N°199 – Septembre 2021

www.linformaticien.com

L'INFORMATICIEN

CLOUD & INFRA

Euclidia veut faire briller le logiciel européen

TRANSFO

ManoMano, Maisons du Monde, Younited Credit...

EMPLOI

Certification Cloud : le ticket gagnant pour booster une carrière

COMMENT PEGASUS VOLE... LES DONNÉES

HPC as a Service

Le calcul intensif sur le Cloud !

CYBERSÉCURITÉ

Contrer le risque de **Supply Chain Attack**

DEVOPS

Booster les **tests logiciels** par l'IA

Logitech Scribe : la caméra qui connecte le tableau blanc

Prenez le contrôle des cyber-incidents complexes

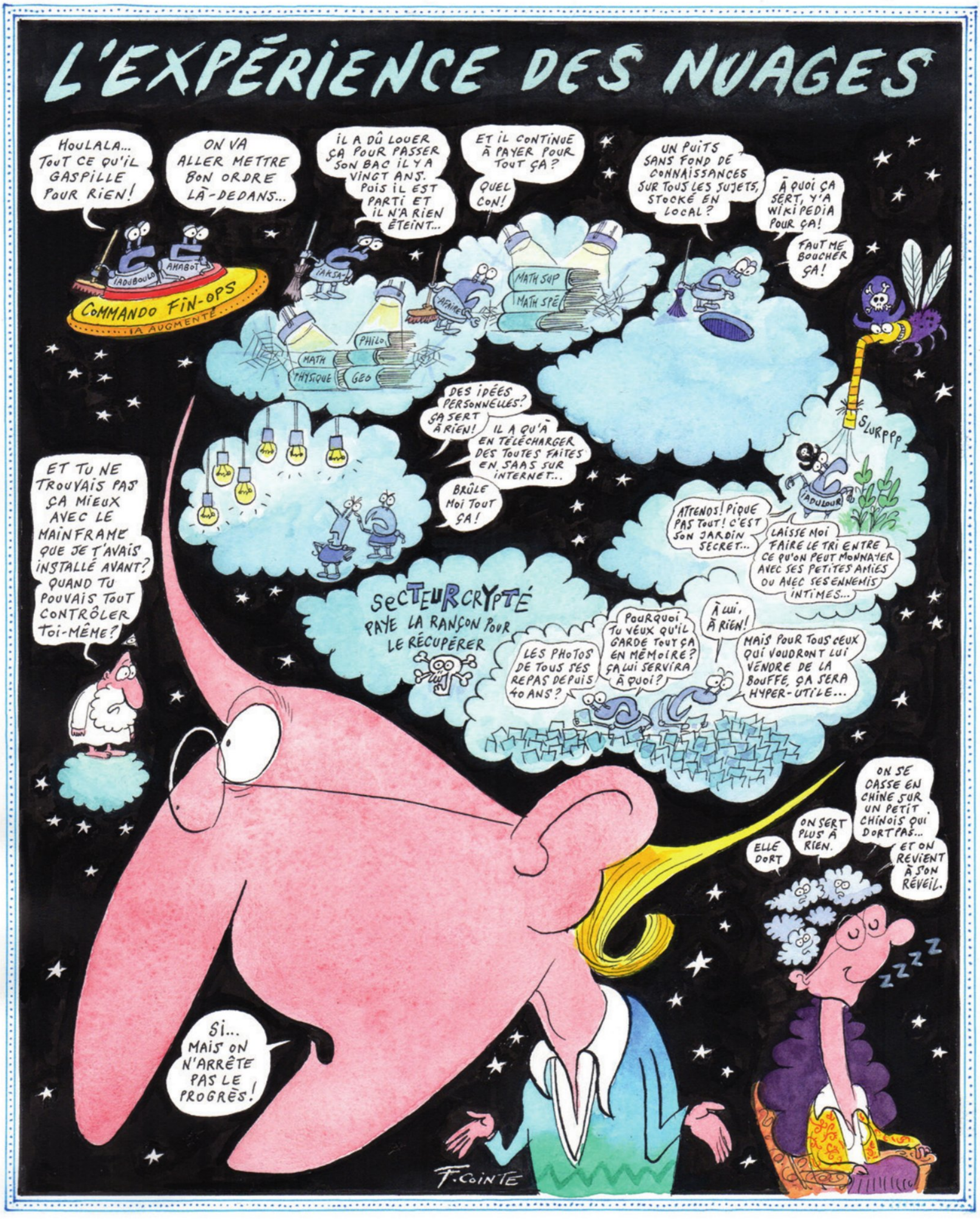
Renforcez la puissance de votre équipe cybersécurité avec des technologies de pointe enrichies par des renseignements de haut niveau sur les menaces, des connaissances et les conseils des meilleurs experts.

kaspersky.fr/enterprise-security

kaspersky BRING ON THE FUTURE

© 2021 AO Kaspersky Lab. Bring on the future : Bienvenue dans le futur.

COINTE


L'EXPÉRIENCE DES NUAGES
HOULALA... TOUT CE QU'IL GASPILLE POUR RIEN!
ON VA ALLER METTRE BON ORDRE LÀ-DEDANS...
IAOUBOULO
AHABOT
COMMANDO FIN-OPS
...IA AUGMENTÉ...
IL A DÛ LOUER ÇA POUR PASSER SON BAC IL Y A VINGT ANS. PUIS IL EST PARTI ET IL N'A RIEN ÉTEINT...
IAKSA-
AFAIRE
PHILO
MATH
PHYSIQUE
GEO
ET IL CONTINUE À PAYER POUR TOUT ÇA?
QUEL CON!
MATH SUP
MATH SPÉ
UN PUITS SANS FOND DE CONNAISSANCES SUR TOUS LES SUJETS, STOCKÉ EN LOCAL?
À QUOI ÇA SERT, Y'A WIKIPEDIA POUR ÇA!
FAUT ME BOUCHER ÇA!
SLURPPP
IADULOUR
DES IDÉES PERSONNELLES? ÇA SERT À RIEN!
IL A QU'À EN TÉLÉCHARGER DES TOUTES FAITES EN SAAS SUR INTERNET...
BRÛLE MOI TOUT ÇA!
ATTENDS! PIQUE PAS TOUT! C'EST SON JARDIN SECRET...
LAISSE MOI FAIRE LE TRI ENTRE CE QU'ON PEUT MONNAYER AVEC SES PETITES AMIES OU AVEC SES ENNEMIS INTIMES...
ET TU NE TROUVAIS PAS ÇA MIEUX AVEC LE MAINFRAME QUE JE T'AVAIS INSTALLÉ AVANT? QUAND TU POUVAIS TOUT CONTRÔLER TOI-MÊME?
SECTEURCRYPTÉ PAYE LA RANÇON POUR LE RÉCUPÉRER
LES PHOTOS DE TOUS SES REPAS DEPUIS 40 ANS?
POURQUOI TU VEUX QU'IL GARDE TOUT ÇA EN MÉMOIRE? ÇA LUI SERVIRA À QUOI?
À LUI, À RIEN!
MAIS POUR TOUS CEUX QUI VOUDRONT LUI VENDRE DE LA BOUFFE, ÇA SERA HYPER-UTILE...
ELLE DORT
ON SERT PLUS À RIEN.
ON SE CASSE EN CHINE SUR UN PETIT CHINOIS QUI DORT PAS...
ET ON REVIENT À SON RÉVEIL.
ZZZZZ
SI... MAIS ON N'ARRÊTE PAS LE PROGRÈS!
F. COINTE

VOUS VOUS SURPASSEZ POUR FAIRE ÉVOLUER VOTRE BUSINESS.

NOUS AUSSI.

Diriger une entreprise en pleine croissance est une aventure. Les conseillers Dell Technologies sont là pour vous aider avec des solutions IT adaptées à chaque étape. Ainsi, rien ne peut vous arrêter.

Contactez un conseiller Dell Technologies
au **0801 800 001*** ou chattez via **WhatsApp****

DELL Technologies

XPS 13 avec Windows 10 Pro

Windows 10

Faites-en plus avec un ordinateur dernière génération équipé de Windows 10 Professionnel.

© 2021 Dell Inc. ou ses filiales. Tous droits réservés. Dell Technologies, Dell, EMC, Dell EMC et d'autres marques sont des marques de Dell Inc. ou de ses filiales. Dell SAS Capital 1 946 545,26 €, Siège Social 1 rond-point Benjamin Franklin 34000 Montpellier. France. N° 351 528 229 RCS Montpellier –APE 4651Z. Photos non contractuelles. Dell n'est pas responsable des erreurs de typographie ou de photographie. Pour plus de renseignements, merci de bien vouloir contacter notre équipe commerciale. Les Conditions Générales de Vente et de Services de Dell s'appliquent. Vous pouvez les consulter à l'adresse www.dell.fr.
*De 9h à 18h du lundi au vendredi (Numéro Vert Gratuit)
**De 9h à 18h du lundi au vendredi (des frais de connexion à internet peuvent s'appliquer)

www.linformaticien.com

L'INFORMATICIEN

RÉDACTION

5, rue Saulnier, 75009 Paris, France.
Tél. : +33 (0)1 74 70 16 30
contact@linformaticien.fr

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

SECRÉTAIRE DE RÉDACTION : Jean-Marc Denis

MAQUETTE ET RÉALISATION : Franck Soulier (chef de studio) avec Aurore Guerguerian
Illustrations vectorielles : Designed by Freepik

PUBLICITÉ

Tél. : +33 (0)1 74 70 16 30
pub@linformaticien.fr

VENTE AU NUMÉRO

France métropolitaine 6 € TTC (TVA 5,5 %)

ABONNEMENTS

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

Toutes les offres :
www.linformaticien.com/abonnement

Pour toute commande d'abonnement d'entreprise ou d'administration avec règlement par mandat administratif, adressez votre bon de commande à :
L'Informaticien, service abonnements,
5, rue Saulnier, 75009 Paris, France
ou à abonnements@linformaticien.fr

IMPRESSION

Imprimé en France par Imprimerie Chirat (42)
Dépôt légal : 3e trimestre 2021

Toute reproduction intégrale, ou partielle, faite sans le consentement de l'auteur ou de ses ayants droit ou ayants cause, est illicite (article L122-4 du Code de la propriété intellectuelle).
Toute copie doit avoir l'accord du Centre français du droit de copie (CFC), 20 rue des Grands-Augustins 75006 Paris. Cette publication peut être exploitée dans le cadre de la formation permanente.
Toute utilisation à des fins commerciales de notre contenu éditorial fera l'objet d'une demande préalable auprès du directeur de la publication.

L'INFORMATICIEN est publié par PC PRESSE, S. A. S. au capital de 130 000 euros.
Siège social : 5, rue Saulnier, 75009 Paris, France.

ISSN 1637-5491

Une publication PCpresse,

GROUPE FICADE

PRÉSIDENT, DIRECTEUR DE LA PUBLICATION :
Gaël Chervet

Édito

« Orwell, reviens ! Ils sont vraiment tous fous »

L'époque est décidément de plus en plus formidable. En cette rentrée 2021, alors que l'épidémie liée à la Covid19 semble ne jamais vouloir se terminer, se succèdent des informations toujours plus inquiétantes pour le contrôle des libertés et la soi-disant sécurité de tous.

Quelques exemples récents. En Australie, le Parlement vient d'autoriser la police fédérale et les enquêteurs criminels à prendre le contrôle et investiguer les comptes et réseaux des criminels sans qu'il soit nécessaire d'obtenir l'autorisation d'un juge. Le problème vient de l'interprétation qui pourrait être faite du vocable « criminels ». De leur côté, les autorités australiennes mettent en avant les 290 arrestations liées à l'opération IronSide menée conjointement par les services américains et australiens au cours de laquelle ils avaient introduit une faille dans un logiciel de messagerie utilisé par les criminels.

En Chine, le contrôle de l'activité « en ligne » des mineurs subit un nouveau tour de vis. Déjà limités à une heure et demie de jeu par jour en semaine, et trois heures pendant les vacances, les nouvelles restrictions sont désormais de trois heures de jeux autorisées par semaine afin de préserver les mineurs de ce qui est qualifié *d'opium intellectuel* par les autorités chinoises. Le marché chinois du jeu en ligne étant désormais le premier du monde avec un chiffre d'affaires de 45 milliards de dollars par an, les entreprises travaillant dans ce secteur ont subi une correction de leur cours boursier.

Mais tout ceci n'est rien à côté de l'énorme problème qu'ont laissé les Américains derrière eux en quittant l'Afghanistan. On ne parle pas du matériel militaire mais d'une gigantesque base de données biométrique permettant de retracer les visages des personnes au moyen de 36 points de captation et pas moins de 40 champs, dont le parcours ou la spécialité militaire de chacun de ces 500 000 enregistrements. Selon Technology Review qui rapporte cette information, cette base de données est *« connue sous le nom d'APPS, ou Afghan Personnel and Pay System. Utilisé à la fois par le ministère afghan de l'Intérieur et le ministère de la Défense pour payer l'armée et la police nationale, il s'agit sans doute du système le plus sensible du genre dans le pays, pénétrant dans les moindres détails sur le personnel de sécurité et leurs réseaux étendus ».* Les Américains ont indiqué qu'ils avaient pris des précautions afin que les données ne tombent pas dans les mains des Talibans mais des témoignages venus du terrain suggèrent l'inverse.

Une nouvelle illustration du proverbe qui veut que, pour dîner avec le diable, il vaut mieux se munir d'une très longue cuillère… ✖

La Rédaction

VOTRE PARTENAIRE CERTIFICATIONS

CERTyou

+ 33 1 42 93 52 72
www.certyou.com
contact@certyou.com

FORMATIONS EN INFORMATIQUE ET MANAGEMENT

COBIT 5 AN ISACA® FRAMEWORK · IIBA · ISTQB · ITIL® APPROVED EXAMINATION ORGANIZATION · PMI Project Management Institute · PRINCE2® APPROVED EXAMINATION ORGANIZATION · Scrum.org

SOMMAIRE

N°199 – Septembre 2021

À LA UNE

Comment Pegasus vole… les données ! ..... **p. 8**

BIZ'IT

Cybersécurité : les géants de la tech promettent des investissements massifs ..... **p. 14**

Microsoft monte les prix d'Office et de Microsoft 365 ..... **p. 15**

L'Institut national de l'information géographique et forestière (IGN) ouvre ses données ..... **p. 15**

Vers une taxation des multinationales ..... **p. 16**

Agenda IT : les prochains événements à ne pas manquer ..... **p. 16**

Levées de fonds Bubble, Algolia, Spendesk, Cybereason, Netskope... **p. 18**

Iliad sort de la Bourse… … SAS s'apprête à y entrer ..... **p. 19**

TRANSFO

La transformation numérique par le Cloud

▶ **ManoMano** se libère de l'infrastructure ..... **p. 21**

▶ La stratégie globale de migration de **Maisons du Monde** ..... **p. 23**

▶ **Younited Credit** envoie son ERP dans le Cloud ..... **p. 25**

NXO : histoire d'une résurrection .... **p. 26**

Munich Re modernise ses espaces de travail ..... **p. 27**

Le long chemin de la transformation numérique ..... **p. 28**

CYBERSÉCURITÉ

Comment contrer le risque de Supply Chain Attack ..... **p. 30**

FIDO2, un standard qui s'impose ..... **p. 34**

IMT et Airbus Security font bonne chaire ..... **p. 36**

TACTIC

Les yeux plus grands que le ventre .. **p. 39**

CLOUD & INFRA

HPC as a Service : pourquoi le Cloud bouscule les supercalculateurs ..... **p. 42**

Le Lakehouse prend ses aises ..... **p. 46**

Euclidia veut faire briller le logiciel européen ..... **p. 50**

Customs Bridge s'appuie sur OVH pour développer sa solution ..... **p. 52**

Au Computex : Laptops, desktops et serveurs font le show ! ..... **p. 54**

DEVOPS

Booster les tests logiciels par l'IA ..... **p. 58**

EMPLOI

Certification cloud : le ticket gagnant pour booster une carrière .... **p. 64**

Logitech Scribe
La caméra qui connecte le tableau blanc ..... **p. 66**

Offres d'abonnement ..... **p. 63**

Comment Pegasus vole… les données

Apple n'a cessé de vanter et de vendre ses systèmes d'exploitation comme les plus sûrs au monde. L'affaire Pegasus démontre, au contraire, que loin d'être invulnérables, iOS et MacOS peuvent être attaqués, avec des conséquences lourdes sur la vie privée de leurs utilisateurs. Si la plupart de ces failles sont demeurées secrètes, certains éléments publiés permettent de comprendre comment Pegasus réussit à s'infiltrer jusqu'au cœur de smartphones réputés imprenables.

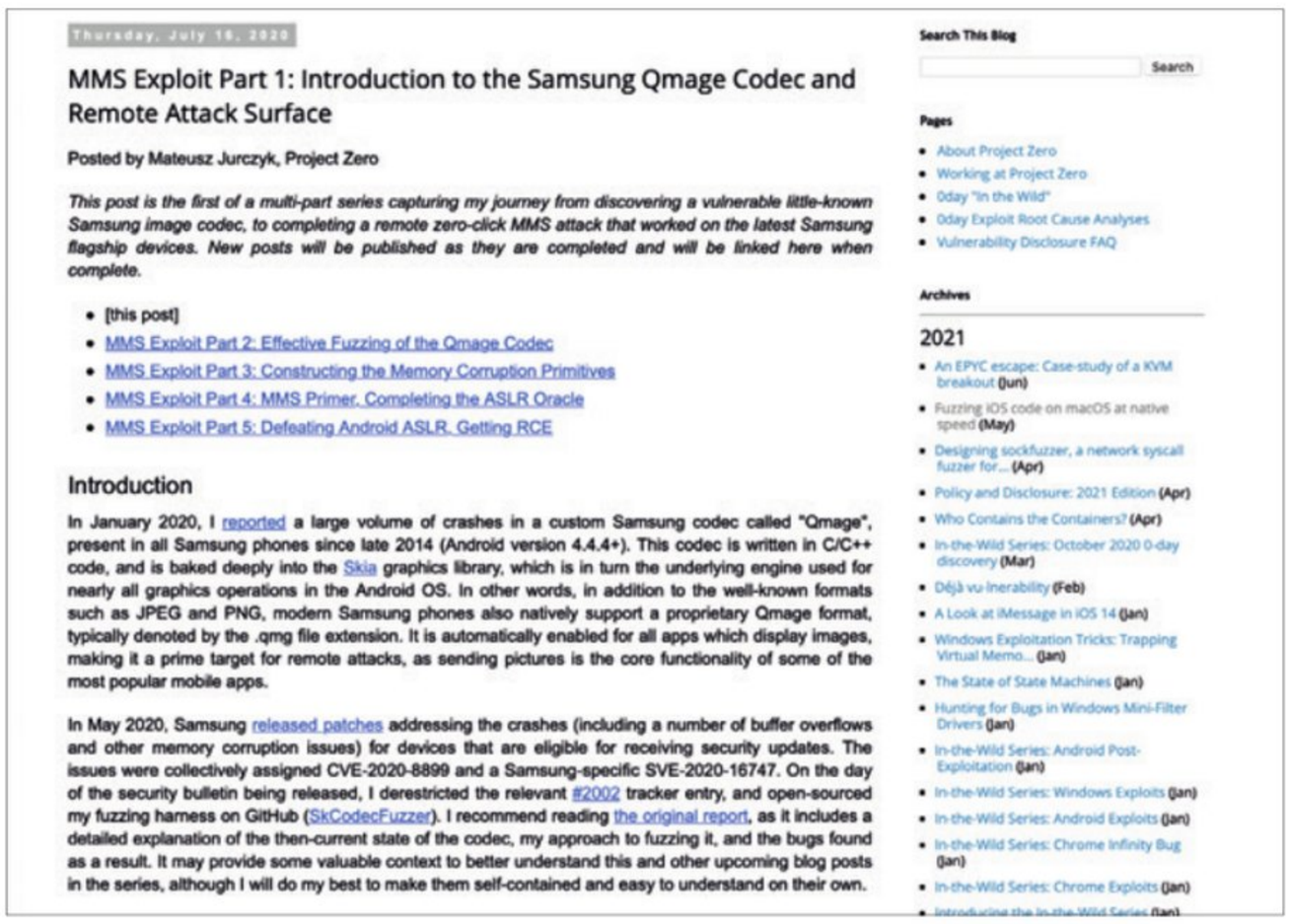
Quand on demande aux utilisateurs avertis quels sont les systèmes d'exploitation les plus sûrs qu'ils connaissent, on peut parier qu'ils répondront soit MacOS, soit Linux. Rares sont ceux qui songerait à citer Windows, a priori. Il faut dire que le produit phare de Microsoft n'a cessé, au long des années, de donner une piètre image de ses performances, rythmées par les nombreux bugs et autres écrans bleus qui furent – et sont parfois encore – le quotidien de ses utilisateurs.

Il faut cependant faire attention, car nous avançons ici en terrain miné. La mauvaise réputation de *Windows* résulte avant tout de son instabilité. Certes, le système d'exploitation compte de nombreuses failles ; mais ce que les utilisateurs subissent au quotidien relève plus du syndrome du crash aléatoire que de la cyberattaque – même si, malheureusement, ces dernières – les ransomware, entre autres – tendent à se multiplier. Il convient de soigneusement distinguer instabilité et sécurité. Un système peut crasher toutes les cinq minutes, tout en garantissant une sécurité absolue. La réciproque est également possible : un système qui ronronne se révèlera n'être qu'une *vulgaire* passoire.

Aux yeux du profane, la plupart du temps ces deux notions se confondent : stabilité rime avec sécurité. Cette opinion ne repose sur aucun fondement factuel, juste une sensation. Le discours marketing d'Apple se nourrit de cette sensation de sécurité faussement éprouvée par les utilisateurs de Mac et d'iPhone, qu'il n'hésite pas à qualifier de *« machines les plus sûres du monde »*. Le même sentiment d'impunité affecte également, pour d'autres raisons, les utilisateurs de Linux. Il est vrai que ces deux systèmes ont jusqu'ici été relativement peu ciblés par les attaques ; il ne faudrait cependant pas voir dans cette immunité une conséquence de la qualité de leur code, mais plutôt le constat d'une réalité économique : avec des parts de marché assez faibles, le bénéfice tiré d'éventuelles cyberattaques sur ces plates-formes ne compense pas l'investissement économique, assez lourd, nécessaire à l'identification puis l'exploitation des vulnérabilités. Mais les choses changent, et *l'affaire Pegasus* en est un bon exemple.

L'exemple de la vulnérabilité CVE-2016-4656

On peut se demander comment, en l'espace de quelques cycles CPU, une application malveillante arrive à prendre le contrôle total d'un téléphone tant vanté pour sa sécurité et sa robustesse, pour le transformer en parfaite petite « balance » ? Si le mécanisme de pénétration des versions les plus récentes de Pegasus n'a pas été rendu public, certains groupes de *white hackers* ont analysé des failles par lesquelles ce même logiciel avait déjà réussi, il y a cinq ans, à forcer les barrières érigées par les développeurs d'Apple. L'exemple le mieux documenté est lié à la mise à jour iOS 9.3.5 de 2016, correspondant à la faille dénommée CVE-2016-4656. Apple ne publie jamais les détails de ses patches, pour éviter que des



Thursday, July 16, 2020

MMS Exploit Part 1: Introduction to the Samsung Qmage Codec and Remote Attack Surface

Posted by Mateusz Jurczyk, Project Zero

This post is the first of a multi-part series capturing my journey from discovering a vulnerable little-known Samsung image codec, to completing a remote zero-click MMS attack that worked on the latest Samsung flagship devices. New posts will be published as they are completed and will be linked here when complete.

- [this post]
- MMS Exploit Part 2: Effective Fuzzing of the Qmage Codec
- MMS Exploit Part 3: Constructing the Memory Corruption Primitives
- MMS Exploit Part 4: MMS Primer, Completing the ASLR Oracle
- MMS Exploit Part 5: Defeating Android ASLR, Getting RCE

Introduction

In January 2020, I reported a large volume of crashes in a custom Samsung codec called "Qmage", present in all Samsung phones since late 2014 (Android version 4.4.4+). This codec is written in C/C++ code, and is baked deeply into the Skia graphics library, which is in turn the underlying engine used for nearly all graphics operations in the Android OS. In other words, in addition to the well-known formats such as JPEG and PNG, modern Samsung phones also natively support a proprietary Qmage format, typically denoted by the .qmg file extension. It is automatically enabled for all apps which display images, making it a prime target for remote attacks, as sending pictures is the core functionality of some of the most popular mobile apps.

In May 2020, Samsung released patches addressing the crashes (including a number of buffer overflows and other memory corruption issues) for devices that are eligible for receiving security updates. The issues were collectively assigned CVE-2020-8899 and a Samsung-specific SVE-2020-16747. On the day of the security bulletin being released, I derestricted the relevant #2002 tracker entry, and open-sourced my fuzzing harness on GitHub (SkCodecFuzzer). I recommend reading the original report, as it includes a detailed explanation of the then-current state of the codec, my approach to fuzzing it, and the bugs found as a result. It may provide some valuable context to better understand this and other upcoming blog posts in the series, although I will do my best to make them self-contained and easy to understand on their own.

Search This Blog

Search

Pages

- About Project Zero
- Working at Project Zero
- 0day "In the Wild"
- 0day Exploit Root Cause Analyses
- Vulnerability Disclosure FAQ

Archives

2021

- An EPYC escape: Case-study of a KVM breakout (Jun)
- Fuzzing iOS code on macOS at native speed (May)
- Designing sockfuzzer, a network syscall fuzzer for... (Apr)
- Policy and Disclosure: 2021 Edition (Apr)
- Who Contains the Containers? (Apr)
- In-the-Wild Series: October 2020 0-day discovery (Mar)
- Déjà vu lnerability (Feb)
- A Look at iMessage in iOS 14 (Jan)
- Windows Exploitation Tricks: Trapping Virtual Memo... (Jan)
- The State of State Machines (Jan)
- Hunting for Bugs in Windows Mini-Filter Drivers (Jan)
- In-the-Wild Series: Android Post-Exploitation (Jan)
- In-the-Wild Series: Windows Exploits (Jan)
- In-the-Wild Series: Android Exploits (Jan)
- In-the-Wild Series: Chrome Infinity Bug (Jan)
- In-the-Wild Series: Chrome Exploits (Jan)

Extrait du blog du projet groupezero de Google. Ce dernier publie régulièrement de nouvelles failles de sécurité sur les différents systèmes et la manière de les exploiter ou de les corriger.

groupes malveillants ne profitent des informations avant que tous les utilisateurs aient eu le temps d'installer un correctif. A posteriori cependant, il est possible de savoir quels éléments du noyau ont été modifiés en comparant les deux versions binaires successives. En principe, le binaire du noyau ne devrait pas être lisible. Effectivement, celui d'iOS 9 était protégé par un triple mécanisme : le binaire était crypté, et seul le firmware savait à quel endroit se trouvait la clef de décryptage[1]. De plus, à chaque mise en route du téléphone, le noyau se plaçait à une adresse RAM aléatoirement choisie : le décalage entre l'adresse théorique du noyau et son adresse réelle est appelée « KASLR ». Enfin, le noyau résidait évidemment en mémoire superviseur, à laquelle les applications n'ont normalement pas accès.

Alors, comment faire ? En pratique, le mécanisme de décryptage du noyau d'iOS 9 avait une faiblesse : il décryptait toujours le code au même endroit en mémoire superviseur *(kernel cache)*, puis copiait le résultat à l'adresse définitive une fois le KASLR déterminé. Il suffisait donc de gagner accès à l'espace superviseur pour récupérer non seulement le code du noyau, mais les symboles qui allaient avec et qui indiquaient où résidait chaque fonction. Gagner cet accès, quitte à lire le noyau octet par octet, n'était pas très complexe, comme le prouve la suite. Une liste de failles plus récentes, dont certaines permettent de calculer le KASLR, est disponible sur le blog du projet Zéro de Google : *https://googleprojectzero.blogspot.com*.

La plupart de ces failles utilisent des mécanismes de bas niveau du noyau, une tâche simplifiée par le fait que Apple publie une grande partie de ses noyaux en Open Source sous le nom XNU. Comme toute arme à double tranchant, la publication du code permet également à des auditeurs externes de repérer des failles avant que celles-ci ne soient exploitées.

Deux failles différentes dans une seule fonction

Dans le cas de la CVE-2016-4656, le mécanisme de bas niveau utilisé exploite deux erreurs dans la fonction *OSUnserializeBinary*. Cette dernière sert à créer en mémoire une instance d'un objet de type conteneur (liste, dictionnaire…) à partir d'une représentation binaire – objet dit sérialisé. La première vulnérabilité réside dans l'absence de contrôle de la longueur des valeurs de type *kOSSerializeNumber*, autrement dit, de la longueur utilisée pour stocker un entier dans l'objet sérialisé. Cette omission permet de construire une instance sérialisée malveillante comportant une entrée *kOSSerializeNumber* de longueur quelconque.

Il suffit d'utiliser cette pseudo-instance dans un appel noyau pour ouvrir une fenêtre d'accès à la mémoire superviseur qui va permettre de casser le KASLR. On utilise pour cela la fonction *io_service_open_extended*. Elle n'est pas documentée par Apple (API privée), mais apparaît dans le code source de XNU, qui, rappelons-le, est *open sourced*. Ces API privées n'implémentent généralement pas le même niveau de sécurité que les API publiques.

Une fois l'instance frauduleuse créée et enregistrée par le noyau, il suffit de lire ses propriétés à l'aide d'une autre fonction privée *(io_registry_entry_get_property_bytes)*.

Cette fonction se fie aux tailles des sous-instances spécifiées dans l'instance : si celles-ci sont anormalement grandes, la fonction renverra un nombre quelconque d'octets de la pile, où résident les variables dynamiques… mais aussi les adresses de retour des appels aux fonctions. Or, puisque nous avons accès à la table des symboles du noyau, nous connaissons l'adresse de base de chaque fonction. Récupérons, dans les données « fuitées », l'adresse de la fonction appelante modifiée par le KASLR, et nous en déduisons par une simple soustraction la valeur de ce dernier et *« bingo !»*

Il reste maintenant à prendre le contrôle du système. Facile ! C'est l'objet de la deuxième partie de la vulnérabilité CVE-2016-4656. Celle-ci exploite une faille

1 Ce mécanisme de chiffrement du noyau a été abandonné avec iOS 10.

appelée « utilisation après libération » : autrement dit, un accès illicite à la mémoire utilisée par une instance alors que cette dernière est censée avoir été effacée. Ce bug va permettre de créer une instance truquée qui va servir à effectuer un *su root* sans vérification.

Dans le détail, le code d'*OSUnserializeBinary* devrait libérer les espaces mémoire provisoires utilisés pour construire au fil de l'eau les instances des sous-objets du conteneur et invalider toutes les références à ces zones. Mais dans le cas d'un sous-objet de type chaîne, si le code libère correctement la mémoire (*free*), il garde une référence valide sur la zone libérée (pas d'appel à *release*). Là-dessus, la politique de l'allocateur de mémoire de MacOS/iOS (appelé *zalloc*) consiste à ré-allouer prioritairement les derniers blocs libérés. En créant une fausse instance sérialisée contenant une chaîne quelconque de taille *ad-hoc*, puis juste derrière une instance de type *raw data* remplie de zéros, nous allons conduire iOS à créer une fausse instance d'objet chaîne vide, sur laquelle nous garderons un pointeur valide.

```
case kOSSerializeNumber:
    bufferPos += sizeof(long long);
    if (bufferPos > bufferSize) break;
    value = next[1];
    value <<= 32;
    value |= next[0];
    o = OSNumber::withNumber(value, len);
    next += 2;
    break;
```

Le code fautif de la fonction OSUnserializeBinary. Comme on le voit, à aucun moment le paramètre len ne fait l'objet d'un contrôle de pertinence – il peut donc prendre n'importe quelle valeur. [Source : https://jndok.github.io]

Prise de contrôle de la page 0

Qu'allons-nous faire de cette instance vide ? Les ABI des compilateurs C++ indiquent que les adresses des méthodes virtuelles se trouvent dans un espace appelé *vtable*, qui réside en tête de la mémoire dédié à l'instance. Le cas qui nous intéresse ici est celui de la méthode virtuelle *retain* (nous verrons pourquoi plus loin), héritée de *OSObject*, et utilisée pour incrémenter le compteur de référencement d'une instance. Il est facile de déterminer à quel offset de la *vtable* se trouve l'adresse de la méthode *retain* (il suffit pour cela d'examiner une instance de la classe de base). Ici, on trouve 32. Comme notre instance ne contient que des zéros, cela signifie que, sur appel de la méthode *retain*, le système d'exploitation se branchera à l'adresse indiquée à la position mémoire 0 (celle de la *vtable*) + 32 (*offset* de *retain*) = 32. À nous d'écrire à cette adresse un pointeur vers le code que nous souhaitons voir exécuter par le noyau.

En règle générale, ce scénario d'attaque ne fonctionne pas, car la plupart des systèmes d'exploitation interdisent l'accès à la « page 0 », qui contient les adresses virtuelles de 0 à 4096[2]. Mais la version 32-bit d'iOS n'implémente pas cette politique, pour des raisons de compatibilité. Un code très simple permet donc d'écrire n'importe quelle valeur dans la page 0, à condition de le compiler en mode 32-bit et d'utiliser l'option de compilation *-pagezero_size,0*.

À l'adresse 32, nous aurons 0. Nous allons donc placer à l'adresse 0 un minuscule bout de code *(gadget)* qui ira écraser le pointeur de pile (RSP), puis exécutera l'instruction *ret* et ainsi transférera l'exécution dans une zone de mémoire plus vaste contenant la suite de notre code. Celui-ci élèvera les privilèges de la tâche courante, simulant ainsi un *su root*. Cette tactique de transfert d'exécution s'appelle « attaque ROP » *(Return-Oriented Programming)*.

Dernière étape : faire en sorte que notre piège soit déclenché par un code exécuté en mode superviseur – requis si nous voulons modifier la structure de description de la tâche, qui contient, entre autres, son UID. *OSUnserializeBinary* nous offre cette possibilité : les sous-objets d'un conteneur peuvent en effet contenir des références à d'autres sous-objets du même conteneur. Il va donc suffire d'ajouter une telle référence sur l'instance chaîne vérolée pour déclencher automatiquement un appel à sa méthode *retain*. Bingo de nouveau ! Il ne reste plus qu'à appeler une fonction du noyau qui prendra comme argument l'objet sérialisé forgé, par exemple *io_service_get_matching_services_bin*, pour activer le piège. Au retour de l'appel, le processus courant aura son UID égal à 0 *(root)*, donc la faculté d'accéder librement à toutes les ressources système.

Un marketing ennemi de la sécurité ?

Comme on le voit, il suffit d'un minuscule trou de souris pour ouvrir les portes du système en grand ! Prétendre qu'un système d'exploitation, c'est-à-dire souvent plusieurs dizaines, voire centaines de milliers de lignes de code, ne contient aucune vulnérabilité de ce type, c'est aussi prétentieux que d'affirmer ne jamais avoir conduit au-dessus de la vitesse limite. Ces vulnérabilités ne sont pas évidentes à identifier, mais il semble que NSO, la société israélienne qui édite le *spyware Pegasus*, n'a pas lésiné sur les moyens pour constituer une équipe d'auditeurs compétents capable de les localiser. Plus compétents que ceux d'Apple, en tout cas, si l'on en croit l'historique de la

2 Ceci évite, par exemple, une vulnérabilité potentielle lors du dé-référencement d'un pointeur NULL.

DIRECT SOFTWARES

ÉLIMINEZ VOS SERVEURS D'IMPRESSION

Votre parc d'impression mobilise trop votre temps et vos ressources ?

Vous êtes responsable informatique ? alors vous savez que la gestion des copieurs et des imprimantes vous prend trop de temps.

Déployer les matériels, gérer les drivers, support utilisateur, assurer la stabilité depuis une session virtuelle (TSE / Citrix). Ajoutés à cela le trafic réseau et le budget serveur.

Pourquoi cette situation ? Un seul coupable, votre architecture basée sur le serveur d'impression.

Et si vous modernisiez et sécurisiez votre environnement ?

L'alternative ? C'est la suppression de vos serveurs d'impression, basculez vers l'impression directe IP avec gestion centralisée.

Une seule interface pour l'administration et le support de tout votre parc, quelle que soit la marque ou les OS utilisés.

Des jobs d'impression qui restent sur le réseau local, pas besoin de réseau ni VPN.

Une disponibilité améliorée et un temps de support et d'administration réduit de 60%.

La bonne nouvelle ? le retour sur investissement se fait dès la première année dans plus de 90% des cas et le déploiement en moins de 5 jours.

Rejoignez des centaines d'entreprises et éliminez vos serveurs d'impression.

Démarrez un essai gratuit dès maintenant

mydyalog.com

dyalog

Simplifions ensemble
la gestion des parcs d'impression

ARMOR PRINT SOLUTIONS

correction de cette vulnérabilité : le premier *patch* publié ne réglait que partiellement le problème, il a dû être suivi dans la foulée d'un second correctif. Examiner un code pour en déceler les faiblesses nécessite du temps et de l'expertise. Si Apple a les moyens de s'offrir l'expertise, depuis la mort de Steve Jobs le géant californien a fait le choix marketing regrettable de sortir une version majeure de ses systèmes d'exploitation tous les ans, au lieu de tous les deux ans auparavant.

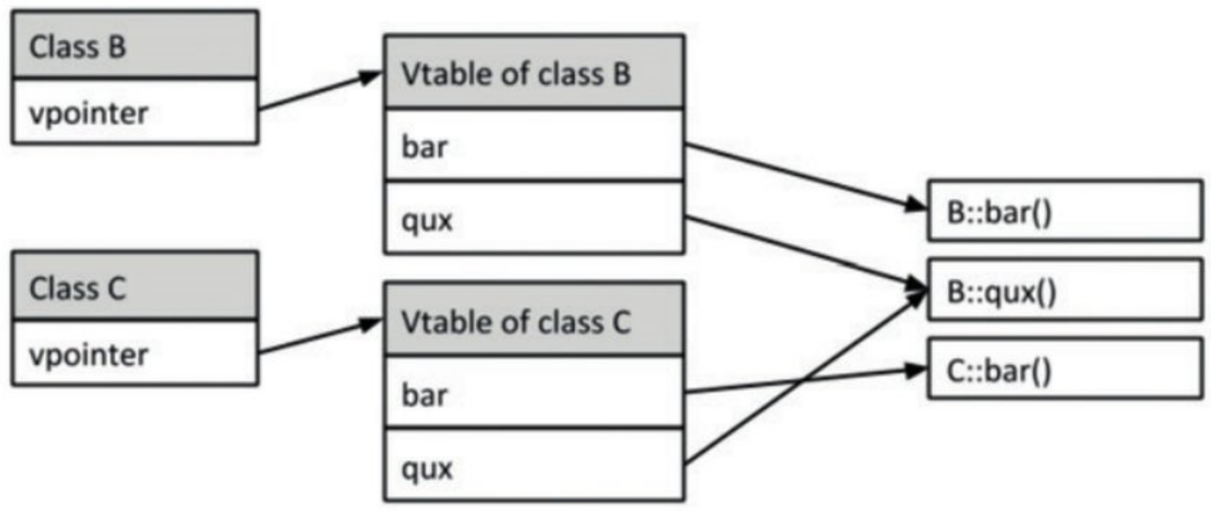
Résultat : non seulement les nouveautés proposées sont souvent cosmétiques et décevantes, mais les équipes de développeurs font face à une pression accrue, ont moins de temps pour tester et relire le code, dont la qualité se détériore. En face de cela, rien ne semble indiquer que Apple a renforcé ses équipes d'auditeurs sécurité, et la société ne peut pas toujours compter sur la bonne volonté d'auditeurs externes pour jouer les pompiers.

On pourra aussi incriminer le choix douteux d'incorporer dans le noyau du code C++ *(IOKit)* au milieu d'une base robuste écrite en C. La vulnérabilité que nous venons de discuter, qui exploite directement la *vtable*, n'aurait pas existé si le code de l'IOKit avait été écrit en C, qui n'est pas un langage orienté objet [3].

Des contre-mesures inefficaces

La découverte de traces de Pegasus dans des iPhones tournant la dernière version d'iOS indique clairement que toutes les failles n'ont pas été corrigées, ou que d'autres ont été ouvertes ailleurs, possiblement dans les applications pré-installées. On ne pourra qu'admirer – d'un point de vue théorique – le travail des analystes de NSO, car, contrairement au code du noyau, qui est public, celui des applications n'est pas divulgué, ce qui complique singulièrement la découverte des vulnérabilités.

3 Probablement la raison pour laquelle les noyaux des systèmes UNIX de type BSD sont toujours écrits en pur C.



Exemple de stockage en mémoire de deux objets C++, B et C, le second héritant du premier. La recherche du code des méthodes s'effectue au travers d'une table de pointeurs de fonctions appelée vTable. La fonction qux, héritée mais non-modifiée, n'est pas dupliquée : les pointeurs des vTables de B et de C sont identiques.

Face à ces « effractions » répétées, les contre-mesures prises par Apple relèvent plus du *« sparadrap sur la fracture »* que du véritable travail de fond. La mise en place du système *csr/sip* sur MacOS, par exemple, permet d'éviter, entre autres, qu'un processus root ne puisse effacer des fichiers jugés essentiels au système. Malheureusement, d'une part il n'est pas certain que ce dispositif ne soit pas contournable, par exemple en ré-écrivant des routines d'E/S disque : est-ce la raison pour laquelle Apple n'a pas communiqué sur le format de son nouveau *file system* APFS, rendant tous les utilitaires disques tiers inopérants, et, d'autre part, certains utilisateurs pourraient souhaiter effacer des applications *(Stocks, Home, Stickies, Photo Booth, Automator…)* dont ils n'ont pas besoin, ce qui n'est plus possible sauf à désactiver le mécanisme par une procédure lourde et peu documentée.

Autrement dit, il en va ici comme dans la vie courante : plutôt que d'investir dans une véritable politique de sécurité – audit fouillé et correction du code –, on préfère restreindre la liberté des utilisateurs. Tout cela afin de préserver un sentiment de confiance propice à la marque.

Du côté de l'iPhone, le système BlastDoor, inauguré avec iOS 14, et qui était censé protéger les utilisateurs d'iMessage contre des intrusions via des SMS malveillants, n'aura pas empêché NSO de s'engouffrer dans une faille « zero day » (initiale), suffisamment grave pour une nouvelle fois permettre à Pegasus de prendre le contrôle du téléphone et ce, apparemment, sans même que l'utilisateur n'ait à ouvrir le message incriminé. BlastDoor serait-il lui même à l'origine de cette vulnérabilité ?

Que faut-il retenir de tout cela ? Qu'il n'y a pas de panacée en cybersécurité. Plus un système est complexe, plus il est exposé, et plus les données qu'on lui confie seront en danger, quand bien même son fabricant vous affirme farouchement le contraire. Si vous souhaitez passer des communications et des SMS en toute confidentialité, faites comme les espions : achetez un petit téléphone à clapet vendu quelques euros, surtout sans accès à la data, accompagné d'un abonnement téléphonique prépayé et d'un carnet d'adresses papier. Et revendez votre smartphone sur un site spécialisé. ✖

Vincent Habchi

Cette article s'inspire directement de l'–unique– article du blog https://jndok.github.io. On y trouvera également une liste assez complète de lien permettant d'obtenir de plus amples informations techniques. On pourra aussi consulter le blog du groupe allemand « Sektion Eins » à l'adresse https://www.sektioneins.de/en/categories/blog.html

WWW.SIDO-EVENT.COM

#SIDO2021

Les événements
de la convergence
des technologies IoT, IA,
XR et Robotique pour
la transformation numérique
des entreprises !

LYON
PARIS

sido

IoT – AI – ROBOTICS – XR

SIDO Lyon

22 > 23 septembre 2021

Cité internationale
250 Exposants
60 Conférences

Créer votre badge gratuit
-> www.sido-lyon.com

SIDO Paris

09 > 10 novembre 2021

Palais des Congrès
150 Exposants
60 Conférences

Créer votre badge gratuit
-> www.sido-paris.com

Showroom + Conférences + Networking,

2 rendez-vous pour 2 x plus de business

Usine du futur, E-Santé, Transport Intelligent, Supply Chain, Environnement, Energies et Utilities, Agriculture connectée, Banque, Secteur public, Infrastructure du Numérique... et bien d'autres !

SUIVEZ-NOUS SUR NOS RÉSEAUX !

@SIDOevent
@SIDO_Paris

SIDO Lyon
SIDO Paris

SIDO Event

sido.event

DES ÉVÉNEMENTS

65

INFOPRO digital

Les infos premières du mois

Cybersécurité : Les géants de la tech promettent des investissements massifs

FOCUS

Le 25 août, le président américain Joe Biden a rencontré les principaux dirigeants du secteur américain du numérique. Étaient ainsi présents Tim Cook, Arvind Krishna et Sundar Pichai, ainsi que le patron de JP Morgan et d'autres dirigeants de banques et de compagnies d'assurance, de même que des représentants d'associations. Contrairement à ce que cet illustre aréopage peut laisser penser, il ne s'agissait pas d'une réunion au sujet de l'antitrust et des pratiques monopolistiques des gens, mais bien d'un sommet sur la cybersécurité.

Car les États-Unis, comme de nombreux autres pays, sont sous le feu. Aussi bien les collectivités et les administrations fédérales que le secteur privé subissent attaque après attaque. Colonial Pipeline n'est qu'un exemple parmi d'autres, et quel exemple ! Si le géant de l'acheminement de combustible fossile assurait que les stocks étaient suffisants, sa paralysie a provoqué une certaine panique sur la Côte Est, les files de voitures s'allongeant devant les stations-services de la Floride à l'Illinois.

Vous pouvez le faire !

L'heure est donc grave, selon le *President of The United States*. *« La réalité est que la plupart de nos infrastructures essentielles appartiennent et sont exploitées par le secteur privé, et le gouvernement fédéral ne peut pas relever ce défi seul »*, a ainsi déclaré Joe Biden avant le sommet. *« Nous avons vu à maintes reprises comment les technologies sur lesquelles nous comptons, de nos téléphones portables aux pipelines jusqu'au réseau électrique peuvent devenir la cible de pirates informatiques et de criminels. »* Puis, s'adressant aux dirigeants réunis autour de lui : *« Vous avez le pouvoir, la capacité et la responsabilité, je crois, de relever la barre en matière de cybersécurité. »* Ce n'est pas la première action dans ce domaine décidée par la Maison Blanche depuis le début du mandat. Le président a publié en mai un décret exécutif sur la modernisation de la protection des systèmes informatiques du gouvernement fédéral. En juillet, c'est un mémorandum présidentiel qui venait fixer des objectifs, non obligatoires, quant à la cybersécurité des infrastructures critiques.

Cette réunion du 25 août visait à poursuivre cet effort consistant à faire de la cybersécurité une priorité nationale. *« L'objectif de la réunion était de discuter des opportunités de renforcer la cybersécurité du pays en partenariat et individuellement »* indiquait la Maison Blanche dans un résumé des discussions. L'administration a mené la danse en annonçant que le NIST *(National Institute of Standards and Technology)* allait travailler avec le secteur privé de sorte à élaborer un nouveau cadre qui fournira aux secteurs privé et public les lignes directrices de la sécurisation des technologies et des infrastructures, un projet auquel Microsoft, IBM et Google collaborent.

Les entreprises présentes se sont quant à elles livrées à une véritable surenchère d'annonces, notamment financières. Apple, qui entend mettre en œuvre un nouveau programme d'amélioration de la sécurité de sa supply chain, semble bien timoré en comparaison des autres Gafam. Google assure ainsi qu'il investira 10 milliards de dollars au cours des cinq prochaines années pour étendre les programmes Zero Trust, sécuriser la supply chain logicielle et améliorer la sécurité des logiciels libres, tout en formant 100 000 Américains à la cybersécurité. Petit joueur !, aurait pu s'exclamer alors IBM. Big Blue formera 150 000 personnes sur trois ans, en s'associant notamment à des écoles majoritairement afro-américaines pour diversifier les ressources humaines dans le secteur de la cyber. Microsoft, jetant un regard plein de mépris sur ses camarades, annonçait de son côté un investissement de 20 milliards de dollars dans la cybersécurité au cours des cinq prochaines années. Et 150 millions de dollars de services techniques à l'attention des administrations fédérale, étatiques et locales. Pour sa part, Amazon mettra à la disposition du public gratuitement la formation de sensibilisation à la sécurité qu'il offre déjà à ses employés. Il fournira également l'authentification multi-facteur aux utilisateurs d'AWS sans surcoût.

Microsoft monte les prix d'Office et de Microsoft 365

FOCUS

Redmond profite de la rentrée pour annoncer des prix à la hausse. Ses suites Office 365 et Microsoft 365 connaîtront à partir du 1er mars 2022 une hausse substantielle de leur tarif. La première depuis 2011, justifie Jared Spataro, vice-président chargé de Microsoft 365. *« Cette mise à jour des prix reflète la valeur accrue que nous avons offerte à nos clients au cours des dix dernières années »*, explique-t-il dans un post de blog. Il souligne ainsi l'arrivée il y a quatre ans de Microsoft 365 et de Teams, puis de Power Apps, Power BI, Power Automate, OneDrive, Yammer, etc., ainsi que *« plus de 1 400 nouvelles fonctionnalités et capacités »*. *« En cours de route, nous avons continuellement réinvesti pour répondre aux besoins changeants de nos clients »*, ajoute-t-il. Ce qui justifie ladite augmentation de prix. Ainsi, à compter du 1er mars prochain, Microsoft 365 Business Basic passera de 5 à 6 dollars par utilisateur, tandis que la version *Business Premium* grimpera de 20 à 22 dollars. Microsoft 365 E3 prend 4 dollars dans la vue, de 32 à 36 dollars. Du côté d'Office 365, la version E1 passe de 8 à 10 dollars, l'E3 de 20 à 23 et enfin l'E5 de 35 à 38 dollars. À noter que ces augmentations ne concernent que les versions pro et entreprise des suites de Microsoft, les prix des moutures grand public et éducation demeurent inchangés. Redmond fait en outre remarquer que ces changements tarifaires s'appliqueront à l'échelle mondiale *« avec des ajustements du marché local pour certaines régions »*.

L'Institut national de l'information géographique et forestière ouvre ses données

FOCUS

Accompagnant la mise à disposition gratuite de ses données, l'IGN lançait le 1er janvier dernier le site geoservices.ign.fr. Ce site, complémentaire du géoportail, s'adresse aux professionnels de la géomatique et aux utilisateurs de cartographie numérique. De nombreux types de données sont disponibles dont le fond de plan de référence de l'IGN pour les usages professionnels sur mobile, site web et SIG, la modélisation 2D et 3D du territoire et de ses infrastructures sur l'ensemble du territoire français, l'image géographique du territoire national, la France vue du ciel, un référentiel géographique forestier pour les professionnels de la filière bois et pour les acteurs de l'environnement et de l'aménagement du territoire métropolitain, le modèle numérique de terrain (MNT) maillé qui décrit le relief du territoire français à grande échelle, la version numérique de la carte au 1:25 000.

Pour visualiser des données et des cartes ou réaliser des géo-traitements dans des applications et des sites internet, les services web sont désormais accessibles sans inscription ; il suffit d'utiliser les URL d'accès prêtes à l'emploi et en libre-service. S'il est ainsi mis fin aux clés d'accès, une clé active au 20 juillet 2021 reste utilisable jusqu'au 1er février 2022 inclus, afin de laisser suffisamment de temps pour migrer vers les URL en libre accès.
Le site propose une présentation par usage dans différents secteurs d'activités : agriculture, aménagement du territoire, climat, défense, éducation, innovation et numérique, télécoms, transports et mobilité, tourisme, etc. Une mise en perspective de l'information géographique est proposée en fonction du domaine sélectionné, appuyée par des exemples d'usages, de témoignages d'utilisateurs, et des suggestions de données et de services adaptés. Les modalités d'hébergement des données IGN sont amenées à évoluer au cours des prochains mois et le site Géoservices ouvre dans une période de transition. Le service de téléchargement en particulier pourra connaître des limitations compte tenu des contraintes de capacité actuelles.

Vers une taxation des multinationales

FOCUS

C'est réunis mi-juillet dans une Venise vidée de ses touristes que les ministres des Finances du G20 sont parvenus à un accord sur une taxation à hauteur de 15 % des bénéfices des multinationales dans les pays où ils sont réalisés, un mois après un « accord historique » du G7. *« Après quatre ans de combat acharné avec le président de la République, c'est acté : nous mettons fin à l'optimisation fiscale et les géants du numérique paieront enfin leur juste part d'impôt. C'est la plus grande révolution fiscale depuis un siècle »*, a immédiatement tweeté Bruno Le Maire.

Le projet est encore perfectible, aussi bien en termes de modalités d'application que de critères de taxation. Ainsi, comment taxer les bénéfices réalisés dans un pays mais déclarés dans un autre, à la fiscalité plus clémente et qui ne se sentira sans doute pas concerné par cette taxe de 15 % ? Ils sont encore sept à l'OCDE à s'opposer à cette taxation, dont trois Européens : la Hongrie, l'Estonie et, sans surprise, l'Irlande !

Pour Bruno Le Maire, il est certain que la France récupérera la différence, mais sans préciser par quel moyen. Le sujet est à l'étude au sein de l'OCDE, sans qu'une solution idéale ne se détache pour l'heure. Autre souci, le taux de 15 % ne s'applique pas à toutes les multinationales. Première condition : elles ne seront prélevées sur leur bénéfices qu'à la condition qu'elle fasse plus de 10 % de marge. Ce trimestre, la marge nette d'une petite PME internationale du nom d'Amazon s'élevait à… 6,42 %.

Bref, il reste du travail à faire, bien que, aux yeux du G20, s'il n'est pas indispensable que tous les pays soient signataires, le poids des 19 pays les plus riches du monde, des 132 pays de l'OCDE et de l'UE, pourrait bien suffire à faire fléchir les récalcitrants. Mieux encore, les moteurs de cet accord que sont la France, l'Allemagne et les États-Unis espèrent que le taux finalement adopté soit supérieur aux 15 % proposés. De même, pour la redistribution locale des bénéfices, ils penchent en faveur d'un taux à 25 %. Mais il fallait également composer, au G20, avec cette petite controverse qui monte et qui risque de faire capoter l'accord. Les États-Unis, par la voix de la Secrétaire au Trésor Janet Yellen, ont chargé le projet de la Commission Européenne d'une taxation de 0,3 % sur les ventes en ligne dans le cadre du financement du plan de relance. Ce que Washington voit comme discriminatoire à l'égard de ses entreprises, doublement taxées, demandant à l'UE d'abandonner le projet ; un avis partagé par plusieurs États membres. Le ton est monté, les États-Unis assurant que cette taxe sur les ventes en ligne risque de « faire dérailler complètement » les discussions sur la taxe internationale. Au lendemain du G20, Janet Yellen se rendait alors à Bruxelles. Et, au terme de la rencontre, la Commission s'inclinait. *« La réussite de ce processus nécessitera une dernière impulsion de la part de toutes les parties, et la Commission s'est engagée à se concentrer sur cet effort. C'est pourquoi nous avons décidé de mettre en pause notre travail sur une proposition de taxe numérique »*, expliquait un porte-parole de l'institution européenne. Du moins jusqu'à l'automne, sachant que les discussions de l'OCDE doivent s'achever en octobre et que, en fonction des résultats des négociations, *« la Commission entend relancer ce débat public à l'automne »*, sur le cadre de gouvernance économique.

L'agenda IT

TESTS LOGICIELS

13e édition de la Journée Française des Tests Logiciels le **14 SEPTEMBRE** à Montrouge (Beffroi).

DREAMFORCE

Événement mondial annuel de Salesforce du **21 AU 23 SEPTEMBRE** sur invitation à San Francisco et en ligne (inscription gratuite).

SIDO LYON

Événement IoT, IA, robotique & XR les **22 ET 23 SEPTEMBRE** à Lyon, Cité internationale.

BIG DATA & AI

Deux événements regroupés en un seul les **28 ET 29 SEPTEMBRE** à Paris, Palais des Congrès.

SALONS SOLUTIONS

Le rendez-vous ERP, CRM, démat, BI, etc., se tient les **5 ET 6 OCTOBRE** à Paris, Porte de Versailles.

LES ASSISES DE LA SÉCURITÉ

Les experts de la cybersécurité ont rendez-vous du **13 AU 16 OCTOBRE** à Monaco, Grimaldi Forum.

CYBER SECURITY

Le salon de la sécurité numérique des entreprises vous attend le **23 NOVEMBRE** à Toulouse, Centre de congrès Pierre-Baudis.

WEB SUMMIT

La conférence tech mondiale revient cette année à Lisbonne (Altice Arena & FIL) du **1ER AU 4 NOVEMBRE**.

PLUS D'INFOS SUR WWW.LINFORMATICIEN.COM /AGENDA

LA 21

LES ASSISES

13.10.21 →→ 16.10.21

/MONACO///

→ lesassisesdelacybersecurite.com

DG CONSULTANTS

COMEXPOSIUM

Levées de fonds

Bubble lève 100 millions de dollars

La jeune pousse américaine spécialisée dans le no-code annonce la levée de 100 millions de dollars. En 2019, Bubble levait déjà 6,25 millions de dollars auprès de SignalFire et de Neo, ainsi que d'une poignée de business angels à l'instar des fondateurs d'Okta et de Mulesoft. À l'occasion de cette première levée, la jeune plate-forme comptait un peu plus de 250 000 utilisateurs. Elle en revendique désormais 1 million. Bubble, qui vise à terme *« 95 % des logiciels écrits par des personnes sans formation formelle en ingénierie »*, va pouvoir accélérer dans la poursuite de cet objectif grâce à une nouvelle levée de fonds menée par Insight Partners. Ont participé à ce tour de table les deux investisseurs historiques, SignalFire et Neo, ainsi que quelques business angels parmi lesquels les fondateurs de Hootsuite et de Datadog. La jeune pousse lève ainsi 100 millions de dollars, des fonds qui seront employés à développer sa plate-forme afin de la rendre accessible à un public plus large encore. Et accessoirement de s'imposer « aggressivement » sur le Ô combien concurrentiel marché du no code.

Algolia réalise une Série D à 150 millions de dollars

Algolia, c'est une start-up française qui cartonne, mais qui s'en va outre-Atlantique. Depuis sa création en 2012, l'entreprise née en France a multiplié bureaux, recrutements, clients et levées de fonds. Et s'est au passage délocalisée aux États-Unis. En 2019, elle levait ainsi 110 millions de dollars lors de sa Serie C à laquelle participaient notamment Accel, son principal investisseur historique, et Salesforce Ventures. Œuvrant dans le « Search-as-a-service », la solution d'Algolia consiste à simplifier l'intégration de moteurs de recherche sur des sites et applications tierces au moyen notamment d'API. Elle réalise un tour de table de Serie D, mené par Lone Pine Capital suivi d'autres nouveaux investisseurs tels que Twilio, tandis que Accel et Salesforce Ventures remettent au pot. Ce faisant, Algolia lève 150 millions de dollars, portant le total des fonds levés depuis sa création à 315 millions… et quadruple presque sa valorisation qui grimpe à 2,2 milliards de dollars.

Spendesk lève 100 millions d'euros en Série C

La solution de gestion des dépenses opérationnelles pour les entreprises réalise une levée de fonds en série C d'un montant de 100 millions d'euros, portant le total des fonds levés par la société à 160 millions d'euros. Le tour de table, mené par le fonds d'investissement privé General Atlantic, réunit également les investisseurs historiques de la société, dont Index Ventures et Eight Roads Ventures. Ce nouveau financement permettra à Spendesk de poursuivre sa politique de recrutement à l'international et d'accélérer le développement des produits. L'éditeur souhaite doubler ses effectifs d'ici deux ans.

Cybereason lève 275 millions de dollars

En 2019, Softbank investissait 200 millions de dollars dans Cybereason. L'éditeur de solutions de détection et de protection des endpoints (EDR) dépassait alors le milliard de valorisation. On apprend que Softbank vient de remettre au pot, mais ce n'est pourtant pas lui qui menait ce tour de table de Serie F. Softbank et Neuberger Berman abondent à hauteur de 75 millions de dollars au capital de Cybereason, tandis que 200 millions sont apportés par Liberty Strategic Capital. Ce tout jeune fonds d'investissement est né un peu plus tôt cette année, fondé par l'ancien Secrétaire au Trésor de Donald Trump, Steven Mnuchin, qui rejoint le board de Cybereason.

Netskope explose les compteurs

L'éditeur américain, positionné sur le très neuf créneau du SASE (Secure Access Service Edge), a bouclé un nouveau tour de table, raflant au passage 300 millions de dollars. Cette levée, menée par l'un des investisseurs existants, Iconiq Growth, a été alimentée par Lightspeed Venture Partners, Accel, Sequoia Capital Global Equities, Base Partners, Sapphire Ventures et Geodesic Capital. Ainsi, Netskope pèse 7,5 milliards de dollars.

Bourse

Xavier Niel sort Iliad de la Bourse

Le patron de Free s'inscrit dans les pas de son frère ennemi et camarade milliardaire, Patrick Drahi. À la fin 2020, ce dernier prenait le monde financier de court en annonçant vouloir sortir Altice d'Euronext, de sorte pour Altice Europe *« d'atteindre plus efficacement et avec plus de succès ses objectifs dans un environnement privé et détenu à 100 %, en bénéficiant de l'engagement continu à long terme du fondateur dans l'entreprise »*. C'est peu ou prou le projet dévoilé par Xavier Niel pour Iliad en juillet. Le trublion des télécoms a annoncé sa volonté de reprendre, par le biais de sa holding HoldCo, suffisamment du capital restant du groupe pour le sortir des marchés financiers, sachant qu'il détient directement ou indirectement 70,6 % de son capital et 78,7 % des droits de vote.

« J'ai fondé Iliad en 1999 et je suis très fier du parcours du Groupe et de la valeur créée pour tous les actionnaires. Désormais, la nouvelle phase de développement d'Iliad exige des transformations rapides et des investissements significatifs qui seront plus aisément menés à bien en tant que société non cotée. Notre ambition pour Iliad nous pousse à accélérer son développement pour en faire un leader des télécommunications en Europe », écrit Xavier Niel.

Nouvelle phase, transformations rapides, agilité de la société non cotée… on retrouve là les mêmes arguments que ceux employés par Patrick Drahi en septembre dernier. Dans le détail, l'offre est proposée à 182 euros par action, soit un mieux de 62 % par rapport au cours d'Iliad à la clôture la veille de l'annonce. Le Conseil d'administration d'Iliad a accepté la résolution à l'unanimité, estimant qu'elle « offre aux actionnaires minoritaires une opportunité de céder leurs actions à des conditions faisant ressortir une prime significative de 61,0 % ». En parallèle, Xavier Niel indique avoir obtenu le soutien des actionnaires historiques d'Iliad qui se sont engagés à suivre l'offre, portant la part du capital d'Iliad détenu par Xavier Niel à 74,9 %, et 83,6 % des droits de vote. *« À l'issue de l'offre, si le nombre d'actions non présentées à l'Offre ne représente pas plus de 10 % du capital et des droits de vote d'Iliad, HoldCo II demandera à l'AMF la mise en œuvre d'une procédure de retrait obligatoire »*, précise le communiqué. Un comité ad hoc devait rendre ses conclusions au Conseil d'administration en août, pour un lancement de l'offre publique de rachat le mois suivant.

SAS prêt à entrer en Bourse pour s'éviter un rachat par Broadcom

Grand est l'appétit du géant Broadcom, tout occupé qu'il est à sa diversification. Depuis le rachat de CA Technologies en 2018, puis de l'activité Entreprises de Symantec, celui qui était surtout connu pour ses semi-conducteurs continue *« à renforcer ses franchises pour répondre à la demande croissante de solutions logicielles d'infrastructure »*, dixit son PDG, Hock Tan. Désormais, il lorgne du côté de SAS. L'éditeur de solutions de BI et de gestion et d'analyse de données, est toujours dirigé par ses deux cofondateurs, Jim Goodnight et John Sall, qui ont créé l'entreprise dans les années 1970 sur les bases posées par le programme universitaire Statistical Analysis System.

SAS s'est bien développé depuis lors, comptant 12 545 employés à travers le monde, 82 000 clients issus aussi bien du secteur privé que public suite à l'acquisition plus tôt cette année de son partenaire Boemska. Selon le *Wall Street Journal*, Broadcom ferait bien du vénérable SAS son *quatre-heures*, un projet qui valorise l'éditeur entre 15 et 20 milliards de dollars.

Mais c'était sans compter sur les irréductibles fondateurs de SAS, qui ont annoncé dans la foulée que l'éditeur de BI entrera en Bourse. Pas tout de suite : SAS vise une introduction d'ici à 2024. En amont, l'entreprise veut travailler à la refonte de ses procédures de reporting financiers, la rationalisation de certains processus opérationnels et se concentrer sur ses activités à valeur ajoutée. SAS compte, avec cette annonce, être en mesure de continuer *« d'investir de manière significative »* dans ses logiciels et ses solutions analytiques ainsi que dans l'IA, de sorte à *« étendre son leadership dans un marché en pleine croissance, très concurrentiel et de plus en plus dynamique »*. Et s'éviter de tomber dans l'escarcelle de Broadcom.

BIGDATA & AI PARIS by corp

Conférence et Exposition

10e Edition • 28 & 29 septembre 2021

Palais des Congrès • PARIS

DevOps

Ethique

Reinforcement learning

TIME TO ACCELERATE

Robotique

Data for Good

15 000 PARTICIPANTS

200 PARTENAIRES

350 CONFÉRENCES & ATELIERS

Cybersecurité

Gouvernance et qualité

Cloud

IA Green

Machine learning

Automatisation

NLP / NLG

Inscrivez-vous sur www.bigdataparis.com

Transformation numérique par le Cloud

ManoMano se libère de l'infrastructure

ManoMano s'est lancé il y a trois ans dans sa migration vers le Cloud. En forte croissance, la société ne voulait pas se retrouver bloquée dans son développement par son infrastructure. Elle a choisi le Cloud public d'AWS pour y parvenir.

Antoine Jacoutot, *VP Platform Engineering* de ManoMano, veut être précis et revient en arrière : *« Il y a trois ans, nous étions partis sur un Cloud infogéré. De ce fait les équipes n'avaient pas un accès direct à la plate-forme en Bare Metal. Nous espérions pouvoir nous appuyer sur cela pour être plus agiles afin de faire évoluer notre plate-forme alors que nous commencions une période de forte croissance. La plate-forme n'était pas aussi élastique et aussi dynamique que nous le voulions, ne serait-ce que pour ajouter un serveur. C'est là que nous sommes partis pour bénéficier véritablement de l'évolutivité du Cloud de manière horizontale en réalisant un lift and shift de notre infrastructure sur le Cloud pour ne pas être en danger d'être bloqué par notre infrastructure. »*

ManoMano a ainsi porté les machines virtuelles applicatives dans des instances EC2 d'AWS en s'appuyant sur des méthodes *infrastructure as code*. Cela ne nécessitait a priori pas forcément de l'industrialisation. Concrètement les maigres ressources spécialisées existantes en interne ont développé une application sous Terraform pour le portage vers des containers et des micro-services sous ECS et EKS. Il restait à faire évoluer le cœur monolithique dont certaines fonctionnalités ne pouvaient migrer vers cette pile de nouveaux services. Antoine Jacoutot précise que cela a nécessité *« beaucoup de réécriture. D'un PHP shop, nous avons basculé vers Java et Go. De bonnes techniques avec des usages plutôt orientés vers la créativité. On évolue dans ces différents langages avec en ligne de mire une architecture événementielle »*. Il ajoute : *« Nous avons fait de la période de confinement une opportunité et la migration s'est conclue quatre mois avant la date prévue. »* Les équipes se sont de plus réapproprié la plate-forme avant les points de contention

ManoMano emploie huit cents personnes à Paris, Bordeaux et Barcelone.

par de l'amélioration continue pendant six mois. La refonte est maintenant quasi complète et a gagné en agilité sur les déploiements avec un frontend en React, une librairie Javascript qui a l'avantage de permettre de visualiser une page web dynamique ou interactive de manière simple, directe et rapide.

Un double axe de développement

Chez ManoMano, la technologie est d'abord là pour appuyer le métier de l'entreprise, puis pour exprimer l'expertise et renforcer la place de l'entreprise sur son marché vertical. « *Notre premier défi est de créer un socle solide afin d'accélérer la création de nouveaux services autour de notre place de marché, comme du conseil par exemple qui a été mis en place à la fin de l'année dernière pour nos clients et marchands avec des outils spécifiques.* » Un site dédié, ManoMano Pro, a été mis en place pour les artisans et les utilisateurs B2B avec différentes fonctions : gestion de catalogue, facturation, pas à pas ou mise en relation. Le site va permettre aussi d'asseoir l'empreinte de l'entreprise sur ses différents marchés en Europe avec la création de communautés ou l'échange de savoir-faire autour des thèmes abordés par la plate-forme.

Antoine Jacoutot, VP Platform Engineering.

Profiter de l'industrialisation

Le passage au Cloud a été aussi l'occasion de revisiter les processus internes et l'organisation afin de bénéficier pleinement de l'industrialisation et de l'orchestration que peut apporter le Cloud. Aujourd'hui la volonté est de redonner du prestige au développeur et au code livré avec une approche qui le place comme un « artisan » fier de sa réalisation. Avec pour soutien un processus DevSecOps. Une petite équipe FinOps fait même le lien avec la finance, les métiers et les équipes techniques pour l'optimisation des ressources cloud et diminuer les coûts, éliminer le gâchis et améliorer l'impact carbone de la plate-forme.

De la même manière, la sécurité autour de la plate-forme est très structurée. Fabien Lemarchand, *Head of security*, explique : « *En termes de sécurité le Cloud apporte la résilience et la possibilité d'évoluer rapidement tout en simplifiant la notion de reprise d'activité* ». Il continue : « *Lors d'une migration vers un environnement totalement cloud il faut structurer les pipelines et revoir les processus pour rendre plus simples les contrôles de sécurité.* » *Ainsi chez ManoMano, il n'y a qu'une seule manière de livrer le code pour* industrialiser et automatiser les contrôles de sécurité.

AWS, un précurseur

Le choix d'AWS s'est décidé du fait de l'antériorité technique de la plate-forme et de l'offre importante de

Fabien Lemarchand, Head of security.

services. Mais ManoMano ne met pas tous ses œufs dans le même panier. Ainsi le moteur de recherche ou les outils connexes comme le tracking ne sont pas chez AWS.

La solution est maintenant largement adoptée et les premiers retours sont très positifs. Les équipes sont devenues plus autonomes et proposent davantage qu'auparavant tout en fournissant des services plus créatifs, plus rapidement à grande échelle. En se dégageant des couches basses, ManoMano a réussi à réellement se recentrer et se concentrer sur les couches business de sa plate-forme en faisant évoluer ce que nos interlocuteurs ont mis en avant, le changement de culture. ✖

Bertrand Garé

ManoMano **en bref**

C'est en 2013 que Philippe de Chanville et Christian Raisson démarrent leur aventure avec pour objectif de révolutionner l'univers du bricolage-jardinage en le faisant entrer dans l'ère numérique. ManoMano emploie 800 personnes réparties dans quatre bureaux (Paris, Bordeaux et Barcelone) et opère sur six marchés européens : France, Belgique, Espagne, Italie, Allemagne, Royaume-Uni. ManoMano fédère plus de 3 600 partenaires marchands et propose plus de 10 millions de références. En 2020, l'entreprise a dépassé le milliard d'euros avec un CA de 1,2 milliard en doublant son chiffre d'affaires de 2019. L'entreprise revendique 7 millions de clients actifs en progression de 100 %.

Transformation numérique par le Cloud

La stratégie globale de migration de Maisons du Monde

Maisons du Monde a fait le choix stratégique du Cloud public de Google pour transformer son métier et profiter des technologies proposées.

Pour Maisons du monde, le voyage vers le Cloud commence en 2015 sur le digital à travers les données précise Guillaume Apostoly, DSI du groupe Maisons du Monde. *« Nous n'utilisions alors quasiment pas les données, mais à travers les besoins de croissance de l'e-commerce et les contraintes sur la logistique avec ses aspects transverses comme la charge sur les entrepôts, nous avons mis le pied dans le Cloud en 2017 avec le choix de Google Cloud Platform (GCP) et sa technologie Big Query pour sa facilité d'accès par rapport à ce que les métiers voulaient intégrer »*, rappelle-t-il.

Pour avoir un ordre d'idée, la partie digitale croît de 30 % par an depuis 2010. La volonté a été d'abord d'accumuler les données provenant des magasins, les données de stocks, et de les centraliser dans un data lake sur des technologies cloud sur étagère chez Google avec Big Query et Python ainsi que SQL pour les requêtes. Une fonctionnalité de calcul géospatial permet d'avoir une vue complète des zones de chalandise même si les achats se réalisent en ligne.

Ambiance Maisons du Monde : merchandising par thème.

La refonte du digital

Sont venues ensuite des calculs prédictifs sur la valeur du cycle de vie des clients pour optimiser les achats et le marketing. À ce stade, Maisons du Monde était à la tête d'une IT à deux vitesses avec une branche digitale relativement mature dans des centres de données en actif/actif et un cœur IT sur site. La refonte de la plateforme sur GCP a ainsi permis l'année dernière d'absorber les pics et de revenir facilement à la normale ensuite. *« À partir de cela, nous avons bâti une trajectoire globale de migration vers le Cloud, avec à la fois des réécritures pour du lift and shift et chercher des solutions SaaS pour aller vers l'informatique cible par du best of breed et les outils de Cloud pour faire la glue de notre SI en intégrant les meilleures solutions sur étagère. Cela se traduit par une transformation globale de notre SI »*, explique le DSI de Maison du monde.

Des **retours** concluants

Au cours de notre entretien Guillaume Apostoly a donné quelques repères chiffrés de ce qu'a apporté la transformation autour du Cloud. Ainsi cela a permis d'absorber des pics 10 fois plus importants que le trafic normal. Les commandes sont descendues de dix heures à dix minutes, ce qui comprend le temps de préparation dans l'entrepôt. Cette dynamique a permis de plus de ramener à quasi zéro les écarts de stocks dans le SI.

Guillaume Apostoly, DSI de Maisons du Monde.

Des changements notables pour les métiers et les clients

« GCP est très orienté données dans notre vision ce qui est très structurant avec la mise en place d'une architecture de messaging. Cela a eu pour conséquence que les vieux systèmes sont passés d'un gros batch nocturne à une informatique en semi temps réel. Cela a eu un impact direct et concret pour nos clients », estime Guillaume Apostoly. Il continue : *« Les flux de données réels sont maintenant au cœur de notre stratégie, ce qui est structurant avec par exemple un référentiel client unique. »* Auparavant, le système fonctionnait à partir du système de caisse dont la synchronisation avec GCP était difficile. Désormais, à chaque fois qu'un changement survient dans la base de référence, il est publié dans tous les systèmes : *« La prochaine étape sera d'ajouter de l'apprentissage machine en temps réel, mais qui sera absorbé en streaming, et pour le temps réel asynchrone nous passerons par le système de messaging »*, ajoute-t-il.

Une priorité pour les métiers

« Mon travail en tant que DSI est de trouver les technologies et les transformations qui peuvent accélérer notre activité, nos projets et notre stratégie autour du Cloud. Comment créer un service de Click & Connect en trois mois avec les stocks en magasin en temps réel et s'appuyer dessus pour les clients est une question centrale. Tout cela se construit autour de bonnes pratiques pour démonter l'existant et le recréer dans le Cloud et de transformer les usages. » Guillaume Apostoly ajoute que pour conclure une bonne stratégie de transformation réussie, il faut *« mélanger agilité et stratégie mais elle se coconstruit avec les métiers, avec une priorisation par les risques et les opportunités. »* Cela ne se fait pas en un jour. *« Les métiers doivent être murs et il doit y avoir un alignement de la feuille de route entre les métiers et la stratégie. »*

La sécurité dès le développement

Sous la direction d'un RSSI avec une forte culture cloud, les développeurs ont la charge de réaliser la sécurité par design mise en place. Car pour Guillaume Apostoly, il est *« plus facile de bien faire de la sécurité ainsi »*. Pour l'infrastructure, Maisons du Monde s'appuie sur un outil de Google qui permet de contrôler l'infrastructure cloud.

Encore du chemin à parcourir

Le chantier de la transformation n'est pas encore achevé. Le parc applicatif va être remplacé à moyen terme. À un horizon plus proche, il n'y aura plus d'hébergement sur site. Guillaume Apostoly est confiant : *« Avec notre expérience passée, nous savons que nous pouvons le faire. Avec notre équipe FinOps nous savons même ce que cela va nous coûter. »* Un autre axe sera d'accélérer l'usage de l'apprentissage machine dans certains cas d'usages, comme l'optimisation de l'assortiment Monde de l'approvisionnement des magasins et sur la plate-forme digitale.

Rendre à César…

Maisons du Monde n'a pas réalisé tout cela tout seul. Guillaume Aposotoly a mis aussi en exergue l'aide de Converteo autour de ce qui concerne les données. En plus de cette agence, le plan de transformation s'est construit avec le renfort de Google et de Wavestone, à la fois pour la stratégie mais aussi sur le schéma directeur de la transformation. La formation sur la partie technique a été réalisée par Sfeir. ✖

B. G.

Maisons du Monde : **45 % à l'international**

Le spécialiste de la décoration et de l'ameublement a réalisé un CA de 1,182 milliard d'euro en 2020. La société détient 376 magasins et sept franchises dans 12 pays. Maisons du Monde emploie 8 628 ollaborateurs. L'international représente 45 % de ses ventes. Un quart de la vente globale est réalisé en ligne. L'entreprise dispose de 444 000 m² d'entreposage et de 432 000 m² de surfaces de vente. Les ventes aux Pays-Bas, Royaume-Uni et Autriche sont exclusivement en ligne.

Transformation numérique par le Cloud

Younited Credit envoie son ERP dans le Cloud

L'institution financière spécialisée dans le crédit à la consommation 100 % en ligne a choisi de placer son ERP sur le Cloud d'Oracle.

Le choix du Cloud pour son ERP, de la part de Younited Credit, n'est pas vraiment surprenant. Stéphane Alizon, le CTO de Younited Credit, a opté dès 2015 pour le Cloud. Au départ du projet, ou même dans le cahier des charges, aucun outil n'était véritablement ciblé et tout restait possible en l'absence de spécifications fortes ou de directives imposant que l'éditeur devait être aussi le fournisseur du Cloud ou un tiers. Il fallait cependant que la solution soit nativement cloud pour profiter des avantages que cela peut procurer, comme d'avoir un logiciel toujours à jour sans avoir à gérer les montées de version, ou d'éviter les à-coups dans l'intégration de nouvelles versions. D'ailleurs, la société travaille aussi sur Azure et sur Google Cloud Platform (GCP) pour des tâches en relation avec les données.

Le choix Oracle Cloud

Finalement, le choix s'est porté sur le Cloud et le logiciel d'Oracle. Xavier Pierart, CFO de l'entreprise, s'en explique : *« La solution Oracle Cloud cochait vraiment toutes les cases du cahier des charges, que ce soit côté métier ou côté technique. »* Sans compter que le paramétrage est « très souple » et la gestion des droits d'accès « très efficace ». La solution comprend l'ensemble de la comptabilité générale et bancaire ainsi que le module pour les immobilisations, les traitements fournisseurs et les réconciliations bancaires. La société utilise aussi le module de Business Intelligence intégré pour manipuler les données de gestion par une clé comptable. *« Aujourd'hui, les comptes de gestion peuvent être suivis dans toutes les dimensions souhaitées et il est possible de piloter l'activité par pays, par partenaire… »*, explique le CFO de Younited Credit.

La solution est désormais totalement stabilisée et il est prévu d'apporter des extensions sur certains modules avec des intégrations plus poussées dans les douze mois à venir. Une de ces intégrations sera réalisée *« avec le système core banking »*, qui n'est aujourd'hui que semi-automatisé avec encore des opérations manuelles.

Un autre axe est de pousser les intégrations de plus de sources de données dans Oracle BI en provenance des systèmes opérationnels afin d'apporter des éléments d'industrialisation. Cela se fera de manière latérale avec ce module du fait des besoins encore assez réduits dans ce domaine. Tout au long du projet, la société a pu compter sur l'aide « précieuse » de Kaora, un cabinet de conseil en management.

Xavier Pierart, CFO de Younited Credit.

Accompagner la croissance

Younited Credit connaît de plus une croissance importante et se développe à l'international. Xavier Pierart précise : *« Nous avons une vision de croissance à long terme et Oracle nous permet d'accompagner cette évolution, ce qui n'était pas forcément anticipé au début du projet. On ne fera pas tout à la fois. Les choses se feront progressivement pour être sûr de la robustesse et du niveau industriel des évolutions. »*

Une manipulation fluide des données

« L'aspect des données est très important pour nous, que ce soit les données métier, comptables ou réglementaires. La fluidité dans la manipulation des données autorise la fourniture de données à la volée de manière simple. Nous avons le besoin de fournir des données selon des fréquences différentes, tous les jours, hebdomadairement ou mensuellement. Il suffit maintenant de le paramétrer et d'assurer le suivi opérationnel de production des états ou données. »

B. G.

NXO : histoire d'une résurrection

En près de 20 ans, l'entreprise NXO est passée par toutes sortes de phases. Aujourd'hui, elle envisage l'avenir sereinement.

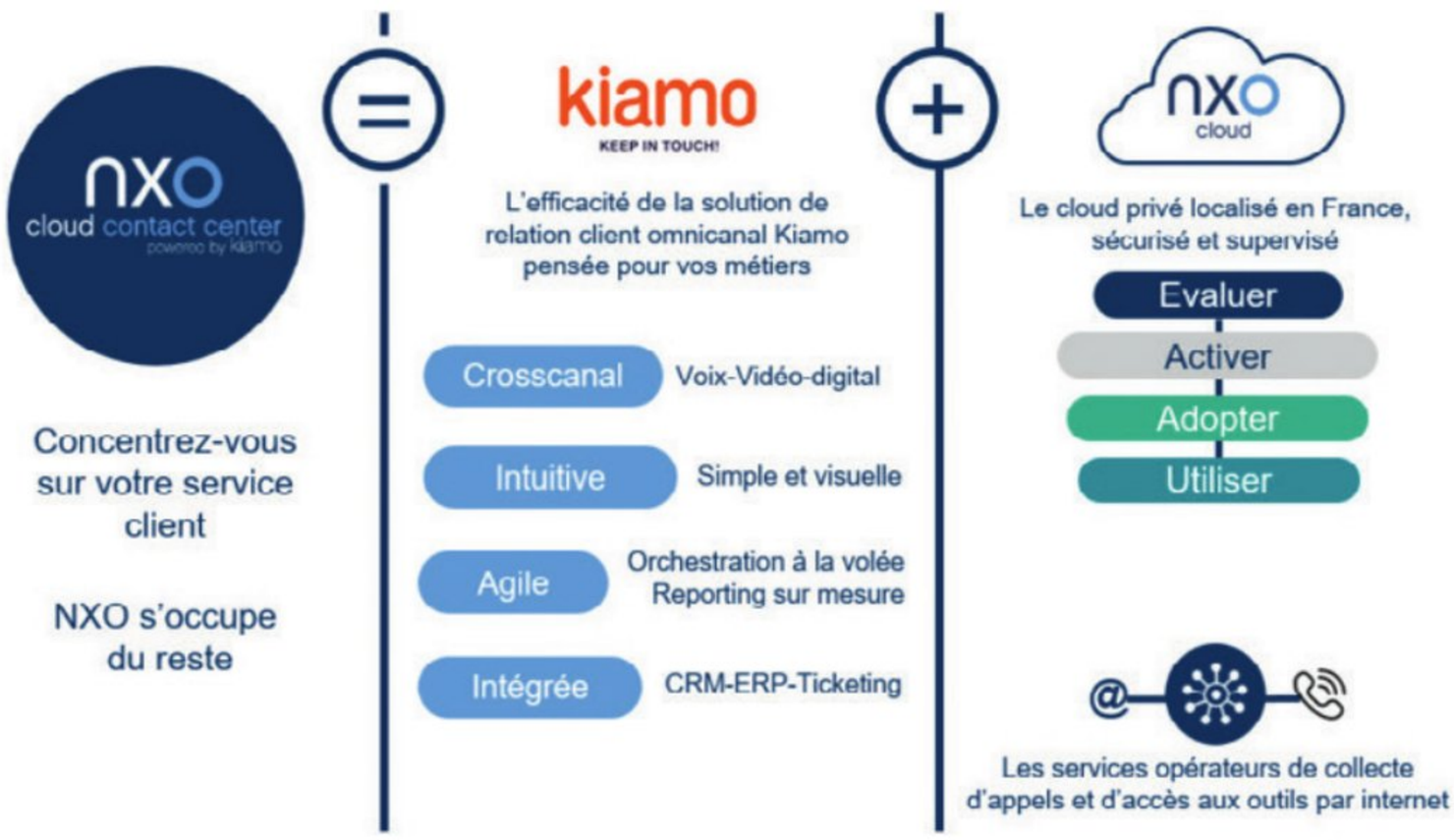
L'histoire de l'entreprise NXO est jalonnée de rebondissements. En avril 2002, Alcatel Réseaux d'entreprises est racheté par le fonds Platinum Equities et devient NextiraOne, une entreprise répartie sur sept agences régionales et qui emploie 2 200 personnes. Las, les difficultés s'accumulent pour l'entreprise et, en 2015, NextiraOne est contrainte de déposer son bilan. La société est alors placée en redressement judiciaire mais, grâce à une ordonnance entrée en vigueur le 1er juillet 2014, l'hypothèse de trouver un repreneur a pu être envisagée avant ledit dépôt et cela aboutît à la reprise par le fonds Butler, et ce, quelques semaines après la mise en redressement avec conservation des emplois – redescendus à 1 380. Quatre ans après la procédure, NextiraOne va beaucoup mieux avec un chiffre d'affaires stabilisé à 240 millions d'euros et des résultats nets positifs de 5,5 M€ en 2018. Toutefois, le modèle économique de départ, l'intégration et l'exploitation de systèmes de communication et d'équipements Réseaux tend à s'essouffler, en particulier sous la poussée du Cloud.

Se transformer soi-même

Alors, avant de proposer des services de transformation à ses clients, NextiraOne va s'attacher à se transformer d'abord elle-même. L'entreprise se rebaptise NXO en 2019 et fait évoluer massivement son offre de produits et services autour du Cloud.
Durant l'année 2018, est mise en place une infrastructure mutualisée de Cloud privé au sein de deux datacenters franciliens en colocation sur la base de laquelle a été bâtie une série de services hébergés. La société propose ainsi une offre de centre de contact sous forme de service sur la base de la technologie Kiamo de Conecteo ; une solution de collaboration unifiée motorisée par la solution OpenTouch Enterprise Cloud d'Alcatel ; et une solution de pare-feu mutualisé d'origine Fortinet… Au-delà du Cloud, l'intégrateur s'est ensuite attaché à développer des compétences et son catalogue dans les serveurs et le stockage ainsi que dans la sécurité au travers de partenariats avec Fortinet et Palo Alto Networks. Il a également beaucoup investi autour des solutions SBC (Session Border Controller) d'Oracle et d'Audiocode.

Une offre cloud 100 % made in France

Opérateur historique de la téléphonie d'entreprise et des communications unifiées, NXO a étendu son offre aux solutions de travail collaboratif ou de vidéo-collaboration ou encore au développement des centres de contact, en particulier pour les ETI, jusque-là un peu délaissées par les différents acteurs du marché. Comme l'explique Julien Baraton, *« Nous avons un historique d'opérateurs de réseaux à laquelle nous avons ajouté une nouvelle offre de téléphonie, notamment hybride cloud, et une dimension de cybersécurité. Nos communications Webex – la plate-forme Cisco – sont sécurisées de bout en bout et notre expertise réseaux nous permet d'optimiser fortement les flux, tout en s'intégrant avec le système d'Information. »*
De quoi séduire le Conseil départemental du Nord (59) qui a souhaité renforcer sa plate-forme Nord Emploi, suite à la crise sanitaire du Covid-19 et son impact sur l'emploi. Cette plate-forme met en relation des entreprises locales et des personnes en recherche d'emploi bénéficiaires du RSA. Le Département cherchait une nouvelle solution de centre de contacts simple et flexible dans le Cloud pour permettre aux agents de continuer à assurer leur mission de service public depuis leur domicile sans prérequis technologique lourd.
« La réponse rapide, la proposition d'une solution cloud française flexible qui répond aux besoins immédiats du département du Nord, ainsi que la vitesse de déploiement ont été décisifs dans le choix de NXO », selon Frédéric Dryepondt, directeur adjoint de la DSI au Conseil départemental.✖



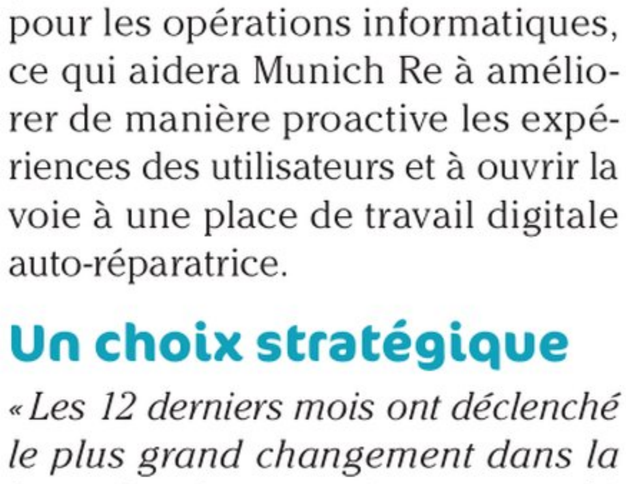
Munich Re modernise ses espaces de travail

Le réassureur allemand a chargé HCL de moderniser les environnements de travail de ses salariés pour améliorer l'expérience utilisateur de ceux-ci et afin de mettre en place un service d'assistance très personnalisé.

HCL va moderniser et standardiser les espaces de travail numériques des 16 000 employés de Munich Re dans 40 pays. La solution Fluid Workspace qui sera mise en œuvre vise à apporter à l'assureur allemand la flexibilité nécessaire pour changer rapidement les pratiques de travail à distance en fonction de l'évolution des besoins de l'entreprise, dans le but d'atténuer les risques liés à l'incertitude entourant la pandémie. De plus, la solution WorkBlaze de HCL fournira des analyses prédictives et des capacités d'IA pour les opérations informatiques, ce qui aidera Munich Re à améliorer de manière proactive les expériences des utilisateurs et à ouvrir la voie à une place de travail digitale auto-réparatrice.

Un choix stratégique

« Les 12 derniers mois ont déclenché le plus grand changement dans la façon dont les entreprises responsabilisent et soutiennent leurs employés », indique Robin Johnson, directeur informatique du Groupe Munich Re. *« Désormais, la transformation de l'expérience utilisateur est devenue une priorité stratégique pour nous. Il était essentiel d'avoir un partenaire qui puisse nous aider à créer un espace de travail numérique moderne et soutenu par les dernières innovations technologiques pour offrir une expérience utilisateur de nouvelle génération à nos employés. Il était également impératif que notre partenaire offre des capacités de support multilingue à l'échelle mondiale. La force des offres en matière de digital workplace et notre relation existante ont facilité la décision de s'associer à HCL. »*



Le siège de Munich Re.

Solution globale, support de proximité

Si la solution a permis de rationaliser le parc applicatif de Munich Re et de globaliser la solution offerte au salarié, HCL va fournir de plus un support

de proximité par des ressources locales. Le support se réalisera en différentes langues comme l'allemand, le mandarin ou l'espagnol. La solution de support proposée va s'appuyer sur des fonctions automatisées et des services en self-service pour améliorer l'efficacité et l'expérience utilisateur des collaborateurs. ✖

B. G.

HCL embarque de l'IA dans le digital workspace

L'annonce est possiblement passée inaperçue au cours du mois d'août. HCL a lancé la suite DRYiCE AEX pour AI-Driven and Automation-Powered Employee Experience. Cette solution vise à optimiser les coûts et à améliorer la productivité et l'expérience utilisateur par l'automatisation et l'Intelligence artificielle.

AEX automatise la productivité des utilisateurs grâce à une surveillance et une remédiation proactive. La solution permet une assistance personnalisée à tout moment, et résout de manière préventive les problèmes de système et d'application grâce à une automatisation non-assistée et un mécanisme d'auto-réparation. Il simplifie l'expérience des employés en répondant aux demandes quotidiennes de services informatiques et commerciaux par le biais d'une marketplace d'entreprises unifiée et d'un assistant virtuel piloté en langage naturel. Les parties prenantes de l'entreprise peuvent obtenir des informations précieuses et exploitables grâce à la surveillance et aux rapports sur l'expérience des utilisateurs. La solution s'appuie sur 10 ans de R & D en Intelligence artificielle, selon HCL.

Le long chemin de la transformation numérique

L'ESN indienne Tata Communications a rendu publique une étude sur l'état actuel de la transformation numérique dans les entreprises. Pas moins de 90 % d'entre elles n'ont pas encore atteint leurs objectifs.

Les conclusions de l'étude ne sont pas vraiment surprenantes. En effet, son présupposé indique la part de la pandémie dans l'accélération des plans de transformation numérique dans les entreprises. Réalisée auprès de 750 cadres en entreprise en avril dernier, l'étude distingue différents niveaux de maturité dans les entreprises ayant entrepris une transformation numérique.
Les « trailblazers », c'est-à-dire les pionniers, cumulent évidemment tous les avantages en étant déjà dans un stade avancé de l'établissement d'un modèle digital opérationnel mature. Viennent ensuite les « migrators » qui ont commencé à entreprendre des progrès partiels par la numérisation. Suivent les « aspirants » qui sont au tout début de la démarche.
Les différences sont notables en termes d'avantages ressentis dans les entreprises. Les premiers de la classe sont plus sécurisés, plus agiles, mieux connectés et profitent d'une meilleure expérience que les autres entreprises. Ainsi seulement 10 % des entreprises disposent des modèles d'exploitation, des plates-formes de connectivité et des stratégies digitales les plus avancées pour garantir des opérations sécurisées et fiables.
Pas moins 63 % d'entre elles attribuent la croissance de leur chiffre d'affaires à leur stratégie axée sur le numérique ; 52 % des entreprises reconnaissent avoir entrepris une numérisation limitée de leur activité et doivent encore s'améliorer dans plusieurs domaines en termes de capacité numérique ; et 38 % des entreprises se trouvent au premier stade de leur digitalisation et n'ont pas pu améliorer leur croissance en raison d'un manque de maturité numérique.

Encore du travail à réaliser

L'étude révèle que 90 % des entreprises n'ont pas encore atteint leurs objectifs en matière de transformation numérique et 49 % d'entre elles admettent que la cybersécurité représente leur priorité numéro un.
Le rapport démontre que 45 % des entreprises ont perdu en productivité pendant la crise en raison de problèmes de connectivité et 41 % d'entre elles considèrent le recours à des modèles d'exploitation axés sur le numérique comme essentiel pour maintenir leur part de marché au cours de la pandémie ; 44 % des entreprises n'ont pas réussi à fournir un modèle opérationnel axé sur le numérique pour leur écosystème.
Pour résoudre ce problème, les avantages de la transformation numérique obligent les organisations à aller bien au-delà du transfert de certains processus industriels. Ces organisations ont besoin d'un modèle opérationnel numérique cohérent qui, au fil du temps, réinvente chaque canal, processus et offre le service de base pour maximiser les opportunités qu'offre la digitalisation.
Jusqu'à 91 % des entreprises admettent qu'elles ne sont pas en mesure de fournir des expériences numériques de haute qualité à leurs clients, employés et partenaires commerciaux. Et seuls 49 % d'entre elles affirment que la cybersécurité est l'aspect le plus important de leur stratégie numérique pour faire évoluer leur offre. Néanmoins, 34 % considèrent que leur modèle d'exploitation n'est pas assez agile. ✖

B. G.

La sécurité est une priorité mais pas dans les faits

RGPD : Sécurisez vos appareils, sécurisez vos données !

Après les menaces en ligne et la divulgation involontaire de données, les appareils mobiles et la perte physique constituent la plus importante source de violations de données.[1]

Tous les jours, en moyenne, plus de 5 millions d'enregistrements de données sont perdus ou volés[2], et plus d'1/3 des entreprises n'ont aucune politique de sécurité physique pour protéger les ordinateurs portables, les appareils mobiles et les autres biens électroniques.[3]

Pour y palier, Kensington propose une large gamme de solutions pour protéger les appareils contre le vol, même en l'absence d'encoche de sécurité.

En cas d'infraction, l'amende peut s'élever jusqu'à 4 % du chiffre d'affaires annuel ou 20 millions d'euros. Investir dans la sécurité physique n'a jamais été aussi judicieux !

MicroSaver® 2.0 & ClickSafe® 2.0

Pour les appareils avec encoche de sécurité Kensington standard

N17

Pour les appareils avec une encoche non-standard Wedge

Solutions pour Microsoft Surface™

Pour Surface™ Pro, Book, Studio et Surface Laptop

Station de sécurité

Pour les ordinateurs sans encoche de sécurité

Trouvez le bon câble de sécurité pour votre appareil : **kensington.com/securityselector**

1. 2016 Data Breaches - Privacy Rights Clearinghouse 2. Breach Level Index, Septembre 2017 3. Kensington IT Security & Laptop Theft Survey, Août 2016

Kensington®

The Professionals' Choice™

Comment contrer le risque de Supply Chain Attack

Depuis quelques années, le patron de l'Anssi le martèle à chaque grande conférence cyber : le danger vient aussi de vos prestataires, de vos partenaires ! Ce risque de « Supply Chain Attack », ou risque tierce partie, est aujourd'hui une réalité qui a éclaté au grand jour avec les affaires Kaseya ou SolarWinds.

C'est sans doute la « Supply Chain Attack » la plus étonnante de l'histoire ! En 2017, un casino de Las Vegas s'est fait voler 10 Gigaoctets de données sur ses joueurs les plus lucratifs à cause du thermomètre connecté de l'aquarium décorant l'accueil du casino. Le dispositif était connecté au réseau interne du casino, ce qui a permis aux attaquants d'accéder au système d'information… Autre exemple édifiant : l'attaque du géant de la distribution américain Target en 2014. Les attaquants se sont infiltrés dans le réseau de la chaîne de magasins en passant par un accès ouvert pour un prestataire, le sous-traitant en charge des systèmes de climatisation… En quelques semaines, les attaquants ont mis la main sur les

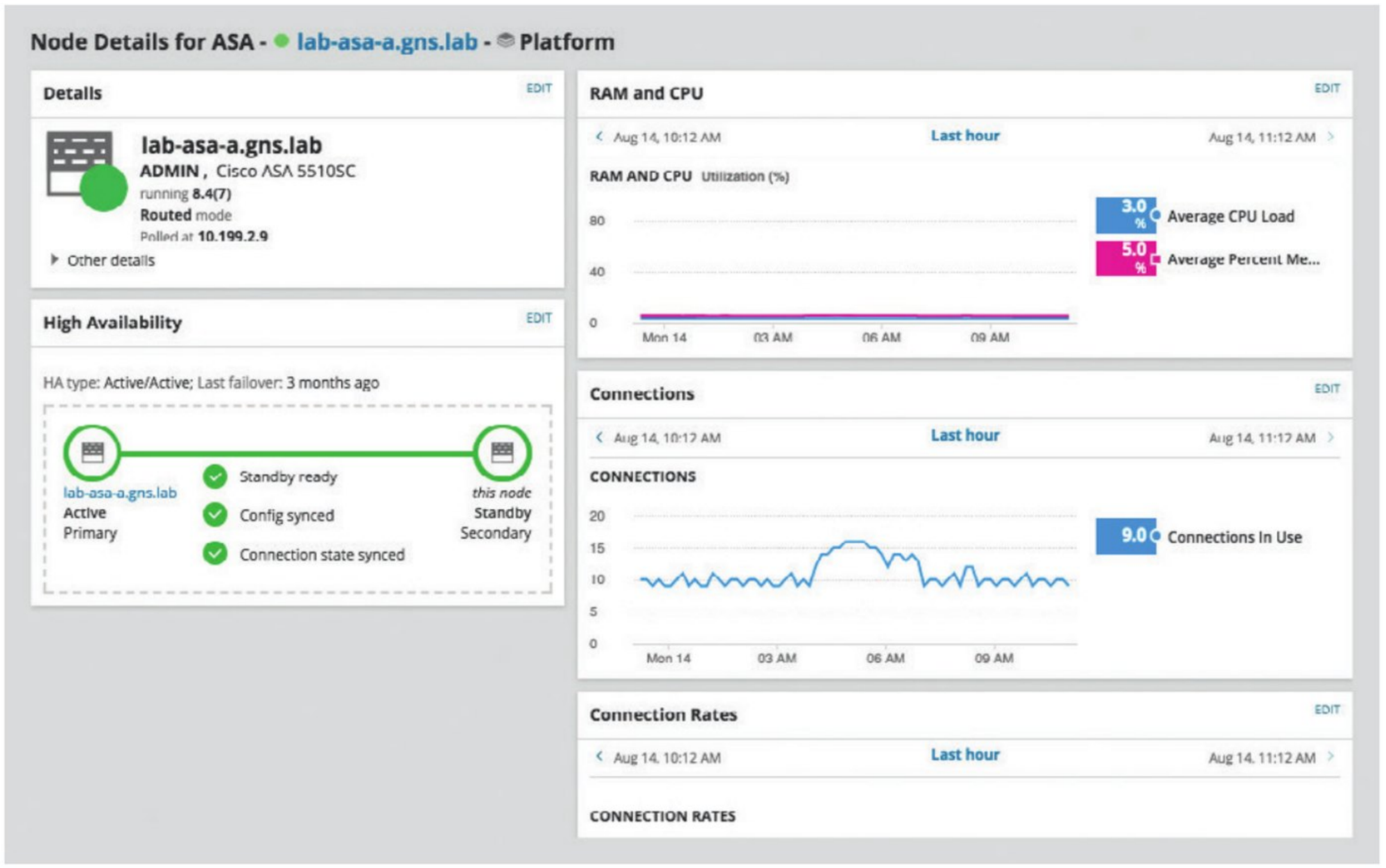
coordonnées bancaires de 40 millions de clients, ce qui a coûté 202 millions de dollars à l'enseigne.

Les prestataires, des utilisateurs à surveiller de près

Si ces exemples sont emblématiques du risque de Supply Chain Attack, un risque lié à une tierce partie faisant partie de la Supply Chain de l'entreprise, ce qui semblait un épiphénonème est devenu un risque majeur. Les ransomware frappent aveuglément les PME et ETI, chaque fournisseur touché offre potentiellement une possibilité de rebond vers un plus gros poisson. N'importe quel prestataire, qu'il s'agisse de l'entreprise en charge du ménage, du gardiennage ou de l'entretien de certains équipements sont des cibles potentielles mais les partenaires IT représentent une cible de choix. On se souvient que Sopra Steria avait fait face à l'attaque du ransomware Riuk en 2020. Le prestataire, qui compte Air France, BNP-Paribas, l'AP-HP et le ministère de l'Intérieur parmi ses clients, avait dû couper de nombreux serveurs dès le début de l'attaque. L'impact de cette attaque a été estimé entre 40 et 50 millions d'euros sur la marge opérationnelle de l'ESN !

Avec leurs ingénieurs en poste chez leurs clients, les ESN sont déjà dans la place et viser ces prestataires est potentiellement très intéressant pour un attaquant. Une segmentation réseau stricte des ressources accessibles par ces collaborateurs externes est un moyen de contenir le risque et pour les comptes à privilèges élevés comme les DBA, les administrateurs réseau ou système, une solution de PAM (Privileged Access Management) vient ajouter une couche de surveillance supplémentaire. L'élimination systématique des mots de passe par défaut des équipements et la mise en place de règles strictes sur la couche accès (IAM) vis-à-vis de la complexité des mots de passe et de leur durée de vie, doublée par une généralisation d'une identification multi-facteur (MFA) permet d'éviter que les mots de passe valides ne se retrouvent diffusés de manière incontrôlable. En outre, une gestion du cycle de vie des identités « au carré » doit permettre de désactiver un compte utilisateur dès que le prestataire a achevé sa mission, tous les comptes laissés à l'abandon représentant un risque d'intrusion de la part d'un collaborateur parti en mauvais termes avec l'entreprise.

Très visé comme fournisseur de solutions de sécurité, mais aussi en tant qu'acteur majeur dans le secteur de la défense, Thales surveille de près la multiplication des attaques sur la Supply Chain comme l'explique le porte-parole de l'entreprise : *« Chacune des alertes a été notifiée à notre CSIRT (Thales-CERT) par la victime comme demandé dans nos contrats fournisseurs, ou pris en compte sur la base des infos média à défaut. Un point avec la victime potentielle est alors fait pour mesurer le risque pour l'entreprise Thales et prendre les mesures conservatoires éventuelles en bonne intelligence avec la victime. La sécurité de nos produits et services livrés aux clients reste notre première priorité. »* Le groupe



SolarWinds Orion, le logiciel qui a révélé au grand jour le risque couru par les entreprises vis-à-vis de leurs fournisseurs de solutions IT.

a lancé une grande campagne d'évaluation de maturité cyber de sa Supply Chain incluant le devoir d'alerte.

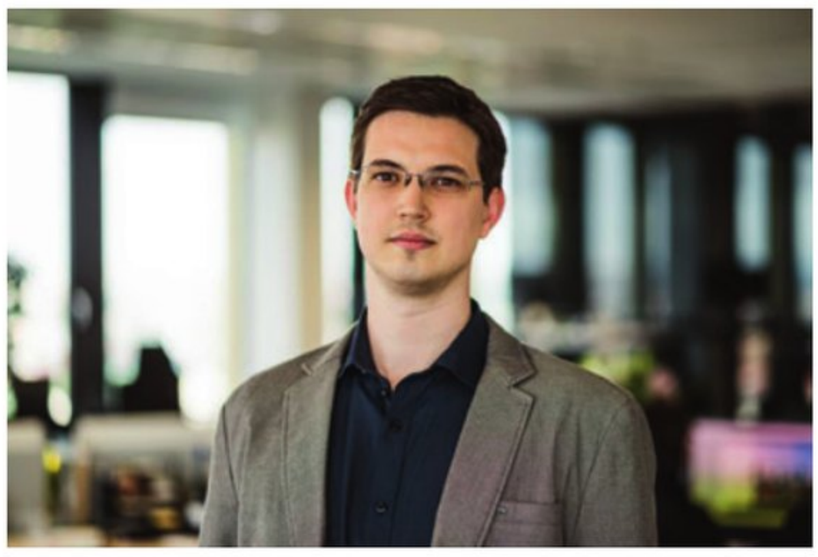
Les acteurs de l'IT, une cible de choix

Les attaques liées aux vulnérabilités présentes dans les solutions de prise en main à distance de Kaseya, les appliances d'échange de fichiers Accelio ou encore les solutions de gestion d'infrastructures de SolarWinds montrent que les éditeurs IT sont désormais particulièrement ciblés par les attaquants. En exploitant une faille « 0-Day » dans leurs produits, ceux-ci n'ont plus qu'à choisir leurs victimes dans le portefeuille client de ces acteurs. L'exemple le plus frappant est celui de l'attaque sur le logiciel Orion de SolarWinds, un logiciel de gestion informatique qui comptait plus de 33 000 entreprises utilisatrices. Selon l'éditeur, 18 000 de ces références clients auraient été touchés par l'attaque, dont Microsoft.

Bertrand Trastour, directeur général Kaspersky pour la France, l'Afrique du Nord, Centrale et de l'Ouest

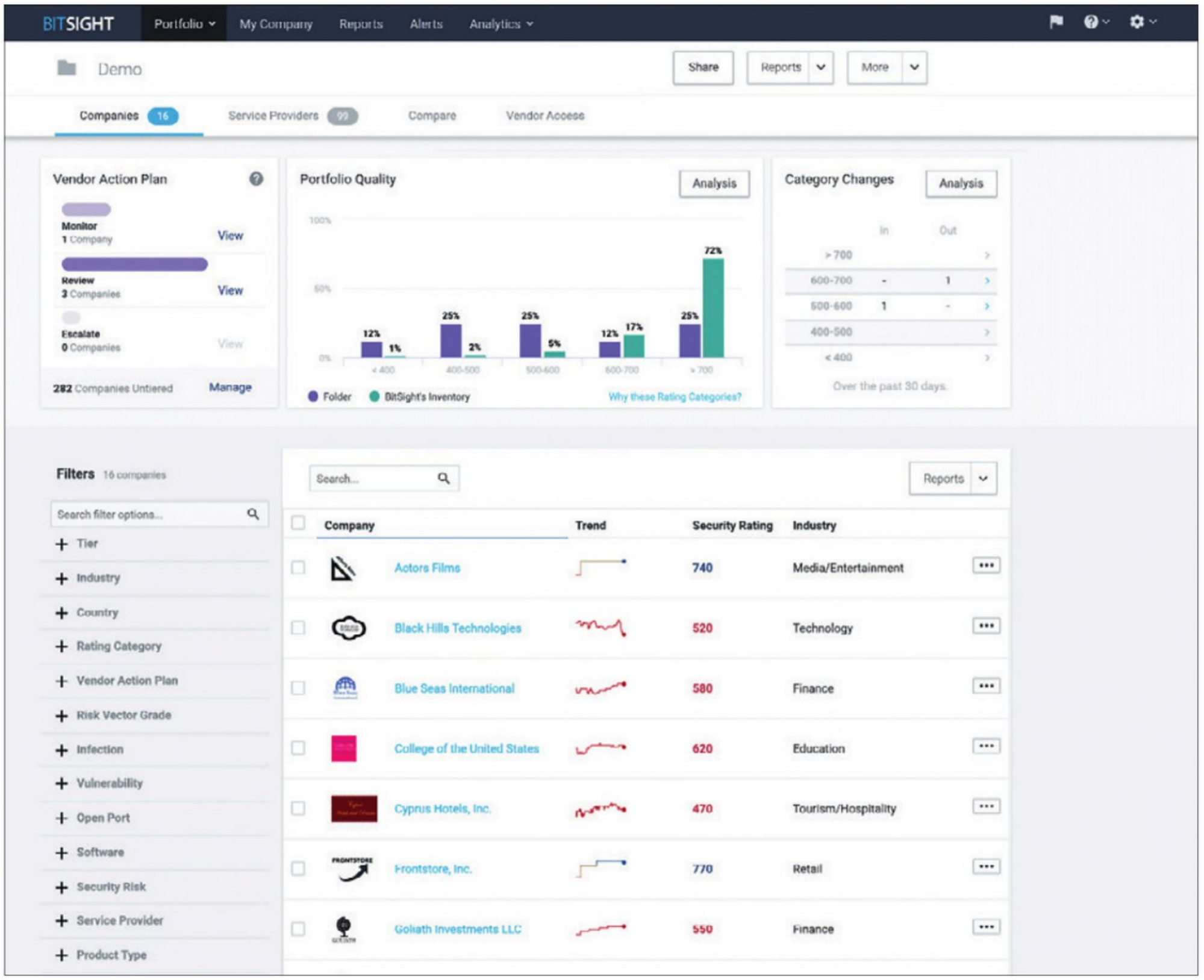
« Face au risque de* Supply Chain Attack *et au risque tierce partie, trois aspects me semblent importants à mettre en avant : d'une part, la sensibilisation des collaborateurs est, et doit rester, un axe majeur dans la première ligne de défense. D'autre part, la mise en place d'une gouvernance cyber au plus haut niveau de l'entreprise avec une claire vision des enjeux business qui y sont liés doit être une priorité. Enfin, la mise en œuvre des moyens techniques mais aussi humains et d'un plan de formation idoine doit être le reflet de cette gouvernance. L'empilement des couches de solutions techniques ne doit plus être la solution . Il convient de repenser son architecture de sécurité à l'aune des enjeux business de l'entreprise. »

Michal Salát, directeur du Renseignement sur les menaces chez Avast



« Il faut toujours planifier à l'avance ! Cela s'applique à tout incident de cybersécurité, y compris les attaques de la chaîne d'approvisionnement. Bien qu'il soit impossible de tout planifier, vous devez avoir un plan en place au cas où quelque chose se produirait sinon vous ne pourrez pas réagir assez rapidement et vous perdrez votre capacité à tirer des leçons de l'événement et à passer à autre chose. La conservation des preuves médico-légales si, ou quand, une attaque se produit vous aidera à comprendre l'étendue ou la portée de tout dommage subi. Dans le cadre de ce plan, assurez-vous d'avoir une stratégie de sauvegarde et de reprise après sinistre, et une compréhension approfondie des actifs les plus importants au sein de votre organisation afin que vous puissiez continuer vos activités pendant toute la durée de l'incident. C'est également une très bonne pratique de penser intelligemment aux partenariats pour s'assurer que vos chaînes d'approvisionnement agissent comme vous du point de vue de la sécurité et de la confidentialité. »

Face au risque de piratage qui pend au nez de tout acteur IT, ceux-ci ont dû prendre des mesures afin de réduire ce risque. Bertrand Trastour, directeur général de Kaspersky, souligne les efforts déployés par l'éditeur : *« Nous avons mis en place depuis plusieurs années des processus internes et des outils techniques nous permettant de nous prémunir vis-à-vis d'attaquants. Cela passe par exemple par un programme de gestion responsable et réactive des vulnérabilités. »* Misant sur la transparence, l'éditeur a lancé voici quatre ans une Initiative Mondiale de Transparence (GTI) vis-à-vis de ses clients, partenaires et institutionnels. *« Dans le cadre de notre stratégie de transparence, l'infrastructure de stockage et de traitement des données clients – auparavant située en Russie – a été relocalisée en Suisse, à Zurich. Nous nous sommes également engagés dans la certification (ISO 27001) et des audits indépendants de nos processus internes. »* Enfin, l'éditeur a ouvert des Centres de transparence dans lesquels le code source et les mises à jour des principaux produits de l'éditeur sont à la disposition des acteurs souhaitant les



L'utilisation du Security Rating permet à une entreprise de connaître le niveau de sécurité de ses fournisseurs, d'engager avec eux une démarche d'amélioration. Le coût limite toutefois l'usage de tels services aux grandes entreprises.

auditer. *« L'objectif est de démontrer que nos outils ne disposent d'aucune porte dérobée ou autre outil potentiellement malveillant »*, ajoute Bertrand Trastour.

La conformité aux standards est-elle suffisante ?

Si la conformité des prestataires aux normes, telles que l'ISO 27001 sur le management de la sécurité, l'ISO/IEC 27035 sur la gestion des incidents de sécurité et l'ISO/IEC 27017 sur la sécurité cloud, ces normes ne constituent pas une assurance tous risques. Pour s'assurer du sérieux de la sécurité de leurs prestataires, les RSSI leur envoient une liste de questions relatives aux moyens de sécurité en place et leurs procédures en cas d'incident. Cette méthode déclarative est relativement simple à appliquer, mais présente des biais évidents. Un prestataire va être naturellement tenté de surévaluer son niveau de sécurité ou éluder certains manquements pour ne pas perdre son client. Pour les fournisseurs les plus critiques, le RSSI peut leur imposer un « PenTest » (Test de Pénétration) afin de vérifier la solidité de leurs protections et lui imposer une mise à niveau si nécessaire. La démarche est très coûteuse – même si elle est payée par le fournisseur lui-même – et demande beaucoup de temps. Elle ne peut être généralisée aux centaines voire milliers de fournisseurs que compte une grande entreprise.

Des entreprises privées se sont positionnées sur le « Security Rating », des notes de sécurité calculées sur le modèle des agences de notation financières. Ces agences attribuent des notes globales de sécurité en s'appuyant essentiellement sur des outils d'audit de sécurité automatisés, sur les données glanées sur Internet et dans le DarkNet à propos de l'entreprise et/ou des questionnaires en ligne. Les grandes entreprises telles que AT&T, Amadeus, Rackspace, NYSE font appel à des agences de ce type, notamment BitSight, Upguard ou Security Scorecard. Moins complets qu'un « PenTest » classique, ces services de Rating s'adressent aux RSSI des grands comptes qui souhaitent vérifier le niveau de sécurité de leurs nombreuses filiales et fournisseurs. L'approche reste anglo-saxonne, mais l'essor des attaques sur les tierces parties pourrait bien généraliser le recours à de tels services. ✖

Alain Clapaud

FIDO2, un standard qui s'impose

FIDO n'a pas remplacé le mot de passe comme principal moyen d'authentification, mais l'Alliance ne désespère pas et multiplie les améliorations pour faciliter son adoption. Notamment au sein des entreprises : c'est le sens des dernières mises à jour des protocoles CTAP et WebAuthn sous-jacents à FIDO2.

Voilà maintenant plus de trois ans que la spécification FIDO2 a été lancée. Et qu'elle doit remplacer le combo identifiant/mot de passe. Si ce second objectif semble encore bien lointain, le standard combinant CTAP (*Client to Authenticator Protocol)* et *WebAuthn* du W3C n'en démord pas. L'alliance FIDO annonce quatre milliards de terminaux compatibles, avec un ralliement début 2020, et non des moindres : Apple. *« FIDO est devenu un standard de référence »*, nous explique David Turner, *Director of Standards Development* chez l'Alliance FIDO. Pour mémoire, le standard FIDO2 permet une authentification à des services web par le biais d'authentificateurs tels que la biométrie, les clés de sécurité physiques ou encore des appareils mobiles. Si le système peut être utilisé de manière totalement autonome, il est surtout employé comme second facteur d'authentification en complément du traditionnel mot de passe, FIDO2 s'avérant beaucoup plus sûr qu'un code envoyé par SMS ou par mail.

« L'un des principaux enjeux va consister à faire que ce standard soit adopté par les utilisateurs et par le milieu professionnel », souligne Laurent Nézot, le directeur des ventes France de Yubico. *« Le fait que Apple ait rejoint début 2020 l'Alliance atteste bien que les plus grands acteurs de la technologie, même s'ils sont connus pour un positionnement à contre-courant, ont un intérêt pour FIDO2. De même, grâce à l'adoption du standard par les éditeurs, nombre d'utilisateurs ont pris conscience d'un besoin impérieux d'une authentification forte, d'autant que les menaces ont évolué. »* Or l'adoption croissante du standard, qui a succédé au *FIDO Universal Second Factor* (FIDO U2F) et au *FIDO Universal Authentication Framework* (FIDO UAF), mène à une demande de plus en plus forte des utilisateurs et des éditeurs d'un soutien dans la mise en œuvre de FIDO2. S'y ajoute la démocratisation du télétravail, qui place, selon l'Alliance, l'authentification des collaborateurs en tête des priorités des entreprises. C'est justement en réponse aux besoins de ces dernières que FIDO2 et le W3C ont mis à jour leurs spécifications respectives (WebAuthn Level 2 et CTAP 2.1).

« FIDO2 suffit aujourd'hui à développer une solution complètement passwordless dès aujourd'hui, quand bien même des améliorations peuvent toujours y être apportées »

David Turner – *Director of Standards Development* de l'Alliance Fido

Des améliorations tournées vers le monde de l'entreprise

« Une des caractéristiques essentielles de FIDO2 est d'être plus léger que ses prédécesseurs en matière de gestion par l'IT sans sacrifier le niveau de sécurité apporté. Alors que nous nous dirigeons aujourd'hui vers des modes de collaboration hybrides en entreprise, avec le télétravail notamment, FIDO2 par sa simplicité et son adaptation aux mondes du Cloud et du Web va permettre de répondre aux enjeux de sécurité de l'utilisateur dans toutes ces situations », assure Laurent Nézot. C'est pourquoi ces dernières améliorations vont notamment permettre aux DSI de mieux gérer les authentifiants FIDO des salariés. On y trouve ainsi les attestations d'entreprises. Un ensemble de fonctionnalités de CTAP et de WebAuthn facilite l'ajout d'une identité utilisateur lors du processus d'enregistrement de telle sorte que les administrateurs puissent suivre la

distribution et l'utilisation des clés. Un processus qui donne accès à certaines informations de l'utilisateur : ce sont les entreprises qui pré-programment les authentificateurs à l'aide de ces attestations spécifiques. En outre, les « BLOB » sont désormais pris en charge, *« une anticipation de scénarios à venir où FIDO2 interagira avec d'autres protocoles, des connexions SSH par exemple »*, indique David Turner.

Les fonctions d'inscription et de gestion biométriques ont elles aussi eu droit à quelques améliorations, avec notamment côté entreprises la possibilité de définir la longueur minimale des codes PIN. Enfin, FIDO2 permet désormais une vérification de l'utilisateur indépendante de la partie utilisatrice : schématiquement, les services activant cette fonction exigeront toujours une vérification de l'utilisateur, au moment d'une signature électronique par exemple. S'ajoutent à ces apports la prise en charge des iFrames d'origine croisée, des attestations Apple et enfin une amélioration des justificatifs résidents permettant une réauthentification automatique. Cette dernière entend faciliter l'utilisation de FIDO comme principal moyen d'authentification.

Épine dans le pied

Dans la même logique, l'Alliance a profité de cette mise à niveau pour publier ses lignes directrices relatives à l'expérience utilisateur (UX). Cette liste de bonnes pratiques entend conseiller les fournisseurs de services sur l'implémentation de FIDO2 sur leurs sites et applications en environnement desktop… et mentionne dès le début du processus, ce qui n'a pas manqué de nous sauter aux yeux, la création d'un combo identifiant-mot de passe. Interrogé à ce sujet, David Turner reconnaît que la dimension « passworless » revêt encore une signification négative pour le consommateur, pour qui *« pas de mot de passe = pas de sécurité »*. Pour Laurent Nézot, le passage de FIDO2 de second à principal facteur d'authentification est *« une évolution en cours »*, en ce que *« l'utilisation de FIDO2 diffère selon les éditeurs et le passwordless a des définitions différentes selon les acteurs »*. Toutefois, à ses yeux, la meilleure expérience est encore FIDO sans identifiant (après enregistrement sur le service évidemment) ni mot de passe. *« C'est ce vers quoi on va aller dans le futur »*, note-t-il.

> ***« FIDO2 par sa simplicité et son adaptation aux mondes du Cloud et du Web va permettre de répondre aux enjeux de sécurité de l'utilisateur »***
>
> **Laurent Nézot** – directeur des ventes France de Yubico

Mais il reste encore un certain nombre d'obstacles à surmonter pour en arriver là, et pas seulement des obstacles psychologiques. *« Du côté technique un des principaux défis est une récupération de compte sans difficulté [seamless account recovery] »*, selon David Turner. *« Sur le sujet, les discussions ne font que commencer, quand bien même certains éditeurs à l'instar de Microsoft, travaillent déjà sur ce type de fonctions. »* Toutefois, aux yeux du *Director of Standards Development* de l'Alliance Fido, *« FIDO2 suffit à développer une solution complètement passwordless dès aujourd'hui, quand bien même des améliorations peuvent toujours y être apportées »*. Il note d'ailleurs que la version2 du standard n'est pas un horizon indépassable : *« Si jamais la récupération de clés demande des changements significatifs, cela pourra suffire à justifier un passage à un FIDO3. »*

IoT et identité, les nouveaux chantiers

D'où cette « emphase », pour ne pas dire insistance, de FIDO sur ce chiffre de quatre milliards de terminaux compatibles. Il s'agit de montrer que *« l'accès à la plateforme n'est pas la barrière »*, dixit David Turner. La barrière, selon lui, est l'appréhension par le public et les entreprises de leur besoin d'un système d'authentification autre que le sempiternel mot de passe. *« On a vu des violations de données et des incidents de sécurité qui auraient pu être évités si les entreprises avaient utilisé une authentification multifactorielle »*, explique-t-il. *« Ce qui participe à cette prise de conscience, en plus de l'adhésion récente d'Apple qui permet à FIDO de fonctionner partout. »*

L'adoption croissante de FIDO2 et son relatif achèvement autorise en parallèle à ses travaux habituels l'Alliance à se pencher sur d'autres sujets, parmi lesquels l'IoT et la vérification d'identité. Dans le premier cas, il s'agit pour FIDO de combler le fossé entre la sécurité des systèmes d'information et celle des systèmes industriels, en s'attaquant à ce dernier secteur et en y apportant son expérience, puisque le mot de passe ne semble pas adapté aujourd'hui à des outils de production toujours plus connectés. Une première version des spécifications de l'Alliance pour l'IoT a été publiée plus tôt cette année. Du côté de l'identité, le principal problème de FIDO est que, lors d'une authentification faciale, se pose la question : *« Est-ce une vraie personne, et non une vidéo ou une photo ? »* De même, s'agit-il de la même personne qui utilise à nouveau telle clé d'authentification ? Autant de sujets sur lesquels les membres de l'Alliance FIDO discutent en ce moment même, avant la publication à l'automne d'un ensemble de critères pouvant servir à l'identification. ✖

Guillaume Périssat

IMT et Airbus Security font bonne chaire

L'Institut Mines-Télécom (IMT) et l'IMT-Atlantique étendent leur partenariat avec Airbus CyberSecurity pour des collaborations dans la formation, la R&D et le recrutement d'ingénieurs et de docteurs en cybersécurité.

L'Institut Mines-Télécom (IMT) et l'IMT-Atlantique étendent leur partenariat avec Airbus CyberSecurity pour des collaborations dans la formation, la R&D et le recrutement d'ingénieurs et de docteurs en cybersécurité.

Initié en 2017, le partenariat avec Airbus CyberSecurity met à disposition la plate-forme CyberRange d'Airbus CyberSecurity pour accompagner la formation des ingénieurs dans le domaine des réseaux et de la sécurité. CyberRange est une solution de simulation avancée qui permet de modéliser facilement des systèmes IT/OT composés de dizaines ou centaines de machines, et d'y jouer des scénarios réalistes comprenant de véritables cyberattaques. Elle permet de concevoir des réseaux virtualisés ou hybrides, d'émuler des activités unitaires comme des communications entre deux machines ou encore pour lancer des scénarios complexes reproduisant une activité réaliste – échange de fichiers, e-mail, trafic web et potentiellement de véritables cyberattaques.

Avec ce partenariat, IMT va accéder aux contenus développés sur CyberRange en provenance de l'ensemble de la communauté autour de la solution. IMT-Atlantique pourra de plus solliciter des experts d'Airbus CyberSecurity.

Approfondir la relation

Les différentes entités vont également accentuer leur partenariat en matière de recherche et d'innovation. Il s'agit en premier lieu de mettre en place une structure d'analyse amont afin d'identifier les appels à projets pertinents et de développer des activités de R&D et R&T conjointes au niveau national et européen. IMT-Atlantique et Airbus CyberSecurity entendent par ailleurs intervenir de concert sur les modalités de programmes de thèses, dès l'identification des sujets et le recrutement des doctorants, jusqu'à la validation des publications et la formation doctorale. C'est notamment l'objet de la chaire CyberCNI (Cybersécurité des Infrastructures Critiques).

Le partenariat prévoit aussi des interactions dans le domaine du recrutement des ingénieurs et des docteurs diplômés de l'école avec la participation d'Airbus CyberSecurity aux sessions d'orientation et de choix de carrière des élèves d'IMT-Atlantique. Il ouvre des opportunités de stages et de contrats d'alternance pour les élèves tout au long de leur cursus au sein d'Airbus CyberSecurity et plus largement du groupe Airbus.

Un exemple concret : la chaire CNI

La chaire CNI travaille sur la sécurité des infrastructures de réseaux critiques dans les milieux industriels. Elle est dédiée à la recherche, la formation, l'innovation et l'enseignement sur ces réseaux critiques. La chaire couvre l'ensemble de la chaîne, du capteur à l'interface utilisateur, même en réalité hybride et les politiques de sécurité. Marc-Olivier Pahl, en charge de la chaire, indique plus globalement les principaux centres d'intérêts des travaux effectués : le design de sécurité par défaut et l'automatisation, la détection des attaques et des anomalies, les méthodes de remédiation et la nécessité de remettre l'humain dans la boucle de ces processus.

La chaire s'appuie sur une plate-forme d'expérimentation qui combine éléments physiques et virtuels qui analyse les interactions sur des « pots de miel » sur des infrastructures critiques. Elle se présente comme un atelier de tests qui repose sur CyberRange et des réseaux virtuels pour simuler des environnements industriels complexes, voire plusieurs environnements en parallèle. Les données issues des tests sont ensuite chargées dans un cluster big data pour être analysées. ✖

B. G.

Signature de la convention avec Anne Beauval, directrice déléguée de l'IMT-Atlantique (à gauche), Frédéric Julhes, directeur d'Airbus CyberSecurity France (au centre), et Françoise Prêteux, directrice déléguée à la recherche et au développement économique de l'Institut Mines-Télécom (IMT).

CYBERNIGHT

La 1ère édition
des Awards de l'Innovation Cybersécurité

Lundi 4 octobre 2021 - Théâtre de la Madeleine - Paris

Pour en savoir plus : www.republik-cyber.fr

RÉPUBLIK CY-BER

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

SALONS SOLUTIONS

100% en présentiel !

5 & 6 octobre 2021

PARIS EXPO
PORTE DE VERSAILLES

SALONS SOLUTIONS erp

SALONS SOLUTIONS démat

SALONS SOLUTIONS crm

SALONS SOLUTIONS bi

SALONS SOLUTIONS e-achats
20 ans

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

@SalonsSolutions
#salonssolutions

SalonsSolutions

salons-solutions.com

LES YEUX PLUS GRANDS QUE LE VENTRE

PAR BERTRAND GARÉ

TACTIC

Quelle entreprise oserait dire quelle n'est pas « data driven » avec à la clé l'exploitation du « nouvel or noir » du business, les données ? Elles sont peu nombreuses comme le montre une étude du cabinet américain Forrester réalisée pour le compte de Dell auprès de 4 036 décideurs data dans 45 pays. Les résultats s'appuient sur l'Indice de transformation numérique biennal de Dell Technologies visant à évaluer la maturité digitale des entreprises dans le monde entier.

En France, 59 % des entreprises se déclarent comme data driven affirmant que *« les données sont essentielles au fonctionnement de leur entreprise »*. Cela semble logique dans le cadre d'un plan stratégique de transformation numérique qui vise à avoir le plus de données possibles pour améliorer la relation avec les clients. Les données apporteraient ainsi les éléments nécessaires à une vision complète des interactions avec le client, quel que soit le canal qu'il utilise pour acheter ou se renseigner sur les produits de l'entreprise.

En fait tout cela semble n'être qu'un grand *foutage de gueule* généralisé ! Seuls 13 % des entreprises en France indiquent qu'elles accordent une importance capitale aux données et donnent la priorité à leur usage dans leur entreprise.

Une drogue dure

Autre enseignement de cette étude, 75 % des répondants indiquent qu'ils collectent des données plus rapidement qu'ils ne peuvent les analyser et les exploiter, mais simultanément, 70 % affirment qu'ils ont constamment besoin de quantités de données que leurs capacités actuelles ne sont pas en mesure de fournir. Bref, toujours plus pour ne rien en faire ! En conséquence, 68 % des répondants indiquent qu'ils ne peuvent pas respecter leurs exigences de sécurité et de conformité en raison de la quantité colossale de données en leur possession, tandis que 59 % affirment que leurs équipes sont déjà submergées par les données dont elles disposent. Mais selon Komprise, un éditeur de solutions de gestion des données, plus de 70 % des données ne sont plus accédées durant plus d'une année.

Datameer, un éditeur de solution de gestion du pipeline de données, indique que 60 % des données ne sont pas utilisées pour des analyses. Dans la même proportion les cadres dirigeants ou les managers affirment ne pas avoir confiance dans les données à leur disposition. Et alors que ce sont les données non ou semi structurées qui explosent dans les entreprises, elles n'utilisent le plus souvent que des données structurées pour réaliser les analyses. Sur les 40 % restants, un faible pourcentage est utilisé à des fins d'analyse. Seulement 30 % des données non structurées entrent dans le cadre d'outils analytiques.

L'étude de Forrester cherche à expliquer pourquoi on arrive à un tel constat : 62 % stockent une quantité significative de données dans des datacenters qu'ils détiennent ou contrôlent, malgré les avantages avérés du traitement à la périphérie, où ces données sont générées et 72 % admettent que le management ne pose pas en priorité les stratégies d'exploitation et d'analyse des données de l'entreprise. Et 47 % ajoutent des data lakes à leur environnement au fur et à mesure, au lieu de consolider leurs ressources existantes pour collecter encore plus de données non structurées à des fins d'analyse… plus tard !

28 % seulement des entreprises ont une personne en charge des données, le fameux *Chief Data Officer*

Le prix de l'inaction

L'étude constate quatre conséquences principales à la faible utilisation de l'analytique dans les entreprises. Tout d'abord, la boulimie de collecte des données entraîne des coûts de stockage toujours plus élevés. Le deuxième élément est de mettre en exergue l'obsolescence du système d'information des entreprises pour y faire face avec des entrepôts de données peu optimisés. Dernier point, les processus d'analyse restent manuels et ne répondent pas aux besoins des utilisateurs.

Si on corrèle ces problèmes avec le fait que la plupart des données sont dites froides, le coût du stockage devient rapidement un réel problème. Sur les 70 % de données stockées non accédées depuis un an, la proportion de celles qui ne seront utilisées qu'une seule fois est de 80 %. Pourtant elles restent en majorité sur des baies de stockage primaire, habituellement des équipements très performants, avec des disques très chers, des capacités hors normes et des performances très hautes. Bref le Top mais le Top du prix aussi !

Des espoirs pour l'avenir...

Malgré leurs difficultés actuelles, beaucoup d'entreprises comptent passer à l'action pour l'avenir, 57 % prévoient de déployer le Machine learning pour automatiser la détection des données anormales, 61 % envisagent de passer à un modèle data-as-a-service et 61 % comptent réaliser une analyse approfondie de leur grille de performance pour repenser leur traitement et leur utilisation des données.

... mais des ressources insuffisantes

Devant ces volontés affichées, le mur de la réalité s'impose : 67 % des entreprises n'ont pas mis en place de programme cible de développement des salariés pour avoir une véritable culture de la donnée. Seulement 13 % ont mis en place des programmes de motivation pour que les employés innovent et utilisent plus les données ; 28 % seulement ont une personne en charge des données, le fameux *Chief Data Officer*, présent dans leur conseil de direction ; 70 % n'ont même pas mis en place les étapes nécessaires pour montrer que la direction supporte ce type de projet. Et 38 % des entreprises interrogées déclarent manquer de ressources spécialisées pour effectuer ce type de tâches. Finalement, 88 % des répondants dans le monde négligent les technologies et les processus tout aussi bien que la culture et les ressources pour parvenir à apporter cette culture « data driven ». Clairement seulement 13 % des entreprises, principalement des grands comptes dans certains secteurs d'activité, peuvent se targuer d'être des « Data champions » et ils ne sont pas beaucoup en France. La réponse apportée est souvent d'externaliser le problème en se cachant derrière du « Data as a Service » : 57 % des entreprises comptent migrer vers ce modèle. Les justifications de ce choix sont souvent assez classiques : recherche d'agilité, d'adaptation à la charge face aux changements des exigences des clients, et la planification de la charge des applications. Dans la même proportion, les entreprises veulent améliorer les gisements de données existants (Data Lakes et Datawarehouse).

La réponse est connue d'avance depuis les débuts de l'externalisation : on ne met pas un problème au dehors de l'entreprise, sous peine d'une probable perte de contrôle. ✖

CLUB DECISION DSI

1er Club Français de décideurs informatiques & télécoms

1250 MEMBRES

Véronique Daval
Présidente

Un réseau indépendant et privé au sein duquel siègent 11 DSI ambassadeurs de leur secteur d'activité

Julien Daval
Vice-Président

LES MEMBRES DU BUREAU ET AMBASSADEURS DU CLUB

Armand ASSOULINE
CIO
MSC FRANCE

Christian DOGUET
DSI
CHAINE THERMALE DU SOLEIL

Trieu HUYNH-THIEN
DSI ADJOINT
CENTRE GEORGES POMPIDOU

Dominique TROUVE
DSI
HÔPITAUX AVICENNE

Gilles BERTHELOT
RSSI
GROUPE SNCF

Damien GRIESSINGER
CTO
EPPO

Stéphane MALGRAND
DSI
Laboratoire national de Métrologie et Essais

Claude YAMEOGO
ARCHITECT SI
ALSTOM

Christophe BOUTONNET
SOUS-DIRECTEUR
SCHÉMA DIRECTEUR ET POLITIQUE SI

MINISTÈRE DE LA TRANSITION ÉCOLOGIQUE ET SOLIDAIRE
MINISTÈRE DE LA COHÉSION DES TERRITOIRES

Christophe GUILLARME
DSI
GROUPE AB TÉLÉVISION

Lionel ROBIN
DSI
GROUPE LA RESERVE

Le Club accompagne les DSI à faire les bons choix technologiques et aligner l'informatique sur la stratégie de l'entreprise

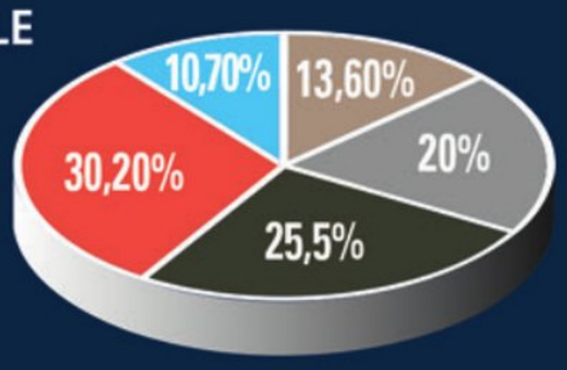
CLUB DECISION DSI EUROPE

EVOLUTION DU CLUB DECISION DSI

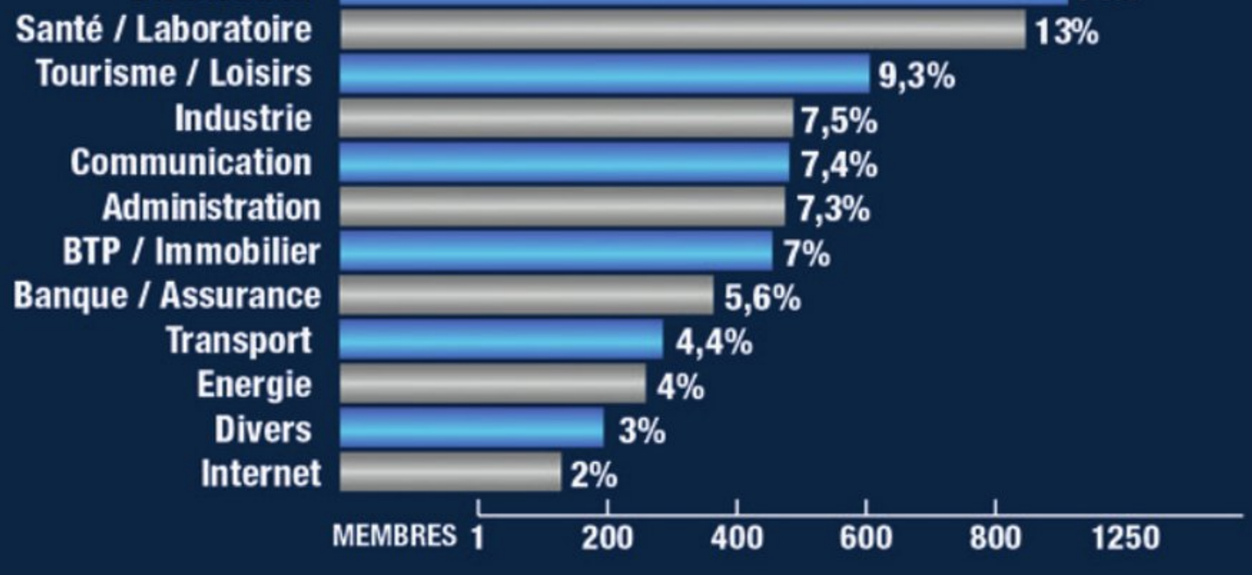
LES MEMBRES DU CLUB

1200 CIO, DOSI, DSI, DI Membres du Club, sociétés de + 300 salariés PARIS/IDF

TAILLE SALARIALE



SECTEURS D'ACTIVITÉ



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

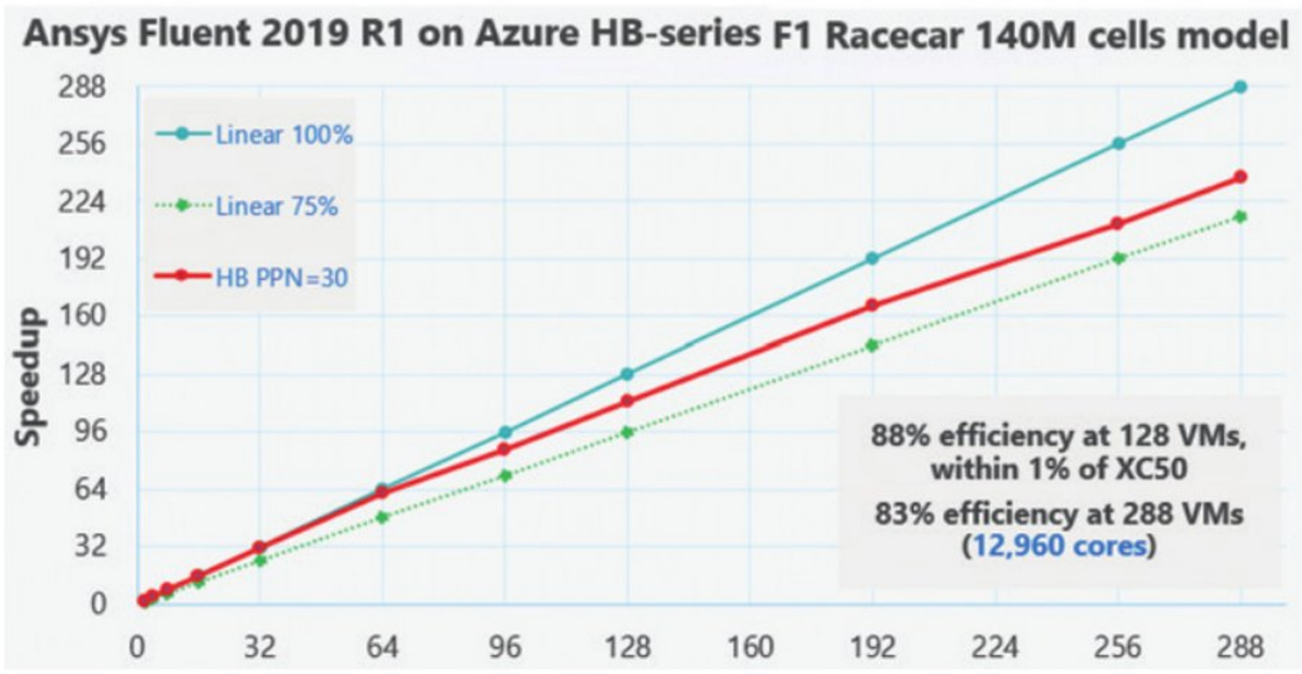
@clubdecisiondsi

www.lmstudio.fr

Pourquoi le Cloud bouscule les supercalculateurs

Avec sa promesse de capacités de calcul quasi infinies, le Cloud a de quoi susciter l'intérêt des entreprises adeptes du calcul intensif. Pourquoi dépenser des dizaines de millions de dollars pour acquérir un supercalculateur quand on peut acheter de la puissance « As a Service » pour quelques *cents*…

Le Cloud va-t-il causer une extinction de masse des supercalculateurs ? C'est la question qui va hanter les nuits des patrons des grands centres de calcul ces prochaines années. Tous les *hyperscalers* avancent désormais leurs pions auprès des entreprises utilisatrices. Si la course des États à celui qui aura le plus gros supercalculateur se poursuit dans les grands centres de calcul affiliés à la recherche nucléaire, notamment, pour les entreprises privées, le Cloud public vient sérieusement brouiller les cartes. L'époque où les infrastructures techniques des opérateurs cloud n'étaient pas prises au sérieux par les experts en simulation numérique s'achève. Les fournisseurs de Cloud public proposent des instances avec divers types de processeurs ARM et x86, y compris les modèles les plus haut de gamme, mais ils disposent aussi d'instances GPU, de FPGA pour certains, et même de puces spécifiquement conçues pour l'apprentissage machine. En outre, sur le volet interconnect, traditionnel talon d'Achille des infrastructures cloud, les fournisseurs ont mis en place l'Infiniband 100 Gbit/s, ce qui crédibilise le Cloud sur ce marché très exigeant du HPC. Pour Gilles Tourpe, *Business Development HPC* chez AWS, le Cloud représente un changement de paradigme pour le HPC : *« On n'approche plus du tout la thématique HPC de la même manière. On passe d'un environnement fini avec de multiples goulets d'étranglement à un environnement où on va chercher la bonne infrastructure en fonction de chaque étape du workflow. »* L'élasticité du Cloud est sans conteste l'argument qui lézarde le plus la forteresse HPC puisqu'il est désormais possible de choisir l'infrastructure de calcul la plus adaptée pour chaque workload et ne payer que



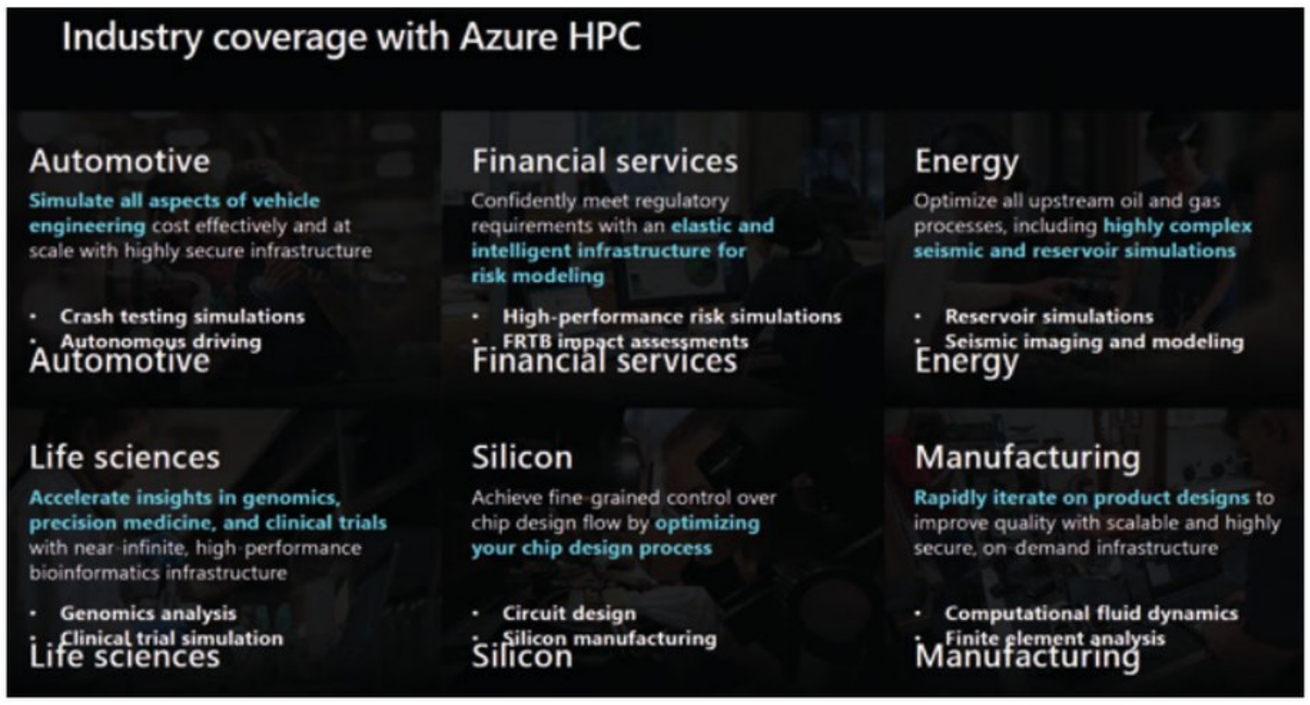
Un benchmark réalisé par Ansys sur sa solution CFD Fluent 2019 sur un modèle de Formule 1 a mesuré le gap d'efficacité entre une infrastructure on-premise optimisée pour le calcul HPC et une infrastructure cloud. Pour ce calcul sur 140 millions de cellules, l'éditeur annonce un taux d'efficacité d'un calcul sur Azure HB Series de l'ordre de 88 % pour un calcul sur 128 VM et de 83 % pour 288 VM, soit 12 960 cœurs.

Chiffres clés : le HPC dans le Cloud, un marché de 9 milliards $ en 2024

Année	*2018*	*2019*	*2020*	*2021*	*2022*	*2023*	*2024*	*Taux de croissance annuelle moyen 2019-2024*
Dépenses HPC Cloud (M$)	*2 466*	*3 910*	*4 300*	*5 300*	*6 400*	*7 600*	*8 800*	*+17,6 %*

Source : Hyperion Research

En 2020, le marché du HPC dans le Cloud à représenté 4,3 milliards de dollars ; un chiffre à comparer aux 13,7 milliards de dollars représentés par les ventes de machines HPC.



Les principaux cas d'usage HP sur Microsoft Azure.

pour ce calcul précis. *«Si je veux faire de l'inférence, je peux utiliser les puces Nvidia ou la puce F1 développée par AWS pour ses propres besoins»*, argumente Gilles Tourpe. *«Si on veut faire de la simulation numérique, on n'a plus à choisir entre des processeurs Intel ou AMD au moment de l'achat de l'infrastructure. On va benchmarker l'application et décider en fonction de ses exigences de performances, de qualité et de précision, de coût et de délai quelle architecture répond le mieux à ce besoin.»* Et selon le porte-parole d'AWS, il ne s'agit pas que de «petit» calcul : dès 2018, AWS réalisait la démonstration d'un cluster de 1,3 million de vCore sur des instances spot EC2 avec le broker Tibco GridServer pour coordonner l'ensemble. Selon le porte-parole d'AWS, faire tourner des workloads HPC sur 800 000 ou 1 million de vCore est désormais chose fréquente.

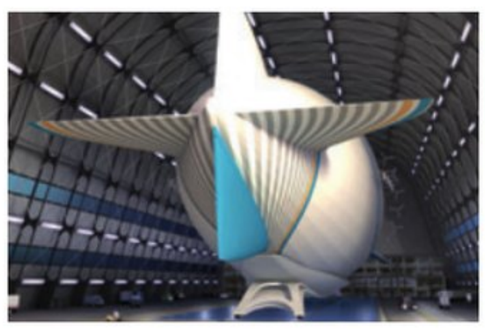
Au-delà du coût d'investissement d'un supercalculateur, l'atout numéro 1 du Cloud public, c'est son agilité. Philippe Bricard, président d'UCit, éditeur de solutions HPC, souligne la différence entre le temps long de la recherche académique et le besoin d'agilité des industriels : *«Le cycle de vie des*

TÉMOIGNAGE

Flying Whales adepte de l'HPCaaS chez AWS

Start-up créée en 2012, Flying Whales met au point un dirigeable de transport de charges lourdes de 200 m de long pour lever 60 tonnes. Son département aérodynamique utilise la simulation numérique pour des calculs CFD, avec des modèles aérodynamiques dont les résultats sont croisés avec les campagnes de tests en soufflerie menées avec l'Onera. Un modèle thermique du dirigeable a aussi été créé et, à moyen terme, le calcul va être utilisé pour dimensionner la structure en fonction des charges critiques. *«Nous avons les besoins d'un avionneur classique, mais avec les contraintes d'une start-up. Nous ne sommes qu'une centaine et nous n'avons pas les moyens d'avoir un département IT en mesure de gérer des ressources HPC sur site»*, **résume Guillaume Martinat, Lead aerodynamics engineer chez Flying Whales.**

Le Cloud était donc la solution naturelle mais les ingénieurs ont voulu vérifier les performances des fournisseurs sur un cas de test comptant environ 31 millions de cellules. Trois fournisseurs cloud dont AWS ont été benchmarkés, ainsi que le Genci. *«Notre benchmark nous a permis de vérifier que le Genci reste à l'état de l'art en termes de scalabilité et reste ce qui se fait de mieux, mais avec les machines virtuelle AWS, Intel MPI et l'interconnect à 100 Gbit/s, nous avons atteint des performances très satisfaisantes et qui nous permettaient de faire ces calculs assez rapidement.»* **L'ingénieur pointe la possibilité de choisir les machines en fonction du niveau de priorité des calculs.** *«Si on a besoin d'aller très vite, on peut choisir des machines très performantes AWS C5, en revanche on peut aussi choisir des machines Graviton (ARM) moins performantes mais avec un rapport coût/performance bien meilleur, ce qui permet d'abaisser le coût du calcul de 30 %. Par rapport au on-premise, un modèle où on est obligé de vivre avec ce que l'on a acheté, le Cloud nous apporte la flexibilité et un vrai gain de productivité»*, **conclut l'aérodynamicien.**



infrastructures HPC telles qu'on les connait est de l'ordre de 3 à 5 ans. Dans le Cloud, un cluster peut être déployé en quelques minutes et décomissionné tout aussi rapidement. Les entreprises ont des besoins de simulation complexe et les cas d'usage du HPC sont de plus en plus fluctuants, mais avec de moins en moins d'effectifs. Ces contraintes ont fait naître ce besoin du HPC as a Service. Dans ce cadre, la possibilité de recourir à des Cloud publics est de plus en plus importante.»

Le Cloud va faire exploser les nouveaux cas d'usage du HPC

En faisant sauter le verrou du hardware, le *HPC as a Service* va permettre à de nombreuses entreprises de franchir le pas et leurs ingénieurs se lancer dans le calcul intensif sans même disposer d'équipe IT. Dans une enquête menée par l'éditeur de solution de simulations numériques Ansys auprès de ses clients, 40 % d'entre-eux déclarent limiter volontairement la taille de leurs modèles de simulation à cause des capacités de calcul auxquelles ils ont accès. *«Tous les ingénieurs n'ont pas accès à des milliers de nœuds de calcul, mais via le Cloud ça devient de plus en plus possible»*, explique Wim Slagter, *HPC and Cloud Alliance Director* chez Ansys. *«Le Cloud rend l'accès à ces technologie beaucoup plus simple. Un calcul mené dans le Cloud peut être monitoré depuis l'application Ansys ou directement sur le portail Cloud et le résultat de la simulation peut être visualisé dans le Cloud puis téléchargé vers la station de travail.»* Les principaux éditeurs de solutions de simulation ont réalisé l'intégration de leurs solutions avec les fournisseurs majeurs du marché si bien que l'ingénieur aérodynamicien ou en mécanique va lui même basculer ses calculs sur le fournisseur de son choix sans qu'il soit besoin de faire appel à un informaticien.

Si les fournisseurs cloud ont fait monter en puissance leurs infrastructures, interconnecté leurs instances les plus puissantes en 100 Gbit/s, le rôle de ceux-ci va au-delà du seul hardware. C'est la position d'Alexandre Jean, *Technical Specialist* chez Microsoft Azure : *«Le matériel n'est pas suffisant et nous avons toute une offre d'orchestration de ces workloads, la gestion des workflows. Nous nous appuyons sur nos partenaires afin de déployer des solutions sur Azure comme Ansys ou Rescale et bien d'autres. Nous offrons l'opportunité d'intégrer de nouveaux services comme l'IA dans les workflows HPC afin d'optimiser l'ensemble de la chaîne de calcul HPC.»*

Le SuperPod DGX, un supercalculateur clé en main conçu par Nvidia et NetApp pour booster l'apprentissage des modèles de Machine Learning/ Deep Learning. Une machine disponible en mode locatif.

Entre «on-premise» et «As a Service», le supercalculateur en location

Si le *Business Model* des hyperscaler cloud est bien rodé et correspond bien aux besoins financiers des entreprises qui privilégient l'OPEX et l'agilité aux investissements sur un temps long, l'approche traditionnelle n'a pas dit sont dernier mot. D'une part les grands centres de calcul ont bien vu émerger ce modèle *As a Service* et se sont adaptés. À l'image du Genci, Grand équipement national de calcul intensif de la recherche française, l'accès au calculateur a été assoupli et va tendre vers un tel mode de consommation *As a Service*.

En outre, les constructeurs de supercalculateurs se sont mis au diapason. Atos pousse depuis plusieurs années son offre Bull Extreme Factory, son offre *HPC as a Service*. Celle-ci s'appuie sur la gamme de supercalculateurs maison, les BullSequana et une couche logicielle de type portail pour en simplifier l'accès aux utilisateurs.

Stéphane Requena, directeur Technique & Innovation / CTO du Genci

«Les hyperscalers et leurs offres «as a Service» ont fait bouger les lignes vers des modèles plus flexibles, à la demande, plus adapté notamment aux besoins imprévus et aux optimisations des coûts IT des entreprises. Pour le Genci, et notamment avec l'arrivée de la machine Jean-Zay à l'IDRIS – dédiée notamment aux besoins de la communauté française en IA – nous avons mis en place les accès dynamiques. Ils permettent en quelques clics et en quelques jours d'avoir accès sur la machine et de pouvoir lancer des calculs, tout cela gratuitement pour des travaux de recherche ouverte et sur des moyens de calcul souverains. C'est un début de réponse mais cela devrait continuer avec des discussions avec certains Cloud providers FR pour mettre en place un portail d'accès unifié et souverain donnant accès à la fois à des ressources de calcul, mais aussi et surtout à des services d'expertise à la demande (IA, métier), formation à la demande ou veille techno à la demande. Ce sont par ces services d'accompagnement et d'expertise qui sont encore peu développés par les grands hyperscalers et avec lesquels nous entendons nous différencier, avec, bien sûr, l'argument d'un hébergement souverain.»

L'offre est disponible en mode public mutualisé, public réservé, privé sur site, privé hébergé.
Plus récemment, c'est Nvidia qui a créé la surprise avec ses SuperPod DGX. Très présent tant dans l'architecture des supercalculateurs que dans les infrastructures des Cloud provider, Nvidia propose une nouvelle approche aux entreprises qui ont besoin de puissance de calcul pour entrainer des modèles d'IA. Son DGX SuperPod est un calculateur optimisé pour l'IA clé en main, prêt à l'usage et disponible en mode locatif. *« Traditionnellement il faut six mois ou plus pour concevoir et déployer un cluster de calcul de la taille nécessaire pour résoudre des problèmes complexes d'IA ou de HPC »*, rappelle Tony Paikeday, *Senior Director des systèmes* d'IA chez Nvidia. *« Avec le DGX SuperPOD, toute entreprise peut déployer le sien en trois semaines seulement et commencer à développer ses applications. »*

L'offre a été montée avec NetApp qui fournit la partie stockage du SuperPOD et Equinix pour l'hébergement de la *bête*. Ce SuperPOD se destine donc aux entreprises qui veulent booster l'apprentissage de leurs modèles d'IA sans investir dans de coûteuses infrastructures, ni confier leurs workloads à un fournisseur cloud. La limite de l'approche, c'est bien évidemment son prix : on parle d'un prix d'entrée de l'ordre de 90000 dollars par mois pour pouvoir jouer avec ce DGX SuperPOD. Alors à vos calculettes : acquisition, Cloud public ou location mensuelle, à vous d'opter pour le bon modèle. ✖

Alain Clapaud

Tony Paikeday, *Senior Director "AI Systems"* de Nvidia

« Alors que de plus en plus d'entreprises cherchent à insuffler l'IA dans leurs activités, le besoin d'accéder à une infrastructure prête à l'emploi et conçue spécialement pour répondre aux exigences uniques des charges de travail de l'IA va augmenter de manière exponentielle. La plupart des entreprises ne disposent pas de l'expertise nécessaire pour construire des plates-formes de supercalculateurs capables de prendre en charge les recommandations d'IA, l'IA conversationnelle et les systèmes de vision par ordinateur les plus complexes. De plus en plus, ces organisations rechercheront des offres gérées plus simples, clés en main, qui leur permettront d'accéder facilement aux performances dont elles ont besoin. C'est pourquoi nous avons récemment lancé des offres comme Nvidia Base Command Platform et Nvidia AI LaunchPad – qui rendent la puissance de DGX SuperPOD accessible aux entreprises dans un modèle de consommation simple basé sur un abonnement. L'un des avantages de ces offres est qu'une entreprise peut accéder rapidement à une infrastructure de premier ordre, sans avoir à la concevoir, la déployer et la gérer elle-même. Leurs développeurs peuvent constater l'impact immédiat sur leurs projets et lorsque l'organisation est prête, elle peut même choisir d'acheter sa propre infrastructure à plus long terme. »

Le lakehouse prend ses aises

Une nouvelle architecture, le « lakehouse », commence à se faire une place dans le petit monde de l'analytique. Elle vise à combiner le meilleur de deux technologies : le Datawarehouse et le data Lake, architecture chère au Big Data.

Depuis les années 80 du siècle dernier, le Datawarehouse – ou entrepôts de données – a connu différentes évolutions pour combler ses défauts. La principale a été l'apport du traitement massivement parallèle pour permettre de traiter d'importants volumes de données. Cette technologie convient toujours parfaitement pour gérer les données structurées dans l'entreprise, pour simplifier les données qui sont bien rangées dans les bases de données.

Le terme de Data Lake est beaucoup plus récent et date de 2010. Il précise l'endroit où sont stockées les données qu'il semblait impossible de gérer ou d'utiliser avec les outils SQL de l'époque, ce que réalisait Hadoop en ouvrant ainsi la porte au Big Data. Depuis, on a pu constater la croissance dans les entreprises des données dites non ou semi structurées, ou brutes. C'est la catégorie de données qui augmente le plus vite dans les entreprises. Au fil du temps la gestion de ces données est devenue de plus en plus importante pour autoriser la mise en œuvre de multiples applications, principalement les applications analytiques, de Business Intelligence, d'apprentissage machine ou d'Intelligence artificielle.

Selon Nicolas Maillard, *Senior Director Field Engineering Central & SEMEA Databricks*, la notion de données et l'analytique ont débordé des entrepôts de données : *« Pour contourner cela, de nouvelles architectures sont apparues pour gérer de grands volumes de données de sources différentes pour monter des produits de données. La notion de data lake est apparu en miroir du datawarehouse. »*

Les entreprises se trouvaient d'un côté avec une technologie très agile mais se posaient aussi la question de la qualité de la donnée, des formats, de la fraîcheur des données et de la stabilité de la solution. De l'autre côté, les données sont primordiales dans les prises de décision des métiers, cela nécessite d'avoir confiance dans les sources de données, ce que procure un datawarehouse.

Nicolas Maillard évoque d'ailleurs des essais d'architectures différentes pour arriver aux mêmes buts, comme les architectures Lambda et Kappa.

L'architecture Lambda a été imaginée afin de faire simultanément du traitement de type batch – par bloc de données – et du traitement en temps réel – de manière continue. Contrairement au Datalake qui sert essentiellement au stockage, l'architecture Lambda permet de fusionner le traitement par bloc de données (batch) et les nouvelles données entrées (temps réel).

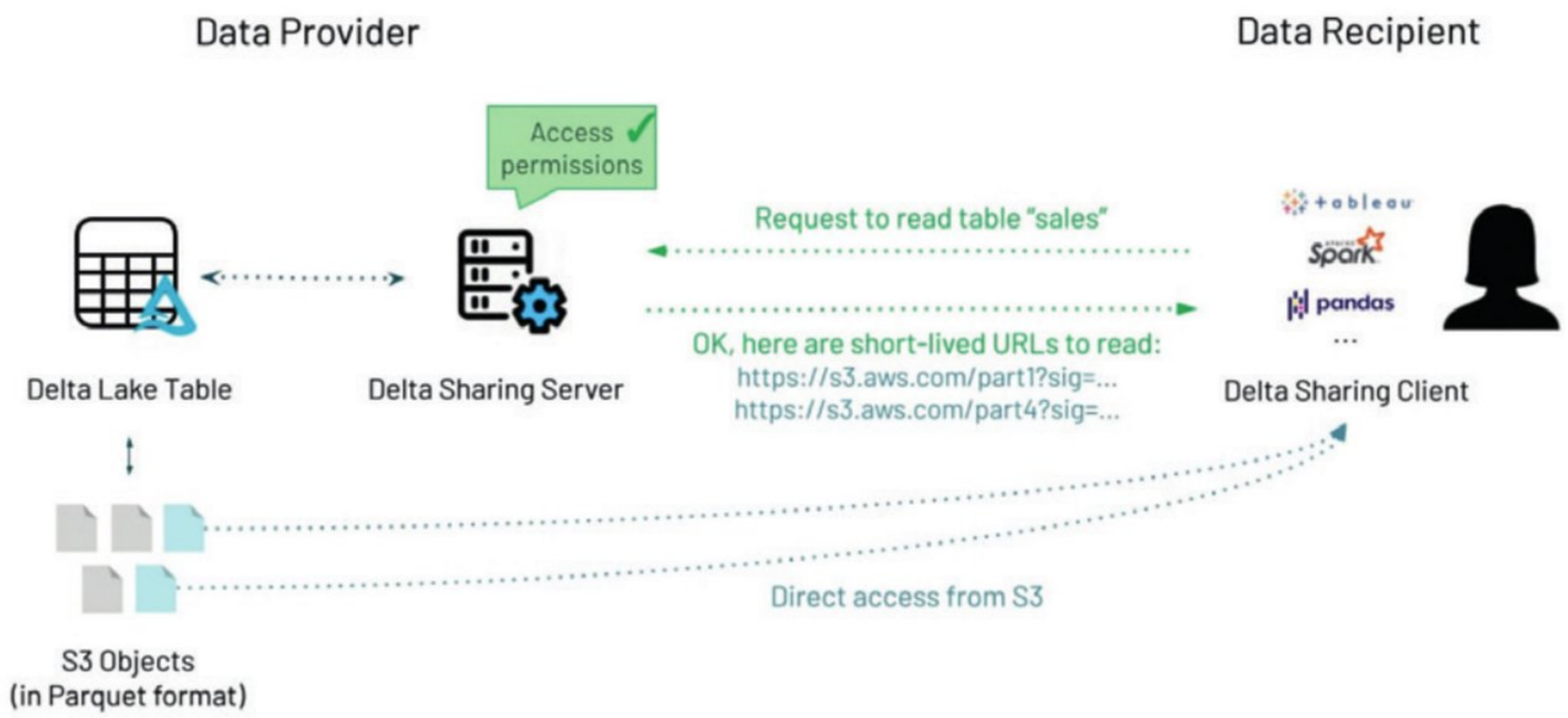
L'architecture Kappa a été pensée pour remédier à la complexité de l'architecture Lambda. Elle repose sur le principe de fusion de la couche temps réel et batch, ce qui la rend moins complexe que l'architecture Lambda. Ne permettant pas le stockage de manière permanente, cette architecture est faite pour le traitement de données. Nicolas Maillard juge sévèrement ces architectures : *« Le diable est dans les détails car si les architectures étaient très belles sur le papier, il manquait la couche de gouvernance pour recréer l'ensemble. »*

« La notion de données et l'analytique ont débordé des entrepôts de données. Pour contourner cela, de nouvelles architectures sont apparues pour gérer de grands volumes de données de sources différentes pour monter des produits de données. La notion de data lake est apparue en miroir du datawarehouse »

Nicolas Maillard
Senior Director – Databricks

La fin du grand écart ?

Récemment une nouvelle architecture technique, le lakehouse, a



Un modèle de partage de fichiers dans Delta de Databricks.

émergé et commence à prendre sa place dans les entreprises avec pour but de combiner le meilleur des deux mondes. *« Les outils ont la valeur que procurent les produits et les décisions à partir des données »*, ajoute Nicolas Maillard. Il cite l'exemple de l'apprentissage machine ou les data frames, une liste de type data, ne sont pas miscibles avec les tables d'une base de données ou le langage SQL. De là est venue l'idée du lakehouse. Cette architecture ne se bâtit pas forcément en s'appuyant sur différentes approches avec des points d'intégration. Nicolas Maillard souligne d'ailleurs que cela *« devient complexe et génère beaucoup de points de faiblesse. »* Il définit alors le lakehouse comme une plate-forme capable de comprendre les différentes grammaires autour des données tout en conservant le caractère agile du data lake.

Les principales fonctions du lakehouse

Pour Nicolas Maillard, la Business Intelligence a *« besoin de données très structurées. Pour les données non structurées il y a besoin de streaming pour prendre des décisions en quasi temps réel par une faible latence et de l'apprentissage machine ou de l'Intelligence artificielle pour automatiser et ajouter du savoir provenant d'autres technologies »*, comme la technologie de graphe, mais cela ne suffit pas, il y a besoin de métadonnées pour apporter cette compréhension de la donnée : *« De quoi ai-je besoin ? Les applications accèdent à cette structure de données qui peuvent être parfois très strictes. Les applications font ce choix. De la même manière, les métadonnées permettent au système de faire ce choix. LPI est capable de comprendre l'expression de la donnée et attaque le fichier distribué qui est descendu par des fonctions mathématiques, des notions tabulaires et un optimiseur de requêtes. Ce format est à sa façon structuré. Le besoin est repoussé vers la plate-forme plutôt que de le définir. L'interface va ensuite traiter cela comme des tables. Cela se passe de la même façon pour d'autres abstractions. Le système attaque le fichier et pas la table elle-même ».*

L'ensemble est maintenu cohérent par un référentiel dans Delta, la solution de Databricks, qui apporte la couche de gouvernance ainsi que Unity, un catalogue des données ouvert et qui peut être enrichi par d'autres solutions de catalogues des données.

Par ce moyen, la solution supporte le caractère ACID (Atomicity, Consistency, Isolation, Durability) des transactions. Elle doit de plus permettre la mise en application des différents schémas des bases de données et leurs évolutions, comme les schémas en étoile ou les formats plus spécifiques, comme celui de Snowflake. Les lakehouse doivent permettre d'utiliser les solutions de Business Intelligence directement à partir des sources de données. Il en est de même pour le support du streaming, les différents types ou formats de données et les différents workloads.

Autre caractéristique importante de cette technologie, le stockage est découplé du traitement ou calcul dans des clusters séparés pour assurer l'évolutivité et la montée en charge selon les besoins. Enfin, la plate-forme se doit d'être ouverte pour être accessible par les différents moteurs et outils que peuvent choisir les utilisateurs, même si le stockage est souvent standardisé autour de certains outils comme Parquet pour l'écosystème Apache Hadoop. Il est similaire aux autres formats de fichiers de stockage colonnaires disponibles dans Hadoop, à savoir RCFile et Optimized RCFile. Il est compatible avec la plupart des frameworks de traitement de données de l'environnement Hadoop. Ce type de solution permet aussi le partage des données, un point important. Snowflake possède déjà une place de marché de données, tout comme Dawex. Databricks devrait sans nul doute aller dans ce sens dans les mois à venir.

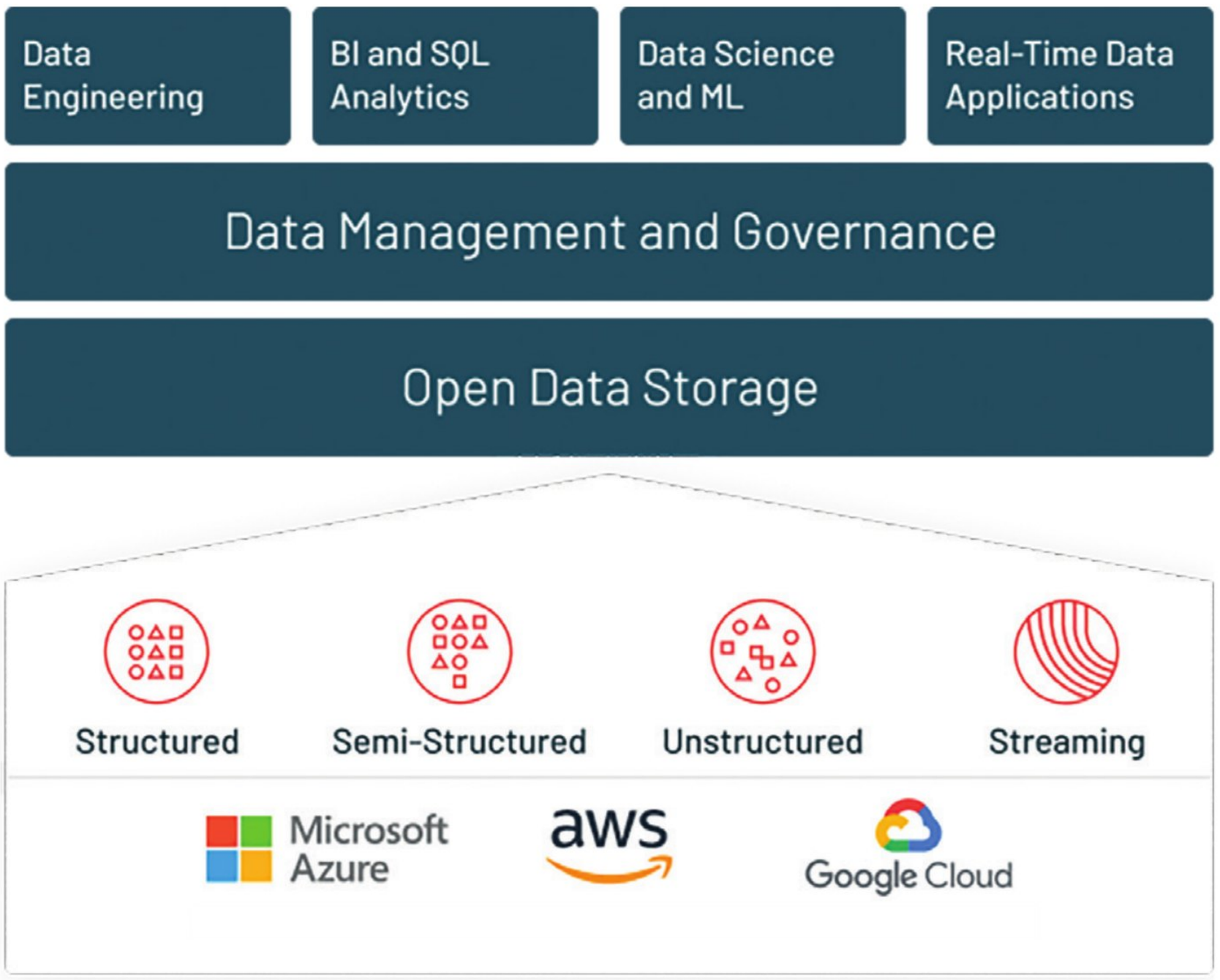
De nombreuses alternatives

Si nous avons parlé de la technologie de Databricks, il est loin d'être le seul sur le lakehouse, que ce soit sous forme managée ou non. Azure Synapse, Big Query de Google, Redshift Spectrum d'AWS ont plusieurs caractéristiques proches des solutions de lakehouse. Des éditeurs comme Dremio et Snowflake jouent dans la même cour. Des projets open source comme Apache Iceberg montrent le bout de leur nez. Et IBM, avec son architecture de référence de data lake cloud, qui combine SQL Query, DB2 Warehouse et l'analytique de Watson Studio et Watson Machine Learning avec IBM Object Storage, vise aussi à prendre une place sur ce marché. N'oublions pas le survivant du Big Data hadoopien, Cloudera. Tout cela montre un intérêt qui se renforce autour de cette technologie encore émergente mais qui séduit les entreprises. TotalEnergies ou la SNCF sont des clients de Databricks.

Un simple buzz marketing ?

Certaines voix s'élèvent cependant pour dénoncer le buzz marketing réalisé autour du lakehouse et trouvent que ce concept émergent est encore souvent bien mal compris et sujet à beaucoup de spéculations ou d'un battage immérité. Du fait de la jeunesse du concept, ils mettent en avant le fait que la technologie est loin des fonctionnalités développées depuis des années par les acteurs des deux technologies : datawarehouse et datalakes. Ils pensent d'ailleurs que les deux technologies vont encore coexister avec le lakehouse pendant des années suivant les besoins et les investissements consentis par les entreprises. Un article en avril dernier relevait que les déploiements autour de cette technologie étaient encore trop limités pour en tirer des conclusions et que cette approche *one size fits all* représentait un pas trop grand pour les entreprises qui avaient investi dans les data lakes et les datawarehouses. En tout cas les mois à venir vont apporter les réponses à ces questions dans un marché autour de la donnée très mouvant, mais aussi progressant très vite technologiquement parlant.✖

Bertrand Garé



Les principales applications du lakehouse.

asp serveur | econocom

PARCE QUE CERTAINS SYSTÈMES SONT CRITIQUES
NOS SERVICES DATACENTER AFFICHENT 100% DE DISPONIBILITÉ DEPUIS 10 ANS

bsi. ISO/IEC 27001 Information Security Management

Certification ISO 27001 pour les services Datacenter, Cloud, hébergement, supervision NOC/SOC, administration, innovation, commercialisation

bsi. HDS Healthcare Data Storage

Certification Hébergeur de données de santé sur les 6 périmètres

PCI DSS Certified

Agrément PCI-DSS : Conformité et sécurisation des paiements

RGPD

Conformité RGPD, hébergement souverain, contrats de droit français

www.aspserveur.com
Email : commercial@aspserveur.com - Tel. 0805 360 888
Siège social : 785 voie Antiope, 13600, La Ciotat
SIREN 451 777 254 RCS Marseille

Euclidia

veut faire briller le logiciel européen

Alors que certains ministres semblent convaincus que les Européens n'ont guère d'avenir en matière de technologies, une poignée d'acteurs du logiciel se sont unis dans un collectif, Euclidia. Ce dernier entend bien démontrer que l'excellence technologique européenne existe bel et bien et que, non !, les Américains ne l'ont pas encore emporté sur le terrain du Cloud.

Peu avant que nous tombions tous dans notre torpeur estivale annuelle, un nouveau collectif a émergé pour faire bouger les lignes du Cloud européen. *L'European Cloud Industrial Alliance*, ou plus simplement Euclidia, est né à l'initiative de Jean-Paul Smets, fondateur de Nexedi et de Rapid.space, et de plusieurs entreprises et associations européennes, notamment françaises et allemandes.
Ainsi le groupe rassemble Abilian, Amarisoft, Beremiz, BlueMind, Clever cloud, E. corp, Jamespot, Innoroute, Linbit, Netframe, Nexedi, Nextcloud, ng-voice, Nitrokey, OpenSVC, Patrowl, Rapid.Space, Scaleway, SenX, Signal18, Submer, Vates et XWiki. Il est soutenu par le CNLL (Conseil national du logiciel libre), le FDL (Fonds de dotation du libre), OW2 et l'Eangti *(European Association of Next Generation Telecommunications Innovators)*.

Euclidia n'est pas Gaia-X

Cette nouvelle entité mêlant dans sa communication Cloud, logiciel libre et Europe, il n'a pas fallu longtemps pour que le parallèle soit fait entre Euclidia et Gaia-X. Pour autant il serait erroné de croire que le nouveau projet se construit en opposition à Gaia-X, les deux ne sont d'ailleurs pas comparables.
Plusieurs membres fondateurs d'Euclidia font d'ailleurs partie de l'initiative franco-allemande précédente, voire en sont des cofondateurs. En outre Gaia-X est un projet aussi bien politique que technique, qui doit aboutir à la mise en place de data hubs et élabore une architecture commune facilitant l'interopérabilité, la réversibilité, la protection des données… Car l'initiative se concentre sur la couche « data ». Euclidia pour sa part se consacre à la « partie basse » de l'offre, la brique logicielle sous la data, sujet sur lequel s'interrogeaient déjà les trois fournisseurs de Cloud français comptant parmi les cofondateurs de Gaia-X.
Néanmoins force est de constater que Gaia-X a eu une influence sur la naissance d'Euclidia. On peut même parler d'une réaction moins au projet en soi qu'à certaines évolutions dans sa gouvernance. Pour Alain Garnier, CEO de Jamespot, *« Gaia-X est une très bonne idée, très intéressante par sa partie industrielle – normes communes, interopérabilité, etc. – mais a rapidement été noyautée. »* Yann Lechelle, CEO de Scaleway, reconnaît que le projet franco-allemand génère « d'énormes frustrations » car si certains se sont battus pour une gouvernance européenne de cette initiative qui entend fédérer divers acteurs, y compris américains et chinois, par la data, ce sont les acteurs proches des Américains qui l'ont emporté au dernier renouvellement du board en juin dernier. Puis Bleu, le projet d'un hyperscaler français monté par Orange et Capgemini avec pour premier partenaire Microsoft, a en quelque sorte mis le feu aux poudres. Tout comme les propos de l'exécutif sur le logiciel français.

L'Europe en retard ? Que nenni !

Aux yeux de Jean-Paul Smets, comme des autres membres d'Euclidia, il existe parmi les politiques français une croyance en une France et une Europe qui, en matière de logiciel, ne valent pas tripette. De Bruno Le Maire vantant les mérites des géants américains à Cédric O affirmant la victoire des Clouds américains, *« nous avons en commun d'avoir été extrêmement choqués d'entendre nos ministres parler de nous comme n'ayant pas la capacité de*

« Euclidia permet aussi de voir l'avenir du Cloud, les futures technologies qu'on trouvera dans les services de Cloud, et donne une chance de les intégrer dans des services européens plutôt qu'américains »

Jean-Paul Smets – fondateur de Nexedi et de Rapid.space

« *Euclidia défend les intérêts européens d'un point de vue logiciel sur les sujets du Cloud et discute avec toutes les parties prenantes de manière pédagogique autour de notre excellence logicielle* »

Yann Lechelle – Scaleway

faire notre travail et de réussir. On n'imagine pas de tels propos dans d'autres secteurs, l'agriculture par exemple », déplore Alain Garnier. On voit mal en effet un ministre français de l'Agriculture défendre le prosecco contre le champagne, ou un ministre de l'Économie soutenir que Volkswagen est meilleur que Renault.

« Cette croyance en un retard européen est complètement erronée », assène Jean-Paul Smets qui rappelle que ce sont des Européens qui ont été pionniers du Cloud à l'instar de Burges sur l'automatisation des opérations en 1991 ou encore Kamp et les conteneurs, en 1999. *« Euclidia, c'est d'abord montrer aux pouvoirs publics qu'ils sont dans l'erreur, montrer un par un les développements technologiques logiciels, et parfois matériels, qui existent en Europe et leurs succès »*, insiste-t-il. Car Euclidia n'entend pas créer un « méta-cloud » souverain, français ou européen. Le collectif est né de la volonté de *« représenter les intérêts européens d'un point de vue technologique »*, selon Yann Lechelle. Soit un lobby qui s'organise à travers *« des acteurs européens dont les activités logicielles génèrent une très forte valeur ajoutée, défend les intérêts européens d'un point de vue logiciel sur les sujets du Cloud et discute avec toutes les parties prenantes de manière pédagogique autour de notre excellence logicielle »*.

Lobby

D'où l'existence de ce groupe, qui ne s'est pas construit à partir d'une page blanche. La plupart de ses membres se connaissent bien et travaillaient déjà ensemble, mais aussi bien par des projets commerciaux que techniques. *« Nous n'avons pas besoin d'un projet Euclidia pour travailler ensemble, pas besoin d'un projet géré de façon centralisée pour travailler en pair à pair »*, souligne Jean-Paul Smets. Mais il est également question d'y associer des entreprises qui n'ont pas pour habitude de jouer dans les mêmes catégories, notamment des acteurs de l'Open Source. *« La question, c'est comment ouvrir les communautés open source à ceux qui ont des solutions propriétaires, et inversement, et comment partager la valeur créée »*, nous explique Alain Garnier. On voit déjà poindre des idées qui dépassent la seule représentation d'intérêts communs au sein d'Euclidia, mais, pour le fondateur de Nexedi, il est encore trop tôt pour se lancer dans l'intégration technique ou les collaborations commerciales. *« Notre première action concrète, c'est de diffuser les success cases du Cloud européen. Et ensuite de demander la mise en place de quota pour le Cloud en Europe, que ce soit grâce aux règles sur l'exception culturelle de l'OMC ou à un type de Small Business Act »*, précise Jean-Paul Smets. Les projets commerciaux, par exemple la mise en relation des demandeurs et des entreprises d'Euclidia, ne viendra qu'après, et encore… si c'est pertinent. L'objectif premier reste de renforcer la visibilité des développements technologiques européens.

« Nous sommes tous membres d'autres associations, et nous avons pour principe de ne pas faire ce qui est fait ailleurs, c'est pour ça que Euclidia est sur un créneau très restreint, avec une idée de coordination relativement souple d'un grand nombre d'acteurs industriels avec des associations existantes en cas de besoin d'un relais », souligne Jean-Paul Smets. *« Euclidia permet aussi de voir l'avenir du Cloud, les futures technologies qu'on trouvera dans quelques années dans les services de Cloud, et donne une chance de les intégrer dans des services européens plutôt qu'américains »*, ajoute-t-il. Avec peut-être à la clé des interconnexions entre les solutions de chacun, moins dans le cadre d'Euclidia que de partenariats multilatéraux. Les ponts entre les différents acteurs sont en tout cas un des sujets de discussions sur les flux du collectif. Mais, contrairement à Gaia-X, pas question pour Euclidia de proposer un schéma d'architecture. *« Si nous devons un jour proposer quelque chose, ce seront des briques techniques issues de chacun des acteurs qui viendront consolider quelque chose de commun »*, assure Alain Garnier. *« Je pense que ce modèle est plus résilient qu'une grande cathédrale. »*

Guillaume Périssat

© Nathalie-Oundjian

« *Nous avons en commun d'avoir été extrêmement choqués d'entendre nos ministres parler de nous comme n'ayant pas la capacité de faire notre travail et de réussir* »

Alain Garnier – CEO de Jamespot

Customs Bridge s'appuie sur OVH pour développer sa solution

Customs Bridge est une start-up dans le domaine de la « deep tech », de jeunes entreprises qui appuient leurs solutions sur l'Intelligence artificielle ou l'apprentissage machine, pour créer un moteur de classification de produits automatique.

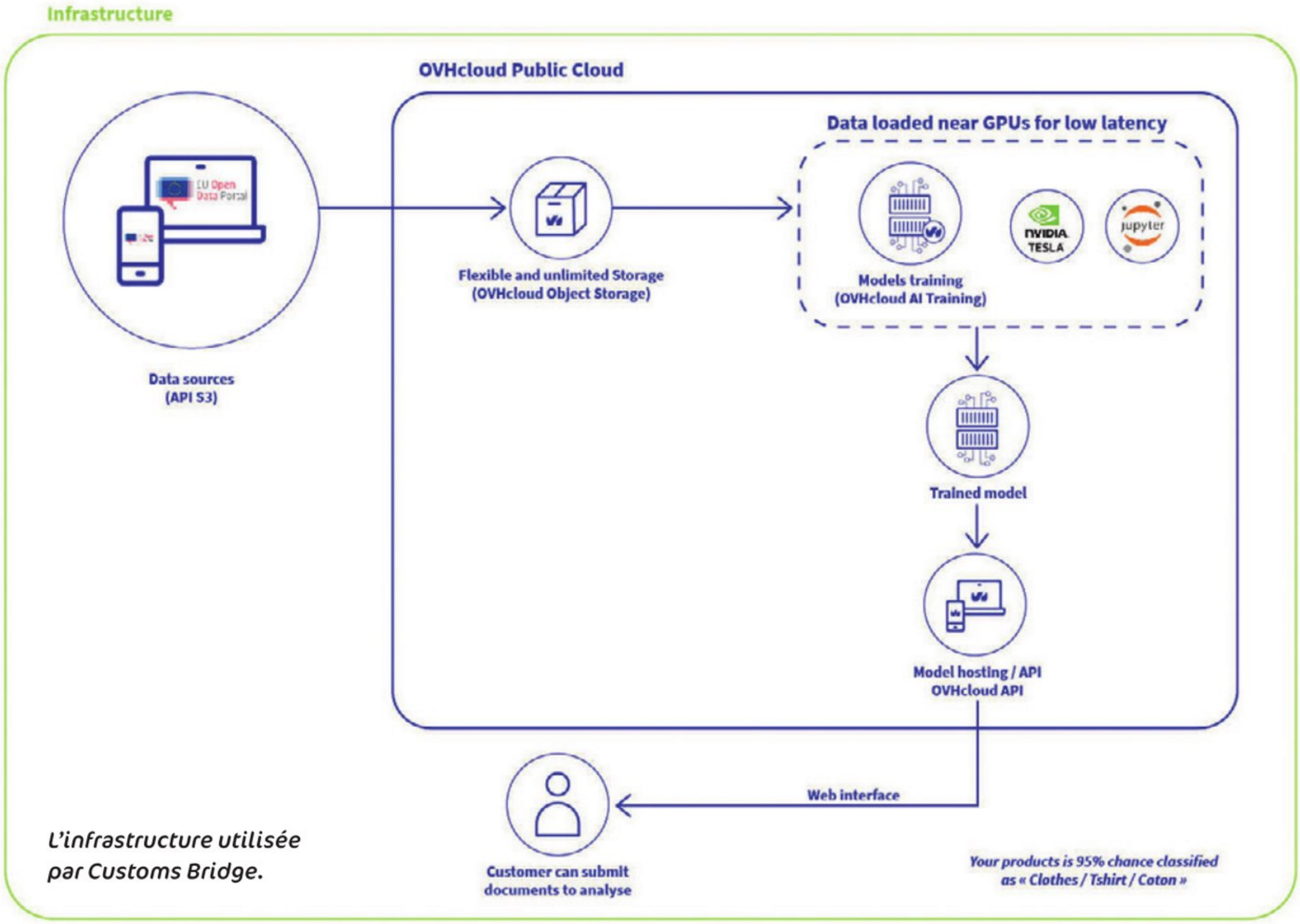
La start-up Customs Bridge destine ce service aux importateurs européens car chaque produit importé dans l'Union Européenne doit être précisément catégorisé selon une nomenclature qui compte plus de 24 000 entrées. Toute la complexité pour les importateurs est de choisir la bonne catégorie à partir du descriptif fourni par le fabricant, un descriptif qui peut être très succinct, voire incomplet. Tout produit importé dans l'Union Européenne doit être déclaré selon un code en fonction duquel les droits de douane sont calculés. Ce code définit aussi la réglementation qui va s'appliquer au produit. Toute erreur d'affectation peut donner lieu à des sanctions, à un retrait du marché et à des redressements fiscaux. Cette classification peut être parfois très compliquée car, si ce code est uniforme dans la Communauté Européenne, il peut être différent d'autres pays comme les États-Unis, la Chine ou maintenant le Royaume-Uni. Par exemple, le descriptif d'un produit peut aussi le faire basculer d'une catégorie à une autre, un bracelet-montre n'étant pas classifié de la même façon qu'une chaîne de montre. La gageure pour Customs Bridge est de créer un moteur de classification de produit le plus fiable possible pour affecter le bon code douanier à un produit même si le descriptif est plus ou moins formalisé. Hamza Saouli, directeur de l'Innovation de l'entreprise précise la genèse du moteur. *« Pour réaliser l'apprentissage de nos modèles d'Intelligence artificielle, nous avons commencé par utiliser des données accessibles en Open Data, notamment la base de données communautaire EBTI, pour European Binding Tariff Information. »* Il ajoute que cette base de données compte 250 000 lignes mais qu'elle ne couvre *« que 10 à 15 % de la nomenclature complète. Nous avons pu lancer*

« Avec les GPU Nvidia V100 mis à disposition par OVHcloud, l'apprentissage d'un Transformers sur 250 000 lignes ne représente qu'une trentaine de minutes de calcul »

Hamza Saouli – directeur de l'Innovation chez Customs Bridge

ML Serving : l'accélérateur d'apprentissage machine

Que ce soit sur un modèle propre ou un modèle fourni par OVH, ML Serving permet de le déployer et de l'exploiter en quelques clics, via une API dédiée, pour quelques analyses ou le traitement d'un important volume de données. Que vous exportiez vos modèles directement (via Scikit-Learn, Pandas ou Keras) ou que vous utilisiez des logiciels comme Dataiku ou H20.Ai, ML Serving accepte vos modèles aux formats standard en data science : ONNX, PMML et TensorFlow. L'infrastructure sous-jacente suit les besoins pour procurer une expérience optimale. Certifiée HDS, la solution peut héberger des données de santé. Chaque déploiement est versionné et s'effectue sans coupure pour la mise à jour des modèles. Cette offre complète celles proposées autour des GPU, ou les travaux de calcul sur Spark.



L'infrastructure utilisée par Customs Bridge.

l'entraînement de plusieurs modèles d'apprentissage sur cette source de données avec des résultats probants sur un code, un chapitre. Sur les produits électroniques importés de Chine, généralement bien décrits, cet apprentissage a obtenu de bons résultats mais sur des produits moins fréquemment importés nous n'avons pas eu de résultats probants faute de données disponibles en grande quantité et de bonne qualité ».

Pour disposer d'un volume de données plus important, l'éditeur a dû utiliser des modèles plus avancés de réseaux de neurones et l'infrastructure en place ne suffisait plus pour répondre efficacement à ces nouveaux besoins. C'est à ce moment que Customs Bridge s'est tourné vers la solution d'OVH dédiée à l'entraînement des modèles. En parallèle, la start-up exploite des instances OVH afin de déployer ses modèles en production et supporter le pipeline d'alimentation en données. Dans un avenir proche, ce pipeline est appelé à devenir plus complexe. L'équipe travaille sur un « augmentateur de texte », un algorithme qui part d'un jeu de données existant et qui va l'enrichir afin d'optimiser l'apprentissage des modèles. L'algorithme va ainsi faire passer la base de données initiale de 200 000 ou 300 000 lignes pour la faire monter à 3 ou 4 millions de lignes via des techniques de génération de texte automatique. Pour entraîner ses premiers modèles de Transformers, le directeur de l'Innovation s'est appuyé sur environ 2,5 To de données. Pour les modèles de Machine Learning, les volumes de données sont plus faibles, de l'ordre de 30 à 40 Go de données d'entraînement. *« Avec les GPU Nvidia V100 mis à disposition par OVHcloud, l'apprentissage d'un Transformers sur 250 000 lignes ne représente qu'une trentaine de minutes de calcul. C'est à la fois très rapide et le coût est véritablement modique puisqu'une heure de calcul est facturée environ 1,75 €. C'est la raison pour laquelle nous n'envisageons absolument pas d'acquérir de machines pour réaliser ces calculs en interne »*, ajoute l'expert.

En parallèle à ce travail mené sur les modèles d'IA, Hamza Saouli travaille aujourd'hui sur un chatbot qui interagira avec les clients pour obtenir les informations sur le produit recherché. Outre l'apprentissage de ses modèles, phase traditionnellement très coûteuse en espace mémoire et en puissance de calcul, Customs Bridge réfléchit aujourd'hui à la scalabilité de son modèle au niveau de la production lorsque la start-up signera ses premiers clients avec la possibilité d'utiliser la solution ML Serving d'OVHcloud. ✖

B. G.

Un programme **pour les start-up**

OVH propose depuis 2015 un programme de soutien aux start-up. Déjà 1 800 entreprises ont rejoint ce programme à ce jour. Concrètement le programme offre jusqu'à 100 000 € (équivalent devise locale) de crédits technologiques offerts à utiliser des solutions cloud, un maximum de vingt heures d'accompagnement spécifique et des solutions cloud. Ils s'y ajoutent des outils marketing comme la présence conjointe sur des événements internationaux, la publication de cas d'usages et de témoignages et des opportunités de prise de paroles pour présenter sa start-up. OVH peut aussi jouer le rôle d'entremetteur d'experts en propriété intellectuelle, d'incubateurs, de sociétés de capital-risque ou accélérer l'accès à d'autres programmes de soutien d'OVH.

COMPUTEX

Laptops, desktops et serveurs font le show !

Annulé en 2020 en raison de la pandémie de Covid-19, le salon taïwanais Computex a pu se tenir cette année lors d'une longue session virtuelle. À l'occasion de cette grand-messe, les fabricants asiatiques – mais pas seulement – ont pu présenter quelques-unes des principales nouveautés de l'année. Certains produits sont d'ores et déjà disponibles quand d'autres le seront d'ici peu. Tour d'horizon des principales annonces dans le secteur des ordinateurs portables, PC de bureau et autres serveurs.

L'Asus Flow X13 marie jeu et travail.

Le salon taïwanais Computex a pu se tenir via une session virtuelle qui s'est déroulée dans un format regroupant keynotes, présentations de produits et conférences autour de thèmes comme la 5G, l'innovation ou l'Intelligence artificielle. L'occasion pour les grands fabricants asiatiques d'annoncer des PC portables et de bureau et des serveurs. Le contingent le plus important concerne les laptops de stars, comme Asus et Acer.

Asus a ainsi présenté des appareils pour les gamers, dont le ROG (Republic of Gamers) Flow X13. Cet ultra-portable se distingue par sa double utilisation : le mariage entre jeu et travail. Il s'agit d'un *deux-en-un* de 13 pouces et 1,3 kilo, avec une carte graphique Nvidia GeForce GTX 1650 et un processeur AMD Ryzen de 3,1 GHz. Pour améliorer l'expérience de jeu, Asus y associe la station XG

Mobile et son processeur graphique externe avec une carte Nvidia GeForce RTX 3080. Cette unité mobile dispose de sa propre alimentation (280 watts) qui peut faire fonctionner le Flow X13, de quatre ports USB-A, de connexions DisplayPort et HDMI, d'une prise Ethernet et d'un emplacement pour carte SD. Cette association dispense un système rapide aux multiples facettes pour les gamers exigeants. Le jury des Computex d&i Award ne s'y est pas trompé en accordant un prix à ce combo. Asus a aussi présenté son nouveau ROG Zephyrus Duo 15 SE GX551 (15 pouces), également récompensé par un d&i Award. Ce laptop est doté d'un processeur AMD Ryzen 7 de 3,2 GHz, d'une carte GeForce RTX 3060 et d'une mémoire de 16 Go (DDR4) extensible à 32.

Un premier 17 pouces

Parmi les poids lourds taïwanais, Acer a dévoilé son dernier-né : le Swift X. Le fabricant annonce faire *« passer le design des PC ultra-portables au niveau supérieur »*, avec son processeur AMD Ryzen 5000 Series, une carte Nvidia GeForce RTX 3050 Ti et 16 Go de mémoire. D'un poids de 1,39 kg et 17,9 mm d'épaisseur, cet ultra-portable revendique une autonomie allant jusqu'à 17 heures. *« Les portables d'Acer sont conçus pour offrir le plus grand choix possible d'appareils informatiques ultra-portables et performants »*, a commenté James Lin, directeur général des ordinateurs portables de la division produits informatiques d'Acer. Parmi les points forts du Swift X, on note la présence d'un capteur d'empreintes digitales, la suppression du bruit améliorée par l'IA et la technologie Acer BlueLightShield pour réduire la fatigue oculaire. Toujours chez Acer, il faut aussi noter la sortie de quatre gammes de chromebooks dans un large éventail de formes et de designs, y compris le premier chromebook 17 pouces (Acer Chromebook 317). *« Nous avons franchi une étape en étant le premier fournisseur de chromebook de 17,3 pouces, la taille idéale pour les utilisateurs qui travaillent à domicile »*, a annoncé James Lin. L'écran FHD est doté d'un revêtement antireflet sans oublier un processeur Intel Celeron N4500 et une autonomie annoncée de dix heures.

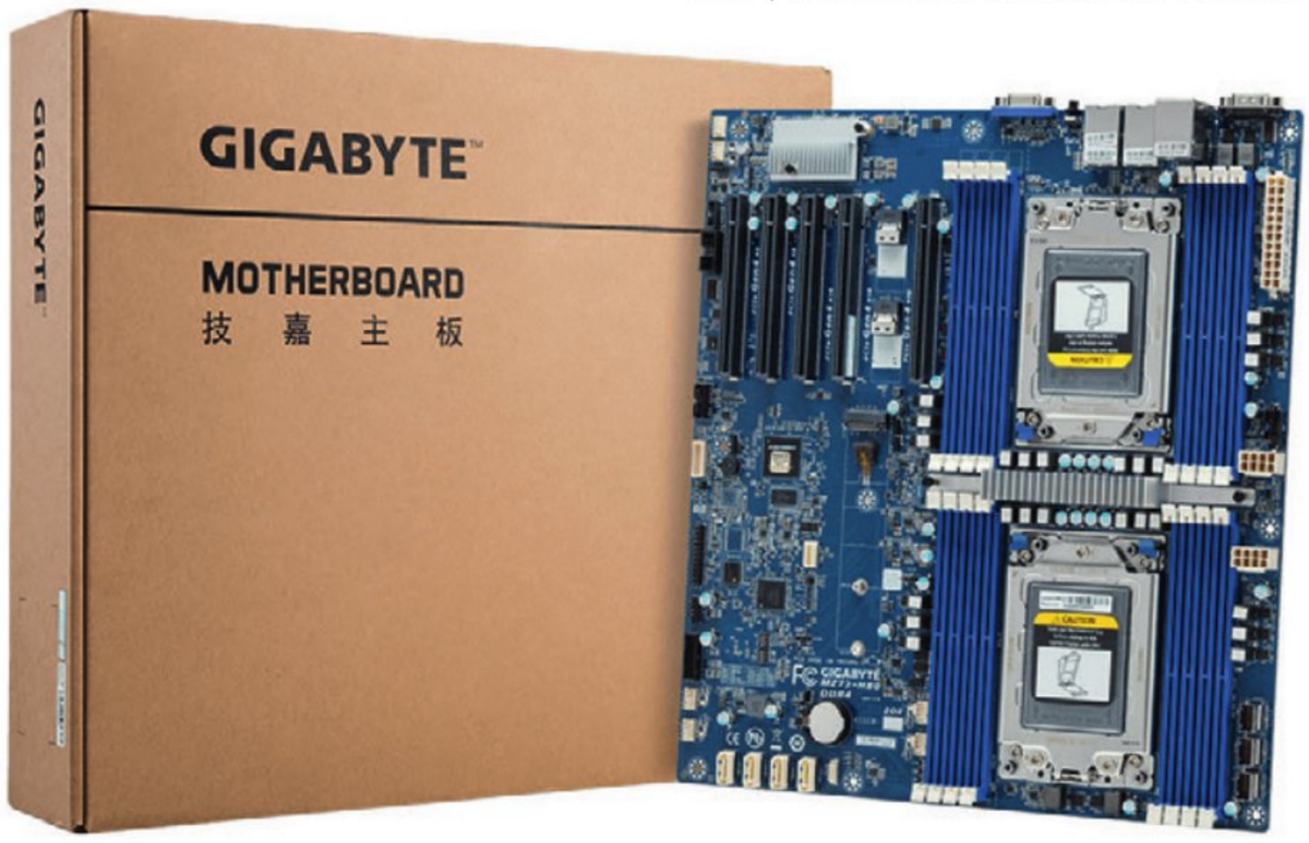
Acer propose 4 gammes de chromebooks offrant un large éventail de formes et de designs.

Zbox Magnus One, mini-PC puissant et polyvalent.

Des PC plus compacts

Concernant les PC de bureau, le Hongkongais Zotac a fait forte impression avec le Zbox Magnus One, un mini-PC puissant et polyvalent. Le Magnus One offre des performances intéressantes avec sa carte graphique GeForce RTX 3070. Celle-ci assure des graphismes *« haute-fidélités et des fonctions d'IA »*, souligne le fabricant. Avec un processeur Intel Core i7, une mémoire et un stockage évolutifs, des options de connectivité complètes avec le réseau Killer (WiFi 6), le Magnus One se veut idéal pour les jeux, les tâches quotidiennes, le divertissement et la création de contenu.

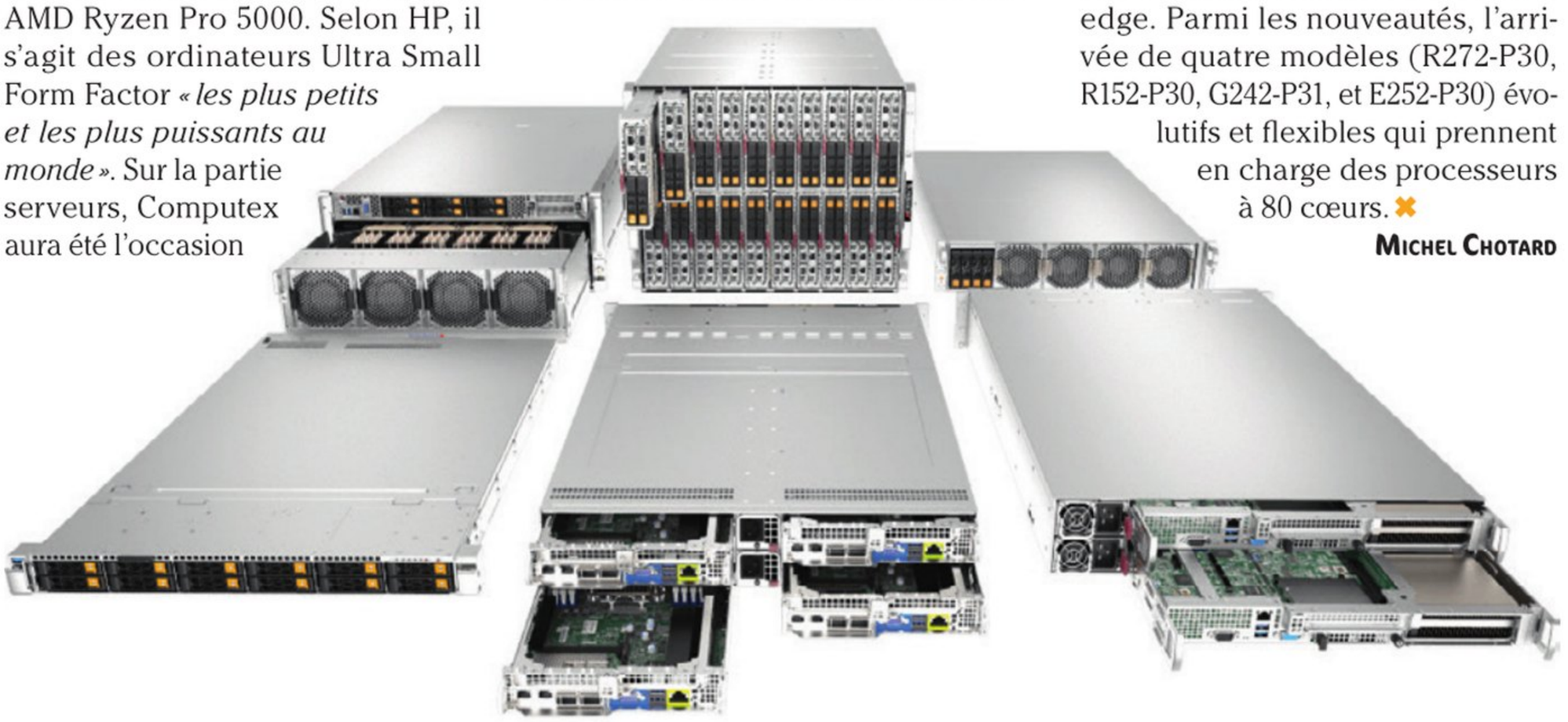
Chez Acer, le fabricant a annoncé le rafraîchissement de sa gamme de PC pour le gaming à travers les modèles Predator Orion 3000 et Nitro 50. Les



La carte mère Gigabyte MZ72-HBO, prend en charge les processeurs AMD EpycSerie 7003.

Acer rafraîchit sa gamme de PC pour le gaming à travers les modèles Predator Orion 3000 (photo) et Nitro 50.

produits ont été mis à jour avec l'installation des derniers processeurs Intel Core (11e génération) ou AMD Ryzen Serie 5000. Par exemple, le Predator Orion 3000 est conçu pour les joueurs qui recherchent une expérience totale grâce à la présence d'un processeur Intel Core i7, une carte graphique Nividia GeForce RTX 3070 et jusqu'à 64 Go de mémoire DDR4 à 3 200 Hz. Bien entendu, ce modèle affiche des performances de connexion optimale avec l'Intel Killer E2600 et une compatibilité WiFi 6. Lors de Computex, HP a également présenté de nouveaux PC de bureau dans ses gammes Elite et Pro. Ils seront dotés des dernières puces AMD Ryzen Pro 5000. Selon HP, il s'agit des ordinateurs Ultra Small Form Factor *« les plus petits et les plus puissants au monde »*. Sur la partie serveurs, Computex aura été l'occasion pour Super Micro Computer (SMCI) de dévoiler une gamme complète qui intègre les processeurs Intel Xeon. SMCI propose les systèmes d'économie d'énergie *« les plus performants avec de nouveaux systèmes intégrant les derniers processeurs Intel »*, a déclaré Charles Liang, président et CEO de la société taiwanaise, *« Notre nouvelle gamme de produits Hyper est conçue pour des performances maximales et peut accueillir 32 DIMM de mémoire haute vitesse, quatre processeurs haute performance et un LAN jusqu'à 400 Gbit. Cela répond aux besoins les plus exigeants de nos clients. »* Selon le fabricant, plusieurs solutions utilisant les processeurs Intel Xeon seront aussi bientôt disponibles, notamment des solutions certifiées Oracle Linux et SAP. SMCI a également indiqué que de nombreux produits de la gamme sont équipés des puces AMD Epyc.



Super Micro dévoile une gamme de serveurs économes en énergie.

À ce sujet, AMD a fait le point sur le lancement de la 3e génération de processeurs AMD Epyc, destinée à renforcer ses perspectives sur le marché des serveurs. *« Les processeurs AMD Epyc 7003 Series visent à améliorer les résultats pour les clients du Cloud et les entreprises en général »*, a expliqué Lisa Su, présidente et CEO d'AMD. Selon le manufacturier, ces processeurs doivent aider les entreprises en améliorant le traitement des bases de données, avec de meilleures performances dans les interactions entre homme et machines.

Du côté de Gigabyte, un large focus a été fait sur la carte mère MZ72-HBO, entièrement revisitée et prenant en charge les processeurs AMD Epyc Serie 7003. Cette carte offre une variété de caractéristiques, dont une grande capacité de stockage et comprend un port LAN Gigabit Management pour un accès à distance. Le Taïwanais a aussi annoncé la sortie de serveurs conçus pour les processeurs Ampere Altra. Basés sur l'architecture ARM, ces appareils devraient rencontrer du succès sur le marché des serveurs cloud et edge. Parmi les nouveautés, l'arrivée de quatre modèles (R272-P30, R152-P30, G242-P31, et E252-P30) évolutifs et flexibles qui prennent en charge des processeurs à 80 cœurs. ✖

Michel Chotard

MARDI 23 NOVEMBRE 2021

TOULOUSE - CENTRE DE CONGRÈS PIERRE BAUDIS

CBC

CYBER SECURITY Business Convention

Le salon de la Sécurité Numérique des Entreprises

80% des entreprises* envisagent d'acquérir des solutions de cybersécurité

Présentez la vôtre !

En savoir plus :

cbc-convention.com

* Source : Baromètre de la cybersécurité des entreprises - CESIN, janvier 2021

Organisé par : DÉPÊCHE EVENTS

Avec le soutien de : ADOCC, AGENCE DU NUMÉRIQUE EN SANTÉ, RÉPUBLIQUE FRANÇAISE, BOOST AEROSPACE, CESIN, RÉPUBLIQUE FRANÇAISE, CYBER MALVEILLANCE .GOUV.FR, CYBER'OCC, Gendarmerie nationale, La Mêlée, OCSSIMORE

Partenaires média : DÉPÊCHE ÉCO, Global Security Mag, L'1FO, LA DÉPÊCHE, la lettre M, Midi Libre

Booster les tests logiciels par l'IA

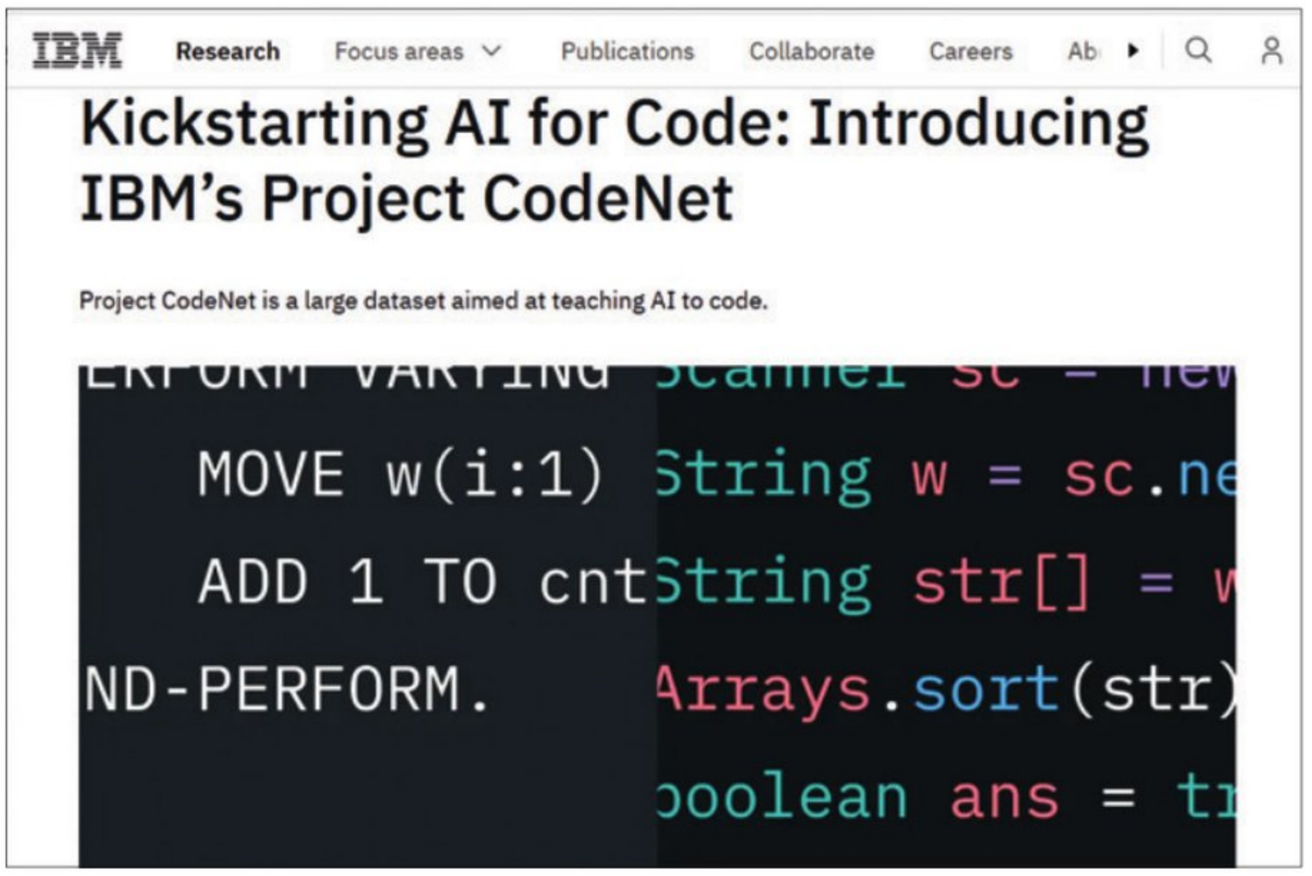
S'il est un domaine dans lequel l'Intelligence artificielle peut apporter de grands services, c'est bien celui des tests logiciels. L'IA peut soulager les testeurs des aspects les plus routiniers, répétitifs et sujets aux erreurs. Nous allons tenter ici de voir comment.

Les enjeux des tests logiciels à base d'IA

La nécessité de tester un logiciel à chaque phase de son cycle de développement est reconnue par tous les professionnels de l'IT. Cela reste néanmoins une activité coûteuse en temps et en argent et difficile à maintenir sur le long terme. Pour répondre à cette problématique, des outils et des techniques permettant d'automatiser une partie des tests logiciels ont été développés. Cette automatisation n'est pas si simple à mettre en place. Il faut écrire les scripts et les maintenir à jour de façon régulière. Ceux-ci deviennent de moins en moins pertinents au fil des modifications et leur évolution peut se transformer en maintenance pure, rajoutant de la complexité pour un gain de moins en moins évident. Comment faire, alors, pour ne plus rédiger tous les cas de tests ? C'est ici que l'IA intervient.

L'Intelligence artificielle, kesako ?

Le terme « intelligence » n'a pas la même signification en anglais qu'en français, ce qui est souvent source de confusion. En anglais, *intelligence* se traduit plutôt par savoir, connaissance, sans notion aucune de conscience. Le terme IA, de nos jours, s'entend globalement comme la capacité d'une machine à apprendre d'elle-même par la pratique et un nombre important de données de références (*Machine Learning* et *Deep Learning*), à communiquer avec les humains de manière « naturelle » sans suivre un programme déterministe, sous la forme d'une conversation – le fameux test de Turing, du nom du célèbre informaticien anglais qui a, entre autres choses, cassé le cryptage des nazis et facilité le débarquement allié. Les exemples les plus courants sont les ChatBots, la reconnaissance d'images, la traduction automatiques, le ML et le DL en général.



Grâce au projet open source CodeNet, et d'après nos amis de Big Blue, l'utilisation de l'Intelligence artificielle pour la correction du code des applications sort enfin du stade expérimental.

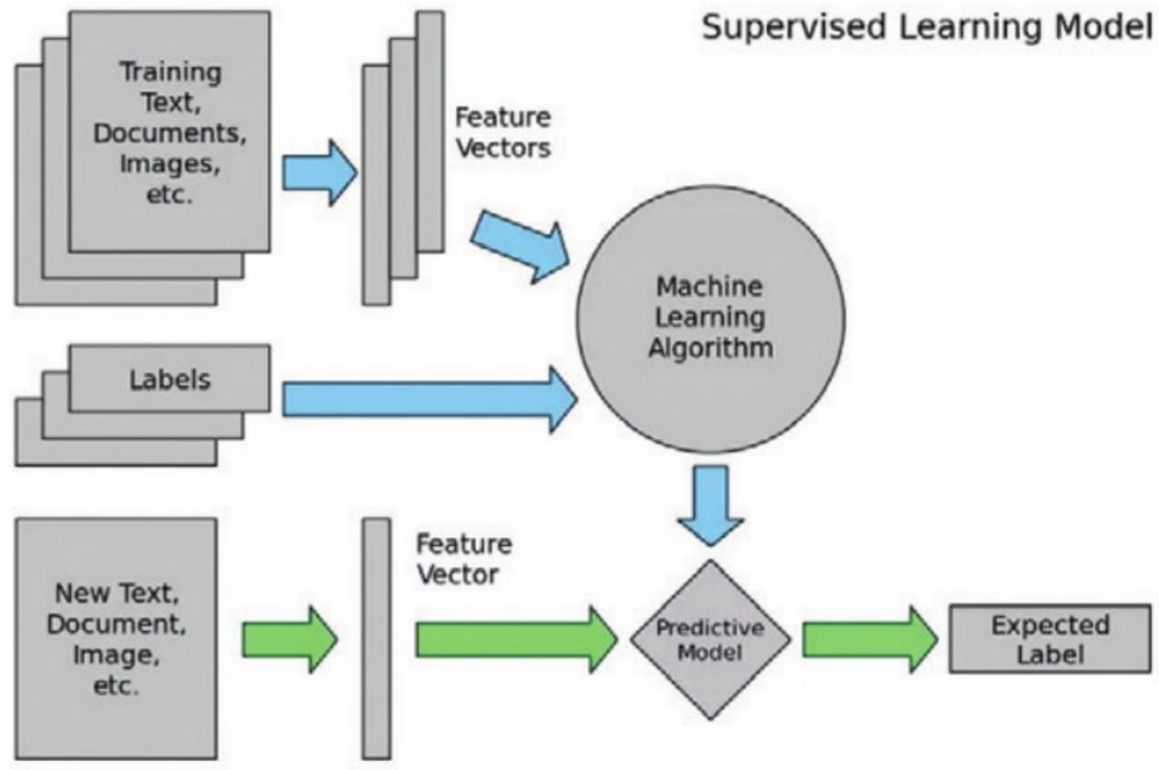
L'apport de l'IA pour le testing et les types de tests concernés

Le développement et l'intégration de l'Intelligence artificielle dans les tests logiciels permet d'introduire une certaine automatisation des tests tout en éliminant une maintenance importante. Le but recherché est qu'elle soit la plus autonome possible, l'objectif étant qu'à terme les IA soient capables de détecter automatiquement les nouveautés d'une application, de créer les tests adéquats et de déterminer s'ils sont conformes ou non et s'ils comportent des bugs. Plus une application avance dans son cycle de développement, plus elle devient complexe et plus les efforts à fournir pour la tester dans son intégralité sont importants. Les possibilités offertes par

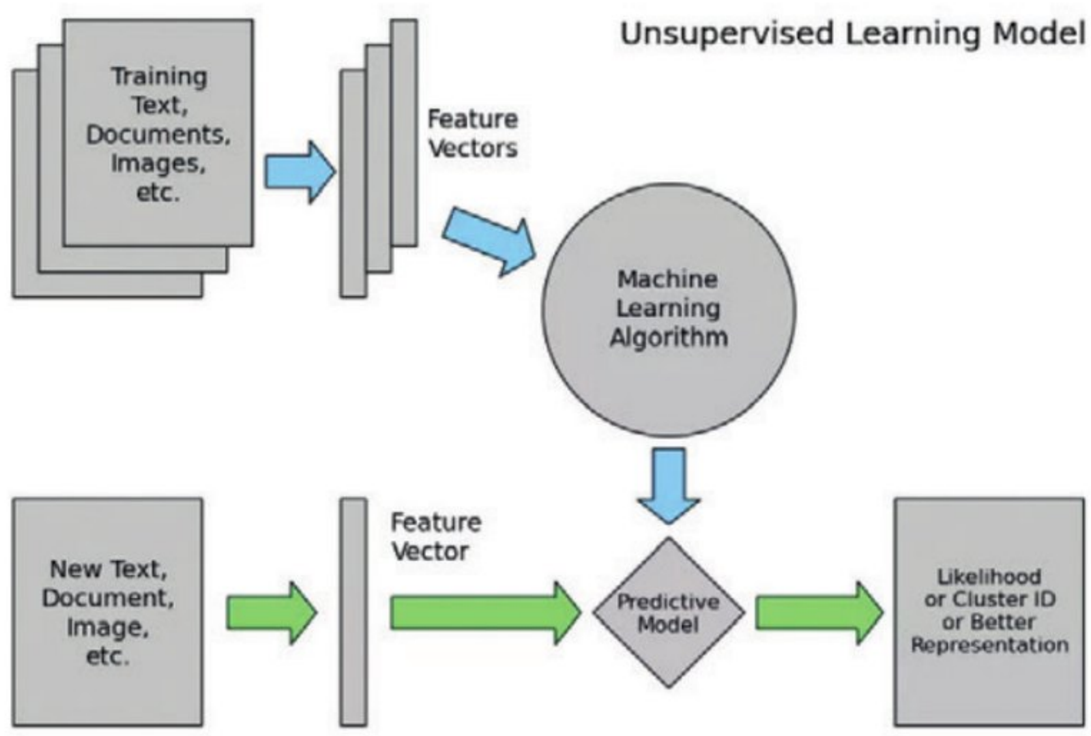
l'Intelligence artificielle appliquée dans ce domaine du test sont très encourageantes. Les IA dédiées à ce travail sont capables d'effectuer un nombre de tests très important dans un délai très court, de repérer et de documenter instantanément les changements apportés dans l'application. Elles prennent un « cliché » d'une application avant et après chaque mise à jour pour les comparer. Elles peuvent ainsi apprendre à mieux travailler et gagner en efficacité après chaque cycle de test. Les IA de tests ont depuis déjà un certain temps appris par ML et DL en traitant des milliers voire des millions d'applications. Les types de tests pour lesquels elles sont les plus efficaces sont les tests de spécifications, ceux de non régression (TNR), les stress test et la prédiction des anomalies. Elles sont de plus en plus à même de générer des scripts à partir des spécifications, de faire de l'analyse statistique et, bien entendu, de générer des données de test.

La prédiction des défauts ou anomalies du code d'un logiciel

L'idée est ici de créer une espèce de modèle prédictif à partir des releases précédentes afin d'estimer le plus précisément possible les parties du code où le risque de rencontrer des défauts sera le plus élevé. Ceci est d'autant plus intéressant lorsque la release comporte un nombre de lignes de code très important. Cela permet de prioriser les composants à tester et d'ainsi optimiser l'effort de test (approche classique préconisée par l'ISTQB). Cela se fait via la vectorisation des données d'entrées qui prend en compte différents indicateurs. Ceux-ci sont la complexité du code, le nombre de lignes de code, la métrique d'Halstead, le nombre cyclomatique, celui de dépendances, le processus de développement, les révisions du composant, le nombre de refactoring, le nombre de corrections par rapport à leur ancienneté, le nombre de lignes de code modifiées, l'ancienneté du composant, l'identité du/des développeur(s) et le nombre de développeurs qui sont intervenus sur le module ou le projet global.



Deux grandes méthodes permettent à l'Intelligence artificielle « d'apprendre » : de manière supervisée ou de manière non supervisée.



Amélioration des tests exploratoires et rétro modélisation

L'IA peut également aider à l'automatisation de l'établissement du flow graph des applications. La problématique qui se pose généralement avec ce graphe est qu'il peut être très grand et du coup très difficile de le parcourir pour arriver à une branche pertinente et tester une fonctionnalité de l'application. L'IA peut être entraînée à reconnaître les étapes les plus importantes d'un flow graph afin de fluidifier son parcours automatique. Dans le cas de tests exploratoires, cela permettrait par exemple de parcourir l'application en commençant par les cas d'usages (use case) les plus employés par une première analyse de l'application et de son utilisation. Cela peut également permettre de générer des cas de test de non régression (TNR) de façon plus ciblée, sans devoir modéliser manuellement l'application en amont (approche de type MBT : Model Base Testing, complétant l'approche TDD, Test Driven Development).

Reconnaissance de forme

Les IA employées dans le domaine de la vision par ordinateur peuvent permettre de reconnaître certains éléments d'une interface graphique par leurs caractéristiques. Elles peuvent être employées pour automatiser une partie des tests d'affichage, soit à partir d'un modèle donné alimentant l'IA

en analysant ce qui ne correspond pas au dit modèle d'une version à l'autre, soit en corrigeant/réécrivant automatiquement des scripts d'automatisation de test lorsqu'un script ne fonctionne plus ou qu'un objet n'est plus reconnu.

Application à l'optimisation des TNR

L'IA peut aussi être employée pour analyser les TNR (Tests de Non Régression) existants afin de trouver la meilleure combinatoire et le meilleur ordre d'enchaînement. Les points concernés sont, principalement, les tests diminuant le temps d'exécution, la réduction du nombre de cas de tests pour atteindre un objectif de testing, les tests permettant une couverture complète, ceux liés à des changements de code récents et les tests dépendant d'exigences avec un risqué élevé.

Quels sont les outils de testing automatique employant l'IA ?

Parmi les quelques exemples d'outils de testing faisant d'ores et déjà usage de l'Intelligence artificielle, nous pouvons citer Austin, EvoSuite, Functionize, Infer ou Intellitest. Infer est un outil d'analyse statique de code Java et Objective-C utilisé entre autres par Facebook pour ses développements d'application mobile. Il est capable de détecter automatiquement des anomalies dans le code via une approche Devops.

EvoSuite est capable de générer automatiquement des cas de test pour des projets écrits en Java. Il gère la couverture globale du code.

EvoSuite, des tests unitaires pour Java

Pour réussir à trouver des dysfonctionnements dans un logiciel, il faut créer des cas de test automatiques, des oracles et des prédictions évaluant l'exactitude du comportement observé lors de l'exécution du logiciel. EvoSuite est capable de générer automatiquement des cas de test avec des assertions pour les classes Java. Il applique pour cela une nouvelle approche hybride en générant et optimisant les ensembles de test complets. Son algorithme est évolutif. Il créé une population initiale générée au hasard avec l'évaluation des performances de chaque individu. EvoSuite gère la couverture globale du code, les mutations et la reproduction par mélange des caractéristiques de chaque individu ainsi que la réitération du processus.

Voici, en résumé, ce que propose EvoSuite :

- La génération de tests JUnit pour les classes sélectionnées
- L'optimisation de différents critères de couverture tels que les lignes, les branches, les sorties et les tests de mutation
- La réduction du nombre de tests : seuls ceux contribuant à la couverture sont conservés
- La génération de JUnit permet de capturer le comportement des classes testées
- Les tests s'exécutent dans un bac à sable afin d'éviter tout risque potentiel
- L'emploi d'un système de fichiers et d'un réseau virtuels.

IntelliTest for .NET, les tests unitaires avec Visual studio

L'écriture d'une combinaison de tests unitaires exerçant et validant de manière exhaustive la logique du code n'est pas si aisée. La fonctionnalité IntelliTest d'expédition dans Visual

Les différentes types d'apprentissage **des IA**

Une IA peut «apprendre» selon deux grandes méthodes, soit de manière supervisée, soit de manière non supervisée. Avec la méthode supervisée, la machine apprend via des exemples fournis avec des résultats attendus, avec des réponses de type OK/KO sur les données d'apprentissage. Le résultat dépend alors grandement du volume des données mais aussi de leur qualité. En employant l'autre méthode, la non supervisée, les valeurs de sorties ne sont pas totalement prévisibles. Les algorithmes d'apprentissage non-supervisés doivent être capables de trouver des corrélations dans les données d'entrée. Cela permet de réaliser des regroupements de fonctions ou d'objets ou ayant un comportement attenant ou de détecter des comportements anormaux relativement aux comportements habituels de telle fonction ou telle application, cela pouvant être très utile pour détecter d'éventuelles anomalies.

Studio Enterprise Edition permet d'obtenir une couverture de code élevée pour un coût raisonnable. Lorsque vous exécutez IntelliTest sur votre code .NET (C#, VB .Net, F#, …), il génère des cas de test en analysant dynamiquement le code du programme. C'est un outil encore assez sommaire mais très pratique.

Functionize

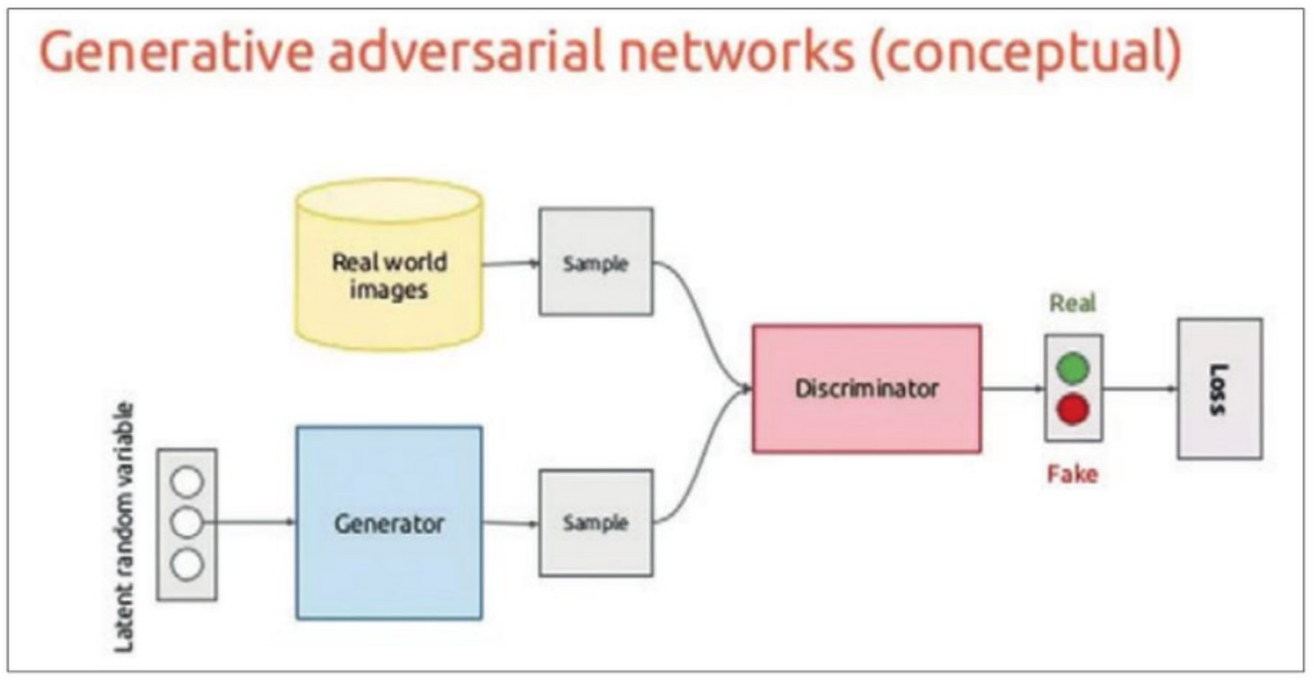
Functionize est un outil dans le Cloud pour l'enregistrement des tests basé sur une extension Chrome. Il génère automatiquement des tests à partir des utilisateurs réels des sites web.

Sapienz

Open source, Sapienz est un outil basé sur les techniques de recherche méta-heuristique (algorithme génétique, recherche de type tabu, emploi de l'optimisation combinatoire…). Son rôle est d'optimiser des données et des cas de test.

Appdiff

Appdiff s'utilise uniquement sur les applications Android. C'est un outil SaaS permettant d'uploader le fichier apk d'une application Android pour le faire analyser. Contrairement à du monkey testing, l'IA permet de parcourir les branches les plus pertinentes de l'application en classifiant les actions réalisables pour chaque interface d'affichage.



Les GAN (Generative Adversarial Network) permettent de gérer deux types d'IA à la fois, l'une spécialisée dans la classification et l'autre dans la génération de données.

En résumé, les outils de testing employant l'IA se concentrent principalement sur les tests unitaires, l'intégration, l'affichage et la génération de données de test. Ils se positionnent comme des outils d'aide aux testeurs avec la réparation automatique des scripts et l'analyse de risque. Les nouvelles IA de testing, les GAN notamment (lire l'encadré), ne sont pas disponibles dans tous les outils proposés actuellement, loin s'en faut.

Automatisation des tests sans code

Le mouvement no-code ayant pris de l'ampleur depuis déjà quelques années, il devient de plus en plus pertinent dans le domaine des tests. Les outils de test sans code sont basés sur des algorithmes d'IA qui utilisent la modélisation visuelle pour créer rapidement et automatiquement des

cas de test. Tout cela doit être basé sur d'autres tests automatisés développés au préalable par des ingénieurs qualité, mais cela reste une excellente alternative pour écrire facilement des scénarios de test en peu de temps. Les tests sans code étant efficaces et très faciles à réviser, de plus en plus d'outils tels que Ghost Inspector, tests.ai, Testsigma, ou TestComplete sont employés par de petites entreprises.

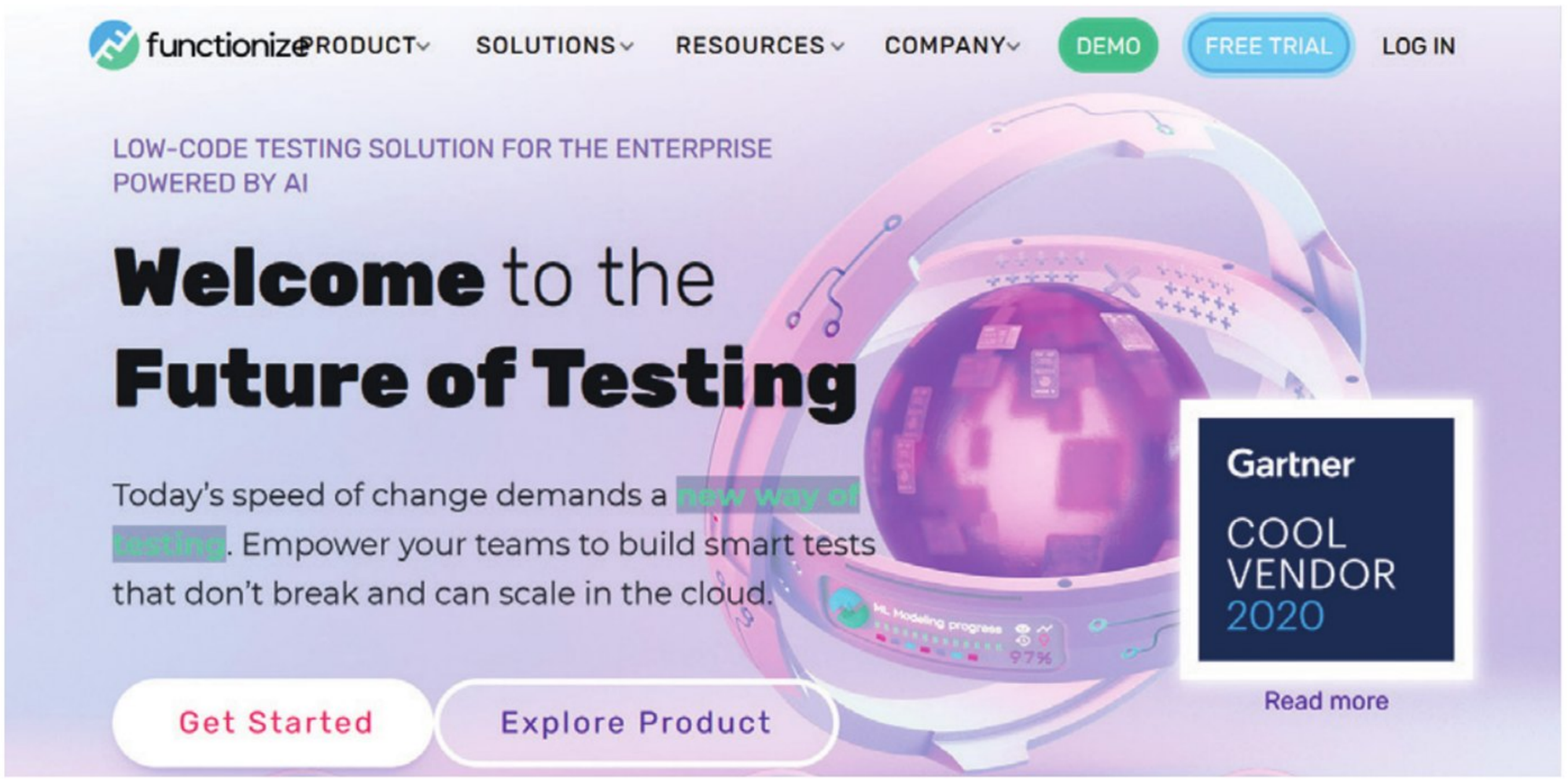
IBM dope la correction de code à l'IA avec CodeNet

Le projet open source CodeNet (https://github.com/IBM/Project_CodeNet) vise à faire pour l'IA for code ce que ImageNet a fait pour la vision par ordinateur, dixit IBM. L'utilisation de l'Intelligence artificielle pour la correction du code des applications sort enfin du stade du Proof-of-concept, toujours d'après Big Blue. Avec sa volumineuse base d'échantillons de code, le projet va contribuer à sa généralisation. L'énorme dataset de CodeNet comprend près de 14 millions de soumissions de code, dont plus de la moitié sont acceptées, les autres étant associées à différentes causes de rejet. Le projet CodeNet a l'ambition d'aller plus loin dans *l'AI for code*. Il a pour objectif de fournir à la communauté un vaste ensemble d'exemples de code, organisé et diversifié. Il comporte en tout 500 millions de lignes de programmation dans plus de 55 langages différents : 95 % d'entre elles dans l'un des six langages les plus couramment employés : C, C++, C#, Java, Python et Ruby. Chaque échantillon est présenté comme une solution à l'un des 4 000 problèmes de codage. Ce qui distingue CodeNet des initiatives déjà menées, c'est d'une part la mise à disposition d'exemples sur plus de 50 langages, avec différentes informations : la taille, l'empreinte mémoire, le runtime CPU, ainsi que le statut qui indique les types d'acceptation ou d'erreur. Plus de 90 % des problèmes rencontrés sont décrits, avec les formats d'entrée et de sortie. *« Les utilisateurs peuvent exécuter les échantillons de code acceptés afin d'en extraire des métadonnées supplémentaires et de vérifier l'exactitude des résultats des modèles d'IA génératifs »*, toujours d'après IBM.✖

Thierry Thaureaux

Les GAN

Les *Generative Adversarial Network* (GAN) permettent d'entraîner deux intelligences artificielles à la fois, l'une appliquée à la classification, l'autre à la génération de données appartenant à l'une des classes déterminées par la première. Elles génèrent de manière autonome des jeux de données de test. Le traitement peut se résumer ainsi : génération des données d'entrées (jeux de données de test) et classification des données d'entrées pertinentes. Elles sont, à l'heure actuelle, appliquées essentiellement au traitement d'images mais leur utilisation s'étend à d'autres domaines. Il ne faut pas perdre de vue que les données d'entrées représentent une problématique majeure du testing. Plus le spectre d'utilisation du logiciel est grand, plus la création et la sélection de tests pertinents par le testeur est longue et complexe. Le testeur doit à la fois générer des configurations de tests dans un espace très grand et faire en sorte qu'elles soient pertinentes. C'est exactement ce que fait un GAN en générant des données déjà classifiées.



Avec Functionize, vous entrez de plain pied dans le monde des solutions de testing low code pour vos sites web.

www.linformaticien.com

ABONNEZ-VOUS À L'INFORMATICIEN

linformaticien.com/abonnement

Une **offre triple** pour ne rien manquer
des dernières tendances
et innovations de la transformation numérique

MAGAZINE

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

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

NUMÉRIQUE

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

1 AN : 49 €
2 ANS : 89 €

COUPLAGE

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

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

Accès aux versions numériques seules des deux publications.

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

Certification cloud

Le ticket gagnant pour booster une carrière

Quelles sont les meilleures certifications cloud ? Quels types de connaissances et de compétences faut-il avoir et comment les obtenir ? Voici quelques éléments de réponse.

Un an et demi après le début de la pandémie, les entreprises continuent d'adopter les technologies cloud à marche forcée. Les demandes d'emplois liés au Cloud ont littéralement explosé, mais les employeurs se retrouvent confrontés à une pénurie d'experts dans ce domaine qui nécessite des connaissances et des compétences bien spécifiques. Rien que sur la plate-forme LinkedIn, plus de 13000 emplois sont à pourvoir actuellement en France dans le Cloud Computing!

Dans ce contexte, obtenir une ou plusieurs certifications cloud peut constituer un énorme avantage concurrentiel pour débuter ou améliorer une carrière. Les certifications cloud permettent non seulement de valider une expertise, mais également de prouver à un employeur que l'on possède bien les aptitudes qu'il recherche.

Il existe différentes certifications délivrées par les principaux fournisseurs de services tels que AWS, Google Cloud Platform, Microsoft Azure, IBM, Salesforce, VMware, etc.

De plus en plus d'entreprises ont besoin de profils spécialisés pour les aider à gérer leurs options cloud, sécuriser leurs documents, et maintenir leurs systèmes à jour. Les experts en Cloud Computing constituent désormais les profils les plus recherchés dans l'industrie de la tech et la concurrence fait rage. L'obtention de certifications est devenue quasi indispensable dans ce secteur en croissance constante. Elles ont pour but de valider les connaissances et les compétences acquises pour gérer, développer, et fournir des services de solutions cloud pour les entreprises. Il est difficile de dire quelle est la meilleure certification cloud, mais certaines s'avèrent plus prisées et reconnues par les employeurs que d'autres. Les certifications des poids lourds du marché, AWS, Google, Microsoft, sont considérées comme les meilleures en 2021.

Les certificats de connaissance en sécurité cloud (CCSK) pouvant être obtenues auprès de l'organisme neutre *Cloud Security Alliance* jouissent également d'une excellente réputation. Cet acteur majeur de la sécurité cloud a l'avantage de proposer d'acquérir des compétences en sécurité pouvant être appliquées à d'autres plates-formes. En règle générale, les meilleures certifications sont celles qui correspondent le mieux à ses besoins en fonction de son niveau d'expertise, ses objectifs et

l'entreprise ciblée. Acquérir une certification d'une solution cloud moins répandue (IBM, VMware, Saleforces…) que celles des géants du marché peut néanmoins représenter une énorme valeur ajoutée pour décrocher un poste dans une entreprise qui l'utilise. Face aux nombreuses certifications cloud proposées, il est donc impératif de bien peser le pour et le contre avant de faire son choix.

Préparer les tests des certifications

Le Cloud, qui représente un marché de plusieurs centaines de milliards par an, est le nouvel eldorado de l'économie et par ricochet celui du marché de l'emploi. Les entreprises manquent toutefois cruellement de compétences disponibles et des milliers d'emplois restent vacants. Les géants du Cloud redoublent donc d'efforts pour faire face à la demande et aider les professionnels de l'IT à se former gratuitement pour obtenir des certifications cloud. AWS, Microsoft, Google et bien d'autres ont développé des programmes de formation en ligne entièrement gratuits destinés aussi bien aux débutants qu'aux experts les plus chevronnés. Les certifications cloud sont un gage de qualité connu et reconnu dans l'industrie IT. Elles s'adressent à une large variété de métiers comme les développeurs, les architectes ou ingénieurs en informatique, les administrateurs réseau, les experts en cybersécurité, les administrateurs de bases de données, les data analysts, les directeurs de projets, etc.
Avec la crise sanitaire mondiale qui continue de sévir, les entreprises qui se tournent massivement vers le télétravail accélèrent leur transition vers le Cloud. La demande de profils compétents va donc continuer à augmenter considérablement dans les années à venir. Les professionnels de l'informatique détenant une ou plusieurs certifications majeures vont être de plus en plus convoités. Selon le site talent.com, le salaire moyen annuel d'un expert cloud en France est de 51 500 € et peut grimper jusqu'à 125 000 € pour les experts les plus expérimentés. De quoi faire naître quelques vocations. ✖

Jérôme Cartegini

Les 5 certifications cloud les plus prisées en 2021

1 – AWS Certified Solutions Architect - Associate

Pour obtenir cette certification, les candidats doivent passer un examen à choix multiple. Celui-ci consiste à tester les capacités à déployer, gérer, et utiliser différents services de la plate-forme cloud AWS. Obtenir cette certification nécessite de solides compétences dans la gestion du Cloud. Des formations gratuites sont proposées par Amazon pour préparer l'examen. Tarif : 150 $

2 - Google Associate Cloud Engineer

La certification de Google valide les capacités d'un candidat à utiliser Google Cloud Console en ligne de commande. Il doit parvenir à déployer des applications, configurer les accès et la sécurité, planifier et configurer les ressources en réseau, gérer des machines virtuelles, etc. Des cours sur les principes fondamentaux des solutions Google Cloud sont accessibles gratuitement en ligne. Tarif : 125 $

3 - Microsoft Certified : Azure Fundamentals

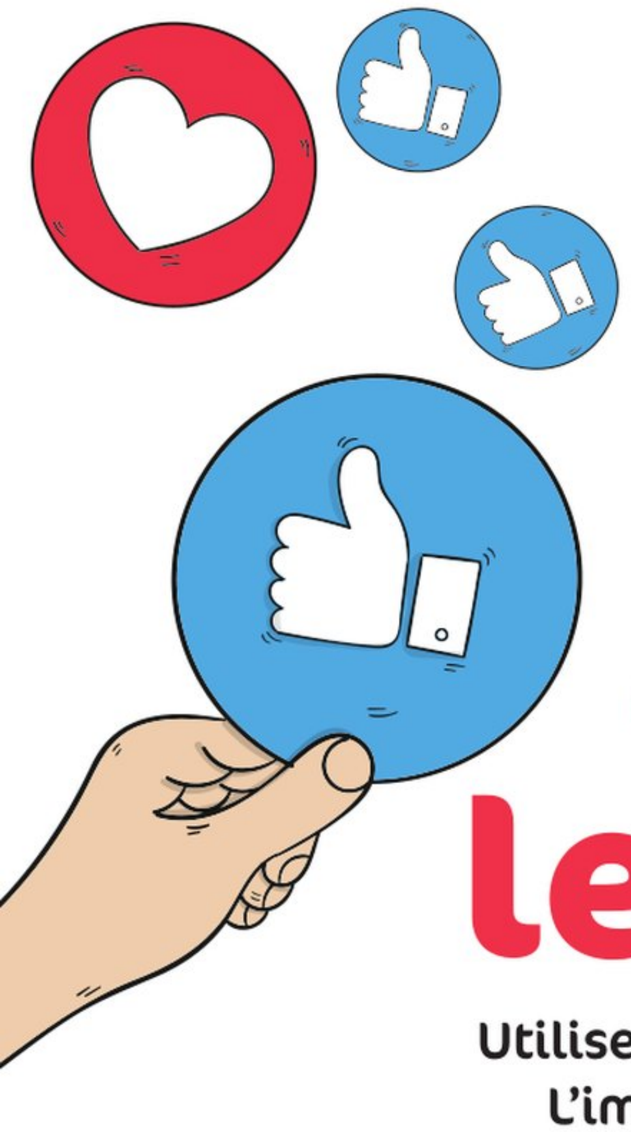
Les candidats à la certification Azure Fundamentals doivent posséder les connaissances fondamentales de base des services cloud de Microsoft ainsi que la façon dont ils sont fournis par Azure. Selon Microsoft, cette certification s'adresse à ceux qui commencent à travailler sur le Cloud et qui ont quelques connaissances du Cloud Azure. Des cours de spécialisation gratuits en ligne permettent de préparer l'examen. Les spécialistes du Cloud Azure qui est très répandu dans les entreprises en France sont très demandés. Tarif : 99 $

4 - Cloud Security Alliance : Certificate of Cloud Security Knowledge (CCSK)

La certification CCSK est délivrée par l'organisation à but non lucratif Cloud Security Alliance. L'avantage de cette dernière réside dans le fait qu'elle permet d'acquérir des compétences pouvant être appliquées sur différentes solutions cloud. Le CCSK se concentre sur les principes fondamentaux de la sécurité du Cloud. Une alternative à prendre sérieusement en compte. Tarif : 395 $

5 - IBM Certified Solution Advisor - IBM Cloud Foundations V2

Même si IBM ne possède pas autant de parts de marché dans le domaine du Cloud que AWS, Google et Microsoft, sa certification peut faire toute la différence dans certaines entreprises utilisant ses services. L'IBM Cloud Foundations V2 est la certification de base du Cloud IBM. Les candidats doivent notamment être en mesure de maîtriser l'analyse des bases de données, la sécurité, les différences entre SaaS, PaaS et IaaS, le Red Hat OpenShift ou encore le Cloud privé virtuel. Tarif : 200 $



Logitech Scribe

La caméra qui connecte le tableau blanc

Utiliser un tableau blanc en visioconférence peut être une vraie gageure. L'image est souvent déformée par la webcam, les écrits et schémas sont difficilement lisibles et l'intervenant sait rarement où se placer. Logitech entend répondre à ces problèmes avec sa caméra Scribe.

Le dispositif consiste en une caméra à fixer au mur au-dessus du tableau. Le calibrage par rapport au tableau est automatique – et il est toujours possible de le régler manuellement – de sorte à avoir une image plate de la surface, qui n'est pas distordue comme c'est souvent le cas avec une simple webcam.

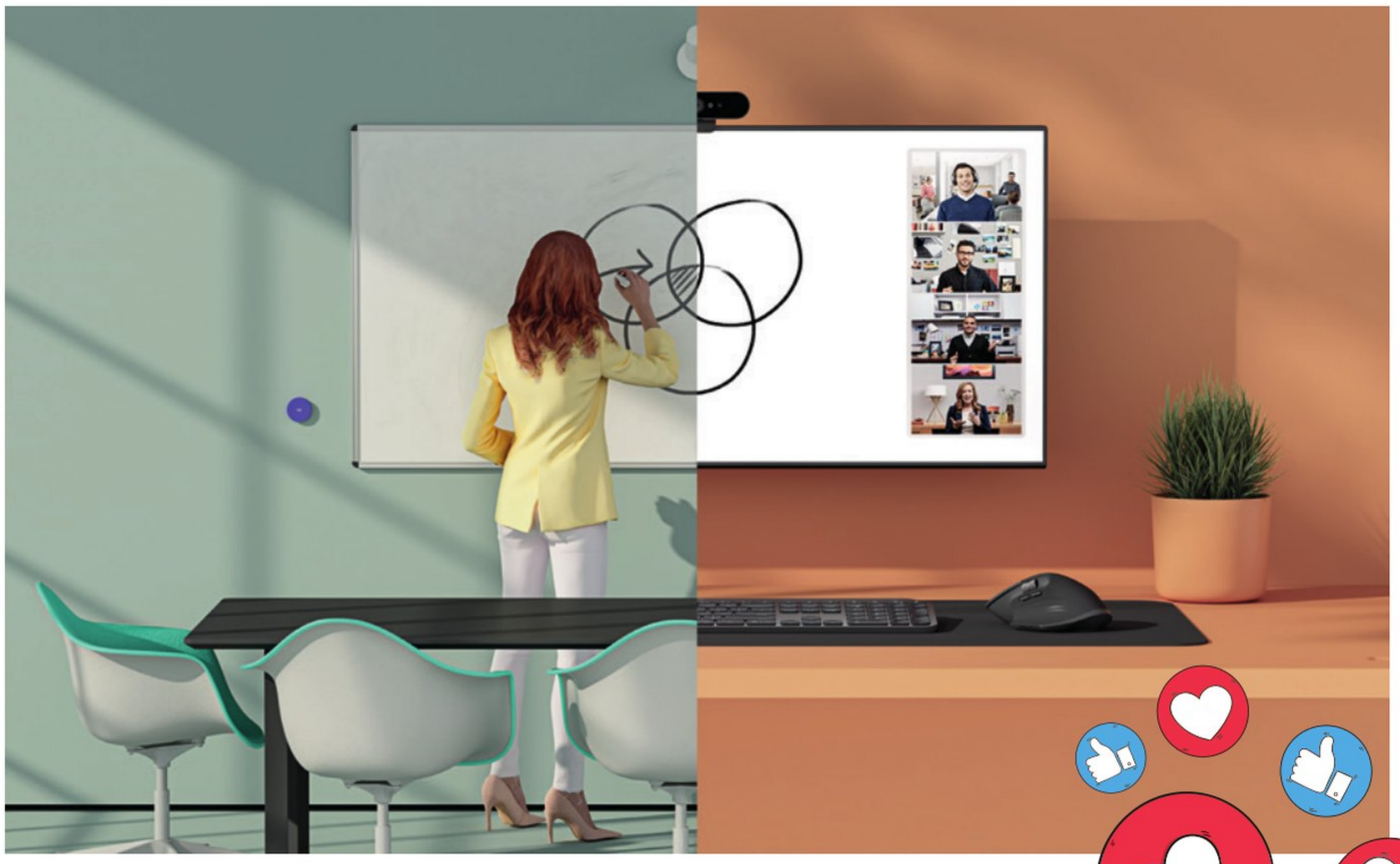
Sont supportés les tableaux blancs d'une dimension de 2 m par 1,2 m, mais pour les tableaux de plus grande taille, Logitech fournit des autocollants permettant de délimiter la zone disponible sur Scribe. Le tout se paramètre via le portail du constructeur, Sync, et le partage du tableau blanc sur Zoom ou Teams s'effectue par le biais d'un bouton Share sur l'application ou par le biais du contrôleur Logitech Tap, ou même manuellement.

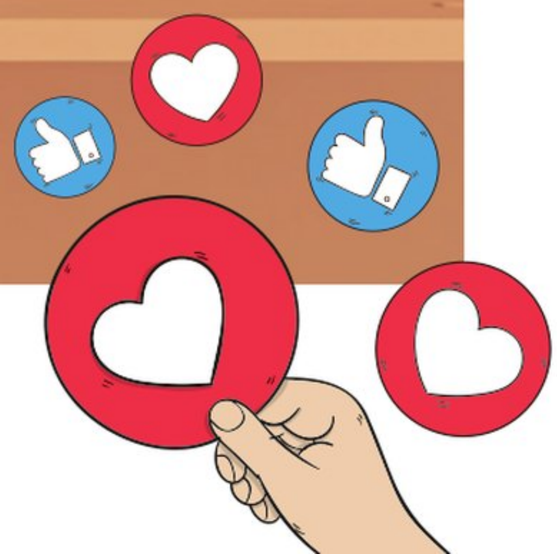
Jusque-là, nous sommes face à un produit somme toute sympathique, car il affiche un tableau aplati à 1018 p et 15 fps, mais après tout rien qui ne saurait susciter un enthousiasme débordant… du moins jusqu'à ce que l'IA mise en œuvre par Logitech entre en action. Nous avons pu voir Scribe fonctionner, et le résultat est proprement bluffant ! D'abord parce qu'il améliore automatiquement la couleur et le contraste du texte écrit sur le tableau, et fait ressortir des contenus tiers, un post-it collé au tableau par exemple. Ceci améliore substantiellement la lisibilité. Ensuite Scribe crée un effet de transparence sur le présentateur, ce qui donne une vue dégagée sur le tableau puisque les participants verront « à travers » l'intervenant.

On a noté néanmoins, lors de la démonstration à laquelle nous avons assisté, une petite latence entre le moment où le présentateur écrit au tableau et l'amélioration graphique à l'écran, mais rien qui ne soit réellement dérangeant.

Voici un produit qui est donc tout indiqué pour les salles de cours ou pour les réunions nécessitant l'usage d'un tableau blanc. Scribe est commercialisé à partir de 1 299 euros. ✖

G. P.

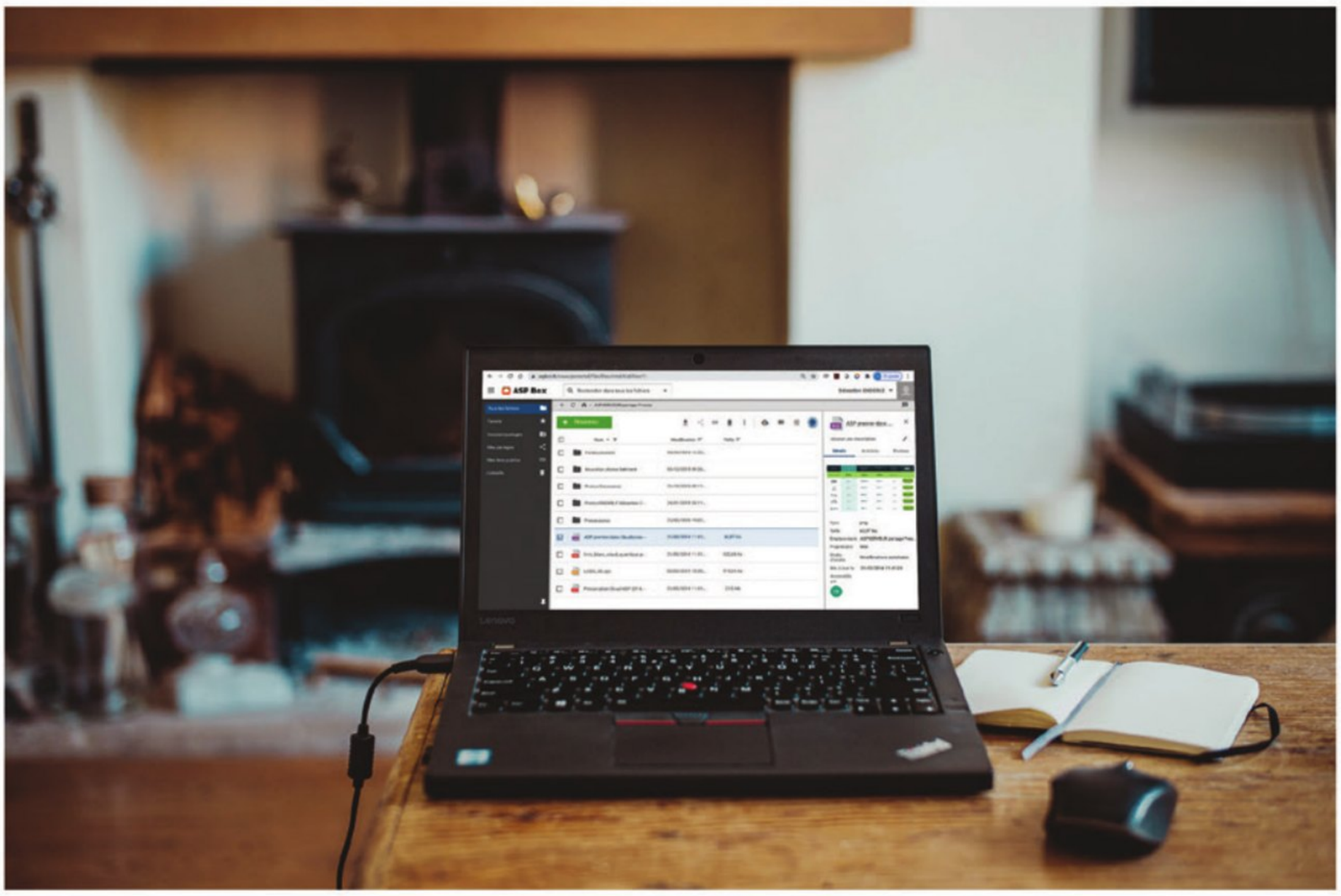




asp serveur | econocom

ATEMPO preserving data ecosystems

PASSEZ AU TELETRAVAIL EN 1 CLIC
EN AMÉLIORANT VOTRE SECURITÉ ET VOTRE CONFORMITÉ !



Solution logicielle complète + laptop LENOVO à partir de 59,90 €HT par mois
Solution logicielle seule à partir de 19,90 €HT par mois

Comprend les suites logicielles ASPBOX™ et ATEMPO LINA™

- Synchronisation de vos données avec votre poste de travail en entreprise.
- Travail collaboratif sur les fichiers, édition des documents en ligne.
- Partage sécurisé de documents en interne ou en externe.
- Versioning et historisation des fichiers.
- Sauvegarde et récupération autonome des fichiers ou de la machine complète.
- Protection continue contre les Ransomware.
- Conformité RGDP, ISO27001, HDS, PCI-DSS, Cloud souverain, société française.
- Options : VPN, Dock Station, Two-Factor authentication, Firewalls dédiés.

bsi. ISO/IEC 27001 Information Security Management

bsi. HDS Healthcare Data Storage

PCI DSS Certified

RGPD

www.aspserveur.com
Email : commercial@aspserveur.com - Tel. 0805 360 888
Siège social : 785 voie Antiope, 13600, La Ciotat
SIREN 451 777 254 RCS Marseille

Bretagne télécom

devient

BT BLUE

On a tout prévu pour la sécurité de vos données

www.bt-blue.com

sales@bt-blue.com

02 30 30 00 12

Certifications :

AYEZ **L'ESPRIT TRANQUILLE**

Nés en Bretagne dans le berceau des Télécoms, nous ne sommes jamais loin de nos clients ni de leurs données. Notre datacenter basé en France est certifié ISO 27001 et HDS. Il assure à nos clients un hébergement sécurisé de leurs données sensibles.