Silicon

INSIGHTS FOR IT PROFESSIONALS

Silicon.fr

INTERVIEW DU DSI DE BOUYGUES SA
LES PROMESSES DE NIS2

CYBER MADE IN FRANCE
POURQUOI ÇA COINCE

GESTION DES IDENTITÉS
LE DERNIER REMPART

N°20 - SEPTEMBRE 2024

L 314277 -20 - F: 25€ - RD

inmac wstore
GROUPE BECHTLE

SNAPDRAGON X ELITE

UTILISEZ L'IA INTÉGRÉE COMME DEUXIÈME, TROISIÈME, ET MÊME QUATRIÈME CERVEAU

EN ATTENDANT NIS2

Quel est l'évènement cyber de cette rentrée 2024 ? La 24e édition des Assises qui réunit, début octobre, les RSSI, éditeurs, prestataires et experts à Monaco ? Pas cette fois.

Pour l'écosystème, il s'agit de cet acronyme promu depuis décembre 2022 par les hautes instances de l'Union européenne : NIS2, soit l'extension de la première version de la directive « Network & Information Security », qui entre en vigueur le 17 octobre.

À l'heure où nous publions ces lignes, on ne peut pas être certain que le calendrier sera respecté à la lettre tant l'instabilité législative qui règne pourrait jouer les trouble-fêtes.

Cependant, l'ANSSI, qui a piloté le projet de loi pour la transposer en droit national, se veut rassurante. Aucune sanction pour non-conformité ne sera appliquée avant 2027. L'essentiel tient dans le projet porté par la directive : harmoniser les pratiques de cybersécurité dans l'UE et élargir son champ d'application à de nouveaux secteurs d'activité et à différents types d'entreprises.

En France, on estime de 10 000 à 15 000, celles qui sont concernées par NIS2. Elles étaient 500 avec NIS1.

Mais qu'en pensent les managers IT ? NIS2 est perçue comme un tournant majeur en imposant des standards européens plus élevés, mais aussi davantage de communication et de transparence sur les cyberattaques. Mieux encore, elle impose une formation et une responsabilisation des dirigeants. Une étape essentielle pour une prise de conscience que les RSSI appellent de leur vœu depuis très longtemps : ne pas limiter la cybersécurité à un sujet d'expert technique, mais l'appréhender comme une thématique centrale de l'entreprise.

Philippe LEROY
Rédacteur en chef
pleroy@netmedia.group

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

NetMediaGroup

PRÉSIDENT
Pascal Chevalier

DIRECTEUR GÉNÉRAL ET DIRECTEUR DE LA PUBLICATION
Hervé Lenglart

DIRECTEUR GÉNÉRAL ADJOINT FRANCE
Jean-Sébastien Rocheteau

ÉDITORIAL
RÉDACTEUR EN CHEF
Philippe Leroy (pleroy@netmedia.group)
RÉDACTION
Clément Bohic (cbohic@netmedia.group)
ONT PARTICIPÉ À CE NUMÉRO
Olivier Bouzereau, Matthew Broersma, Alain Clapaud
RESPONSABLE DU STUDIO
Catherine Saulais
RÉALISATION
Catherine Saulais
Secrétariat de rédaction : Yann Guillaud
Crédits photos Adobe Stock

PUBLICITÉ
DIRECTRICE DU PÔLE AGENCES ET MARKETING
Mélina Lorentz – mlorentz@netmedia.group
CHEFS DE PUBLICITÉ
Simon Leprat (01 41 31 72 41) sleprat@netmedia.group
Mathilde Poirot (01 46 99 22 95) mpoirot@netmedia.group
Paul Gloaguen – pgloagen@netmedia.group
CHARGÉE PRINT
Natacha Forman – nforman@netmedia.group

ABONNEMENT ET MARKETING
RESPONSABLE MARKETING AUDIENCE
Marine-Alizé Lagoidet – mlagoidet@netmedia.group
RESPONSABLE MARKETING CLIENT ET PARTENARIATS
Christophe Minart – cminart@netmedia.group
RESPONSABLE MARKETING ABONNEMENT
Nicolas Cormier – ncormier@netmedia.group

ÉVÉNEMENTS
Jean-Sébastien Rocheteau

IMPRESSION
Léonce Deprez, allée de Belgique, 62128 Wancourt

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

Silicon est édité par Éditialis, SAS au capital de 136 000 €
Actionnaire NetMedia Group
N° ISSN : 2681-1006
Numéro de commission paritaire : 1226T94134
Dépôt légal : novembre 2019
Date de parution : septembre 2024

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

PEFC 10-31-1495 Cette entreprise a fait certifier sa chaîne de contrôle. pefc-france.org

SOMMAIRE

BIGDATA & AI

- PARIS -

13E ÉDITION

15-16 OCT. 2024

PARIS EXPO PORTE DE VERSAILLES

LÀ OÙ VOS [AI]MBITIONS DEVIENNENT RÉALITÉ !

20 000 PARTICIPANTS

250 EXPOSANTS

350 SPEAKERS

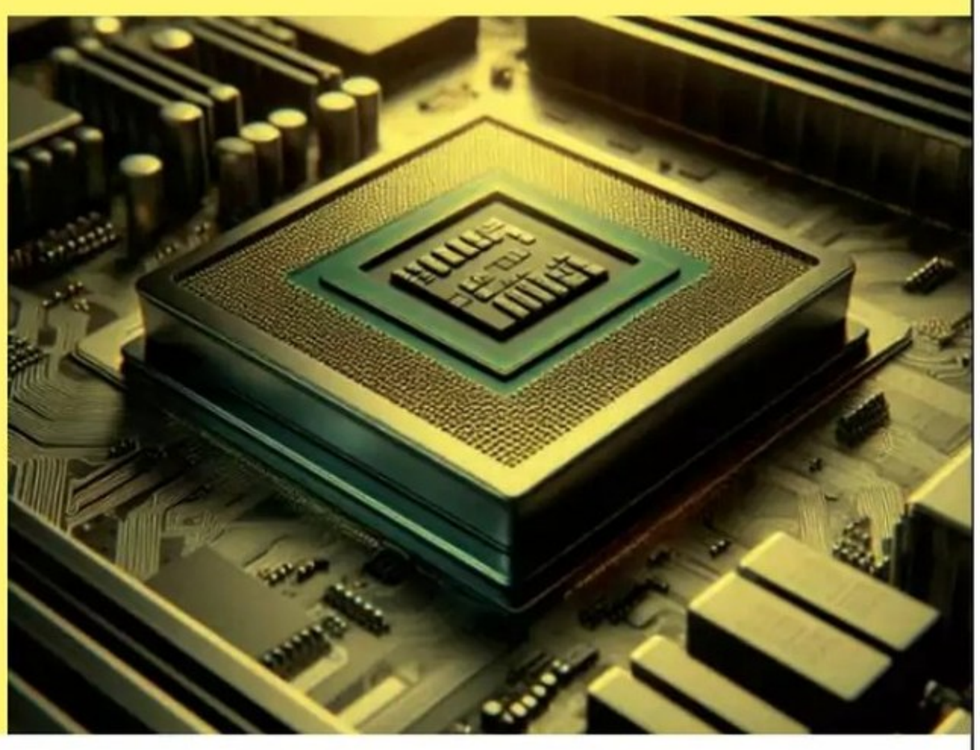
www.bigdataparis.com

Organisé par

RX In the business of building businesses

ZT SYSTEMS, une acquisition à point nommé pour AMD ?

ZT Systems vaut-il 4,9 milliards de dollars ? AMD s'est en tout cas engagé à débourser ce montant pour acquérir le fabricant de serveurs américain. Objectif : boucler la transaction dans le courant du premier semestre 2025. Né il y a près de 30 ans (septembre 1994), ZT Systems fournissait initialement des PC de bureau et des serveurs pour PME. Dans les années 2000, l'entreprise avait pivoté vers le datacenter. Elle fournit aujourd'hui « *des centaines de milliers* » de serveurs par an. Les dernières « *annonces IA* » de ZT Systems impliquant AMD commencent à dater. On en trouve notamment en 2018, avec l'officialisation de serveurs 3U en EPYC et Radeon Instinct, basés sur le projet Olympus. Celui-ci est porté par Microsoft dans le cadre de l'Open Compute Project. ZT Systems rejoindra la division Data Center Solutions d'AMD. Son directeur général prendra la tête de l'activité de fabrication ; son président, celle de l'activité de conception.



BROADCOM FERME L'IT ACADEMY... DE VMWARE

Depuis son rachat de VMware fin 2023, Broadcom a officialisé la fin des programmes IT Academy et Academic Software Licensing. Le premier permet aux enseignants de dispenser des cours sur les technologies VMware (accès à des supports, à des clés de licence et à des coupons de réduction pour des certifications). Le second leur permet d'exploiter les logiciels de l'éditeur en mode lab. Les logiciels en question : Workstation, Fusion, vSphere Enterprise Plus, vCenter Server Standard, vRealize et vSAN Enterprise Edition.

HPE CROQUE MORPHEUS DATA

Avec Morpheus, HPE souhaite se renforcer sur le marché du CloudOps face à de sérieux concurrents comme Red Hat et VMware, mais également des CSP, AWS et Google Cloud en tête. Intégrée à GreenLake, la plateforme Morpheus Data apportera des fonctions d'automatisation, d'orchestration multi-Cloud et d'optimisation des coûts (FinOps).
La transaction doit être finalisée au début du quatrième trimestre. Cependant, Morpheus continuera sa commercialisation en tant que logiciel autonome.

COMMENT L'IA BOOSTE LE CLOUD

L'IA est un gros booster des dépenses mondiales dans le Cloud affirme IDC. Avec plus de 40 % des dépenses totales, le SaaS reste la catégorie dominante du Cloud. Cependant, les segments PaaS et IaaS devraient représenter chacun près de 20 % du marché du Cloud public en 2024. « *Les progrès rapides de l'IA stimulent considérablement l'augmentation des dépenses Cloud. Les entreprises construisent, testent et déploient de plus en plus de plateformes d'IA, créant une interdépendance croissante entre l'innovation dans l'IA et l'infrastructure Cloud, positionnant les services Cloud au cœur du développement et du déploiement de l'IA* », note Andrea Minonne, responsable de recherche Data & Analytics chez IDC.

Gemini s'embarque sur BigQuery et Locker

Google Cloud a intégré Gemni, son assistant à base d'IA générative, dans BigQuery, son service de datawarehouse Cloud, et dans Looker, son offre de BI. Beaucoup de plateformes d'analyse de données ou les autres CSP proposent déjà une couche d'IA générative.

Thalès : 1 - VMware : 0

Thalès a attaqué VMware auprès du Tribunal de commerce de Paris pour pratiques commerciales abusives Le groupe avait commandé, fin 2023, pour plusieurs millions d'euros de solutions en licence perpétuelle avant son rachat par Broadcom qui a modifié les conditions d'exécution du contrat.

UC&C, toujours en hausse

Selon IDC, le marché mondial des communications unifiées et de la collaboration (UC&C) devrait générer 69,1 milliards de dollars de revenus en 2024, une hausse de 7,5 % sur un an. Le cabinet estime que l'introduction continue de capacités d'IA dans les offres est l'un des moteurs de cette croissance.

QUAND

VOUS REFERMEZ

UN 

UNE NOUVELLE VIE

S'OUVRE À LUI.

EN TRIANT VOS JOURNAUX,
MAGAZINES, CARNETS, ENVELOPPES,
PROSPECTUS ET TOUS VOS AUTRES
PAPIERS, VOUS AGISSEZ POUR UN MONDE
PLUS DURABLE. DONNONS ENSEMBLE
UNE NOUVELLE VIE À NOS PRODUITS.

CONSIGNESDETRI.FR

CITEO

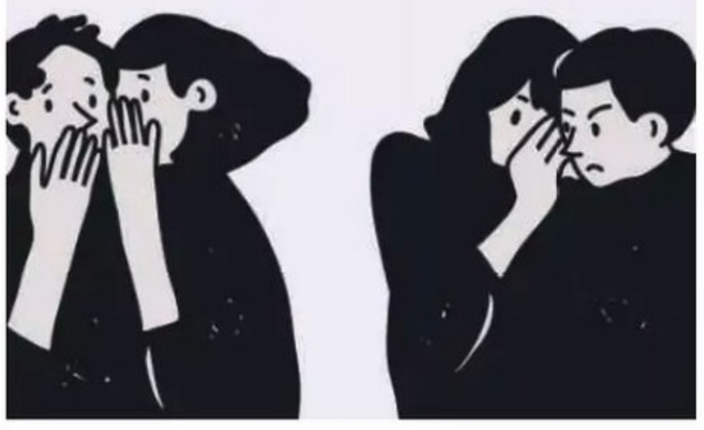
Le nouveau nom d'Eco-Emballages et Ecofolio

Vers un **RÉPERTOIRE** référent des **RISQUES LIÉS À L'IA** ?

Une première version de l'AI Risk Repository concrétise un travail collectif – emmené par le MIT – de compilation des risques associés à l'IA. Ses soutiens le présentent comme « *la première tentative de sélection, d'analyse et d'extraction rigoureuse de frameworks sur les risques de l'IA sous la forme d'une base de données publique, exhaustive, extensible et catégorisée* ». Cette base de données (au format tableur Google ou Excel) regroupe environ 800 risques issus d'une quarantaine de sources. Elle permet un filtrage sur la base d'une deuxième taxonomie centrée non pas sur les causes, mais sur les domaines de risques. Elle s'inspire aussi de travaux antérieurs, signés DeepMind. La filiale de Google est à l'origine de plusieurs autres productions utilisées pour constituer la base de données. Elles traitent par exemple de l'éthique des assistants IA, des risques sociaux des modèles de langage et de l'évaluation des risques extrêmes de l'intelligence artificielle.

OPENAI CHERCHE DES ALTERNATIVES À NVIDIA

Le *Financial Times* rapporte des discussions avec des concepteurs de semi-conducteurs, dont Broadcom. « *OpenAI a des discussions en cours avec les parties prenantes de l'industrie et du gouvernement sur l'augmentation de l'accès à l'infrastructure nécessaire pour garantir que les avantages de l'IA soient largement accessibles. Cela implique de travailler en partenariat avec les principaux concepteurs de puces, fabricants et développeurs physiques de centres de données* », a déclaré OpenAI.



MISTRAL AI DÉVOILE SON LLM LARGE 2

Mistral AI a lancé son LLM de 123 milliards de paramètres appelé Mistral Large 2 (ML2), La start-up française indique que ML2 dispose d'une fenêtre contextuelle de 128k et prend en charge des dizaines de langues, dont le français, l'allemand, l'espagnol, l'arabe, le chinois, le japonais et le coréen. Il supporte aussi plus de 80 langages dont Python, Java, C, C++, JavaScript et Bash. Sa disponibilité, sous licence restrictive MRL, est cependant perçue comme un frein par les observateurs.

MICROSOFT X OPENAI : PAS DE PRISE DE CONTRÔLE SELON L'UE

L'investissement de 13 milliards de dollars de Microsoft dans OpenAI implique-t-il une prise de contrôle sur la pépite américaine de l'intelligence artificielle générative ? En janvier 2024, la Commission européenne avait lancé une enquête sur le sujet, en particulier pour étudier « *certains des accords qui ont été conclus entre les grands acteurs du marché numérique et les développeurs et fournisseurs d'IA générative* » et « *l'impact de ces partenariats sur la dynamique du marché* ». Margrethe Vestager, la commissaire en charge du Digital, a répondu : c'est non.

Box acquiert Alphamoon

Cett start-up polonaise est spécialisée dans le traitement IA des documents. Ses fonctionalités seront intégrées à Box AI. Elle combine des modèles de langage de grande taille (LLM) de pointe avec une technologie OCR et de traitement de documents.

OpenAI lance SearchGPT

Le moteur de recherche est lancé en phase de prototypage. Les utilisateurs doivent s'inscrire sur une liste d'attente pour y accéder. « *Bien que ce prototype soit temporaire, nous prévoyons d'intégrer le meilleur de ces fonctionnalités directement dans ChatGPT à l'avenir* », indique OpenAI.

PC IA : le nouveau marché frémit

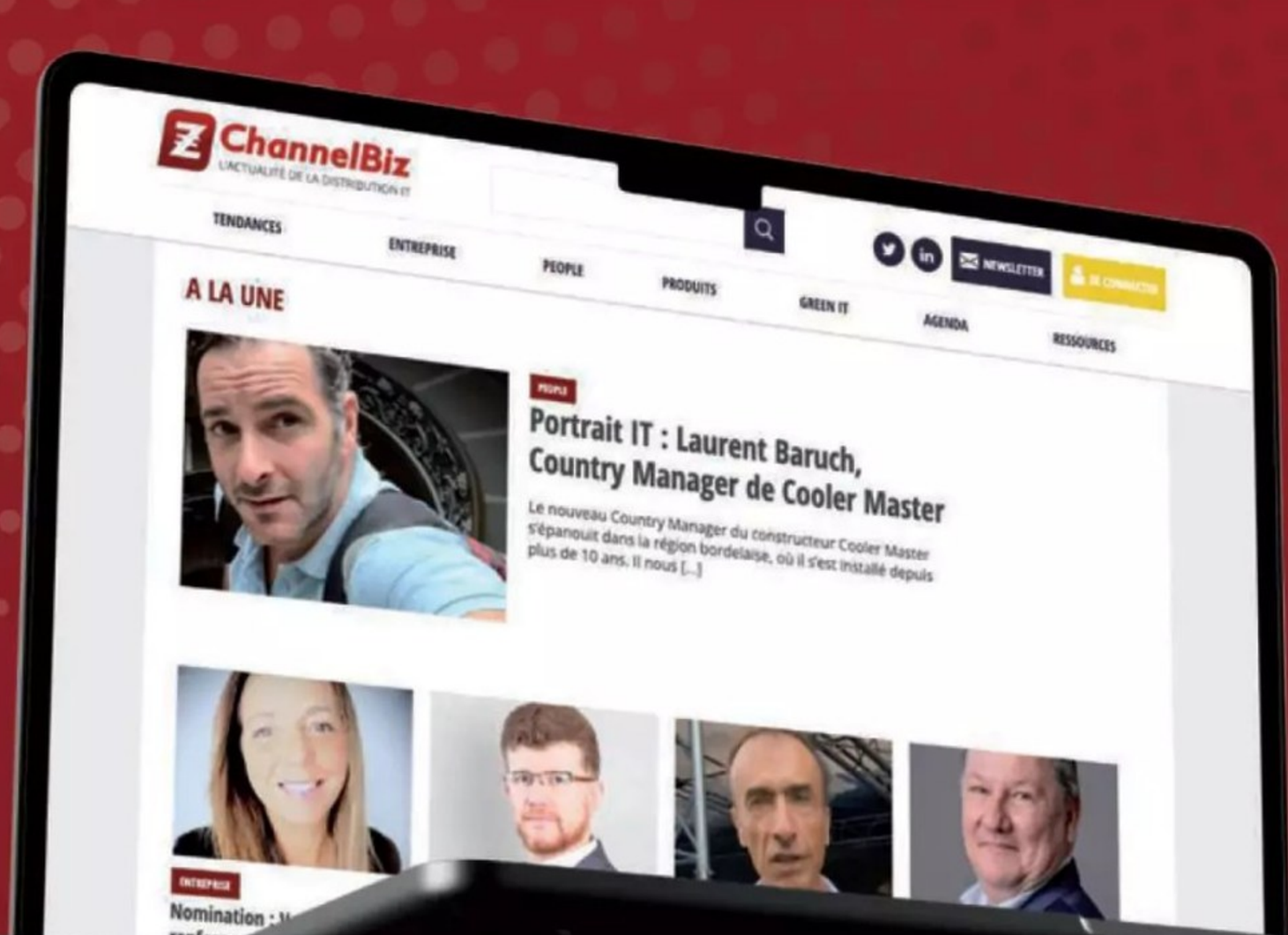
Selon Canalys, 8,8 millions de PC motorisés pour gérer les charges de travail d'IA ont été vendus au deuxième trimestre 2024, soit 14 % des ventes mondiales. Avec les gammes Mac embarquant ses puces M, Apple est le leader de ce nouveau segment sur cette période.

ChannelBiz
L'ACTUALITÉ DE LA DISTRIBUTION IT

En savoir plus

(Re)découvrez ChannelBiz.fr

Le site des Professionnels de la Distribution IT & Tech



- Grossistes
- Revendeurs
- MSP & ESN
- Intégrateurs
- Constructeurs
- Éditeurs

Pour décryper avec vous l'actualité et les tendances des marchés de l'#informatiques, #AudioVisuel, #Cyber, et #Telecom.

Simon LEPRAT
sleprat@netmedia.group
06 71 59 66 52

Suivez-nous sur les réseaux sociaux

MICROSOFT fixe un nouveau rendez-vous pour RECALL

Comparé à une « mémoire photographique », Recall permet de retrouver, par une recherche ou via une timeline, des contenus que l'on a consultés. L'idée de départ était de proposer cette fonctionnalité phare des PC Copilot+ en parallèle de leur lancement commercial en juin 2024. Mais quelques jours avant l'échéance, Microsoft avait changé son fusil d'épaule pour limiter sa disponibilité au programme Windows Insider, en version bêta. Objectif : que la fonctionnalité soit *« conforme à [ses] standards de qualité et de sécurité »*. L'éditeur avait notamment décidé de le mettre en opt-in, sur les appareils grand public. Finalement, Recall sera disponible à partir d'octobre, en version stable, pour Windows Insider avant d'être déployé sur l'ensemble de la gamme PC Copilot+.

CANONICAL ÉTEND SON APPROCHE LTS À L'AUNE DES CONTENEURS

Réduire l'empreinte des conteneurs et la surface d'attaque par la même occasion ? Chez Canonical, on pousse cette logique avec Chisel. L'outil – open source – permet de découper des paquets Debian en « tranches ». Il se fonde sur le fait que les applications n'exploitent généralement qu'un sous-ensemble de chacune de leurs dépendances.

TEAMS : L'UE ADRESSE SES GRIEFS À MICROSOFT

La Commission européenne a informé Microsoft qu'il avait enfreint les règles de concurrence au sein de l'UE en liant Teams à ses suites bureautiques Office 365 et Microsoft 365. Elle estime que *« les limitations de l'interopérabilité entre les concurrents de Teams ont aggravé cette domination. »* Si aucune durée légale n'est prévue pour ce type d'enquête, la communication des griefs ne présume pas pour autant une condamnation de l'éditeur de Windows. La plainte a été déposée par Slack en 2020 pour abus de position dominante.

WSL2 FAIT LE GRAND SAUT VERS LINUX 6.6

Moins de travail pour Microsoft sur la récupération de mémoire, le reporting de pages, les sockets VM et la vCPI ? Linux 6.6 apporte des améliorations sur ces quatre points. Cela va bénéficier à WSL2 qui intègre cette version du noyau. Une forme de décharge pour Microsoft, qui avait jusqu'ici assuré la maintenance de ces fonctionnalités en aval. Les précédentes versions de WSL2 utilisaient Linux 5.15. Une mouture fondée sur Linux 6.1 avait émergé début 2023, mais les développements sur cette base ne se sont pas poursuivis.

Une offre de visionconférence signée X ?

Un développeur de X, Chris Park, a indiqué que le réseau social avait organisé sa première visoconférence avec un outil interne. *« Déjà une alternative très solide à Google Hangouts, Zoom, AWS Chime et certainement... Microsoft Teams »*, a-t-il commenté. Y aura-il une offre commerciale ?

VMware IT Academy, c'est fini

Broadcom a officialisé la fin des programmes IT Academy et Academic Software Licensing de VMware dont il a pris le contrôle en 2023. Le renouvellement des abonnements annuels n'est plus possible tandis que les licences encore valides devaient avoir été attribuées au 31 août.

Grafana Labs se valorise

L'éditeur de la plateforme open source d'observabilité, Grafana Cloud, est valorisé près de 6 milliards de dollars suite à sa dernière levée de fonds de 270 millions de dollars. Il revendique 20 millions d'utilisateurs dans le monde et plus de 250 millions de dollars de revenus annuels.

27-28 NOVEMBRE 2024 | PARIS, PORTE DE VERSAILLES

TECH SHOW PARIS

5 DIMENSIONS DE L'UNIVERS TECH RÉUNIES EN UN MÊME LIEU

Tech Show Paris réunit les leaders des industries Cloud, DevOps, Cyber, Data & AI, et Data Centre, avec pour objectif de s'instruire, partager, innover et générer des opportunités. Venez rencontrer vos pairs, optimiser vos coûts et votre temps, et vous informer sur les dernières tendances technologiques.
Au programme : l'IA, l'éco-responsabilité, la diversité et l'innovation seront au cœur de l'évènement !

+ de 6 200 visiteurs | + 255 exposants I + de 290 conférenciers

RETIREZ VOTRE BADGE GRATUIT

techshowparis.fr

REGROUPANT

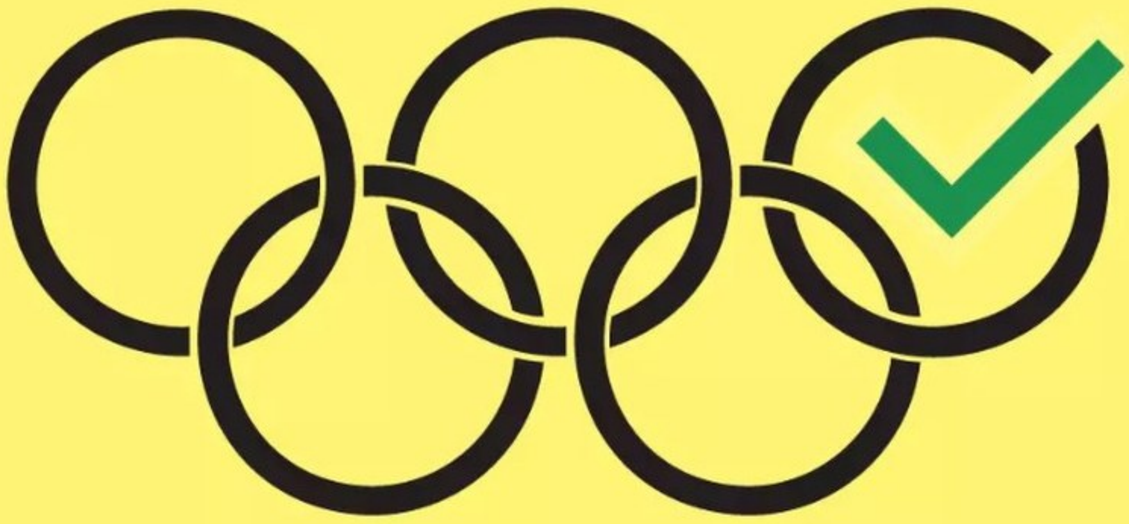
CLOUD EXPO EUROPE | DEVOPS LIVE | CLOUD & CYBER SECURITY EXPO | BIG DATA & AI WORLD | DATA CENTRE WORLD

L'ÉVÈNEMENT DÉDIÉ AUX PROFESSIONNELS DE LA TECH EN FRANCE

ORGANISÉ PAR CloserStill

JO PARIS 2024 : des cyberattaques sans gravité

En cybersécurité, non plus, le pire n'est jamais sûr... On ne peut que s'en rejouir au moment de faire le bilan de Paris 2024. Selon l'Agence nationale de la sécurité des systèmes d'information (ANSSI), 141 *« événements de cybersécurité »*, en lien avec les JO, ont été signalés. Principales cibles : les entités gouvernementales, le sport, les transports et les télécommunications. Dans le détail, l'ANSSI évoque la prédominance des attaques par déni de service (DDoS), mais également des tentatives de compromission, des divulgations de données et des signalements de vulnérabilités. *« Tous les événements cyber survenus au cours de cette période sont globalement caractérisés par leurs faibles impacts »*, affirme l'agence. Et aucun n'a perturbé le bon déroulement des épreuves.



PARIS-SACLAY VICTIME D'UN RANÇONGICIEL

L'établissement public a indiqué être *« accompagné par l'ANSSI pour traiter cet incident »*, en précisant que la situation était *« sous contrôle »*. Il a touché tous les services centraux, les cinq facultés (économie-droit-management, médecine, pharmacie, sciences, sciences du sport), les trois IUT (Cachan, Orsay, Sceaux), ainsi que PolyTech et l'Observatoire des sciences de l'univers.

LA CNIL CRITIQUE L'EUCS

Pas assez protecteur pour les données personnelles. C'est le jugement de la CNIL sur le projet de Certification européenne pour les services de Cloud (EUCS) piloté par l'Agence de l'Union européenne pour la cybersécurité (ENISA). *« Dans son état actuel, le projet de Certification européenne pour les services de Cloud (EUCS) ne permet plus aux fournisseurs de démontrer qu'ils protègent les données stockées contre tout accès par une puissance étrangère, contrairement à la qualification SecNumCloud en France. »*

LE NIST PUBLIE SES PREMIERS STANDARDS POST-QUANTIQUES

Trois algorithmes de chiffrement post-quantique ont désormais le statut de norme NIST, l'agence du gouvernement américain chargée d'établir les normes. Il s'agit de ML-KEM pour sécuriser les accès à des sites via un canal public, ML-DSA qui génère des clés de signature électronique pour des échanges de document et des communications sécurisées, ainsi que SLH-DSA qui crée des clés publiques de signature électronique de plus petite taille. Un quatrième est en ligne de mire à moyen terme.

Whaller DONJON certifiée SecNumCloud

C'est la première plateforme collaborative, en mode SaaS, à obtenir la qualification du référentiel de l'ANSSI. Elle repose sur les solutions IaaS d'OVHcloud, également qualifiées SecNumCloud. Le niveau « SaaS » est le plus complet de la qualification SecNumCloud en garantissant que toutes les couches inférieures (IaaS, CaaS, PaaS) respectent également le référentiel.

Firefox généralise le HTTPS

Avec Firefox 129, publié début août, HTTPS remplace HTTP comme protocole par défaut dans la barre d'adresse, sur les sites non locaux. C'était le cas, depuis 2021, uniquement en mode navigation privée.

Acronis contrôlé par EQT

Le fonds suédois EQT devient l'actionnaire majoritaire de l'éditeur suisse de solutions cyber pour les MSP. Les fondateurs, la direction et les investisseurs existants – CVC, Springcoast et BlackRock Private Equity Partners – resteront des actionnaires minoritaires.

L'IA : un allié incontournable contre les cyberattaques

Les cyberattaques, notamment les ransomwares, prolifèrent à un rythme alarmant, touchant toutes les industries. Face à cette menace, l'intelligence artificielle (IA) se révèle comme un allié précieux pour prévenir et préparer les entreprises à ces attaques.

L'importance de la sensibilisation de tous

Xavier Bourdelois, manager avant-vente chez Commvault, société spécialisée dans la protection des données, souligne que l'IA intégrant une dimension machine learning analyse et sécurise les données de manière proactive. Elle permet de détecter automatiquement les données sensibles et de surveiller les comportements anormaux, réduisant ainsi les risques de failles de sécurité.

L'une des applications critiques de l'IA est la prévention des attaques. Les systèmes basés sur l'IA analysent des volumes massifs de données en temps réel pour identifier les menaces potentielles. Ils utilisent des algorithmes sophistiqués pour reconnaître les comportements suspects, permettant de neutraliser les attaques avant qu'elles ne causent des dommages. Xavier Bourdelois explique que les solutions Commvault embarquent des mécanismes d'apprentissage automatique qui identifient proactivement les risques sur les surfaces d'attaque.

Une autre stratégie innovante est la cyberdéception, qui consiste à créer des leurres pour attirer et piéger les cybercriminels. Ces leurres imitent les actifs numériques les plus précieux d'une entreprise pour détourner les attaquants des vraies cibles. Grâce à l'IA, ces systèmes de leurres s'adaptent en temps réel aux nouvelles tactiques des attaquants. Cette approche proactive permet de détecter les menaces plus tôt et de réduire les risques d'attaques réussies.

En cas d'attaque réussie, l'IA permet une restauration rapide et sécurisée des données. Les algorithmes d'IA peuvent recréer des environnements isolés pour permettre une reprise d'activité rapide, minimisant ainsi les interruptions de service. Xavier Bourdelois précise que Commvault, utilise l'IA afin d'automatiser la restauration des données et assure qu'elles sont exemptes de toute infection. Cela signifie que, même en cas de compromission, les entreprises peuvent récupérer rapidement leurs capacités de service et reprendre leurs activités sans subir de pertes de données significatives.

Une cybersécurité éthique et responsable

L'intégration de l'IA dans la cybersécurité doit se faire de manière éthique et responsable. Xavier Bourdelois insiste sur l'importance de la conformité et de la transparence dans l'utilisation des algorithmes d'IA. Commvault adopte des politiques strictes pour garantir que les données sont sécurisées, anonymisées et conformes aux normes légales. Cette approche éthique est essentielle pour maintenir la confiance des clients et des partenaires commerciaux, tout en assurant une protection optimale contre les menaces numériques.

De plus, Commvault met en place des mesures pour assurer que les algorithmes d'IA utilisés sont fiables et respectent les cadres de conformité en vigueur. Cela inclut l'utilisation du cadre de référence NIST RMF 1.0 pour vérifier la cohérence et la véracité des informations traitées. L'entreprise s'engage à garantir que les données manipulées par l'IA sont authentiques, sécurisées et utilisées de manière responsable. ■

Commvault

ALAIN BOUILLÉ (CESIN)

"IL FAUT SE PENCHER SUR LA DOMINATION CROISSANTE DE THOMA BRAVO DANS LA CYBERSÉCURITÉ"

Le Cesin s'inquiète du rachat d'importants éditeurs de solutions de cybersécurité par le fonds américain Thoma Bravo. Alain Bouillé, délégué général du Cesin, détaille les craintes que cette concentration suscite pour les entreprises françaises.

Vous alertez sur la concentration des éditeurs de cybersécurité au sein du fonds d'investissement Thoma Bravo. Quelles sont les craintes du Cesin* ?

Alain Bouillé – Les craintes sont de plusieurs ordres. Financier d'abord : on connaît trop bien la mécanique de ce type de fonds : il faut absolument rentabiliser l'investissement pour que la plus- value soit la plus élevée possible au moment de la revente. Et un des moyens les plus simples pour atteindre cet objectif, c'est d'augmenter les prix ! Pour la plupart des solutions rachetées par Thoma Bravo, il est très difficile d'en changer car elles sont souvent très imbriquées au SI de l'entreprise. Je pense en particulier aux solutions d'IAM comme SailPoint qui prennent souvent des années à être déployées. Les entreprises sont quasiment prisonnières et subiront immanquablement ces augmentations de coûts.

Le deuxième aspect est le fait que par accident, une entreprise peut se retrouver à mettre tous ses œufs dans un même panier. Les entreprises qui ont des politiques de diversification des solutions, qu'elles vont utiliser pour ne pas dépendre que d'un seul fournisseur, vont se retrouver piégées par ces rachats successifs qui, rappelons-le, couvrent un large spectre des panoplies cyber nécessaires à la protection des entreprises. Par ces rachats successifs, on peut se retrouver in fine à avoir toute ou partie de sa panoplie cyber au sein d'un même fonds.

Enfin, ces entreprises de cybersécurité sont extrêmement intrusives en manipulant et stockant des données d'entreprises parfois très sensibles. Tant que ces données sont détenues de manière cloisonnées chez les différents éditeurs, le risque est moindre, mais une fois entre les mains d'un unique acteur, l'intensité du risque est démultiplié.

Alain Bouillé, délégué général du Cesin.

*** Le Club des experts de la sécurité de l'information et du numérique (Cesin) compte plus de 900 membres issus de tous les secteurs d'activité, dont des entreprises du CAC40 et du SBF120, et des ministères.**

Vous évoquez des risques pour les entreprises françaises. À quel type de menaces pensez-vous ?

La principale menace pour les entreprises clientes, du fait des économies devant être réalisées par les entreprises rachetées, encore une fois pour être plus rentables in-fine, est que la R&D, pourtant le nerf de la guerre des solutions cyber, soit sacrifiée sur l'autel des économies. Les exemples comme ceux de Symantec ne manquent pas. Une solution cyber qui ne suit pas, ou ne précède pas, les innovations des attaquants va devenir beaucoup moins pertinente, mais de manière pernicieuse car ça ne se verra pas tout de suite.

Vous suggérez la mise en place de mesures adaptées pour prévenir la dépendance involontaire et sécuriser les infrastructures critiques en France et en Europe. Pouvez-vous en citer quelques-unes ?

On pourrait de manière cynique se réjouir de cette situation en imaginant que cela soit profitable au marché français et donc à la souveraineté, car les entreprises pourraient se tourner vers le marché européen afin d'à nouveau diversifier leur panoplie et minimiser les risques de concentration. On vient de voir qu'Imperva, passée entre les mains de Thoma Bravo, vient d'être rachetée par Thalès. Mais ça ne suffit pas. Il manque en France un géant du logiciel cyber du type Palo Alto capable de couvrir la majorité des pans de la cybersécurité des entreprises. Nous avons de belles pépites sur notre territoire, mais le marché est fragmenté et donc trop fragile face à ces géants. ■

Propos recueillis par Philippe Leroy

L'ÉVÉNEMENT DU CHANNEL DIGITAL

IT Partners

5 & 6
FÉVRIER
2025

PARIS LA DEFENSE ARENA

RX In the business of building businesses

itpartners.fr

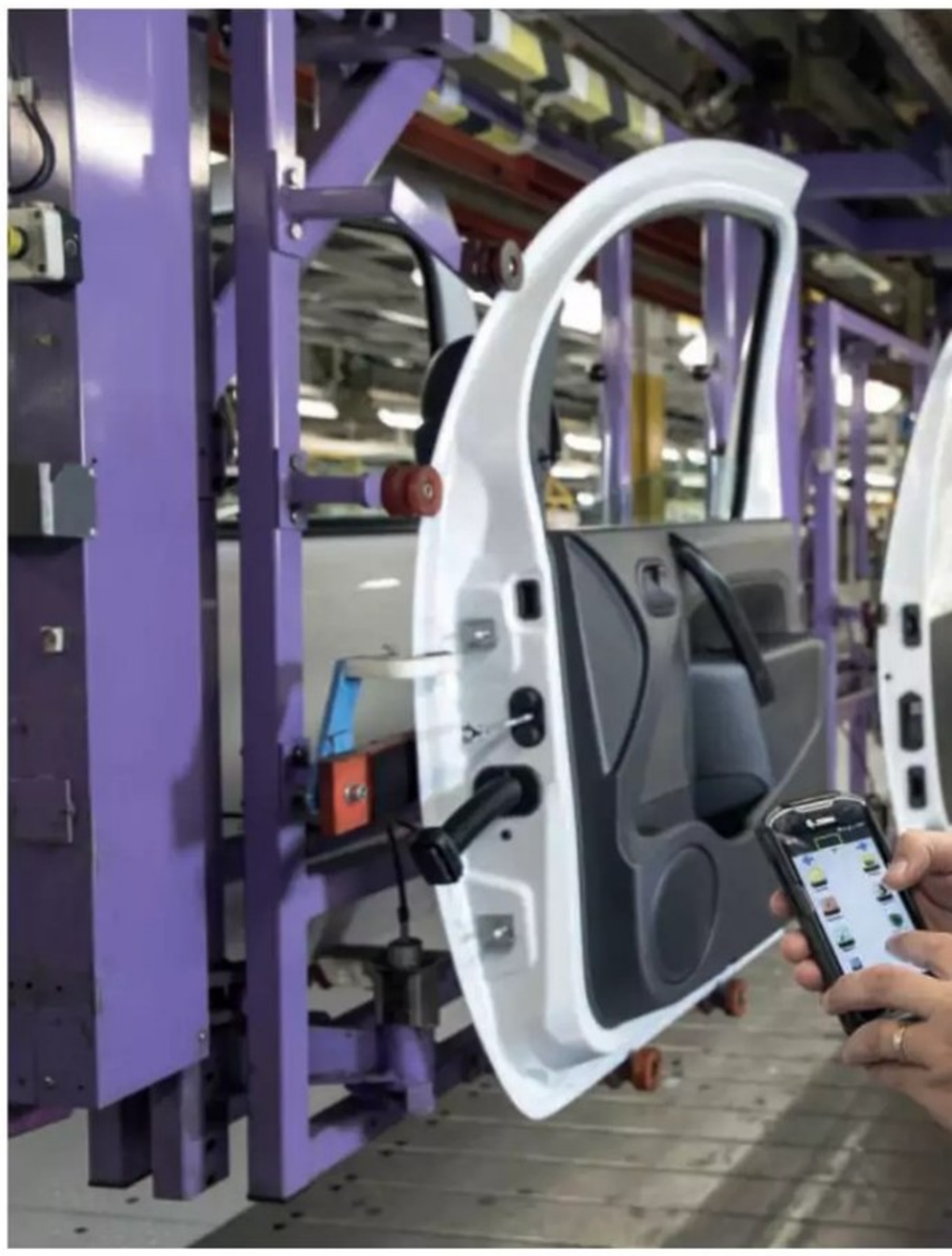
CYBER OT : LA PRISE DE CONSCIENCE DU SECTEUR INDUSTRIEL

Les systèmes industriels s'ouvrent et s'exposent bien plus largement aux risques de cybersécurité que par le passé. À l'heure de leur transformation digitale, la stratégie du château fort ne tient plus.

DANS SON RAPPORT ANNUEL sur l'état de la sécurité des systèmes industriels, Fortinet pointe une forte augmentation des tentatives d'intrusion en 2024. 31 % des industriels interrogés expliquent avoir détecté plus de six intrusions. Si le nombre de malware est en baisse, les attaques par phishing et par emails compromis sont très fréquentes.

De risque potentiel et très exceptionnel, une attaque sur un système industriel est devenue un risque systémique. « *On observe une prise de conscience sur le fait que l'industrie regroupe aujourd'hui des activités numérisées et interconnectées. À ce titre, la question de la cybersécurité est devenue cruciale. On observe un rattrapage par rapport à un historique* », soutient Nicolas Arpagian, vice-président Cybersecurity strategy & Digital risks au cabinet Headmind Partners.

L'expert souligne qu'outre le poids de l'industrie dans l'économie, les entreprises sont souvent internationalisées, avec des supply chains intégrant de multiples acteurs, et travaillent sur des marges faibles. Or, quand un industriel se trouve immobilisé par un malware, les pertes économiques sont immédiates et une attaque peut potentiellement avoir des conséquences dans le monde physique... « *Le concept d'interdépendance des acteurs s'applique particulièrement bien à RTE, puisque nous ne produisons rien, mais nous sommes extrêmement dépendants des fournisseurs d'énergie et des consommateurs* », explique Xavier Carton, son RSSI. « *Les niveaux de maturité en termes de résilience de ces acteurs sont très différents. Une autre particularité de notre marché porte sur les échelles de temps : de quelques millièmes de seconde, pour réagir en cas d'incident sur le réseau, et de 10 à 15 ans pour les investissements* », précise-t-il. Et de souligner qu'en cas d'incident majeur chez RTE, la lumière va immédiatement s'éteindre chez les abonnés, puis ce seront les télécoms et les hôpitaux quand ils arriveront au bout des capacités de leurs groupes électrogènes, ce qui se traduira par des pertes en vies humaines. Nicolas Arpagian pointe le retard des fournisseurs de technologies cyber vis-à-vis de ce marché OT (des technologies opérationnelles ou d'exploitation) très spécifique : « *Comme il s'agissait d'un domaine économique moins numérisé, les industriels étaient moins attractifs pour les éditeurs de*



En mai 2017, une simple attaque par le ransomware WannaCry immobilisait plusieurs usines du groupe Renault. Une attaque purement IT qui a eu de lourdes conséquences sur l'outil industriel du constructeur automobile.

12,75 Mds $

C'est le chiffre d'affaires mondial du marché de la cybersécurité pour les systèmes industriels en 2023, selon ABI Research (juin 2024).

> *« Il s'agit majoritairement d'attaques sur l'IT qui rebondissent sur l'OT ; soit par un défaut dans l'architecture, soit une simple clé USB. »*
>
> ***Loïs Samain, RSSI EDF Hydro.***

Si les systèmes SCADA des grands constructeurs embarquent aujourd'hui des capacités de protection relativement avancées, et sont conçus dans une approche « Secure by Design », la durée de vie des matériels industriels est telle qu'il faudra des décennies pour remplacer le parc existant. Des firewalls spécialisés sont conçus pour protéger ces systèmes critiques, mais vulnérables.

solutions de sécurité. Le jeu de l'offre et de la demande a fait que les éditeurs n'ont pas jugé utile d'investir dans des solutions propres au monde industriel. Il y a eu une phase où on a cherché à plaquer des solutions qui n'étaient pas issues du monde industriel. Or l'industrie a de fortes spécificités techniques. »

Les industriels doivent muscler les défenses de leurs systèmes industriels, mais restent tout autant exposés aux attaques IT très classiques. C'est le souci de Loïs Samain, RSSI EDF Hydro : *« On parle de plus en plus de cyberattaques contre les systèmes industriels, mais les vraies attaques spécifiques se comptent encore sur les doigts d'une main. Il s'agit majoritairement d'attaques sur l'IT qui rebondissent sur l'OT ; soit par un défaut dans l'architecture, soit une simple clé USB. On se souvient tous de l'attaque Stuxnet. Ce risque de rebond doit nous pousser à réfléchir à la façon dont on cloisonne ces systèmes, notamment avec l'arrivée du Cloud et des données industrielles qui vont sur AWS ou GCP. »*

Ce risque de rebond est d'autant plus fort que les grands industriels travaillent avec des supply chains très intégrées, avec des sous-traitants et des prestataires qui collaborent et échangent des données via de multiples plateformes et applications. Philippe Verhé, Head of Managed Services chez Airbus Protect raconte les conséquences d'une cyberattaque sur un fournisseur de rang 2 qui a affecté la livraison des avions de ligne : *« Le groupe Airbus est avant tout un intégrateur et, sur ce plan, la sécurité de la supply chain est capitale. Nous avons connu l'année dernière une attaque sur un fournisseur de rang 2 qui produit des équipements plutôt anodins et pas de haute technologie. L'attaque a paralysé sa chaîne de production. Or, travaillant à flux tendu, celui-ci n'a pu livrer notre fournisseur de rang 1 qui n'a pu nous livrer. Cela à eu un impact sur la chaine d'assemblage et, au final, un impact sur la livraison des avions. »*

Les montants financiers de tels retards de livraisons sont conséquents, sans compter l'impact en termes d'image pour l'industriel... Si Airbus a mis en place des exigences cyber vis-à-vis de ses fournisseurs, le décalage entre le rythme cyber et celui des investissements OT reste criant. Il faudra des décennies pour sécuriser les grandes installations industrielles. ■

Par Alain Clapaud

COMMENT ACCOR A BASCULÉ SON SYSTÈME DE RÉSERVATION SUR AWS

La plateforme de réservation du groupe Accor, TARS, est exploitée sur AWS depuis fin 2023. Une migration à haut risque menée avec succès sans rupture de service grâce à une approche de type “blue/green”. Retour d’expérience.

FILIALE À 100 % d’Accor, D-Edge assure l’exploitation de TARS (« The AccorHotels Reservation System »), la plateforme de réservation du groupe hôtelier. Cette plateforme traite toutes les réservations des 5 600 hôtels du groupe et sur l’ensemble des canaux de distribution. Un composant logiciel de cette plateforme est particulièrement critique, c’est le moteur d’inventaire qui gère la disponibilité et les tarifs de l’ensemble des chambres des hôtels du groupe. Cela nécessite de partager énormément d’informations et de s’appuyer sur un moteur de disponibilité qui répond à chaque demande.

Thierry Lefort, vice-président engineering de D-Edge résume l’enjeu colossal lié à la migration de ce logiciel dans le Cloud : *« Le but était de quitter une infrastructure on-premise et d’aller sur AWS, un service dont la disponibilité est critique. Il s’agit d’une application déployée sur 220 serveurs, mobilisant 3 To de RAM et capable de répondre en moins de 100 ms à l’ensemble des requêtes. »*

De nombreuses équipes ont été mobilisées chez Accor et D-Edge pour mener ce projet, avec l’assistance d’Ippon technologies, un partenaire AWS certifié sur les processus de migration vers AWS.

Outre les aspects business et techniques, une contrainte forte existe : le projet doit être bouclé avant le 31 décembre, les licences logicielles sur site devant être renouvelées le 1er janvier.

Une migration de type Blue/Green est privilégiée

Damien Rollet, CTO de l’agence parisienne d’Ippon technologies et architecte Cloud participe au projet. Outre le « move to Cloud » de l’application, le projet était aussi l’occasion de la moderniser : *« Il fallait aussi gérer un contexte organisationnel avec des périmètres de responsabilité différents et s’inscrire dans le cadre du programme de migration Cloud Accor beaucoup plus large. »* Le projet est mené en appliquant le programme de migration MAP (« Migration Acceleration Program ») d’AWS, composé de plusieurs phases : l’« assessment », le « mobilize » et enfin le « migrate/modernize ». *« Cette méthodologie de migration donne un cadre et nous apporte des avantages, notamment le support des équipes AWS pour la migration »*, explique Damien Rollet. Et d’ajouter : *« Sur le planning initial, tout a changé... sauf la date de fin que nous sommes parvenus à tenir, ce qui est un énorme succès pour Accor. Cela a nécessité un gros engagement des équipes Ippon, D-Edge et Accor. »*

Lors de l’assessment, l’équipe va réfléchir à l’architecture cible et aux services managés AWS qui seront mis en œuvre pour remplacer les logiciels sur site et à une manière de migrer pour exclure tout risque de rupture de service et de problèmes de production une fois l’application migrée.

L'équipe veut disposer de la capacité de fonctionner en double flux et pouvoir mener une migration progressive hôtel par hôtel, et opérer un roll-back totalement transparent pour les hôtels. « *Un élément clé de succès était d'élaborer un business case qui puisse convaincre la direction générale de lancer cette migration* » explique Thierry Lefort. « *Si le service tombe, Accor ne peut plus prendre de réservations du tout, ce qui représente 250 000 réservations et 50 millions de chiffre d'affaires par jour !* »
Autant dire qu'une migration en mode big bang n'est pas envisageable.
Le mode de migration choisi est de type « blue/green », avec deux environnements en parallèle : l'environnement sur site d'un côté (blue) et l'environnement cible sur AWS de l'autre (green).
L'équipe garde la capacité de basculer son application de l'un à l'autre en fonction des tests à mener, jusqu'au moment où l'environnement blue est arrêté. Ainsi, le moteur de disponibilité de TARS va fonctionner en « double run » pendant près de quatre mois, le temps de préparer sereinement la migration. « *Nous avons fait des allers/retours de l'une à l'autre pour assurer le fine tuning de la plateforme* », explique Thierry Lefort. « *C'est une approche que nous avons pu défendre auprès de notre direction et expliquer que c'est en procédant comme cela que nous aurions une migration sans arrêt de service* », précise-t-il.

La priorité : automatiser les opérations

La procédure de roll-back transparente a permis aux équipes qui arrivaient le matin à 9h de basculer 100 hôtels sur AWS, réaliser un fine tuning sur cet échantillon , puis opérer un roll-back à 17h pour basculer sur le on-premise pendant la nuit, etc. « *Nous avons travaillé dans ce mode pendant pratiquement deux mois. Si nous n'avions pas adopté cette démarche et tenté une telle migration en big bang, nous nous serions retrouvés en incident de production dès le jour 1 !* », insiste le vice-président engineering de D-Edge. En termes de modernisation, l'application qui mettait en œuvre un cluster Cassandra à basculé sur le service managé Amazon Keyspaces. « *Nous avons pu bénéficier du support d'AWS sur le tuning et valider que cela allait bien fonctionner. Nous avons aussi travaillé sur l'optimisation des tables de données. Un monitoring a été mis en place dès le début* », détaille Damien Rollet.
C'est bien évidemment le passage des machines virtuelles aux conteneurs sous AWS Fargate qui a représenté la plus grosse évolution et a obligé à réfléchir sur l'organisation à mettre en place pour opérer la plateforme. « *On ne travaille pas de la même manière dans le Cloud. Le rôle des équipes évolue. Il faut donc réfléchir à l'aspect organisationnel pour construire une trajectoire d'un état initial au démarrage du projet à l'état cible, une fois l'application migrée* » argumente Thierry Lefort. Une migration blue/green implique un haut niveau d'automatisation et un meilleur partage des responsabilités entre infrastructure et développement que par le passé.
« *La partie Dev est maintenant totalement autonome pour réaliser ses déploiements sous le contrôle de l'infra. Chacun a ses scripts Terraform. Avant, une mise en production pouvait prendre de 3 heures à 3 jours. Aujourd'hui, cela se fait en un clic. Nous avons énormément gagné en tranquillité et en autonomie* », précise Thierry Lefort.

La maîtrise des coûts du Cloud

Alors que l'infrastructure sur site présentait des coûts d'infrastructures fixes et un « capacity planning » établi à l'avance, l'équipe D-Edge doit désormais gérer les coûts variables d'AWS. « *L'avantage de fonctionner en blue/green est de pouvoir tester les optimisations et d'avoir droit à l'erreur. Nous avons ainsi pu passer d'un usage de 3,4 To de mémoire à 2,6 To en migrant vers AWS* », assure-t-il. Son équipe a gagné en agilité et mené des optimisations qu'il n'était pas possible de mener sur une infrastructure sur site. « *Le monitoring permet de traquer finement le fonctionnement de l'application, mieux comprendre ce qui se passe en production et optimiser la plateforme. Cela permet de se projeter et d'évaluer l'impact d'une modification en termes de coût.* »
Cette agilité et cette capacité d'optimisation ont permis de tenir le budget pendant que les coûts sur site s'envolaient du fait de l'inflation... En optant pour une migration de type blue/green, D-Edge a opté pour la solution la plus sûre, ce qui n'a pas empêché les équipes de tenir la deadline initiale. L'ensemble des flux ont basculés sur la nouvelle infrastructure fin novembre 2023 et jamais l'équipe n'a pu opérer de retour en arrière. L'infrastructure sur site devait être maintenue en l'état jusqu'à fin décembre 2024, en cas de problème. Elle a finalement pu être décommissionnée en début d'année et les licences sur site n'ont pas été renouvelées. ■ *Par Alain Clapaud*

220

C'est le nombre de serveurs sur lesquels la plateforme de réservation TARS est déployée.

HP ADHÈRE AVEC MODÉRATION AU CONCEPT DU PC COPILOT+

HP lance ses premiers PC Copilot+, mais les met en avant sous une marque spécifique et pousse ses propres services IA.

NE DITES PAS « Copilot+ PC », mais « next-gen AI PC » ? HP tient à cette distinction. Microsoft est à l'origine du label Copilot+ PC. Le cahier des charges associé impose trois grandes spécifications techniques minimales : 16 Go de RAM, 256 Go de disque et un NPU délivrant 40 TOPS (milliers de milliards d'opérations par seconde). Ces critères *« vont forcément évoluer »*, estime HP. Une raison de privilégier l'appellation next-gen AI PC, que d'autres constructeurs ont d'ailleurs adoptée.

HP veut détacher l'étiquette Copilot...

Là n'est pas le seul motif. HP compte aussi démontrer que « l'IA, ça n'est pas [que] Copilot »... Et développe effectivement ses propres services. En vitrine : AI Companion. Cette boîte à outils apporte, pour le moment, une assistance à la recherche en langage naturel, à l'analyse et à la synthèse de documents (pdf, txt, docx), à la composition de texte et à l'optimisation des performances*. HP va précharger AI Companion sur certaines machines. Il le diffuse aussi par l'intermédiaire du Microsoft Store. Dans tous les cas, il est nécessaire d'avoir un next-gen AI PC. Officiellement, cela ne marchera pas avec « AI PC » tout court, c'est-à-dire avec les ordinateurs disposant d'un NPU à moins de 40 TOPS.

L'EliteBook 1040 G11 en fait partie. Récemment ajouté au catalogue, ce 14 pouces Intel est disponible aux formats coque et convertible. Châssis magnésium pour le premier, alu pour le deuxième, avec dans les deux cas 90 % de matériaux recyclés. Le clavier en comporte aussi. En l'occurrence, des filets de pêche. HP a aussi intégré de l'huile de cuisson dans la fabrication de certains PC. Il affirme réfléchir à utiliser, entre autres, des algues marines, du polystyrène et de la fast fashion.

4,5 M

C'est le nombre de PC que HP devrait vendre cette année en France.

19 %

C'est la part des PC compatibles IA parmi les expéditions totales de PC en 2024, selon Statista.

À défaut d'AI Companion et de ses fonctionnalités génératives, l'EliteBook 1040 G11 et les autres « AI PC » embarquent des technologies qui tirent parti de leur NPU. Elles ont essentiellement trait à l'optimisation audio-vidéo : suppression du bruit de fond, captation dynamique, cadrage automatique, etc. En toile de fond, l'acquisition de Polycom, qui se manifeste d'ailleurs en l'objet de Poly Camera Pro, console permettant de régler les paramètres pour tous les logiciels de visio.

... et pousser AI Companion

HP n'a pas la même latitude pour intégrer ses services sur les Chromebooks : *« Google garde la main sur l'image [...]. Même sur le design. »* Il ne faut, plus globalement, pas s'attendre à une communication spécifique au sujet de la marque Chromebook Plus (forme de pendant des PC Copilot+). Reflet d'un marché *« très petit en France »* : sur les 4,5 millions de PC que HP pense vendre cette année en France, moins de 100 000 devraient être des Chromebooks. Il n'en a pas dans son catalogue pro et sur la partie grand public, *« c'est moins de 5 % des ventes »*. Le segment *« est encore en plus grande décroissance que le reste de l'environnement PC »*.

Le format 17 pouces a plus de succès en France. En tout cas sur le segment grand public (25 % des ventes) et les grandes diagonales sont en croissance, même sur le premium. *« Une force, puisque Apple, sur le 16 pouces, est [sur] des prix très élevés »*, veut croire HP.

Hors stations de travail, 30 % des ventes en France sont des PC de bureau. Sur les workstations, le mobile, dominant lors de la période Covid, est repassé derrière le desktop (55/45). HP évoque *« une raison évidente de puissance »*... et ne manque pas de rappeler avoir lancé son logiciel AI Studio destiné à collaborer sur la création de LLM. ■

Par Clément Bohic

* Certaines fonctionnalités ne sont pas totalement locales. Interrogé, HP ne donne aucune précision.

16 POUCES, 16 : 10

Pourquoi choisir le nouveau standard de l'industrie

Avec son Lenovo ThinkPad E16 Gen 1, et contrairement au reste du marché, Lenovo propose dès le début de sa gamme ThinkPad des écrans en 16 : 10. Moins d'encombrement, plus d'affichage. Alexandre Dimitrov, Responsable Informatique chez Midas France, a accepté de passer au peigne fin ce changement en testant la version AMD.

Alexandre Dimitrov
Responsable Informatique chez Midas France

Yann Noël
AMD Client Technologist chez Lenovo

Révolution de la résolution : c'est quoi le 16 : 10 ?

« La taille de l'écran est le premier atout qui saute aux yeux à l'ouverture du produit », s'exclame Alexandre Dimitrov, dès les premiers échanges sur ce nouvel appareil. Ce dernier affiche 16 pouces, et se distingue surtout par un dimensionnement en 16 : 10, alors que le format 16 : 9 est un standard établi depuis de longues années. Une singularité visiblement appréciée. *« You see what you get »*, résume-t-il, en décrivant un écran plus confortable à travailler, notamment pour l'utilisation de certains outils métiers qui demandent une résolution minimale. *« En format 16 : 10, j'ai l'impression d'avoir mon vrai outil, alors que le format classique a tendance à écraser le texte. On est sur du pro pour du pro »*, se réjouit-il. Lenovo est le premier acteur à proposer cette innovation avec l'objectif de la rendre facilement accessible.

« Prendre soin du confort visuel était l'un de nos premiers souhaits, au moment de la conception », explique Yann Noël, AMD Client Technologist chez Lenovo. Dans le cas de l'utilisation d'un tableur, cette innovation permet d'afficher quelques colonnes et quelques lignes supplémentaires par exemple, sans nécessité de recourir aux barres de défilement. *« C'est également le cas pour certains logiciels métiers que nous utilisons, qui nécessitent une résolution minimale. Plus l'écran est grand, plus les informations affichées sont visibles. Il en va de même pour la messagerie ou le nombre de lignes de mails lisibles sur un même écran est plus important. Le premier gain concerne donc surtout un confort d'utilisation et une efficacité améliorée sur un plan bureautique »*, ajoute Alexandre Dimitrov.

À noter par ailleurs que le rendu visuel avec un format 16 : 10 est plus conforme et adapté à la restitution d'éléments visuels imprimés sur papier. Sur un dimensionnement en 16 : 9, les textes peuvent apparaître légèrement plus écrasés, ce qui peut poser quelques difficultés. *« Le passage du 16/9 au 16/10, entre le Lenovo ThinkPad E15 et le ThinkPad E16, permet de gagner 11 % de surface d'écran supplémentaire »*, précise Yann Noël. L'écran occupe davantage d'espace par rapport à l'ensemble du matériel, comme en témoigne le STBR (Screen To Body Ratio) qui s'élève à 91,2 %, contre 85 % précédemment. Cependant, cet ordinateur portable est plus fin, plus léger et moins large que ces prédécesseurs. ■

Pour en savoir plus, téléchargez notre livre blanc

LA XDR PEUT-ELLE REMPLACER LES SIEM DANS LES SOC ?

La technologie XDR peut-elle démoder les SIEM au cœur des grands SOC ? Plus qu'un remplacement, la XDR pointe les insuffisances du SIEM actuel et pousse les éditeurs à le réinventer. Avant une convergence des solutions.

L'ACQUISITION de Splunk par Cisco pour 28 milliards de dollars en 2023 a mis un coup de projecteur sur une brique indispensable aux SOC de toutes les grandes entreprises : le SIEM (système de gestion des événements et des informations de sécurité). La solution collecte et centralise les logs du système d'information et permet aux analystes de traiter les incidents de sécurité. Technologie mature, le SIEM est aujourd'hui arrivé à son plateau de développement. IBM a vendu sa solution QRadar à Palo Alto Networks, Logpoint a été repris par un fonds, et LogRhythm et Exabeam sont en cours de fusion.

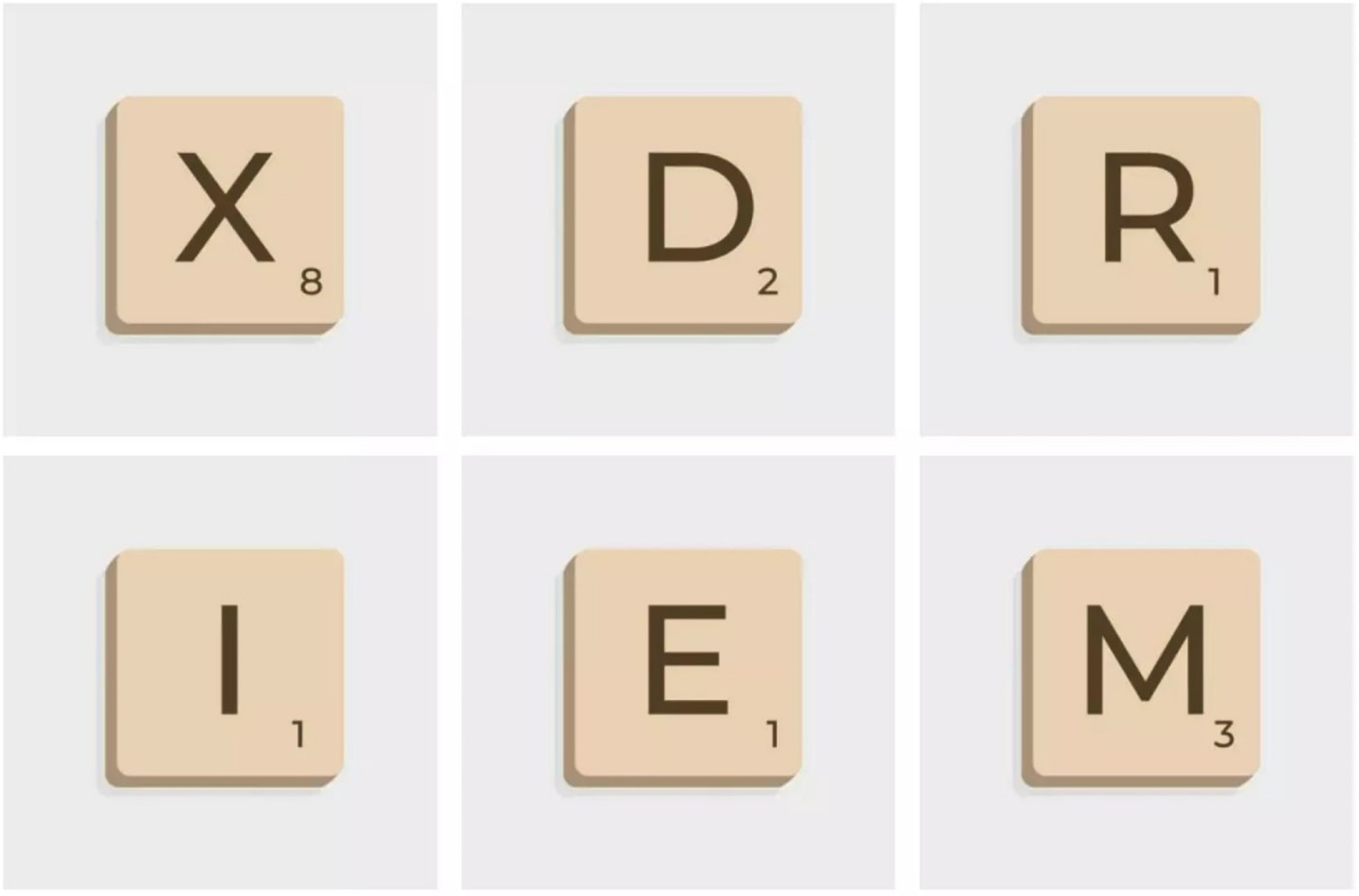
La XDR monte en puissance dans les SOC

Avec une croissance de 20 à 38 % par an selon les analystes, la XDR (détection et réponse étendues) s'impose dans les centres d'opérations de sécurité (SOC). Pour autant, cette nouvelle approche en temps réel peut-elle remplacer son ainée ? Rien n'est moins sûr. Flavien Vivier, Senior Solutions Engineer France chez SentinelOne souligne que beaucoup d'entreprises sont encore en phase d'observation et évaluent encore le rôle que peut avoir la XDR par rapport au SIEM : *« L'énorme inconvénient du SIEM reste son coût et le fait qu'il s'agit d'une boîte vide qu'il faut personnaliser avec des compétences internes. »* À l'inverse, il estime que les solutions EDR (détection et réponse des terminaux) déjà en place accumulent déjà des volumes de données importants pour constituer des règles de protection et facilitent ce passage vers la XDR. *« La XDR est une évolution naturelle de l'EDR et nous poussons pour la démocratiser en apportant plus de sources. Il faut être capable de répondre à des questions pour établir le début de l'attaque, ses cibles, mais aussi sur les autres signaux détectés par les endpoints qui auraient dû mettre en garde l'entreprise. »*

XDR et SIEM sont complémentaires

Matthias Maier, EMEA Cybersecurity Market Advisor chez Splunk ajoute : *« Les solutions XDR et SIEM sont tout à fait complémentaires. À première vue, les solutions XDR intègrent plusieurs fonctionnalités de type TDIR (détection des menaces et réponse aux incidents), en particulier en matière de détection et de réponse (qui est le point fort d'une solution XDR). Les solutions XDR et SIEM sont très complémentaires pour les*

> *Les technologies SIEM ne sont pas conçues pour répondre à une alerte dans un délai restreint comme l'imposent les nouvelles réglementations. »*
>
> ***Freddy Milesi, fondateur et PDG de Sekoia.***



grandes organisations dotées d'un SOC mature, car elles peuvent aider à établir une approche plus efficace et stratifiée pour renforcer la posture de cybersécurité. »

Luis Delabarre, Group SOC Director chez Nomios, (un opérateur de SOC managés), estime que du point de vue technologique, l'idéal est de combiner SIEM et XDR : « *La XDR permettra d'apporter ses capacités de détection en temps réel, faire ce que l'on appelle du "data stitching" et corréler différentes sources d'information. Disposer d'un SIEM à côté permettra de faire de la traque de menaces sur du temps long. Les deux approches vont converger et c'est notamment ce que fera j'imagine Cisco avec le rachat de Splunk.* »

Sur la convergence en cours chez les éditeurs, Freddy Milesi, fondateur et PDG de Sekoia est plus tranché : « *Dans ce débat entre XDR et SIEM, notre approche a été de plateformiser et transformer la XDR en simple cas d'usage. Nous mettons à disposition des cas d'usage qui étaient jusqu'à présent portés par les SIEM comme l'investigation, le machine learning, le reporting et l'automatisation des processus répétitifs. Les technologies SIEM ne sont pas conçues pour répondre à une alerte dans un délai restreint comme l'imposent les nouvelles réglementations. En cela, les SIEM vont devenir caduques.* » Selon lui, toutes les fusions/acquisitions que connaissent aujourd'hui les éditeurs de SIEM « legacy » ne sont que la preuve de la fin d'un monde. Une divergence de vues entre les anciens et les modernes. ■

Par Alain Clapaud

28 Mds $

C'est le prix d'acquisition de Splunk par Cisco en 2023.

Éclairage marché

Matthias Maier, EMEA Cybersecurity Market Advisor chez Splunk

Un besoin de complémentarité

« Une solution XDR complète un SOC avec une télémétrie "high-fidelity", car elle accélère les investigations et la réponse en pré-analysant une télémétrie spécifique qui n'est pas envoyée au SIEM. Certains de nos clients ont déjà intégré leur solution XDR à Splunk. XDR aide à éliminer certains des problèmes auxquels les analystes de bruit ("noise analysts") sont souvent confrontés, et Splunk donne aux équipes la capacité de traiter les scénarios d'utilisation au-delà du terminal. C'est une situation gagnant-gagnant. »

“Nous achevons la migration de nos VM et de nos conteneurs applicatifs dans le Cloud”

Christophe Charbonnier, DSI de MPSA

Christophe Charbonnier, DSI de MPSA, retrace les évolutions de son système d’information aux défis de la logistique, du négoce de pneus et de pièces techniques automobiles avec les garagistes.

Créé en 1908 à Cannes, le groupe familial MPSA distribue 3,5 millions de pneumatiques par an, soit près de 12 % du marché français, ainsi qu’une large gamme d’accesoires automobiles via le réseau Avatacar.com qui compte 1 500 garages partenaires. Il réalise un chiffre d’affaires de 270 millions d’euros avec un effectif de 350 salariés. Son directeur des systèmes d’information (DSI), Christophe Charbonnier, revient sur ses choix technologiques – dont le Cloud hybride et le réseau SD-WAN – et les résultats obtenus.

Quelle est l’évolution principale du métier de DSI au niveau de l’organisation ?

Avec le Web, puis le Cloud, les responsabilités des partenaires IT évoluent. L’externalisation d’infrastructures et de services devient la règle. La mise en place de réseaux exigeait autrefois plus de travail à mesure que le nombre d’agences à connecter augmentait. Ce n’est plus le cas à présent. La DSI peut se consacrer pleinement aux projets business. Je travaille beaucoup avec les métiers, en phase avec la direction. Nous

partageons avec le directeur général, Cédric Massa, des idées sur les transformations numériques à mener, puis dressons une stratégie. Ensuite, je priorise les projets pour mettre en œuvre cette stratégie.

Quels projets pilotez-vous actuellement ?

Côté infrastructure, nous avions deux hébergeurs régionaux (Koesio Noeva et Monaco Telecom) et basculons vers le Cloud AWS en mode VMware, pour rationaliser nos traitements externalisés. Orange nous accompagne dans cette migration Cloud. Nous disposons encore d'une quinzaine de sites connectés en MPLS que nous allons regrouper derrière un réseau SD-WAN. En 2024, il nous faut amener de la cybersécurité partout ; l'approche « zero trust » devient incontournable. Et nous démarrons la transformation de nos services Web éligibles vers des applications Cloud natives, de sorte à pouvoir équilibrer les workloads sur plusieurs centres de données.

L'IA figure-t-elle à votre agenda ? Comment préparez-vous votre système d'information ?

Dans ce domaine, les applications de logistique devraient être servies en premier. Une prédiction optimale des ventes, à partir d'un datalake, pourrait nous aider à déterminer un stock type par saison, à le mettre en place pour mieux servir 13 000 comptes clients aux profils distincts, tout en affinant nos tarifs. Actuellement nous stockons environ 600 000 pneus sur 5 000 références, toutes marques confondues. Plutôt que de foncer vers les IA génératives souvent biaisées, j'envisage la mise en œuvre du machine learning au service du négoce de pneus. Par ailleurs, pour soutenir notre expansion internationale, l'IA pourra nous aider à automatiser la collecte de fiches marketing et d'argumentaires commerciaux, ce qui optimisera notre position sur les moteurs de recherche.
Mes techniciens évaluent l'apport de l'IA au développement, lors des revues de codes. Les administrateurs s'y penchent aussi, mais je leur recommande la plus grande prudence lorsqu'on ignore la politique d'alimentation des données. Au CIP Med, dont je suis le vice-président, nos réflexions sur le low code et l'IA nous amènent à constater l'ampleur des changements en cours, et la nécessité de partir sur de bonnes données.
Du code plus simple à créer et des infrastructures externalisées procurent l'opportunité de nous rapprocher davantage des métiers. Mais le risque de shadow IT augmente avec des bouts d'IA et de low code assemblés par des stagiaires durant l'été, encouragés par les métiers. On ne va pas manquer de travail à la rentrée ! C'est inévitable.

De nouvelles compétences doivent-elles rejoindre votre équipe ?

On s'acculture aux hyperscalers AWS et Azure, à leur scalabilité. À mesure que nous montons en compétences sur le Cloud, FinOps compris, je note que notre informatique devient plus attractive. Nous attirons de jeunes talents de Sophia-Antipolis, prêts à s'atteler à la création de « tenants » (NDLR : nuages privés pour stocker les données des locataires). En outre, nos premières migrations vont retirer des freins à l'émergence de l'IA et à d'autres services évolués. Elles encouragent l'optimisation de notre chaîne CI/CD et de nos pratiques DevOps, alors que je prévoyais de les faire progresser avant de migrer vers le Cloud.
J'évalue à deux ans le délai requis pour maîtriser l'écosystème d'un acteur comme AWS ; il y a bien une courbe d'apprentissage. Depuis notre choix de migrer notre bureautique sous Office 365, nous sommes déjà en multi-Cloud.
Les containers d'AWS et l'IA vont nous conduire vers davantage de Clouds hybrides. Mais nous devons veiller aussi à ne pas laisser sur le bord de la route des informaticiens expérimentés sur des technologies plus anciennes.

Comment parvenez-vous à rendre les garagistes moins hermétiques au numérique ?

Depuis 2020, notre socle Cloud hybride soutient les échanges numériques d'un réseau de 13 000 garagistes, dont 1 500 partenaires monteurs et près de 300 franchisés.
Notre rôle consiste à aider les mécaniciens réparateurs automobiles à se numériser. Ces dépanneurs de proximité sont appréciés pour leurs compétences et leur sens du service, mais le numérique les rebute parfois encore.
Grâce à notre Webapp, fonctionnelle sur mobile comme sur desktop, ils peuvent suivre toute la prestation commandée en ligne par le client final. Ils disposent d'une gestion d'agenda et reçoivent une notification de rendez-vous lorsqu'un devis est accepté. Des photos captées par un simple smartphone peuvent aider le garagiste à vérifier l'état du véhicule. De plus, il obtient une liste de points de contrôle facilitant le suivi de leurs prestations et fournit toutes les données utiles au back-office jusqu'à la restitution du véhicule au client. ■ *Propos recueillis par Olivier Bouzereau*

22
collaborateurs composent la DSI renforcée par quelques alternants.

STRATÉGIE NUMÉRIQUE DE L'ÉTAT : LE "DOIT (VRAIMENT) MIEUX FAIRE" DE LA COUR DES COMPTES

La Cour des comptes estime que la Direction interministérielle du numérique (Dinum) doit encore construire sa légitimité. Elle critique autant ses réalisations que son positionnement sur les nouveaux enjeux du numérique.

QU'EST-CE QUI accusait un coût total de 15 millions d'euros minimum fin 2023, pour moins de 200 000 utilisateurs ? Une réponse possible : la « Suite numérique de l'agent public ». Offre peu lisible, inclusion insuffisante des destinataires, risque d'arrêt à défaut d'une diffusion plus massive de la brique d'authentification unique (SSO)... Ce projet de suite collaborative interministérielle – qu'il est question de décliner auprès des collectivités territoriales – n'emporte pas l'adhésion de la Cour des comptes, qui met en doute la plus-value des produits numériques interministériels et souligne l'arrêt de certains d'entre eux malgré des investissements importants. Entre autres, geo.data.gouv et MonFranceConnect (1,2 million d'euros chacun).

En toile de fond, un constat : la légitimité de la Direction interministérielle du numérique (Dinum) reste à construire. La contribution du numérique au redressement des finances publiques en est une autre facette. En la matière, il n'y a toujours pas de consolidation au niveau de l'État. Et ce, malgré de multiples alertes depuis 2016 (la Cour des comptes avait notamment proposé que la Dinsic ait accès à Chorus).

La nouvelle feuille de route de la Dinum n'a pas retenu l'objectif d'une optimisation des dépenses publiques grâce au numérique. C'était l'une des boussoles du programme « TECH.GOUV », arrêté en 2022. La Direction du budget a néanmoins récemment amorcé un travail de consolidation. La Cour des comptes le juge d'autant plus nécessaire que les dérives budgétaires des grands projets numériques demeurent importantes. En juin 2023, le taux moyen s'élevait à 16,7 % (pour 23,8 % de taux de dérive calendaire).

La légitimité par un exercice plus effectif des pouvoirs...

La loi définit comme « grands projets » ceux dont le coût complet dépasse 9 millions d'euros. Elle les soumet à une procédure d'avis conforme auprès de la Dinum. Avec huit agents, le pôle qui met en œuvre cette procédure n'est pas assez doté, estime la Cour des comptes. Surtout, la Dinum semble incapable de se saisir pleinement du pouvoir qui lui est conféré. Quand bien même elle émet quasi systématiquement des recommandations et assez régulièrement des réserves, la proportion d'avis défavorables apparaît faible.

La procédure en elle-même est lourde, sans modèle adapté à la taille des projets. Et les ▶▶▶

15 M€

C'est le coût du développement de la « Suite numérique », fin 2023, pour moins de 200 000 utilisateurs.

salon des maires et des collectivités locales

ACCÉLÉRATION.

+50 000 visiteurs

1 300 exposants

400 prises de parole

PRIX DE L'INNOVATION TERRITORIALE avec 8 catégories de prix

9 secteurs d'exposition

2 salons tenus conjointement

ENVIE DE RENCONTRER LES ACTEURS DU TERRITOIRE EN PARTICIPANT AU SALON DES MAIRES ET DES COLLECTIVITÉS ?

Événement majeur pour les décideurs territoriaux, le salon éclaire les territoires autour des enjeux auxquels ils sont confrontés. C'est un espace de rencontres, d'échanges et de partage qui propose des solutions adaptées aux besoins de chacun.

PRÉSENTEZ VOS SOLUTIONS AU SEIN DU SECTEUR NUMÉRIQUE & CONNECTIVITÉ !

RÉSEAUX ET INFRASTRUCTURES TÉLÉCOMMUNICATIONS | MATÉRIEL ET ÉQUIPEMENTS IT, RECONDITIONNEMENT SYSTÈMES CONNECTÉS ET INFRASTRUCTURES INTELLIGENTES, IOT | ÉNERGIE & CLIMAT | DÉMATÉRIALISATION, ADMINISTRATION ÉLECTRONIQUE, GUICHET NUMÉRIQUE | GESTION, UTILISATION ET PARTAGE DES DONNÉES OUTILS DE CONCERTATION ET CONSULTATION CITOYENNE | CYBER SÉCURITÉ, SYSTÈMES DE PROTECTION, STOCKAGE | CONSEIL ET STRATÉGIE NUMÉRIQUES | MODÉLISATION ET RÉALITÉ VIRTUELLE

19-21 NOVEMBRE 2024
Paris – Porte de Versailles

Plus de détails
en scannant ce QR code

Tenue conjointe avec SALON DES SPORTS | SALON DE LA BIODIVERSITÉ ET DU GÉNIE ÉCOLOGIQUE

Organisé par infoprodigital | AMF

ministères ne comprennent pas toujours les recommandations formulées. Il leur arrive de faire remarquer qu'elles ne tiennent pas assez compte des enjeux liés à leurs métiers. Ou qu'elles portent sur des questions formelles (inscription dans la doctrine « Cloud au centre », recours à la méthode agile) plutôt que sur des questions de fond.

C'est sans compter les multiples voies de contournement. Les ministères ne notifient pas toujours les grands projets à la Dinum. Ou ils le font tardivement, parfois après publication des appels d'offre. Voire après le lancement du dispositif audité. Illustration avec la plateforme numérique nationale dédiée au dispositif expérimental du SAS (« service d'accès au soin »). Lorsque notifiée, elle était déjà en production dans 22 départements.

Autre écueil : les projets que portent les opérateurs de l'État n'entrent pas dans le champ de la procédure d'avis conforme. Or, ils représentent une part croissante des « grands projets ». En outre, les ministères confient parfois certains de leurs projets aux opérateurs, ce qui brouille la distinction. En témoigne la refonte du SI de gestion des aides à l'emploi du ministère du Travail.

... et par la prise en compte des nouveaux enjeux

La Dinum doit aussi, du point de vue de la Cour des comptes, construire sa légitimité sur de nouveaux enjeux comme l'IA, le numérique écoresponsable et l'évaluation de la dette technique des acteurs publics.

IA : mieux coordonner l'action publique

Sur le premier volet, les initiatives s'articulent trop faiblement avec les réalisations du « Lab IA », moteur de la nouvelle stratégie axée sur la réutilisation des données publiques plus que sur leur production. En première ligne, la coopération public-privé AllIAnce. Constituée en incubateur, elle doit porter l'expérimentation de la GenAI au sein du service public.

La Cour des comptes souligne, de manière plus générale, la nécessité d'une coordination de l'action publique quant aux recherches, expérimentations et déploiements. Elle prend pour exemple le modèle du coordonnateur national pour l'intelligence artificielle. Hébergé au sein de la Direction générale des entreprises (DGE), il est chargé de l'action de l'État en ce qui concerne l'IA du secteur privé.

13

C'est le nombre d'équivalents temps plein (ETP) pour gérer « Tchap », la messagerie chiffrée pour les agents de l'État.

La MINumEco, peu visible et d'une organisation complexe

Sur le deuxième volet, on avait franchi un cap en 2020 avec la création de la MINumEco (Mission interministérielle pour le numérique écoresponsable). Elle rassemble la Dinum, la Direction numérique du ministère de la Transition écologique et le Commissariat général au développement durable.

Sous son impulsion, des pilotes ont bien été identifiés, mais le taux d'actions réalisées reste très faible (1 sur 23). La MINumEco dispose encore de peu de visibilité et l'organisation est complexe entre les parties prenantes. Ce qui freine le déploiement et le suivi des actions. En parallèle, la nouvelle feuille de route de la Dinum ne fait pas du numérique responsable une priorité, alors que cet enjeu fait l'objet d'une circulaire de 2020.

Des occasions manquées sur la dette technique

Pour ce qui est de la dette technique, les coûts qu'elle engendre sont mal connus à ce jour. Bercy et les ministères chargés des affaires sociales ont commencé à prendre la question en compte, mais leurs actions restent très incomplètes.

En 2023, l'actualisation des plans de transformation numérique des ministères de la Justice et de l'Intérieur auraient pu être l'occasion d'intégrer la résorption de la dette technique. Ce ne fut pas le cas. La Cour des comptes perçoit un palliatif dans la migration des applications vers un Cloud souverain. Mais elle juge que la Dinum ne s'est pas positionnée comme pilote de ce chantier. ■

Par Clément Bohic

Learning Experience:

VOS CONSEILLERS DE VENTE DEVIENNENT DES KINGS

Les dispositifs de "*learning experience*" imaginés sur mesure pour nos clients décuplent la performance commerciale et relationnelle de vos conseillers de vente.

Basés sur des aventures formatives, interactives et immersives, ils mobilisent et impliquent vos équipes pour en révéler tout leur potentiel.

Et votre expérience client devient (grrrh) mémorable !

contact@sequoia.fr
sequoia.fr

SEQUOIA
Corporate is back!

LE CLOUD DE CONFIANCE À LA RECHERCHE DE SON SECOND SOUFFLE

Si la place de SecNumCloud dans le référentiel de sécurité européen EUCS reste encore à définir, la qualification décernée par l'ANSSI reste une référence pour les acteurs français du Cloud de confiance. Plusieurs fournisseurs se préparent à la certification de leurs services.

ALORS QUE L'ANSSI vient de publier ses recommandations* pour l'hébergement dans le Cloud des systèmes d'information sensibles, le marché du Cloud de confiance français se structure. Désormais tous les hyperscalers et Oracle disposent de datacenters en France et de structures pour garantir à leur client une certaine protection vis-à-vis des lois extraterritoriales américaines. Mais cette localisation est loin d'être suffisante pour assurer la confiance. « *Limiter la souveraineté à la localisation des données et au chiffrement n'est pas suffisant. On peut être localisé aux États-Unis et orchestrer un cluster Kubernetes en Europe, avoir tous ses administrateurs systèmes, administrateurs de bases de données et même les chargés de compte aux Etats-Unis* », estime estime Julien Levrard, CISO d'OVHcloud, en soulignant que les Clouds sont mondiaux, interconnectés, et l'endroit où se trouve physiquement la donnée n'a pas tellement d'importance.

La souveraineté ne se limite pas à la localisation

Pour l'heure, le véritable étalon de la souveraineté Cloud reste la qualification SecNumCloud de l'ANSSI. La liste des prestataires qualifiés compte Cloud Temple, OutScale, OOdrive, OVHcloud et Worldline. Ils ont été rejoints par quelques éditeurs verticaux, comme Index Education. La liste des prestataires en cours de qualification s'allonge et devrait croître encore ces prochains mois. En effet, la nouvelle vague des prestataires de confiance arrive. Les Bleu, S3ns et NumSpot visent à offrir des offres SecNumCloud à terme.

Porté par Thales, S3ns veut proposer une déclinaison souveraine de la Google Cloud Platform. Le 1er février dernier, il présentait sa première offre baptisée « Contrôles locaux ». La solution n'a pas vocation à être qualifiée SecNumCloud, puisqu'elle est très limitée : il ne s'agit que de garantir la localisation des données en France ou dans l'UE, assurer le chiffrement avec des clés maîtres détenues par le client et enfin assurer un support technique par les équipes S3ns. C'est bien au deuxième semestre que S3ns va véritablement lancer son offre IaaS et entrer dans la bataille du Cloud de confiance.

Créé par la Banque des territoires, Docaposte, Dassault Systèmes et Bouygues Télécom, NumSpot avance vite et bénéficie surtout de la qualification SecNumCloud de son partenaire OutScale. *« Nous nous appuyons sur les services IaaS qualifiés d'Outscale afin de proposer des services PaaS pour que ces usages du Cloud soient plus simples »*, résume Servane Augier, directrice Commerce et Marketing chez NumSpot. Lancée en février 2023 avec de l'hébergement de snapshots, de VM et des GPU, son offre s'est nettement étendue cet été : *« Nous avons ouvert cet été notre service OpenShift managé en beta, notre service Kubernetes et, depuis septembre, la base de données PostgreSQL en mode managé. Nous avons également lancé cet été notre service de stockage en mode objet S3, ainsi que notre IAM, un service de gestion des identités totalement unifié à travers notre portail »*, poursuit la responsable. Au-delà de cette grosse phase de lancement, NumSpot compte continuer à enrichir son catalogue PaaS.

Bleu, troisième acteur de cette nouvelle génération, a pris six mois de retard en attente du feu vert de l'autorité de la concurrence européenne. Coentreprise détenue à 50/50 par Capgemini et Orange, elle veut proposer aux entreprises et aux administrations une version souveraine de Microsoft Azure.

Bleu n'a pu être juridiquement formé que le 1er janvier 2024, mais le projet avance désormais rapidement. *« Sur la partie infrastructure, nous sommes prêts ! Nos deux datacenters sont en place et 10 000 serveurs ont été installés dans notre datacenter en région parisienne et dans le sud de la France, pour le second. Désormais, nous travaillons à la mise en place de la couche logicielle et le lancement de nos services s'effectuera en plusieurs temps »*, indique Jean Coumaros, CEO de Bleu.

Il faudra attendre la fin de l'année 2024 pour voir arriver les premiers services. Ceux-ci correspondront à la couche IaaS de Microsoft Azure. Mi-2025 devraient arriver la couche PaaS, ainsi que la suite collaborative Microsoft 365, et enfin la marketplace Bleu pour accéder à des solutions d'éditeurs tiers. Faire qualifier les processus et la plateforme Microsoft Azure hébergée par Bleu reste un défi. Un audit de code complet est impossible, mais Bleu prévoit des inspections dans les mises à jour fournies par Microsoft et un véritable audit de code sera mené sur le composant qui déploie ▶▶▶

Éclairage marché

Julien Levrard, CISO d'OVHCloud

Piloter une stratégie Cloud

« On explique aux DSI qu'ils ne doivent pas devenir des chefs de projet pour migrer chez AWS ou Azure. Placer des workloads chez l'un ou l'autre, c'est très bien, mais il faut piloter une stratégie Cloud dans la durée, c'est-à-dire maîtriser tous les types de Cloud, toutes les technologies, savoir migrer de l'un à l'autre et mettre tous ces acteurs en concurrence sur les appels d'offres, faire levier sur les prix. La souveraineté, c'est aussi former les DSI et les décideurs pour disposer de ces leviers pour ne pas s'enfermer dans une situation où ils pourront moins prendre de décisions par la suite. »

Éclairage marché

Servane Augier, directrice Commerce et Marketing chez NumSpot

Simplifier les usages

« Numspot a pour vocation de simplifier les usages du Cloud pour la transformation numérique des entreprises qui ont des données sensibles à protéger. Elles veulent passer dans le Cloud pour des raisons d'agilité, de "time to market" et de compétitivité, mais elle ne souhaitait pas le faire pour leurs données sensibles du fait des réglementations américaines qui ont un impact sur le territoire européen, de contraintes liées à leur marché comme la directive "Cloud au centre" pour le secteur public ou encore Dora, etc. Enfin, une des raisons les plus importantes, c'est la protection cyber et avoir la certitude que leurs données seront gérées avec le plus haut niveau de protection. Nous leur apportons une réponse Cloud avec la vocation d'être SecNumCloud sur l'ensemble du périmètre. »

1,2 Mds€

C'est le montant de la subvention de la Commission européenne pour le « projet important d'intérêt européen commun » (IPCEI) dédié au Cloud souverain, lancé en décembre 2023.

▶▶▶ ces mises à jour, une démarche transparente vis-à-vis de l'ANSSI.

Des offres souveraines qui gagnent en maturité

En parallèle, les acteurs souverains en place ne restent pas l'arme au pied. Ainsi, Cloud Temple joue à la fois la carte d'une offre IaaS SecNumCloud et l'interopérabilité avec Microsoft Azure et AWS. Cet outsider a décroché la qualification SecNumCloud de son offre OpenShift, comme l'explique Nicolas Dufour, directeur du développement et de la stratégie de Cloud Temple : *« En juin, nous avons qualifié notre PaaS OpenShift qui est non seulement un orchestrateur de conteneurs, mais surtout un socle qui va permettre de déployer toute une série de services qui pourront être consommés par nos clients pour accélérer leur transformation numérique. Nous avons aussi le stockage objet S3 qui est très attendu par nos clients, et qui est utilisé dans de nombreux cas d'usage. »* Le responsable estime que la feuille de route actuellement appliquée par le CSP va lui permettre de passer un nouveau cap en termes de nombre de services.

Tout semble se mettre en place pour que le marché du Cloud de confiance accélère au deuxième semestre et en 2025. Reste à voir quel sera l'impact du futur schéma de certification européen sur ce bel élan. ■

Par Alain Clapaud

* Un document qui recommande le référentiel SecNumCloud pour les applications traitant des données à diffusion restreinte, les SI sensibles relevant de la doctrine Cloud au centre de l'État, ceux des opérateurs d'importance vitale (OIV) et des systèmes d'information d'importance vitale (SIIV).

Témoignage

Sébastien Marie, CTO de Matmut

Concilier les enjeux data et IT

« La refonte de notre infrastructure data est un élément structurant de notre système d'information. Nous devions concilier la vue des data scientists très open source et nos enjeux de la production informatique. Ce mariage un peu difficile s'est vu compliqué par la régulation interne, qui nous a interdit certaines voies technologiques. Nous avons regardé avec attention l'offre S3ns car elle nous a permis de répondre à la fois à l'accès à un catalogue Google assez riche, qui sied à nos data scientists, l'accès à un Cloud industriel, qui sied à nos contraintes d'exploitation et de production, et la construction de S3ns qui sied à nos juristes. Forts de ce triptyque, nous avons considéré l'offre "Contrôles locaux" pour commencer la construction de notre écosystème de data science et nous nous intéressons à la trajectoire Cloud de confiance de S3ns, car cela ouvrira des perspectives d'utilisation plus vastes et la consommation de services novateurs, notamment de IaaS. »

« Nous travaillons à la mise en place de la couche logicielle et le lancement de nos services s'effectuera en plusieurs temps. »

Jean Coumaros, CEO de Bleu.

big youth

Accompagner les marques dans la création *d'expériences e-commerce désirables.*

Contactez-nous

bigyouth.fr — *01 80 05 99 10*

Eres

Sublimer
une maison de luxe par son minimalisme.

Sarenza

Affirmer
l'identité lifestyle d'un pure player du fashion retail.

Nature & Découvertes

Infuser
l'expérience magasin dans le parcours e-commerce.

Picard

Proposer
une expérience de marque omnicanale augmentée.

Caravane

Repenser
la décoration

Bulgari

OÙ EN EST LA CYBER "MADE IN FRANCE" ?

Alors que la question de la souveraineté des solutions Cloud est de plus en plus mise sur la table, qu'en est-il des solutions cyber "Made in France" ? Si l'offre est riche et souvent très en pointe, elle ne parvient pas à rivaliser avec les éditeurs américains...

LE CONSTAT DU RADAR

annuel Wavestone - Bpifrance des start-up cybersécurité françaises est particulièrement enthousiasmant pour 2024 : l'écosystème français compte 168 start-up et 42 scale-up. 11 sont notamment positionnées sur la sécurisation des modèles d'IA, une niche de marché potentiellement très porteuse. Si le montant des levées de fonds a chuté sur la période 2023/2024 avec 229 millions d'euros levés, il reste néanmoins élevé et les chiffres de la Banque de France montrent que le niveau d'activité des start-up françaises continue de croître fortement.

L'avis unanime des acteurs de la cybersécurité est de souligner le dynamisme de cet écosystème : « *On ne peut que noter le très haut niveau d'innovation de cet écosystème : il y a beaucoup d'idées nouvelles, beaucoup de jeunes entrepreneurs* », se félicite le vice-amiral d'escadre (2S) Arnaud Coustillière, président du Pôle d'excellence cyber. « *Ces entrepreneurs poussent pour créer des alternatives aux solutions israélo-américaines qui, même si elles sont performantes, posent un problème d'autonomie. Jusqu'à présent, ces entrepreneurs pouvaient lever de l'argent assez facilement. Aujourd'hui, c'est un peu plus délicat et certains sont en difficulté et doivent revenir aux fondamentaux, c'est-à-dire parfaire leurs offres.* » Il y a beaucoup d'innovations techniques, mais une difficulté à passer à l'échelle et à conquérir des marchés internationaux.

C'est assez différent pour les start-up israéliennes par exemple, chez qui le côté marketing et

« Il y a des entreprises européennes qui ont ce potentiel de passer à l'échelle. Néanmoins, le marché européen est très fragmenté et on ne peut pas aller aussi vite en rapidité d'exécution. »

Jean-Noël de Galzain, président d'Hexatrust.

commercial est davantage mis en avant. Jean-Noël de Galzain, président d'Hexatrust, le groupement de champions français et européens de la cyber et du Cloud de confiance déplore le flux sortant d'entreprises de technologies françaises qui continuent d'alimenter les entreprises américaines : *« Les sociétés françaises de la cyber continuent à se faire racheter et tant que l'on n'arrivera pas à mettre des outils de financement capables d'investir 50, 100 millions d'euros et plus dans une sale up, que ce soit en France ou au niveau européen, nos entreprises seront obligées d'aller chercher des fonds aux États-Unis et continuer à se faire racheter. »* Hexatrust compte aujourd'hui 135 membres qui réalisent un chiffre d'affaires de huit milliards d'euros et 18 000 emplois.

L'émergence d'un champion français se fait toujours attendre

« Sans évoquer Atos/Eviden, Thales ou Airbus seraient bien placés pour devenir les grands acteurs de la consolidation du marché français de la ▶▶▶

Éclairage marché

Freddy Milesi, fondateur et p-dg de Sekoia.io

Les atouts de la cyber Made in France

« Une caractéristique de l'écosystème cyber français, c'est la masse des nouveaux entrants : il y a toujours plus de nouveaux projets qui sont lancés dans les différents accélérateurs, le Cyber Booster, etc. D'autre part, les créateurs de start-up sont jeunes, ils ont la trentaine et vont pouvoir s'investir une dizaine d'années pour porter leur projet et scaler. Un second point est que les acteurs de notre génération commencent à être visibles en dehors de nos frontières. Les analystes tels que Gartner nous référencent en tant que champions technologiques. Des acteurs français commencent à être matures, sont présents à l'international et se confrontent à la compétition mondiale. Enfin, la volumétrie des commandes augmente. Les acteurs du CAC 40 et les grosses administrations nous testent sur de très gros projets. C'est en décrochant de gros contrats que nous atteindrons la taille critique. Le vrai critère de succès reste le montant des commandes. »

STRATÉGIE

« Il est absolument nécessaire que les DSI et les RSSI aient la capacité d'opter pour des solutions françaises ou européennes. »

Alain Bouillé, délégué général du Cesin.

Cybersécurité », estime Alain Bouillé, délégué général du Cesin, le club qui réunit tous les grands acheteurs de technologies cyber en France. *« Cela suppose une volonté des dirigeants de ces entreprises, mais aussi une volonté politique. Je suis un fervent défenseur de l'écosystème cyber français, car le fait d'être pieds et poings liés avec les éditeurs israélo-américains pose question. Quand on regarde la concentration des acteurs cyber à laquelle est en train de se livrer Thoma Bravo actuellement, ou encore ce qu'il est advenu de Symantec après le rachat par Broadcom, il est absolument nécessaire que les DSI et les RSSI aient la capacité d'opter pour des solutions françaises ou européennes. »* S'il se félicite de l'acquisition récente d'Imperva par Thales, les membres du Cesin attendent toujours la naissance d'un géant français ou européen de la cyber dont l'offre pourrait être comparable à celle de Cisco ou de Palo Alto Networks.

Pour le président d'Hexatrust, des futurs géants de la cyber sont déjà là : *« Plusieurs entreprises sont aujourd'hui au stade où Palo Alto a explosé il y a quelques années. Il y a des entreprises européennes qui ont ce potentiel de passer à l'échelle. Néanmoins, le marché européen est très fragmenté et on ne peut pas aller aussi vite en rapidité d'exécution. On a besoin de plus de temps et de plus de moyens pour y parvenir. »* Jean-Noël de Galzain souligne le besoin de pouvoir s'appuyer sur des fonds de plusieurs milliards pour porter la croissance des scale-up. *« Il existe par exemple le fond Tibi 1, créé en 2019, et qui a permis d'investir plus de 6 milliards d'euros sur la période 2020-2022. La phase 2, initiée en 2023, représentait un engagement de 7* milliards *de la part de ses investisseurs partenaires, mais aujourd'hui personne n'a encore vu son impact. »*

229 M€

C'est le montant des levées de fond réalisées par les start-up françaises du secteur de la cybersécurité en 2023/2024.

Open XDR, un exemple à suivre

S'il faut encore attendre la naissance de ces géants mondiaux de la cybersécurité en France, les start-up et scale-up françaises peuvent chasser en meute pour convaincre les entreprises de leur faire confiance. C'est notamment ce qu'a fait l'éditeur Sekoia en initiant en 2021 l'initiative Open XDR. Celle-ci fédère de nombreux éditeurs français apportant chacun une brique technologique à une XDR commune. Freddy Milesi, fondateur et p-dg de Sekoia.io raconte : *« Ce qui n'était qu'un projet en 2021 s'est transformé en réalité opérationnelle. L'important était de montrer qu'il existe une offre souveraine sur l'intégralité des sujets clés dans la sécurité opérationnelle. Il y a une vraie couverture des besoins des entreprises fournie par des acteurs français, mais ces acteurs savent aussi travailler ensemble. Tous nos directeurs techniques ont travaillé ensemble afin de rendre leurs produits interconnectés et interopérables. HarfangLab qui édite une EDR travaille avec Sekoia auprès d'une centaine de clients, et on a le même scénario avec des acteurs tels que Glimps, Gatewatcher, etc. »*

Comme aime le rappeler Jean-Noël de Galzain, avec la richesse de son écosystème cyber, la France peut jouer en Europe le rôle de vivier d'innovation qu'Israël joue pour les États-Unis depuis quelques décennies. ■

Par Alain Clapaud

Plus de start-up en France, mais moins de levées de fonds en 2024

Dans sa 6e édition, le Radar 2024 des start-up cybersécurité françaises de Wavestone, en partenariat avec Bpifrance, relève la création de 50 jeunes entreprises supplémentaires sur un an et des levées de fonds moins importantes. Wavestone souligne que 42 entreprises sont considérées comme des scale- up, plus matures sur leur modèle d'affaires et le niveau de revenus récurrents.

À noter, le nombre de liquidations qui a doublé (10 contre 5 en 2022/2023) illustre une tension accrue sur le marché. Signe de normalisation : le ralentissement du montant des levées de fonds en une année. Alors que la période 2022/2023 affichait un total de 341 millions d'euros, le montant s'affiche à 229 millions pour 2023/2024.

L'IA : un bouclier essentiel contre les attaques sophistiquées

Lors de la matinale Silicon du 4 juillet dernier, Yacine Drid, consultant en cybersécurité chez Bechtle Comsoft, a mis en lumière le rôle crucial de l'intelligence artificielle (IA) dans l'amélioration de l'efficacité opérationnelle des systèmes de sécurité.

Yacine Drid

Consultant en cybersécurité chez Bechtle Comsoft

L'IA, une réponse aux défis de cybersécurité

Les chiffres sont éloquents : 4 000 tentatives de vol de mots de passe par seconde et un temps moyen de 72 minutes pour accéder à des informations sensibles. Cette réalité souligne l'urgence d'une réponse robuste face à des menaces de plus en plus sophistiquées. De plus, une pénurie de 3,5 millions de professionnels de la cybersécurité aggrave la situation, rendant les entreprises vulnérables.

L'IA émerge comme une solution clé pour surmonter ces défis. En intégrant des technologies avancées comme «Copilot for Security» de Microsoft, les entreprises peuvent automatiser la détection des menaces et la réponse aux incidents. Cette solution, lancée en avril 2024, utilise l'IA pour améliorer les capacités d'analyse des équipes de sécurité, permettant une détection plus rapide des anomalies et une résolution proactive. Yacine Drid a souligné que cette automatisation est essentielle voire nécessaire pour compenser le manque de personnel spécialisé.

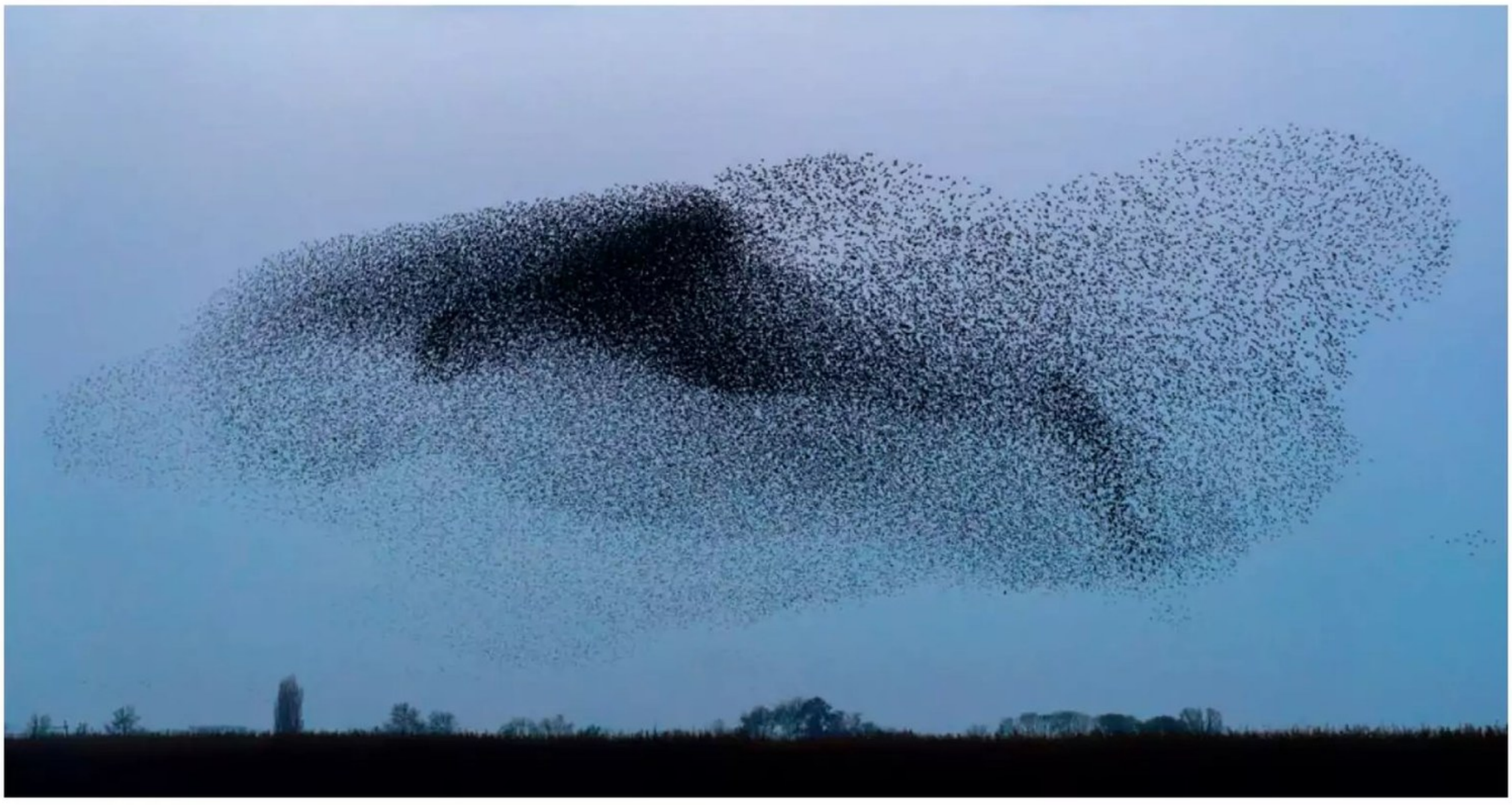
Une efficacité opérationnelle accrue grâce à l'IA

L'IA ne se contente pas de renforcer les défenses contre les cyberattaques, elle optimise également la gestion des identités et des endpoints (appareils de terminaison), qui sont des cibles courantes pour les cybercriminels. Selon Yacine Drid, les systèmes d'IA peuvent analyser en continu les comportements utilisateurs, détecter des accès suspects, et appliquer automatiquement des mesures de protection.

Par exemple, la fonctionnalité de «Communication Compliance» de Microsoft Purview utilise l'IA pour surveiller et filtrer les communications internes, détectant ainsi les tentatives de fuite de données. Ou encore, Microsoft Defender XDR permet une surveillance exhaustive des systèmes, assurant une couverture complète contre les menaces provenant de différents points d'entrée, y compris les emails, les identités, et les appareils. Cette approche centralisée simplifie la gestion de la sécurité et améliore l'efficacité opérationnelle.

Comme l'a résumé Yacine Drid, l'intelligence artificielle est désormais indispensable pour protéger les entreprises contre les cyberattaques sophistiquées. ■

bechtle



MIGRATION CLOUD : COMMENT FM LOGISTIC A DÉPLOYÉ SON INFRASTRUCTURE VMWARE

Le groupe de logistique français a mené un projet “move to Cloud” avec l’objectif de fermer, à court terme, son datacenter. La solution “VMware Cloud on AWS” a permis de déplacer ses serveurs virtuels tels quels, sans même devoir changer d’adresses IP.

PRÉSENT tout au long de la supply chain, FM Logistic propose une offre de services du type omnicanal. Avec des modes de livraison qui vont du 35 tonnes jusqu’au triporteur, en passant par les véhicules électriques, elle s’adresse à un panel de clients allant de l’industriel au client final, en passant l’hypermarché. *« La particularité de FM Logistic est d’être une entreprise familiale, avec une direction qui a une vision à long terme »*, explique Olivier Hamel, responsable Opérations du système d’information chez FM Logistic. Dès 2021, l’entreprise dévoilait son plan « Powering 2030 » qui doit l’amener à une neutralité carbone de ses installations d’ici 2030.

L’entreprise est présente dans douze pays et gère 4,8 millions de m² d’entreposage. Bien que l’IT ne constitue qu’une faible part de son empreinte carbone, elle a mis en place une stratégie de migration dans le Cloud. *« Pour toute nouvelle application ou solution existante qui doit évoluer, pour des raisons de montée de version ou obsolescence, nous nous posons la question si elle existe en SaaS. Si c’est le cas, on privilégie ce déploiement dans le Cloud. Si ce n’est pas possible, alors on va*

10 Gbit/s

C’est la puissance de la connexion entre le datacenter FM Logistic et AWS.

en on-premise », résume Olivier Hamel. L'objectif est de ne conserver en mode on-premise que les applications Edge, c'est-à-dire les applications qui contrôlent les robots et les engins automatiques guidés qui se déplacent dans les entrepôts. Celles-ci ont besoin de temps de latence très faibles, et il n'est techniquement pas possible de centraliser ces applications opérationnelles dans le Cloud, estime le responsable.

860 serveurs à migrer sur VMware Cloud on AWS

Reste au logisticien à « cloudifier » tout son existant. Le projet (nom de code « Iris ») vise à migrer le datacenter de FM Logistic, hébergé chez Equinix, vers les installations d'un acteur du Cloud. En parallèle, la direction voulait disposer d'un solide plan de remédiation en cas d'attaque cyber. *« Le RSSI fait tout ce qui est dans son pouvoir pour protéger le SI, mais que se passe-t-il le jour où l'on est attaqué ? Il fallait trouver une solution »,* détaille Olivier Hamel. La migration Cloud doit s'accompagner par la mise en place d'un solide DRP (« disaster recovery plan »). L'écosystème IT de FM Logistic repose alors essentiellement sur des progiciels métiers déployés sur des serveurs VMware. « *L'une des possibilités qui s'offraient à nous était de faire un "replatforming"* [migration d'applications]. *Or cela s'est avéré impossible. 96 % de nos applications sont des progiciels qui ne sont pas développés par nous. Nous dépendons des éditeurs et nous ne pouvons les forcer à aller vers du Cloud natif. De même, nous avions aussi une problématique avec des licences Oracle qu'on ne peut emmener n'importe où. Là encore, on ne peut forcer les éditeurs à délaisser Oracle pour aller vers PostgreSQL »,* précise Olivier Hamel.

Plusieurs autres défis doivent être relevés par la DSI. Celle-ci va devoir assurer les mêmes niveaux de service des applications aux directions métiers, car ce n'est pas du ressort du fournisseur Cloud de les assurer. Il va falloir assurer la montée en compétences des équipes, notamment celles qui seront en charge du volet MCO de la plateforme une fois le build achevé. De même, le chef du projet Iris doit résoudre une forte contrainte : « *Nous avions 860 serveurs à déplacer dans le Cloud, mais nous ne voulions pas changer toutes les adresses IP. En effet, changer l'adresse IP d'un serveur impliquait d'intervenir sur site pour modifier la configuration des terminaux radio des opérateurs, les montres connectées, etc. Le réseau est un point critique dans ce type de projet. Notre adressage réseau devait rester identique.* »

4,8 Mm²

C'est la surface d'entreposage de FM Logistic.

Un modèle « datacenter-less » achevé en septembre 2024

Déjà client de la Google Cloud Platform pour porter sa stratégie data, FM Logistic retient AWS pour son informatique de production. Son choix : migrer toute l'infrastructure VMware d'un bloc vers le service « VMware Cloud on AWS » opéré à la fois par VMware et AWS. La connexion du datacenter FM Logistic avec AWS est assurée en 10 Gbit/s en direct, avec un megaport Cloud router (MCR) et via un autre MCR placé chez Interxion. Deux zones de disponibilité AWS (AZ) sont mises en œuvre afin de porter les serveurs de production sur VMware Cloud on AWS SDDC, ainsi que l'infrastructure de secours. La migration du datacenter SSDC sur site vers le SDDC Cloud est alors menée avec la solution HCX de VMware. Pour autant, une fois la migration des VM menée et le projet Iris achevé, le travail des équipes d'Olivier Hamel ne s'arrête pas là. L'objectif reste bien d'aller vers un modèle « datacenter-less ». Il faut encore décommissionner tous les serveurs et équipements encore en production chez Equinix, notamment des serveurs HP-UX et les équipements NAS existants pour les placer sur AWS. De même que des équipements, tels les reverse proxy et toute l'infrastructure réseau SD-WAN, qui assurent les échanges de données entre différents sites logistiques de l'entreprise. Sur ce plan, Olivier Hamel se montre très prudent : « *Il faut faire très attention sur les coûts réseaux. Mettre en œuvre une "transit gateway" présente un coût et nécessite d'analyser finement le trafic pour l'optimiser. J'ai été très méticuleux sur le contrôle des coûts, mais ma conclusion est qu'il est impossible de les prévoir exactement. On peut se faire une idée, mais prédire des coûts à 100 € près chaque mois est impossible.* »

Le projet de migration vers le « datacenter-less » doit s'achever en ce mois de septembre. La DSI de FM Logistic va pouvoir s'attaquer aux prochaines évolutions de son infrastructure multi-Cloud. « *Nous serons dans un nouvel écosystème avec deux Cloud providers. Cela nous ouvre le champ des possibles, notamment sur le traitement des données entre elles. Nous poursuivons notre transformation en exploitant les nouvelles possibilités qui nous sont offertes aujourd'hui »,* conclut Olivier Hamel. ■

Par Alain Clapaud

POURQUOI S'INTÉRESSER AUX SOLUTIONS DE GESTION DE LA SURFACE D'ATTAQUE ?

Industrialiser une démarche au croisement entre la cartographie du SI et la gestion du risque cyber présente quelques atoûts. C'est la promesse du CAASM.

ACRONYME encore peu connu dans la communauté des RSSI, le CAASM (« Cyber Asset Attack Surface Management) est pourtant considéré par l'ANSSI comme un outil indispensable à la maîtrise du système d'information. Il est notamment obligatoire pour les opérateurs d'importance vitale (OIV). Une étude conjointe entre le Cesin et l'éditeur français OverSOC révèle la méconnaissance de l'ensemble du périmètre interne et externe à protéger auprès des RSSI interrogés. Ce serait même la difficulté numéro un, devant le manque de ressources humaines ! L'étude, qui sera actualisée en fin d'année, rappelle les objectifs de ces solutions. D'une part, mieux anticiper les attaques et anticiper les actions malveillantes. D'autre part, renforcer la défense cyber en réduisant le délai de réponse. Enfin, la réaction doit être renforcée avec la mise en place d'un dispositif de réponse. Outre les pure players, tels qu'Axonius, JupiterOne, Noetic et le français OverSOC, les grands éditeurs se sont déjà positionnés sur ce marché. C'est le cas de CrowdStrike, d'IBM, Microsofot, Palo Alto et Tenable qui ont tous réalisé des acquisitions.

3,8 M€

C'est le montant de la levée de fonds (Seed) réalisée par OverSOC fin 2023 auprès de CyberK1 et Auriga Cyber Ventures, avec les investisseurs historiques Alacrité France et Finovam Gestion.

Un agrégateur de données avant tout

Pour Théo Plantier, Chief Executive Officer d'OverSOC, une solution CAASM doit permettre de sortir de dix années de déploiement de solutions d'inventaire très diverses et spécifiques. *« Dans ces applications, il y a des données pertinentes et l'objectif du CAASM est de réconcilier et consolider toutes ces sources. »* On parle dans ce cas des informations purement business, notamment la liste des processus métier critiques qui portent l'activité de l'entreprise. Le CAASM doit faire ressortir quels assets sont clés dans le fonctionnement d'une organisation. Ces données doivent être corrélées avec celles de la couche IT et celles de la couche cyber, qui définit le niveau de risque qui pèse sur ces couches IT.

« Pour nos clients, la priorité d'un CAASM c'est son système de connecteur pour aspirer toutes ces données hétérogènes. Il faut une solution pour ne pas avoir à écrire un script maison pour mener chaque intégration. Enfin, il faut pouvoir réconcilier ces sources. » Pour la partie cyber, outre les données d'inventaire, le CAASM s'appuie sur les données issues des scanners de vulnérabilité, des agents EDR et des sondes NDR pour livrer une vision la plus précise possible de la surface d'attaque de l'entreprise. Dès lors que ce référentiel est en place, il devient possible d'automatiser la génération des indicateurs de conformité, des indicateurs liés au niveau de risque de chaque business unit métier. ■

Par Alain Clapaud

> *« La priorité d'un CAASM c'est son système de connecteur pour aspirer toutes les données hétérogènes. »*
>
> ***Théo Plantier, CEO de OverSOC.***

DEVOPS REX

LA CONFÉRENCE **DEVOPS** FRANCOPHONE

100% retour d'expérience

PARIS - 04 & 05 DÉCEMBRE 2024 - PALAIS DES CONGRÈS

Une conférence
sur 2 jours dédiée à l'application du devops en entreprise.

Des témoignages concrets,
100% retours d'expérience, sans placement de produit !

Un espace de solutions,
pour rencontrer des acteurs et networker.

INFOS ET RENSEIGNEMENTS

sur **www.devopsrex.com**
avec le code d'inscription **P-SILDREX24**

(profitez jusqu'au 15/10 des tarifs Early Bird)

Suivez-nous

Un événement organisé par infoprodigital TRADE SHOWS

Aux mêmes dates et lieu que OPEN SOURCE EXPERIENCE

l'événement
Tech – Usages – Business
dédié aux solutions
IT Open Source.

PROTECTION DES ACCÈS : PRIORITÉ NUMÉRO UN DES ENTREPRISES

Dans un environnement IT de plus en plus ouvert et multi-Cloud, l'identité devient le dernier rempart. La mise en œuvre du MFA s'impose, de même que la rénovation des infrastructures de gestion des identités. L'objectif reste néanmoins de tendre vers le "Zero Trust".

L'ÉDITION 2024 de l'étude « Trend of IT » menée par Silicon et KPMG l'a bien montrée : la gestion des accès et, plus particulièrement, la marche vers le modèle « Zero Trust » est la priorité numéro un des décideurs et experts IT. (voir *Silicon,* n° 19) Le vol d'identité représente un risque majeur pour une entreprise, car avec la prolifération des comptes, qu'ils soient destinés aux humains ou aux machines, chaque identité peut devenir une porte d'entrée potentielle sur le réseau d'entreprise.

Le MFA ne suffit pas

Active Directory est devenu une cible prioritaire et même l'authentification multifactorielle (MFA), un système qui accroît la sécurité des accès en combinant mots de passe, tokens de sécurité et applications mobiles d'authentification, n'est pas à l'abri. Pour Noé Mantel, responsable produit chez Specops Software, le MFA est essentiel, mais n'est pas une solution universelle : « *Le MFA améliore considérablement la sécurité en exigeant des étapes de vérification supplémentaires, réduisant ainsi le risque d'accès non autorisé. Cependant, il doit faire partie d'un cadre de sécurité global qui inclut des audits de sécurité réguliers, la formation des utilisateurs et une gouvernance solide des identités.* »
Il souligne aussi que toutes les solutions MFA ne se valent pas. Certaines méthodes, comme les jetons matériels et l'authentification biométrique, offrent une protection plus forte que d'autres.
Pour Noé Mantel, le renforcement de la gestion des mots de passe reste indispensable. L'éditeur propose une solution de réinitialisation de mot de passe en libre-service (SSPR) qui supporte de nombreuses options d'authentification, y compris les codes par SMS, Microsoft Authenticator, Google Authenticator, Okta, YubiKeys, des questions secrètes et l'identification du manager AD. « *Cette diversité garantit que les organisations peuvent mettre en œuvre une approche de sécurité multicouche adaptée à leurs besoins, tout en améliorant l'expérience utilisateur et en réduisant la charge sur le support informatique* », ajoute-t-il.
Active Directory, brique du SI cruciale dans la sécurité des identités, est bien sûr une cible de choix pour les attaquants et de nombreux éditeurs proposent des solutions de protection dédiées. L'éditeur Netwrix a réalisé l'acquisition de PingCastle cet été et dispose d'une offre solide dans ce domaine critique. « *Nous fournissons une sécurité de bout en bout pour Active Directory, en suivant à la lettre les recommandations du NIST*

31,45 Mds $
C'est la taille du marché mondial du « Zero Trust » en 2023, selon Fortune Business Insigths.

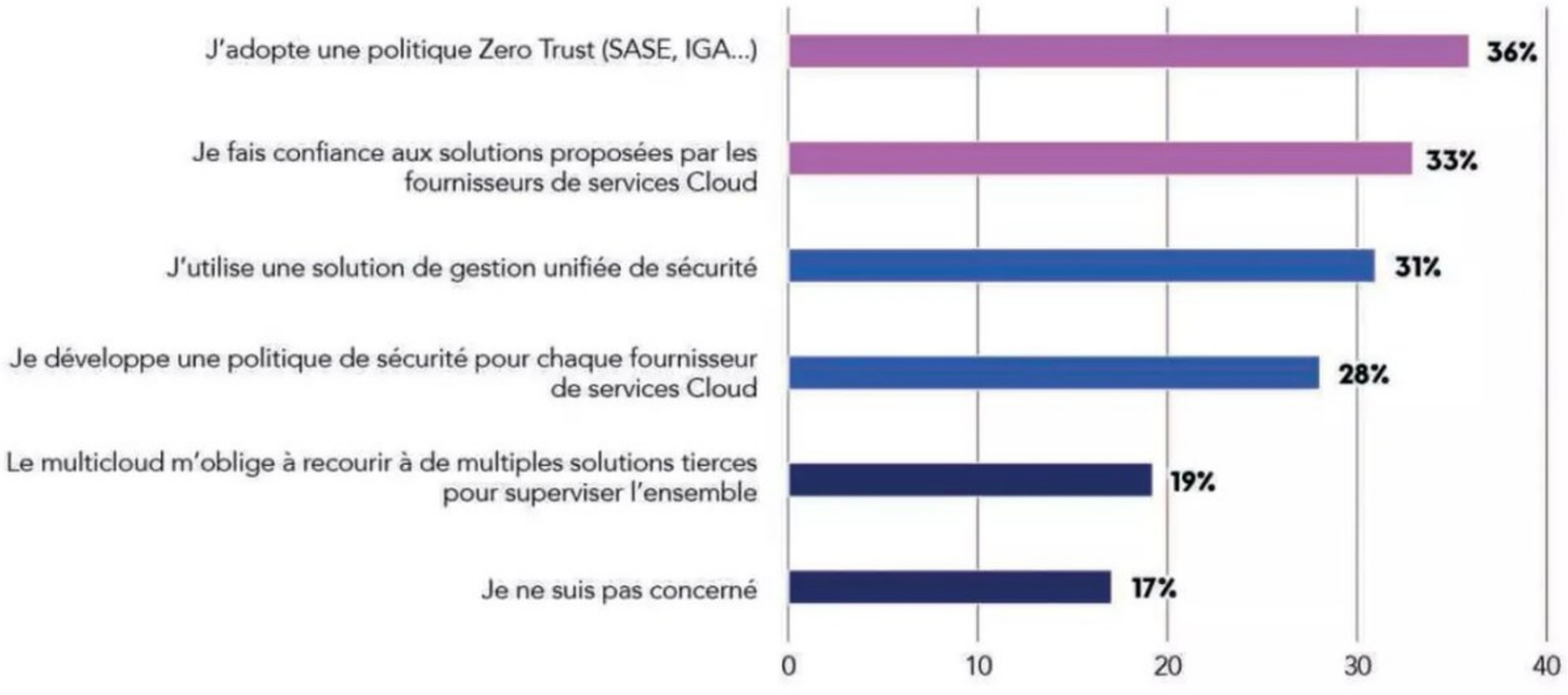
Éclairage marché

Thevie Chea, directrice Solutions Engineering France et Italie chez Okta

Intégration cruciale du MFA

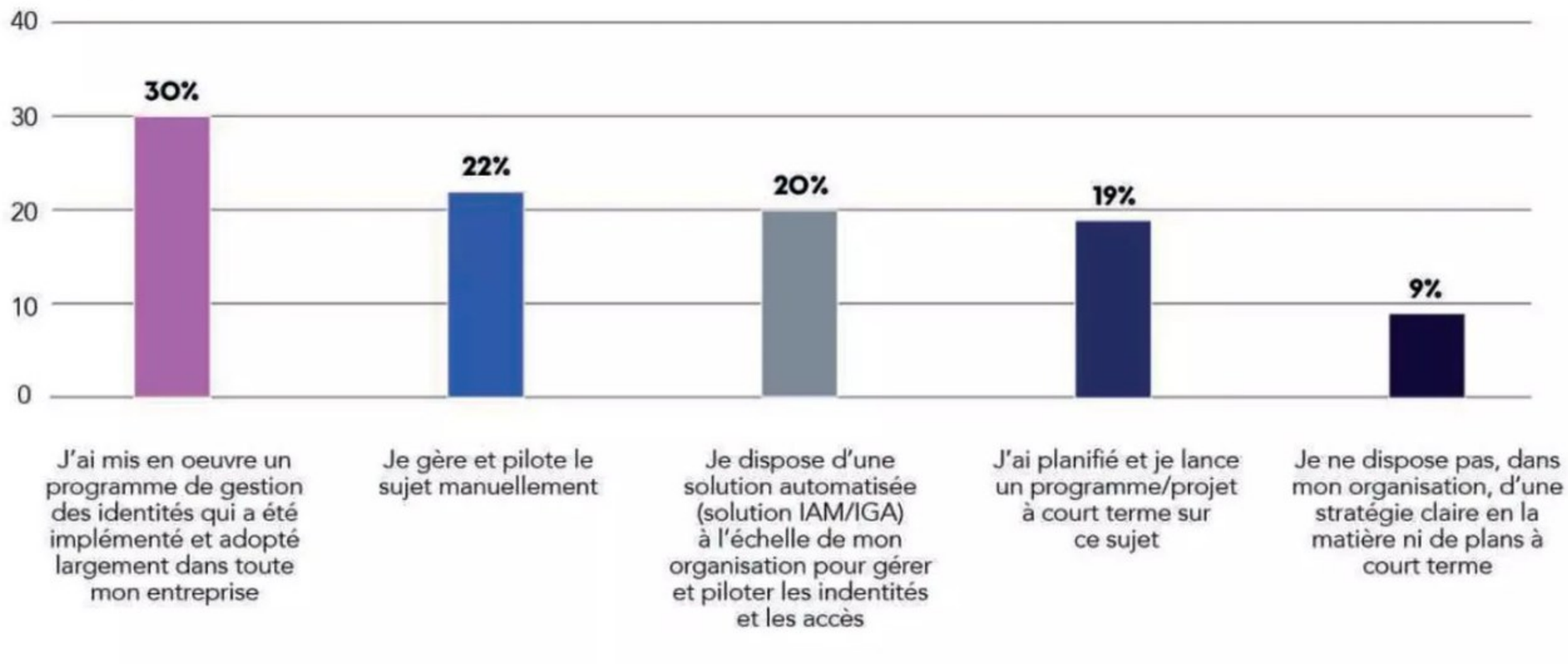
« La modernisation des accès au système d'information doit se concentrer sur plusieurs axes prioritaires. La mise en œuvre du modèle de sécurité "Zero Trust" est essentielle. De même, l'intégration généralise de l'authentification multifactorielle (MFA) est cruciale pour renforcer la sécurité des accès. Un autre axe porte sur la modernisation des systèmes IAM qui permet de centraliser et de sécuriser la gestion des identités et des accès, en facilitant l'adoption de politiques de sécurité robustes et flexibles. L'automatisation des processus de gestion des accès et la mise en place de workflows de sécurité orchestrés permettent de réagir rapidement aux menaces et de réduire les erreurs humaines. Enfin, l'adoption de solutions de surveillance et d'analyse en temps réel pour détecter les comportements anormaux et les menaces potentielles est indispensable. »

Quelles solutions avez-vous déployées pour mieux maîtriser les risques liés à la sécurité dans un environnement multicloud ? *Plusieurs réponses sélectionnables*



L'étude Silicon/KPMG « Trends of IT 2024 » classe les projets Zero Trust prioritaires devant les solutions de sécurité des fournisseurs Cloud et la gestion unifiée de la sécurité.

Quel est la situation de votre organisation en matière de gestion et de gouvernance des identités et des accès ?



Cybersecurity Framework, qui est très similaire à l'approche de l'ANSSI : identifier, protéger, détecter, répondre et récupérer, avec une gouvernance au-delà de tous ces piliers » explique Anthony Moillic, Field CISO EMEA & APAC chez Netwrix. La solution identifie de manière proactive les chemins d'attaque et autres vulnérabilités, pour ajouter une couche de défense en détectant les menaces à leurs débuts, et en bloquant les changements et authentifications considérés comme risqués via l'agent LSASS.

Resserrer les processus liés aux identités

Pour renforcer les accès au SI, Jean-Christophe Vitu, vice-président Solutions Engineer chez CyberArk estime indispensable la modernisation des ▶▶▶

Éclairage marché

Noé Mantel, responsable produit chez Specops Software

Renforcer les mots de passe

« Pour renforcer l'accès à un système d'information (SI), la priorité devrait être l'amélioration de la sécurité des mots de passe tout en intégrant des couches de protection supplémentaires, telles que l'authentification multifactorielle (MFA). Les mots de passe restent un élément fondamental de la sécurité, mais ils doivent être gérés et renforcés efficacement pour atténuer les vulnérabilités. Notre stratégie de sécurité de l'identité se concentre sur plusieurs domaines clés. L'un d'eux consiste à permettre à nos clients de gérer et de sécuriser plus efficacement les identités basées sur le Cloud. Pour y parvenir, nous prévoyons d'intégrer tous nos produits de sécurité des identités actuels dans la plateforme Cloud Netwrix, ce qui maximisera les résultats grâce à un ensemble unifié de fonctionnalités de la plateforme. »

Éclairage marché

Jean-Christophe Vitu, vice-président Solutions Engineer chez CyberArk

Une méfiance par défaut

« Il est possible de protéger les identités et d'atténuer les risques grâce aux principes du "Zero Trust" qui consistent à une approche de méfiance par défaut et en imposant des vérifications continues. Pour ce faire, il est essentiel de mettre l'accent sur le chevauchement de la protection, une véritable défense en profondeur, ainsi qu'une approche de sécurité segmentée en couches, un robuste programme de protection des identités, des analyses efficaces et, en fin de compte, une politique de Zero Trust solide. »

36 %

C'est la part des managers IT français qui affirment avoir déployé une stratégie Zero Trust en 2024, selon Silicon/KPMG (« Trends of IT 2024 »).

▶▶▶ systèmes de gestion des identités et des accès (IAM). *« L'IAM est cruciale pour garantir que seuls les utilisateurs autorisés accèdent aux ressources nécessaires, en automatisant la gestion des permissions et en appliquant des principes comme le moindre privilège ou l'isolation des sessions, afin de limiter les mouvements horizontaux et verticaux des acteurs malveillants »,* indique-t-il. Et de souligner l'importance de mettre en place des systèmes avancés de surveillance et de détection des anomalies pour identifier et réagir rapidement aux tentatives d'accès non autorisé. Éditeur venu du monde des accès à privilèges, CyberArk propose désormais une plateforme complète de gestion des identités. Il innove notamment sur l'intelligence artificielle et la technologie de détection et réponse aux menaces liées aux identités, l'ITDR (« Identity Threat Detection and Response »).

Spécialiste de la gestion d'identité, Sailpoint met en avant le rôle joué par l'IAM et, plus généralement, les plateformes IGA (« Identity Governance & Administration ») dans la sécurisation des accès. *« La gestion des identités vient répondre à la question "qui a accès à quoi et quand ?" »,* explique Jonathan Gosselin, vice-président groupe Dach & Europe du Sud de Sailpoint. *« Les identités couvrent non seulement les identités physiques, mais aussi virtuelles. La gestion des identités permet de gérer les autorisations et accès privilégiés qui peuvent mener à l'attribution de rôles dans l'entreprise en fonction des différents profils. En outre, la gestion des identités participe à l'implémentation des normes règlementaires telles que le RGPD et NIS2. »*

Le secteur de la gestion des identités innove, notamment en intégrant des algorithmes d'IA pour simplifier l'intégration des applications. Elle intervient aussi dans l'automatisation des prises de décisions et pour faire des recommandations sur l'attribution de rôles lorsqu'on a plusieurs profils similaires. Enfin, elle vient détecter les utilisateurs atypiques pour revoir leurs accès plus fréquemment. À cet arsenal vient désormais s'ajouter l'ISPM (« Identity Security Posture Management »). L'objectif des solutions de ce type est d'apporter une visibilité complète sur les identités, les accès et les permissions, sur l'ensemble de l'organisation. *« La solution effectue des évaluations continues des risques associés aux identités et aux accès, identifiant les vulnérabilités et les comportements anormaux qui pourraient indiquer une compromission »,* détaille Thevie Chea, directrice Solutions Engineering France et Italie chez Okta. *« En automatisant les politiques de sécurité basées sur les risques, ISPM permet d'appliquer des mesures de protection adaptées en temps réel, réduisant ainsi les risques de sécurité »,* ajoute-t-elle. Enfin, l'ISPM va aider les entreprises à se conformer aux réglementations en matière de sécurité et de protection des données, en assurant une gestion rigoureuse des identités et des accès, un besoin qui va nettement s'amplifier avec l'arrivée de NIS2 et DORA. ■

Par Alain Clapaud

FAIRE CONVERGER L'HUMAIN ET LA MACHINE : une question d'équilibre

Le 4 juillet dernier s'est tenue la Matinale Silicon consacrée à l'IA et la cybersécurité. À cette occasion, Nicolas Millet, Responsable de l'activité cybersécurité pour le Groupe Sigma a partagé sa vision de l'enjeu et ses convictions sur la nécessaire combinaison des intelligences...

Selon le Baromètre de la cybersécurité des entreprises d'Opinionway pour le CESIN, 49 % des entre-prises déclarent avoir subi au moins une cyberattaque avec un impact significatif. Comme le souligne Nicolas Millet, « *la question n'est plus de savoir si une entreprise subira une cyberattaque, mais plutôt quand, à quelle fréquence et avec quel impact* ». Face à cette menace grandissante, l'intelligence artificielle (IA) et l'intelligence humaine doivent travailler en symbiose pour assurer une défense efficace.

Nicolas Millet
Responsable de l'activité cybersécurité pour le Groupe Sigma

L'importance de la sensibilisation de tous

La première ligne de défense contre la cybermenace est l'humain. « *Le comportement inapproprié des utilisateurs reste toujours l'un des premiers vecteurs d'attaque informatique* », martèle Nicolas Millet. En réponse à cette réalité, Sigma a développé un parcours de sensibilisation qui aborde chaque mois un point clé de la sécurité informatique. « *Notre approche de sensibilisation s'appuie d'abord sur le levier humain de l'acculturation en veillant bien à ne pas dispenser des messages anxiogènes. Nul besoin d'IA pour confier aux équipes un guide des bons réflexes et faire de l'humain le maillon fort de sa sécurité.* »

L'IA : un allié indispensable, mais pas suffisant

L'IA joue un rôle crucial dans la lutte contre la cybercriminalité. Sa capacité à analyser d'énormes volumes de données en temps réel permet de détecter des anomalies qui pourraient échapper à l'œil humain. Pour Nicolas Millet, « *l'IA permet de comprendre, de cerner, d'analyser des millions d'événements de sécurité qui se produisent chaque seconde* ». Cependant, celle-ci ne peut pas, elle ne doit pas tout faire ! Comme le précise Nicolas Millet, « *l'humain apporte la pertinence dans l'analyse d'un incident de sécurité. Chez Sigma, nous utilisons la suite IBM Qradar qui intègre les composants l'IA augmentant les capacités de l'analyste : l'humain peut alors se concentrer sur la qualification et la remédiation des incidents majeurs et l'accompagnement du client dans sa gestion de crise et la reprise de ses activités.* »

Le SOC : internaliser ou externaliser ?

Dans un contexte où les systèmes d'informations s'hybrident pour répondre aux nouveaux usages, la décision d'internaliser ou d'externaliser le Security Operations Center (SOC) est un choix stratégique pour toute entreprise. Un SOC internalisé peut offrir une meilleure connaissance des actifs et process de l'organisation, mais nécessite des compétences multiples et un investissement important en formation. Un SOC externalisé quant à lui, peut apporter une expertise pointue et une disponibilité 24/7, mais il peut être moins familier avec le contexte spécifique de l'entreprise. Mais le débat va plus loin ! L'IA permet d'exploiter une kyrielle de signaux faibles, qui nous permettent de dépasser la détection et la réponse aux menaces pour nous inscrire dans une démarche préventive et prédictive. Car Nicolas Millet en est convaincu : « *C'est en combinant le meilleur des deux mondes que nous pourrons atteindre la cyber résilience, vivre avec les cybermenaces qui resteront durablement notre quotidien et protéger l'activité de nos entreprises* ». ■

SiGMA
NUMÉRIQUE À IMPACT

NIS2 : À L'AUBE DE SA MISE EN APPLICATION, LES ENJEUX SONT DE TAILLE

Même si la directive propose un mécanisme de proportionnalité en termes d'exigence, en fonction du niveau de criticité, la mise en œuvre peut devenir un projet conséquent, onéreux et exigeant en termes techniques, en fonction de la maturité initiale de l'entreprise.

AUJOURD'HUI, les systèmes d'information (SI) ne sont pas seulement le cœur des entreprises ; ils sont le champ de bataille sur lequel se jouent la sécurité des organisations. Depuis l'adoption de NIS2 en janvier 2023, il s'y joue la sécurité informatique de l'Union européenne (UE). Les activités sont de plus en plus numérisées, et les interconnexions entre systèmes et entités sont multipliées. L'utilisation généralisée des technologies de l'information et de la communication expose davantage la société dans son ensemble aux cybermenaces. NIS1 avait pour objectif d'assurer un niveau de sécurité élevé, et commun, pour les réseaux et les SI de l'UE. Toutefois, au vu de l'évolution rapide du paysage numérique depuis sa mise en application en 2016, NIS1 s'est vite vue dépassée. La directive NIS2 reprend, complète et améliore ainsi la précédente directive en corrigeant les lacunes identifiées – comme le manque de cohérence entre les États membres et les différents secteurs, le faible niveau de connaissance commune des risques cyber ou encore l'absence de réaction commune en cas de crise. À l'aube de son entrée en vigueur en France en octobre 2024, il est donc important pour les entreprises de se renseigner sur les sujets suivants.

Suis-je concerné par la directive NIS2 ?

NIS1 s'étendait, dans un premier temps, aux secteurs les plus critiques : énergie, transports, banques, infrastructures de marchés financiers, secteur de la santé, fourniture et distribution d'eau potable, infrastructures numériques.
Pour faire face à la hausse des cybermenaces et la professionnalisation des groupes d'attaquants, NIS2 cherche aujourd'hui à étendre ce périmètre en ajoutant des secteurs qui ont beaucoup évolué numériquement ces dernières années, et dont la sécurité de leurs systèmes devient un impératif. Il s'agit là des eaux usées, de l'espace, de l'administration publique, des services postaux et d'expédition, de la gestion des déchets, de la chimie, de l'alimentation, de la fabrication, de la recherche, et des fournisseurs numériques. Les entreprises concernées seront divisées en deux catégories : les entités importantes et les entités essentielles. Cette distinction permet de proposer un niveau d'obligation adapté, et proportionné, selon leur niveau de criticité.
La directive concerne ainsi tout type d'entreprise, des PME aux grands groupes du CAC 40, mais aussi les administrations publiques. Elle offre la possibilité aux États membres d'inclure les collectivités territoriales ou toute autre entreprise spécifique dont l'activité nécessiterait une sécurisation accrue. Aussi, la directive exige un niveau de sécurité minimal pour tous les acteurs de la chaîne d'approvisionnement d'une entreprise concernée par NIS2, même si ces derniers ne correspondent pas aux critères initiaux. L'objectif : lutter contre les attaques par rebond qui consistent à utiliser et infecter les acteurs tiers, souvent moins bien protégés et matures, pour corrompre les systèmes de leur cible principale.

NIS2 : une directive plus exigeante

La nouvelle directive renforce les exigences de la précédente, et dresse un ensemble de mesures qui doivent être prises en compte par toutes les entités concernées. Ces mesures incluent notamment des politiques liées à l'analyse des risques et la PSSI (politique de sécurité du système d'information),

la gestion des incidents grâce à un processus de notification d'incident plus strict, la mise en place de plans de continuité d'activité (PCA) et de reprise d'activité (PRA), la sécurisation des sauvegardes et la gestion des crises, la sécurité de l'acquisition, ainsi que le développement et la maintenance des réseaux et SI. Elles incluent aussi le traitement et la divulgation des vulnérabilités, l'évaluation des mesures de gestion des risques cyber, la sécurité de la chaîne d'approvisionnement, les politiques et procédures liés à la cryptographie, la sécurité des ressources humaines, les politiques de contrôle d'accès, la gestion des actifs, l'adoption de solutions d'authentification multifactorielle (MFA) ou continue, ou encore l'utilisation d'outils de communication sécurisés et de systèmes de communication d'urgence en cas de crise. Par ailleurs, la responsabilité personnelle des incidents sera désormais attribuée aux chefs d'entreprise, qui seront aussi dans l'obligation de se former sur le sujet. Les équipes de direction devront approuver les mesures de cybersécurité, et assumer la responsabilité en cas de violation de la directive. NIS2 souhaite, par cette mesure, induire l'appropriation des risques par les cadres de la direction afin de garantir une meilleure gouvernance des risques.

Une cohésion des États membres renforcée

La directive NIS2 ne fait pas que réglementer le niveau de sécurité des entreprises. Elle encourage aussi les États membres à renforcer leur coopération en matière de gestion de crise cyber, notamment par le lancement officiel du réseau CyCLONe (« Cyber Crisis Liaison Organisation Network ») – qui rassemble l'ANSSI et ses homologues européens. Ce réseau poursuit deux objectifs. Le premier, permettre des consultations sur les stratégies nationales de réponse, et le second permettre une analyse d'impact coordonnée sur les conséquences d'une crise cyber d'ampleur ou de crise informatique transfrontalière. Le réseau CyCLONe de l'UE contribue à la mise en œuvre du plan d'action de la Commission pour une réaction rapide en cas d'incident ou de crise de cybersécurité transfrontalière de grande ampleur.

Une obligation et un pouvoir confiés aux autorités nationales

La transposition française de la directive doit être effectuée avant fin octobre 2024, et la mise en conformité sera obligatoire. NIS2 confère aux autorités nationales le pouvoir de contrôler la mise en conformité de la directive : une grande nouveauté par rapport aux différentes réglementations. L'ANSSI n'aura plus seulement un rôle de conseil, elle jouera dorénavant un rôle de surveillance et de supervision de la mise en œuvre de la directive. L'ANSSI pourra ainsi émettre des avertissements et des ordres à l'encontre des entités contrôlées qui ne respectent pas la directive NIS2. Si ceux-ci ne suffisent pas, l'ANSSI peut établir des amendes administratives – qui seront à minima de 10 millions d'euros ou de 2 % du chiffre d'affaires annuel mondial pour les entités essentielles, et de 7 millions d'euros ou de 1,4 % du chiffre d'affaires annuel mondial pour les entités importantes.

Une mise en application imminente : comment bien se préparer ?

Même si la directive propose un mécanisme de proportionnalité en termes d'exigence, en fonction du niveau de criticité, la mise en œuvre peut devenir un projet conséquent, onéreux et exigeant en termes techniques, en fonction de la maturité initiale de l'entreprise. Toutefois, les mesures de sécurité présentes dans NIS2 sont semblables à celles contenues dans les normes de la famille ISO 27000 ou de la norme américaine NIST. Être certifié ISO 27001, ou faire appel à des prestataires qualifiés par l'ANSSI, permettra aux entreprises de valider directement leur conformité vis-à-vis d'une majeure partie de la directive. Pour la mise en conformité, l'ANSSI conseille fortement d'être accompagné par des experts. Enfin, certaines entreprises ne répondant pas aux critères initiaux peuvent se retrouver soumises à la directive, si elles sont actrices de la chaîne d'approvisionnement d'une entreprise concernée par NIS2. Il est donc conseillé, à toute entreprise exerçant cette fonction, d'évaluer l'éligibilité de leurs clients à la directive et d'effectuer une mise en conformité NIS2, le cas échéant.

Cela leur permettra d'éviter de subir les engagements « clés en mains » fournis par leurs clients grands comptes, qui pourraient s'avérer être trop engageants et dangereux pour leur activité. ■

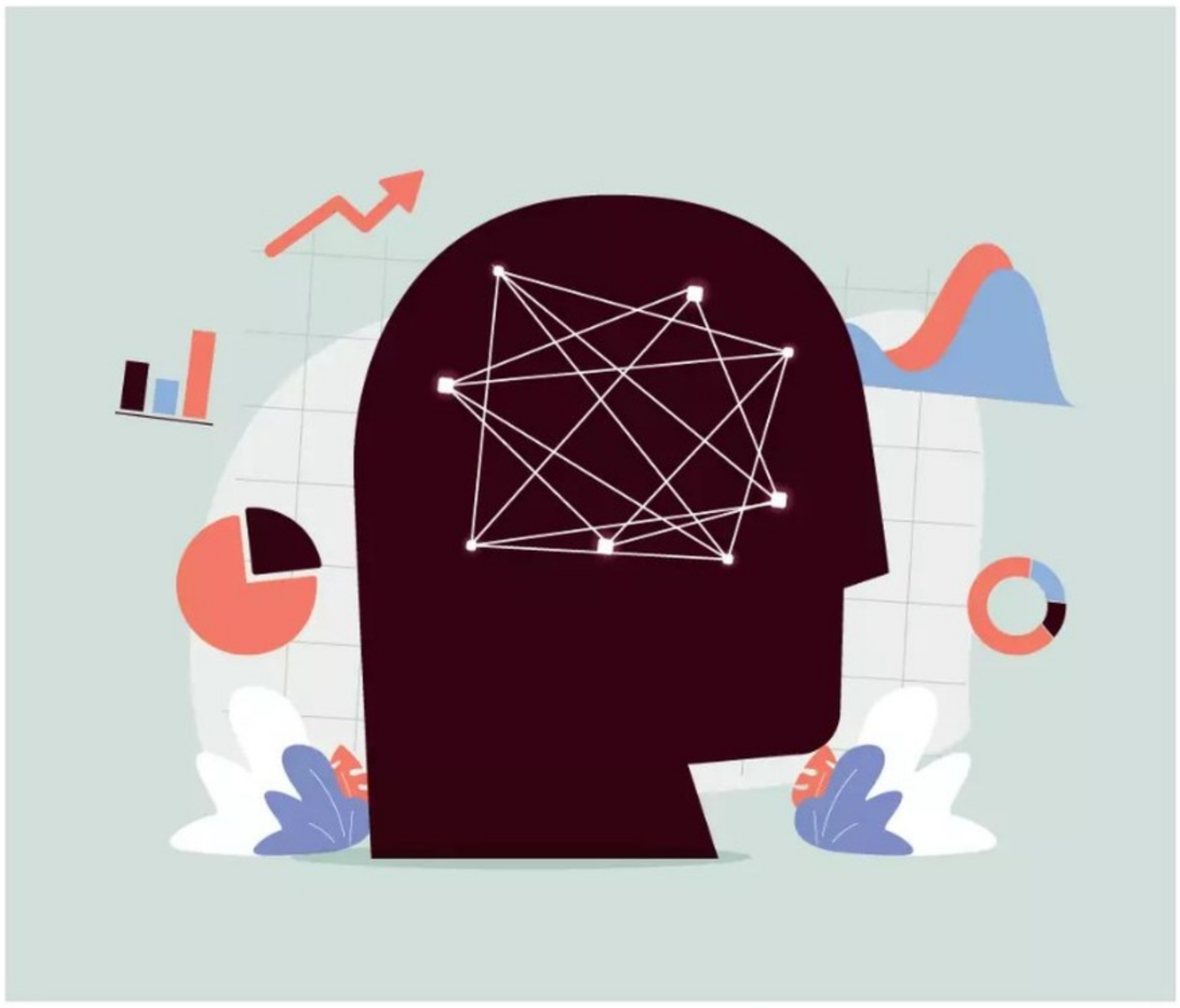
Par Elwynn Dauphin,
consultant au sein de Synetis

10 000

C'est l'évaluation du nombre d'entités importantes et d'entités essentielles, ainsi que leurs prestataires, concernées par NIS2.

COMMENT SALESFORCE A TESTÉ LES LLM DÉDIÉS AU CRM

Salesforce a réalisé un benchmark des LLM sur des cas d'usage CRM. Passage en revue de la méthode et des résultats.



QUELLE TAILLE DE PROMPT ? Quel juge pour les évaluations automatisées ? Quelles conditions d'exécution pour les modèles non disponibles sur une API publique ? Autant de questions que Salesforce a dû aborder pour constituer son benchmark de grands modèles de langage (LLM). Ce benchmark a la particularité de cibler des cas d'usage propres à la gestion de la relation client (CRM), dans deux domaines : ventes et service. Ils couvrent la synthèse et la génération de contenus textuels.

Pour le moment, Salesforce n'a évalué que des modèles génériques entraînés pour le suivi d'instructions. Ils émanent de huit fournisseurs :

- AI21 (Jamba-Instruct)
- Anthropic (Claude 3 Haiku, Claude 3 Opus)
- Cohere (Command R+, Command Text)
- Google (Gemini Pro 1.0, Gemini Pro 1.5)
- Meta (Llama 3 8B, Llama 3 70B)
- Mistral AI (Mistral 7B, Mixtral 8x7B)
- OpenAI (GPT-4o, GPT-4 Turbo, GPT-3.5 Turbo)
- Salesforce (XGen 2)

À benchmark spécifique, méthodologie spécifique

Chacun de ces modèles s'est vu attribuer un score de précision. Il en résulte une évaluation sur quatre critères : l'exhaustivité, la concision, la factualité des réponses, ainsi que la qualité de suivi des instructions en termes de contenu et de format.

Quatre critères aussi pour la partie « *confiance et sûreté* », à savoir :

- Capacité à refuser de répondre à des prompts indésirables.
- Respect de la vie privée (en 0-shot et 5-shot).
- Aptitude à corriger de fausses informations dans les prompts.
- Résistance aux biais de genre et de compte.

Le benchmark compare par ailleurs le temps de réponse des modèles, le nombre moyen de tokens dans les réponses et le coût global. Salesforce l'a calculé à partir de la tarification standard pour les modèles sur API publique (celle du fournisseur pour OpenAI, Google et AI21 ; via Bedrock pour Anthropic et Cohere). Pour les autres, autohébergés, il l'est sur un plan horaire, en supposant un niveau d'usage correspondant à un CRM en production.

Les modèles autohébergés ont été déployés avec partitionnement sur des instances EC2 (g5.x48large pour les 7B, p4d.24xlarge pour les 70B), en utilisant le framework d'inférence DJL. Pour tester la latence, Salesforce a pris en considération deux cas d'usage différents sur le nombre de tokens en entrée (500 vs 3 000). Ses mesures valent pour une « *connexion haut débit* », précise-t-il.

L'éditeur a évalué la partie confiance et sûreté sur des datasets publics... et les biais sur des ▶▶▶

48 Mds $

d'ici 2033. C'est l'estimation du marché des solutions IA dédiées au CRM, selon Market.us.

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

SALONS SOLUTIONS

9 & 10 octobre 2024

PARIS EXPO
PORTE DE VERSAILLES

Avec en parallèle

mobility for business

SALONS SOLUTIONS erp

SALONS SOLUTIONS démat

SALONS SOLUTIONS crm

SALONS SOLUTIONS IA & data

SALONS SOLUTIONS e-achats

SALONS SOLUTIONS SiRH

Réservez dès maintenant votre badge gratuit sur www.salons-solutions.com

Platinum sponsor

axelor

Gold sponsor

coupa

Silver sponsors

pennylane systhen Making data valuable UNIT4

@SalonsSolution1
#salonssolutions

MC SalonsSolutions

salons-solutions.com

données du CRM. Pour le genre, il a joué avec les noms des personnes et les pronoms. Pour les comptes, sur le nom des entreprises remplacées par ceux de concurrents du même secteur. Llama 70B a fait office de LLM juge pour évaluations automatiques. Salesforce justifie ce choix par le niveau de corrélation avec les évaluateurs humains.

Une longueur d'avance pour OpenAI… sur la précision

Sur les évaluations manuelles, on trouve systématiquement en tête un modèle d'OpenAI. Le plus souvent, c'est GPT-4o. Il domine le classement sur le résumé d'appels et la génération d'e-mails côté ventes. Même chose, côté service, pour la création de bases de connaissance et la fourniture d'insights en direct pendant une conversation. Toujours dans une perspective de service au client, la palme revient à GPT-4 Turbo pour la fourniture de recommandations de réponses en direct. Et à GPT-3.5 Turbo pour le résumé d'appels.

Derrière les modèles d'OpenAI, se distinguent :

- Les modèles Llama pour la génération d'e-mails côté commerciaux de connaissances.
- XGen 2 pour les insights en cours de conversation.
- Claude 3 Haiku pour les recommandations de réponses en direct.

Sur les évaluations automatisées, les modèles d'OpenAI ressortent souvent en tête. Claude 3 Opus a cependant l'avantage sur le résumé d'appels, autant côté ventes que service au client. Llama 3 70B se distingue sur la génération d'e-mails et de recommandations de réponses. Mistral 7B est rarement à son avantage. Il est même le seul à obtenir un score inférieur à 3 (sur 4 points possibles) pour les recommandations de réponses, et à 2 sur la capacité à mettre à jour des enregistrements CRM.

> *« Ce banc d'essai LLM dédié au CRM apporte plus de clarté sur les capacités et les limites des différents LLM. »*
>
> ***Silvio Savarese, Chief Scientist chez Salesforce AI Research.***

39 %

des équipes de vente ont déjà mis en œuvre l'IA sous une forme ou une autre dans leurs systèmes CRM, selon Zipdo.

Il arrive que dans une même famille, le plus petit modèle fasse mieux. Sur le résumé d'e-mails commerciaux, par exemple, Llama 3 8B dépasse Llama 3 70B. Sur le résumé d'appels, Mistral 7B dépasse Mixtral 8x7B (même si on ne peut pas comparer l'architecture de ces deux modèles).

Mistral AI intéressant sur les temps de réponse…

Sur le temps de réponse, les valeurs sont peu différenciées entre cas d'usage. Sur sept d'entre eux, Mixtral 8x7B mène la danse, avec une exécution en 2,44 secondes. Il devance Claude 3 Haiku (2,78), XGen (3,71), Llama 3 8B (3,76), Jamba-Instruct (4), GPT-3.5 Turbo (4,5) et GPT-4o (5,1). Llama 3 70B est bon dernier (20,1). Les cas d'usage en question : mise à jour d'enregistrements CRM, résumé d'appels et d'e-mails (ventes & service), création de bases de connaissances et résumé de conversations en direct.

Sur les quatre autres cas d'usage (génération d'e-mails, résumé de conversations, insights et recommandations en direct), Claude 3 Haiku arrive en tête (2,2 secondes). Suivent Mixtral 8x7B (2,41), XGen (2,64), Llama 3 8B (3,23), Jamba-Instruct (4), GPT-3.5 Turbo (4,2), Gemini Pro 1 (4,4) et GPT-4o (5). Llama 3 70B est à nouveau en queue de peloton (29,4).

… et sur les coûts

On retrouve presque la même division entre cas d'usage sur la question des coûts (seule la création de bases de connaissances change de groupe).

Sur le premier groupe, qui comprend essentiellement des tâches de synthèse, Mistral 7B est l'unique modèle à entrer dans la catégorie *« bas coût »*. Sept modèles entrent dans le segment *« coût moyen »* : Claude 3 Haiku, Gemini Pro 1, GPT-3.5 Turbo, Jamba-Instruct, Llama 3 8B, Mixtral 8x7B et XGen 2. Les coûts sont élevés pour Claude 3 Opus, Command R+ et Command Text, Gemini Pro 1.5, GPT-4o, GPT-4 Turbo et Llama 3 70B.

Sur le deuxième groupe, qui comprend essentiellement des tâches génératives, Mistral 7B n'est plus seul dans la catégorie *« bas coût »*. Il voisine avec Claude 3 Haiku, Gemini Pro 1, GPT-3.5 Turbo, Jamba-Instruct, Llama 3 8B et Mixtral 8x7B. En *« coût moyen »*, il y a Command Text, Gemini Pro 1.5, Llama 3 70B et XGen 2. Les coûts restent élevés pour Claude 3 Opus, Command R+, GPT-4o et GPT-4 Turbo. ■

Par Clément Bohic

SEPTEMBRE EN OR

UN PETIT GESTE POUR VOUS, UN GRAND DON POUR EUX

Crédit photo : Ward Ivan Rafik

Chaque mois, 200 enfants et adolescents sont diagnostiqués d'un cancer en France. Pendant **SEPTEMBRE EN OR**, continuons de nous mobiliser contre ce fléau.

Faites un don sur : imagineformargo.org

IMAGINE FOR Margo
Children without CANCER

« Avec NIS2, on ne peut plus se cacher et on ne peut plus jouer avec le feu.»

Olivier Hoberdon,
DSI de Bouygues SA

À la tête de la DSI de Bouygues SA, qui chapeaute toutes les activités du groupe français, Olivier Hoberdon partage ses réflexions sur l'évolution de la gestion de la cybersécurité.

Comment analyser le mouvement majeur de déploiement des solutions cyber sur le Cloud en mode as a service ?

Olivier Hoberdon - De plus en plus d'entreprises ont transféré une partie de leur SI dans le Cloud, ce qui les amène à s'intéresser aux offres de cybersécurité en mode service. C'est aussi une manière pour Bouygues SA comme de nombreuses entreprises de se recentrer sur son cœur du métier qui n'est pas d'être éditeur de solutions cyber ! C'est un moyen de gagner rapidement une posture cyber contre les menaces qui évoluent sans arrêt. Et c'est encore plus vrai avec le développement de l'intelligence artificielle générative. Concrètement, la « cyber as a service » donne accès à toutes les briques de sécurité, sans consentir

d'investissement lourd comme un SIEM, et avec des mises à jour permanentes qui repoussent le risque d'obsolescence. Cela permet aussi d'assurer la scalabilité. Cependant, quand j'échange avec mon RSSI, on recentre le sujet sur les avantages et les risques du passage sur le Cloud. Il y a beaucoup de solutions cyber sur plusieurs plateformes. L'enjeu c'est de rationaliser les choix techniques parce qu'on ne peut pas multiplier les effectifs, les compétences et le nombre de consoles à regarder. Un autre sujet, c'est l'introduction des risques en externalisant. Il faut s'assurer que la posture cyber que tu t'imposes soit la même chez ton prestataire. Ceci dit, je constate une maturité croissante des offres cyber qui couvrent tous les piliers de NIST, que ce soit pour les outils de gouvernance, de détection ou de reprise d'activité.

La question de la gouvernance des identités et des accès apparaît comme une préoccupation majeure des RSSI. Est-ce la clé de voûte d'une politique cyber ?

Oui, et encore plus maintenant avec l'ouverture du SI à nos prestataires et à toutes ces applications SaaS. Le point commun, c'est cette gouvernance des identités regroupée sous le vocable IAM. Cela devient l'élément clé de ta politique cyber. Elle aide à prévenir les violations de données, à assurer la conformité, à améliorer l'efficacité opérationnelle et à gérer les risques. Le fait de dire « je contrôle qui a accès à quoi, quand, comment et pourquoi », c'est vraiment la quadrature. C'est ce qu'on retrouve derrière le « Zero Trust ». C'est un chapitre qui est extrêmement important, voire obligatoire, dans une bonne politique cyber. Le principe du moindre privilège, du « just in time » et des accès conditionnels, c'est ce qu'on pratique chez Bouygues SA. Il a fallu trouver un juste équilibre entre la sécurité et le confort des utilisateurs. Nous avons eu un gros travail de formation et de sensibilisation des collaborateurs, mais aussi surtout des administrateurs. Car n'oublions pas que les comptes à privilèges restent une surface d'attaque de choix ! Ceci dit, les projets d'IAM sont des projets complexes et coûteux à mener.

Cette tendance forte de l'externalisation impose-t-elle une sélection plus rigoureuse des prestataires ?

Oui. D'abord un bénéfice. Cette externalisation rapproche les fonctions DSI et RSSI. C'est une véritable danse à deux car il y a une confrontation entre performance et sécurité. Le DSI amène les contraintes liées au business et le RSSI ses contraintes cyber. C'est pour cette raison qu'il faut énormément échanger afin de grandir ensemble. Le juste équilibre, c'est le management par le risque pour développer le business en respectant les règlementations. C'est illusoire de vouloir tout protéger. Il m'est arrivé d'avoir un « no-go » du RSSI pour une solution SaaS, parce que le fournisseur ne répondait pas à nos exigences de posture cyber. Car oui, la tendance croissante vers l'externalisation, vers le Cloud ou des solutions SaaS nécessite une sélection plus rigoureuse des prestataires en matière de cybersécurité. Pour chaque application SaaS, on a un questionnaire d'exigence annexé au contrat. C'est une étape obligatoire avant toute contractualisation, qui nous permet de connaître la posture cyber de notre prestataire. Il y a quatre points qui sont vraiment importants. Le premier, c'est la gestion des données. On a besoin de garantir le même niveau de confidentialité, d'intégrité et de disponibilité que si on l'avait fait en interne. Le deuxième, en lien direct avec le premier, c'est la conformité réglementaire, avec par exemple la localisation des données. Le troisième point, c'est la gestion des risques, en particulier avec la sélection des prestataires. Et le dernier point, c'est la capacité à la récupération après-sinistre : comment le prestataire va gérer son PRA (plan de reprise d'activité) et minimiser les perturbations pour votre organisation. Cette méthode permet d'engager une discussion avec le prestataire avant la contractualisation. Cela nous permet d'apprécier leur maturité cyber, leurs pratiques de sécurité, leurs investissements sur cette thématique et de clarifier les responsabilités, surtout entre les différents modèles de SaaS (de l'infrastructure - IaaS - au logiciel - SaaS - en passant par la plateforme - PaaS). C'est un point essentiel pour éviter que le divorce soit compliqué à gérer, surtout en cas de crise cyber.

Est-ce que NIS2 va contribuer à élever le niveau de compétences des prestations cyber ?

Je pense que oui. NIS2 devrait contribuer à élever le niveau de compétences des prestations cyber, en imposant des standards plus élevés et plus homogènes, et en favorisant l'échange de bonnes pratiques et de retours d'expérience. Une entreprise attaquée partagera avec l'agence les caractéristiques techniques de l'incident (les indicateurs de compromission ou IoC) et le partage avec les autres entreprises permettra que chacun se protège. Avec NIS2, on ne peut plus se cacher et on ne peut plus jouer avec le feu. D'autre part, la directive va ▶▶▶

Son parcours

DSI de Bouygues SA depuis 2018 et co-animateur de BYTECH, la communauté IT et Digital du Groupe Bouygues. De formation ingénieur en travaux publics et passionné d'informatique, il est passé par différents postes du support utilisateur au responsable de production. Il a été élu « DSI engagé 2021 » pour son engagement alliant ambition et réalisme autour des sujets liés au numérique responsable.

INTERVIEW

« Il faut s'assurer que la posture cyber que tu t'imposes soit la même chez ton prestataire. »

▶▶▶ imposer une formation et une responsabilisation des dirigeants : cela fait prendre conscience que la cybersécurité n'est plus seulement un sujet d'expert technique, mais bien une thématique d'entreprise à considérer. Cette démarche renforcera l'hygiène sécurité de tous nos prestataires. Parce que nous sommes tous interconnectés, ou au moins interdépendants, ce sont des écosystèmes entiers qui vont progresser. Dans un monde de plus en plus digital, aucune entreprise peut dire ne pas être concernée par cette cyber résilience.

On perçoit une préoccupation forte des RSSI face à l'émergence rapide de l'IA générative. Certains y voient une recrudescence de risques, d'autres y voient un terrain d'opportunités. Quelle est votre perception ?

C'est vraiment une forte préoccupation parce qu'il y a une augmentation des risques, mais aussi des opportunités. C'est souvent pareil... Le verre à moitié plein, à moitié vide. Bien que cette technologie stimule la création de contenu et améliore les processus métier, elle peut également être utilisée à des fins malveillantes (manipulation, falsification, désinformation). L'IA générative peut créer du contenu réaliste voire très réaliste, ce qui peut être utilisé pour des attaques de phishing ou d'ingénierie sociale. Cela peut affecter la réputation de l'entreprise et la confidentialité des données. Nous avons besoin de sensibiliser les collaborateurs à ces enjeux, à la fois éthiques et juridiques. Comme beaucoup d'entreprises, nous avons adopté une charte sur l'utilisation responsable de l'IA. Parce qu'on ne veut pas et que l'on ne peut pas l'interdire, il faut qu'on se l'approprie et qu'on la comprenne. Et c'est aussi vrai du côté de la défense cyber, c'est un fabuleux sujet parce que la cyber a produit une quantité astronomique de données. Donc c'est un terrain vraiment très fertile pour développer des modèles comportementaux (par exemple la détection des voyages impossibles, des tentatives de connections à des heures inhabituelles). Je vois que toutes les solutions, ou presque, qu'on nous propose sur le marché s'appuient beaucoup sur les modèles comportementaux. Je trouve que c'est bénéfique parce que ces sujets-là, il y a encore trois ans, on ne les voyait pas aussi finement. C'est une opportunité car on repère davantage de signaux faibles avec le SOC couplé avec de l'IA. Cela permet de faire un « hunting » plus fin, de faire des corrélations plus sophistiquées entre plusieurs indicateurs et de gagner en vélocité. Mais ce n'est pas magique, on a encore besoin de l'humain. Nos collaborateurs restent notre meilleur rempart contre les attaques.

Sur le marché, tous les éditeurs cyber prétendent avoir intégré de l'IA générative dans leurs solutions. Comment jugez-vous cela ?

Pour certains, c'est du PowerPoint... du marketing. C'est quand même malheureux de dire que si je n'ai pas mis le logo IA, finalement, ma solution n'est pas bonne. Donc, attention à cela. Encore une fois, ça ne remplacera jamais une compétence d'un RSSI ou la compétence d'un analyste. L'IA générative, les attaquants l'ont aussi.

Le recrutement de talents et leur fidélisation restent des préoccupations majeures des RSSI. Comment abordez-vous cette problématique chez Bouygues ?

Le recrutement et la fidélisation des talents en cybersécurité sont en effet des défis majeurs pour le Groupe dans un paysage où la demande de compétences en sécurité informatique dépasse largement l'offre disponible. Tout comme la data, nous sommes sur des métiers pénuriques. Au sein du Groupe, nous avons une communauté IT et Digital BYTECH qui réunit plus de 3 500 collaborateurs. Parmi cette communauté, depuis deux ans, nous avons une communauté dédiée BYTECH Cyber qui est composée de plus 250 collaborateurs cyber avec une dimension internationale. Afin de faire connaître la richesse de nos métiers, nous participons à des événements spécifiques comme « Women and Cyber » en mars, ou plus récemment l'« European Cyber Cup » lors du FIC. Des rencontres avec des écoles spécialisées (par exemple École 2600) sont aussi organisées. Chaque année, nous organisons un CTF interne permettant à l'ensemble des membres de la communauté d'échanger, de partager, de connaître les filiales du Groupe et de favoriser les mobilités internes. Enfin, chaque métier du Groupe développe des parcours de formation continue et certifiante sur la thématique cyber ■

Propos recueillis par Philippe Leroy

L'agence B2B au service de vos stratégies

Envie de booster votre performance marketing ? Contactez-nous !

WE FACTORY &co

hello@we-factoryandco.fr
01 41 31 72 44

ARCHITECTURE LOGICIELLE : LES CHOIX DE DECATHLON DIGITAL

Organisation, outillage, méthodologies... Voici comment Decathlon Digital déploie ses processus de décision en matière d'architecture logicielle.

AVEC QUOI GÉRER ses comptes rendus de décisions d'architecture ? Chez Decathlon Digital, anciennement appelée Decathlon Technology, plusieurs BU ont opté pour Structurizr. Cet outil open source propose un langage spécifique pour créer des « diagrammes en tant que code ». La société l'utilise aussi pour ses modélisations C4. Elle y a consacré un post, inscrit dans une présentation plus large de ses processus de décision en matière d'architecture logicielle.

Subsidiarité dans une « anarchie organisée »

En la matière, la vision s'inspire du « modèle de la poubelle », également dit « anarchie organisée ». Celui-ci postule, dans les grandes lignes, que les parties prenantes participent de façon

intermittente aux prises de décisions. Lesquelles résultent d'une combinaison aléatoire de problèmes, de solutions et de temporalités. D'où la métaphore de la corbeille, dans laquelle on jette de façon chaotique ces problèmes et ces solutions. Le modèle n'englobe pas toute la réalité des prises de décisions (évaluation des solutions alternatives et des conséquences de chaque solution, entre autres). Pour combler ce manque, Decathlon Digital a mis en place des comités d'architecture, au niveau des BU. Ces comités ne prennent pas les décisions pour les ingénieurs. Ils les aident à définir les problèmes et leur contexte, à comparer des solutions en assurant la conformité avec les lignes directrices du groupe... puis à documenter les décisions. Les chefs des comités d'architecture participent à des « Special Interest Groups », y font remonter les cas d'usage susceptibles d'aboutir à la création, ou à la mise à jour, de trois éléments internes : standards, radars technologiques et matrices de maturité. Les propositions qui ont le plus d'impact passent par une autre instance, un comité de supervision technique, composé de CTO et d'autres managers techniques seniors.
Sur cette chaîne, le principe de subsidiarité s'applique. Ainsi, toute décision n'affectant qu'une équipe doit, si possible, être prise à ce niveau. Le comité d'architecture intervient alors en tant que conseiller. Ses KPI sont essentiellement le niveau de satisfaction des ingénieurs (NPS), l'impact sur le SLO et les métriques DORA. Un tel mécanisme allonge les délais de décision, mais favorise l'inclusion des bonnes parties prenantes.

Du modèle C4 au « system thinking »

Pour associer la bonne méthodologie à chaque problème, Decathlon Digital utilise le modèle C4 (contexte, conteneur, composant, code). Pour un changement donné, les niveaux C4 impactés dictent la stratégie. La méthodologie retenue dépend des archétypes de problème (principale question : en connaît-on ou non les frontières ?). Le remplacement d'une dépendance par une autre dans un conteneur est un exemple de problème aux frontières définies. Il suppose effectivement des listes finies d'occurrences à modifier dans le code et de composants impactés. On peut le résoudre avec une approche réductionniste (linéaire). Au contraire, la refactorisation de plusieurs composants en interaction dans un conteneur n'a pas de frontière claire. Diviser le travail en une liste de tâches ne garantit pas la compatibilité de chaque décision avec l'output attendu. On adoptera une approche holistique examinant le lien entre toutes les portions du problème.
En combinant les deux approches, on tombe dans le « system thinking ». Un nouveau lien peut mettre en lumière une nouvelle perspective... et donner une nouvelle valeur à des solutions. Decathlon Digital donne l'exemple d'une amélioration de parcours client couvrant plusieurs systèmes. Le constat : le taux de conversion chutait du fait d'une expérience utilisateur incohérente entre deux applications. La première de type serveur, écrite en Svelte et bundlée avec Vite. La deuxième de type client, écrite en Svelte et bundlée avec Webpack.

Comment Decathlon Digital documente ses décisions

Parallèlement à la réflexion sur les solutions à adopter, on a demandé à l'équipe produit sa vision à long terme. Sa réponse : pour un bon moment, les pages allaient rester autonomes et les services, isolés. Après un certain temps, les composants pourraient interagir en mode cross-app. Le critère « pages autonomes » permit de fusionner trois problèmes en un (« applications Svelte et React autonomes et liées »). Combiné avec l'approche micro-front-end, on en est arrivé à « micro front-end vertical ». Et on y a associé des solutions : CSI (« Client Side Include »), SSI (« Server Side Include ») et ESI (« Edge Side Include »). À « page autonome », on a associé « composant ouvert », « composant web », « fédération native », « SingleSPA » et « iframes ». Puis on a identifié les principales synergies. Par exemple, la fédération native permet de construire une architecture qui supporte le rendu côté serveur et côté client, d'être compatible SSI et de passer à un micro-front-end horizontal. Pour documenter les décisions prises, Decathlon Digital emploie donc notamment Structurizr. Il y associe un générateur spécifique de sites statiques pour afficher les diagrammes. L'hébergement est centralisé. Une solution qui favorise autant le contrôle qualité que les références aux dépendances externes des systèmes (liens C1-C1 dans le modèle C4). La structure de gouvernance est récursive (BU, sous-BU, équipe, conteneur). À chaque couche, deux fichiers (model.dsl, views.dsl) et deux dossiers (adrs, docs). Séparer modèles et visualisations permet de mieux séparer les responsabilités et facilite l'import/export de compositions. ■

Par Clément Bohic

Decathlon en chiffres :

100 000
Plus de 100 000 salariés.

1 750
magasins dans 70 pays.

320
magasins en France.

14 Mds €
de chiffre d'affaires (25 % en France).

« L'IA est un incontournable, à plus d'un titre, en cybersécurité »

Olivier Ligneul, directeur cybersécurité du Groupe EDF

Le directeur cybersécurité du groupe EDF analyse comment l'IA a déjà largement impacté la cybersécurité et les usages du leader européen de la production d'énergie nucléaire.

L'intelligence artificielle devient inéluctable dans de nombreux métiers. En cybersécurité, est-ce un assistant loyal ou un maître dangereux ?

Olivier Ligneul - L'IA est un incontournable à plus d'un titre, en cybersécurité. C'est, d'une part, une technologie qui va être utilisée massivement par nos métiers, pour un certain nombre de finalités dont on ne connaît pas tous les développements. De ce point de vue là, on doit donc s'y intéresser. On doit vérifier les dangers, comment la présenter et comment, éventuellement, participer à sa régulation. Mais également, l'IA devient un outil formidable ou extrêmement dangereux pour les acteurs de la cybersécurité. Elle m'apporte déjà beaucoup de valeur ajoutée pour pouvoir faire notre travail, pour pouvoir démultiplier. Entre les mains d'attaquants, cet outil devient également très dangereux, lorsqu'il est exploité à des fins belliqueuses. L'automatisation existait déjà, mais l'IA permet de virtualiser toute une armée de malveillances. Un tout petit nombre d'individus peut ainsi coordonner des attaques d'envergure, sur lesquelles nous devons, pour le moins, nous interroger.

Des exemples de biais ou d'hallucinations en cybersécurité ?

Il ne faut pas faire croire que l'IA fera des choses qu'elle ne sera jamais capable de faire. Nous n'aurons pas l'IA des films *2001 l'Odyssée de l'espace*, *Terminator* et *Skynet*. Ceci étant dit, l'IA permet tout de même à son utilisateur d'avoir une sorte de conscience augmentée. Elle peut aussi devenir un outil très intéressant d'acculturation et de protection des patrimoines sensibles pour un RSSI.

Voyez-vous des perspectives d'améliorations dans vos environnements ?

Oui et pas seulement avec l'IA. Pour une meilleure intégration de la sécurité, je note que les automatisations, les mécanismes et moyens de gouvernance autour de l'IT et de l'OT [technologies d'exploitation] sont en train de se structurer. On attire l'attention des directeurs techniques et des directeurs organisationnels sur le pilotage sécurisé de leurs activités. De ce point de vue, cela ouvre davantage la communauté des RSSI à un ensemble d'acteurs du numérique et des objets connectés. On peut ainsi créer des ponts entre eux.

Faut-il redoubler de prudence face aux dépendances multiples entre systèmes IoT, systèmes industriels et systèmes informatiques ?

À mon avis, il faut surtout s'adapter aux contextes d'emploi. C'est l'approche que nous retenons au groupe EDF. Le contexte d'emploi d'une OT n'est pas celui d'une IT. La finalité d'un système industriel c'est de continuer à produire de manière constante. Les enjeux de l'IT sont plutôt la confidentialité, la massification, la standardisation et l'ouverture vers l'externe où certains mondes sont dangereux. On est plutôt assez convergent au sein du groupe EDF, où nous évoquons régulièrement la question, notamment avec les automaticiens. On constate un début de convergence technologique. Il y aura des contextes d'emploi différents, pendant un bon moment, mais du point de vue de la technologie et des acteurs, il est assez probable que cela converge.

La cybersécurité est-elle embarquée dès la conception des dernières centrales nucléaires ?

À l'époque où l'on a construit les premières centrales nucléaires, il n'y avait pas encore de cybersécurité by design. D'ailleurs, il n'y avait même pas d'IT ; on était plutôt dans l'électronique. Depuis, le monde a changé. À présent, la préoccupation de la cybersécurité est prise en compte, dans l'ensemble de nos ouvrages, dès la conception. Nos autorités ont légiféré et sont très intégrées dans les réflexions et dans les validations sur les différents éléments retenus en lien avec la cybersécurité. De la même manière, sur l'ensemble de nos travaux de construction et chantiers, on intègre aussi la cybersécurité dès qu'il y a un peu de numérique.

Les équipes EDF participent-elles à des cas d'usage ou aux projets de recherche cyber ?

Oui, notre entité de R&D compte 2 000 chercheurs, dont une cinquantaine d'ingénieurs en cybersécurité travaillant sur les méthodes formelles permettant de valider l'exécution d'algorithmes, sur les problématiques d'homomorphisme, ou sur la sécurité quantique. On se tient informé des évolutions technologiques et des résultats de la recherche académique. Un de nos centres de R&D a d'ailleurs été bâti à Saclay pour faciliter les collaborations avec d'autres centres de recherche, y compris dans le domaine de l'IA.

Pouvez-vous résumer votre parcours professionnel et vos responsabilités ?

D'abord, après un diplôme d'ingénieur, j'étais dans le monde des télécoms jusqu'à la fin des années 1990. Je travaillais alors autour des infrastructures réseaux et des datacenters. Plus récemment, j'ai travaillé autour de la cybersécurité, dans le cadre de mon intégration à l'ANSSI, fin 2009 dès la création de l'agence. Puis, pendant sept ans, d'abord en tant que responsable des activités de conseils et assistance, où j'ai accompagné plusieurs ministères. Après une forte cyberattaque, j'ai intégré le Secrétariat général des ministères économiques et financiers, jusqu'en 2015. À cette date, j'ai rejoint le groupe EDF où, comme directeur de la cybersécurité, je m'occupe de la cybersécurité de toutes les filiales et divisions du groupe, industrielles et IT.

Des missions associatives en complément ?

J'ai progressivement participé aux activités de l'écosystème cybersécurité. J'ai contribué à la création de TOSIT (« The Open Source I Trust »), une association qui regroupe de grandes entreprises et des ministères pour sécuriser les différents environnements open source. Au sein du Cesin, ce club de plus de 1 000 RSSI, je me concentre sur l'animation de la communauté des grandes entreprises et administrations. Enfin, président du club EBIOS qui promeut la méthode d'analyse de risques éditée par l'ANSSI, j'accompagne les évolutions de cette méthode. ■ *Propos recueillis par Olivier Bouzereau*

LES QUATRE MYTHES DU "ZERO TRUST"

Il est essentiel de démystifier les mythes sur la confiance zéro pour aider les organisations à les comprendre et à y remédier, afin d'aider les équipes à améliorer leur posture de sécurité et à mettre en œuvre le « Zero Trust » de manière plus efficace.

LE MODÈLE DE SÉCURITÉ « Zero Trust » repose sur le principe « ne jamais faire confiance, toujours vérifier ». Il s'agit d'une stratégie de sécurité dynamique visant à renforcer la cyber-résilience, qui part du principe que les menaces peuvent exister aussi bien à l'extérieur qu'à l'intérieur du réseau, éliminant ainsi l'approche traditionnelle basée sur la confiance qui se concentre uniquement sur les menaces externes. Le modèle est né parce que le modèle de confiance

« Si elle est bien appliquée, la confiance zéro réduit la complexité de la cybersécurité.

John Kindervag, fondateur de Zero Trust.

permet aux charges de travail malveillantes, qui contournent inévitablement le pare-feu, de se déplacer librement au sein du réseau et d'accéder aux données de grande valeur d'une organisation. Cette prise de conscience a conduit au développement d'un modèle qui élimine le concept de « confiance » dans les systèmes numériques, les organisations se rendant vulnérables aux violations de données, aux menaces internes et à une visibilité et un contrôle limités. Depuis plus de dix ans, le Zero Trust est un sujet de discussion majeur dans le domaine de la sécurité de l'information. Aujourd'hui, la situation est plutôt positive, car les organisations de tous les secteurs d'activité ont adopté le modèle de confiance zéro. Une étude de Forrester a révélé que 72 % des décideurs en matière de sécurité dans les grandes entreprises envisagent de lancer une initiative de confiance zéro, ou l'ont déjà fait. Toutefois, un certain nombre de facteurs et d'idées fausses ralentissent cette évolution.

Mythe 1 : le Zero Trust rend un système « fiable »

Dans le contexte de la confiance zéro, il ne s'agit pas de rendre les systèmes fiables, mais d'éliminer le concept de « confiance » de tous les systèmes informatiques.

Toutes les interfaces doivent avoir la même confiance : zéro ! Cela signifie que l'équipe accorde à chaque utilisateur, interface réseau et appareil le même niveau de confiance par défaut : zéro.

La confiance concerne exclusivement les individus et non les environnements numériques. Les informations d'identification sont susceptibles d'être compromises, les réseaux sont susceptibles d'être piratés et des personnes internes malveillantes occupent souvent des postes de confiance.

Lorsqu'un acteur externe malveillant accède au réseau interne, il devient automatiquement un « initié de confiance ». Cela lui permet d'exploiter le modèle de confiance à des fins malveillantes. Par conséquent, il est impossible de s'assurer que la source du trafic réseau est réellement « digne de confiance » : une identité revendiquée n'est qu'une revendication, et non la vérification d'une personne. Dans les cas des violations de données Snowden et Manning, il s'agissait d'utilisateurs « de confiance » qui utilisaient des appareils « de confiance ». Ils disposaient des niveaux de correctifs corrects et des correctifs mis à jour sur leurs appareils. Le réseau qu'ils ont compromis disposait de systèmes d'identité robustes et d'une authentification multifactorielle forte. Mais personne n'a vérifié les paquets après l'authentification. Ils ont exploité le « modèle de confiance » des réseaux gouvernementaux sur lesquels ils avaient des références.

Mythe 2 : le Zero Trust est une question d'identité

De nombreuses personnes commettent l'erreur de penser qu'une fois l'identité en place, elles ont achevé leur parcours de confiance zéro, mais ce n'est pas le cas. L'identité est consommée dans le cadre de la confiance zéro par le biais d'une politique, mais il y aura toujours un moyen de contourner l'identité. La confiance zéro reconnaît que le périmètre de sécurité traditionnel est devenu obsolète, mais considérer l'identité comme le ▶▶▶

VISION EXPERT

nouveau périmètre est problématique. Bien qu'il soit nécessaire de valider les attributs d'identité du paquet, nous ne pouvons pas utiliser ce seul point de données pour déterminer l'accès à une ressource. Un contrôle d'accès adéquat requiert des critères multiples. Les organisations ont plutôt besoin d'une approche holistique qui incorpore des données contextuelles, telles que l'heure de la journée, le type d'appareil, les contrôles de posture et les évaluations des risques. Dans un contexte de confiance zéro, les cinq questions suivantes doivent être posées : « Qui doit avoir accès à quelle ressource ? », « Quand cet accès doit-il être autorisé ? », « Où se trouve la ressource (la surface de protection) ? », « Pourquoi avons-nous mis en place cette politique (balises, étiquettes, classification des données ou autres métadonnées utiles) ? », et enfin « Comment examinons-nous le paquet pour décider si nous l'autorisons à accéder à la ressource ? ». C'est ce qu'on appelle la méthode Kipling. Le contexte ne doit pas être ignoré lorsqu'une organisation discute du contrôle d'accès. L'identité doit être prise en compte, puis des marqueurs contextuels avancés doivent être ajoutés pour garantir un accès sécurisé.

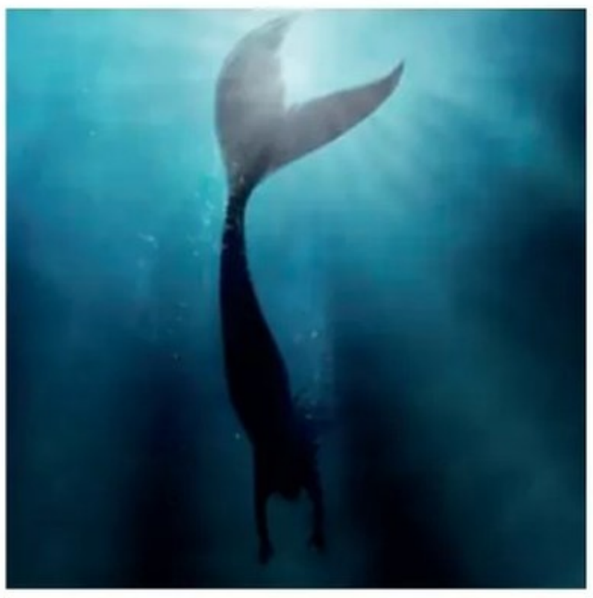
Mythe 3 : Il existe des produits de Zero Trust

La confiance zéro n'est pas un produit, c'est une stratégie, qui offre une grande flexibilité, car elle se concentre sur ce que l'organisation essaie de protéger, plutôt que sur la technologie. Il est important de noter que dans le cadre du Zero Trust, la stratégie et les tactiques sont découplées de par leur conception, car la stratégie ne change pas, mais les technologies s'améliorent de plus en plus au fil du temps. Cela signifie que les équipes de sécurité peuvent utiliser de nombreux outils

« La confiance zéro n'est pas un produit, c'est une stratégie qui se concentre sur ce que l'organisation essaie de protéger. »

72 %

des décideurs en matière de sécurité dans les grandes entreprises envisagent de lancer une initiative de confiance zéro ou l'ont déjà fait, selon Forrester.



pour mettre en œuvre des infrastructures de sécurité de confiance zéro. Cela signifie également que cette dernière ne nécessite pas une refonte complète des systèmes de sécurité existants. Au contraire, la technologie actuelle peut être utilisée pour soutenir le réflexe de la confiance zéro, en ajoutant de nouveaux outils si nécessaire.

Mythe 4 : le Zero Trust est trop difficile

Si elle est bien appliquée, la confiance zéro réduit en fait la complexité de la cybersécurité. En effet, cette approche est triple : incrémentale (une surface de protection à la fois), itérative (une surface de protection à la fois) et non perturbatrice (une seule surface de protection est le plus grand système qui peut être contesté à un moment donné). Les organisations devraient s'efforcer d'acquérir une certaine maturité en se concentrant sur leurs surfaces de protection les plus sensibles, au lieu d'essayer de tout faire en même temps, faute de quoi elles ne feront jamais de progrès significatifs.

Gérer le Zero Trust

La confiance zéro est une stratégie préconisée par les gouvernements et les régulateurs comme étant la seule véritable solution pour atténuer l'impact des cyberattaques sophistiquées. Elle rend très difficile la compromission d'un système et vise à détruire le mythe répandu dans le secteur de la sécurité selon lequel les équipes de cybersécurité doivent empêcher toutes les intrusions, une mission qui est tout simplement irréalisable. Le Zero Trust n'empêche pas les intrusions, mais les violations de données, que des réglementations telles que le RGPD définissent comme la suppression non autorisée de données sensibles du réseau. C'est indéniablement la meilleure stratégie de sécurité pour les environnements modernes qui sont devenus de plus en plus complexes, distribués et sans périmètre.

Il est essentiel de démystifier les mythes sur la confiance zéro pour aider les organisations à les comprendre et à y remédier, afin d'aider les équipes à améliorer leur posture de sécurité et à mettre en œuvre le Zero Trust de manière plus efficace. ■

Par John Kindervag, fondateur de Zero Trust

ABONNEZ VOUS !

INSIGHTS FOR IT PROFESSIONALS

-30%

Silicon

La solution d'information qui comprend :

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

boutique.editialis.fr/marketing-commercial/silicon

BULLETIN D'ABONNEMENT

OUI, je m'abonne pour 1 an à **Silicon** au prix de ~~120 €~~ **84 €**

Silicon

À remplir et retourner à :
ABOMARQUE
CS 60003
31242 L'UNION CEDEX
Tél. : 05 34 56 35 60
(du lundi au vendredi de 10h à 12h et de 14h à 17h)

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

❑ Mme ❑ M.

Nom : .....

Prénom : .....

Fonction : .....

Société : .....

Adresse : .....

.....

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

Ville : .....

Pays : .....

Tél. : .....

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

Offre valable en France métropolitaine jusqu'au 30/10/2024

Je joins mon règlement par :

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

❑ Carte bancaire n° :

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

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

SIGNATURE

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

L'HÔPITAL AMÉRICAIN DE PARIS PLANIFIE SON STOCKAGE À LONG TERME

Les performances évolutives et les mécanismes de protection de la donnée offrent aux 335 médecins de l'établissement de santé une continuité d'accès aux données des patients et aux soins prodigués.

« CEINTURE, *bretelles et parachute. On ne se prive pas de mettre en place de la sécurité autour de nos données numériques »,* résume Adrien Bournat, le directeur technique de l'Hôpital américain de Paris. L'organisme à but non lucratif reconnu d'utilité publique, où exercent 335 médecins de toutes les spécialités médicales majeures, met à leur disposition des équipements avancés d'imagerie et une flopée d'indicateurs de performances. *« Par une constante amélioration de notre système d'information, nous cherchons à offrir une prise en charge d'excellence à nos patients, et à la fois un vrai confort de travail pour nos médecins de notoriété internationale. Ils s'attendent à avoir la meilleure infrastructure possible pour délivrer un service de premier ordre avec 80 applications métiers destinées aux soignants. Le parc informatique compte 140 applications en tout, dont la gestion électronique de documents est hébergée en interne pour préserver les textes et comptes-rendus médicaux »,* précise le CTO.

Stockage et dossiers patients informatisés

Le facteur de longévité des données reste essentiel aux activités de l'établissement, les données des patients devant être conservées durant deux décennies. L'infrastructure précédente de

20 ans

C'est la durée de conservation des données des patients.

« Nos sessions de travail, nos analyses des besoins et notre accompagnement ont convaincu l'établissement d'adopter une solution performante et pérenne. »

Yann Chalhoub, directeur des activités Data Services & Solutions de SPIE ICS.

stockage SAN (« Storage Area Network ») arrivait en fin de vie, ce qui se manifestait par des performances dégradées et une volumétrie incompatible avec la croissance des activités de l'hôpital. *« Notre volumétrie ne diminuera pas. Nous avons beau essayer de faire des efforts de gestion du cycle de vie de la donnée et respecter l'environnement autant que possible, il nous est impossible de détruire les données patients avant 20 ans. Nos efforts passent donc par l'excellence opérationnelle, via un taux de déduplication élevé »*, détaille Adrien Bournat. Et de préciser : *« Nous sensibilisons toujours les utilisateurs à tous les niveaux, afin qu'ils soient plus alertes sur ces sujets et adoptent une bonne hygiène informatique. Notre enjeu, en cette année 2024, consiste à mettre en place et à tester notre plan de continuité informatique. Il s'articule autour de deux salles informatiques au sein de l'hôpital, avec des serveurs redondants et un stockage croisé à base de solutions PureStorage. Les deux salles sont dimensionnées de sorte que l'une absorbe la charge de l'autre, dès que cela s'avère nécessaire. »*

Performances et volumétries évolutives

La migration technique des équipements de stockage, déployés sur deux salles, a duré près de quatre mois. Avant de lâcher sa précédente baie SAN, la direction technique a tenu à interviewer des clients du constructeur américain pour vérifier quelques critères de conception et d'exploitation. *« Il s'avère que la solution PureStorage, au travers du contrat Evergreen, permet de faire évoluer tous les trois ans les contrôleurs, mais aussi la capacité de stockage, de manière indépendante. Nos entretiens avec l'intégrateur SPIE ICS et ses clients nous ont rassurés. Nous devrions avoir moins de pertes de performances dans le temps, sans basculer vers une infrastructure hyperconvergente, nos serveurs de machines virtuelles ayant déjà été renouvelés préalablement. On espère aussi en finir avec la routine usuelle de remplacement des baies SAN tous les sept à huit ans »*, indique Adrien Bournat.

Des perspectives de nouveaux services

Le dimensionnement, la mise en place et la sécurisation des solutions de stockage reste un chantier structurant qui exige expertise et précision. *« Nous cherchons sans cesse à mettre en place de nouveaux services. Nous développons un nouveau portail innovant afin que chaque patient puisse suivre son parcours dans l'établissement, avec tous les processus internes expliqués. Notre roadmap prévoit des traitements pour les soignants, la sécurisation des soins, la prévention et le soutien de recherches médicales. Nous travaillons aussi sur un datalake avec la startup Arkhn pour optimiser nos indicateurs de performances. Et nous devons aussi garantir la cybersécurité »*, énumère le directeur technique. Pour Yann Chalhoub, directeur des activités Data Services & Solutions de SPIE ICS, la refonte de l'infrastructure de stockage a permis de s'étendre aux missions de sauvegarde, de cybersécurité, au soutien des utilisateurs du corps soignant et à l'amélioration de la hotline. *« Nos sessions de travail, nos analyses des besoins et notre accompagnement ont permis de convaincre l'établissement qu'il pouvait partir, avec nous, sur une solution de stockage performante et pérenne qui réponde à leurs projets, à leurs objectifs techniques et financiers. »* ■

Par Olivier Bouzereau

« Notre parc informatique compte 140 applications dont la gestion électronique de documents qui est hébergée en interne. »

Adrien Bournat, CTO Hopital americain de Paris.

COMMENT RANSOMHUB PROSPÈRE SUR LES CENDRES DE LOCKBIT ET BLACKCAT

Le FBI met en garde contre la croissance rapide du gang RansomHub, dont les affiliés ont piraté au moins 210 organisations depuis février.

DES AFFILIÉS DU GANG RANSOMHUB ont mené des attaques contre au moins 210 organisations depuis février, ont averti les autorités américaines. RansomHub fonctionne sur un modèle d'infrastructure en tant que service, où les affiliés utilisent son infrastructure pour compromettre une cible et crypter ses systèmes, exigeant une rançon pour fournir une clé de décryptage. Comme c'est de plus en plus courant, les affiliés de RansomHub exfiltrent également des données et menacent de les rendre publiques si la rançon n'est pas payée.

Différents affiliés utilisent diverses méthodes pour exfiltrer des données, ont déclaré le FBI, la Cybersecurity and Infrastructure Security Agency (CISA) et deux autres agences dans un avis commun. Les affiliés ont, selon l'avis, ciblé un large éventail de secteurs, notamment l'eau, l'informatique, le gouvernement, la santé, les services d'urgence, l'agriculture, les services financiers, la fabrication critique, le transport et les infrastructures de communication critiques.

Les cibles comprenaient la coopérative de crédit Patelco, la chaîne de pharmacies Rite Aid, la maison de vente aux enchères Christie's, le fournisseur de télécommunications Frontier Communications et le géant des services pétroliers Halliburton, qui a révélé dans un dossier SEC qu'il avait été compromis le 21 août. Le gang, anciennement connu sous le nom de Cyclops et Knight, *« s'est imposé comme un modèle de service efficace et réussi »*, ont déclaré les agences.

La croissance rapide de RansomHub est en partie due à la disparition de deux groupes majeurs plus tôt cette année, ont-ils déclaré : LockBit, qui a été perturbé par une action policière internationale en février, et AlphV, également connu sous le nom de BlackCat, qui a fermé ses portes en mars. Les fournisseurs d'infrastructures de ransomware reçoivent normalement le paiement avant d'envoyer la part due à l'affilié qui a mené l'attaque, mais les affiliés doivent faire confiance au fournisseur pour leur envoyer leur part.

RansomHub sur les traces de Lockbit et BlackCat

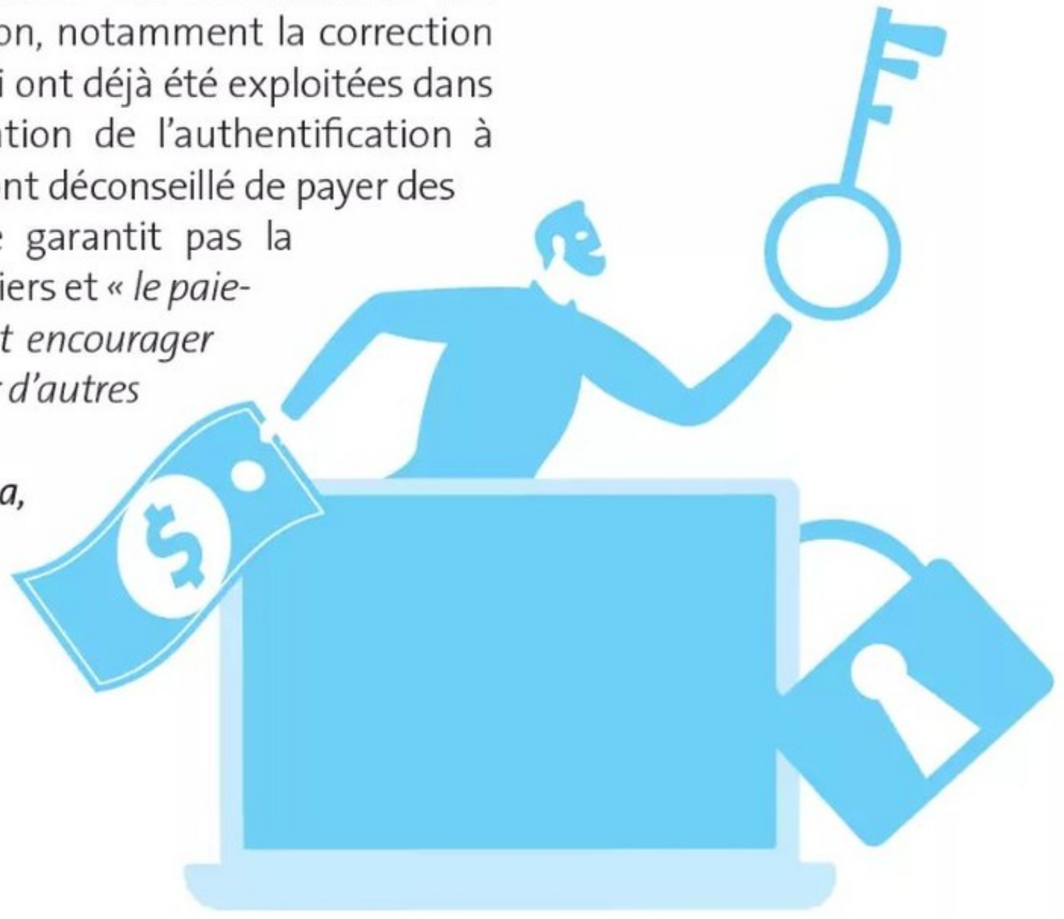
En mars, ce système a pris un coup avec la disparition du gang AlphV, également connu sous le nom de BlackCat, qui aurait reçu un paiement de 22 millions de dollars du fournisseur de paiements de soins de santé américain Change Healthcare, avant de disparaître sans payer son affilié. RansomHub permet aux affiliés de percevoir eux-mêmes les paiements, ce qui rend l'opération d'autant plus attrayante pour les anciens affiliés d'AlphV, ont déclaré des experts en sécurité.

Les agences américaines ont recommandé des mesures d'atténuation, notamment la correction des vulnérabilités qui ont déjà été exploitées dans la nature et l'utilisation de l'authentification à deux facteurs. Elles ont déconseillé de payer des rançons car cela ne garantit pas la récupération des fichiers et *« le paiement peut également encourager les adversaires à cibler d'autres organisations »*. ■

Par Matthew Broersma, Silicon UK

30 %

C'est la progression des attaques informatiques à des fins d'extorsion contre les entreprises françaises entre 2022 et 2023, selon l'ANSSI.



VOUS AVEZ LA VALEUR ?

Vous avez même incliné la tête.

Contactez-nous en
scannant ce QR code

Vos futurs clients aussi !

La prochaine fois, communiquez dans

Silicon
INSIGHTS FOR IT PROFESSIONALS

TATA COMMUNICATIONS

TATA

Réinventer la sécurité et la **performance** de votre réseau avec **HOSTED SASE**

SIMPLIFIEZ
votre transition vers SASE
avec une plateforme de gestion centralisée.

BÉNÉFICIEZ
d'une connectivité fiable,
assurant des performances constantes et optimales.

PROTÉGEZ
vos données et vos opérations
avec une sécurité proactive.

DIMINUEZ
votre TCO
jusqu'à 40%.

Pour plus d'informations, rendez-vous sur notre site.