apptronik précise que cette levée de fonds lui permettra de répondre à une demande croissante et de satisfaire des commandes dans des secteurs tels que l'automobile, la fabrication électronique, la logistique tierce, l'embouteillage et l'emballage.

Nokia prolonge son partenariat avec **Orange**

Dans le cadre de cet accord, Nokia fournira des équipements issus de son portefeuille 5G AirScale conforme aux normes O-RAN. Cela comprend les solutions de bande de base AirScale de nouvelle génération, les radios Habrok légères et à haut rendement Massive Mimo, ainsi que le portefeuille Pandion de têtes radio distantes multibandes FDD de Nokia pour couvrir tous les cas d'utilisation et les scénarios de déploiement. Ces radios sont toutes alimentées par la technologie ReefShark System-on-Chip à haut rendement énergétique et se combinent pour offrir une couverture et une capacité supérieures. Nokia fournira également sa solution de gestion de réseau radio alimentée par l'IA, MantaRay NM, qui prend en charge toutes les technologies de base radio et mobiles. Pour sa part, Orange va tester les solutions 5G Cloud RAN de Nokia.

Cisco s'associe à **Mistral** pour améliorer l'expérience client

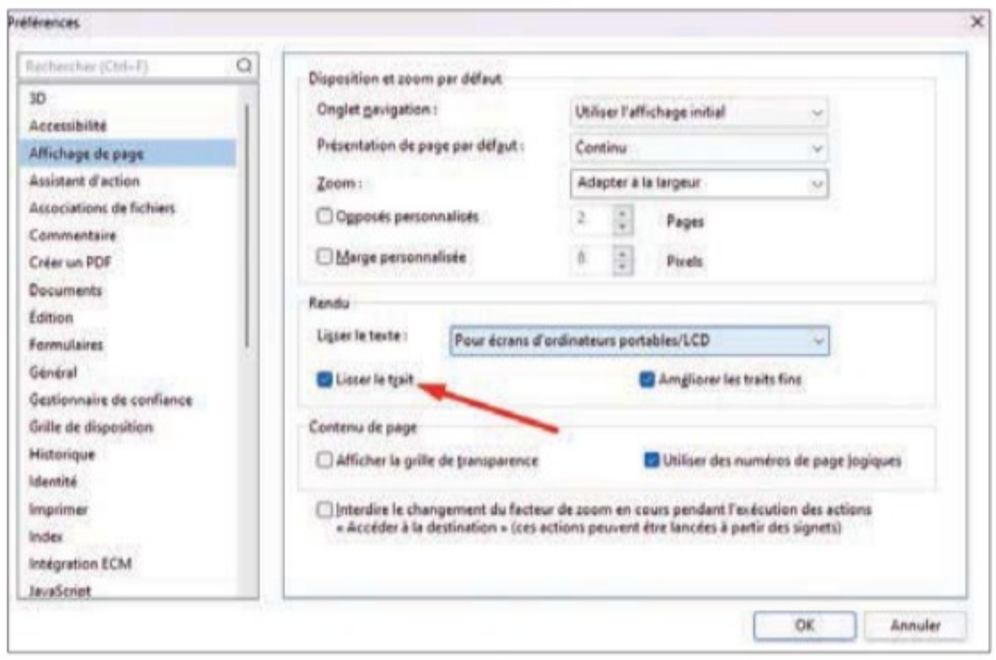
L'IA Renewal Agent automatise et optimise le processus de renouvellement en agrégeant plus de 50 sources de données pour créer des propositions adaptées aux besoins des clients. Il fournit également une analyse des sentiments en temps réel, des recommandations résumées, une automatisation intelligente et une personnalisation, liées aux résultats des clients et aux indicateurs clés de performance. Conçue à l'aide d'un modèle d'IA personnalisé, la solution fonctionne sur site, garantissant la sécurité, la confidentialité et la conformité des données, tout en permettant l'optimisation des performances et des coûts. Il est estimé que l'IA Renewal Agent pourrait réduire jusqu'à 20 % le temps consacré à l'élaboration d'une proposition de renouvellement et à la préparation d'un engagement client. Un chiffre qui devrait augmenter à mesure que l'agent d'IA s'améliore en fonction de l'utilisation, et que davantage de flux de travail sont automatisés. Le nouvel agent est la dernière innovation en matière d'IA pour la branche Customer Experience (CX) de Cisco. Il est prévu de développer d'autres agents du même type dans le futur.

Amadeus étend son partenariat avec **Microsoft**

À ce jour, avec ce partenariat, Amadeus a migré plus de la moitié de ses applications dans le Cloud public. La société va continuer à travailler avec Microsoft pour développer de nouveaux logiciels innovants pour les voyages d'affaires, les services aéroportuaires et l'hôtellerie.
Cytric Easy, un outil de réservation et de gestion des dépenses en ligne pour les déplacements professionnels, intégré à Microsoft Teams, sera encore amélioré grâce à la performance de l'IA générative pour créer une nouvelle expérience conversationnelle. L'introduction d'Amadeus Virtual Airport Operations Centre permet aux acteurs aéroportuaires, tels que les compagnies aériennes, les aéroports, les services de contrôle aux frontières et les prestataires de services, de coopérer au sein d'un centre d'opérations aéroportuaires entièrement numérisé. Avec Amadeus Advisor, Amadeus vise à simplifier la capacité d'un hôtelier à rechercher et à comprendre les données de veille stratégique, en utilisant la fonctionnalité de chabots pour aider la prise de décision fondée sur des données.
Par ailleurs, Amadeus utilise largement CoPilot avec 10 000 licences déployées dans l'entreprise, permettant aux employés de se concentrer sur la créativité et la productivité, avec une adoption de 94 % et un gain de temps moyen auto-déclaré par personne de plus d'une heure et demi par semaine.

FoxIT disponible sur la marketplace **Pax8**

L'éditeur de solutions de documents PDF et de signature électronique propose maintenant ses quatre produits sur la place de marché Pax8. FoxIT Editor et Editor + sont des logiciels pour créer, éditer et gérer des documents PDF. Ils sont dotés de fonctions d'intelligence artificielle pour résumer des documents complexes, d'améliorer l'écriture et de traduire des documents dans plus de 30 langues. eSign for Business est la solution d'e-signature sécurisée et transparente qui permet aux utilisateurs de s'affranchir des solutions d'eSign à l'emporte-pièce, et aux entreprises de faire signer des documents, d'encaisser des paiements et d'assurer la fluidité des flux de travail. AI Assistant améliore la productivité et rationalise les flux de documents, offrant à ses utilisateurs la possibilité de résumer des documents en quelques secondes, de réécrire rapidement des documents avec clarté et précision, et de discuter naturellement pour prendre des décisions plus éclairées, plus rapidement.



Une vue de l'écran de configuration dans FoxIT, support module de FoxIT Editor.

Zelros s'associe à **IBM** pour l'utilisation de watsonx

En intégrant watsonx, Zelros met à disposition de ses utilisateurs des modèles de langage de nouvelle génération, tels que Mistral, Llama et Granite, directement activables depuis son studio. Ces modèles permettent de répondre à divers cas d'usage au sein des équipes marketing, des agents et conseillers, ainsi que des départements IT et data, tout en s'adaptant à l'environnement existant des banques et compagnies d'assurances. Par cette intégration, Zelros améliore la découverte des besoins (magic questions), le conseil assurantiel et bancaire personnalisé (magic recommendations), fournit des réponses précises et instantanées (magic answers) et automatise les processus clés (magic automations).

Databricks et **SAP,** ensemble pour accélérer sur la Business AI

SAP Business Data Cloud unifie l'ensemble des données SAP et des données tierces au sein des entreprises, fournissant la base de données fiable dont les organisations ont besoin pour prendre des décisions plus efficaces, et favoriser le développement d'une intelligence artificielle de confiance. Cette solution harmonise les données des applications les plus critiques des organisations, grâce à l'ingénierie des données et aux capacités d'analyse métier, ouvrant ainsi la voie à l'innovation et à de nouvelles perspectives. La nouvelle solution intègre nativement les technologies de Databricks, notamment pour l'ingénierie des données, l'apprentissage automatique et les charges de travail liées à l'intelligence artificielle.
La plateforme fournit des produits de données SAP entièrement gérés, couvrant l'ensemble des processus métier : des données financières, des dépenses et de la logistique dans SAP S/4HANA et SAP Ariba, aux données de formation et de gestion des talents dans SAP SuccessFactors. Ces produits de données conservent leur contexte métier et leur sémantique d'origine, garantissant un accès immédiat à des données.
SAP Business Data Cloud proposera également de nouvelles fonctionnalités baptisées « insight apps ». Ces applications exploitent des produits de données et des modèles d'IA connectés à des données en temps réel, pour fournir des analyses avancées et optimiser la planification dans toutes les fonctions de l'entreprise, notamment l'analytique métier, la finance et les ressources humaines. Le logiciel vise aussi à améliorer la façon dont Joule, le copilote basé sur l'IA générative de SAP, accélère les flux de travail transverses, et améliore la prise de décision grâce aux agents IA. Alimenté par les données business et par la solution SAP Knowledge Graph, qui propose un modèle de données accessible aux entreprises. Les agents Joule comprennent les processus de bout en bout et peuvent collaborer entre les fonctions pour résoudre des défis commerciaux complexes.

Une plateforme dédiée à Databricks

SAP Databricks réside dans sa capacité à permettre aux clients de combiner facilement leurs données SAP avec le reste de leurs données d'entreprise. Grâce au partage bidirectionnel des données via Delta Sharing entre leur environnement SAP Databricks et leur environnement Databricks natif (non-SAP), ils peuvent unifier toutes leurs données sans ingénierie complexe. L'ensemble du patrimoine de données est gouverné et sécurisé de manière cohérente avec Unity Catalog, permettant aux entreprises de construire sur une base fiable, et de mener des analyses exploratoires en data science et en SQL à grande échelle, avec une compréhension complète de la sémantique métier. De plus, les capacités de Mosaic AI permettent aux entreprises de développer facilement des applications IA spécifiques à leur domaine, entraînées sur leurs données SAP privées, pour créer des agents IA pour les fonctions les plus importantes de leur activité.
Le nouveau produit, SAP Databricks, est commercialisé par SAP dans le cadre de SAP Business Data Cloud, et sera disponible progressivement sur AWS, Azure et Google Cloud.

AGENDA

Nvidia GTC
17-20 mars 2025
Convention Center
San Jose, USA

Adobe Summit
18-20 mars 2025
The Venetian Convention and Expo Center,
Las Vegas USA

Qualtrics X4
18-20 mars 2025
Salt Palace Convention Center,
Salt Lake City USA

Digital Workplace
19-20 mars 2025
Porte de Versailles, Paris

Solutions RH
19-20 mars 2025
Porte de Versailles, Paris

I-Expo
19-20 mars 2025
Porte de Versailles
Pavillon 3, Paris

Documation
19-20 mars 2025
Porte de Versailles, Paris

All4Customers
19-20 mars 2025
Porte de Versailles
Pavillon 4, Paris

Big Date and AI World
9-10 Avril 2025
Recinto Montjuic, Barcelone, Espagne

TRIBUNE PARTENAIRE

Construire *l'avenir des réseaux unifiés et convergés* avec Omada SDN de TP-Link

Dans un contexte de transformation numérique accélérée, les entreprises ont besoin d'infrastructures capables de supporter sur les mêmes réseaux de plus en plus d'applications telles que la téléphonie IP, la visioconférence, la vidéosurveillance et bien d'autres applications critiques, tout en garantissant stabilité, performance et sécurité.

Face à la demande croissante pour des liens Internet plus rapides et l'explosion des applications toujours plus gourmandes en débit, il devient indispensable de déployer des réseaux optimisés qui assurent une gestion intelligente des flux et une connectivité ultra-performante, garantissant ainsi une expérience utilisateur fluide et résiliente.

La solution Omada by TP-Link offre de nombreux avantages pour construire des réseaux unifiés et convergents tels que :

▪ Une gestion centralisée pour plus d'agilité : les technologies SD-WAN et SD-LAN offrent des avantages considérables en améliorant la performance, la résilience et la gestion des flux réseau. Grâce à Omada SDN, l'administration centralisée facilite la convergence des applications, assurant une répartition intelligente des flux voix, vidéo et données pour une expérience utilisateur optimale.

▪ Des performances et une connectivité de pointe : conçue pour supporter des réseaux Multi-Gigabit et la connectivité de nouvelle génération avec WiFi 7, la plateforme garantit des vitesses de transmission ultra-rapides et une latence minimale. L'optimisation WiFi par IA ajuste dynamiquement les paramètres pour maintenir une qualité de connexion optimale, même en environnement haute densité.

▪ Une grande résilience et une continuité du service
La gestion avancée du Multi WAN et le Backup 4G/5G de votre lien fibre principal assurent une connectivité ininterrompue. En cas de défaillance de la connexion fibre, la solution bascule automatiquement vers une connexion de secours, garantissant ainsi la continuité des opérations.

▪ Une sécurité renforcée
Omada SDN intègre des mesures de cybersécurité robustes, notamment avec des fonctionnalités telles que IDS/IPS, DPI (Couche applicatifs), filtrage de contenu, etc. Mais aussi des connexions sécurisées avec des VPN en 1 clic qui permettent de créer des tunnels sécurisés pour protéger les données sensibles. Cette approche proactive sécurise l'ensemble du réseau contre les menaces et les intrusions.

▪ L'intégration de la sécurité et de la surveillance pour plus de valeur ajoutée
L'intégration de la vidéosurveillance pro directement dans Omada permet de centraliser le contrôle vidéo et de renforcer la sécurité globale de l'infrastructure, tout en optimisant la gestion des flux liés aux communications unifiées et collaboratives.

Omada SDN de TP-Link conjugue SD-WAN, SD-LAN, convergence des applications, optimisation Wifi par IA, Multi WAN, Backup 4G/5G, cybersécurité, VPN en 1 clic, réseaux Multi-Gigabit, WiFi 7, vidéosurveillance pro intégrée. Cette solution offre aux entreprises la flexibilité, la résilience et la sécurité indispensables pour réussir leur transformation numérique et construire l'avenir des réseaux convergents. □

DAF

Les moteurs du changement

La fonction financière dans les entreprises a entrepris sa mutation numérique depuis des années mais les nouvelles contraintes, qu'elles soient réglementaires ou économiques, demandent aujourd'hui à ce que cette transformation passe à une vitesse supérieure. L'automatisation, et principalement celle que peut procurer l'intelligence artificielle est au cœur de cette nouvelle étape pour la fonction, à qui il est demandé de devenir un vrai contributeur stratégique pour les métiers de l'entreprise, pour accéder au rôle demandé.

Les nouveaux **guides de l'entreprise**

Si les directions financières et comptables tenaient déjà un rôle central dans les entreprises, il leur est demandé maintenant de servir de guide pour conduire l'entreprise dans un contexte incertain et complexe. Cela passe par une direction financière modernisée en s'appuyant sur les données.

Dans une étude intitulée « Retour sur investissement », OneStream Software, a interrogé 2000 entreprises pour tenter de voir ce que serait une direction financière en 2035. 65 % des leaders d'entreprise pensent que leur rôle sera plus important à l'avenir. Les DAF (Directeur administratif et Financier) sont 75 % à constater que les attentes à leur égard se sont multipliées au cours des 3 à 5 dernières années. À mesure que cette pression s'intensifie, les directeurs financiers se doivent d'étoffer et renforcer leurs compétences déjà très variées pour rester stratégiques. Que ce soit les PDG ou les directeurs métiers de l'entreprise, ils sont respectivement 69 et 78 % à attendre du DAF qu'il soit un moteur ambitieux de la croissance de l'entreprise. Devant un cahier des charges de plus en plus imposant, les DAF sont 69 % à dire qu'ils ont du mal à piloter la stratégie et la croissance de l'organisation.

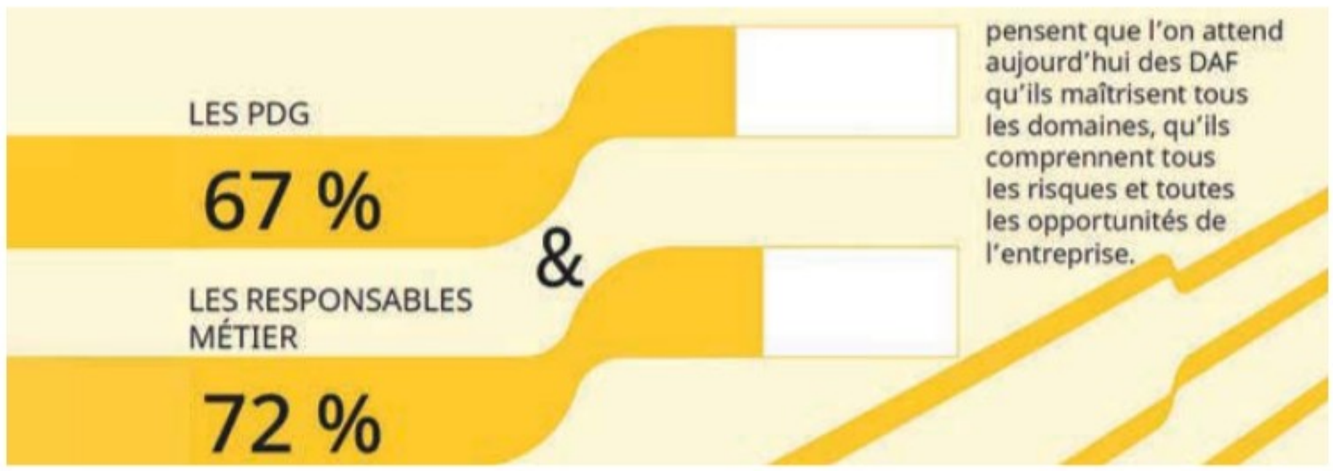
Une demande trop forte ?

67 % des leaders dans les entreprises attendent de leur DAF d'être les nouveaux *« Pic de la Mirandole »* de l'entreprise et souhaitent qu'ils maîtrisent tous les domaines, qu'ils comprennent tous les risques et toutes les opportunités de l'entreprise. Le chiffre se monte à 72 % pour les directeurs métiers.

Les clés de l'avenir

Selon l'étude, pour réussir en 2035, les DAF doivent supprimer les cloisonnements, investir dans la technologie et développer les compétences d'équipe. Les données unifiées joueront un rôle essentiel dans la transformation de l'équipe financière. A 74 % ils estiment que l'IA et l'automatisation auront complètement transformé les fonctions financières des organisations. Ce constat est vu comme un point essentiel. 68 % des DAF pensent que les organisations qui n'investissent pas dans la technologie, l'infrastructure et les compétences aujourd'hui ne survivront pas aux cinq prochaines années. 74 % affirment que les données unifiées et la prise de décision fondée sur les données sont aujourd'hui les facteurs déterminants de la réussite organisationnelle. Cela va amener la fonction à devoir se réinventer.

Pour les leaders d'entreprise, l'un des principaux moteurs de l'importance accrue du DAF sera la capacité de celui-ci à exploiter les technologies de pointe comme l'IA pour améliorer la prise de décision financière. Ils semblent cependant qu'ils sont prêts à relever les défis à venir. 72 % des DAF indiquent que ce sont eux qui jouent le rôle le plus important dans l'amélioration des performances de l'entreprise. D'ailleurs 67 % des PDG estiment que le succès ou l'échec d'une organisation repose sur son DAF. Les leaders d'entreprise apprécient de plus en plus la valeur d'un DAF stratégique, capable de donner un point de vue impartial reposant sur des données chiffrées. Ils aspirent à être guidés par un juge honnête, capable de trouver l'équilibre entre les besoins des différents départements et ceux de l'entreprise, et de les aider à identifier les sources de bénéfices. Concernant les compétences et les attributs les plus importants pour la réussite d'un DAF, les PDG continuent de privilégier les compétences essentielles en finances et en capital. De leur côté, les responsables métier attendent des responsables financiers qu'ils adoptent une vision plus large : 70 % pensent qu'il est maintenant plus important pour les DAF de comprendre l'organisation de façon holistique, plutôt que de maîtriser les aspects techniques des finances.



Des adaptations nécessaires

69 % des responsables métier affirment que le DAF doit collaborer étroitement avec d'autres leaders de l'entreprise pour réaliser pleinement les opportunités de croissance de l'organisation. Alors qu'historiquement, on n'attendait

PROPORTION DE LEADERS D'ENTREPRISE ET D'INVESTISSEURS PENSANT QU'EN 2035, LA TECHNOLOGIE ET L'IA...

pas des responsables financiers qu'ils soient des experts en communication. Ces compétences sont aujourd'hui essentielles pour réussir. Selon John Kinzer, membre du conseil d'administration de OneStream, *« L'abandon des anciens systèmes et l'adoption de l'automatisation seront essentiels à la modernisation de la fonction financière. Les DAF ont intérêt à identifier les tâches à faible valeur ajoutée qu'ils peuvent automatiser afin de libérer leurs équipes. Cela leur permettra de consacrer plus de temps à l'analyse stratégique et de se plonger dans d'autres domaines de l'entreprise. Les DAF les plus à l'écoute de leur organisation veillent à ce que les équipes financières forgent des partenariats étroits avec les dirigeants de l'ensemble de l'organisation, des opérations au marketing en passant par les ventes ».*

Des obstacles identifiés

Les DAF considèrent qu'une collaboration transversale limitée constitue un obstacle important à l'exercice efficace de leur fonction. Les silos limitent le flux d'informations entre les départements, ce qui produit des données fragmentées et incohérentes. Cette absence d'alignement ralentit la prise de décisions, nuit à l'innovation et limite la flexibilité. 72 % d'entre eux se plaignent des systèmes anciens et des limitations technologiques qui constituent un obstacle important à l'accomplissement efficace de leur mission. Les technologies anciennes sont rigides et difficiles à faire évoluer. Elles reposent souvent sur des processus manuels chronophages et sujets aux erreurs. Ainsi, les équipes doivent investir du temps et des ressources dans ces solutions inefficaces, au détriment de leurs initiatives stratégiques.

Le troisième frein à leur évolution tient en un manque de compétence sur le marché pour renforcer le département financier. Un nombre croissant de comptables publics agréés (CPA) approchent de la retraite et le nombre d'étudiants dans cette discipline diminue. Le vivier de professionnels diminue rapidement. Dans le même temps, de nombreuses équipes financières établies ne maîtrisent pas les outils et les technologies financières modernes, ce qui les empêche de mettre en œuvre et d'exploiter ces ressources de manière efficace.

John Kinzer, membre du conseil d'administration de OneStream.

« L'abandon des anciens systèmes et l'adoption de l'automatisation seront essentiels à la modernisation de la fonction financière. »

Le rôle primordial des données

Trois quarts des directeurs financiers (75 %) pensent que, d'ici 2035, les données seront l'actif le plus précieux de leur organisation. Pour devenir le moteur de la stratégie commerciale de leur entreprise, les départements financiers doivent passer de la réactivité à la proactivité : 76 % des DAF estiment qu'il est important que la fonction financière évolue pour piloter les prévisions et les initiatives de l'entreprise, au lieu de se contenter de tenir des registres traditionnels.

La gouvernance des données revêt une importance croissante pour garantir la qualité, la sécurité et la régularité des données au sein des organisations, tout en favorisant la confiance des investisseurs. Cependant, les départements financiers doivent gérer des volumes de données toujours croissants. Trois quarts des PDG (76 %) affirment que les DAF ont du mal à donner la priorité à la croissance de l'entreprise en raison d'un volume écrasant de données et d'informations. Pour surmonter ces obstacles, il est essentiel de disposer de systèmes de données unifiés, améliorés par l'IA et l'apprentissage automatique. 74 % des DAF estiment que les données unifiées et la prise de décision fondée sur les données s'imposent aujourd'hui comme les principaux moteurs de la réussite de l'organisation. Pour ce faire, il faut regrouper les données financières et opérationnelles afin de prendre des décisions éclairées en matière de stratégie, de planification et d'exécution des activités. □

B.G

Les **nouveaux outils** de la finance

Pour répondre à l'évolution de leur rôle dans les entreprises, les directions financières se dotent de nouveaux outils. Les anciens systèmes limitent par trop par leur rigidité la concentration des équipes financières sur les questions stratégiques et l'analyse car trop occupées par des tâches manuelles répétitives et sans réelle valeur.

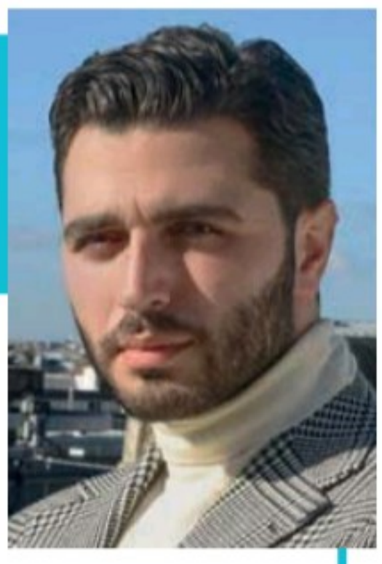
Pour Samuel Rouayrenc, vice-président pour la région Europe du Sud chez Blackline, *« un des enjeux aujourd'hui auxquels font face les départements finances, c'est l'accélération des besoins de la production des chiffres. Donc on a besoin de clôturer et de pouvoir reporter, que ce soit au marché ou en interne, de plus en plus rapidement »*.

La bataille contre le temps

C'est aussi dans cette idée de course contre le temps que s'est créé PayHawk. Valentin Gerbi, directeur France pour la Fintech Payhawk explique : *« C'était l'idée à la base de l'entreprise : redonner du temps aux directions financières et replacer les directions financières à la bonne place, c'est-à-dire ne pas être des bons exécutants de tâches réverbatives, mais être au cœur de la stratégie et du pilotage d'une entreprise »*. L'autre versant de cette course contre le temps est le temps réel et non le temps des batches. Valentin Gerbi ajoute : *« il y a un premier sujet qui est le temps réel. C'est-à-dire de ne plus avoir de décalage entre une dépense qui est effectuée, sa réconciliation et le moment où elle est en comptabilité. Pourquoi ? Parce qu'on a une vélocité dans les entreprises qui est de plus en plus importante et on a besoin de prendre des décisions stratégiques, non pas dans une semaine, mais maintenant. Et donc d'avoir les bons éléments pour prendre ces décisions stratégiques. Donc, le temps réel et la capacité, notamment, par exemple, si on est une entreprise qui a plusieurs entités juridiques et qui vont former un groupe, la capacité à avoir une visibilité en temps réel sur toutes les entités, toutes dépenses confondues et d'avoir cette synchronisation entre les dépenses et ce qui est dans l'ERP, qui est mon référentiel de données, puisque les CFO ne jurent plus que par leur ERP, c'est critique. Ça, c'est ultra-important, gérer le temps réel »*.

Automatiser les tâches

Guy Mettrick, Industry Manager for financial Services chez Appian, indique : "nous vivons une troisième vague d'évolution des services Finance. Les entreprises cherchent vraiment à transformer les processus finaux, à éliminer les processus manuels qui existent entre les données et processus silotés, des îles d'automation,



Valentin Gerbi, directeur France Payhawk.

> *« On a une vélocité dans les entreprises qui est de plus en plus importante et on a besoin de prendre des décisions stratégiques, non pas dans une semaine, mais maintenant. »*

comme nous les appelons, et à vraiment commencer à transmettre des processus finaux, des processus numériques, où vous consommez des données de différents systèmes ». Le complément de cela est de fournir des processus optimisés. Le principal lieu de cette automatisation se tient dans la phase de contrôle, une tâche souvent longue, répétitive et rébarbative. Samuel Rouayrenc opine : *« c'est là où est le besoin d'utiliser de la technologie pour automatiser ces activités de contrôle »*.

C'est là aussi que rentre en jeu l'intelligence artificielle. Selon Brice Mannevy, directeur marketing de N2JSOFT, fintech française créatrice de N2F (solution de gestion des notes de frais) : *« L'IA transforme profondément la gestion comptable et des notes de frais. Elle rend les processus plus rapides, plus fiables et même prédictifs. Mais loin de remplacer l'humain, elle permet aux comptables de se concentrer sur des missions plus stratégiques nécessitant créativité, analyse et intelligence émotionnelle. »* Samuel Rouayrenc ajoute : *« il y a beaucoup de tâches dans la fonction finance, par exemple des tâches de justification, de lettrage, de réconciliation, c'est-à-dire toutes les phases de révision comptable, ce sont des tâches qui*

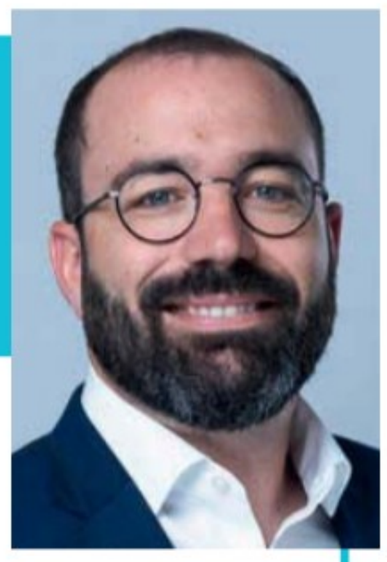
sont très répétitives. Je dirais que même la majorité des contrôles sont très répétitifs. Ces contrôles-là, puisqu'on est sur une activité, la comptabilité qui est une activité normée, on est capable de suivre des règles, des règles qui, elles, peuvent être dématérialisées, qui permettent d'effectuer ces contrôles répétitifs de manière automatisée. Donc ça, c'est le premier niveau d'automatisation avec des règles. Ensuite, il y a un deuxième niveau d'automatisation quand on a un volume de données qui est très important sur lequel il faut effectuer des contrôles. Là, il faut utiliser des outils un petit peu plus puissants qui puissent d'un, importer et intégrer la donnée de manière automatique, et puis analyser cette donnée pour pouvoir la lettrer. Et donc là, effectivement, on a un nombre de règles d'automatisation qui est beaucoup plus important. Et c'est là que ça devient intéressant d'essayer d'augmenter les capacités d'une solution en utilisant potentiellement de l'intelligence artificielle ou du machine learning». Il continue : «*il y a aussi l'IA générative, et ça c'est l'IA la plus connue et entre guillemets aujourd'hui la plus répandue, notamment avec ChatGPT, où là on peut utiliser l'intelligence artificielle pour produire des analyses. Et donc là, on rentre dans la production d'analyses, qui je pense nécessitera toujours un avis humain, in fine, pour compléter et produire cette analyse, et en vérifier la véracité. Mais c'est un domaine d'automatisation qui commence à être ouvert et à s'appliquer sur le domaine finance*».

Guy Mettrick,
Industry Manager for financial Services chez Appian.

«Nous vivons une troisième vague d'évolution des services Finance. Les entreprises cherchent vraiment à transformer les processus finaux, à éliminer les processus manuels qui existent entre les données et processus silotés.»

Le SaaS omniprésent

Pour les entreprises, le choix se réduit de plus en plus sur le mode de déploiement de solutions pour les directions financières et comptables. Le modèle SaaS domine et seuls les très grandes entreprises soumises à des règlements ou des règles de conformité très strictes demandent encore d'avoir des déploiements sur site. La peur de voir des données sensibles en dehors de l'entreprise s'estompe peu à peu et les entreprises se convertissent au Cloud, public ou privé, pour répondre à des besoins de flexibilité, de performance, même si la promesse de réaliser des économies n'est plus réellement l'argument mis en avant.



Samuel Rouayrenc,
vice-président pour la région Europe du Sud chez Blackline.

«Un des enjeux aujourd'hui auxquels font face les départements finances, c'est l'accélération des besoins de la production des chiffres.»

Le marché est dominé par les ERP, SAP en tête mais Oracle et son petit frère Netsuite suivent de près. Ces outils visent clairement le haut du marché. Sage Intacct reste lui plutôt sur le segment middle market ainsi que Workday. Ce dernier monte cependant en puissance sur les grands comptes et affiche une progression par son approche regroupant données financières, RH et analytiques. Les autres logiciels disponibles se positionnent sur une partie des fonctions des directions financières. Ils sont très nombreux et très spécialisés. Certains logiciels d'éditeurs investissent de plus des niches de marché qui ont été abandonnées par les banques le secteur de la finance comme la paiement, le paiement instantané, le cash back et autres possibilités de régler des achats. D'autres comme Anaplan remplissent la partie concernant la planification et l'optimisation budgétaire. Appian, Pega ou Celonis ont l'expertise pour analyser et optimiser les processus de bout dans la partie finance. Tous embarquent désormais des éléments d'intelligence artificielle et sont disponibles en ligne. Ces outils sont complémentaires des ERP ou sont centralisés les données financières.

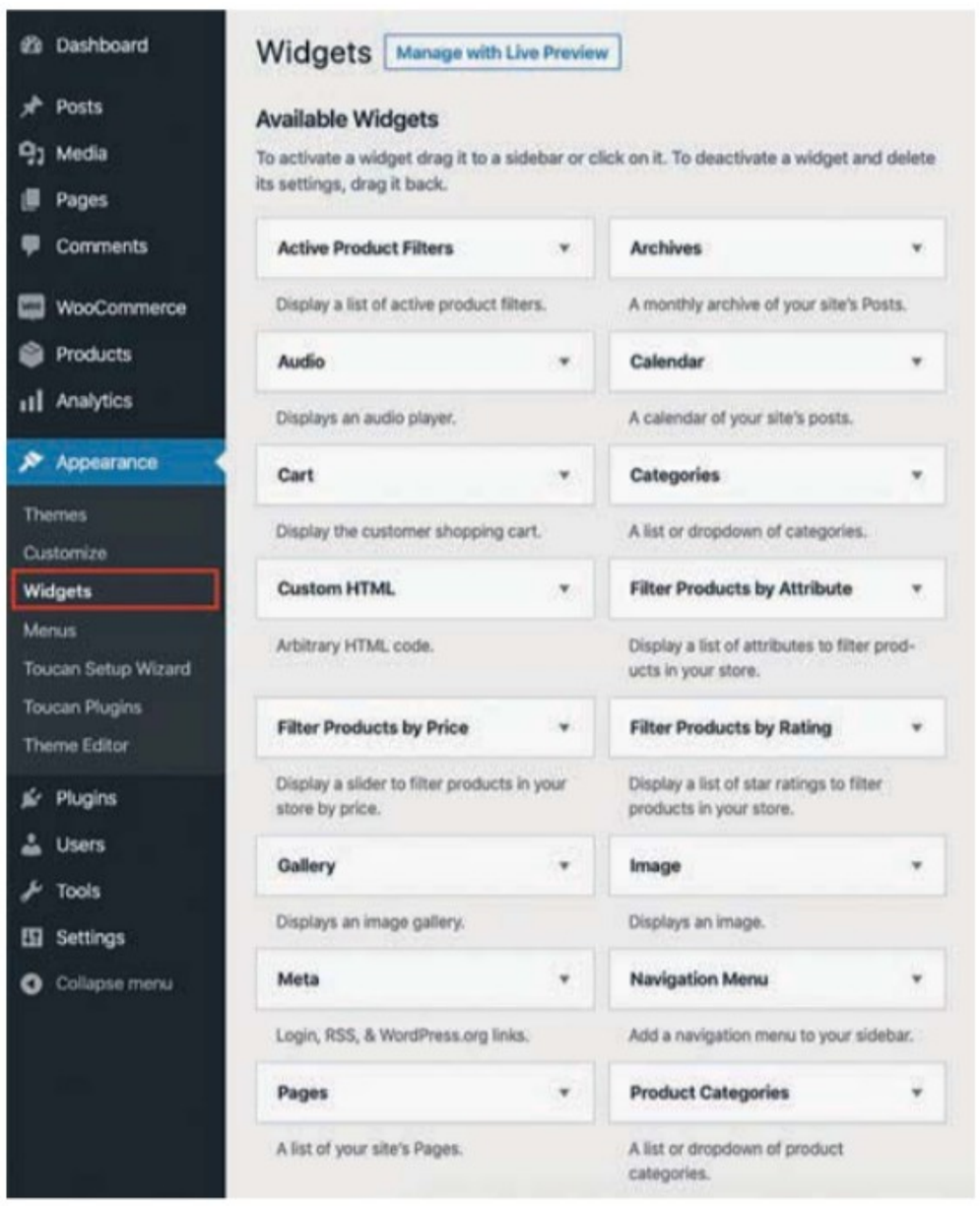
Tous ces outils concourent à apporter aux directions financières ce statut stratégique que leur demande les directions générales. Par ces automatisations, la fonction se transforme à nouveau pour devenir plus qu'un soutien aux lignes de métiers de l'entreprise mais un véritable guide pour le business. □

B.G

Des **exemples récents** de déploiements

L'évolution des directions financières se développe sous différents aspects que mettent en exergue quelques déploiements récents dans les entreprises en voici quelques exemples récents.

Avec SAP S/4HANA, Europcar Mobility Group effectue une transition en douceur vers le cloud, sans interruption versus l'ancienne solution. L'ensemble des process métiers de la finance est désormais pris en charge de bout en bout, améliorant ainsi l'efficacité en termes de temps et réduisant les coûts pour toute l'organisation. *« Nous avons désormais accès à des données centralisées, fiables, sécurisées et actualisées, qui nous permettent de connaître la situation de notre groupe en un clic. Revoir la chaîne de data de bout en bout, et mettre en place une solution sur une technologie innovante, a réuni les équipes Product and Tech autour d'un projet ambitieux et extrêmement motivant pour les collaborateurs. »* déclare Valérie Leffray, Group Product & Technology — Cockpit Director, IT programme lead de la Transformation Finance d'Europcar Mobility Group pour Product & Technology.



Un widget de Toucan.

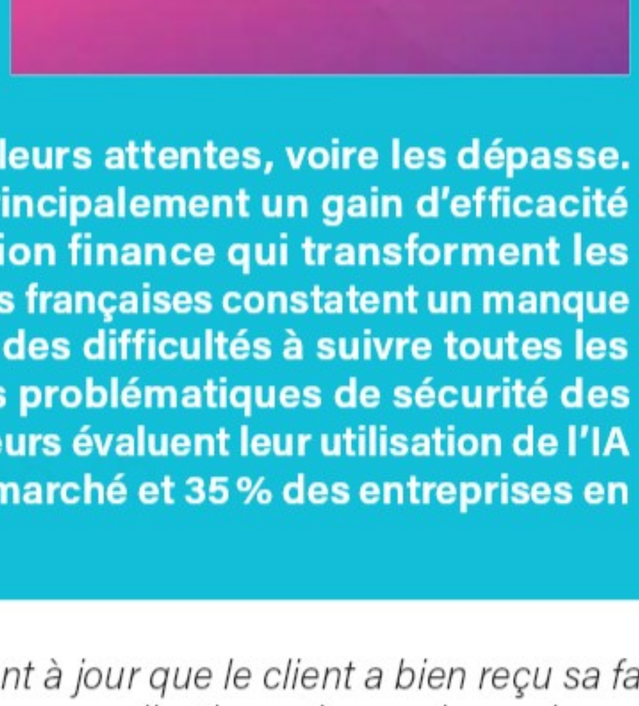
Une utilisation en interne et en externe de l'IA

Le cabinet Comptable Exponens a eu une approche assez originale de l'utilisation de l'IA à la fois pour ses 450 salariés mais aussi pour ses clients avec la mise à disposition d'un portail qui met à disposition à la fois le suivi de la comptabilité mais aussi les analyses du cabinet. Thierry Legrand associé du cabinet explique : *« Nous leur proposons effectivement un outil collaboratif qui permet d'avoir une vision en direct sur leur comptabilité. c'est-à-dire que au fur et à mesure où les éléments sont enregistrés en comptabilité, ils ont des widgets qui leur permettent de visualiser leur chiffre d'affaires, leur trésorerie, leur niveau charge, leurs encours client, leurs encours fournisseurs, leur top clients, leur top fournisseurs, et ça à chaque fois qu'une écriture est passée. L'information est remontée sur le sur la dataviz et ce qui était important pour nous, c'est d'avoir un outil qui permette aux dirigeants d'avoir cette vision de manière synthétique rapide et de pouvoir avoir des Data qui sont très visibles et de pouvoir ensuite aller un peu plus en profondeur en allant au-delà d'un simple widget qui est affiché à l'écran. La solution s'appuie sur la bibliothèque de widgets de Toucan. Les données sont collectées à partir de la comptabilité, transformées puis mises à disposition vers les clients et les salariés suivant les droits*

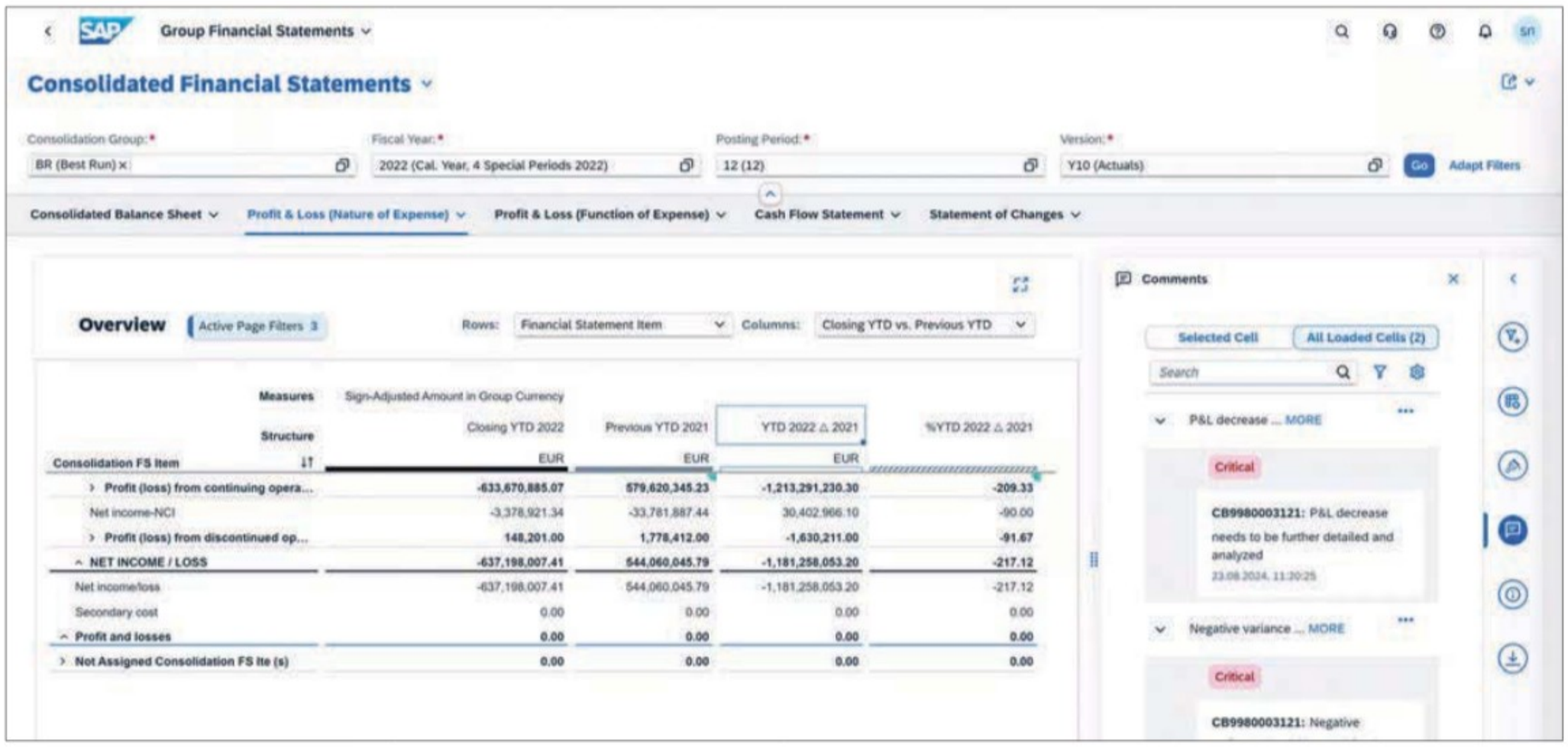
d'accès. Thierry Legrand voit un intérêt important à la possibilité de personnaliser les widgets selon les demandes ou besoins des clients du cabinet. Il précise : « on peut avoir des éléments qui sont fixes qui sont prêts pour tous les clients et ensuite on peut adapter puisque l'intérêt de toucan, c'est qu'on peut on peut développer des apps qui sont génériques pour l'ensemble des clients et avec son connecteur, il vient sur l'App générique et il a les éléments et on peut pour certains clients avec leur code d'accès aller sur une app distincte qui va reprendre l'ensemble des éléments, plus des éléments personnalisés pour les clients, c'est-à-dire que par exemple un client qui va utiliser de l'analytique, on va pouvoir lui présenter un compte de résultat par activité. On peut lui présenter des éléments dont il a besoin pour ces reportings propres, on peut lui présenter des éléments budgétaires. Et ça, sans développement spécifique qui sont faits à partir des éléments ce qu'on a mis en place de manière générique et on les personnalise pour certains clients ». Il ajoute : *« on l'utilise en interne aussi par exemple tous les collaborateurs ont accès à la balance client et de du cabinet pour vérifier qu'effectivement les encaissements sont à jour que le client a bien reçu sa facture. Toucan c'est une application qu'on a mis en place qui est spécifique à Exponens ».* □

B.G

LES DIRIGEANTS FRANÇAIS PARMI LES PLUS OPTIMISTES FACE AUX BÉNÉFICES DE L'IA



Selon une étude de KPMG, 73 % des entreprises françaises estiment que le retour sur investissement de l'IA dans la fonction finance correspond, voire dépasse leurs attentes contre 66 % dans le reste du monde. 87 % des dirigeants français estiment prendre de meilleures décisions grâce à l'IA contre 72 % des dirigeants à l'international. 78 % en France contre 58 % dans le reste du monde, affirment que l'IA permet un accès rapide aux données clés. 74 % des entreprises françaises voient dans l'IA la possibilité de réduire certains coûts versus 60 % dans le monde. 73 % des entreprises françaises et 95 % dans le monde estiment que le retour sur investissement de l'utilisation de l'IA dans la fonction finance répond à leurs attentes, voire les dépasse. Aujourd'hui les entreprises y voient principalement un gain d'efficacité et de productivité au sein de la fonction finance qui transforment les méthodes de travail. 57 % des entreprises françaises constatent un manque d'expertise en interne, 39 % partagent des difficultés à suivre toutes les réglementations et 43 % évoquent des problématiques de sécurité des données. 64 % ont besoin que les auditeurs évaluent leur utilisation de l'IA dans la production de l'information au marché et 35 % des entreprises en attendent un éclairage régulier.



Un reporting financier sous S4 HANA.

Datacenter

Pourquoi AMD a battu tous ses records en 2024

Alors que le CA d'Intel baissait de 7% au quatrième trimestre, celui d'AMD progressait de 24%. Ce dernier est encore deux fois plus petit que son rival de toujours, mais la différence de dynamiques est évidente. AMD marque désormais des points sur les segments stratégiques des datacenters et de l'IA.

Pour les gamers, le match est plié. En 2024, l'AMD Ryzen 7 9800X3D et son monstrueux cache de 104 Mo, était incontestablement le CPU à acheter pour les joueurs les plus exigeants... En 2025, l'AMD Ryzen 9 7950X3D devrait enfoncer le clou. AMD a mis Intel au pas dans ce marché très spécifique et très exigeant, mais traditionnellement, c'est Intel qui régnait en maître dans les datacenters. Déjà, au troisième trimestre 2024, les ventes de processeurs Epyc d'AMD avaient dépassé celles du bon vieux Xeon. Un croisement des courbes historique pour AMD, et lors du quatrième trimestre, l'équipe des rouges a creusé l'écart. Sur les trois derniers mois de l'année, la progression sur le segment Datacenter a été de +69%, une croissance essentiellement portée par les ventes des GPU Instinct et des CPU Epyc. Sur l'année, AMD a réalisé une croissance supérieure à 14%, ce qui confirme le regain de forme du fabricant depuis 2020 et surtout depuis l'accélération connue en 2022.

Lisa Su, présidente et PDG d'AMD

« À l'horizon 2025, nous voyons clairement des opportunités de croissance continue basées sur la force de notre portefeuille de produits et la demande croissante pour l'informatique de haute performance et adaptative »

« 2024 a été une année de transformation pour AMD, car nous avons enregistré un chiffre d'affaires annuel record et une forte croissance des bénéfices », expliquait le Dr Lisa Su, présidente et PDG d'AMD, lors de la présentation des résultats annuels. *« Le chiffre d'affaires annuel du segment Data Center a presque doublé grâce à l'accélération de l'adoption des processeurs EPYC, et nous avons réalisé plus de 5 milliards de dollars de chiffre d'affaires pour les accélérateurs AMD Instinct. »*

EPYC cartonne dans les entreprises

La quatrième génération des processeurs EPYC (nom de code Genoa) semble avoir trouvé son public dans les entreprises, et les Epyc de génération Turin devraient poursuivre cette dynamique. Pourtant, tout n'a pas été rose chez AMD en 2024. Sur les postes client, la progression était très significative (+52%), par contre, sur le segment Gaming, AMD a connu une baisse de 58% pour atteindre 2,6 milliards de dollars de vente. Les ventes de consoles n'ont pas cartonné à Noël, et AMD qui équipe à la fois la PlayStation 5 et la Xbox, a clairement souffert de ces méventes. Dans l'embarqué, AMD est carrément en difficulté, en baisse de 33% sur l'année.

Dans son rapport sur les livraisons de processeur x86 du dernier trimestre 2024, Mercury Research soulignait le fait qu'AMD réalise désormais 35,5% de ses ventes sur le marché des serveurs, soit plus que les Desktop (27,3%) et que les portables (21,6%). Au global, AMD a gagné 4,3% de parts de marché sur l'année et 0,7% au dernier trimestre.

Cette progression dans les datacenters n'est pas fortuite. Déjà, sur la niche des supercalculateurs, AMD s'est taillé une place significative. Trois des cinq plus gros calculateurs en production sont motorisés par AMD, notamment El Capitan du centre de recherche nucléaire américain de Livermore. Sur ce marché, où le rapport puissance de calcul sur puissance électrique est clé, AMD avec le diptyque EPYC 24C, son CPU à 24 cœurs et son APU (combiné CPU + GPU) Instinct MI300A, a des arguments de poids.

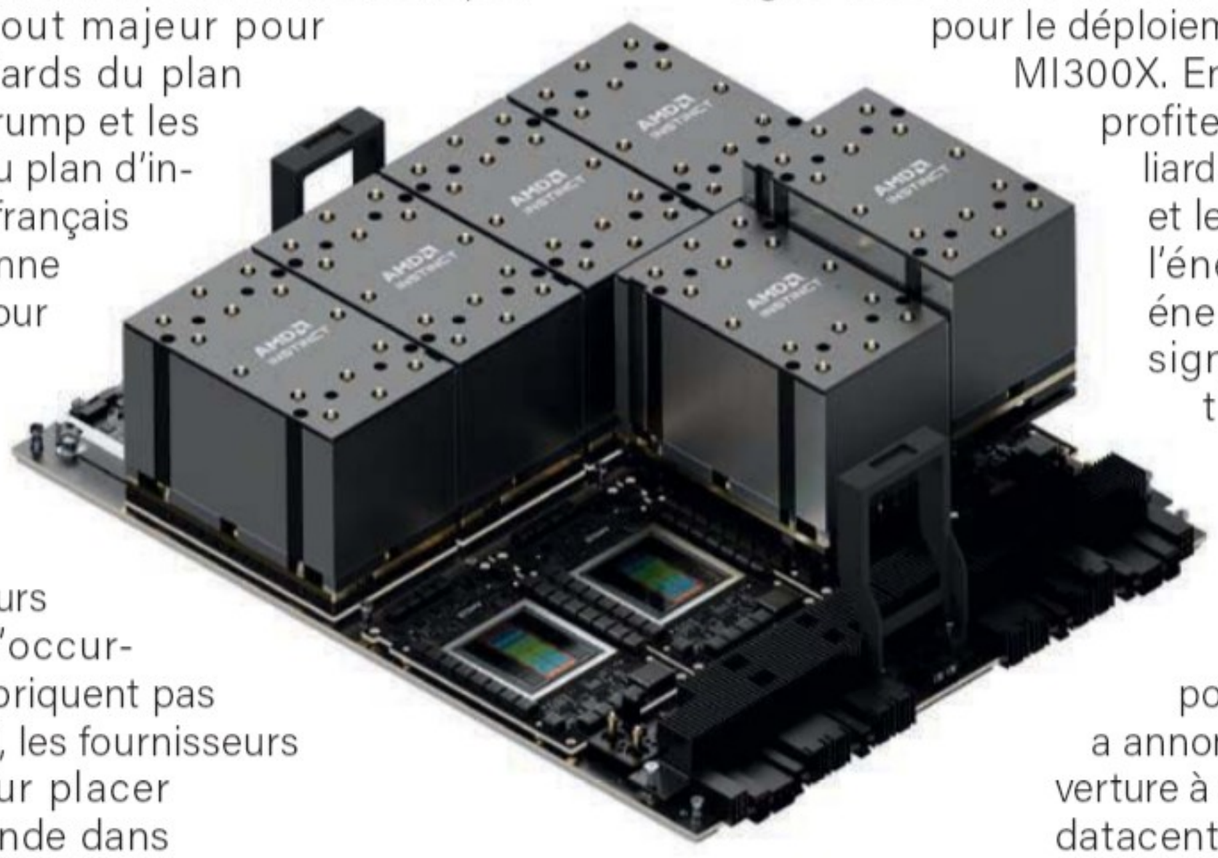
La pactole des plans nationaux IA à l'horizon

Disposer d'un GPU performant et relativement peu énergivore est un atout majeur pour l'avenir. Les 500 milliards du plan Stargate de Donald Trump et les 109 milliards d'euros du plan d'investissement dans l'IA français vont constituer une manne colossale et, comme pour la ruée vers l'or, ce sont les fournisseurs de pelles qui empocheront le pactole, les fournisseurs de composants et opérateurs de datacenters, en l'occurrence. Quand ils ne fabriquent pas eux-mêmes leurs NPU, les fournisseurs Cloud se battent pour placer leurs bons de commande dans la pile à traiter de Nvidia, mais on en voit de plus en plus proposer les instances avec GPU MI300A. Avec la prochaine génération, la MI325X, AMD veut détrôner la Superchip Nvidia H200, actuellement au sommet de la chaîne alimentaire de l'IA. Comme le soulignait récemment Octave Klaba, les générations de GPU actuellement disponibles sur le marché permettent de faire l'entraînement sur environ 100 K GPU en fonctionnant ensemble, mais pour pouvoir construire les datacenters de 1GW spécifiquement conçus pour l'entraînement des IA. *« Le facteur limitant est la distance entre les deux GPU les plus éloignés physiquement : à partir d'un certain nombre de GPU connectés ensemble, la distance fait ralentir le fonctionnement de l'ensemble de GPU. C'est pourquoi pour le besoin de l'entrainement, une nouvelle génération de GPU arrive sur le marché : les Superchips. »* Avec la MI325X, AMD affirme pouvoir rivaliser avec la puce Blackwell B200, dévoilée au début de l'année 2024. Dans une interview au Financial Times, Lisa Su ne cachait pas son ambition de se placer en tant que leader sur ces applications IA, concluant son interview par ce leitmotiv : *« Ceci est le commencement, et non pas la fin de la course à l'IA. »* Le ton est donné, et la roadmap d'AMD est très agressive, avec une nouvelle évolution 4 de l'architecture CONA de l'AMD Instinct en 2025 pour les MI350, et une architecture de nouvelle génération CONA Next attendue pour 2026, et la motorisation de la puce MI400.

L'essor des Superchips place AMD dans les roues de Nvidia

Le classement Green500 traduit déjà cette tendance : les superchips Grace Hopper de Nvidia trustent 5 des 10 premières places contre 4 pour AMD, et 1 seule pour Intel. Avec son MI300A et le futur MI325X, AMD pourrait bien jouer la carte du challenger contre Nvidia, alors qu'Intel n'a tout simplement rien à proposer...

Dans son communiqué financier, AMD a annoncé avoir signé avec IBM, Vultr et l'allemand Aleph Alpha pour le déploiement de ses superchips MI300X. En France, AMD devrait profiter du plan des 190 milliards d'euros pour l'IA. AMD et le CEA (Commissariat à l'énergie atomique et aux énergies alternatives) ont signé une lettre d'intention qui verra les deux entités coopérer sur les infrastructures IA dédiées à l'énergie et la santé. En marge du Sommet pour l'action sur l'IA, AMD a annoncé avec DataOne l'ouverture à Grenoble d'un nouveau datacenter dédié à l'IA, en lieu et place des locaux de Hewlett Packard et de DXC Technology.



La plateforme AMD Instinct MI325X permet de monter 8 Instinct MI325X sur une carte de 41,7 cm x 55,3 cm. Une intégration très appréciée des concepteurs de datacenter pour l'IA.

Si Nvidia reste l'acteur incontournable du marché de l'IA, les tarifs extrêmement élevés de ses superchips, (on parle de plusieurs dizaines de milliers de dollars par puce) et des délais de livraisons à rallonge vont mécaniquement pousser de nombreux acteurs qui veulent se positionner sur le marché de l'IA à chercher des alternatives, ce qui pourrait les pousser dans les bras d'AMD.

Si l'acquisition d'ATI par AMD en 2006 fut longue et douloureuse et n'avait guère démontré sa pertinence jusqu'à présent, la révolution de l'IA générative et ce besoin d'intégration entre CPU et GPU à grande échelle porte enfin ses fruits, 18 ans plus tard ! □

A.C

Serveurs

NetApp se renforce dans le stockage bloc

Depuis 18 mois, NetApp développe une stratégie qui élargit son champ d'action au stockage bloc. Les dernières annonces visent à couvrir l'entrée et le milieu du marché des entreprises avec de nouvelles baies ASA.

S'il est le plus utilisé dans les entreprises, le stockage en mode bloc peut parfois sembler complexe car difficile à configurer, gérer et maintenir. De plus la plupart des solutions sur le marché ont du mal à évoluer quand les besoins se font sentir et elles peuvent s'avérer coûteuses.

S'affranchir des problèmes du bloc

Les nouveaux modèles de la famille ASA visent à éviter ces problèmes en proposant des solutions simples à administrer, avec de fortes capacités d'évolution en capacité et en performance à un prix raisonnable, voire très agressif. Le prix des baies commence à 25 K$ pour l'ASA A20 et propose des capacités s'échelonnant de 15 To à 734 To bruts avec des configurations en rack pouvant culminer à 3,2 Po. La configuration en cluster peut aller jusqu'à 19 Po bruts sur des serveurs 2U contenant 24 disques NVMe. Les baies supportent différents protocoles : NVMe/FC, NVMe/TCP, FCP, iSCSI. Les modèles ASA A30 et A50 offrent des capacités supérieures par des disques NVMe plus capacitifs dont les disques 15,3 To.

Une simplification du déploiement et de l'administration

La console a été simplifiée et évite le jargon afin que n'importe qui puisse réaliser le déploiement ou l'administration de la baie. NetApp assure que la solution peut se déployer en une minute et que la protection des données d'une application se réalise en un seul clic. Ces possibilités sont inhérentes à l'OS employé, OnTap.

Les nouvelles baies ASA.

De la même manière les performances des baies sont largement améliorées. Ainsi l'ASA A20 apporte 70 % de performance en plus comparé à la génération précédente avec le ASA 150. Les gains de performance vont jusqu'à 171 % pour l'A50 comparativement au plus ancien ASA A400.

Des services associés

Les nouvelles solutions ASA sont aussi couvertes par différentes garanties et services comme un programme tout au long du cycle de vie de la baie et des garanties sur les fonctions de compression et de réduction de données, la haute disponibilité et la restauration après une attaque de rançongiciel.

Flexpod et vSAN supportés

Avec Data infrastructure Insight, NetApp propose une suite de logiciels de monitoring des environnements SAN (Storage Area Network). La solution comprend SAN Analyzer qui regarde les interactions entre les matériels et suit le chemin des données. S'appuyant sur l'intelligence artificielle SAN Anomaly Detection identifie et résout les anomalies avant qu'elles aient un impact sur le stockage de l'entreprise. Infrastructure Change Analysis cartographie et corrèle les données afin de déterminer les problèmes dans l'infrastructure pour des résolutions d'incidents plus rapides.

Pour les environnements VMware, la suite supporte vSAN avec vSAN Support qui préconise les bons paramètres et configurations pour éviter les problèmes de performance que ce soit pour les clusters ou la configuration des tâches. Storage Infrastructure Optimization and Reclamation vise à optimiser la capacité de stockage en réclamant le stockage non utilisé et optimise les ressources à partir des données observées.

Flexpod, l'architecture préconçue, intégrée et validée qui combine les serveurs Cisco Unified Computing System (Cisco UCS), la gamme de commutateurs Cisco Nexus, les commutateurs Cisco MDS Fabric et les baies de stockage NetApp a été testée et validée sur les nouvelles baies ASA et propose 240 architectures de références. □

B.G

Backup

Hathor a raison pour la sauvegarde déconnectée

La jeune entreprise française propose une appliance de stockage dédiée à la sauvegarde, qui permet une déconnexion physique et automatisée de ses espaces disques. Compatible avec la plupart des solutions du marché, elle permet d'assurer qu'une sauvegarde soit toujours isolée du réseau en cas d'attaque.

Hathor est une solution de sauvegarde déconnectée développée par Julien Le Breton et Julien Boissat, anciens collègues dans le secteur de la revente IT. Après l'acquisition de leur entreprise en 2023, ils ont décidé de se lancer dans un nouveau projet répondant à un besoin précis, identifié au cours de leurs années sur le terrain. L'objectif était d'offrir aux petites entreprises une solution de sauvegarde conforme aux préconisations de l'ANSSI, capable d'être automatiquement déconnectée du réseau après chaque backup. *« Notre idée était de proposer une alternative aux solutions existantes, comme le Tankr EUKLES, qui étaient trop rigides, coûteuses et surchargées de fonctionnalités inutiles pour les TPE et les PME »*, détaille Julien Le Breton.

Pour créer leur solution, les deux entrepreneurs se sont entourés de spécialistes de l'électronique. Ils ont développé une carte réseau, couplée à un routeur 4G. Le système est simple et innovant. Cette carte intégrée à l'appliance gère l'ouverture et la fermeture des ports qui donnent accès à deux espaces disques (ou plus) strictement isolés. Les instructions pour l'ouverture et la fermeture des ports sont reçues, via le réseau 4G, depuis une interface hébergée dans un datacenter Ionos. *« L'objectif était que le système qui pilote l'ouverture et la fermeture des ports soit entièrement isolé du réseau du client. Par ailleurs, il est strictement impossible d'ouvrir tous les ports en même temps, sauf pour passer en mode restauration. Pour les environnements sans réseau mobile, nous pouvons mettre en place un VLAN spécifique »*, précise Julien Boissat.

Une automatisation complète via REST

Comme évoqué plus haut, les appliances sont pilotées à distance depuis une interface développée par les deux entrepreneurs et hébergée sur Ionos. Celle-ci est spécifiquement protégée par un Web Application Firewall (WAF). Chaque appliance est préparamétrée pour être reliée via un lien unique à son interface dédiée. *« L'un des principaux défis du projet était de proposer une solution entièrement automatisée. Là où certaines entreprises bricolent des méthodes de déconnexion manuelles via des switchs, Hathor assure une déconnexion physique et sécurisée après chaque sauvegarde. En mode incrémentiel, une copie prend en moyenne sept minutes, garantissant une continuité sans impact sur la productivité et un pilotage fin des sauvegardes »*, explique Julien Boissat.

Hathor se veut compatible avec le plus grand nombre d'éditeurs de solutions de sauvegarde, via une API REST. *« Pour les solutions maison, ou qui ne sont pas compatibles avec REST, nous avons mis en place des scripts qui permettent d'automatiser la gestion des appliances »*, précise Julien Boissat. Les solutions Hathor peuvent ainsi être utilisées comme support de stockage des sauvegardes avec un maximum de solutions.

Pour limiter les dépenses de stockage, Hathor propose également le Hathor Disconnect, une appliance réseau complémentaire. Elle reprend le même fonctionnement que l'appliance Hathor, mais sans disque intégré pour utiliser à la place des solutions existantes, à condition qu'elles soient équipées d'un port RJ45.

Des ambitions mesurées

Julien Boissat et Julien Le Breton (de g. à dr.) ont fondé Hathor, fin 2023, afin de proposer une nouvelle approche de la sauvegarde taillée pour les PME.

L'équipe derrière Hathor vise particulièrement les TPE et PME. *« Elles sont souvent victimes de prestataires qui leur assurent une sauvegarde, mais sans réelle garantie. Ces entreprises ont besoin de solutions fiables et accessibles »*, détaille Julien Le Breton. L'entreprise qui travaille déjà sur une V3, intégrant un espace disque supplémentaire totalement déconnecté, permettant de stocker une copie des espaces disques principaux sans jamais être connectée à internet, reste ouverte aux opportunités de financement. Elle préfère toutefois avancer à son rythme, en consolidant sa production (à Lille), et en assurant la qualité de son produit. □

O.Ba

B2B

Synology passe à l'offensive sur la sauvegarde

Le fabricant de NAS vient de présenter une offre complète de sauvegarde et de restauration comprenant un nouvel OS dédié, ainsi que des appliances capables de répondre aux besoins des petites et des grandes entreprises.

Synology poursuit sa mue en acteurs BtoB avec une offre de sauvegarde. À l'occasion de son événement Solutions Day 2025, qui s'est tenu à Paris début février, le spécialiste des solutions NAS a dévoilé ActiveProtect, une solution avancée de sauvegarde et de protection des données, liée à une nouvelle gamme de baies baptisée les DP.

« Nous proposions déjà une solution de sauvegarde avec Active Back-up qui était une application que nous installions sur les NAS via notre OS DiskStation Manager, ce qui limitait ses capacités. ActiveProtect est un tout nouveau système d'exploitation, dédié uniquement à la protection des données et lié aux appliances DP », explique Ivan Lebowski, sales team lead de Synology.

ActiveProtect en tour de contrôle

ActiveProtect repose ainsi sur une approche tout-en-un, intégrant à la fois un logiciel et des appliances dédiées. Elle se veut compatible avec une large gamme de solutions. Synology annonce la prise en charge de serveurs physiques (Windows Server et Linux), des machines virtuelles (Hyper-V et VMware), des bases de données (Oracle et Microsoft SQL Server), des fichiers (Nutanix et NetApp) et du SaaS (Microsoft 365). La solution propose également une déduplication des données à la source et intersite, afin d'optimiser les volumes de stockage.

La solution se dote par ailleurs d'ActiveProtect Manager, une interface centralisée permettant de définir et d'appliquer automatiquement des politiques de sauvegarde à tous les appareils d'un réseau. Il est possible de définir des politiques spécifiques pour chaque groupe et type de solutions (SaaS, terveur, terminaux, etc.). Le système assure également une détection automatique des nouveaux éléments sur le réseau pour appliquer automatiquement les politiques de sauvegarde.

Des fonctionnalités avancées de restauration et de test

ActivProtect autorise par ailleurs la mise en place de politiques d'accès granulaires basées sur les solutions IAM et PAM des utilisateurs. Les utilisateurs finaux peuvent par exemple accéder à leurs fichiers directement dans la sauvegarde pour les restaurer eux-mêmes. Évidemment, Synology s'appuie sur un modèle de sauvegardes immuables, et embarque des mécaniques de restauration et de test pour assurer la disponibilité des back-up. La société a notamment développé un hyperviseur sur base KVM et l'a intégré à sa solution pour tester directement les données des VM. Celui-ci peut également être utilisé comme solution de secours pour assurer la continuité de l'activité en cas d'attaque. Enfin, ActiveProtect intègre des outils avancés de vérification et de réparation automatique des données, avec des tests de cohérence via BTRFS.

L'offre logiciel ActivProtect de Synology est directement liée à de nouvelles appliances dédiées. La DP7400 au format rack 2U, qui embarque un cache SSD et des ports 10Gb/s, s'adresse aux plus grosses entreprises. Elle est capable de protéger 83,5 To de données, et peut être facilement mise en cluster sur un mode web scale, chaque appliance embarquant ses propres systèmes réseau. Sur le même principe, Synology propose au format tour les DP340 et DP320, avec des capacités respectives de 14,5 To et 4,5 To de données protégées. Comme la DP 7400, la DP340 embarque un cache SSD et un port 10Gb/s, tandis que la DP320 ne possède pas de cache et s'appuie sur un port 1Gb/s.

Une politique de licence à l'appliance sans limite de volume

Toutes les appliances reposent sur un concept d'Air Gap physique et logique, permettant de séparer les sauvegardes du réseau de production pour limiter les risques d'intrusion.

Le Air Gap logique est assuré par un firewall qui bloque toutes les connexions entrantes, autorisant uniquement les communications sortantes pour assurer le clustering. Pour le Air Gap physique, l'appliance désactive sa carte réseau et s'éteint automatiquement selon les planifications de sauvegarde, garantissant un isolement total des données critiques.

L'atout majeur mis en avant par Synology pour son offre de sauvegarde réside dans sa politique de licence. Contrairement à certaines solutions concurrentes, Synology ne facture pas de licence en fonction du stockage, du nombre d'appareils ou du type de processeur. ActivProtect est ainsi fournie gratuitement pour les clusters 1 à 3 DP. Au-delà, il faudra compter une licence par appliance supplémentaire. Celles-ci sont facturées 1 800 euros HT pour une durée de 3 ans. □

O.Ba

IN CYBER FORUM

1-3 AVRIL 2025
LILLE GRAND PALAIS

Au-delà du *Zero Trust*, la confiance pour tous

europe.forum-incyber.com

ORGANISÉ PAR

Forward

AVEC LE SOUTIEN DE

Région Hauts-de-France

MEL MÉTROPOLE

RETROUVEZ-NOUS SUR

YouTube LinkedIn X

Infrastructure

NTT Data : une ESN débridée

L'ESN d'origine nipponne faisait un peu profil bas. Aujourd'hui elle affiche de nouvelles ambitions. Avec une stratégie de renforcement à l'internationale, l'entreprise développe une stratégie en plusieurs points. Rencontre avec David Hubert, son patron pour la France, pour faire un point précis.

David Hubert retrace le contexte dans lequel se développe la stratégie actuelle de NTT Data. *« Il y a une dizaine d'années, un peu plus, le groupe NTT, puissant au Japon, qui rayonne par capillarité en Asie, s'est posé la question de ses relais de croissance. Ils sont arrivés à la conclusion que les relais de croissance passaient essentiellement par une très grande force internationale qui dépassait largement la force internationale qu'il pouvait avoir par rayonnement capillaire en Asie. Et donc, le groupe NTT s'est lancé dans beaucoup d'acquisitions, puisque les Hiragana et Katagana s'exportent relativement mal. Le niveau d'anglais des Japonais étant parfois un peu limité, ils sont rentrés dans une structure d'extension par acquisition. Et il y avait deux grands domaines qui étaient ciblés à l'époque dans les acquisitions qui étaient stratégiques pour NTT. Un domaine autour des infrastructures de communication, de télécommunication et les infrastructures IT en général. Et puis, un domaine autour de tout ce qui était applicatif et conseil, et notamment conseil dans les solutions métiers, avec des acquisitions sur des sociétés de conseil qui sont généralement structurées en verticaux. Ici, l'acquisition d'une société qui est spécialisée dans la finance et la banque, là une autre spécialisée dans l'industrie, etc. Et finalement, le groupe NTT a fait ses acquisitions sur une dizaine d'années. Et à la mode japonaise, pendant très longtemps, il n'y avait pas forcément un plan précis d'intégration, de regroupement, de fédération de ces activités »*. Puis l'entreprise est passée par la phase d'intégration de toutes ces activités. David Hubert ajoute : *« depuis 2021 à peu près, NTT s'est lancé dans cet effet de mutualisation et d'agrégation de l'ensemble de ses portefeuilles en dehors du Japon, jusqu'aux annonces récentes, puisqu'en 1er avril 2024, un patron de l'ensemble des activités de NTT hors Japon a été nommé »*.

David Hubert, PDG de NTT France NTT Ltd.

Un regroupement sous une marque unique

Aujourd'hui la société propose une offre qui s'étend du conseil stratégique jusqu'aux infrastructures. Tout ce qui tourne autour de la donnée est au cœur de ce continuum qui va des solutions métiers jusqu'à la capacité de rendre des services IT, de traiter ces données, de les transporter, de les agréger, de les stocker et de les analyser, eh bien, NTT pense que c'est un avantage concurrentiel que peu de compétiteurs ont aujourd'hui sur le marché. En France l'ensemble des activités ont été regroupées sous une houlette unique. Et en France, ça se traduit aussi par sa volonté d'investir en France, d'acheter des terrains pour construire des data centers et accompagner la croissance de ses clients.

La force des « Assets »

Un des points forts de l'ESN s'articule autour des « assets », des solutions développées en propre pour certains clients verticaux et qui font énormément écho sur d'autres clients du même vertical. David Hubert précise : *« dans un secteur de l'énergie, typiquement, on travaille actuellement avec un très grand compte français, et finalement, la solution qu'on est en train de mettre en place chez eux, c'est une solution qu'on avait déjà développée sur un compte espagnol, dans un contexte un peu différent, mais c'est une solution qui n'existe pas sur le marché »*. Il ajoute : *« c'est un est un savoir-faire que NTT a développé à travers ses missions et son expertise de secteurs d'activité et qui*

NTT DATA ÉTEND SON **PARTENARIAT AVEC PALO ALTO NETWORKS**

En associant le pare-feu de nouvelle génération (« Next-Generation Firewall » ou NGFW) de Palo Alto Networks, les abonnements OT/IoT et l'architecture de 5G privée de NTT DATA, cette nouvelle offre permet aux clients de bénéficier d'une meilleure visibilité du réseau, d'un meilleur contrôle d'accès et de capacités automatisées de détection et de réponse aux menaces. Grâce au NGFW de Palo Alto Networks, les entreprises peuvent adopter une stratégie de sécurité Zero Trust en incorporant le Machine Learning (ML) à leurs processus afin d'activer uniquement les connexions, les applications et les protocoles pertinents nécessaires à leur réseau, en toute sécurité. Cette offre combinant la 5G privée de NTT DATA et la technologie de Palo Alto Networks est à la fois simple à mettre en place et à gérer, et s'intègre de manière fluide aux environnements IT/OT des entreprises.

finalement répond à une problématique du secteur, mais qui est une problématique qui n'avait pas forcément été encore envisagée ou regardée par certains des acteurs français ».

Une solution homogène

Pour la partie infrastructure, l'approche a été assez originale. *« Lorsque l'intégration de la partie infrastructure s'est effectuée chez NTT, on a pris une stratégie qui consistait à dire qu'il faut que nos plateformes de services, que ce soit pour du cloud, que ce soit pour du réseau, que ce soit pour de la cyber, que ce soit pour l'expérience client, fonctionnent sur une architecture et des outils qui soient intégrés dans une stratégie commune. Un des leviers différenciateurs par rapport à nos concurrents là-dessus, c'est de dire que si vous êtes chez NTT et que vous avez par exemple une infrastructure dans laquelle NTT manage votre réseau, demain vous voulez nous confier le management de vos clouds, c'est la même solution avec le même look and feel, les mêmes outils, le même reporting, la même façon de procéder, la même façon d'interagir avec vos propres infrastructures »* précise David Hubert.

Un soutien par la R&D

Plusieurs solutions de NTT Data sont soutenus par un travail de recherche et de développement spécifique dont un service de transmission photonique. *« L'idée est de pousser le plus loin possible la transmission photonique dans l'ensemble des services et des infrastructures IT, ce qui est une innovation en cours qui devraient changer beaucoup de choses, d'une part en termes de consommation des activités, des services informatiques, notamment dans les datacenters, et deuxièmement qui va changer aussi, à mon avis, la technologie et l'architecture du monde des datacenters en permettant d'avoir des temps de latence qui sont extrêmement réduits et qui permettent donc de faire du disaster recovery de manière totalement différente de celui qui est fait aujourd'hui »* indique le patron de NTT Data France. Il ajoute : *« nous sommes abreuver solutions qui sont en cours de développement mais qui vont avoir un impact dans la durée à la fois sur la durabilité et à la fois sur l'architecture du monde informatique ».* □

B.G

LES NOUVELLES MISSIONS DE CONSEIL INFORMATIQUE

Alternative

Un asiatique face aux ESN indiennes

FPT n'est pas encore connu du grand public pourtant cette ESN vietnamienne a réussi à faire son entrée dans les grands comptes français.

Christophe Schwanengel a récemment pris la tête de FPT en France. Après avoir passé huit ans dans une ESN indienne, il a préféré *« la courbe ascendante à la courbe plate de l'évangélisation »*. Historiquement, la société est le bras armé du gouvernement vietnamien pour la technologie. Elle a donc pu grandir sans grande difficulté. Aujourd'hui, FPT est présent dans 30 pays, compte plus de 48 000 employés et sert plus de 1100 clients dans le monde, dont près de 100 figurent dans le classement Fortune Global 500. La transformation numérique (DX) est son moteur de croissance depuis 10 ans et représente aujourd'hui 40 % de son chiffre d'affaires. Les services informatiques mondiaux génèrent un chiffre d'affaires de plus d'un milliard de dollars.

Une stratégie à long terme

Pour les 10 prochaines années, FPT va continuer à accélérer ses investissements dans l'IA, la mobilité électrique (EV), les semi-conducteurs et la transition verte afin de maintenir son rythme de croissance, pour doubler son chiffre d'affaires tous les trois ans. Ce développement passe aussi par le marché européen, et français en particulier. La France est d'ailleurs le premier pays européen où la société s'est implantée. FPT compte 3 000 employés dédiés au marché européen : 1 000 en local et 2 000 en offshore. En France, FPT a plus de 100 experts, dont une majorité de talents locaux. Objectif d'atteindre 500 experts en France, avec une présence renforcée en Belgique, Suisse, Luxembourg, Maroc et Tunisie

Une alternative aux acteurs indiens

Un des différenciateurs de la société est de miser sur le local. Le dirigeant de l'ESN en France met en avant la relation historique et culturelle avec la France et du fait que tous les employés de la société en France parle et échangent avec les clients en français. La société s'appuie aussi sur la large communauté vietnamienne présente dans notre pays. Il, souligne que de nombreuses entreprises souhaitent diversifier leurs fournisseurs pour réduire leur dépendance à des pays où les rapports sont plus complexes du fait du contexte international. Le Vietnam représente une alternative fiable et neutre, souvent comparée à la Suisse pour sa position équilibrée.

Trois priorités pour la filiale française

Le premier levier de croissance identifié est évidemment l'intelligence artificielle et est vu comme un moteur de la transformation numérique des entreprises françaises qui semblent un peu en retard face à d'autres pays comme les USA ou la Grande-Bretagne. Les applications possibles suivent aussi les secteurs de prédilection de FPT comme l'automobile où l'ESN a développé du logiciel et FPT Automotive vise à passer du rôle de sous-traitant logiciel à celui de concepteur technique pour les SDV. L'ESN va donc concentrer ses efforts sur le manufacturing, la santé et l'énergie.

Christophe Schwanengel, Directeur Général de FPT France.

Ces industries restent des priorités pour le développement et l'accompagnement technologique. La transition vers le cloud et la modernisation des infrastructures IT deviennent incontournables pour la compétitivité. De grands acteurs comme Capgemini ou Sopra se concentrent sur les gros projets, laissant des opportunités pour des acteurs plus flexibles sur les projets plus petits.

Une politique RH différente

FPT adopte une approche du recrutement qui se distingue des grands acteurs du secteur IT comme Capgemini ou Accenture. Plutôt que de privilégier uniquement les jeunes recrues, l'entreprise valorise l'expérience, notamment celle des professionnels de plus de 45 ans, souvent écartés des circuits de recrutement classiques. Elle vise à intégrer des talents ayant une réelle adéquation avec la philosophie et les besoins de l'entreprise. De plus, les recrues seniors apportent une expertise précieuse en gestion de la relation client, développement commercial et savoir-faire stratégique, des compétences difficiles à formaliser mais essentielles pour le succès d'une entreprise en forte croissance. □

B.G

Un Stargate à l'Européenne

par Bertrand Garé

Il était difficile, en ce mois de février, de passer à côté de ce qui concernait l'intelligence artificielle. Cela a commencé avec l'annonce du plan Stargate aux USA. Donald Trump décidait ainsi que certains devaient mettre 500 milliards de dollars sur la table afin de consacrer la domination américaine sur le monde. Financé par Softbank, Open AI et Oracle ayant des rôles plus opérationnels comme de fournir l'IA et le Cloud, Stargate va s'échelonner sur quatre ans. Une première tranche de 100 milliards de dollars devraient marquer le véritable début du projet afin de construire l'infrastructure, fournir l'énergie, les constructions et les équipements nécessaires. Il est prévu que le projet crée 100 000 emplois aux USA. Le projet affiche aussi clairement les buts de garder la prééminence de la technologie aux USA et de barrer la route aux concurrents éventuels, particulièrement la Chine qui semble avoir de l'avance dans les domaines de la robotique et des véhicules autonomes. Pas question donc de brider la future grande Amérique, dont le président réélu semble vouloir changer la géographie.

Choc et contre-choc

L'annonce a évidemment créé un choc, pas seulement des autres pays sur la planète, mais aussi boursier avec une envolée des valeurs liées à l'intelligence artificielle. Il n'a pas fallu longtemps pour que le contre-choc arrive avec l'annonce chinoise de DeepSeeK, et de voir en quelques heures des milliards de dollars de valorisation boursière partir en hallucinations des investisseurs. Le pitch de DeepSeek : faire autant, voire mieux, que les intelligences artificielles américaines mais pour beaucoup moins cher en ne nécessitant que beaucoup moins d'équipements et d'énergie. Et Alibaba et sa caverne de produit qui fait comme les autres et aligne plus de 50 milliards de dollars en centre de données et recherche en intelligence artificielle. Depuis on découvre peu à peu que, bof, DeepSeek n'est pas si génial que cela, que sa sécurité est minimale. De ce fait, plusieurs pays, dont la Corée du Sud, ont interdit son usage. Le bot est aussi persona non grata dans les agences américaines ainsi que dans d'autres pays. Une fois de plus, les critères politiques, stratégiques et militaires ont pris le dessus. Nous en parlions déjà dans une chronique précédente, et nous évoquions comment l'intelligence artificielle avait changé le visage des combats dans le conflit russo-ukrainien avec des innovations dignes de films de science-fiction. Comme lors de la course à l'espace ou à l'atome, l'intelligence artificielle est devenue le nouveau nœud pour démontrer la puissance et l'avantage technologique d'un continent sur un autre. Au passage, on oublie aussi que les Russes ne restent pas les deux pieds dans le même sabot et que eux aussi développent des modèles d'IA et depuis longtemps. Un ex-champion du monde d'échec Mikhail Botvinnik a été pendant longtemps à la tête d'un programme informatique de jeu d'échec.

L'Europe aussi veut sa part

L'Europe a évidemment voulu montrer qu'elle n'allait pas se laisser faire et d'aligner 200 milliards répartis entre budget européen, contributions d'entreprises présentes dans l'écosystème de l'intelligence artificielle. Bon, Stargate US c'est plus du double sur cinq ans, là c'est sur 15 ou 20 ans. La mobilisation est donc là, et pas seulement pour encadrer et rajouter des règles et directives, mais c'est en dessous de ce qui est nécessaire face à la concurrence pour rattraper le retard ou creuser une avance quelconque face à eux. Faire mieux pour moins cher et plus durable est toujours un bon point, mais cela risque de ne pas faire le poids face à des gouvernements qui n'ont que faire des règles, de la planète et dont les moyens financiers sont largement

supérieurs. Un des avantages possibles est certainement l'atout français d'une énergie décarbonée et relativement peu chère : le nucléaire civil. Je dis relativement, car quand on voit le coût de la dernière centrale EPR, on peut relativiser la formule. De plus, une petite anecdote, lors de la dernière GTX de NVidia qui présentait ces nouvelles puces Blackwell, des collègues et moi-même nous sommes amusés à calculer la consommation telle qu'elle était annoncée par NVidia sur l'environnement maximum de la technologie présentée. Nous sommes arrivés au résultat que cela demandait un dixième de production de cette dernière centrale EPR.

Cependant, on peut comprendre que cela attire le chaland puisque les Saoudiens envisagent très sérieusement d'investir sur un méga centre de données en France, du fait des dons de la bonne fée électricité.

Dans un article tiré du « GrandContinent », une revue d'étude éditée par le Groupe d'études géopolitiques, un centre de recherche indépendant domicilié à l'École normale supérieure et reconnu d'intérêt général, pour la France, un objectif minimal serait de sécuriser sur son territoire une capacité de calcul dédiée à l'IA équivalente à 10 % de celle des États-Unis, reflétant ainsi son poids relatif dans le PIB américain — soit environ 5-6 GW à horizon 2028. Si elle se fixait l'objectif de représenter 16 % — en proportion de son poids dans l'économie mondiale — de la puissance de calcul globale en IA à horizon 2030, elle devrait porter à 20 GW sa puissance énergétique dédiée à l'IA. Cela chiffrerait l'objectif français à 250-300 milliards d'euros d'investissements (soit plus de deux fois le montant de 109 milliards annoncés par le président Emmanuel Macron le 9 février) et l'objectif européen à 600-850 milliards.

La dernière fois que les États se sont mis en quatre comme cela, c'était pour acquérir le feu nucléaire et nous étions partis sur près de 70 ans de dissuasion. Aujourd'hui, avec la prolifération, de nombreux pays ont la bombe et on craint plus une bombe sale d'un groupe terroriste qu'un véritable bombardement de missiles nucléaires sur un pays. De la même manière, la course actuelle à l'intelligence artificielle n'empêchera pas les pays d'y accéder. Pour citer le lièvre et la tortue : *« rien ne sert de courir, il faut partir à point »*. Tout le discours au sujet de sujétion d'un état, du fait de l'avancement de l'IA d'un autre n'est que pure illusion servant des intérêts autres que ceux des populations vu la hauteur des investissements consentis. Il serait bon que, là aussi, soit préservée la raison et pas seulement les capacités de raisonnements de l'intelligence artificielle. □

IA L'AI Act entre en application en Europe

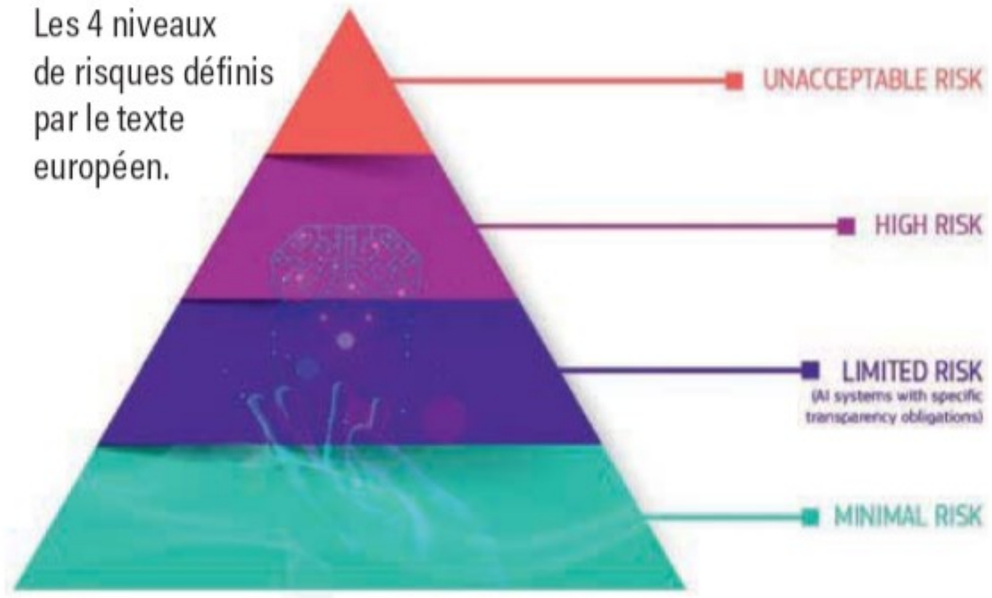
Depuis le 2 février 2025, les deux premiers chapitres du texte commencent à s'appliquer en Europe. A l'heure où les États-Unis et la Chine font feu de tout bois en la matière, ce règlement va cadrer, de manière extrêmement détaillée, le développement et les usages de l'IA sur le vieux continent. Un texte qui divise.

Faut-il favoriser l'innovation et laisser les start-ups et géants de la tech la bride sur le cou, ou protéger au maximum les citoyens contre les effets néfastes des IA ? L'Europe a clairement tranché. La loi sur l'IA européenne, le fameux AI Act, est entrée en vigueur le 1er août 2024 et ces différents chapitres vont entrer en application entre 2025 et 2027, puis sera réévalué en 2028. *« A la différence d'une directive qui doit être retranscrite en droit national, l'AI Act est un règlement. Son application est immédiate dans les 27 pays européens, et s'applique tant aux entreprises européennes qu'aux entreprises qui introduisent des produits d'IA sur le marché européen »* explique Maître Gérard Haas, avocat à la Cour, spécialiste en propriété intellectuelle et IA.

Pas de scénario à la Black Mirror ou Minority report possible

Le chapitre 1 du règlement évoque l'interdiction de systèmes d'IA qui déploient des techniques subliminales pour manipuler ou fausser le comportement des personnes. Il interdit aussi le fameux score social ou encore de créer un système d'IA pour évaluer le risque d'une personne à commettre une infraction pénale. Aucun état européen ne peut donc se doter d'une police Précrime à la Minority Report… De même, l'utilisation de systèmes d'identification biométrique à distance « en temps réel » dans des espaces accessibles au public est interdite à des fins répressives.

Les 4 niveaux de risques définis par le texte européen.



Outre ces IA strictement interdites, de nombreuses contraintes s'activent selon leur criticité, sur une échelle de quatre niveaux. *« À chaque niveau de risque correspond une liste d'obligations »*, précise Maître Haas. *« L'article 4 est très intéressant pour les entreprises qui mettent en place et déploient des IA, car il les oblige à former leurs collaborateurs afin de donner aux futurs utilisateurs de l'IA une maîtrise suffisante de l'outil. »*

Comme pour les autres textes européens, façon RGPD et NIS, un éventail de sanctions est défini pour les contrevenants. L'article 5 évoque 40 millions de dollars d'amende ou 7 % du chiffre d'affaires mondial de l'entreprise.

Si le calendrier de mise en application de l'AI Act suit son cours, le récent retrait de la proposition de texte sur la responsabilité sur les dommages liés aux IA a été considéré par beaucoup comme un recul vis-à-vis du lobbying des GAFAM. *« Ce retrait ne remet pas en cause l'AI Act, mais laisse un vide juridique »*, souligne l'avocat. *« Celui-ci pourrait néanmoins être comblé par un autre texte qui porte sur les produits défectueux. L'IA étant considérée comme un produit par l'UE, ce texte pourra s'appliquer aux applications et aux bugs inhérents aux logiciels, mais aussi aux IA et leurs biais. »* ☐

AC

MAÎTRE GÉRARD HAAS, AVOCAT À LA COUR, SPÉCIALISTE EN PROPRIÉTÉ INTELLECTUELLE ET IA

« L'approche de ce texte est intéressante dans la mesure où il considère l'intelligence artificielle comme étant un produit. Ce produit fait donc l'objet d'une régulation pour son développement, sa mise sur le marché et son utilisation. L'option retenue par le régulateur a été de définir quatre niveaux de risque, depuis les IA dont le risque est jugé minime et auxquelles aucune obligation spécifique n'est fixée, aux IA dont le risque est considéré comme inacceptable et dont l'usage est strictement interdit. Pour les IA qui présentent des risques spécifiques, elles impliquent des règles de transparence et les IA qui présentent un risque élevé, leur concepteur doit prévoir des systèmes d'atténuation des risques, la qualité des données d'entrainement. Il doit fournir des instructions claires aux utilisateurs. »

Unification

TP-Link Omada SDN : une solution réseau avancée pour les TPE et PME

Avec Omada SDN, TP-Link simplifie la gestion des réseaux pour les petites et moyennes entreprises, grâce à une plateforme centralisée. Accessible partout et à tout moment via une interface cloud unique, elle permet de superviser l'ensemble de l'infrastructure réseau. Grâce à son architecture Software Defined Networking (SDN), Omada offre un contrôle unifié des périphériques TP-Link, et s'adapte aussi bien aux environnements mono-site qu'aux déploiements multisites et multi-tenant.

Face aux exigences croissantes en matière de connectivité, de performance et de sécurité, les entreprises ont besoin de systèmes flexibles et intuitifs. Spécialisé dans les solutions réseau, TP-Link répond à cette demande avec une plateforme SDN (Software Defined Networking) évolutive pensée pour les TPE/PME. Omada SDN permet d'administrer à distance divers équipements TP-Link, tels que des routeurs VPN Multi-WAN, des switches administrables ou encore des points d'accès. Hébergé sur le cloud de TP-Link, le contrôleur Omada centralise leur gestion via une interface unique. Un gros avantage pour les entreprises multisites qui peuvent déployer et configurer leurs réseaux sans avoir à faire intervenir un technicien sur chaque site.

Installation et prise en main

Lors de notre test avec le routeur TP-Link VPN ER707-M2, le switch SG3210XHP-M2 et le point d'accès Wi-Fi 7 BE9300, nous avons pu constater à quel point l'installation se révèle simple et intuitive. Même avec des connaissances réseau limitées, quelques minutes suffisent pour configurer l'ensemble du matériel via l'interface Omada Cloud. La mise en service du routeur ER707-M2 peut toutefois nécessiter des ajustements en fonction du fournisseur d'accès : la configuration est automatique avec une Livebox Orange, tandis qu'il faut activer le mode « bridge » au préalable avec une Freebox, par exemple. Une fois branché à la box via un câble RJ45, le routeur garantit des performances réseau élevées (jusqu'à 10 Gbit/s), tout en offrant des options de sécurité avancées et une gestion centralisée via Omada SDN. Lancé récemment, le switch administrable SG3210XHP-M2 constitue un atout majeur pour concevoir une infrastructure réseau performante. Relativement compact, il dispose de huit ports RJ45 2,5G/PoE+ capables de connecter et alimenter divers équipements (points d'accès, caméras), ainsi que de deux ports SFP+ et un port micro-USB pour brancher d'autres switches ou un PC hôte.

Compatible avec la nouvelle bande 6 GHz, le point d'accès plafonnier TP-Link Wi-Fi 7 BE9300 offre quant à lui une connectivité sans fil ultra rapide pouvant atteindre jusqu'à 5760 Mbps. Il est équipé de deux ports 10 Gbit/s (PoE+) permettant de brancher des périphériques filaires tout en assurant une couverture Wi-Fi optimisée. Grâce à la technologie Omada Mesh, le réseau sans fil peut être étendu très facilement avec d'autres points d'accès TP-Link qu'il suffit ensuite de brancher au secteur.

Une gestion centralisée et intuitive

Après avoir créé gratuitement un compte via l'application mobile Omada (Android ou iOS) ou l'interface Web dédiée, il suffit de scanner les QR codes situés sous chaque périphérique TP-Link pour les intégrer individuellement au réseau. En quelques secondes, les appareils apparaissent dans le tableau de bord sur le cloud, prêts à être configurés. Outre une ergonomie simple et intuitive, celle-ci propose de nombreuses fonctionnalités avancées. L'administrateur peut mettre à jour les firmwares des équipements, surveiller la bande passante et prioriser certains flux, appliquer des politiques de sécurité, identifier et limiter

Grâce à Omada SDN, TP-Link s'impose comme un acteur majeur sur le marché des équipements réseau destinés aux TPE et PME.

l'accès des appareils connectés (smartphones, tablettes, ordinateurs, caméras IP…), analyser les performances du réseau via des outils de reporting détaillés, etc.

Sécurité et segmentation avancée

La sécurité constitue l'un des éléments clés des infrastructures réseau. La solution Omada SDN intègre des fonctionnalités avancées telles que l'authentification 802.1X, la segmentation VLAN pour isoler les différents types de trafic, et l'option de portail captif pour les réseaux invités. Avec le routeur VPN ER707-M2, les entreprises bénéficient d'un chiffrement de bout en bout via les protocoles VPN (IPsec, OpenVPN, WireGuard…) qui garantissent une connexion sécurisée. La solution prend également en charge des fonctions de détection et de prévention d'intrusion (IDS/IPS) pour renforcer la protection du réseau contre les cybermenaces.

Une solution évolutive, mais limitée à l'écosystème de TP-Link

Grâce à son architecture modulaire, Omada SDN permet aux entreprises d'adapter leur infrastructure réseau en fonction de leur croissance. L'ajout de nouveaux équipements (switches, bornes Wi-Fi…) se fait en toute transparence et sans interruption de service. Les derniers équipements compatibles Wi-Fi 7 de la marque, comme le plafonnier TP-Link Wi-Fi 7 BE9300, garantissent un débit très rapide et une gestion optimisée des connexions simultanées. TP-Link commercialise une large gamme de bornes (intérieures et extérieures), de plafonniers, et d'antennes sans fil permettant d'assurer une excellente couverture Wi-Fi dans différents types d'environnements. Pour accompagner les utilisateurs novices ou plus expérimentés, TP-Link propose un support technique en français, des tutoriels vidéo et une documentation détaillée. Bien que la solution Omada SDN offre une gestion centralisée efficace, elle est exclusivement compatible avec le matériel TP-Link. Cette dépendance peut constituer un frein pour les entreprises disposant déjà d'équipements réseau d'autres marques.

Conclusion

Avec Omada SDN, TP-Link fait face à des concurrents comme Ubiquiti UniFi, Cisco Meraki ou Aruba Instant On. Ubiquiti propose une solution comparable avec une gestion cloud avancée et une flexibilité matérielle plus large. Cisco Meraki et Aruba Instant On, quant à eux, offrent des fonctionnalités réseau et de sécurité plus avancées, mais reposent sur des modèles avec abonnements. L'offre de TP-Link constitue une option intéressante pour les petites et moyennes entreprises souhaitant centraliser et sécuriser leur réseau tout en maîtrisant leur budget. Omada SDN est en effet gratuit, et les équipements réseau professionnels de TP-Link affichent des tarifs souvent plus compétitifs que ceux de la concurrence. Cette attractivité s'accompagne toutefois d'une certaine dépendance à l'écosystème de la marque. □

J.C

CARACTÉRISTIQUES TECHNIQUES

ROUTEUR VPN OMADA TP-LINK VPN ER707-M2

- 2 ports 2,5 G : 1 port WAN 2,5 G et 1 port WAN/LAN 2,5 G
- 6 ports WAN
- VPN : SSL/IPSec/PPTP/L2TP et OpenVPN
- Intégré à Omada SDN : provisionnement sans contact (ZTP), gestion centralisée du cloud, surveillance intelligente…
- Fonctions de sécurité étendues : pare-feu avancé, défense DoS, filtrage IP/MAC/URL…
- Prix : 283 €

SWITCH TP-LINK SG3210XHP-M2

- 8 ports PoE+ 2,5G
- 2 emplacements SFP+ 10 Gbit/s
- Intégré à Omada SDN : Zero-Touch Provisioning (ZTP), gestion centralisée du cloud et surveillance intelligente
- Stratégies de sécurité robustes : liaison IP-MAC-port, ACL, sécurité des ports, DoS Defend, contrôle des tempêtes, surveillance DHCP, 802.1X, authentification
- Applications vocales et vidéo : QoS L2 / L3 / L4 et surveillance IGMP
- Prix : 426 €

POINT D'ACCÈS TP-LINK WI-FI 7 BE9300 TRIBANDE

- Wi-Fi 7 tri-bande : 5 760 Mb/s (6 GHz) + 2880 Mb/s (5 GHz) + 574 Mb/s (2,4 GHz)
- 1 port LAN 10 Gbit/s
- Bande 6 GHz
- Bande passante 320 GHz
- Prise en charge de la gestion centralisée Omada SDN, maillage et itinérance IA
- Prix : 250 €

Supervision

L'AIOps transformera les réseaux d'entreprise en 2025

L'IA génère des volumes de trafic réseau inédits, nécessite une latence ultra-faible et introduit des couches de complexité supplémentaires. Pour les opérateurs réseau, c'est un véritable défi. Heureusement l'AIOps est là, et elle nous sauvera tous. Nous allons voir, dans cet article, quels sont ses composants clés, ses avantages, mais aussi ses défis et ses perspectives.

L'année 2025 devrait être charnière pour l'industrie des réseaux, poussée par les innovations liées à l'utilisation de plus en plus intensive de l'IA. Les fusions, les transformations technologiques et les nouvelles solutions intégrées redéfinissent les contours d'un secteur en pleine effervescence. Le secteur des réseaux a longtemps été un domaine relativement stable. Puis, sont arrivés les « agents perturbateurs », l'IA, ChatGPT et la GenAI qui ont tout bouleversé. L'AIOps est l'IA qui va régler les problèmes introduits par… l'IA, mais pas seulement.

Quelle définition de l'AIOps ?

L'AIOps (le terme aurait été inventé par le cabinet d'études Gartner en 2016) est l'abréviation de Artificial Intelligence for IT Operations. Cette méthodologie associe des techniques d'IA, le machine learning et l'analyse de données en vue d'améliorer et d'automatiser les opérations informatiques. L'AIOps s'appuie sur des algorithmes avancés, afin d'analyser en temps réel de grands volumes de données générées par les systèmes informatiques et les composants d'infrastructure. Cette analyse est censée fournir des analyses prédictives, des informations exploitables et des capacités de self-healing, pour optimiser les performances des systèmes informatiques et améliorer la fiabilité et les délais de résolution. L'AIOps est très souvent utilisé comme outil de supervision afin de déterminer quelles ressources doivent être prises en charge par quelles applications et comment les interconnecter. L'analyse des données recueillies et du trafic réseau en temps réel permet de réagir très rapidement aux cyber-incidents, réduisant ainsi les risques d'intrusions, d'infections et de vols de données. Les fonctionnalités des plateformes AIOps de pointe garantissent la fiabilité des services dans tous les domaines du réseau : filaire, sans-fil, SD-WAN, WAN Edge, datacenters et sécurité. Elles garantissent que les connexions réseau sont fiables, mesurables et sécurisées, accroissent l'efficacité et la productivité des opérateurs réseau, et améliorent l'expérience des utilisateurs finaux.

Révolutionner vos opérations informatiques grâce à l'IA

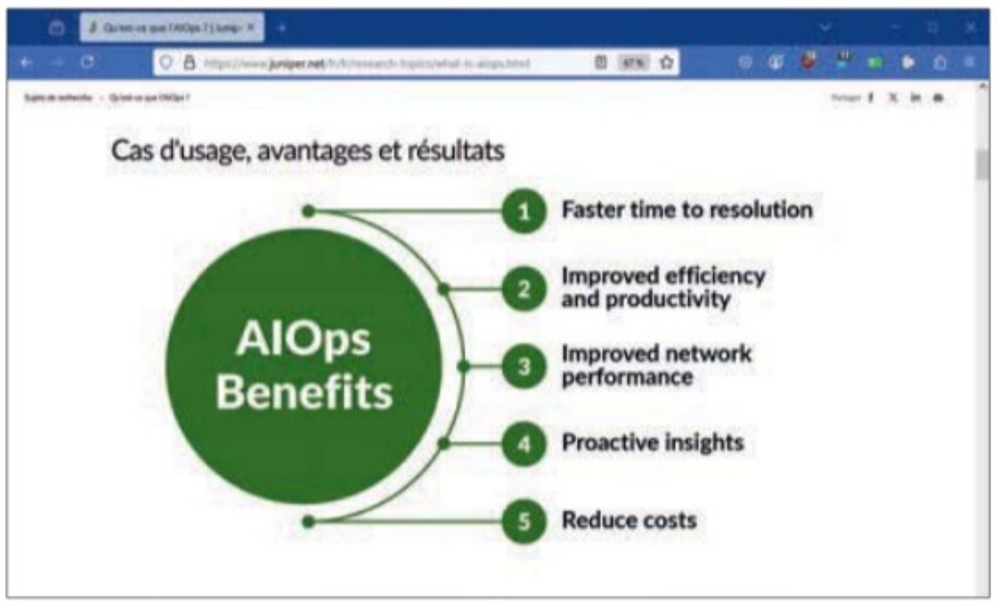
Les mutations technologiques ainsi que d'autres facteurs impactent la DSI, rendant les environnements IT toujours plus complexes et les exigences des utilisateurs et des organisations de plus en plus élevées. C'est pourquoi les méthodes traditionnelles de gestion des infrastructures informatiques ne suffisent généralement plus. De nouveaux processus doivent être mis en place en vue de fournir aux entreprises les ressources dont elles ont besoin aussi bien en amont qu'en aval pour rester compétitives. C'est pour cette raison que les organismes doivent exploiter sans attendre la puissance de l'IA et du machine learning.

Les opérations IT (ITOps)

Les opérations IT sont les processus de gestion, d'implémentation et de support des services informatiques. Elles sont indispensables à toute entreprise souhaitant prendre en charge son infrastructure informatique afin de répondre aux besoins des utilisateurs, de l'implémentation de nouvelles technologies à la supervision du réseau et

LES DÉFIS ET ENJEUX DE L'AIOPS

L'adoption d'une nouvelle technologie se faisant rarement sans difficultés, voici les principaux défis soulevés par l'AIOps :
Qualité et intégration des données : l'AIOps s'appuie sur des données de qualité provenant de sources multiples. L'intégration de solutions informatiques connexes permettra de garantir une bonne communication entre ces données, leur exactitude, leur cohérence et la compatibilité des données ne sera pas une moindre tâche.
Les compétences : la maîtrise d'une solution AIOps nécessite des compétences en Data science, en ML et dans d'autres technologies de l'IA. Les collaborateurs devront être formés pour être efficaces ou il faudra embaucher des personnes ayant déjà ces aptitudes.
Gestion du changement : l'AIOps nécessitera des changements culturels et organisationnels profonds. La sensibilisation du personnel sera essentielle.
Sécurité et confidentialité : l'AIOps nécessite la collecte, le traitement et l'analyse de données sensibles des organismes. La prudence doit être de mise et la sécurité de ces données doit être garantie.



Les cas d'usage, avantages et résultats de l'AIOps présentés par Juniper avec sa solution Mist AI.

des applications, en passant par la réalisation de sauvegardes de données et la résolution automatique des incidents. Le rôle de l'ITOps est de s'assurer que tous les systèmes informatiques de l'entreprise fonctionnent de manière fluide et optimale, sans interruption de service, tout en maintenant les systèmes sécurisés et conformes. Une interruption de services ou une faille de sécurité peuvent impacter l'ensemble d'une organisation. C'est pour cela qu'elles doivent être traitées rapidement. Elles peuvent impacter financièrement l'ensemble de l'entreprise mais aussi ses clients. Afin d'éviter ou de réduire les temps d'arrêt, des solutions ITOps robustes doivent être mises en place. L'utilisation de l'IA dans la gestion des opérations IT améliorera l'efficacité de ces processus. Dans un environnement informatique de plus en plus complexe, l'AIOps réduit les temps d'interruption et accélère la résolution des problèmes.

Les composants clefs de l'AIOps

L'AIOps permet de connecter votre environnement informatique multimodal, en regroupant des équipes jusqu'alors cloisonnées et en intégrant les outils d'opérations IT d'une organisation dans un environnement informatique unique. Elle crée un espace commun et partagé pour superviser les performances et les processus des applications. L'AIOps utilise les données collectées pour détecter les problèmes et agir le plus rapidement possible. Les principaux composants de l'AIOps, et la manière dont chacun d'entre eux affecte votre environnement informatique sont les suivants :

La collecte des données : l'AIOps permet de collecter des données provenant des multiples sources de l'écosystème informatique de l'entreprise grâce à des agents de collecte et des API. L'AIOps utilise notamment les données historiques sur les performances et les incidents, ainsi que celles portant sur l'infrastructure IT.

Le traitement des données : une fois les données collectées, elles doivent être traitées et normalisées pour en garantir la cohérence. Des techniques d'analyse avancées sont employées comme la détection d'anomalies, l'analyse de corrélation et la reconnaissance de formes en vue d'identifier les informations intéressantes et de dégager des tendances.

Les modèles de machine learning : les modèles de ML sont employés pour analyser les données historiques. Le but est de prédire les problèmes ou anomalies pouvant survenir, d'anticiper par exemple une panne de serveur.

L'analyse des causes premières : l'AIOps rationalise le processus de résolution d'incidents et des problèmes IT en recherchant — et en trouvant — leurs causes premières. Ainsi les équipes informatiques peuvent identifier les malfaçons dans l'architecture IT de leur organisation.

Automatisation et orchestration — L'AIOps permet d'automatiser les tâches courantes et les workflows, et de réduire ainsi l'intervention humaine.

Les bénéfices de l'AIOps

L'objectif à long terme de l'AIOps est l'automatisation des opérations informatiques afin de faciliter l'auto-supervision, le self-healing et l'optimisation des systèmes IT sans intervention humaine. Ainsi les équipes IT pourront se concentrer sur des sujets stratégiques et sur des tâches à plus forte valeur ajoutée que la résolution d'incidents 1000 fois répétés. A plus court terme, l'AIOps permet de mieux gérer un environnement IT de plus en plus complexe et de réagir plus rapidement en cas d'incidents. Les quelques avantages clefs de l'AIOps peuvent être résumés ainsi :

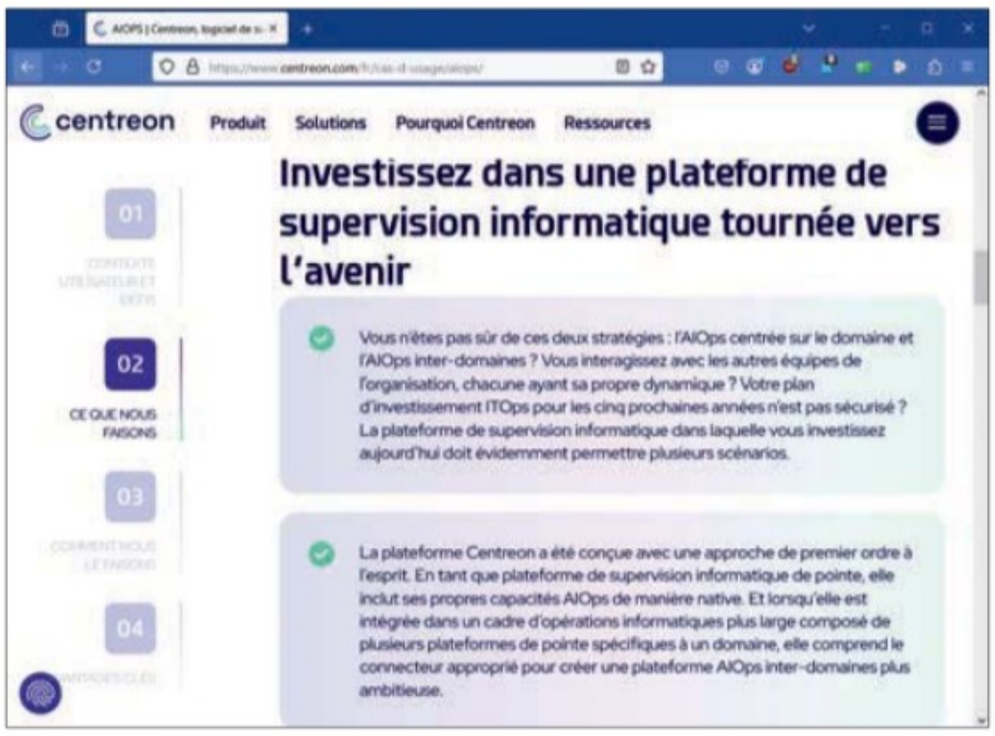
Une visibilité améliorée : l'AIOps apporte une visibilité complète sur l'ensemble de l'infrastructure informatique, permettant de gérer plus efficacement les environnements IT complexes.

La résolution proactive des problèmes : Les problèmes et incidents peuvent être identifiés et même anticipés avant qu'ils n'aient un impact sérieux sur les opérations de l'organisation, minimisant ainsi les interruptions de service et les temps d'arrêt des serveurs en permettant même de les planifier s'ils sont inévitables.

Une efficacité accrue : L'automatisation permet aux équipes informatiques de se concentrer sur des sujets stratégiques et les tâches à forte valeur ajoutée, plutôt que sur des tâches redondantes. Les techniciens Réseau et Système auront plus de temps pour monter en compétences dans différents domaines, dont l'IA en général et l'AIOps en particulier.

L'évolutivité : L'AIOps s'adapte aisément aux volumes croissants des données et à la complexité grandissante des infrastructures. □

T.T



La plateforme Centreon suit elle aussi la mode du moment et intègre l'AIOps.

Dynatrace Perform

Une observabilité préventive pour un cloud plus sécurisé

Lors de la conférence, le spécialiste de l'observabilité a dévoilé de nouvelles fonctionnalités pour ses outils avec, en toile de fond, l'expansion de Davis AI.

Les innovations incluent « Observability for Developers », avec un Live Debugger pour un débogage lors de la production sans interruption, et Cloud Security Posture Management (CSPM) pour une sécurité automatisée. Grâce à l'IA prédictive et à l'automatisation, Dynatrace entend simplifier la gestion IT et renforcer la résilience des entreprises.

Anticiper plutôt que prévoir

Dynatrace a introduit plusieurs améliorations à ses solutions dans le but d'accroître les opérations informatiques, la productivité des développeurs et la sécurité du cloud à de nouveaux niveaux. Ces innovations positionnent Davis AI, le moteur d'intelligence artificielle développé par Dynatrace, au cœur d'un changement de paradigme : passer d'une approche réactive à une approche préventive, permettant aux entreprises et organisations d'anticiper et de prévenir les problèmes informatiques au lieu de simplement y réagir.

Devant plusieurs milliers de personnes présentes sur place ou devant leur écran, Dynatrace a dévoilé « Observability for Developers », un ensemble d'outils conçu pour offrir aux développeurs logiciels des informations clés en temps réel, un débogage piloté par l'IA et un Live Debugger innovant et très intéressant, éliminant de nombreuses difficultés traditionnelles du dépannage des applications en production. De plus, l'entreprise a élargi son portefeuille de sécurité avec une nouvelle solution de Cloud Security Posture Management (CSPM), permettant aux entreprises de surveiller en continu leur conformité, d'automatiser les flux de travail de sécurité et d'intégrer les insights de sécurité aux données d'observabilité globales. Cette approche garantit que les environnements cloud restent résilients, sécurisés et efficaces.

Automatisation, intelligence contextuelle et IA

Avec l'ensemble de ces innovations, Dynatrace a réaffirmé son engagement en faveur d'une observabilité unifiée, une stratégie qui intègre l'IA, l'automatisation et l'intelligence contextuelle à travers les équipes IT, de développement et de sécurité pour accroître l'agilité métier et l'efficacité opérationnelle. Depuis plus d'une décennie, Dynatrace est à la pointe des opérations informatiques pilotées par l'IA, améliorant en permanence son moteur Davis AI pour automatiser l'analyse, optimiser l'infrastructure et réduire le MTTR (Mean Time To Resolution). Cependant, les dernières avancées marquent un tournant important : le passage d'une AIOps réactive à des opérations véritablement préventives.

En effet, la surveillance informatique traditionnelle repose sur la détection et la réponse aux incidents, au fur et à mesure qu'ils se produisent. Mais dans des environnements numériques hypercomplexes et distribués, les entreprises ne peuvent plus attendre une panne avant d'agir. Les interruptions de service peuvent entraîner des pertes financières de plusieurs millions d'euros, une atteinte à la réputation et une perte de confiance des clients. Grâce à l'AIOps préventive, Davis AI permet aux entreprises d'anticiper et de corriger les problèmes potentiels, avant qu'ils n'impactent les opérations.

Davis AI s'enrichit de nouvelles fonctionnalités

Parmi les dernières mises à jour de Davis AI, Dynatrace a inclus des artefacts générés par l'IA pour la remédiation automatisée. Avec cela, Dynatrace peut désormais générer automatiquement des ressources de déploiement Kubernetes, ajustant dynamiquement les limites de processeurs et de mémoire en fonction des modèles

© Dynatrace

Comme toujours, Bernd Greifeneder, directeur technique de Dynatrace, a fait le show, lors du keynote de présentation des innovations de l'entreprise.

© Dynatrace

Les quelque milliers de participants ont pu découvrir les innovations de Dynatrace dans la zone d'exposition avec de nombreuses démonstrations. Les principales nouveautés seront disponibles d'ici 90 jours environ.

d'utilisation en temps réel. Les ressources ne sont ainsi ni surapprovisionnées, ni sous-approvisionnées, éliminant les inefficacités avant qu'elles ne deviennent critiques. Autre nouveauté : l'analyse avancée des causes racines avec explications en langage naturel. Davis AI fournit désormais des résumés de problèmes et des recommandations contextuelles en langage clair, permettant aux équipes de comprendre rapidement ce qui s'est passé, pourquoi cela s'est produit et comment le résoudre — sans nécessiter une expertise technique approfondie.

Pour finir, Dynatrace s'appuie sur des capacités prédictives de l'IA, afin de garantir des opérations véritablement préventives. Ainsi, Davis AI prédit le comportement futur des systèmes en se basant sur les données historiques d'observabilité et la télémétrie en temps réel, permettant des corrections proactives avant qu'un incident ne survienne. *« Le passage d'opérations réactives à préventives représente la prochaine évolution de l'AIOps »*, a déclaré Bernd Greifeneder, directeur de Dynatrace. *« Il ne s'agit pas seulement de détecter plus tôt les problèmes ou de les résoudre plus rapidement : il s'agit de prévenir les problèmes avant même qu'ils ne se produisent »*, a-t-il encore ajouté.

Productivité et débogage pilotés par l'IA

A mesure que le développement d'applications cloud-native devient plus complexe, les développeurs ont besoin d'une observabilité en temps réel pour garantir la performance, la sécurité et la fiabilité de leurs logiciels. L'initiative Observability for Developers apporte des bases de connaissance pilotées par l'IA, directement entre les mains des ingénieurs, leur permettant de déboguer, d'optimiser et de déployer leurs applications plus efficacement que jamais.

Une des fonctionnalités les plus marquantes de cette nouvelle offre est le Live Debugger, qui permet de définir des points d'arrêt dans leur code, sans stopper l'exécution. Contrairement au débogage traditionnel, qui nécessite souvent de reproduire un problème dans un environnement de test, Live Debugger permet d'analyser le code en temps réel, en production, sans interruption. *« Live Debugger donne aux développeurs un nouveau superpouvoir »*, a assuré Bob Wambach, vice-président de la stratégie produit chez Dynatrace. *« Vous pouvez inspecter votre code sans arrêter son exécution, rendant le dépannage plus rapide et plus facile que jamais »*, a-t-il encore expliqué.

En 2025, Dynatrace s'attaque également à un problème majeur rencontré par les équipes de développement : l'excès d'outils et la complexité d'intégration. Grâce à un nouveau modèle d'observabilité en libre-service, les équipes peuvent intégrer sans effort la surveillance pilotée par l'IA, les logs OpenTelemetry enrichis, les métriques et les traces dans leurs flux de travail, tout en garantissant des actions en conformité avec les règles de gouvernance des différents pays ou secteurs.

Conformité automatisée et atténuation des risques

Dans un autre registre, la sécurité reste l'un des plus grands défis pour les entreprises opérant dans des environnements hybrides et multi-cloud. Dynatrace élargit son portefeuille de sécurité avec une solution de CSPM, offrant une surveillance continue de la conformité, une priorisation des risques et une remédiation automatisée. Parmi les principales fonctionnalités de Dynatrace CSPM, on peut citer la surveillance continue des normes réglementaires qui permet une prise en charge des cadres de conformité, tels que PCI DSS, CIS, RGPD et autres cadres, garantissant que les déploiements cloud restent sécurisés et conformes.

Autre fonctionnalité : la priorisation des risques, pilotée par l'IA. Ainsi, Davis AI vient classer automatiquement les menaces de sécurité en fonction de leur impact sur l'activité, permettant aux équipes de se concentrer sur les vulnérabilités les plus critiques. Pour finir, il faut également évoquer la remédiation automatisée qui permet d'appliquer les politiques de sécurité de manière proactive avec une auto-réparation automatique, réduisant ainsi l'intervention humaine. *« Avec notre approche unifiée, les entreprises bénéficient d'une solution unique pour des insights de sécurité continus, une analyse des risques pilotée par l'IA et une remédiation automatisée »*, analyse Steve Tack, directeur des produits de Dynatrace.

Bref, avec les nouvelles capacités de Davis AI, « Observability for Developers » et la solution CSPM, Dynatrace continue de transformer la gestion de la complexité numérique, en rendant les opérations toujours plus intelligentes, automatisées et sécurisées. Des actions qui permettent ainsi de réduire la charge de travail des équipes et de leur permettre de se focaliser sur des tâches importantes. Ces nouveaux produits seront disponibles d'ici trois mois environ. □

Michel Chotard

Orchestration

Workday centralise le pilotage des agents IA

L'éditeur spécialisé dans les ressources humaines et les outils pour les directions financières vient de dévoiler Illuminate, une solution centralisée pour piloter l'ensemble des agents IA d'une entreprise, qu'ils soient développés par Workday ou par des tiers.

La plate-forme donne la capacité aux entreprises de piloter l'ensemble de leurs agents IA — qu'ils soient créés par Workday ou des tiers — depuis une interface unique. Une solution qui arrive au bon moment et qu'une majorité d'éditeurs de logiciels lancent leurs agents IA alors que la multiplication des agents complexifie le déploiement, la sécurité, s'assurer de leur conformité tout en maximisant leur impact et en serrant les coûts. Illuminate propose une approche structurée pour intégrer les agents IA, définir leur périmètre d'action, mesurer leurs résultats, anticiper les coûts et favoriser leur évolution. En centralisant la gestion des agents IA utilisés dans l'entreprise, les dirigeants peuvent disposer d'une vision claire et d'un contrôle total sur l'impact de l'IA dans leur organisation.

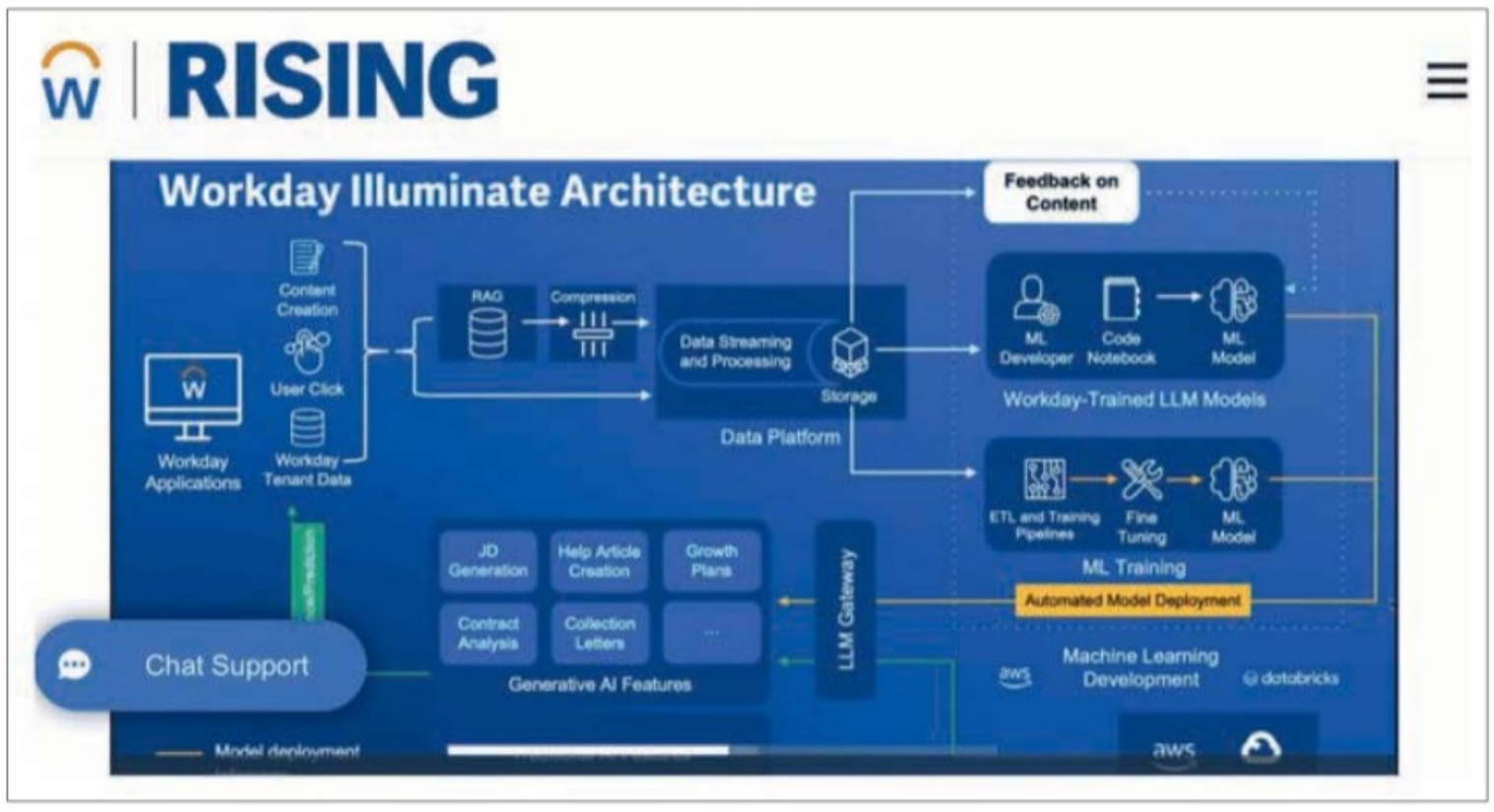
Les bénéfices attendus

Outre la simplification de la gestion des agents, la plate-forme simplifie l'intégration pour proposer un déploiement rapide des nouveaux agents avec des rôles et compétences définis, et un accès sécurisé aux données pertinentes, accélérant les délais de rentabilisation. Ces déploiements sont sécurisés grâce à une configuration automatisée, des contrôles d'accès rigoureux et une conformité aux politiques pour réduire les risques. Illuminate apporte aussi une visibilité en temps réel sur le suivi des activités, l'application des règles et contrôle des coûts pour une performance et un retour sur investissement optimal. Elle effectue une vérification continue de l'identité des agents, de leur orchestration et des coûts financiers pour une performance optimale. Des fonctions permettent de budgétiser, de prévoir et d'optimiser le retour sur investissement de l'utilisation des agents IA.

Des agents pour optimiser les processus métiers

En plus de la plate-forme, l'éditeur étend son panel d'agents IA. Contrairement aux agents actuels du marché qui sont conçus pour gérer des tâches spécifiques et pour suivre des instructions prédéfinies, les agents Workday disposent d'un ensemble de compétences configurables leur conférant plus d'autonomie pour accompagner efficacement les collaborateurs dans leurs missions. Chaque agent peut exécuter des centaines de tâches distinctes. Les nouveaux agents se positionnent sur différents processus. Contracts Agent analyse en permanence l'ensemble des contrats de l'entreprise, détecte les obligations et opportunités cachées dans les données non structurées, et génère des actions concrètes pour créer de la valeur et réduire les risques. Payroll Agent détecte et rectifie les anomalies liées à la paie, automatise les audits, fournit des insights et propose des solutions, tout en veillant à la conformité. Financial Auditing Agent optimise les processus et réduit les risques lors des missions d'audit en reliant intelligemment les documents complexes pour suivre les transactions, rapprocher les comptes et contrôler les processus internes. Cela permet aux cabinets d'audit de développer des applications directement connectées à leurs clients Workday. Enfin, Policy Agent assimile en continu les dernières mises à jour des politiques d'entreprise et les communique de manière proactive aux collaborateurs et responsables en fonction de leurs besoins. Les différents agents sont disponibles sur la place de marché de l'éditeur. À l'avenir, clients et partenaires pourront également enrichir, personnaliser et compléter les agents IA qui s'intégreront à Workday grâce à la plateforme de développement Workday Extend. Ces différents produits seront en disponibilité générale au cours de cette année. □

B.G



L'architecture de Workday illuminate.

Processus métiers

Oracle généralise les agents dans ses solutions

Oracle tire à feu tendu avec des agents IA pour la plupart de ses solutions cloudifiées : chaîne d'approvisionnement, gestion RH et expérience clients sont les derniers exemples.

La logistique vit aussi sa révolution par l'intelligence artificielle. L'éditeur présente différents agents qui vont enrichir sa solution Fusion Cloud Supply Chain and Manufacturing. Transportation Management aide les responsables du transport à prévoir les temps d'arrivée optimaux, à éviter les ports encombrés et à prévenir les retards douaniers en identifiant les itinéraires d'expédition les plus rentables. De plus il vient en support pour améliorer la planification des expéditions et à réduire les coûts associés aux retards en identifiant les expéditions à risques et en partageant les prévisions d'arrivée en temps réel. Il permet aux responsables des transports d'identifier des itinéraires maritimes plus durables et plus économes en énergie en calculant les émissions de transport pendant le processus de planification des expéditions.

Dans le même ordre d'idée Global Trade Management allège le traitement des programmes d'incitations commerciales afin de mieux utiliser les programmes de ristourne de droits et à atténuer l'impact des tarifs sur la supply chain en suivant les marchandises et les droits de l'importation à l'exportation. Voilà qui devrait faire un tabac pour tous ceux qui exportent vers les USA ! De plus la solution génère rapidement les données et les rapports requis pour préparer et déposer les demandes de ristourne auprès des autorités douanières.

Pour les spécialistes des commandes Order Management fournit des mises à jour de statut précises et dans les temps pour les commandes retournées en récapitulant toutes les informations pertinentes sur les commandes, y compris les caractéristiques des articles et les commentaires utilisateur. Le module réalise aussi le récapitulatif des promotions générées par l'IA et vérifie la disponibilité des articles ainsi que d'affiner les dates de livraison de commande avec une visibilité sur les retards potentiels ou les problèmes d'autorisation.

Et pour les RH ?

Les nouveaux agents d'IA automatisent des workflows fastidieux de bout en bout pour libérer le potentiel humain et donner plus de temps aux collaborateurs pour des tâches plus utiles. Intégrés à Oracle Cloud HCM, ils permettent d'améliorer l'expérience collaborateur et de stimuler la productivité en fournissant une assistance professionnelle personnalisée, en automatisant les tâches administratives et en rationalisant de nombreux processus complexes, de l'intégration et des contrats aux analyses de performances et avantages. Les nouveaux agents d'IA prennent en charge les plans de carrière, assiste le salarié à définir et à atteindre ses objectifs de performance. Par exemple, l'agent peut suggérer des moyens d'améliorer la rédaction des objectifs et d'élaborer des plans potentiels pour aider les collaborateurs à suivre le rythme pour atteindre les objectifs avant les analyses de performances. Il peut aussi apporter son support pour trouver des opportunités de formation pour faire progresser leurs compétences et leur carrière.

Les autres agents dévoilés concernent la gestion des rémunérations et des avantages, le cycle de vie du collaborateur dans l'entreprise. □

B.G

Les processus et tâches de Global Trade Management.

Identité

Memority présente sa feuille de route

Lors des Memority Days, la conférence des clients et partenaires de l'éditeur, il a été présenté les futures pistes de développement du spécialiste de la gestion des identités.

Le développeur de l'Identity Factory, une plateforme permettant de suivre et de gérer les identités sous tous ses aspects réunissait sa communauté et a présenté l'évolution de son modèle opérationnel qui s'appuie sur les partenariats dont le plus important peut être avec S3NS. L'idée est de créer un écosystème dynamique autour d'événements, de relations et de partenariats. Première annonce le support de b.connect le service d'authentification sans mot de passe développé par 5 banques de la place afin de limiter la fraude.

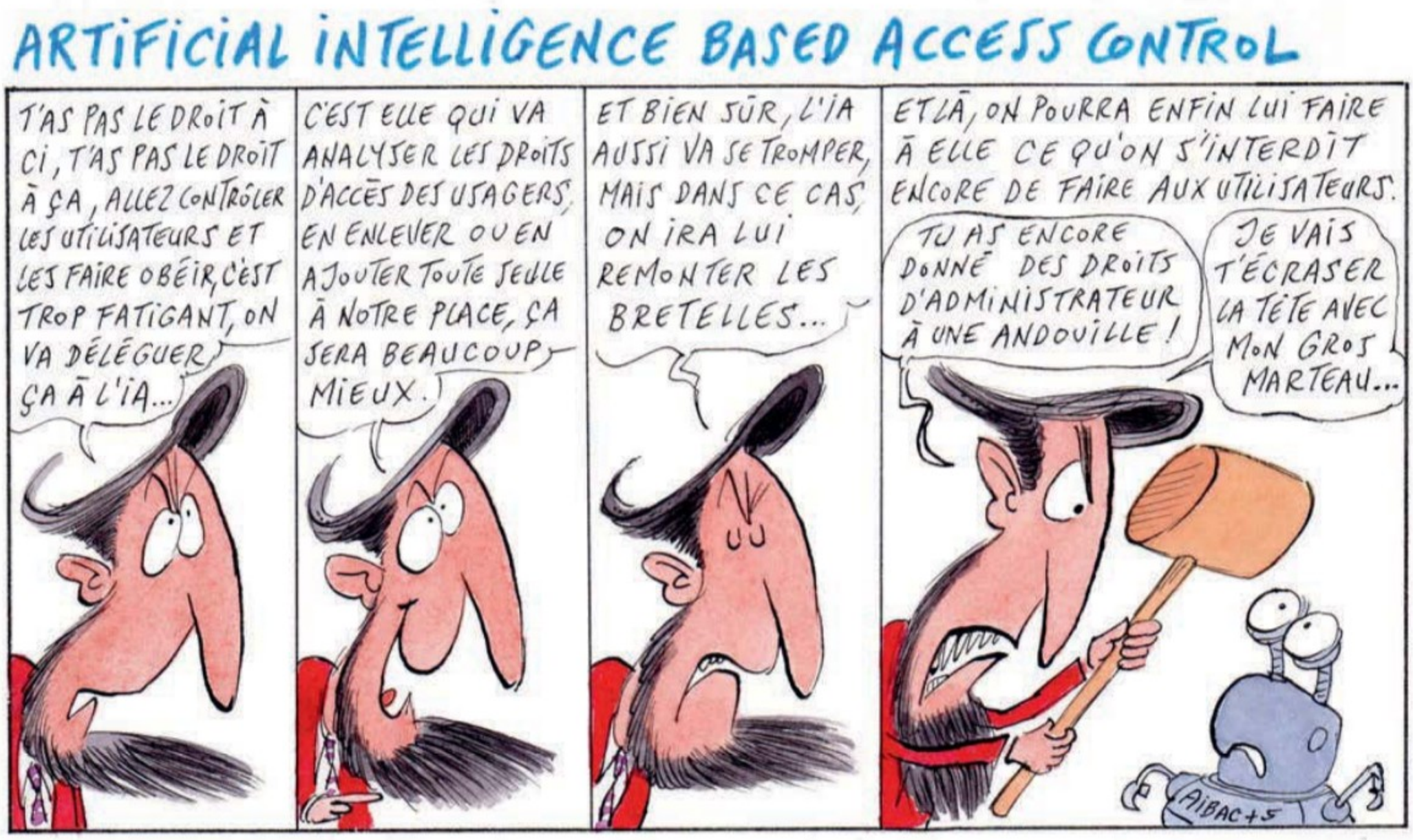
IDaaS est mort ! Longue vie à IDaaS

Véritable pionnier de l'authentification IDaaS, Memority reconnaît les limitations de la norme pour certains cas d'usages. Son modèle statique n'est pas la réponse attendu dans le contexte actuel de la cybersécurité. Après ce constat, l'éditeur a donc dévoilé les pistes de ses prochains développements autour de 4 axes principaux : l'acquisition de nouvelles certifications (SecNumCloud et EUCS), améliorer l'expérience utilisateur avec des dashboards, l'identification des risques sur les identités et une place de marché. Sans surprise Memority va ajouter de l'intelligence artificielle pour la détection des identités non conformes par exemple. De plus un ITDR (Identity Threat Detection & Response) et un CIEM (gestion des droits d'accès à l'infrastructure Cloud) sont dans les cartons.

AIBAC arrive

On connaissait beaucoup de type de gestion des accès, le principal étant aujourd'hui le Role Based Access, l'accès donné selon le rôle que vous avez dans l'entreprise. L'inconvénient de ce modèle est qu'il est statique. Memority vise donc à laisser l'IA faire ce travail mais avec des interactions avec l'IA afin d'affiner le modèle. Ce modèle permettrait d'avoir des réponses en temps réel en cas de menace. Le modèle prend d'ailleurs plus de paramètres en ligne de compte et réalise une authentification en continu à partir d'informations de contexte sur la situation et sur l'historique de l'identité. Ces différentes innovations devraient trouver leur place dans la version 3 de l'éditeur qui s'échelonnera sur le période de 2025 à 2027. □

B.G



Firewall

Cloudflare muscle son WAF pour protéger les LLM

Cloudflare a ajouté une fonction de sécurisation des LLM dans son WAF (Web Application Firewall). Appelée Firewall for AI, elle analyse les requêtes et évite leur exploitation malveillante. Nous allons voir, dans cet article, quels sont ses principes de fonctionnement.

Les spécialistes du cloud et de la cybersécurité se penchent, telles de bonnes fées, sur la protection des modèles de langage de grande taille, les fameux LLM (Large Language Model). Le dernier en date est Cloudflare qui a mis à jour son WAF — son firewall applicatif — en y ajoutant une fonction baptisée Firewall for AI. Celle-ci a été spécialement conçue pour les applications utilisant des LLM. Elle est constituée d'outils WAF existants et de nouvelles capacités à analyser les invites soumises, et d'identifier les tentatives d'exploitation frauduleuses.

Le pare-feu WAF de Cloudflare met en œuvre les informations sur les menaces et l'apprentissage automatique pour bloquer les dernières menaces, y compris zero-day.

Une protection pour les développeurs

Avec Firewall for AI, Cloudflare propose la protection des LLM aux utilisateurs de Workers AI, sa plateforme serverless pour développeurs. Cette barrière de sécurité a pour fonction de détecter les tentatives d'attaques, avant qu'elles ne ciblent ces modèles d'IA spécialisés dans l'interprétation du langage humain et d'autres formes de données complexes. Le pare-feu WAF de Cloudflare met en œuvre les informations sur les menaces et l'apprentissage automatique (Machine Learning), le tout soutenu par l'intelligence de plateforme du cloud de connectivité de Cloudflare, pour bloquer les dernières menaces, y compris zero-day. Le réseau mondial de Cloudflare traite quelque 100 millions de requêtes HTTP par seconde (en pic). Cela lui permet clairement de proposer une protection inégalée contre les attaques, même les fameuses zero-day. *« À chaque avancée technologique correspondent de nouvelles menaces. Ce constat est également valable pour les technologies propulsées par l'IA. Avec notre service Firewall for IA, nous entendons intégrer la sécurité dès le début dans l'écosystème de l'IA »*, a déclaré Matthew Prince, cofondateur et PDG de Cloudflare. Du fait de leur capacité à traiter d'énormes quantités de données et à générer du texte, les LLM sont exposés à plusieurs types d'attaques bien spécifiques.

Des attaques spécifiques

Ces attaques peuvent viser soit à exploiter les vulnérabilités inhérentes à ces modèles, soit à profiter de leur fonctionnement pour mener à bien des actions malveillantes. Les attaques par injection de données, par exemple, consistent à introduire des données malveillantes ou trompeuses durant le processus d'apprentissage du modèle, dans le but de le manipuler pour qu'il génère des réponses biaisées ou inappropriées. Les modèles peuvent également être exploités pour générer du contenu trompeur comme des fake news, des escroqueries par hameçonnage ou toutes autres formes de contenus malveillants en exploitant leur capacité à créer des éléments crédibles, texte, son ou vidéo. *« Firewall for AI est agnostique par rapport au déploiement spécifique. Il peut être employé pour protéger des modèles hébergés sur Cloudflare Workers AI, mais aussi sur n'importe quelle autre infrastructure tierce, du moment que le trafic transite en proxy via Cloudflare WAF »*, a encore déclaré le PDG du fournisseur de cloud. Le service Firewall for AI de Cloudflare fournit aux équipes de sécurité les outils nécessaires afin de sécuriser leurs applications basées sur les LLM. En se positionnant en amont de n'importe quel LLM déployé sur la plateforme Workers AI, le pare-feu permet l'identification des menaces. Il a la capacité de repérer les tentatives malintentionnées d'exploitation des modèles grâce à l'analyse et l'évaluation des requêtes des utilisateurs.

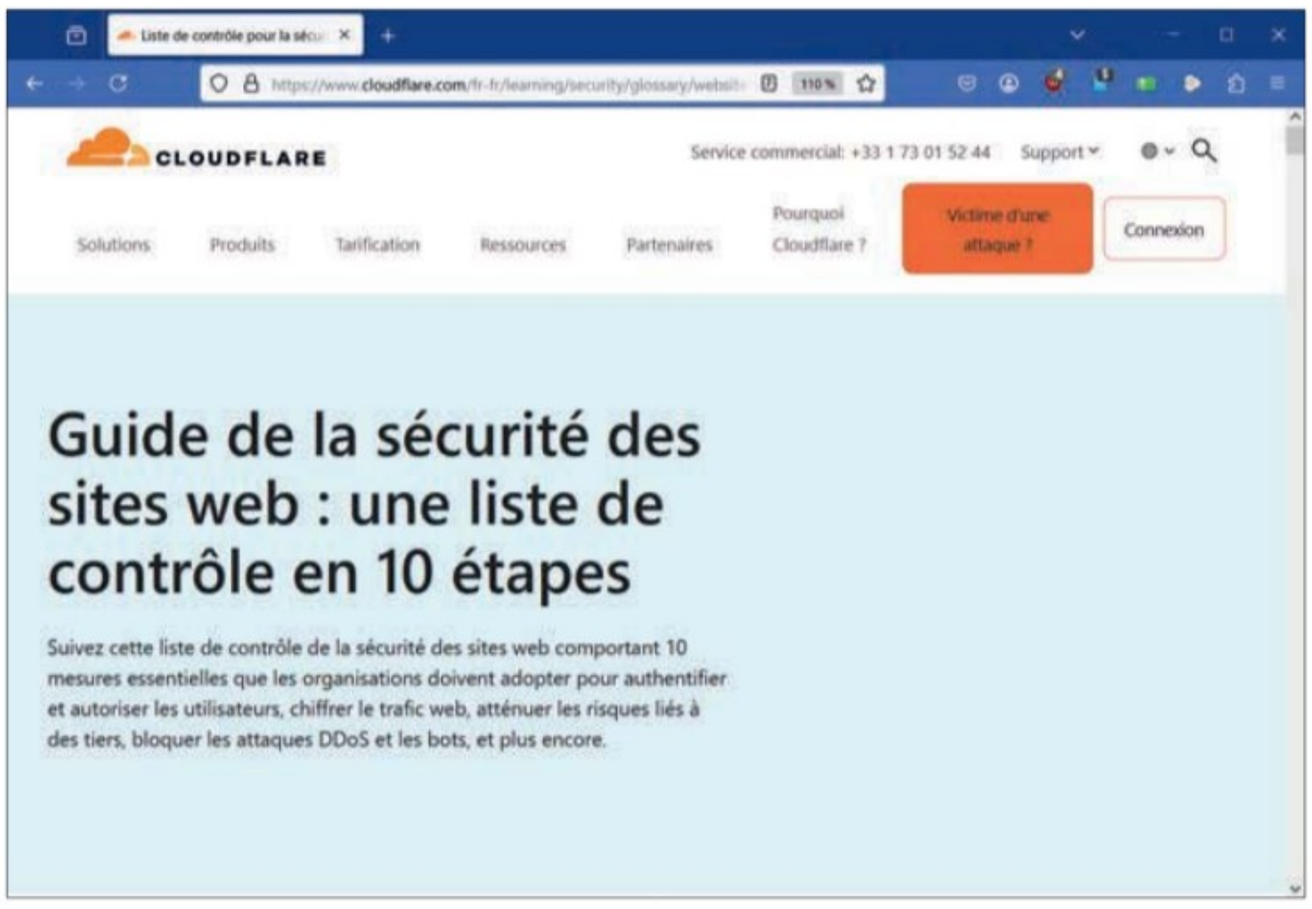
Protection contre le déni de service et les fuites de données

Firewall for AI est donc spécifiquement destinée aux clients qui exécutent une IA sur Workers AI. Elle protège notamment contre la fuite de données et l'injection d'invites. L'IA

défensive analyse et évalue les invites soumises par un utilisateur, afin de bloquer l'exploitation de modèles et les tentatives d'extraction de données. Sa puissance repose sur une combinaison d'heuristiques et de couches d'IA propriétaires permettant d'évaluer les invites et d'identifier les abus et les menaces. *« Firewall for AI protège contre le déni de service par modèle et la divulgation d'informations sensibles, grâce à des outils et des fonctionnalités disponibles pour tous les clients de l'offre WAF »*, a encore déclaré le PDG de Cloudflare. Firewall for AI exécute également une série de détections, afin d'identifier les tentatives d'injection rapide et d'autres abus, en s'assurant par exemple que le sujet reste dans les limites définies par le propriétaire du modèle.

Une IA défensive à même de détecter les comportements anormaux

Dans le cadre du programme Defensive AI, Cloudflare travaille sur des systèmes IA capables d'examiner les modèles de trafic de clients spécifiques et, à partir de là, de construire une base de référence de comportements normaux. A partir de cette base établie, toute anomalie dans les API, environnements, accès aux employés, courriels ou autres pourra être détectée. *« Defensive AI sert à comprendre comment les systèmes intelligents peuvent améliorer l'efficacité des solutions de sécurité »*, dit encore le dirigeant de l'entreprise. *« Cloudflare utilise l'IA pour augmenter le niveau de protection dans tous les domaines de la sécurité, que ce soit celle des applications, du courrier électronique ou de la plateforme Zero Trust de Cloudflare. Les modèles d'IA sont adaptés à une application spécifique, de sorte que la protection de l'API utilise des modèles différents de ceux du Zero Trust ou du courrier électronique »*, a-t-il encore ajouté. Quand bien même la mise en œuvre peut différer, les concepts généraux sont similaires.



Vous trouverez, sur le site de Cloudflare, un très bon guide de la sécurité des sites web avec une liste de contrôle en 10 étapes.

FONCTIONNEMENT

En plus des règles de l'OWASP, les règles gérées de Cloudflare proposent une protection rapide contre les attaques zero-day. Des ensembles de règles personnalisées permettent aux entreprises d'adapter leur pare-feu WAF, afin de mettre en place des politiques totalement spécifiques à leur organisation. Le WAF s'exécute sur son réseau mondial et se place en amont des applications web, afin d'être capable d'arrêter une vaste gamme d'attaques en temps réel grâce à de puissantes règles prédéfinies, de mesures de vérification des identifiants exposés, de mesures avancées de contrôle du volume des requêtes, de services d'analyse du contenu importé et de bien d'autres mesures de sécurité préétablies.

Les LLM, des cibles privilégiées pour les cybercriminels

Une enquête récente a mis en lumière que seulement 25 % des dirigeants se sentiraient prêts à affronter les risques associés à l'IA. La protection des LLM représente donc un défi de taille, notamment parce qu'il est quasi impossible de restreindre les interactions des utilisateurs avec de tels systèmes dès leur conception. Ces modèles, de nature non déterministe, sont susceptibles de générer une multitude de résultats variés à partir d'un même ensemble de données. C'est pour cela que les LLM sont exposés à des risques de manipulation, de détournement et d'attaques, en faisant des cibles privilégiées pour les cybercriminels. Le système de Cloudflare propose en outre la possibilité de bloquer automatiquement ce type de menaces, sans qu'une intervention humaine soit nécessaire. Le fournisseur de cloud peut faire profiter de l'immense couverture de son réseau mondial, avec plus de 250 points de présence et un service qui peut être activé au plus près des utilisateurs finaux. Cela garantit généralement une réponse immédiate et efficace face aux attaques. De plus, Cloudflare assure une protection par défaut, sans frais supplémentaires, à tous les utilisateurs exploitant des LLM au sein de l'environnement Workers AI. Cette extension est essentielle pour réduire les risques associés à l'injection de commandes malveillantes et prévenir les fuites de données.

Détection basée sur l'apprentissage automatique

Le pare-feu WAF de Cloudflare s'appuie sur le Machine Learning pour bloquer automatiquement les menaces émergentes en temps réel. Il s'intègre aux autres produits de sécurité des applications de Cloudflare. Aucune formation, ni aucun service professionnel n'est nécessaire pour l'utiliser. Il se configure en seulement quelques clics. ☐ **T.T**

Intégration

Rocket Software fédère les données en périphérie

Le spécialiste de la modernisation des environnements mainframe propose maintenant une nouvelle suite DataEdge pour intégrer les données dans les environnements hybrides.

Cette nouvelle solution comble le fossé entre les applications transactionnelles, les systèmes distribués et les environnements cloud gérant de façon transparente les taches de découverte, d'intégration et de gestion des données. Alors qu'un nombre croissant d'entreprises adopte ce type d'infrastructure, l'intégration en temps réel des données mainframe, distribuées et cloud est essentielle pour informer les modèles d'IA et générer des informations pleinement exploitables. Pourtant, d'importantes quantités de données critiques provenant de systèmes transactionnels demeurent largement inaccessibles aux initiatives d'IA et d'analytique. Les modèles d'IA et d'analytique qui n'exploitent pas les données mainframe sont souvent dans l'incapacité de fournir des renseignements complets et précis, ce qui limite sensiblement leur aptitude à dégager de la valeur métier.

Au niveau des métadonnées

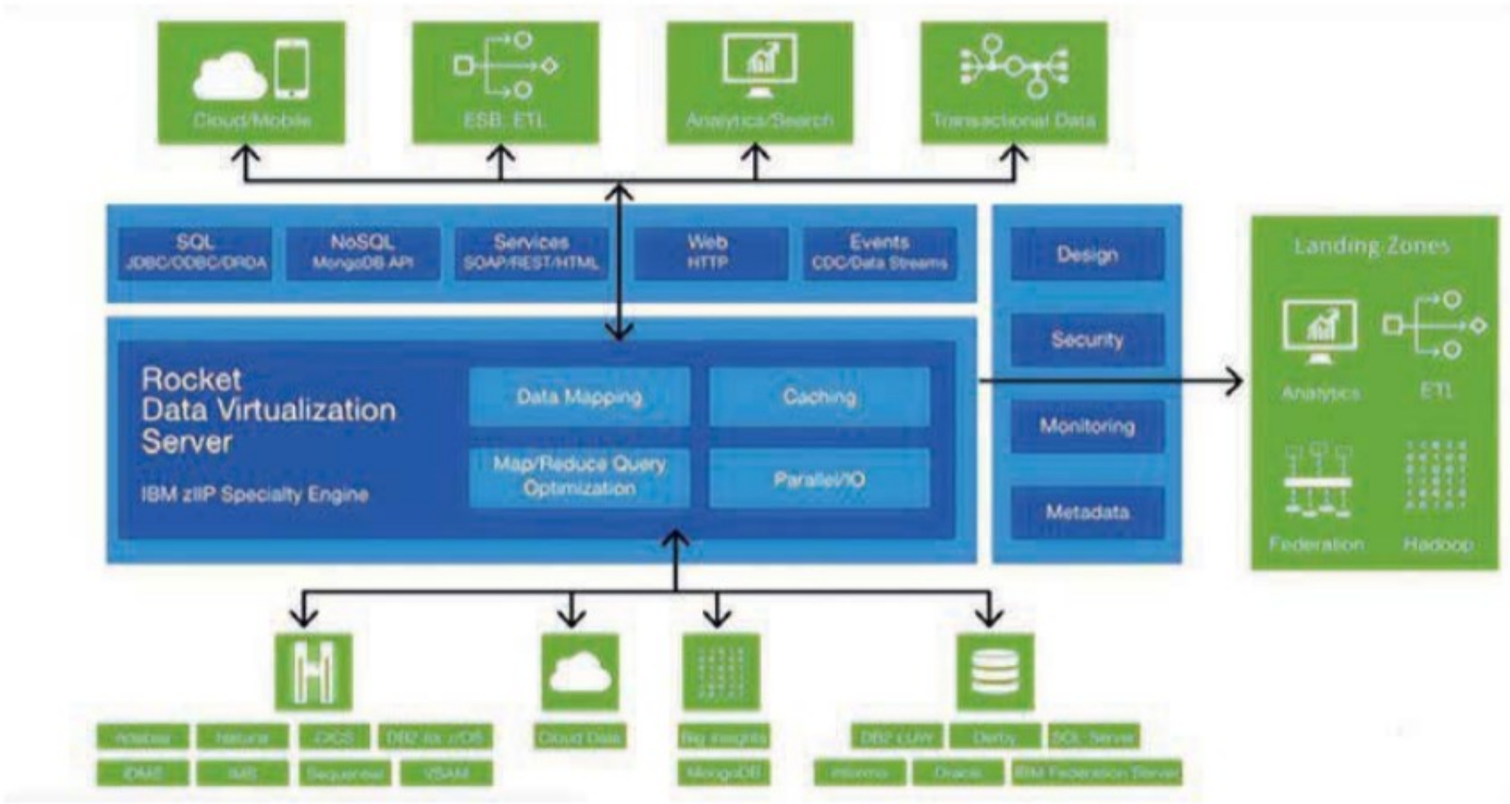
Rocket DataEdge unifie la gestion des métadonnées et l'expérience des utilisateurs dans l'optique d'accélérer des initiatives d'IA et d'analytique qui favorisent les résultats des entreprises. Cette suite se compose des modules suivants : Rocket Data Replicate & Sync, Rocket Data Intelligence et Rocket Data Virtualization.

Avec ces logiciels la connexion des données sur site, IBM i et mainframe difficiles d'accès aux applications cloud, aux data lakes, aux entrepôts de données et aux plateformes de type data lakehouse se réalise plus simplement. l'automatisation du balayage et de l'analyse des métadonnées mainframe et cloud facilite la compréhension des données, ainsi que leur mise en correspondance avec les initiatives de données cloud. En activant les moteurs de traitement de cloud hybride pour optimiser la gestion des données, les entreprises peuvent réduire leurs dépenses, optimiser leurs activités et accélérer les livraisons. la gestion homogène des données minimise la complexité, les retards, les erreurs et les problèmes de compatibilité en unifiant les données de manière transparente entre les différents environnements.

Selon IDC La vision et la feuille de route de Rocket DataEdge permettent de connecter les systèmes transactionnels aux environnements cloud et distribués dans le but d'assurer une gouvernance et un accès aux données de manière transparente et avec un haut niveau de qualité à tous les niveaux de l'entreprise.

Un émulateur sécurisé

Par ailleurs l'éditeur a annoncé un émulateur de terminal axé sur la sécurité qui se distingue par sa capacité à intégrer l'accès par écran vert aux solutions de gestion des identités et des accès (IAM) actuellement disponibles. Cette nouvelle solution assure une protection complète contre des menaces telles que les faux employés et les attaques de phishing tout en aidant les entreprises à se conformer aux règlementations en vigueur grâce à des fonctions de sécurité multicouches — authentification multifacteurs (MFA), authentification unique (SSO) et autres bonnes pratiques de sécurité avancées.



L'architecture du logiciel de voirtualisation des données de Rocket Software.

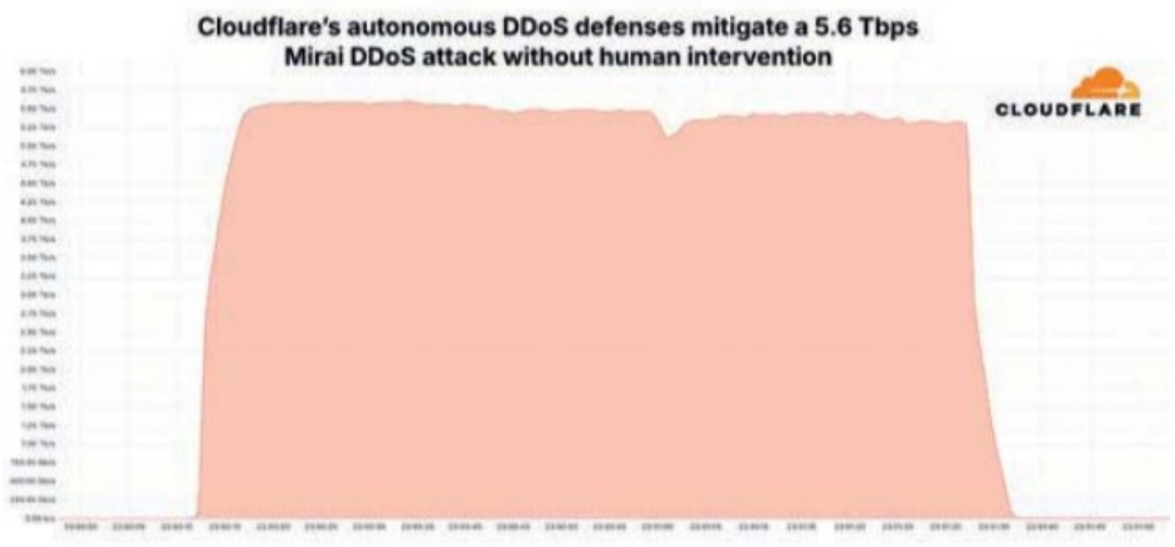
Secure Host Access, le nom du logiciel, assure un accès centralisé aux applications hébergées haute disponibilité, et peut être déployé dans différents systèmes et utilisé via un émulateur de bureau ou Web à empreinte nulle. De plus il étend les bonnes pratiques d'authentification d'entreprise. Elle évite en outre d'utiliser les outils d'autres fournisseurs de sécurité tout en assurant la conformité jusqu'aux applications hébergées. Cette solution complète les fonctions de sécurité déjà présentes dan le portefeuille de Rocket Software. □

B.G

DDoS Cloudflare analyse les attaques par déni de service

Comme chaque trimestre, Cloudflare nous livre son rapport sur l'activité malveillante relevé sur son réseau. Les attaques de déni de service sont toujours aussi présentes et une attaque a même établi un nouveau record pour une attaque.

Dans ce rapport Cloudflare confirme que ce type d'attaque est en constante augmentation. Ainsi durant le dernier trimestre de 2024 Cloudflare a atténué 6,9 millions d'attaques DDoS. Soit, une augmentation de 16 % par rapport au trimestre précédent et de 83 % par rapport à l'année précédente. Déjà au trimestre précédent L'entreprise constatait d'ores et déjà une hausse du nombre d'attaques hyper-volumétriques. Cela se confirme au dernier trimestre 2024, avec un nombre d'attaques dépassant 1 Tb/s augmentant de 1 885 % par rapport au trimestre précédent. Tandis que le nombre d'attaques dépassant 100 millions de p/s (paquets par seconde) a augmenté de 175 % sur la même période. Le 29 octobre, une attaque DDoS de 5,6 Tb/s a ciblé un fournisseur d'accès Internet (FAI) situé en Asie de l'Est. Une attaque durant 80 secondes et lancée depuis plus de 13 000 appareils IoT.



Le système automatique de Cloudflare a réussi à atténuer une attaque record de 5,6 Tb/s sans intervention humaine.

Parmi les attaques DDoS survenues au quatrième trimestre 2024, 49 % (3,4 millions) ciblaient la couche 3 ou la couche 4 et 51 % (3,5 millions) étaient des attaques DDoS HTTP. La majeure partie des attaques DDoS HTTP (73 %) ont été lancées par des botnets connus. Par ailleurs, 11 % des attaques DDoS HTTP interceptées imitaient un navigateur légitime, et 10 % des attaques présentaient des attributs HTTP suspects ou inhabituels. Les 8 % d'attaques restantes étaient des attaques HTTP flood génériques, des attaques volumétriques de type cache busting (infiltration de cache) et des attaques volumétriques ciblant les points de terminaison de connexion.

Le même agent

L'agent utilisateur HITV_ST_PLATFORM représentait la part la plus élevée de requêtes liées à des attaques DDoS par rapport au nombre total de requêtes (99,9 %), s'imposant comme l'agent utilisateur utilisé presque exclusivement lors des attaques DDoS. En d'autres termes, si vous observez du trafic provenant de l'agent utilisateur HITV_ST_PLATFORM, il y a 0,1 % de chances qu'il s'agisse de trafic légitime. La présence de l'agent utilisateur HITV_ST_PLATFORM, qui est associé aux téléviseurs connectés et aux boîtiers décodeurs, suggère que les appareils impliqués dans certaines cyberattaques sont des téléviseurs connectés ou des boîtiers décodeurs compromis. Cette observation souligne l'importance de la sécurisation de l'ensemble des appareils connectés à Internet, notamment les téléviseurs connectés et les boîtiers décodeurs, afin d'empêcher leur exploitation lors de cyberattaques.

Des méthodes différentes

Près de 14 % des requêtes HTTP utilisant la méthode HEAD étaient associées à une attaque DDoS, bien que cette méthode soit à peine présente dans les requêtes HTTP légitimes (0,75 % de l'ensemble des requêtes). La méthode DELETE arrivait en deuxième position, environ 7 % de son utilisation étant liée à des attaques DDoS.

D'où viennent les attaques ?

Le continent Asiatique occupe le top 3 du classement d'où proviennent les attaques DDoS. Hong Kong a progressé de cinq places par rapport au trimestre précédent et Singapour de trois places. Ces pays sont suivis par l'Ukraine, l'Argentine, la Colombie, la Russie, la Bulgarie, la Corée du Sud et enfin l'Allemagne.

Le secteur des télécommunications, des fournisseurs d'accès internet et des opérateurs occupe la première place, devenant le secteur le plus ciblé par les attaques. Suivi du secteur internet en seconde position et enfin des secteurs du marketing et de la publicité en troisième position.

Le but des attaques

Pour ceux qui savent qui est l'attaquant, 40 % ont déclaré que leurs concurrents étaient le principal acteur malveillant à l'origine des attaques. 17 % déclarent que le responsable des attaques était un acteur malveillant mandaté ou soutenu par un État, et un pourcentage similaire a indiqué que le responsable des attaques était un utilisateur ou un client mécontent.

Vous trouverez encore plus de détails à cette adresse : https://blog.cloudflare.com/fr-fr/ddos-threat-report-for-2024-q4/ ☐

B.G

Cloud

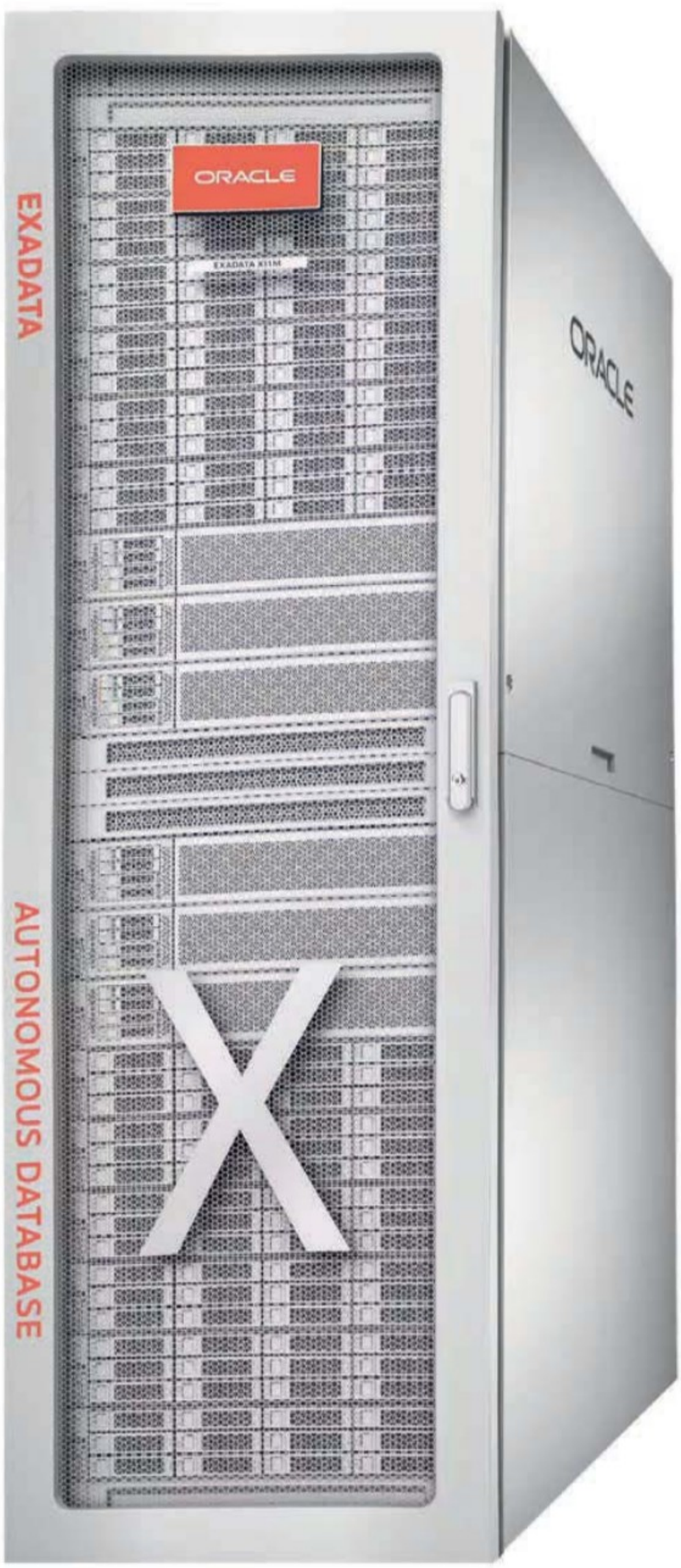
BNP Paribas se rallie à Exadata@customer

Partenaire et utilisateur des logiciels de base de données Oracle depuis longtemps, BNP Paribas a fait le choix d'Exadata pour consolider ses bases de données tout en conservant celles-ci dans ses centres de données.

BNP Paribas s'appuie sur la technologie Oracle pour gérer une partie de ses bases de données on-premise depuis plus de 20 ans. Le Groupe intègre désormais Exadata Cloud@Customer afin d'améliorer la performance de la gestion de ces bases de données. Ce choix répond à l'ambition de la banque de continuer à améliorer ses services tout en garantissant la sécurité des données de ses clients. En effet Bernard Gavgani explique que les grands enjeux des grandes entreprises aujourd'hui tournent autour de la donnée. Il ajoute : *« Les données sont devenues tout. Et en même temps, les volumes des données deviennent de plus en plus impressionnants. Je pense qu'à chaque fois que vous posez la question à un informaticien, on vous parle des données »*. Mais si les données sont le contenu, il convient aussi de s'interroger sur le contenant, les bases de données. Actuellement BNP a une dizaine de plate-formes de bases de données. *« Tout l'enjeu était comment s'en sortir »* indique le DSI de la banque. Il ajoute : *« on a essayé de se projeter dans le futur »*. En fait avec l'intelligence artificielle il est devenu quasiment impossible de prévoir quel sera le volume des données d'ici un, deux, dix ans. Bernard Gavgani résume : *« de toute façons ce sera en augmentation »*.

Différentes contraintes

Tout d'abord il était hors de question de sortir du périmètre de l'informatique de la banque les données sur les clients. Le DSI explique : *« c'est notre engagement vis-à-vis de nous-mêmes et de la confiance que nos clients nous donnent »*. La banque souhaite conserver la protection de ce type de données. A partir de cet a priori, la banque avait deux choix possibles : prendre Oracle sur le Cloud hybride de la banque, pierre angulaire de la stratégie Cloud de la banque, soit tout consolider sur IBM Cloud. *« Ce choix était un vrai raccourci mais intellectuellement insuffisant. En réalité, c'est très compliqué et ça coûte très cher. Parce que vous devez complètement transformer vos bases de données »* précise le DSI. Le choix d'Exadata devenait donc quasiment une évidence principalement du fait que la solution répondait à très grande partie des préoccupations de la banque et de ses enjeux du futur. *« L'adoption d'Oracle Exadata Cloud@Customer s'inscrit pleinement dans la stratégie cloud de BNP Paribas pour continuer à bénéficier du plein potentiel des technologies dans un cadre sécurisé. Grâce à une gestion optimale de ces données, ce partenariat permet à la banque de continuer à innover, de garantir la continuité d'activité et*



Un serveur Exadata-X11M.

toujours assurer la meilleure qualité des services pour nos clients » considère Bernard Gavgani.

Dans la continuité stratégique

La banque pourra allier les avantages d'une infrastructure cloud tout en maintenant ces bases de données on-premise. Cette solution intègre des technologies avancées de chiffrement et de surveillance en temps réel, assurant le plus haut niveau d'intégrité des données. La banque pourra exploiter toutes les fonctionnalités d'automatisation offertes par Oracle Database telles que l'optimisation des traitements, une meilleure accessibilité des bases de données au sein du Groupe et un basculement automatique pour renforcer la fiabilité et la résilience du système, garantissant ainsi une continuité de service optimale. De plus, cette approche permettra de réduire la latence entre les applications et les données, améliorant l'efficacité opérationnelle et les performances globales, tout en simplifiant la gestion de l'obsolescence. Ce partenariat s'inscrit dans la continuité de la stratégie cloud de BNP Paribas. Depuis plusieurs années, la banque investit dans des solutions de cloud privé et de cloud dédié pour optimiser ses infrastructures IT tout en garantissant le contrôle sur ses données hébergées dans les data centers du Groupe. En ligne avec sa stratégie cloud, et pour assurer la sécurité des données de ses clients, BNP Paribas ne met pas de données clients ou d'environnement de production contenant des données sensibles dans le cloud public. Le retour sur investissement est prévu au bout de 2 ans. Ce chiffre n'est pas intangible, car le choix a été fait plutôt autour de la valeur apportée plus que sur l'approche économique du projet.

Un projet d'ampleur

Cette migration vise quasiment 10 000 base de données et court jusqu'à la fin 2026. Il repose sur une usine logicielle d'Oracle qui a été testée et validée avant le commencement du projet. La première étape consiste à faire évoluer les bases de données vers la version 19 puis de déployer les bases de données dans deux centres de données dans le giron de la banque dont un en Belgique pour assurer la résilience. Bernard Gavgani le constate : *« une base de données, ça peut tomber »* !

Un aspect RH important

Le projet va amener à former ou reformer les administrateurs des bases de données dont le rôle va évoluer pour être capable de gérer de très larges bases avec énormément de volume de données. Ils devraient être aidés par les fonctions d'automatisation présentes dans la base d'Oracle comme l'optimisation des traitements ou le basculement automatique pour renforcer la fiabilité et la résilience du système. *« Il n'y aura pas de suppression de postes »* assure le DSI. Des formations seront mises en place pour suivre les évolutions des technologies afin qu'ils deviennent des DBA améliorés pour gérer l'existant, le futur et l'infusion de l'intelligence artificielle dans les métiers de la banque.

Bernard Gavgani, DSI de BNP Paribas.

Une sécurité renforcée

Toutes les données sont chiffrées et les clés sont gérées par la banque dans un système hors environnement Oracle. De plus la solution étant dans les centres de données de BNP Paribas, la banque est loisible de couper tous les accès instantanément.

« Les organisations financières adoptent rapidement les technologies cloud pour réduire les coûts et accélérer leur capacité à exploiter de nouvelles opportunités de marché », conclut Juan Loaiza, vice-président exécutif, Technologies de base de données critiques, Oracle. *« En utilisant Oracle Exadata Cloud@Customer, BNP Paribas fera évoluer son parc de bases de données vers un modèle cloud moderne, agile et rentable qui leur permettra d'innover plus rapidement tout en respectant les réglementations strictes en matière de localisation et de confidentialité des données. »* ☐

B.G

Chiffrement

Thales accélère dans les communications quantiques

Déjà à l'origine du projet TeQuantS, mené avec l'Agence Spatiale Européenne, Thales Alenia Space va également déployer un programme de distribution de clefs de chiffrement par intrication quantique avec l'espagnol Hispasat, qui s'appuiera cette fois-ci sur des satellites géostationnaires plutôt qu'en orbite basse.

Thales Alenia Space (une coentreprise entre le groupe français et l'Italien Leonardo) et Hispasat vont proposer un système quantique de distribution de clés de chiffrement. Ce projet illustre les grandes ambitions du groupe franco-italien dans cette technologie de pointe, qui devrait jouer un rôle clef dans le futur des communications sécurisées, en particulier face aux ordinateurs quantiques.

Thales Alenia Space et Hispasat disposent d'une enveloppe de 103,5 millions d'euros pour mettre en place ce projet, lancé par le Secrétariat d'État espagnol aux Télécommunications et aux Infrastructures numériques, et financé au travers du fonds européen dans le cadre du Plan national de Relance, de Transformation et de Résilience (PERTE Aeroespacial). Les deux partenaires visent un service opérationnel en 2029, basé sur un satellite géostationnaire. L'objectif est de communiquer des clefs de chiffrement sans risque d'interception. Le tout en utilisant l'intrication quantique, un phénomène de la mécanique quantique qui fait que deux particules deviennent inséparables, même lorsqu'elles se trouvent à une grande distance l'une de l'autre.

Un premier essai sera réalisé via une liaison atmosphérique de 140 km dans les îles Canaries, entre La Palmas et Tenerife, afin de valider le segment sol et la charge utile quantique.

Le futur du chiffrement

Car le défi est de taille. La distribution de clés quantiques par satellites est une prouesse technologique qui n'a pour l'heure été accomplie que par un seul pays. En 2017, des chercheurs chinois ont pour la première fois réussi à transmettre une clef à 1400 km de distance, via le satellite Mozi.

Dans un contexte de montée en puissance des cybermenaces, la distribution quantique de clés de chiffrement suscite de nombreux espoirs auprès des experts en cybersécurité. Elle constituerait en particulier un moyen de rendre les techniques de chiffrement résistantes aux ordinateurs quantiques, qui promettent de casser les méthodes actuelles, lesquelles s'appuient sur la factorisation de grands entiers. Pour éviter un scenario cauchemar dans lequel un ordinateur quantique deviendrait capable de décrypter toutes les communications existantes, donc de pirater n'importe quelle banque ou de mettre le président français

sur écoute, plusieurs pistes sont à l'étude. La première, la cryptographie post-quantique, s'appuie sur de nouveaux problèmes mathématiques capables de résister aux ordinateurs quantiques.

La deuxième option, qui est celle sur laquelle planchent Thales Alenia Space et Hispasat, consiste à s'appuyer sur les principes de la mécanique quantique, et en particulier l'intrication.

La distribution de clefs quantiques s'appuie sur la transmission de photons via un canal de communication. Les photons sont codés avec des états quantiques aléatoires, formant ainsi une clé asymétrique. Celle-ci est utilisée pour crypter et décrypter les messages. Du fait des propriétés de la mécanique quantique, qui impliquent qu'observer un photon change ses paramètres, toute tentative d'intrusion par un acteur malveillant sera forcément détectée. *« On peut ainsi savoir avec certitude si la clef a été compromise ou non »*, affirme Angel Alvaro, responsable du projet.

Toutefois, *« la distribution de clefs de chiffrement quantique se heurte à de fortes barrières physiques. Si l'on veut passer par un système terrestre, comme des réseaux de fibres optiques, la transmission ne peut se faire que sur une centaine de kilomètres au maximum. Au-delà, on se heurte à des difficultés physiques qui causent des interférences »*, explique Ludovic Perret, professeur en cryptographie post-quantique à l'EPITA. D'où la nécessite de recourir à des satellites, les interférences étant alors bien moindres.

L'idée étant, à terme, de mettre en place un dispositif hybride, s'appuyant à la fois sur la fibre et les satellites. *« On aura un réseau de fibre local qui assurera la distribution de la clé entre les utilisateurs locaux, et pour l'échange de clef sur de longues distances, c'est le satellite qui va prendre le relais »*, explique Angel Alvaro. Une fois opérationnel, ce dispositif s'adressera en priorité à l'administration publique, aux banques, aux réseaux de communication et d'énergie. Parmi les partenaires, on compte le Centre cryptologique national, l'entité certificatrice espagnole pour tous les réseaux de sécurité, ainsi que des banques et opérateurs des télécoms : Banco Santander, BBVA, Telefonica, Telmex.

La Chine possède une longueur d'avance

Thales Alenia Space a fait de l'exploration des communications quantiques l'un de ses axes stratégiques. Outre le projet avec Hispasat, le consortium européen planche également, avec l'Agence Spatiale Européenne (ESA), sur le projet TeQuantS. Celui-ci vise aussi à construire un réseau de communication quantique à base de satellites et stations sol optiques d'ici 2026. Contrairement au programme mené avec Hispasat, il fonctionnera toutefois avec des satellites situés en orbite basse. L'objectif du projet est notamment de servir les constellations européennes de satellites de sécurisation des communications, Saga (Security And cryptoGrAphic) et Iris2 (infrastructure de résilience, d'interconnectivité et de sécurité par satellite). Mais aussi d'aider les industriels français à se positionner à la pointe de ces technologies au moment où elles seront embarquées sur les satellites européens. Les progrès techniques accomplis dans le cadre de ces projets permettront en outre de poser les jalons d'un futur internet quantique, selon Angel Alvaro.

Si l'Europe accélère depuis quelques années sur cette technologie, c'est pour l'heure la Chine qui continue de dominer. *« Sur la distribution de clés quantiques, les Chinois ont au moins dix ans d'avance sur nous »*, note Ludovic Perret. L'informatique quantique et son application à la cryptographie sont plus généralement des points forts de la recherche chinoise. Début janvier 2023, un groupe de chercheurs de l'Empire du Milieu sont ainsi parvenus à décoder le chiffrement RSA, l'algorithme de cryptographie le plus utilisé en ligne, à l'aide d'un ordinateur quantique.

La Bavière, foyer d'excellence européen

À l'échelle européenne, le projet EAGLE-1, consortium entre le spécialiste des télécommunications par satellite luxembourgeois SES, Airbus et l'organisme de recherche néerlandais TNO, vise actuellement à mettre en place un dispositif similaire à celui sur lequel travaille Thales Alenia Space.

Plusieurs jeunes pousses explorent également les communications post-quantiques, parmi lesquelles Speqtral, une startup de Singapour, ou encore ThinkQuantum, basée en Italie. Sur le Vieux Continent, la Bavière constitue un écosystème particulièrement fertile à cet égard, avec la jeune pousse Keequant, ainsi que l'Université de la Bundeswehr à Munich, qui participe activement à des projets de recherche axés sur la transmission de clés de chiffrement quantiques, y compris le développement de réseaux de communication sécurisés à usage militaire et civil.

La Bavière abrite également le Centre aérospatial allemand, qui mène lui aussi des recherches dans ce domaine, ainsi que le Quantum Business Network et la Munich Quantum Valley, deux organisations qui favorisent la collaboration entre le monde universitaire, l'industrie et les pouvoirs publics pour accélérer l'innovation dans le domaine quantique. □

G.R

Power BI : en images

L'ouvrage d'Augustin de la Fouchardière adopte une approche différente pour nous faire découvrir ou redécouvrir un des outils les plus utilisés dans le monde, Power BI. Des concepts généraux autour du logiciel aux fonctions avancées et les bonnes pratiques à mettre en place pour une utilisation optimale de l'outil, l'auteur se garde de pédantisme et reste très pratique sur ce que peut faire Power BI. L'approche très visuelle permet de rapidement synthétiser et mémoriser les notions importantes autour du logiciel de Microsoft. Au passage, alors que l'IA tient le devant de la scène, l'ouvrage remet au goût du jour la toute simple business Intelligence, celle qui sert les métiers des entreprises tous les jours. À mettre dans toutes les mains ! De plus, l'ouvrage est pour l'instant gratuit, alors profitez-en.

Quelles fonctions DAX faut-il retenir parmi les centaines qui existent, lorsqu'on crée une mesure (un calcul) dans Power BI ?

En voici quelques-unes parmi les plus importantes à mémoriser :

➡ CALCULATE : selon Microsoft : « Évalue une expression dans un contexte de filtre modifié."??!??
Avec mes propres mots, cette fonction doit être utilisée dès que votre calcul est plus qu'une simple aggrégation.
Exemple : vous souhaitez connaitre la moyenne de tous les avis clients ? Un simple AVERAGE de la colonne [AvisClient] suffira. Si c'est une moyenne des avis filtrée sur une catégorie spécifique, vous devrez mettre CALCULATE en préfixe de l'aggrégation AVERAGE.

➡ DIVIDE = plutôt que de faire une division en utilisant un symbole "/", il est préférable de faire DIVIDE, puis les arguments (numérateur, dénominateur, résultat en cas de division par 0). Car, en effet, le DIVIDE gère la division par 0, c'est son principal avantage.

➡ AVERAGE = pour faire une moyenne, AVERAGE est in-dis-pen-sable ! Et pour une somme c'est SUM, pour un min, c'est MIN, pour un max, c'est MAX !

➡ SELECTEDVALUE = cette fonction est INCONTOURNABLE en DAX, elle est par exemple utilisée dans les titres dynamiques et dans les simulations / projections de scénario (paramètres plage numérique). Avant qu'elle n'existe, il fallait combiner IF(HASONEVALUE(FIRSTNONBLANK)).

➡ ALL = cette fonction, hyper pratique, notamment pour créér des jauges, permet de neutraliser un filtre présent sur une page.
Exemple : je veux comparer la température de la ville sélectionnée dans un segment, versus la température de toutes les villes de mon jeu de données. Pour obtenir ce calcul, je fais un CALCULATE(AVERAGE[Temperature]), ALL([Ville]))

Quelles sont les techniques modernes d'investigation sur les données ?

➡ Vous connaissez certainement ces techniques dans d'autres outils (Qlik, Tableau…) mais elles n'existent PAS dans Excel !

➡ Le Drill Down, aka Zoom, mode exploration ou analyse hiérarchique. Très populaire, cette technique permet de creuser dans les données pour y déceler des informations utiles. Par exemple, c'est Continent > Pays > Région > Ville, ou bien Famille de Produit > Sous Famille > Produit > Version du produit.

➡ Le Highlight, ou mise en surbrillance, permet de visualiser les éléments en commun entre deux visuels, alors que le reste est simplement mis en retrait mais toujours visible.

➡ Le Drill Through, ou Extraction, consiste à créer une page d'atterrissage avec des détails sur un produit, un pays, un employé.
Pour cela, il faut définir une variable (dite variable d'extraction) qui doit être sélectionnée depuis une autre page (la page d'accueil).

Mype

TOP 10 FONCTIONS DAX

parmis les plus utiles dans **UNE MESURE**

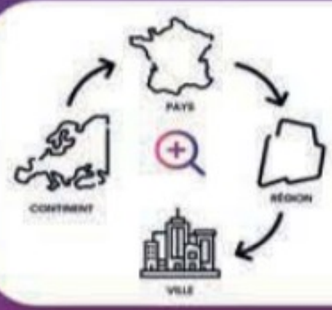
Syntaxe	Explication	Exemple d'utilisation
CALCULATE()	Retourner une expression filtrée	Calculer le chiffre d'affaires filtré sur un produit
DIVIDE()	Effectuer une division	Calculer une variation
AVERAGE()	Calculer une moyenne	Calculer la moyenne des ventes par magasin
SELECTEDVALUE()	Retourner la sélection effectuée par un utilisateur dans une colonne	Récupérer la sélection d'un produit dans un visuel segment
ALL()	Supprimer tous les filtres d'une colonne	Calculer la part d'un chiffre d'affaires d'un produit quand la colonne qui contient le produit fait parti du contexte de filtre
ALLEXCEPT()	Ajouter ou retirer du temps	Comparer le chiffre d'affaires de l'année N et l'année N-1
DATEADD()	Formater la valeur d'une chaine de texte	Modifier le format d'une date
FORMAT()	Retourne la valeur minimale ou maximale d'une colonne.	Trouver la température la plus élevée
MIN() et MAX()	Retourner la valeur minimale ou maximale d'une colonne	Trouver la température la plus élevée
COUNTROWS()	Compter le nombre de lignes dans une table	Connaitre le nombre de factures de ventes

➡ Le Q&A, ou Questions & Réponses, est un visuel permettant de poser des questions, en langage naturel à Power BI qui retournera les réponses avec le visuel adapté (seulement dispo en EN et ES pour le moment). Pour optimiser l'utilisation du visuel, il est préférable de définir des synonymes.

➡ Le Explain the Increase / Decrease, consiste à cliquer sur un point de données avec une variation sur un graphique de type courbe ou histogramme. Microsoft ira lui même interroger les différentes dimensions du modèle sémantique pour expliquer les hausses et les baisses.

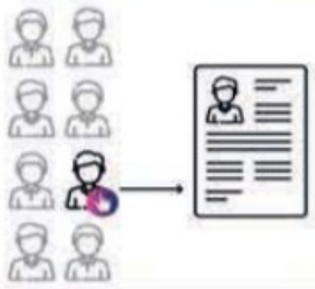
Mype

LES TECHNIQUES D'ANALYSE SUR POWER BI



DRILL DOWN

L'analyse dimensionnelle, ou **drill down**, consiste à zoomer dans un visuel et à descendre d'un niveau à un niveau



DRILL THROUGH

L'extraction, ou drill through permet d'obtenir les détails filtrés d'un point de données sélectionné.

HIGHLIGHT

Lorsque la propriété highlight est activée, le visuel met en surbrillance les données communes à deux visuels.

Q&A

Le visuel Questions et Réponses permet aux utilisateurs de poser des questions en langage naturel et d'obtenir des réponses sous la forme d'un visuel.

TOOLTIPS

Les tooltips sont des infobulles comportant des informations et qui apparaissent lorsqu'on survole un visuel.

ANALYSE

Via la fonction Analyser (Expliquer la hausse/baisse), Power BI créé un visuel qui explique les hausses et les baisses observées dans les graphes.

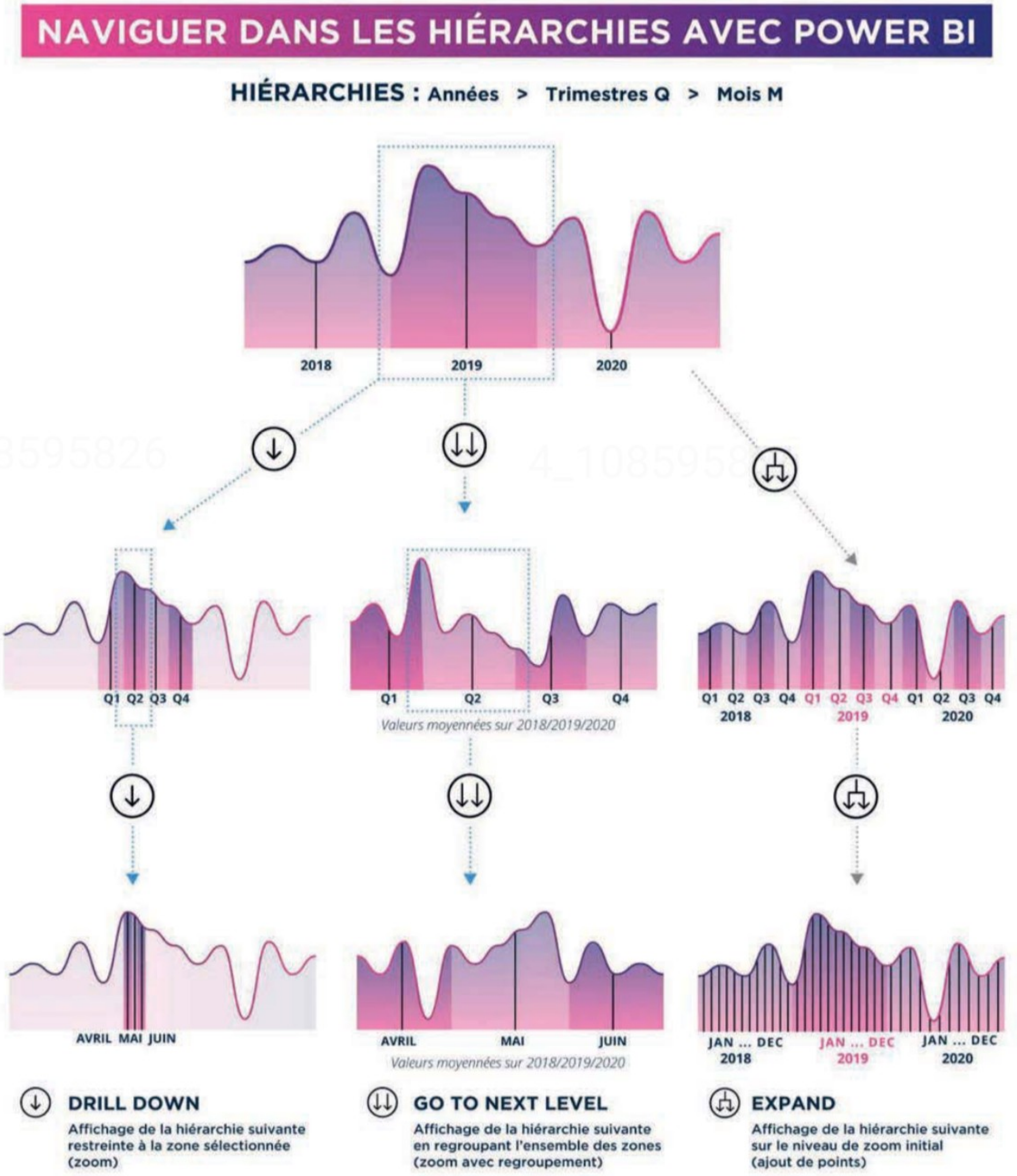
ALORS, PRÊT(E) POUR DEVENIR UN(E) EXPERT(E) POWER BI ?

Comment naviguer dans des hiérarchies avec Power BI ? Pourquoi y a-t-il toutes ces options avec les flèches en haut à droite d'un visuel, et que signifient-elles ?

Quelle est la différence entre « *Drill Up* » (monter dans la hiérarchie), « *Drill Down* » (descendre dans la hiérarchie), « *Expand All (tout développer) et « Go to next level »* (aller au niveau suivant) ?

On explique tout ici.

Power BI en images
Augustin de la Fouchardière
MYPE



Stockage

Pure Storage innove en république tchèque

Il y a quelques semaines, L'Informaticien a eu la chance de visiter un des trois laboratoires de recherche et développement de Pure Storage à Prague en république tchèque.

Le centre praguois a été créé en 2019 et est situé depuis 2020 dans le complexe Amazon Court. Depuis le site ne cesse de grandir à la fois en termes de salariés mais aussi de missions. C'est le plus gros site de ce type en dehors des USA. Il emploie plus de 600 salariés d'une moyenne d'âge de 35 ans. Avant de choisir cette implantation, Pure Storage avait analysé différents choix sur une vingtaine de critères. La richesse et la taille du vivier de talent, le système d'éducation dans le pays et la capacité de Prague a attiré des talents locaux ou internationaux ont fait pencher la balance sur Prague. Les questions de coûts et la force du marché local sont aussi entrés en ligne de compte.

Des réussites qui se concrétisent sur le marché

Les équipes du centre peuvent s'enorgueillir de plusieurs réussites importantes. Un tiers des développements sur les FlashArray proviennent de là. Les FlashBlade//s ont été conçus et testés dans ce laboratoire. Plusieurs fonctions de Pure Fusion, un service de « Storage as Code » ont été créées par les membres de ce laboratoire en particulier sur la sécurité et l'observabilité. Pure Protect, le service de reprise après désastre de l'éditeur est une création 100 % praguoise. Il en est de même pour Portworx Data Service (DBaaS pour Kubernetes) et Pure1.

Une politique continue d'innovation

Rob Lee, le CTO de Pure Storage, est aussi intervenu lors de cette visite pour apporter son éclairage sur les technologies à suivre. La première est évidemment l'intelligence artificielle où Pure Storage déjà engrangé plusieurs clients notables comme Meta ou SoftBank. Il es t revenu aussi sur les succès auprès des hyperscalers. Quatre d'entre eux s'appuient sur les matériels et logiciels de Pure Storage. Les choix techniques comme la généralisation du Flash dans les centres de données correspondent aux besoins de ce type d'entreprise et le design des solutions de Pure lui permet de répondre présent face à des besoins nécessitant performance et robustesse. On peut donc résumer le futur du stockage et des produits comme un modèle totalement Flash opéré comme dans le Cloud.

Une vue des bureaux de Pure à Prague.

La durabilité comme critère

L'aspect autour d'une informatique propre est aussi un des grands enjeux du laboratoire. Et Pure veut aider les entreprises à atteindre leur but environnemental en proposant des équipements moins consommateurs d'énergie, occupant moins d'espace et en réduisant les déchets. Cela va même jusqu'aux conditionnements de livraison chez Foxconn. Un centre de données totalement Flash de l'équipementier peut consommer jusqu'à 5 fois moins d'énergie dans un espace utilisant 5 fois moins de racks. Autre exemple, Les FlashArray//E et FlashBlade//E consomme 86 % de moins que les alternatives concurrentes.

Une visite chez Foxconn

Après le passage au centre praguois, nous avons pu visiter un centre logistique et d'assemblage de Foxconn qui travaille pour Pure Storage. Foxconn est acteur important pour le commerce extérieur tchèque puisque la société fait partie des trois premiers exportateurs du pays à partir de deux sites à Pardubice et Kutná Hora. Depuis 2016, le site de Pardubice produit des baies Pure Storage. Depuis le programme a été étendu et le site produit en standard des FlashArray, des FlashBlade, et des éléments du programme Evergreen. Les équipements fabriqués à Pardubice sont distribués dans le monde entier. □

B.G

IA Elle cherche sa place au soleil

Marseille et la région PACA misent sur la coopération entre le public, le privé et l'Université pour développer localement des filières économiques autour de l'IA et de la cybersécurité. Un campus cybersécurité a été ouvert et les projets impliquant de l'IA se déclinent dans les grandes entreprises de la métropole.

Dans la compétition en cours, et ses débordements, pour développer le secteur numérique en général, et l'IA en particulier, Marseille et plus largement, la région Provence, multiplient les initiatives « innovantes ». Au cours d'une conférence de presse organisée par Provence Promotion[1], l'ex-député et président du Cyber Campus Euromed, Olivier Darrason, a souligné le potentiel de développement dans le bassin méditerranéen à partir de ces technologies, et le rôle que pourrait y jouer la métropole.

PACA, terre de recherche

Cinq pôles de compétitivité, 130 laboratoires de recherche et plus de 400 startups sont présents dans la région. Dernière initiative, la région finance partiellement une nouvelle structure, ouverte en novembre 2024, dénommée Campus Cyber Euromed et destinée à booster le développement de solutions de cybersécurité souveraines et d'applications d'IA. Cette société, une SAS sur le plan juridique, poursuit les mêmes objectifs que le Cyber Campus de la Défense (92). Elle associe acteurs publics, industriels, chercheurs académiques et PME. Côté privé, ses adhérents sont entre autres la FDJ, CMA-CGM, Onet sécurité, Airbus Helicopters ou encore l'Aéroport de Marseille. Des expérimentations sont en cours, comme par exemple un PoC (Proof of Concept) développé avec Air France et Air Corsica, destiné à fluidifier l'embarquement des passagers. L'application génère un QR biométrique, pour ceux donnant leur accord, et hybride, celui-ci avec le QR code de la carte d'embarquement sur chaque smartphone. Cette application devrait passer en production au printemps. Autre exemple, Airbus Helicopters mène des projets impliquant l'IA et le Cyber Campus pour mieux sécuriser ses quelque 18 000 fournisseurs. D'autres structures profitent de cette dynamique.

Des applications sur le terrain

Commandant du port de Marseille-Fos, qui prend en charge autour de 9 400 escales par an, Philippe Affre décrit : *« nous commencons à utiliser massivement l'IA pour la vidéo surveillance des zones sensibles notamment. Le port reste une porte d'entrée pour de nombreux trafics. Des scénarios appliqués à l'IA nous ont donné quelques surprises : des gens qui escaladaient des clôtures… Bien sûr, les images des 850 caméras du réseau de surveillance étaient déjà là, mais les opérateurs ne pouvaient pas avoir l'œil partout »*. Le port multiplie d'autres expérimentations : pour optimiser les temps de chargement/déchargement des cargos, les temps d'attente pour rentrer au port… *« Globalement, cette digitalisation couplée à l'IA va optimiser la performance du port »*, résume Philippe Affre. Tous ces projets soutenus par les institutionnels sont bien sûr censés respecter la réglementation en matière d'IA. Pour faire bonne mesure, le Campus Cyber Euromed et les autres acteurs ont signé une charte éthique incluant une clause de responsabilité sociale.

Le port de Marseille

Optimiser l'IA

Il s'agit aussi d'exploiter au mieux les avancées des laboratoires de recherche reconnus pour leur expérience en IA. Le langage Prolog a été inventé, dans les années 1970, par un chercheur de l'Université de Marseille, fusionnée depuis avec celle d'Aix-en-Provence. Aujourd'hui, deux laboratoires spécialisés en IA et mathématiques, le LIS (Laboratoire d'Informatique et Systèmes) et I2M (Institut de Mathématiques de Marseille) comptent à eux deux environ 340 enseignants-chercheurs et chercheurs. Ces labos participent à des projets impliquant les entreprises locales et espèrent améliorer les performances de ces technologies. Pour Frédéric Échet, chercheur au

1 : Provence Promotion est l'agence d'attractivité économique des Bouches-du-Rhône. Depuis 2020, 38 % des entreprises soutenues par l'agence opèrent dans le secteur numérique.

DÉVELOPPER UNE OFFRE DE FORMATION LOCALE

Développer une filière locale passe aussi par la formation de compétences. Plusieurs structures existent déjà, notamment TheCamp, localisé à Aix-en-Provence qui propose des formations dédiées aux décideurs sur les sujets de transformation digitale et environnementale. Cette structure organise également de nombreux rendez-vous d'affaires dans le secteur numérique. Côté formation, une école d'ingénieurs spécialisée dans le numérique devrait ouvrir sur ce campus l'année prochaine. D'autres centres comme Simplon proposent déjà formations d'experts en cybersécurité et vont encore étendre leurs offres.

LIS : *« la précision de l'IA pourrait progresser en augmentant encore les volumes de données, la puissance de calcul et le nombre de paramètres »*. Une assertion mise en avant par OpenIA, mais *« pas étayée par une théorie mathématique »*, reconnaît le chercheur. Les premières réalisations émergent malgré cette absence. Partenaire du LIS et spin-off de l'Université, VB Tech développe un jumeau numérique du cerveau sur le plan neurologique, pour mieux comprendre et prendre en charge des pathologies comme l'épilepsie. L'IA est mise à contribution pour prédire quelles zones sont « éliptogènes » parce qu'il n'est pas possible de mettre des sondes partout. Un PoC embarquant 350 patients a été concluant d'après son dirigeant. Autre structure de recherche locale, l'Institut Laënnec travaille sur plusieurs champs, en particulier l'oncologie et les neurosciences. Des recherches sont menées sur d'autres domaines en particulier dans la logistique. Conjointement avec CMA-CGM, l'un des projets a pour but de réduire notablement la consommation de carburant des navires, grâce à l'optimisation des routes maritimes avec de l'IA.

Alain Mingam présente le projet de sécurisation de la chaîne logistique d'Airbus, lors d'une conférence de presse dans le Campus Cyber Euromed.

Une connectivité de haut niveau

Les différents partenaires profitent également des interconnexions via les datacenters locaux. Marseille a pris la place de sixième hub mondial en termes de trafic internet, un classement calculé en fonction du nombre de gigabits transitant par seconde. Fabrice Coquio, président de Digital Realty (ex-Interxion), un fournisseur américain de salles blanches, explique : *« plus de 90 % du trafic mondial passe par de la fibre. Et poser des câbles sous-marins reste nettement moins onéreux que creuser. Conséquence, la plupart de ces câbles provenant d'Afrique et d'Asie pour relier l'Europe arrivent à Marseille »*. Aujourd'hui, 18 câbles relie la France à 57 pays en Europe, Afrique, au Moyen-Orient et en Asie/Pacifique. La même raison explique la croissance annuelle, 30 à 35 %, de ce hub, contre les 10 à 15 % pour les hubs continentaux. Aujourd'hui, *« déployer des applications d'IA passent d'abord par des infrastructures »*, ajoute Fabrice Coquio. Digital Realty compte aujourd'hui 13 centres en région parisienne et quatre à Marseille. La région s'appuie également sur les deux poids lourds locaux, CMA-CGM et Airbus Helicopters pour développer de nouveaux usages basés sur l'IA. Le transporteur maritime a créé un centre d'innovation à Marseille, baptisé Tangram, pour identifier les cas d'usage permettant de se différencier de ses concurrents, notamment Maersk et MSC. Il héberge aussi un accélérateur de startups, et a lancé un fonds d'investissement. De son côté, Airbus Helicopters utilise ces technologies, outre la logistique, pour améliorer ses processus de fabrication et la sécurité des vols. Les PME locales sont également invitées à bénéficier de l'IA. La société Riality IA lab, soutenue par la CCI de Marseille, propose un accompagnement pour identifier les cas d'usage pertinents. Elle a par exemple initié un cabinet spécialisé dans la propriété intellectuelle à l'utilisation de l'IA générative. Une liste d'initiatives loin d'être exhaustive.

Toute cette effervescence masque mal l'absence d'éditeurs de taille moyenne ou d'ESN locaux en dehors des filiales d'acteurs américains. Développer une vraie filière locale ne peut se limiter à attirer des entreprises étrangères, d'autant que l'arrivée de ces derniers se traduit rarement par un nombre conséquent d'emplois créés. L'arrivée attendue de Salesforce va se concrétiser par la création de 25 postes. De son côté, Digital Realty n'a pas voulu communiquer sur le nombre de salariés qu'il employait dans ses datacenters marseillais. La dynamique semble tout de même réelle. Reste à transformer l'essai. □

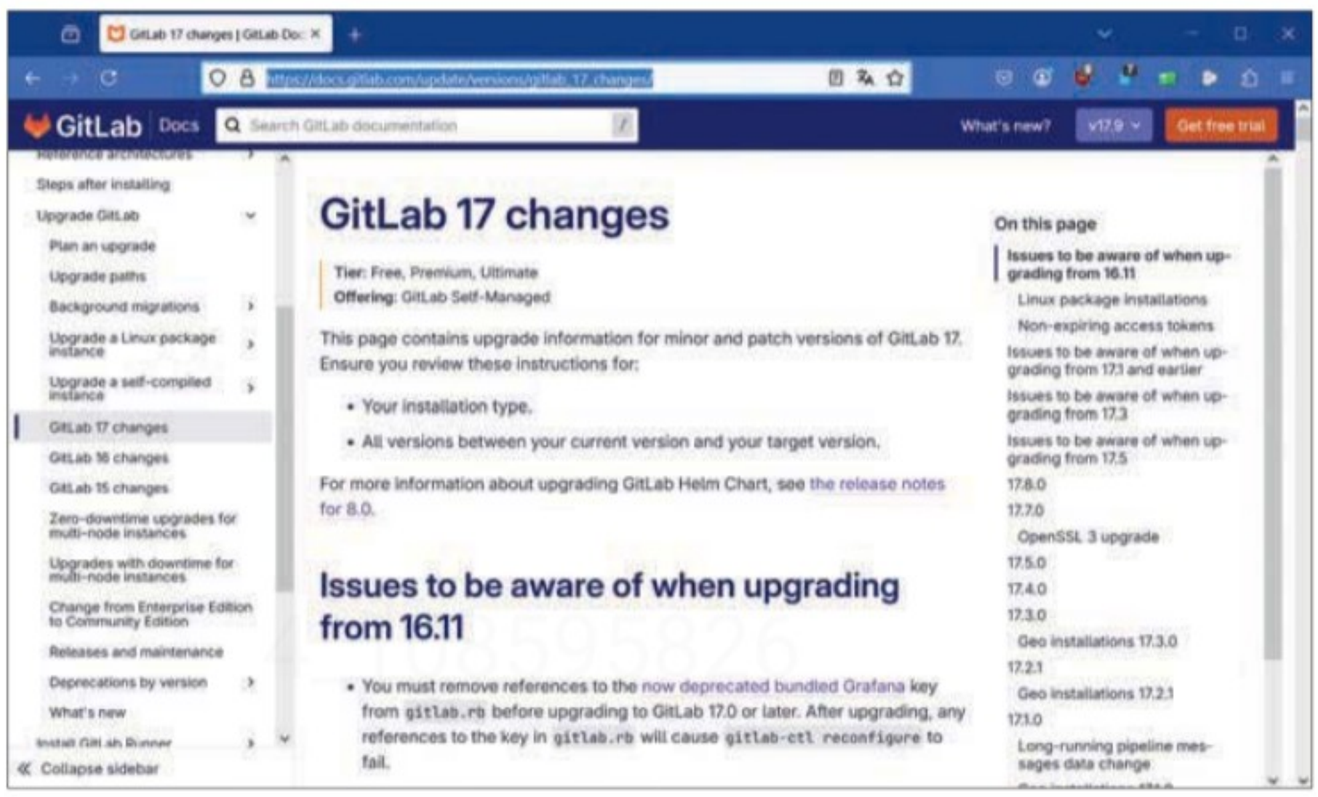
P. Br

Mises à jour

GitLab 17, toujours plus de fonctionnalités

La nouvelle version de GitLab, la 17, est disponible depuis quelques mois. Cette mise à jour majeure regorge de nouvelles fonctionnalités et d'améliorations cruciales, à en croire l'éditeur. Cela va des améliorations de gestion des projets aux commits signés, en passant par le nouveau catalogue de composants CI/CD. Nous allons voir ce qu'il en est dans cet article.

GitLab est sans doute la solution la plus populaire pour gérer des dépôts Git sur site. Il est utilisé par plus de 100 000 organisations. C'est une solution incontournable pour les développeurs et les entreprises qui cherchent à optimiser leurs workflows DevOps. Cette nouvelle version semble confirmer encore une fois l'engagement de GitLab à répondre aux besoins de sa communauté.



Si vous voulez consulter la liste exhaustive des nouvelles fonctionnalités de la version 17, rendez-vous à l'adresse https://docs.gitlab.com/update/versions/gitlab_17_changes

Pile logicielle

GitLab est une application Ruby on Rails qui utilise les logiciels suivants :

- Un système d'exploitation parmi ceux-ci : Ubuntu, Debian, CentOS, RHEL ou OpenSUSE
- Ruby (MRI) 3.2.5
- Git 2.33+
- Redis 6.0+
- PostgreSQL 14.9+

Gestion des projets et importation

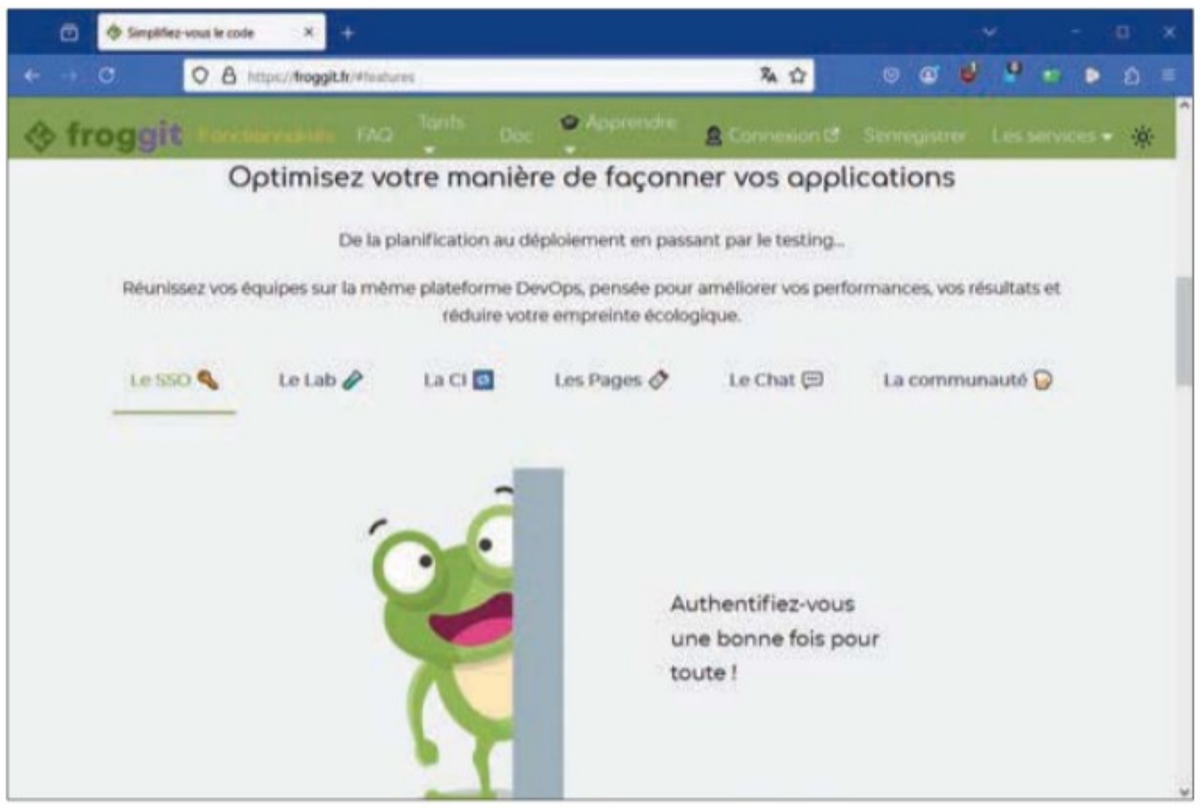
GitLab 17 apporte des améliorations assez significatives à la gestion des projets. Désormais, lors de l'importation d'un groupe ou d'un projet, vous pouvez utiliser le mode de transfert direct entre instances GitLab. Cela simplifie grandement le processus de migration, que vous quittiez gitlab.com pour une instance tierce telle que Froggit, ou inversement. L'interface utilisateur affiche le nom de la personne ayant importé le projet, ajoutant ainsi une couche de traçabilité dans les notes, issues, merge requests and co.

Améliorations diverses

La page des membres des groupes et projets a été repensée afin d'inclure aussi bien les membres directs que ceux invités via des groupes. Les informations sont ainsi fusionnées en un seul endroit, rendant la gestion des membres plus intuitive. Les milestones et itérations apparaissent désormais directement dans l'issue board, améliorant ainsi la visibilité et la gestion des tâches. Vous n'avez plus besoin de créer des labels personnalisés pour suivre les versions, tout est visible d'un seul coup d'œil. Il est désormais possible de signer les commits directement via l'interface graphique, fonctionnalité jusqu'ici réservée aux instances auto-hébergées. Cela renforce considérablement la sécurité et l'intégrité des commits. Le mot-clé rules: exist a été amélioré afin de tester l'existence de fichiers ou répertoires spécifiques avant d'inclure des fichiers dans les pipelines. Des options permettant de spécifier le projet et la branche à tester ont été ajoutées. Les scripts de post-traitement des jobs (after_script) s'exécutent désormais, même si le job concerné est annulé. Cela garantit que les opérations de nettoyage ou de notification sont toujours effectuées. Les erreurs liées aux paquets peuvent maintenant être vues directement dans l'interface utilisateur du registre des paquets, facilitant ainsi le débogage. Si vous utilisez des emojis dans vos issues ou vos commits, cette mise à jour vous permettra de les faire varier. GitLab prend en charge Unicode 15.1, donnant accès à un éventail bien plus large d'emojis. L'édition des règles de branches a été simplifiée. Il n'est plus nécessaire de naviguer dans plusieurs menus. L'interface unifiée rend l'édition plus rapide et intuitive.

Catalogue de composants CI/CD

Le catalogue de composants CI/CD (Continuous Integration/Continuous Deployment) est passé en release et propose une nouvelle section d'inputs dans les fichiers de pipeline. Cela standardise et facilite l'utilisation de composants dans les pipelines et contribue à améliorer l'efficacité des déploiements. GitLab était jusqu'alors quelque peu à la traîne par rapport au catalogue des Github actions.



Froggit est une plateforme Devops francophone de collaboration fondée sur GitLab.

Gestion des utilisateurs

Vous pouvez maintenant ajouter des participants externes à vos tickets via une quick action. Cette fonctionnalité est particulièrement utile pour tenir informées les personnes extérieures à votre instance GitLab, comme des clients ou des partenaires. Les avatars des utilisateurs peuvent être personnalisés via l'API. Cela s'avère particulièrement utile pour distinguer visuellement les utilisateurs bots des utilisateurs humains. La nouvelle fonctionnalité de gestion des sessions actives permet de voir toutes les sessions en cours pour un utilisateur donné. Cette fonctionnalité est très pratique lorsque vous vous connectez à GitLab depuis plusieurs navigateurs ou appareils.

Nouveau rôle : le planificateur

Le rôle planificateur est sans doute l'innovation majeure de cette release. Il enrichit la gestion des permissions et donne accès aux outils de planification de projets dans GitLab. Les avantages qui en découlent sont une meilleure répartition des tâches au sein des équipes et une gestion plus fine des responsabilités. Ce rôle est fait pour la gestion d'équipe ou de plusieurs projets en simultané. Il vous permet par exemple d'attribuer à un membre un accès limité à la planification sans pour autant lui ouvrir toutes les permissions d'un rôle développeur ou gestionnaire.

IL EXISTE TROIS ÉDITIONS DE GITLAB :

- **La Community Edition (CE) disponible gratuitement sous licence MIT Expat.**
- **L'Enterprise Edition (EE) qui inclut des fonctionnalités supplémentaires (https://about.gitlab.com/pricing/#compare-options) qui sont plus adaptées aux organisations comportant plus de 100 utilisateurs du logiciel. Pour utiliser EE et obtenir un support officiel vous devez souscrire à un abonnement.**
- **La JiHu Edition (JH), tailllée sur mesure pour le marché chinois.**

Vous trouverez sur le site about.gitlab.com plus d'informations concernant les abonnements, les services professionnels, la communauté, GitLab Enterprise Edition et GitLab CI, un serveur d'intégration en continu qui peut être aisément intégré à GitLab.

Gestion plus fine des tokens et de l'authentification

La sécurité et la gestion des tokens évoluent dans cette version, avec trois fonctionnalités clefs :

- la description des tokens qui ajoute des contextes précis pour mieux les identifier.
- la rotation simplifiée qui permet désormais de renouveler un token directement depuis l'interface graphique avant son expiration.
- les notifications d'expiration pour régler le problème des tokens oubliés. GitLab vous avertit désormais 60, puis 30 jours avant leur expiration.

Ces nouveautés renforcent la sécurité tout en réduisant les frictions pour les administrateurs. Grâce aux journaux des tokens d'authentification, vous pouvez voir directement quels projets utilisent un token spécifique. Terminé les mystères sur l'origine d'une intégration ou d'un workflow. Tout est dans le journal, il suffit de le lire. La gestion utilisateur est plus fine. Les administrateurs peuvent désormais visualiser et gérer plus facilement les utilisateurs, avec authentification à double facteur, les approbations en attente et le statut des administrateurs actifs. Cette visibilité accrue renforce la sécurité et l'efficacité dans la gestion des équipes.

Intégration à Kubernetes

L'utilisation conjointe de Kubernetes avec GitLab a été largement améliorée. La version 17 apporte le support de Kubernetes 1.31, une des toutes dernières versions, et un dashboard intégré pour configurer les agents et namespaces Kubernetes directement dans les fichiers CI/CD. Ces améliorations simplifient la gestion des déploiements et réduisent considérablement les risques d'erreur. L'intégration à Kubernetes a été renforcée. L'agent Kubernetes peut être configuré via l'API REST. Le démarrage de Kubernetes a

été simplifié. L'agent s'installe et se configure avec deux commandes simples. Les réconciliations Kubernetes peuvent être suspendues ou relancées directement depuis GitLab. Toutes ces fonctionnalités permettent une automatisation et une supervision encore plus efficaces, rendant Kubernetes plus accessible, même pour des équipes non expertes.

Sélection de l'agent Kubernetes dans les jobs

Vous pouvez maintenant spécifier directement, dans un job CI/CD, quel agent Kubernetes utiliser. Cela évite de configurer l'agent au niveau du projet entier. Il faut pour cela utiliser l'attribut environment.kubernetes.agent dans votre fichier YAML de configuration.

Administration personnalisée

GitLab introduit une nouvelle fonctionnalité en expérimentation : les Custom Admin Rules. Cela permet de personnaliser les accès pour les administrateurs. Vous pouvez, par exemple, accorder à un collègue des permissions limitées, comme la gestion des utilisateurs, tout en conservant pour vous ou d'autres les accès aux paramètres critiques de l'instance. Cette granularité représente une vraie révolution pour les entreprises qui gèrent des instances dédiées ou des forges multi-clients.

Changements majeurs dans la migration OpenSSL 3

La migration vers OpenSSL 3 dans GitLab 17.7 a subi des changements importants. Si votre environnement a encore recours à OpenSSL 2, il faudra prévoir un certain temps pour adapter vos configurations. Un guide de migration est disponible afin de vous aider à passer cette étape sans encombre. Il est préférable de tester cette mise à jour dans un environnement de test avant d'effectuer des déploiements sur des serveurs en production.

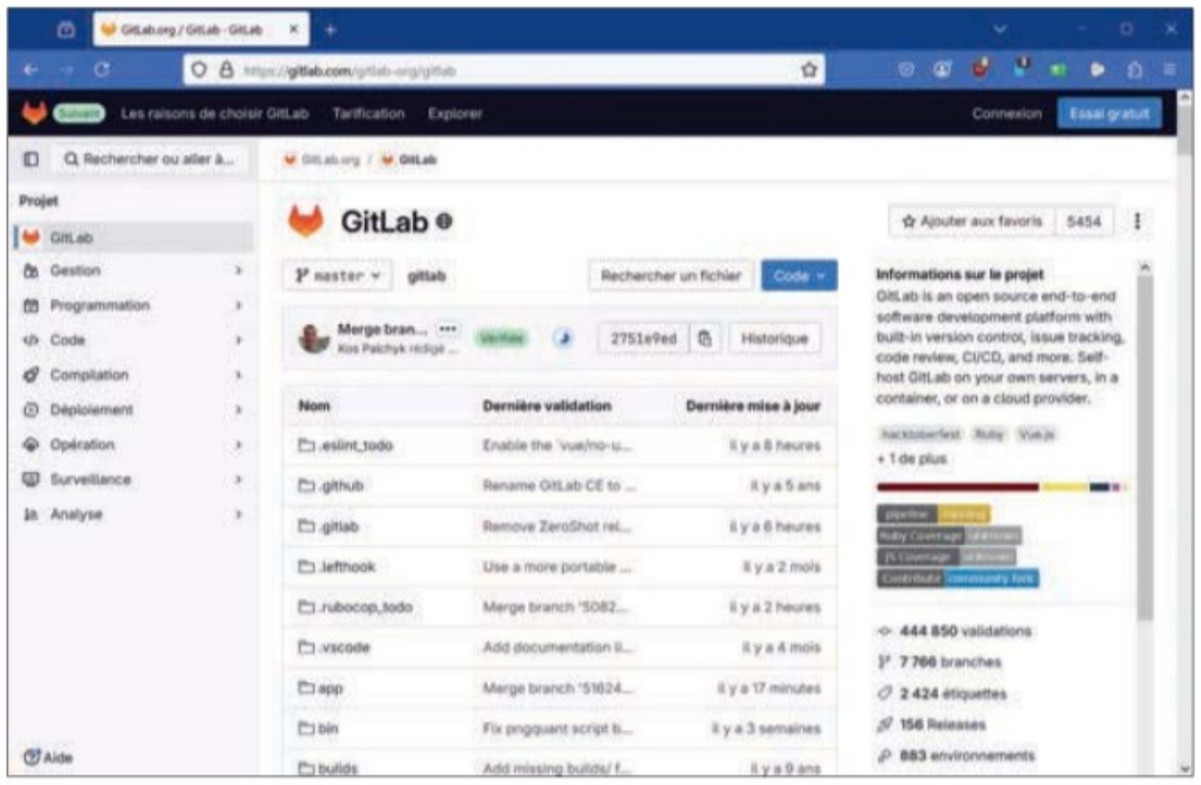
FUSION PROGRAMMÉE

Il est possible dans la nouvelle version de programmer la fusion des merge requests à une date et une heure précise. C'est très pratique si vous devez publier un contenu (un site statique, par exemple) à 7h du matin mais qu'à cette heure-là vous êtes en pleine réunion ou indisponible. Grâce à cette nouvelle fonctionnalité, plus besoin d'être présent. Il suffit de configurer la merge request et de laisser GitLab s'occuper du reste. Toutes les validations habituelles (CI/CD, approbations, etc.) devront bien évidemment avoir été passées avec succès. C'est une fonctionnalité CORE, ce qui veut dire qu'elle est disponible dans toutes les versions, y compris la gratuite. La fusion programmée est probablement l'une des nouveautés les plus utiles pour optimiser les déploiements sans intervention manuelle.

Logiciels open source pour collaborer sur le code

Pour connaitre toutes les fonctionnalités offertes par GitLab, rendez-vous sur la page qui y est dédiée sur le site de Gitlab à l'adresse https://about.gitlab.com/features/. Vous y découvrirez notamment comment :

- Gérer des dépôts Git avec des contrôles d'accès fins permettant de garder votre code sécurisé
- Réaliser des revues de code et améliorer la collaboration avec des merge requests
- Compléter les pipelines d'intégration en continu (CI), ainsi que de déploiement et de livraison en continu (CD) pour construire, tester et déployer vos applications
- Définir pour chaque projet un suivi et une gestion des bugs ainsi qu'un wiki



La référence absolue en matière de développement du logiciel GitLab est hébergée sur GitLab.com

Héberger ses propres modèles de ML

GitLab prend un virage plutôt intéressant en intégrant un registre de modèles de machine learning. Que vous travailliez en SaaS ou en self-hosted, vous pouvez désormais héberger et gérer vos artefacts de ML directement dans GitLab. Cela ouvre la porte à une gestion centralisée des projets de type data science et des workflows ML/AI.

Couverture des tests Java avec JaCoCo

Les développeurs Java n'ont pas été oubliés. Les rapports de couverture de tests JaCoCo sont désormais visibles directement dans l'interface de GitLab. Avant, il fallait plonger dans les logs pour trouver ces informations.

Maintenant, tout est accessible depuis l'interface des merge requests et/ou la page de pipeline. Cela représente un gain important en termes de visibilité et de simplicité pour les équipes de développement.

Déployer des sites statiques avec l'attribut Pages

GitLab simplifie encore le déploiement de sites statiques grâce à l'attribut Pages. Avant, vous deviez nommer le job Pages et respecter des conventions bien précises, afin que GitLab comprenne qu'il s'agissait d'un déploiement de GitLab Page. Il suffit maintenant d'ajouter l'attribut pages : true dans le job YAML, quel que soit son nom. C'est une petite modification, mais qui donne plus de souplesse et rendra les pipelines plus lisibles.

La JiHu Edition (https://about.gitlab.cn/) a été créée spécifiquement pour le marché chinois.

Désactivation partielle de la double authentification

Si vous perdez un appareil d'authentification (une clé physique, par exemple), vous n'aurez plus besoin de désactiver toute votre double authentification. Il suffira de désactiver seulement l'appareil concerné.

Notifications de connexions suspectes

GitLab améliore les emails qu'il envoie en cas de connexion depuis un appareil inconnu. Ces alertes incluent désormais plus d'informations comme la ville et la région de l'adresse IP. Vous pouvez ainsi détecter rapidement, et surtout de manière détaillée, toute tentative de connexion non autorisée.

Déploiements

Les déploiements affichent désormais des informations détaillées comme les tags et notes de release, les jobs utilisés ou les artefacts déployés. Tout est accessible en un coup d'œil, sans devoir naviguer entre plusieurs sections.

Audits et API : nouvelles options

GitLab 17 a ajouté plusieurs fonctionnalités d'audit et d'API pour les administrateurs d'instances self-hosted. Les logs des actions administratives permettent de voir qui a effectué des actions privilégiées et quand. La consultation des tokens via l'API permet d'obtenir son nom, sa date de création et son usage. Ces options renforcent encore plus le contrôle et la sécurité des instances.

Sécurité renforcée des paquets NPM

Des améliorations sur la sécurité des paquets NPM et des nouveautés pour les règles de branche, ainsi qu'une gestion des utilisateurs plus intuitive pour les administrateurs d'instance, font également partie des nouveautés de la version 17. GitLab a introduit des règles pour protéger les paquets contre des suppressions accidentelles. C'est une avancée cruciale pour éviter des interruptions dans les déploiements.

GitLab Duo Enterprise

GitLab Duo Enterprise est un nouvel ajout en matière d'IA construit sur les capacités de GitLab Duo Pro. Il peut être utilisé pour détecter et corriger des problèmes de sécurité, résumer des discussions sur les bugs et les merge requests, résoudre les goulots d'étranglement CI/CD et améliorer la collaboration entre les équipes. Cela inclut un tableau de bord qui fournit un aperçu de l'impact de l'IA sur le cycle de vie du développement. Les autres ajouts à GitLab 17 incluent la disponibilité de GitLab Dedicated on Google Cloud, de nouvelles intégrations SAST, des fonctionnalités d'analyse de produits, d'observabilité, des capacités de planning agile et un registre de modèles pour développer de l'IA/ML à l'intérieur de GitLab. *« GitLab continue à révolutionner la manière des organisations de développer, de construire, de sécuriser et de déployer des logiciels plus vite en tirant parti d'une plateforme DevSecOps complète »*, a déclaré David DeSanto, le chef produit de GitLab. *« GitLab 17 fait rentrer dans le futur de l'innovation des logiciels pilotés par l'IA, en supprimant les silos à travers chaque équipe impliquée par la livraison de valeur logicielle, de l'automatisation des tâches et des workflows complexes, et en garantissant que la sécurité et la conformité sont intégrées dès le départ. »*

Mettre à jour GitLab

Même si vous n'êtes pas encore tout à fait convaincu des apports de la nouvelle version, en mettant à jour GitLab vous profiterez des toutes dernières innovations, vous renforcerez la sécurité et optimiserez vos workflows. Les nouvelles fonctionnalités, telles que le rôle planificateur, la gestion améliorée des tokens ou encore l'intégration avec Kubernetes, apportent des gains bien réels en termes d'efficacité et de collaboration. De plus, n'oubliez pas que rester sur une version obsolète peut exposer votre infrastructure à des failles de sécurité. □

T.T

Orchestration Vers le chaos numérique ?

Une étude réalisée par Coleman Parks pour le compte de Camunda, un éditeur de logiciels spécialisés dans l'orchestration des processus évoque la possibilité d'un cataclysme numérique du fait d'une automatisation mal contrôlée.

La transformation numérique est aujourd'hui sur toutes les lèvres, en particulier dans les entreprises qui cherchent à gagner en efficacité et en compétitivité. Elle a conduit de nombreuses entreprises à se tourner vers l'automatisation et, plus récemment, a alimenté l'engouement autour de l'intelligence artificielle (IA) pour gérer et automatiser les processus de bout en bout. Les infrastructures et processus numériques modernes sont complexes et interdépendants, ce qui fait de l'automatisation des processus de bout en bout un défi de taille.

Une orchestration nécessaire

Créer ou modifier un processus de bout en bout est difficile, car cela implique des changements potentiels dans de nombreux systèmes différents. D'où l'importance de l'orchestration des processus, qui consiste à faire converger et à coordonner toutes les tâches manuelles ou automatisées qui composent un processus. Si l'orchestration des processus vise à relier ces différents endpoints (personnes ou systèmes), elle permet également à l'entreprise de mettre à jour ses divers processus depuis une même interface.

Par exemple, les entreprises comptent en moyenne une cinquantaine de ces endpoints. 85 % des personnes interrogées pour ce sondage affirment qu'il est plus difficile de gérer les processus globaux de bout en bout lorsque de multiples tâches automatisées sont combinées.

La place de l'IA

L'IA peut optimiser de nombreux workflows humains et aider à rationaliser des processus complexes, à améliorer la prise de décision et à débloquer des gains d'efficacité que des processus manuels ne permettraient jamais d'atteindre. La plupart des entreprises souhaitent adopter de nouvelles fonctionnalités d'IA au cours des trois prochaines années dans le but de mieux analyser et d'améliorer les processus.

Motifs de complexité des processus

50 ↑ Les entreprises comptent en moyenne une **cinquantaine** de **composants et d'endpoints**. Ce nombre a augmenté d'environ **19 %** au cours des cinq dernières années.

Composants/endpoints les plus courants :

70 % – Applications d'entreprise (par exemple, SAP, Oracle, Salesforce, etc.)

65 % – Technologies d'automatisation des tâches (automatisation robotisée des processus [RPA], iPaaS, gestion des décisions/règles métier)

48 % – Applications d'IA/apprentissage automatique (OpenAI, Azure OpenAI Hugging Face, traitement intelligent des documents)

41 % – API

86 % déclarent que les réglementations ont augmenté la complexité des processus

78 % déclarent que les modèles de workflows complexes et/ou les processus de longue durée augmentent la difficulté de l'automatisation.

85 % affirment qu'il est plus difficile de gérer les processus globaux de bout en bout lorsque de multiples tâches automatisées sont combinées.

Les causes de cette complexité :

60 % – Logique conditionnelle et/ou de regroupement qui prend en compte des règles métier complexes

56 % – Les systèmes sont anciens et il est difficile de s'y connecter

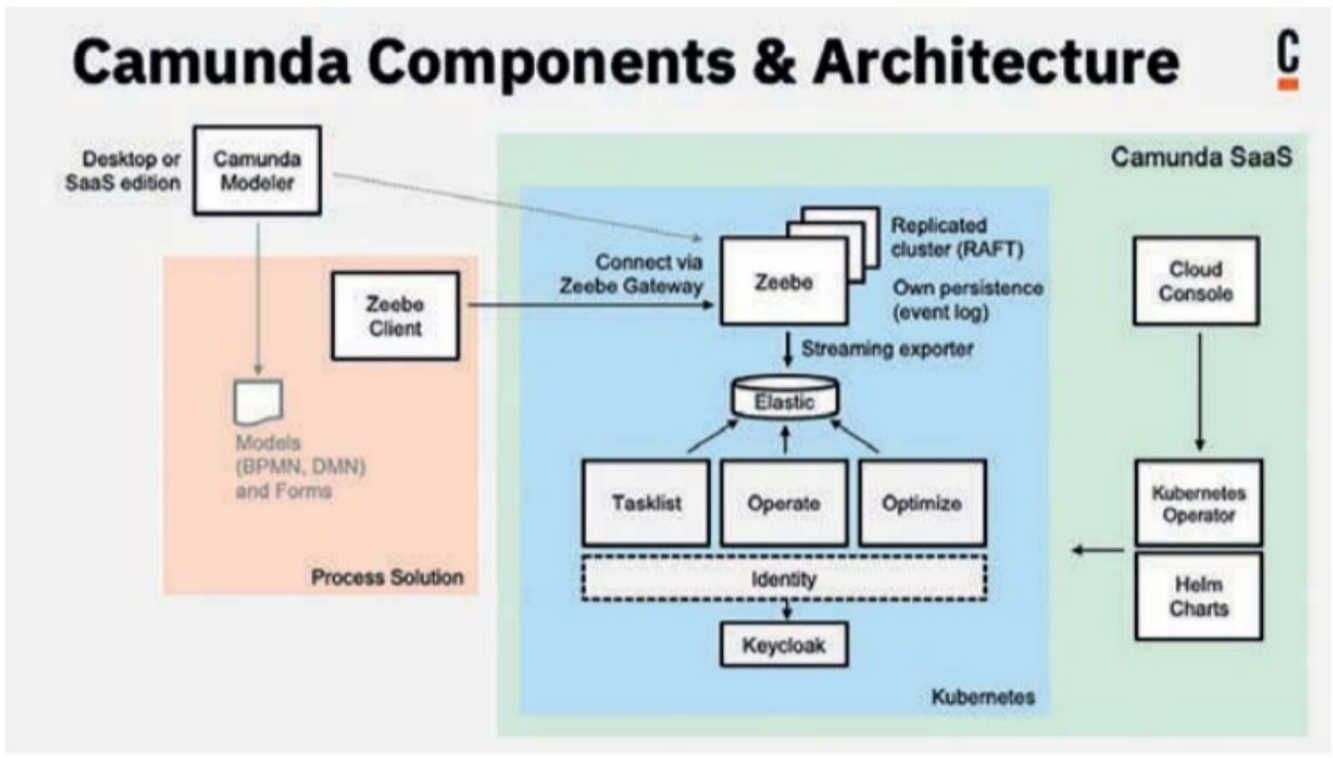
49 % – Plusieurs systèmes doivent être pris en compte

39 % – Il faut composer avec la logique humaine

34 % – Les systèmes sont développés en interne et il est difficile de s'y connecter

23 % – Les sous-processus ou systèmes concernés appartiennent à une autre équipe

83 % **envisagent d'adopter des outils pour orchestrer et coordonner les tâches de bout en bout sur différents endpoints de processus.**



L'architecture et les composants de la suite de Camunda.

Toutefois, elles admettent également qu'elles peinent à faire évoluer l'IA et à la rendre opérationnelle dans toutes les sphères de l'entreprise.

En définitive, presque toutes les personnes interrogées pensent que l'IA devra être orchestrée au sein des processus métier automatisés, au même titre que tout autre endpoint. Ainsi 93 % du panel affirment qu'à terme, les applications et les services d'IA devront être orchestrés dans leurs processus métier si l'entreprise veut tirer le meilleur parti de ses investissements dans l'IA. Cela peut avoir des conséquences notables. 84 % déclarent que le manque de transparence sur la façon dont les applications et les services d'IA sont utilisés dans les processus métier entraîne des problèmes de conformité réglementaire.

Automatisation des processus

Les grandes entreprises s'accordent à dire que l'automatisation des processus est essentielle à la transformation numérique. La quasi-totalité d'entre elles dispose d'ailleurs d'un centre d'excellence pour l'automatisation des processus. De nombreuses entreprises ont constaté une hausse de la croissance de leur activité au cours de l'année écoulée grâce à l'automatisation des processus et ont pris l'engagement d'augmenter leurs dépenses dans ce domaine de 10 % ou plus. Malgré cela, moins de la moitié de leurs processus opérationnels sont automatisés en moyenne à ce jour. Selon elles, leurs solutions actuelles d'automatisation des processus deviennent obsolètes, et les initiatives d'automatisation peinent à suivre le rythme de l'évolution de l'activité. C'est notamment le cas des entreprises qui ont investi dans des solutions ponctuelles pour automatiser des tâches particulières et qui se retrouvent aujourd'hui avec des solutions d'automatisation cloisonnées aux bénéfices limités.

Si 93 % disposent d'un centre d'excellence pour l'automatisation des processus et que 87 % déclarent avoir constaté une hausse de la croissance de leur entreprise grâce à l'automatisation des processus au cours de l'année écoulée et que 83 % prévoient d'augmenter de 10 % ou plus leurs dépenses en matière d'automatisation, il n'en reste pas moins que seuls 46 % des processus organisationnels sont automatisés. 72 % déclarent que les initiatives d'automatisation ne parviennent pas à suivre le rythme du changement dans les entreprises modernes et 82 % déclarent que leurs solutions actuelles d'automatisation des processus commencent à devenir obsolètes.

Une maturité variable

Peu d'entre elles ont atteint le stade avancé, avec tous les avantages que cela implique. La plupart des entreprises disent pratiquer l'orchestration des processus, mais pour un grand nombre d'entre elles, cela signifie simplement l'utiliser pour un seul cas d'utilisation ou workflow. Certaines entreprises ont réussi à intégrer l'orchestration des processus à travers de multiples cas d'utilisation dans plusieurs domaines ou départements. Par contre, elles sont très peu nombreuses à l'avoir intégrée à l'échelle de l'entreprise (12 %).

La collaboration métier/ IT au cœur du débat

Dans la plupart des entreprises, les équipes opérationnelles et informatiques peinent à collaborer sur des processus et des projets individuels, que ce soit lors de la mise en place ou pour leur maintenance et optimisation continues. Une mauvaise communication entre ces équipes peut entraîner la création ou le déploiement de solutions inadaptées pour les clients, ce qui peut avoir un impact notable sur le délai de mise sur le marché ainsi que sur l'expérience et la satisfaction des clients (et des employés).

Les entreprises reconnaissent le manque d'alignement entre leurs équipes informatiques et opérationnelles lorsqu'il s'agit de répondre aux exigences métier. Le risque est bien réel pour les projets d'automatisation dont la mise en place peut être problématique dans des environnements complexes comportant des systèmes hérités. Dans les grandes entreprises, les responsables métier et informatiques s'accordent à dire que les efforts d'automatisation et les stratégies métier ne sont pas assez souvent alignés. D'ailleurs l'incompréhension est des deux côtés. 44 % des collaborateurs informatiques déclarent que les responsables métier ne se rendent pas compte de la quantité de travail que leur demande la modification d'un processus métier alors que 46 % des collaborateurs métier déclarent que les équipes opérationnelles et informatiques n'ont pas la même vision ni la même compréhension des besoins de l'entreprise.

Plus d'un tiers de ceux-ci déclarent que les équipes informatiques refusent souvent de répondre à leurs demandes en invoquant des contraintes techniques. 43 % des utilisateurs métiers s'accordent à dire que les projets sont parfois retardés en raison d'un manque de compréhension et d'une mauvaise communication entre les équipes opérationnelles et informatiques. ☐

B.G

Mode de travail

Freelance, le goût de la liberté

Les missions en indépendant sont assez répandues dans l'IT, favorisées par le mode projet. Le revenu journalier moyen a augmenté depuis cinq ans.

Il n'est jamais trop tard pour devenir indépendant si l'on en ressent l'envie. 9 freelances sur 10 sont d'anciens salariés, selon le « Panorama du freelancing » de la plateforme Freelance.com, publié en 2022. Les canaux pour trouver des missions sont variés : réseau personnel (76 %), réseaux sociaux et prospection (51 %), plateformes de freelancing (41 %). Le freelance souhaite organiser lui-même ses projets, temps et lieu de travail. Ses principales motivations sont *« la liberté de pouvoir exercer son métier sans contrainte hiérarchique, de gérer temps de travail et congés au cours de l'année, l'intérêt des missions en soi et pour améliorer son employabilité »*, d'après Anthony Bergès, DGA de la plateforme Freelance.com.

« L'indépendant est attiré par le changement fréquent d'environnement, l'absence de lien de subordination et le recul vis-à-vis des relations de pouvoir en entreprise », ajoute Sophie Bayle, responsable du département Technology du cabinet de recrutement Michael Page, qui accompagne freelances et managers de transition. Pour Juliette Bricout, UX/UI designer, *« être indépendante, c'est être flexible, libre, ne pas dépendre d'un endroit pour travailler. J'ai déjà travaillé depuis Malte et Barcelon »*.

Les contreparties pèsent leur poids dans la balance : revenus variables et non sécurisés, moins bonne protection sociale, santé et retraite, temps passé aux tâches commerciales et administratives. A chacun de soupeser les risques. *« Expérience, réseau, renforcement de l'expertise par la formation continue et la veille sont les clefs d'obtention des missions »*, remarque Thomas Bettan, expert data.

Il y a un peu plus d'un million de freelances dans les métiers des prestations intellectuelles en France, dont 23 % dans l'IT et l'ingénierie, selon une étude de Datastorm publiée en 2022. Ils sont plus diplômés du supérieur (76 %, 84 % en IT/ingénierie), plus âgés (45 ans en moyenne) et plus masculins (68 %, 84 % en IT/ingénierie) que leurs homologues salariés. 13,1 % des actifs en IT/ingénierie sont des freelances, pour un CA annuel moyen de 44 457 euros, quel que soit leur statut (indépendant, structure type SARL ou SASU, portage salarial). D'après Sophie Bayle, près de la moitié des freelances IT sont en Île-de-France, le travail sur site étant récurrent.

POSTES EN FREELANCE ET MANAGEMENT DE TRANSITION LES + RECHERCHÉS (TMJ)	0-2 ans	2-5 ans	5-10 ans	10 ans et +
Directeur des systèmes d'information/Manager de transition	900 - 1000	900 - 1200	1000 - 1200	1200 - 1500+
Manager de transition (études, infrastructures…)	900 - 1000	900 - 1200	1000 - 1200	1200 - 1500+
RSSI	850 - 1000	900 - 1200	1000 - 1200	1200 - 1500+
Devops	700 - 850	850 - 950	950 - 1050	1050
PMO	600 - 700	700 - 800	800 - 1000	1050
Ingénieur sécurité/cybersécurité	500 - 600	600 - 800	800 - 900	950+
Architecte d'entreprise/Urbaniste	900 - 1000	900 - 1200	1000 - 1200	1200 - 1500+
Architecte (Lead/Système/Infra/Solution/Data/Cloud)	850 - 1000	900 - 1200	1000 - 1200	1200 - 1500+
Lead développeur/Tech Lead	650 - 750	750 - 950	850 - 1000	900 - 1050
Chef de projet MOA/Product owner	600 - 700	650 - 750	750 - 850	800 - 950
Chef de projet MOE/Scrum master	600 - 700	650 - 750	750 - 850	800 - 950
Data Analyst/Data Scientist/Data Engineer	600 - 700	650 - 750	750 - 850	800 - 950
DBA	450 - 550	550 - 650	650 - 850	750 - 950
Ingénieur tests/recettes/QA	450 - 550	550 - 650	650 - 850	750 - 950
Business analyst	450 - 550	550 - 650	650 - 850	750 - 950
Ingenieur études et développement (C#/.Net, Java, Angular, BI…)	500 - 600	600 - 750	700 - 850	750 - 950
Ingénieur systèmes & réseaux	500 - 600	600 - 750	700 - 850	750 - 950
Administrateur systèmes/réseaux	450 - 550	550 - 650	650 - 850	750 - 850
Technicien support (applicatif, exploitation, VIP)	350 - 400	400 - 450	450 - 500	500 +

Le TJM (Taux Journalier Moyen) indiqué est le montant HT présenté au client dans le cadre de sa mission en région parisienne. Ces montants ne comprennent pas les frais annexes (repas, transport, frais de portage, …) et sont basés sur le nombre d'années d'expérience sur la fonction. Les TJM en région sont de 7 à 10% inférieurs par rapport à l'Île-de-France.

Les missions les plus courues en France cette année sont dans les domaines suivants : cybersécurité, cloud, SAP et DevOps. Viennent ensuite celles en data, en vue de projets d'IA.

Des équipes projet hybrides

« Les projets de transformation, à durée donnée, sont structurants pour le freelancing IT, analyse Sophie Bayle. *Aujourd'hui, gérer son activité est facilité par les outils en ligne et le télétravail. L'accès aux missions est aisé, entre réseaux, plateformes, cabinets et ESN. La maîtrise des technologies et les compétences primant sur le statut, l'hybridation est réelle dans les projets qui peuvent réunir salariés de l'entreprise, ESN, freelances en direct et via des ESN »*. Anthony Bergès, aussi DG de l'ESN Inop's qui appartient à

Freelance.com, ajoute : *« Les freelances offrent des compétences plus larges que les ESN, des technologies anciennes à celles de pointe. Et les mondes s'hybrident. Inop's rassemble freelances, PME, startups partenaires et directeur de projet salarié de notre ESN, pour monter une équipe adaptée aux besoins. »*

Des revenus variables

Selon Michael Page, les taux journaliers moyens (TJM) des freelances IT ont augmenté depuis cinq ans, notamment à cause de l'inflation. Ceci recouvre des tarifs très variés, selon l'expérience du freelance, la complexité de la mission et sa durée. Plus celle-ci est longue, moins le TJM est élevé en général. Sophie Bayle avance qu'*« en 2025, les TJM ont tendance à se stabiliser, voire baisser, les entreprises rationalisant leurs dépenses. Les projets en cybersécurité restent néanmoins inflationnistes face à la pénurie de talents »*.

Les freelances français souffrent de la position confortable des ESN sur le marché des prestations de services IT. L'Allemagne et le Royaume-Uni sont plus favorables au freelancing, comme les États-Unis. *« Il existe une marge de progression du freelancing en France, où le salariat reste dominant,* précise Anthony Bergès. *De grandes entreprises restent frileuses vis-à-vis des freelances. Plus on va au Nord de l'Europe, plus le marché du freelancing est mature. »*

*Quels sont pour vous les 2 principaux **avantages** à exercer une activité professionnelle en statut d'indépendant ?*

*Quels sont pour vous les 2 principaux **inconvénients** à exercer une activité professionnelle en statut d'indépendant ?*

Les plateformes, de l'intermédiation aux services

Les plateformes, contre le versement d'une commission sur le prix de la mission — 12 % chez Freelance.com qui comprend 50 000 profils IT, soit les deux tiers de ses profils qualifiés — offrent divers avantages. Le premier : élargir le champ des possibles. Micha Kaufman est cofondateur et PDG de la plateforme américaine Fiverr, présente dans 160 pays : *« Fiverr permet au freelance d'accéder à des opportunités à l'international, au-delà de son réseau local. C'est aussi une communauté d'échange de meilleures pratiques entre freelances. »* Axelle Lenoury, growth marketing manager chez Fiverr France, ajoute : *« Fiverr offre une visibilité mondiale. Le freelance peut présenter ses compétences, trouver des clients de toutes tailles et de tous secteurs, réduire la charge administrative (devis, facturation, relance clients) et fixer ses propres tarifs. Les professionnels de l'IT occupent une position forte en raison de la demande élevée et constante de leurs compétences. »*

Divers services sont offerts par les plateformes : portage salarial, services administratifs et financiers (comme être payé avant le règlement du client), outils de productivité. Fiverr vient de lancer Fiverr Go, une plateforme ouverte d'outils d'IA personnalisés (assistant personnel, création de modèles) pour faire gagner du temps et faciliter le développement commercial. Micha Kaufman précise : *« Nous avons en parallèle lancé Fiverr Dev, l'écosystème de développeurs de Fiverr Go, qui va leur permettre de créer des applications d'IA qu'ils pourront monétiser. »*

Être freelance IT aujourd'hui, c'est savoir allier compétences technologiques et entrepreneuriales (gestion, commercial, communication…), en s'appuyant sur les réseaux et outils pertinents pour développer son activité. □

C.C

UNE UX/UI DESIGNER ET UN EXPERT DATA TÉMOIGNENT

Juliette Bricout, ingénieure en informatique, débute comme développeuse dans l'édition logicielle. Puis elle se forme en 2019 à l'UX/UI design et s'inscrit à plusieurs plateformes de freelancing : internationales comme Upwork et Fiverr, françaises comme Malt et Comet. *« C'est un gain de temps. J'ai commencé avec des prix bas pour avoir des avis et gagner en visibilité, travaillant parfois soir et week-end. Depuis trois ans, je choisis mes missions. J'ai augmenté mes prix et réalise plus vite les tâches. Je travaille pour des micro-entrepreneurs, startups, moyennes et grandes entreprises, beaucoup à l'international, notamment américaines. Ma veille est régulière pour suivre les tendances. Mes revenus augmentent chaque année, la majorité provenant de Fiverr et de clients directs ».*

Thomas Bettan, diplômé d'école de commerce et en informatique de gestion, après une dizaine d'années en expatriation à différents postes en entreprise, crée sa société de prestations IT en 2017 après son retour en France. Il s'appuie sur des plateformes pour travailler pour de grands comptes (aujourd'hui Freelance.com et son ESN Inop's, Malt et Freework). Depuis cinq ans, il s'est spécialisé dans la data, s'appuyant sur une démarche de certification : *« Mon chiffre d'affaires est réalisé à moitié par le réseau, à moitié via les structures partenaires. J'anime aussi des formations. Mes motivations : construire ma propre route, le contenu et la variété des missions, les relations humaines, la volonté de comprendre l'environnement, les défis et process internes du client ».*

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

LE SEUL ÉVÈNEMENT
100% SÉCURISÉ

IT AND CYBERSECURITY MEETINGS FRANCE

one to one Meetings Exhibition
by Weyou Group

WWW.IT-AND-CYBERSECURITY-MEETINGS.FR

18, 19 & 20 MARS 2025

PALAIS DES FESTIVALS ET DES CONGRÈS DE CANNES

ILS SONT DÉJÀ INSCRITS

6cure, ACKnowledge, Adaptive Shield, adista, aDvens, AIST, Akamai, ALL4TEC, allentis, Anozr Way, ARMIS, Arrow, APIXIT, AppOmni, ARCAD,
Avanade Cliquer, axians, bconnex, betasystems, BeyondTrust, Bitdefender, BITSIGHT, Blue Mantis, BlueTrusty, board of cyber, Banques Business, CATO, cegedim, Centhys, CLOUDFLARE,
console, Contrast, CROWDSTRIKE, CRYPT.ON IT, CUSTOCY, CybelAngel, Cyber Guru, CYBER INVESTIGATION, CYBERARK, cybereason, cyberwatch, CYBLEX, DATACORE, dbSQWare, Delinea,
DELL Technologies, devensys, DIFENSO, DIGITAL REALTY, digital.ai, dust MOBILE, EASYVISTA, EATON, efficient IP, elastic, elba, EPOS, ERCOM, ERICSSON, ESET,
eurofiber, EV Observe, EXCUBE, EXCLUSIVE NETWORKS THALES, f5, F24, Filigran, FORTINET, free PRO, GATEWATCHER, GitGuardian, GLIMPS, GROUPE CONVERGENCE, HARDIS GROUP,
HarfangLab, HCLSoftware, HEXANET, HOLISEUM, HUMAN, IBM, IC CONSULT, IDNA MYRIAD, ilex IAM Platform Inetum, infinigate, infoblox, Insight, interdata, iSendPro, ITS Ibelem,
Jabra GN, JUNIPER, Kamaé, KDDI France, KEEPER, keepit, KLEE GROUP, KnowBe4, koesio, LastPass, leviia, Linkt, LOGPOINT, LogRhythm,
Lutessa, Maltem, ManageEngine, Mantra, merox, METSYS, MITEL paloalto, mimecast, mindflow, memority, naitways, nameshield, NASUNI, NEOTRUST,
NeoYAD, NetApp, netskope, netsystem, netwrix, ninjaOne, nomios, NOZOMI NETWORKS, OBJECT FIRST, Oeil pour Oeil, OGO, okta, Olfeo, ONE IDENTITY, oodrive,
opentext Cybersecurity, OPSWAT, Cyberdefense, OVERSOC, OWN, Panasonic CONNECT, Patrowl, Ping Identity, pradeo, PRIMX, proofpoint, PURESTORAGE, Qualys, radware,
RAPID7, RCDevs, REEL iT GROUPE, Riot, rubrik, rubycat, sofec, SailPoint, SCC, sea tpi, sewan, SFR BUSINESS, Sharekey, SILVERFORT, SKYBOX SECURITY,
SNS SECURITY, snyk, solarwinds, SOPHOS, sosafe, SPIE, splunk>, STORMSHIELD, Suricate, SUSE, Symantec by Broadcom, synetis, sysdig, TANIUM, tdf,
TEHTRIS, TELEHOUSE, tenable, Tenacy, THEGREENBOW, TREND, TrustBuilder, tufin, TYREX, UBIKA la nouvelle DenyAll, vade, VARONIS, VEEAM, VERACODE, VirtualBrowser,
WITH SECURE, WIZ, xmco, ZeroTrust, Zerto a Hewlett Packard Enterprise company, zpe

Liste des exposants inscrits arrêtée au 21/02/2025

BY weyou
Professional Exhibitions
one to one Meetings Exhibitions

Une IA au sommet

Sommaire

Les MSSP partout tout le temps ? ... P68

Checkpoint fait le choix de la plateformisation ... P72

Une nouvelle fonctionnalité de mise en quarantaine dans PyPI ... P74

Tribune : Données personnelles, une meilleure sensibilisation en 2025 ... P77

Les enjeux de la journée protection des données ... P78

Eva Chen (Trend Micro) nous livre sa vision du duo IA et cybersécurité ... P79

L'évolution de la menace impose un changement de stratégie des RSSI ... P80

La sensibilisation du personnel hospitalier à la cybersécurité toujours d'actualité ... P82

Désolé, encore de l'intelligence artificielle, mais nous étions un peu obligés d'en parler, alors que février a été marqué par le très attendu Sommet pour l'IA. Nouvelle grand-messe internationale du secteur, cet événement a accordé une place centrale à la cybersécurité, notamment à travers l'axe de l'IA de confiance, si cher à nos acteurs français et européens.

L'InfoCR a eu la chance de rencontrer Eva Chen, cofondatrice et directrice générale de Trend Micro, qui nous a partagé son point de vue sur les avancées de l'IA dans le secteur. Elle nous a expliqué comment l'intelligence artificielle renforce aujourd'hui les capacités des outils et plateformes de cybersécurité.

La transition est toute trouvée avec notre dossier du mois, consacré aux fournisseurs de services de sécurité managés (MSSP). Ce modèle, en plein essor, qui n'a pas manqué, lui non plus, de négocier le virage technologique en intégrant l'IA à ses services.

Et pour rester dans le thème, nous vous informons que le prochain numéro de L'InfoCR sera dédié à la sécurité de l'intelligence artificielle. Promis, après ça, on fera une pause pour un détour vers le chiffrement post-quantique.

Les MSSP partout tout le temps ?

Face au manque de compétences, à la complexification du paysage cybernétique et au besoin croissant de sécurité 24/7, de nombreuses entreprises, grandes et petites, se tournent vers les fournisseurs de services de sécurité managés (MSSP) pour gérer tout ou partie de leur cybersécurité. Une approche qui allie flexibilité et expertise, mais qui reste elle-même confrontée aux défis de recrutement et soulève des questions de réactivité et de maîtrise des environnements critiques.

S'il fallait leur trouver un point de départ, l'émergence des MSSP peut être datée aux années 1990, selon Checkpoint. Durant cette période, des fournisseurs d'accès Internet (FAI) proposaient à leurs utilisateurs des dispositifs de pare-feu gérés par leurs soins. Toutefois, historiquement, les besoins en matière de cybersécurité sont restés, et restent encore, pour une grande partie, gérés en interne après l'achat de solutions auprès d'éditeurs.

Répondre à un paysage complexe

Peu à peu pourtant, le MSSP tend à être adopté comme modèle économique par de nombreuses entreprises de cybersécurité, y compris les éditeurs. Car, avec le temps, la menace a évolué, la surface d'attaque s'est étendue, les réseaux se sont complexifiés, le nombre de terminaux a explosé, en même temps que les besoins de protection et les outils pour répondre aux risques. Avec, pour conséquence, toujours plus de confusion pour les organisations. De cette complexification a émergé ce besoin de services externalisés, proches du modèle des fournisseurs de services managés (MSP), qui assurent un support informatique général pour garantir le bon fonctionnement du système d'information (SI), mais spécialisés en cybersécurité.

En résumé, les MSSP ont pour mission, moyennant abonnement, de fournir et installer des solutions de sécurité complètes, ou d'exploiter et superviser les outils des clients, en assurant à la fois un travail de surveillance et de réponse aux incidents. Et ce, en couvrant les réseaux, les terminaux, ainsi que les infrastructures basées sur le cloud, notamment. Le client peut souffler et se reposer sur les compétences techniques et humaines de son prestataire, sans devoir internaliser une expertise pointue et coûteuse. *« Les MSSP, au sens où je l'entends, regroupent des prestataires externes qui fournissent des services de surveillance, de détection, jusqu'à la réponse aux incidents. Le périmètre de ce que cela peut inclure est très large »*, développe Benoît Marion, senior manager chez Wavestone, un cabinet de conseil qui accompagne les entreprises dans leur transformation.

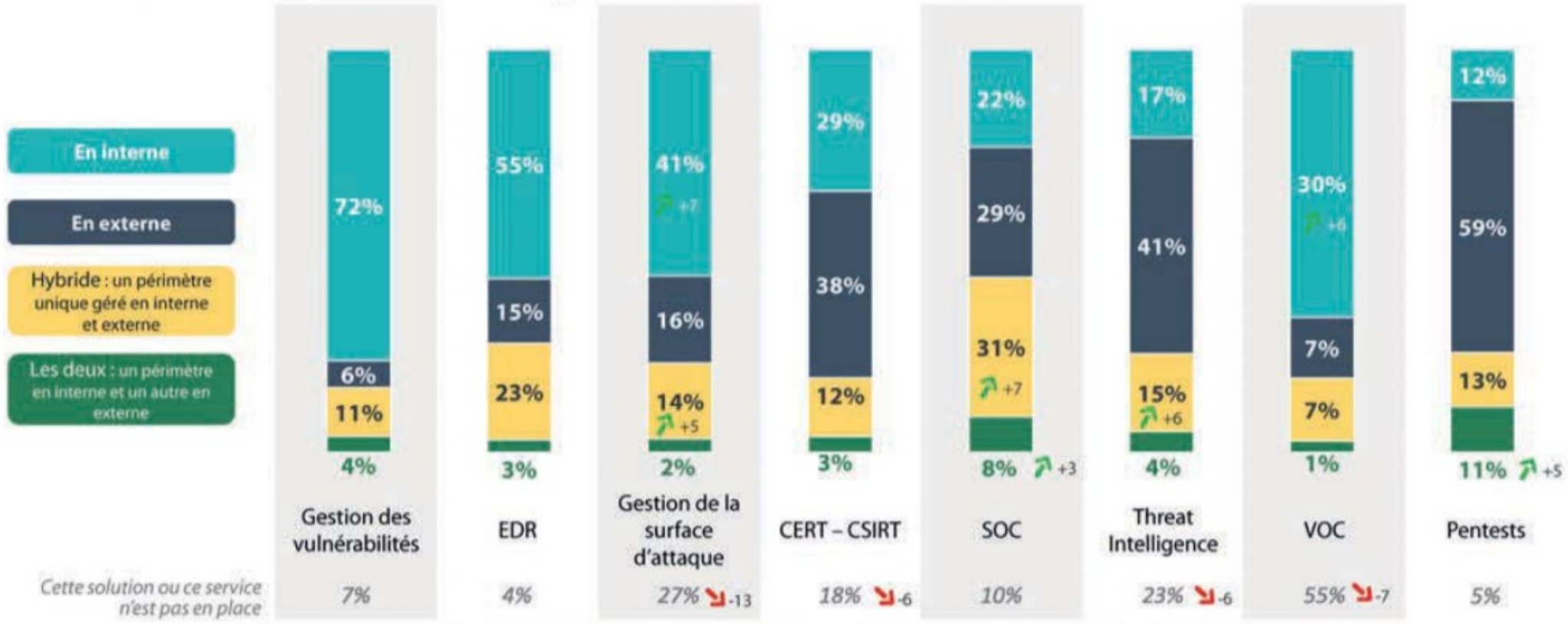
S'affranchir de la configuration et de la gestion

En 2024, de nombreux aspects de la cybersécurité d'une organisation étaient confiés à un tiers. Toutefois, selon le dernier baromètre de la cybersécurité des entreprises du CESIN (Club des experts de la sécurité de l'information et du numérique), le degré d'externalisation varie grandement en fonction des solutions de sécurité (cf. tableau). Concernant le SOC (le Security Operations Center) — qui désigne, dans ou en dehors d'une société, l'équipe en charge d'assurer la sécurité de l'information, et dont la mission est de détecter, analyser et remédier aux incidents

« Grâce à la mutualisation, le MSSP propose une supervision 24/7 abordable. Mettre en place ce service en interne est complexe pour une entreprise, en raison des contraintes budgétaires, des ressources humaines limitées et de la difficulté à recruter des experts prêts à assurer cette mission »

Benoît Marion, senior manager chez Wavestone

Q30b. Comment opérez-vous les solutions et services ci-dessous ?
Base : ensemble – résultats hors solution non mise en place



de cybersécurité — *« 29 % des répondants disent l'avoir entièrement externalisé, 31 % reposent sur un modèle hybride, 22 % l'ont internalisé et 8 % ont un périmètre en interne et un autre en externe »*, explique Alain Bouillé, fondateur, ancien président et actuel délégué général du CESIN. Pour des services exigeant une expertise plus spécifique et pointue, tel le pentest, l'externalisation est d'autant plus marquée avec 60 %, de même que la threat intelligence (41 %), ou encore les CERT et CSIRT — les équipes spécialisées dans la gestion des incidents de sécurité informatique — qui sont, quant à eux, externalisés pour 38 % des répondants. *« Le client va conserver un certain nombre de périmètres gérés en propre, souvent les opérations courantes, et pour d'autres périmètres, qui exigent une veille 24/7 ou une expertise plus pointue qu'ils n'ont pas forcément, par exemple, ils vont alors s'appuyer sur les MSSP »*, éclaircit Nicolas Fried, directeur de l'offre de confiance chez Orange Cyberdéfense.

Un modèle tourné vers l'hybridation

Alain Bouillé s'attarde sur le SOC qu'il qualifie de « sujet phare », car au cœur même de la stratégie des MSSP et à la croisée des solutions de cybersécurité. Il met à disposition des entreprises des équipes d'analystes et assure une surveillance 24/7. Dans leur forme la plus courante, ils s'appuient sur un SIEM (Security Information and Event Management) mutualisé, qui centralise, analyse et corrèle les logs et événements de sécurité issus du système informatique. Cet outil détecte les menaces en temps réel grâce à des règles d'alerte et des analyses comportementales. Les sources des logs incluent les équipements réseau, les applications de sécurité (EDR, IAM, XDR, antivirus) et les activités des utilisateurs. Pratique. Pourtant, ce que nous apprend le baromètre du CESIN, c'est que l'externalisation de ce SOC n'est jamais totale. Comme expliqué plus haut, de nombreuses entités continuent de gérer leurs solutions en interne ou adoptent une posture hybride *(cf. tableau ci-dessus)*. Les raisons qui poussent à opter pour ce modèle sont variées et, en la matière, il n'y a que des cas particuliers. Bien qu'une partie des expertises cyber soient externalisées par manque de compétences internes, certains choisissent sciemment de conserver certains périmètres dans leur giron. *« Le MSSP n'a pas forcément connaissance du contexte et peut ne pas être aussi efficace qu'une équipe interne à temps plein au sein de l'organisation »*, avance Benoît Marion. L'expert pointe également une possible différence de flexibilité et de réactivité entre un fournisseur de services externe, qui gère de multiples clients, et une équipe interne qui peut concentrer ses efforts sur un problème précis. L'action du MSSP étant contractualisée, *« il peut y avoir un peu de latence, car il va agir dans le respect des contrats, des métriques et des niveaux de service définis »*, poursuit-il. Nicolas Fried nuance toutefois car, au-delà de la supervision 24/7, *« nous avons des analystes qui vont gérer un certain nombre de clients dont ils connaissent l'environnement et le contexte »*. La latence existe, mais elle est souvent maîtrisée, et un bon contrat MSSP inclut des SLA (Service Level Agreements) qui garantissent des temps de réponse rapides.

Globalement, Benoît Marion dit observer une tendance à l'optimisation vers un mix interne/externe : *« Nous avons vu des clients retourner vers de l'internalisé […] ou vers le modèle hybride pour les périmètres les plus critiques et pointus. »*

Si une partie de l'externalisation concerne des compétences spécifiques, telles que le pentest ou la threat intelligence, et critiques, *« tout ce qui peut être standardisé et industrialisable, et exécuté sans connaissance pointue du contexte, continue d'être externalisé »*, fait-il remarquer. Cela concerne, par exemple, la surveillance de la sécurité de base, l'identification des alertes et la gestion des incidents de premier niveau dans un SOC (N1). Pour les niveaux N2 et N3, *« je veux des équipes en interne, 100 % concentrées sur le contexte »*, ajoute Benoît Marion.

Aussi, les nombreuses organisations faisant le choix de l'hybridation sont *« celles qui ont des informations sensibles et qui ne veulent pas les exposer »*, relève Alain Bouillé. *« Les OIV – Opérateurs d'importance vitale qui sont soumis à des exigences particulières en matière de sécurité – ont beaucoup adopté ce genre de configuration hybride. »* En effet, l'externalisation soulève des inquiétudes, car elle implique fréquemment de confier des données sensibles à un tiers. *« Par exemple, en externalisant votre SOC, vous transférez la responsabilité de la surveillance et de la gestion des activités de votre réseau »*, prévient Alain Bouillé. À ce titre, il existe des modèles hybrides de SOC internalisé, où l'ensemble des dispositifs (Siem, infrastructures, etc.) sont conservés en interne,

afin de garantir que les données ne quittent pas l'entreprise. *« Toutefois, la supervision est externalisée, faute de ressources suffisantes pour recruter des analystes spécialisés »*, précise Alain Bouillé.

Les MSSP à l'usage des petits

Ce modèle à la carte nécessite une certaine flexibilité budgétaire et un niveau de maturité qui reste l'apanage des grands comptes. Le budget, c'est là l'un des gros arguments en faveur des MSSP, surtout auprès des TPE et PME qui ne disposent pas des ressources nécessaires pour se doter d'une équipe interne, voire d'un DSI (directeur des systèmes d'information) ou d'un RSSI (responsable sécurité des systèmes d'information) et qui manquent de maturité. D'après une étude d'Opinion Way réalisée en 2024, 72 % des TPE-PME ont déclaré n'avoir aucun salarié dédié à la gestion informatique, 68 % allouent moins de 2 000 € chaque année à leur sécurité informatique et 62 % se pensent faiblement exposées.

Pour ces structures, externaliser la compétence cyber devient dès lors une option viable et plus accessible, pour accéder à une expertise disponible. Malgré sa récurrence, le coût dudit service est théoriquement réduit, comparé à une équipe de sécurité interne. *« Les MSSP mutualisent les infrastructures, ressources humaines, et les solutions qui sont partagées entre plusieurs clients, ce qui réduit les coûts individuels »*, développe Benoît Marion. À noter cependant que pour une toute petite structure, le coût peut rester un facteur bloquant, même s'il est mutualisé.

Et quid de la capacité d'une petite entreprise peu mature à évaluer la pertinence de l'offre des MSSP pour son activité ? Toujours selon Opinion Way, 34 % des TPE et PME disent ne pas savoir à qui s'adresser pour atteindre le bon niveau de cybersécurité. *« Cette étude dresse un état des lieux préoccupant du niveau de maturité cyber des TPE-PME, encore trop nombreuses à ne pas être prêtes à faire face à une cyberattaque, ni à ses conséquences. Pourtant, des solutions à la portée de toutes les entreprises existent »*, déclarait Jérôme Notin, directeur général de cybermalveillance.gouv.fr, dans un document présentant les résultats de l'étude.

Parmi ces solutions « à la portée », les fournisseurs de services de sécurité managés déploient des alternatives telles que des micro-SOC, conçus pour répondre aux besoins des PME, des ETI et des collectivités locales, tout en restant alignés sur leur budget. C'est notamment le cas d'acteurs comme OTO-Cyberdéfense ou Orange Cyberdéfense. Ces micro-SOC sont généralement associés à des outils, type EDR ou firewall par exemple, fournis sous le modèle as a service. Des fonctionnalités complémentaires peuvent être ajoutées, comme la protection des e-mails ou du cloud. Orange Cyberdéfense a ainsi développé plusieurs offres micro-SOC pour les postes de travail, axées sur les e-mails, le cloud, les mobiles, ainsi que Micro-SOC Shield, une solution traitant plus précisément la sécurité périmétrique.

Combler la pénurie de talents

Au-delà de la question des moyens, la carence en compétences complique également la tâche des entreprises et est encore un argument en faveur des MSSP. Selon un rapport publié en 2024 par le Boston Consulting Group, en collaboration avec le Global Cybersecurity Forum, il manquerait près de 2,8 millions de professionnels dans le secteur de la cybersécurité à l'échelle mondiale, soit 28 % de postes vacants. Toujours selon cette étude, 43% des RSSI estiment que leurs équipes ne disposent pas des compétences adéquates pour assurer efficacement la sécurité de leur organisation. Sur le papier, la mutualisation des ressources par les MSSP apporte une réponse au moins partielle à cette pénurie de talents. Partielle, car ces prestataires ne sont pas non plus épargnés par les difficultés de recrutement et de formation. En interne, la gestion des analystes est d'ailleurs un enjeu central pour limiter le turnover, souligne Alain Bouillé : *« Dans un SOC, l'activité peut être intense sur certains clients, générant du stress important. À l'inverse, d'autres peuvent avoir une activité plus calme, ce qui peut aussi entraîner un stress lié cette fois au manque de stimulation et de challenge »*. Pour faire face à ces défis, il recommande de maintenir un équilibre entre tâches routinières et missions plus complexes, tout en investissant dans une formation continue afin de garder les équipes à jour.

« L'externalisation suscite des préoccupations. Elle implique souvent de confier des éléments sensibles. Lorsqu'un SOC est externalisé, [...] les données sont envoyées vers un opérateur, ce qui rend crucial le choix d'un partenaire de confiance. C'est pourquoi des entreprises françaises, comme Orange et Advens, rencontrent du succès : leur offre bénéficie de la proximité géographique, les données sont stockées sur le territoire français ou européen »

Alain Bouillé, fondateur, ancien président et actuel délégué général du CESIN

« Nos équipes MicroSOC et nos partenaires français sont localisés en France, et les logs sont hébergés dans des data centers français. Nous travaillons également avec des partenaires américains, mais leurs services peuvent être hébergés sur des tenants en Europe, y compris en France. Par ailleurs, Orange CyberDefense a lancé un cloud souverain (Bleu) et offre la possibilité d'héberger les solutions de nos partenaires sur nos data centers, garantissant ainsi la souveraineté des données. »

Nicolas Fried, directeur de l'offre de confiance chez Orange Cyberdéfense

L'IA pour augmenter les SOC

Face à cette pénurie de talents, l'IA n'aurait-elle pas un rôle à jouer ? Capable de gérer de nombreux cas d'usage à la place des analystes, l'IA peut, selon Alain Bouillé, résoudre « *en grande partie* » les problèmes d'effectifs. À terme, « *le niveau 1, chargé de la surveillance et du tri initial des alertes de sécurité, va être supprimé au profit de l'intelligence artificielle* ». Cela signifie que les analystes N1 « *pourront être formés pour compenser les manques dans les N2 et les N3* », qui se concentrent sur l'analyse approfondie, l'investigation avancée et la réponse aux incidents. Une évolution qui entraînera un besoin de requalification et de formation.

Dans un SOC, l'IA pourra, grâce au machine learning et au deep learning, détecter les menaces de manière plus précise et proactive, analyser les incidents plus rapidement et, dans une certaine mesure, automatiser les réponses — par exemple en mettant en quarantaine une machine infectée, en isolant un réseau ou en supprimant certains fichiers malveillants. Autant d'actions qu'elle pourra exécuter à la place d'un analyste. Pour Pascal Le Digol, country manager France chez WatchGuard, fournisseurs de services MSSP à destination des ETI et PME : « *L'IA va ajouter de l'automatisation, et c'est précisément ce dont nous avons besoin, notamment dans les MDR pour réduire le bruit (détection et réponse managées), un service managé où un prestataire supervise un EDR et/ou un XDR (détection et réponse étendues).* » Dans cette optique, WatchGuard a acquis, début janvier, ActZero, un leader des services MDR exploitant l'IA afin de réduire les faux positifs.

Ciel dégagé pour les MSSP

Au-delà des entreprises qu'ils servent, les MSSP représente une opportunité stratégique pour les éditeurs. « *Il est plus facile d'assurer une rentabilité avec un revenu récurrent et une offre de service groupée, que dans un modèle basé uniquement sur la marge dégagée par la vente de produits* », explique Pascal Le Digol. Chez WatchGuard, une cinquantaine de partenaires ont déjà franchi le pas et proposent des services de sécurité managés. « *J'espère que cela va se traduire dans les chiffres et avoir un effet positif sur la réduction des attaques le plus rapidement possible* », ajoute-t-il.

Avant même de pouvoir évaluer l'efficacité réelle de ce modèle sur le temps long, les perspectives de croissance sont au beau fixe. Pour Alain Bouillé, le constat est sans appel : « *Lorsque j'interroge des MSSP, aucun ne se plaint de voir son chiffre d'affaires chuter. Tous sont en croissance, parfois à deux chiffres.* » Une tendance qui devrait s'accentuer avec l'arrivée de la directive NIS2 (qui doit renforcer la cybersécurité et la résilience des systèmes numériques dans des secteurs critiques), un levier supplémentaire pour renforcer leur position. « *Sur les 15 000 entités concernées en France, beaucoup d'entreprises ne font pas grand-chose en matière de cybersécurité et devront s'y mettre. Et une des solutions les plus accessibles pour beaucoup sera d'externaliser.* » De fait, selon Business Research Insights, le marché mondial des MSSP devrait doubler d'ici à 2032, atteignant 140,08 milliards de dollars contre environ 70 milliards actuellement.

V.M

L'IA générative franchit les portes des SOC

Hamza Sayah est cofondateur et CTO de Qevlar AI, une startup dont l'IA générative a été intégrée aux centres d'opération de Nomios, un intégrateur réseau et sécurité informatique. Il explique : « *aujourd'hui, une grande partie des alertes nécessitent une intervention humaine. Alors que les cybercriminels utilisent des techniques de plus en plus complexes, ce qui entraîne une augmentation du nombre d'alertes. Cependant, il n'est pas possible de recruter une quantité infinie d'analystes* ». Pour y remédier, Qevlar AI développe des agents autonomes capables de traiter les alertes, d'accéder aux systèmes et outils des clients, ainsi qu'à Internet et à des bases de données de threat intelligence. « *Ces agents effectuent des investigations et génèrent des rapports structurés contenant un verdict sur les alertes, les entités identifiées et des recommandations de remédiation. Cela permet aux analystes de gagner entre 30 minutes et plusieurs heures de travail d'investigation* », avance Hamza Sayah. Des rapports générés en moins de cinq minutes.

Check Point fait le pari de la simplification par une plateforme

La conférence européenne du fournisseur de solutions de cybersécurité s'est tenue à Vienne, en Autriche. L'éditeur se rallie pleinement à une stratégie de plateforme, acceptant de ne pas faire tout parfaitement, et s'ouvre sur un écosystème. La principale annonce produit de la conférence tient en l'ajout de nouvelles fonctionnalités sur la plateforme Unity de l'éditeur.

La plateforme vise des objectifs ambitieux : accélérer l'adoption d'une stratégie Zero Trust, renforcer la prévention des menaces, réduire la complexité et simplifier les opérations des équipes de sécurité. CheckPoint part d'un constat assez évident : le monde d'aujourd'hui est hyper connecté, mais les équipes continuent de lutter avec des outils en silos et un environnement complexes pour contrer les menaces et les attaques. Nataly Kremer, chief product officer et patronne de la recherche chez Checkpoint, indique : *« Il se peut que les entreprises prennent plusieurs plateformes, la meilleure pour chaque besoin : une pour le réseau, une pour le SOC (Security Operation Center). On ne peut pas tout mettre sur une plateforme qui ferait tout pour tout le monde. Pour certains clients, cela peut être possible, mais cela sera toujours mieux que l'empilement de 50 solutions comme aujourd'hui ».*

Pour faire face à ce problème, Check Point introduit différentes fonctionnalités qui s'appuient sur des éléments d'intelligence artificielle visant à réduire la complexité et à renforcer les possibilités de gestion de la sécurité sur la plateforme Unity. Elle propose, de plus, des intégrations renforcées avec des produits tiers pour mieux gérer la prévention des menaces.

Nadav Zafrir, le nouveau CEO de Checkpoint, lors de la session générale d'ouverture de CPX

Unifier et simplifier les identités et les politiques

En se reposant sur l'intelligence artificielle et la connaissance des identités, les administrateurs ont la possibilité de mettre en place des politiques de sécurité plus fines et plus efficaces. En unifiant la visibilité et l'analyse des politiques de sécurité sur l'ensemble des environnements, les équipes de sécurité sont plus à même de maintenir une bonne hygiène de sécurité et de rester dans les lignes des conformités. Quantum Policy Insights apporte ainsi l'analyse des politiques existantes et recommande des changements pour améliorer la posture de sécurité. Le logiciel renforce, de plus, les stratégies de sécurité Zero Trust, en interdisant les accès trop permissifs ou les conflits de politiques de sécurité. Quantum Policy Auditor s'assure de l'alignement avec les préconisations ou les politiques de l'entreprise, tout en analysant rapidement l'ensemble

des règles mises en place pour fournir des rapports graphiques, afin d'identifier les politiques qui violent les exigences de l'entreprise. Le service en Cloud Infinity Identity centralise et unifie les identités. Il s'intègre simplement avec les produits tiers présents et supporte de nouvelles sources de données : Microsoft Defender, Microsoft Intune et Harmony Endpoint. Déjà présents, les Playblocks d'Unity prennent en charge l'automatisation et l'orchestration entre la plate-forme et les outils tiers de sécurité. Plus d'une centaine de ces briques de base sont disponibles, qui peuvent être créées ou personnalisées par de l'intelligence artificielle générative.

Simplifier les opérations des équipes

Infinity AIops, un agent d'intelligence artificielle, supervise les passerelles afin d'anticiper de possibles problèmes, tout en fournissant un état en temps réel de l'infrastructure sur de nombreux paramètres. AI Copilot, un assistant conversationnel, rassemble le contexte pour proposer des réponses aux administrateurs afin de simplifier les opérations et écourter le temps de remédiation en cas d'incident. Le logiciel devient ainsi le point d'entrée de collaboration sur la plateforme Unity.

L'IA au cœur du réacteur

L'intelligence artificielle s'immisce partout dans la plateforme. Tous les éléments de la plateforme communiquent avec une identité propre. Les informations sont rassemblées dans le Cloud. Leur analyse apporte aux équipes de sécurité le contexte pour prendre la meilleure décision possible. Nataly Kremer constate : *« L'IA est un outil pour faire plus vite, automatiquement, sur une grande échelle, avec la possibilité d'être personnalisé pour l'utilisateur »*. Interrogée sur le moment où cette IA sera totalement autonome, elle répond : *« Cela dépendra des avancements de la technologie, cela peut prendre quelques jours, des semaines, des mois, des années. Évidemment, cela rendrait la prise de décision beaucoup plus rapide, mais cela demande aussi que nous pouvons avoir réellement confiance dans la prise de décision »*. Si la question est donc posée, on voit encore une certaine gêne a annoncé l'autonomie complète des solutions d'IA, même si cela devrait arriver dans le temps. D'autant que certaines fonctions dans les solutions de Checkpoint le font déjà, comme dans le WAF (Web Application Firewall).

« L'IA est un outil pour faire plus vite automatiquement sur une grande échelle avec la possibilité d'être personnalisé pour l'utilisateur. »

Nataly Kremer,
en charge des produits et de la recherche chez Checkpoint.

Un virage stratégique

En faisant le choix de la plateforme, Checkpoint est donc bien conscient qu'elle ne fera pas tout parfaitement. L'éditeur fait le pari que les clients vont réaliser une consolidation des outils de cybersécurité afin de rendre les opérations des équipes de sécurité moins coûteuses et plus simples. La plateforme lui ouvre aussi de nouvelles opportunités d'extension commerciale, via des fournisseurs de services comme les MSSP. Cette tendance se généralise d'ailleurs chez les acteurs de la cybersécurité, qui deviennent ainsi des fournisseurs de services comme la plupart des principaux concurrents de Checkpoint, mais aussi des acteurs comme Sophos. Pour Checkpoint, cela est plus récent avec la mise en place d'un programme spécifique.
Dans celui-ci, les MSSP bénéficient de la solution Horizon MDR/MPR 24/7/365 de Checkpoint, avec des versions co-brandées et en marque blanche. Cela peut compléter des services similaires que le MSSP offre, ou étendre complètement son ensemble de solutions actuelles. Ils peuvent également exploiter et fournir des versions co-marquées des services de réponse aux incidents (IR) de Checkpoint. Il propose aussi aide, formation, accès à des experts pour les MSSP, ainsi que l'accès à des services axés sur la prévention avec des capacités complètes de gestion des XDR/XPR, MDR/MPR et des événements multiples de sécurité. Ce pas vers les services est appelé à devenir le relai de croissance de l'entreprise, alors qu'elle est attaquée sur son business historique, la fourniture d'appliance de firewall par ses principaux concurrents dont les historiques comme Cisco, Palo Alto ou Fortinet. Checkpoint se place de plus sur le marché porteur du Firewall as a Service qui devrait croitre de plus de 22 % jusqu'en 2030 en moyenne annuelle pondérée, selon une étude Grand View Research. **B.G**

Reconnu dans **l'étude Miercom**

Dans la troisième vague de l'étude de Miercom sur l'efficacité des plateformes, Checkpoint affiche des performances remarquables. La plateforme arbore ainsi un taux de blocage de 99,9 % des Zero Day+1 et un taux de prévention des phishings de 99,7 %. Ces taux représentent les meilleurs sur les cinq solutions testées par le cabinet d'étude. Le benchmark se déroule sur trois mois et est sous le feu roulant de 500 fichiers malicieux en provenance de Virus Total, avec un échantillonnage d'en-tête d'extension de fichiers comme Office docx, Office xlsx, pdf, exe, PowerShell, Bash script, APK, dll et fichiers archivés. L'institut compare chaque solution de firewall sur de multiples fonctions et technologies dont les modules Anti-virus, IPS, Anti-bot, URLF, bac à sable, et tous les moteurs de sécurisation et les moteurs de sécurité d'intelligence artificielle et d'apprentissage machine. Les tests sont joués en parallèle sur chaque solution pour voir ceux bloquant le plus d'attaques modernes.

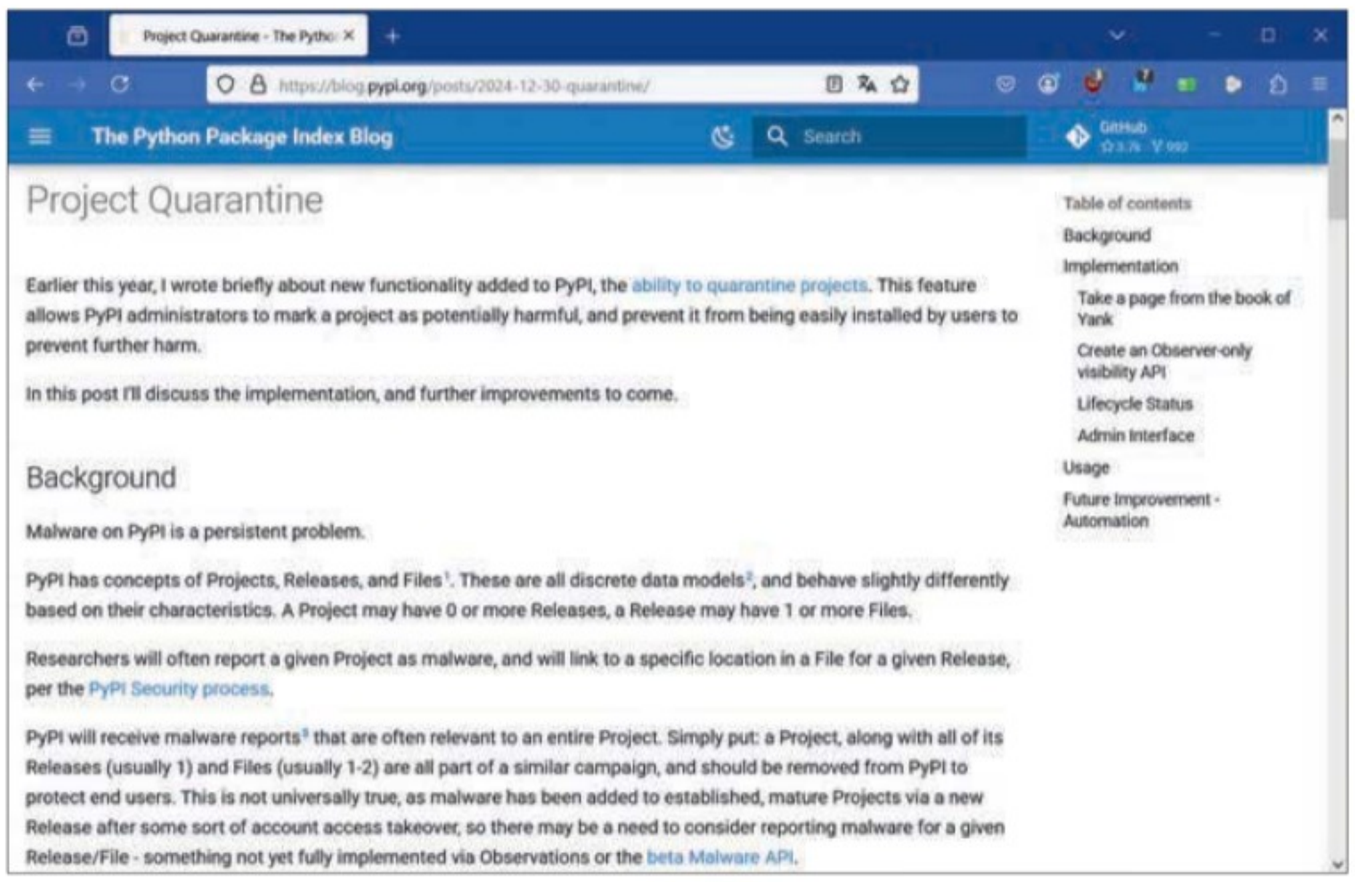
Détection de malwares dans les logiciels Python par PyPI

Une nouvelle fonctionnalité importante a été récemment ajoutée à PyPI, la capacité de mettre en quarantaine des projets. Elle permet aux administrateurs PyPI de marquer un projet comme potentiellement nocif, et empêcher qu'il soit aisément installé par des utilisateurs afin d'éviter plus de dommages. Nous allons voir, dans cet article, les détails de ce projet nommé Quarantine.

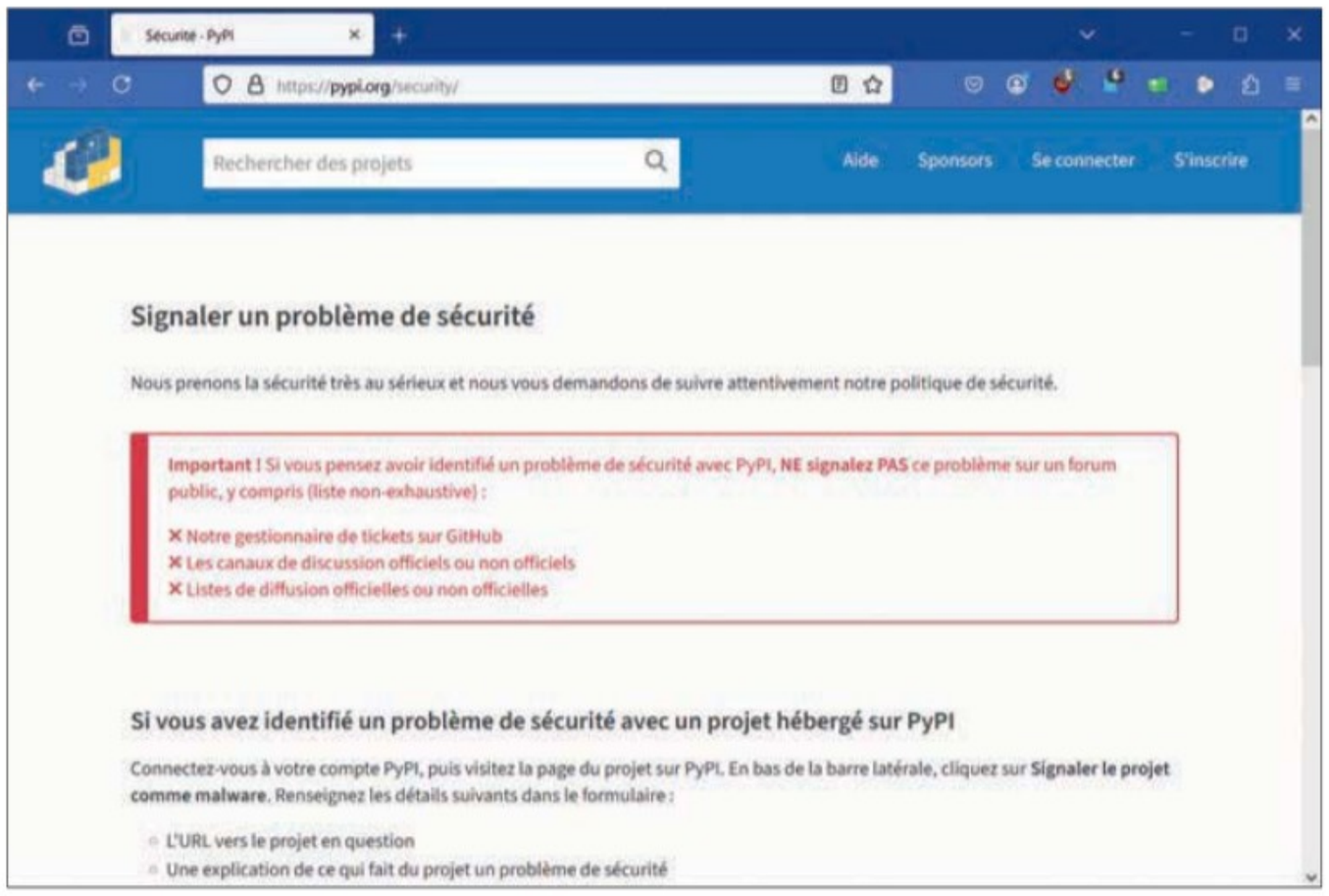
PyPI (pour Python Package Index) est le référentiel officiel des packages logiciels pour le langage de programmation Python. Il s'agit d'une plateforme centralisée sur laquelle les développeurs Python peuvent trouver, installer et partager des packages Python open-source. PyPI est géré par la PSF (Python Software Foundation) et est accessible via l'installateur de packages pip. Celui-ci est inclus directement dans les dernières installations de Python et téléchargeable individuellement pour les anciennes versions. Les utilisateurs peuvent rechercher des packages par leur nom ou par mot-clé, les télécharger et les installer avec une simple instruction pip. PyPI héberge des milliers de packages Python open-source, allant des bibliothèques dédiées au calcul scientifique (NumPy) et à l'analyse de données (Pandas) jusqu'aux frameworks pour le développement web (comme Django ou Flask) et l'apprentissage automatique (Scikit-Learn) en passant par le traitement vidéo et bien d'autres thèmes (tous en fait). PyPI représente une ressource essentielle pour les développeurs de l'écosystème Python, mais il peut aussi être utilisé par de vilains hackers pour propager des virus et prendre le contrôle de machines.

Arrière-plan

Les malwares dans PyPI représentent un problème persistant. PyPI fonctionne avec des concepts de projets, releases et fichiers. Ce sont tous des modèles de données discrets, et ils se comportent légèrement différemment selon leurs caractéristiques propres. Un projet peut très bien avoir 0 ou plusieurs releases, et une release peut être constituée de 1 ou plusieurs fichiers. Les chercheurs vont souvent identifier tel ou tel projet en tant que malware, et vont le relier à un emplacement spécifique dans un fichier pour une release donnée, selon le protocole de sécurité de PyPI. PyPI va recevoir les signalements de malware qui sont le plus souvent propres à un projet dans sa globalité. Il faut simplement effectuer un put : d'un projet, avec toutes ses releases et fichiers. En général, ils font tous partie d'une campagne similaire et devraient être supprimés de PyPI, afin de protéger les utilisateurs finaux. Ce n'est pas une vérité universelle, des malwares pouvant être ajoutés à des projets établis et matures jusqu'ici sains via une nouvelle release après une prise de contrôle de l'accès au compte. Il peut donc s'avérer nécessaire de signaler un malware seulement pour une release et/ou un fichier donné. Lors de l'examen et de la mise en œuvre des signalements de malware, les administrateurs PyPI ont un outil principal à leur disposition leur permettant de supprimer complètement le projet de la base de données. Ceci est souvent associé à l'interdiction de réutiliser le nom du projet. Au passage, PyPI possède une fonctionnalité indépendante des logiciels malveillants pour empêcher la réutilisation de nom de fichiers. L'impact de ces suppressions peut être perturbant, et ces interdictions sont quasiment irrévocables. C'est le même mécanisme que lorsque PyPI avertit les propriétaires de projet à propos du moment où ils décident



Vous trouverez tous les détails sur le projet Quarantine à l'adresse https://blog.pypi.org/posts/2024-12-30-quarantine/



Si vous avez identifié un problème de sécurité avec un projet hébergé sur PyPI, signalez-le à l'adresse suivante : https://pypi.org/security/

de supprimer leur projet de l'index. Il ne faut donc pas le faire à la légère. Qui plus est, plus un projet malicieux reste disponible publiquement, plus les utilisateurs auront de chance d'installer le dit malware et d'agrandir la liste de ses victimes. Avec le manque criant en matière de personnel de sécurité à temps complet actuel de PyPI == 1, il y a une forte probabilité pour que les malwares restent installables par des utilisateurs pendant de longues périodes. Demander à des administrateurs PyPI bénévoles de faire des heures supplémentaires n'est pas non plus une solution viable. Réduire la fenêtre de temps pendant laquelle un projet, une release et/ou un fichier malicieux seraient disponibles pour les utilisateurs finaux, qui deviendraient alors de nouvelles victimes, serait une amélioration considérable, et réduirait de plus l'incitation pour les acteurs malveillants à utiliser PyPI comme leur méthode de distribution préférée.

Implémentation

L'implémentation du projet Quarantine se fait, comme pour beaucoup de projets, en plusieurs étapes. Voici quelques exigences de base nécessaires pour mettre en place cette fonctionnalité :

- Le projet doit exister sur PyPi et avoir des releases et des fichiers (au moins un de chaque). Les projets n'existant qu'en version béta sont donc exclus.
- Le projet n'est pas installable lorsqu'il est en quarantaine (il ne doit pas être accessible simplement depuis l'index)
- Le projet ne peut pas être modifiable par le propriétaire du projet tant qu'il est en quarantaine
- Le statut du projet est visible pour les propriétaires de projets, les chercheurs en sécurité et les administrateurs
- L'état du projet peut être modifié par un administrateur PyPI afin de restaurer sa visibilité globale
- Le projet peut être supprimé par un administrateur PyPI

Avec ces éléments en tête, vous pouvez entreprendre la mise en œuvre de cette fonctionnalité.

Créer une API de visibilité Observer-only

De nouvelles infrastructures d'API béta ont été précédemment créées afin de permettre aux Observers de signaler des projets malicieux. Une idée était d'ajouter un nouveau point d'arrêt d'API authentifiée afin d'autoriser d'effectuer des requêtes sur la liste courante des projets mis en quarantaine, et de fournir des liens vers leurs releases et fichiers afin de les consommer. Ainsi, un chercheur pourrait télécharger les artefacts en question mais pas via l'installateur pip. Il n'est pas prudent de poursuivre cette approche, tant que les API beta authentifiées sont toujours en cours de développement. Il vaut mieux ne pas ajouter de nouvelles fonctionnalités avant de revenir en arrière et de s'apercevoir que des problèmes d'authentification et d'autorisation critiques doivent être résolus pour la gestion future des points de terminaison d'API.

Un nombre d'attaques toujours croissant

Le nombre de packages logiciels open source malicieux trouvés dans des registres populaires est croissant. La meilleure manière de comptabiliser ces attaques consiste à les détecter et à les corriger à la source. PyPI en a fait l'expérimentation avec une fonctionnalité de détection de malwares qui analyse les nouveaux packages et les nouvelles versions de package, recherchant des packages potentiellement malicieux. Malheureusement, ce travail de recherche de logiciels open source malicieux dans le contexte d'un registre communautaire est difficile. Les gestionnaires de registre et les contributeurs ont un temps limité (souvent sur la base du volontariat) pour établir un verdict sur la sécurité d'une revue, un problème rendu plus ardu par des taux élevés de faux positifs et le grand nombre de packages dans de nombreux registres. ▮

T.T

Le projet Yank

Avant cette nouvelle fonctionnalité de mise en quarantaine, une autre du nom de Yank avait été mise à disposition dans la PEP 592. Un projet sans release est listé dans l'API de référentiel simple, mais la page de détails résultante ne proposera aucun lien, le rendant de fait impossible à installer. L'idée était que lorsqu'un projet était en quarantaine, il pouvait être marqué comme n'ayant pas de releases, et il était de fait exclu de l'index. La différence entre Quarantine et Yank est qu'une release « yanked » est toujours installable par des clients, alors que les items en quarantaine ne devraient pas l'être. Il faut donc chercher où effectuer la modification et se demander de quelle manière cela va impacter les clients. Qui plus est, Yank est applicable à une release (et à tous les fichiers qui la composent), mais pas à un projet dans sa globalité.

www.linformaticien.com

ABONNEZ-VOUS À L'INFORMATICIEN

linformaticien.com/abonnement

MAGAZINE

Recevez chaque mois (10 numéros par an) le magazine «papier» et accédez également aux versions numériques.

1 AN FRANCE : 72 €
2 ANS FRANCE : 135 €
1 AN UE : 90 €
2 ANS UE : 171 €
1 AN HORS UE : 108 €
2 ANS HORS UE : 207 €

NUMÉRIQUE

Accédez chaque mois (10 numéros par an) à la version numérique du magazine et retrouvez également via votre compte en ligne les versions numériques des dernières publications.

1 AN : 49 €
2 ANS : 89 €

ÉTUDIANT / ÉCOLE

Abonnez vos étudiants avec une formule dédiée à 60 % du prix normal de l'abonnement sous forme de PDF (10 numéros par an).
Possibilité abonnements groupés en contactant le service abonnements du magazine à abonnements@linformaticien.com.

ABONNEMENT 1 AN : 43, 20 €

2025 : une meilleure sensibilisation et des défis majeurs

Par Paul-Olivier Gibert, président de l'AFCDP

Voici la 14è édition de l'Observatoire trimestriel de l'AFCDP, via lequel l'association souhaite estimer l'évolution de la conformité des organisations, et évaluer la perception des DPO sur des sujets techniques et d'actualité.

Avez-vous confiance dans la protection des données privées au sein de vos organisations ?

Même si 42 % des organisations se sentent confiantes dans leur stratégie de protection des données (stable : 41 % fin décembre), plus de la moitié (56 %) expriment des doutes ou des difficultés.

23 % des répondants ont effectivement répondu PEU (vs 19 % fin 2024), expliquant que le contexte réglementaire changeant crée de l'instabilité dans leur stratégie. Cela souligne une difficulté d'adaptation face aux évolutions législatives et aux nouvelles normes de protection des données.

Ce résultat met en évidence un enjeu stratégique pour les entreprises et administrations en matière de protection des données privées, notamment dans un contexte de réglementations strictes en Europe, comme le RGPD, et celles à venir (IA Act, NIS2, DORA…). Globalement, l'évolution des résultats depuis le début de notre Baromètre, traduit une dynamique positive en matière de confiance (notamment depuis la 8e édition en mai 2023), même si des défis subsistent. La montée en maturité réglementaire et la mise en place d'outils et de formations spécifiques semblent porter leurs fruits, mais les organisations doivent encore faire face à un environnement en constante évolution.

Selon vous, que réserve 2025 aux DPO en termes d'enjeux ?

43 % des répondants estiment que 2025 sera une année difficile pour les DPO, traduisant une anticipation de défis accrus, probablement liés aux nouvelles régulations en cours d'adoption, ou aux exigences croissantes en matière de conformité et de cybersécurité.

Par ailleurs, 34 % considèrent que l'année sera « particulière », suggérant une période de transition marquée par des évolutions réglementaires spécifiques ou des changements structurels impactant directement leur rôle. Seuls 18 % des répondants estiment que 2025 sera une année « classique », ce qui montre que la normalisation des pratiques et la stabilité restent minoritaires dans les projections des DPO.

Enfin, 5 % des participants indiquent ne pas savoir à quoi s'attendre, ce qui pourrait refléter une certaine incertitude quant à l'évolution du cadre réglementaire et des défis émergents.

Les réponses témoignent d'une perception majoritairement prudente, voire inquiète, de l'année à venir de la part des DPO. Ces résultats soulignent ainsi une forte attente vis-à-vis des évolutions à venir, et confirment que le rôle des DPO restera central en 2025, nécessitant anticipation, adaptation et montée en compétences face à un environnement toujours plus exigeant.

Quel est votre sentiment sur les demandes d'exercice des droits (accès, rectification, effacement, etc.) ?

L'évolution des demandes d'exercice de droits (accès, rectification, effacement, etc.) semble suivre une tendance marquée par une hausse notable. En effet, 48 % des répondants constatent une augmentation de ces demandes, traduisant une prise de conscience grandissante des individus de leurs droits en matière de protection des données. Cette dynamique peut être renforcée par une médiatisation croissante des questions de confidentialité et par le renforcement des régulations, incitant les citoyens à exercer plus activement leurs droits. 38 % des répondants estiment plutôt que ces demandes stagnent, ce qui suggère une certaine stabilisation après la forte hausse observée dans les années suivant la mise en application du RGPD. À l'inverse, seuls 6 % indiquent une diminution de ces sollicitations, un chiffre relativement marginal qui démontre que les préoccupations autour de la protection des données restent centrales.

Ces résultats nous confirment que la gestion des demandes d'exercice de droits demeure un enjeu clé pour les organisations, nécessitant des processus efficaces et une vigilance accrue, afin de répondre aux attentes des citoyens et aux exigences réglementaires.

Journée de la **protection des données** : les enjeux pour 2025

Depuis 2007, le 28 janvier marque la Journée mondiale de la protection des données. Initiée par le Conseil de l'Europe, cette journée sensibilise citoyens et organisations à l'importance de la confidentialité des données personnelles. Face à la montée des cybermenaces, la généralisation du cloud hybride et l'explosion de l'IA, cette journée revêt une importance toute particulière en 2025.

Dans un contexte où les cybermenaces se multiplient, et où la transformation numérique accélère l'essor du cloud hybride, la protection des données représente un enjeu stratégique majeur. En révolutionnant les usages, l'IA pose aussi de nouveaux défis en matière de sécurité et de confidentialité.

Des données sous haute pression en 2025

L'essor de l'intelligence artificielle, et en particulier celui de l'IA agentique, bouleverse les approches traditionnelles de cybersécurité et de protection des données. *« Les responsables IT se sont concentrés sur la nécessité de relever les défis en termes de protection des données, à mesure que l'IA transforme les activités des entreprises. Les outils automatisés, y compris l'IA générative, leurs ont permis de fonctionner plus efficacement, mais les ont également exposées à de nouveaux risques liés à la confidentialité des données sur lesquelles ces outils construisent leurs raisonnements »*, explique Neil Thacker, global privacy & data protection officer chez Netskope. L'IA agentique, capable de prendre des décisions avec une intervention humaine minimale, impose une sécurisation rigoureuse des systèmes, des moteurs de raisonnement et des résultats générés.

Une approche proactive

La journée offre aux responsables IT l'opportunité d'échanger sur les stratégies de protection des informations sensibles. Pour Mandy Andress, la protection de la confidentialité des données exige une stratégie de sécurité proactive et exhaustive : *« Il est essentiel de comprendre où les données se trouvent et comment elles sont stockées — sur les différentes plateformes cloud — pour en garder le contrôle et s'assurer qu'elles restent à l'intérieur des limites définies. Des techniques, telles que la micro-segmentation ou la conteneurisation virtuelle, permettent non seulement d'isoler les charges de travail, mais aussi d'imposer des contrôles stricts sur le trafic réseau pour réduire l'exposition potentielle aux menaces. L'adoption d'une politique de* « deny all » *pour les communications inter-système garantit que seul le trafic essentiel est autorisé »*. Au-delà des mesures techniques, la cyber hygiène reste cruciale : utilisation des fonctions de sécurité intégrées, application rigoureuse des correctifs et suppression des systèmes obsolètes.

Jean-Christophe Vitu, VP Solutions Engineer chez CyberArk

Mandy Andress, CISO d'Elastic

La sécurité des identités

En 2024, la France a franchi une étape importante avec l'adoption de la loi SREN (Sécuriser et réguler l'espace numérique), renforçant la protection et la régulation du numérique. Parallèlement, la CNIL a actualisé son *« Guide de la sécurité des données personnelles »*, visant à rappeler les bonnes pratiques pour garantir la protection des informations. Toutefois, selon Jean-Christophe Vitu, VP Solutions Engineer chez CyberArk, *« le travail est loin d'être terminé »*. Il rappelle que le thème de l'édition 2025, *« Prenez le contrôle de vos données »*, met l'accent sur la responsabilité individuelle et collective en matière de sécurité numérique. Selon l'expert, l'un des piliers fondamentaux de la protection des données repose sur la gestion des identités : *« la mise en place de solutions robustes pour la gestion des identités et la protection des identifiants des utilisateurs est essentielle pour réduire les risques et prévenir les violations »*. La gestion des identités et la protection des identifiants sont désormais des priorités pour garantir la confiance numérique, dans un monde ultra connecté en constante évolution.

Un défi collectif

À l'heure où les cybermenaces se diversifient et où l'IA redéfinit les paradigmes de la sécurité, la protection des données ne peut plus être perçue comme une simple contrainte réglementaire, mais comme un impératif stratégique. La Journée de la protection des données 2025 rappelle que la vigilance, l'innovation et la responsabilité collective seront les clés d'un environnement numérique plus sûr et résilient. **J.C**

« *Je voulais arrêter les criminels avant qu'ils n'agissent* »

Eva Chen, cofondatrice et directrice générale de Trend Micro

En parallèle du Sommet pour l'action sur l'intelligence artificielle, organisé à Paris les 10 et 11 février 2024, l'InfoCR a pu rencontrer Eva Chen, cofondatrice et directrice générale de Trend Micro. Entre deux références à la pop culture, elle nous a livré son regard sur le rôle de l'intelligence artificielle dans le passage d'une cybersécurité réactive à proactive. Rencontre.

Rendez-vous est pris dans un hôtel d'une rue calme du 8e arrondissement, à deux pas du Grand Palais, où forces de l'ordre, acteurs économiques et représentants étatiques s'activent pour ce deuxième jour du sommet. Autour d'un café, Eva Chen se dit « honorée » d'avoir été invitée à l'événement, *« car voir tous ces pays influents réfléchir aux implications de l'IA, à leurs préoccupations et à leurs intentions d'utilisation, c'est essentiel »*, juge-t-elle.

Un scénario à la Minority Report

Trente-huit ans après la création de Trend Micro, le monde de la cybersécurité a bien changé, et l'IA n'y est pas étrangère, constate celle qui, il y a deux décennies déjà, se voyait *« policière du futur, arrêtant les cybercriminels avant qu'ils n'agissent »*, plaisante-t-elle — un clin d'œil au film de science-fiction Minority Report, où des mutants peuvent prédire les crimes avant qu'ils ne surviennent.

Pour réaliser cette vision, Eva Chen tente alors d'exploiter la puissance des Field Programmable Gate Arrays (FPGA), des circuits intégrés reprogrammables, pouvant être configurés pour effectuer une variété de calculs, y compris des applications d'IA. Elle fait même appel à un ingénieur de la Nasa pour l'épauler dans sa tâche. *« J'ai échoué dans mon projet, car il y a vingt ans, nous ne disposions ni d'assez de puissance de calcul, ni de modèles capables d'analyser suffisamment de données »*, reconnaît-elle.

Autrefois, la cybersécurité était réactive : il fallait détecter une attaque et y répondre. Aujourd'hui, elle est plus précise et rapide. L'enjeu est désormais d'anticiper et de minimiser les risques pour empêcher l'attaque de se produire. Avec l'IA et la GenAI, la capacité d'inférence permet d'agréger et d'analyser toujours plus de données.

« L'IA et l'IA générative permettent de mieux comprendre l'architecture propre à chaque entreprise, son organisation et ses protocoles, de modéliser les menaces, d'analyser les modes opératoires des attaquants, et de prédire les chemins d'attaque et scénarios spécifiques à chaque organisation », développe Eva Chen, tout en griffonnant des schémas pour appuyer son propos. Et d'ajouter : *« aujourd'hui, les cyberattaques sont très ciblées. Les attaquants utilisent eux-mêmes l'IA et l'analyse de données avancée »*, et disposent potentiellement de chemins d'attaques prédéfinis pour chaque organisation.

Cybertron veille au grain

Dans ces conditions, l'utilisation de l'IA en cybersécurité est-elle encore seulement une option ? Il semblerait que non. Pas une semaine ne passe sans qu'un éditeur n'annonce de nouvelles capacités d'IA dans l'une de ses solutions.

La plateforme de cybersécurité Vision One de Trend Micro ne fait pas exception et intègre, par exemple, un modèle spécialisé en cybersécurité fonctionnant en arrière-plan. Nom de code : Cybertron, en référence à la planète fictive des Transformers.

Basé sur LLaMA 3 de Meta, il est entraîné sur des données de threat intelligence collectées par Trend Micro, enrichies par les environnements de ses clients. Une fois ces sources corrélées, la plateforme peut identifier les *« joyaux de la couronne »* – autrement dit, les actifs les plus critiques de l'entreprise —, repérer les chemins d'attaques les plus probables et générer des recommandations de remédiation.

Bref, Trend Micro, comme ses concurrents, négocie le virage de l'IA. Et dans cette dynamique, l'entreprise susciterait même quelques convoitises. En août dernier, Reuters révélait que la firme envisageait une vente. Interrogée à ce sujet, Eva Chen tempère : *« Nous recevons toujours ce type de propositions (de rachat, ndlr). Il est aussi de ma responsabilité de garder l'esprit ouvert pour les examiner. Trend Micro est ma fille. Un jour, j'espère qu'elle se mariera. Mais je veux m'assurer qu'elle se marie avec la bonne personne. Je veux ce qu'il y a de mieux pour elle. Je suis une maman tigre »*, conclut-elle en riant. Une semaine après cet entretien, selon Reuters, Bain Capital, Advent et EQT auraient fait part de leur intérêt pour racheter Trend Micro. **V.M**

L'évolution des cybermenaces impose un changement de bouclier

Face aux ransomwares, aux deepfakes ou au cyberespionnage, la stratégie des RSSI passe par une meilleure détection des menaces et par l'encadrement des usages les plus récents.

« *Le vol et la revente d'identifiants de connexion forment le grand sujet du moment, de nombreuses attaques poursuivent cet objectif depuis la fin 2024* », expose Denis Blandin, RSSI d'un établissement public francilien à caractère industriel et commercial. D'où ses efforts de résilience centrés sur la détection des menaces, en complément des protections et défenses en profondeur du SI. « *La recherche de résilience nous mobilise autour d'exercices de crises et de procédures efficaces à enclencher rapidement après une attaque* », précise-t-il.

Renforcer l'annuaire d'entreprise

Après une cyberattaque, la convalescence peut s'avérer longue. Lorsqu'un ransomware a frappé le centre hospitalier de Dax début 2021, le déploiement d'un cryptolocker chiffrant plusieurs milliers de fichiers a pris quelques heures, mais il a fallu plus d'un an pour reconstituer le système complet, pour un coût total évalué à 2,3 millions d'euros. « *La cible numéro un des attaquants reste la prise de contrôle de l'Active Directory, vecteur d'attaque du malware pouvant rendre le système indisponible et compromettre ses données* », confirme Nicolas Barbat, architecte cybersécurité chez SPIE ICS, une ESN retenue par la centrale d'achats Resah pour rehausser le niveau de sécurité des établissements de santé. L'authentification multi-facteurs (2FA/MFA) progresse dans de nombreux secteurs. « *Sa mise en place exige de bien connaître les possibilités offertes pour les attribuer à chaque public (utilisateur interne, partenaire, administrateur) et optimiser leur adoption* », observe Clément Oudot, identity solutions manager, chez Worteks, l'ESN lyonnaise qui a mis en place les solutions d'authentification et d'IAM des pompiers de l'Essone, de PME et d'universités.

Face à l'externalisation croissante d'infrastructures, Giuliano Ippoliti, directeur de la cybersécurité de Cloud Temple recommande le cloisonnement des identités, via une séparation des annuaires : « *La certification SecNumCloud exige un annuaire distinct pour les administrateurs d'infrastructures. Notre projet pour l'infogérance va plus loin dans la segmentation, la qualification PAMS de l'ANSSI exigeant un annuaire dédié pour chaque donneur d'ordres infogéré.* » Il confirme le recours croissant aux outils SaaS de sécurisation, notamment avec les approches SASE (Secure Access Service Edge) et Zero Trust.

Contrôler les sauvegardes

Pour gérer la prochaine crise, on gagne à anticiper la reprise d'activités et à vérifier ses backups. « *Nous adaptons notre stratégie de sécurisation du SI de façon continue. Concernant le ransomware, plusieurs mesures renforcent notre politique de sauvegardes : tests de restauration, outils EDR, protection des emails et protection des flux, audits.*

« Seules les grandes entreprises ont les moyens de recruter les équipes techniques nécessaires pour maîtriser plusieurs clouds publics, afin de garantir un plan de reprise informatique efficace… »

Nicolas Martinez,
fondateur et PDG de LayerOps

Nous commençons à voir des deepfakes, mais l'institution n'est pas visée directement. Pour l'heure, nous menons surtout des campagnes de sensibilisation des utilisateurs, » témoigne Sandy Rosada, RSSI de l'Edhec.

La détection des cybermenaces est volontiers sous-traitée. « *L'EDR en mode managé bloque énormément de menaces, et se révèle souvent efficace* », confirme Denis Blandin. En complément, il déploie des passerelles filtrantes sur les terminaux (smartphones et PC), et adopte de bonnes pratiques de cloisonnement du SI. En revanche, pour faire évoluer les sauvegardes, il croit davantage au backup hors ligne qu'aux plateformes immuables : « *Un backup déconnecté du réseau résistera mieux au ransomware car il est immuable par nature* ».

Encadrer les nouveaux usages

La clé USB n'est pas sans risque. De même, chaque nouvel usage reste à encadrer. Pour éduquer ses utilisateurs, le RSSI progresse au rythme de l'IA dorénavant. « *Le facteur humain est critique car l'utilisateur est à l'origine de nombreux problèmes. Nous menons des campagnes de sensibilisation auprès des métiers, pointant l'usage des supports amovibles ou la navigation personnelle* ».

Un communiquant recruté récemment aide Denis Blandin à rédiger des messages adaptés aux risques des développeurs, managers, responsables RH ou comptables : « *Nous maximisons les canaux ciblant ces profils, via la newsletter, l'intranet, et à l'aide d'un chatbot à base d'IA : le bot de Riot Security nous permet d'offrir un coach cyber plaisant. Grâce à lui, chacun peut améliorer sa posture de protection au fil des interactions* », observe-t-il.

Accélérer la reprise d'activités

« *Seules les grandes entreprises ont les moyens de recruter les équipes techniques nécessaires pour maîtriser plusieurs clouds publics, afin de garantir un plan de reprise informatique efficace. Les TPE et PME souhaitent pourtant répartir et mixer leurs ressources informatiques sur des environnements distincts, souvent une salle interne et un cloud de proximité, voire une infrastructure certifiée SecNumCloud* », note Nicolas Martinez, fondateur et PDG de LayerOps.

Cet éditeur basé à Nîmes propose une solution multicloud fondée sur le déploiement rapide de conteneurs d'applications : « *en 15 minutes, l'entreprise dispose d'un environnement multi-fournisseur sur lequel elle peut déployer ses applications, avec une garantie de portabilité et de résilience* ».

Disponible en mode SaaS, LayerOps s'appuie sur des outils open source dédiés au cloud hybride tels LXD, l'hyperviseur de conteneurs de Canonical. L'entreprise utilisatrice évite à la fois le verrouillage et la surfacturation des géants du cloud, tout en gardant le contrôle sur l'emplacement de ses données et leur répartition selon leur sensibilité. Pour garantir une disponibilité continue durant les pics de trafic identifiés, elle planifiera l'équilibre de charge et gagnera en élasticité. Comptez 49 euros par mois pour cinq services, la résilience sur deux instances cloud distinctes, la gestion DNS d'un nom de domaine et le certificat SSL. En cas d'interruption de service, la création d'instance chez l'un ou l'autre des hébergeurs est automatisée, tous les services étant redéployés à partir des dernières sauvegardes. ▮

O.B

Trois questions à Jeff Pollard, vice-président, analyste principal du cabinet Forrester Research

L'InfoCR : A quelles nouvelles cybermenaces les organisations européennes doivent-elles se préparer et comment ?

Jeff Pollard : La première menace concerne toujours le ransomware, mais les deepfakes suivent de près. Ces enregistrements vidéo ou audio, réalisés ou modifiés grâce à l'IA forment de puissants vecteurs de fraudes. Ils peuvent aider à contourner l'authentification. Les stratégies et postures de cybersécurité doivent évoluer de façon continue à cause d'exigences réglementaires, mais aussi d'exigences des clients. En termes d'innovation numérique, l'IA demeure le segment le plus dynamique, et elle s'immisce dans les menaces aussi bien que dans les solutions de cybersécurité.

Quels outils de cybersécurité l'entreprise peut-elle envisager ?

J.P : D'abord, les outils de détection et de réponse aux attaques. Ensuite, la gestion du pipeline de données de sécurité apporte un suivi de l'ensemble des journaux de sécurité avec une télémétrie, tout en optimisant les budgets en fonction des usages. En complément, les solutions de nomenclature logicielle (SBOM) répertorient tous les composants et dépendances logicielles impliqués dans le cycle de développement et de déploiement d'applications. La sécurité des API et les outils de chiffrement postquantique (PQE) peuvent également figurer sur la liste des outils à explorer.

L'InfoCR : Quelles prestations de cybersécurité les organisations devraient-elles considérer ?

J.P : Les services managés de détection et de réaction aux menaces (MDR) affichent une satisfaction client croissante. Les entreprises ont besoin d'aide face aux menaces et cherchent des réponses adaptées. Les prestataires de services MDR assurent l'ingénierie pour détecter les menaces, chasser les codes malveillants, localiser les adversaires avant même qu'ils ne s'infiltrent dans l'environnement, et gérer la réponse pour le compte du client. Je pense que ce marché se développera vite en Europe.

Propos recueillis par O.Bouzereau

« La sensibilisation des soignants et plus largement de tous les personnels hospitaliers à la cybersécurité reste toujours d'actualité »

Philippe Tourron, RSSI ARS PACA et APHM

Les cyberattaques contre les établissements hospitaliers défraient régulièrement la chronique. Dans ce contexte, les Agences régionales de santé cherchent à renforcer les SI, à mutualiser les outils, à trouver des moyens de résilience ou encore, à sensibiliser DSI, personnels de santé et fournisseurs. Un challenge de taille, d'autant plus en l'absence d'un label cybersécurité européen dédié aux SI de santé. La route sera longue...

L'Informaticien : Quel est le rôle d'une Agence régionale de santé — ARS — en matière de cybersécurité ?

Philippe Tourron : Nous avons plusieurs missions. L'une d'entre elles est, une fois prévenue par l'établissement, de propager l'alerte auprès des services concernés en cas de cyberattaque et, plus largement, d'incident IT. C'est une obligation réglementaire. En amont, de ces crises, notre rôle est d'organiser les moyens techniques et les financements pour homogénéiser autant que possible le parc matériel et logiciel des établissements, a minima au niveau des GHT (groupement hospitaliers de territoire).

Concrètement, il s'agit notamment de motiver les différentes parties prenantes dans leurs appels d'offres. Nous avons également un rôle de prospective. Il s'agit de se projeter dans l'année ou les années suivantes, et d'imaginer comment mutualiser et partager au mieux les moyens techniques et humains des établissements. Enfin, la sensibilisation des soignants et plus largement de tous les personnels hospitaliers à la cybersécurité reste toujours d'actualité.

Les SI hospitaliers sont composés de centaines de logiciels et connectés à un nombre croissant d'IoT et d'équipements. Comment aidez-vous les hôpitaux à protéger cet existant ?

P.T : L'objectif global est d'accélérer la maturité des utilisateurs comme des fournisseurs sur ce sujet. Concernant l'existant dans les SI, il n'existe pas de solution miracle. Nous soutenons les établissements dans la mise en place de protection périmétrique. Deux pistes techniques sont particulièrement efficaces, la micro-segmentation des réseaux en particulier pour les IoT (seringues connectées...) considérés comme des objets auxquels on ne peut faire confiance. Concernant les équipements plus lourds (échographes...), la route sera plus longue. Il reste compliqué de faire évoluer le monde industriel et bio médical au même rythme que celui de l'IT.

L'analyse comportementale est également mise à contribution pour détecter les composants suspects. Un nombre croissant d'établissements implantent des sondes logicielles chargées de cette analyse. Le but est aussi à renouveler le SI, au fur et à mesure, avec des composants sécurisés. Nous aidons les établissements, et d'abord les plus petits ne disposant pas de DSI conséquentes, à formaliser leurs exigences en matière de cybersécurité dans leurs appels d'offre. Décrire ses besoins en termes de robustesse de chiffrement, par exemple, demande une expertise.

Le plan gouvernemental Care impose aux établissements de mettre en place des exercices récurrents pour maintenir la prise en charge en cas d'une cyberattaque. Quelles mesures préconisez-vous de votre côté en matière de résilience ?

P.T : Nous soutenons les innovations destinées à faciliter cette résilience. En 2020, nous avons lancé une cellule d'appui à la protection des systèmes d'information (CAPSI). Ce centre était l'un des premiers à proposer un accompagnement en cas d'incident majeur. Il propose également des formations personnalisées en cybersécurité. Autre exemple, le CH d'Avignon a bénéficié d'un financement ARS pour expérimenter un caisson mobile embarquant un SI minimum, permettant à un établissement de poursuivre son activité. Baptisé CleanRoom, cet équipement embarque un serveur et les applications de bases indispensables, comme un annuaire, la gestion des entrées-sorties, le suivi et l'accès aux résultats d'analyse. Il est bien sûr destiné avant tout aux petits établissements.

Prochaine étape, nous réfléchissons à le virtualiser et le mettre en ligne sur une infrastructure sécurisée pour faciliter une reprise des soins rapide suite à une cyberattaque. Ce SI minimum n'a pas vocation à se substituer au légitime, mais peut assurer la continuité de l'activité quelques semaines. Pour être encore plus efficace, cette démarche implique de travailler au niveau national pour définir encore mieux le socle applicatif minimum. Au-delà de ces actions, nous sensibilisons les acteurs politiques pour formaliser un label cybersécurité européen dédié aux SI de santé. Les fournisseurs ne sont soumis à aucune réglementation sur ce sujet. Depuis le plan Care, les établissements le sont, sans pour autant avoir, pour la plupart, les ressources humaines et financières nécessaires. ▮

PBR

SMART TECH

DELPHINE SABATTIER

7H30 | 18H30

VOTRE ÉMISSION QUOTIDIENNE DÉDIÉE À L'INNOVATION

Dans l'émission SMART TECH animée par Delphine Sabattier,
l'actualité du numérique et de l'innovation prend tout son sens.
Chaque jour, des spécialistes décryptent les dernières news, les tendances,
et les enjeux soulevés par l'adoption des nouvelles technologies.

N°230 orange™ | N°246 bouygues | N°163 free

B SMART by Change

Hewlett Packard Enterprise | intel | veeam | KIOXIA

En partenariat avec L'INFORMATICIEN

HPE Vision Summit

L'innovation vous ouvre ses portes

Cite Internationale Universitaire de Paris I Mardi 18 Mars I 18h00
17 boulevard Jourdan, 75014 Paris

Explorez nos solutions | Participez à des ateliers immersifs
Echangez avec nos experts | Partagez un moment convivial

Vos infrastructures, nos innovations
et si le meilleur était encore à venir ?

← Inscrivez-vous