

SMART DSI®



DOSSIER

La gestion
de portefeuille pour
créer de la valeur

INTERVIEW

Rendre le processus
de stockage plus simple
et intuitif

L'ETUDE A RETENIR

Biométrie, Data Science
et Durabilité au cœur
de la sécurité en 2022

INTERVIEW

Tout le monde peut avoir
la chance de comprendre
l'Intelligence Artificielle

EXPERT

La confidentialité
de vos réunions !

L'ŒIL DU FUTUR

Innovation SIRH :
quels changements la crise
sanitaire a-t-elle pu faire
émerger ?

Club Abonnés sur [iTPro.fr](https://www.itpro.fr)



En route vers le DaaS augmenté avec DIB-France®

Conçues pour s'adapter aux spécificités de l'environnement de travail de chaque utilisateur et de chaque société, **les offres Cloud-In-One** de DIB France, sont déclinées en **3 niveaux packagés**. Simples à appréhender, évolutives et sécurisées, elles permettent aux directions IT et métiers de **s'affranchir totalement ou partiellement des contraintes IT** au profit de la flexibilité de service.



CLOUD IN ONE
www.cloud-in-one.fr

Simplicité de
mise en œuvre



Sécurité
renforcée



Infrastructure
Cloud



Flexibilité &
Souplesse





Les femmes au cœur de la cybersécurité!

Après de longs mois de crise sanitaire, la guerre et les horreurs qui y sont associées reviennent en force sur notre continent, accompagnées bien évidemment de nombreuses cyberattaques et d'une mise en alerte maximale des SOC (Security Operations Centers) qui constituent de véritables « war-room » à l'épreuve du temps réel et de la communication. A l'heure où la cyber se révèle encore une fois plus qu'essentielle au cœur d'événements dramatiques qu'on pensait invraisemblables il y a peu, il ne faut négliger aucune compétence.

Ainsi, en ce mois de mars, et notamment de la Journée Internationale de la Femme, jetons un œil du côté de la cybersécurité précisément.

Selon le rapport de Forrester sur les bonnes pratiques pour recruter, former et faire progresser les femmes au sein de la cybersécurité, celles-ci ne représentent que 24 % des professionnels de la sécurité dans le monde, et malgré des efforts, la culture de la sécurité demeure « hostile » aux femmes. Quelques enseignements méritent qu'on s'y attarde un instant, car les solutions existent.

Les entreprises semblent avoir besoin d'une formation sur les préjugés et elles doivent se concentrer sur la fidélisation des femmes dans les rôles de direction. Parmi les profils LinkedIn de plus de 380 entreprises du Fortune 500 et de 150 entreprises de la région EMEA, les femmes n'occupent le poste de responsable de la Sécurité de l'Information qu'à 13% et 8% respectivement. En outre, le manque de diversité est toxique et entraîne de nombreuses démissions. Enfin, les entreprises doivent s'attaquer aux préjugés sexistes. En effet, pour la majorité des RSSI hommes, il est urgent de devenir un allié des femmes dans la technologie et la cybersécurité. Les dés sont jetés, il faut agir rapidement pour faciliter les interactions, favoriser la synergie et capitaliser sur toutes les compétences et expertises.

Pour un véritable changement et une nouvelle dynamique au sein des organisations, la responsabilité personnelle, l'engagement et l'inclusion semblent être décidément de mise.

Bonne lecture !

Sabine Terrey
Directrice de la Rédaction
sterrey@itpro.fr

(1) Source Forrester - Best Practices: Recruiting, Retraining and Advancing Women in Cybersecurity

SMART DSI

SMART DSI - ABOSIRIS
Service des Abonnements
BP 53 - 91540 - Mennecy - France
Tél. +33 1 84 18 10 50
abonnement@smart-dsi.fr
1 an soit 4 n° : 120 € TTC - TVA 2,1%

« SMART DSI est la 1^{ère} revue d'informatique professionnelle trimestrielle dédiée aux décideurs informatiques, aux décideurs métiers et aux professionnels des nouvelles technologies de l'information et de la communication (NTIC). La revue SMART DSI, au travers de chroniques, dossiers, études et analyses, constitue un formidable support d'informations stratégiques, de veille et de formation technologique, à l'intention des décideurs informatiques et experts métiers d'entreprise pour leur permettre de comprendre les enjeux, évaluer les perspectives et conduire, avec leurs équipes, la transformation numérique de l'entreprise ».

SMARTDSI

N°25 | MARS 2022

SMART DSI est un revue trimestrielle éditée par IT PROCOM
Directeur de la Publication : Sabine Terrey
Strategy Center - BP 40002 - 78104 St Germain en Laye, France.
© 2002 - 2022 IT PROCOM - Tous droits réservés
N° ISSN : 2494-9701 - N° CPPAP : 0518 T 93059
www.smart-dsi.fr

6 | DOSSIER

*La gestion de portedeville pour
créer de la valeur*

12 | SPECIAL REPORT DATA3V

*MFT : Data3V propose une offre souveraine
d'échanges sécurisés de données*

14 | L'ŒIL SECURITE

*Envahissement de l'Ukraine par la Russie
La cybersécurité en deuxième ligne et les SOC
en alerte maximale*

17 | L'ETUDE A RETENIR

5 axes pour exploiter les données en 2022

18 | PERSPECTIVES

L'avenir de la fonction finance post pandémie

21 | L'ETUDE A RETENIR

*Biométrie, Data Science et Durabilité
bouleversent la sécurité en 2022*

22 | INTERVIEW

*Wasabi Technologies rend le processus
de stockage plus simple et intuitif*

25 | L'ETUDE A RETENIR

Le difficile défi de rétention des équipes IT

26 | STRATEGIE

*Réaliser une croissance à deux chiffres
grâce aux données zero party*

28 | EXPERT

Azure ARC, hybride et multi-cloud

32 | INTERVIEW

*S!MPL : l'intelligence artificielle proactive
au sein de Simple CRM*

35 | BULLETIN D'ABONNEMENT

36 | INTERVIEW

*Tout le monde peut avoir la chance de comprendre
l'Intelligence Artificielle*



P.6



P.32



P.48



P.28



P.18



P.14



P.42

38 | ANALYSE

Les utilisateurs cloud, victimes privilégiées des ransomwares

42 | EXPERT

Teams : la confidentialité de vos réunions !

48 | INTERVIEW

Aider les entreprises à anticiper et gérer les violations de données : l'objectif des lignes directrices publiées par le CEPD

50 | POINT DE VUE

Comment résister au raz-de-marée de la cybercriminalité en 2022 ?

55 | L'ETUDE A RETENIR

La culture data en 2022 au sein des organisations

56 | L'ŒIL DU FUTUR

Quels changements la crise sanitaire a-t-elle pu faire émerger ?

SMARTDSI

Rédaction

Pour joindre les membres de la rédaction
redaction@smart-dsi.fr

Comité de rédaction associé à cette édition

Thierry Bollet, Didier Danse, Pierre-Yves Popihn, Sabine Terrey, Laurent Teruin, Théodore-Michel Vrangos.

Régie Média & Publicité - Com4Médias

Christophe Rosset – Directeur Commercial
christophe.rosset@com4medias.com
Tél. 01 39 04 24 95

Abonnements

Smart DSI - Service Abonnements
BP 40002 - 78104 St Germain en laye cedex
Tél. 01 39 04 24 82 - Fax. 01 39 04 25 05
abonnement@smart-dsi.fr

Conception & Réalisation

Studio C4M – Philippe Deslandes
conseil@com4medias.com

© 2022 Copyright IT Procom
© Crédits Photos

AdobeStock - Shutterstock - Paul Beaufix - Istock

SMART DSI est édité par IT PROCOM
Directeur de la Publication : Sabine Terrey
IT PROCOM - SARL de Presse au capital de 8.000 €, siège social situé :
10-12 rue des Gaudines, 78100 St Germain en Laye, France.
Principal Actionnaire : R. Rosset Immatriculation RCS :
Versailles n°438 615 635 Code APE 221E - Siret : 438 615 635 00036
TVA intracommunautaire : FR 13 438 615 635

Toute reproduction, représentation, traduction ou adaptation, qu'elle soit intégrale ou partielle, quels qu'en soient le procédé, le support, le media, est strictement conditionnée à l'autorisation de l'Éditeur.

SMART DSI - IT PROCOM, tous droits réservés.

© 2022 IT PROCOM - Tous droits réservés
N° ISSN : 2494-9701 - N° CPPAP : 0518 T 93059

Dépôt légal : à parution - Imprimé en France par
IMPRIMATUR 87400 St Léonard de Noblat

Site officiel : www.smart-dsi.fr

La gestion de portefeuille

POUR CRÉER DE LA VALEUR

> Par Didier Danse

« Créer de la valeur » est sur toutes les lèvres depuis des décennies. Longtemps perçue comme l'affaire du département des ventes, la notion de valeur ne cesse d'évoluer dans le temps. Elle tient désormais compte de l'aspect émotionnel et est désormais l'affaire de l'ensemble des départements qui forment une chaîne de valeur. En tant que fonction support, le département informatique est, de facto, partie prenante dans cette même chaîne de valeur.



Au quotidien, les départements informatiques disposent en effet de nombreux leviers pour créer de la valeur. Certains sont très simples à mettre en œuvre et permettent de créer de la valeur immédiatement. D'autres, plus complexes au premier abord, donnent des résultats pérennes avec une vélocité accrue. La gestion du portefeuille informatique permet d'identifier au plus tôt les activités qui créent de la valeur et de les prioriser en tenant compte de nombreux facteurs pour optimiser cette valeur créée, le tout en s'intégrant avec les processus existants.

Le Larousse ne dénombre pas moins de 14 définitions pour le terme valeur, sans compter les expressions qui contiennent ce mot. Certaines de ces définitions sont purement objectives et se basent sur les coûts de production d'un bien ou d'un service ainsi que le

prix de vente de celui-ci. D'autres font référence à la perception et à l'intérêt par le potentiel acquéreur.

Cette approche conceptuelle relève alors de la combinaison de facteurs forts différents tels que la marque, la culture d'entreprise, l'approche clientèle et bien d'autres. Pour le rendre concret dans le marché financier, un prix lui est alors assigné.

Ainsi, bien que le prix de la brique ne change que très peu d'une maison à l'autre, celui de la maison est très variable, en tenant compte du quartier, de l'infrastructure aux alentours mais aussi de l'histoire de la maison. De même, en observant le prix d'un autographe d'un chanteur connu, on comprend vite que la perception apporte énormément de valeur comparée au prix du papier seul.

Différents axes de la création de valeur

La valeur créée est la différence entre le résultat obtenu et le résultat théorique ou passé si certaines opérations n'avaient pas été effectuées. La valeur créée, ou valeur ajoutée, est bien connue du grand public, notamment du fait de la taxation qui est appliquée à l'aspect financier de la chose.

Dans un précédent papier, nous avons abordé la création de valeur en partant de la proposition de valeur. La proposition de valeur permet d'exprimer ce que le bien ou le service amèneront à l'utilisateur de celui-ci, de manière similaire à ce que la vision et la mission indiquent vers quoi tend une collectivité et comment elle se positionne pour y parvenir.

La proposition de valeur répond alors à ces trois questions :

- Quel est le problème à résoudre ?
- Qu'est-ce qui rend la solution unique ?
- Comment mesurer le résultat fourni par cette solution ?

La création de valeur est un des autres pendants du sujet. Elle est le reflet de l'implémentation des méthodes pour répondre à la proposition de valeur. On entendra d'ailleurs souvent parler de la création de valeur par tel ou tel intermédiaire tel que « la création de valeur par le marketing ». Chacun joue en effet un rôle dans la création de valeur à proprement parler. Si l'un ou l'autre venait à sous-performer, il en résulterait que la valeur créée serait bien plus faible voire nulle. C'est, par exemple, le cas lorsque des entreprises font des choix hasardeux quant à leurs partenaires pour la distribution des biens ou la revente de services alors que le produit avait une valeur élevée avant la distribution. La valeur créée est donc négative dans ce cas.

La chaîne de valeur de Porter

La chaîne de valeur, outil créé par Porter il y a près de 50 ans, a pour objectif de structurer des activités afin d'obtenir un avantage concurrentiel que ce soient des coûts inférieurs aux concurrents, des caractéristiques uniques, ou un segment de marché très particulier.

Pour faire simple, les activités sont groupées en deux grandes catégories : les activités de base et les activités de soutien. Les premières sont les activités plus facilement visibles de l'extérieur de l'entreprise tandis que les secondes sont celles nécessaires pour permettre aux premières d'exister.

Bien que schématiquement, il s'agit de créer des « cases », l'ensemble de ces activités doit être vu comme un bloc, en évitant tout cloisonnement. En effet, le positionnement des uns peut avoir des impacts, positifs ou négatifs, sur les autres. On pourrait citer quelques moyens de créer de la valeur qui exercent en effet une influence sur les autres départements : payer plus tard, louer, favoriser un mode de paiement plutôt qu'un autre, utiliser le cash différemment, adapter le prix des services, proposer des offres alléchantes (freemium par exemple), et bien d'autres.

Pour optimiser la création de valeur, une analyse systématique des activités doit permettre d'identifier les opportunités d'optimisation ou même la possibilité d'externaliser un certain nombre de ces activités notamment pour faire appel à des ressources spécialisées pour une durée déterminée. Par ailleurs, comme on peut aisément le comprendre, il peut y avoir plusieurs chaînes de valeur imbriquées les unes dans les autres, notamment pour la fourniture de services à différentes étapes.

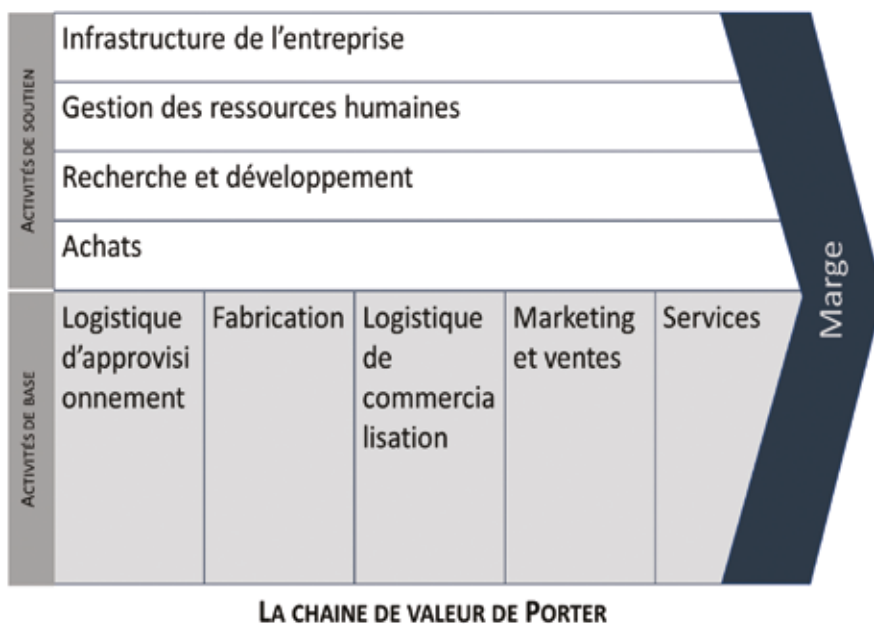
Tout cela est bien joli, mais concrètement qu'est-ce que cela veut dire en informatique ?

La création de valeur par l'informatique

Créer de la valeur de manière pérenne nécessite de prendre et d'implémenter des décisions long-terme qui doivent tenir compte de la stratégie, des priorités et des bonnes pratiques.

Pour créer de la valeur, il sera nécessaire de se poser les questions suivantes :

- Qu'est-ce qui est critique pour l'entreprise et crée un aspect concurrentiel fort au point de garder les sujets en interne ?



- Quelles stratégies doivent être appliquées aux différents sujets ? En général, 4 orientations peuvent être envisagées : investir, tolérer, arrêter ou remplacer.
- Comment l'organisation permet-elle de générer de la valeur ou à l'inverse qu'est-ce qui peut l'impacter négativement ?

La gestion de portefeuille informatique

Pour répondre à ces questions de manière systématique, la gestion de portefeuille est une approche très efficace. On parle bien ici de portefeuille et non de catalogue qu'il faut différencier. Les catalogues sont la liste des éléments actifs. Un portefeuille est en quelque sorte l'extension du catalogue puisqu'on y retrouve l'ensemble des éléments présents dans un catalogue mais aussi l'historique et les éléments candidats à être présents dans ce catalogue.

On trouve de nombreux catalogues : projets, technologies, services, licences, contrats, ou encore fournisseurs.

La gestion de portefeuille fait partie intégrante de la gouvernance informatique et se positionne entre la stratégie et l'architecture d'entreprise, le premier permettant de définir les objectifs et les priorités tandis que le second met en avant les plans de transition et les dépendances qui impactent les investissements dans l'informatique pour y parvenir. La gestion de portefeuille a ainsi pour but de définir les investissements adéquats et de s'assurer que chaque euro, chaque heure de travail génère quelque chose de positif. On retiendra bien souvent l'aspect financier de la chose puisqu'il est généralement possible de représenter un engagement, une formation et d'autres aspects par une valeur financière.

Pour parvenir à créer de la valeur de manière permanente, de nombreuses activités sont nécessaires : l'alignement stratégique des projets, la mesure de l'optimisation, la gestion des ressources optimale, l'augmentation de la capacité de livraison, la diminution des dépenses auprès de fournisseurs, l'amélioration de la qualité, et la responsabilisation des parties prenantes.

Quelques activités clés de la gestion de portefeuille

Comme nous l'avons abordé précédemment, la gestion de portefeuille fait le lien avec de nombreuses autres activités et processus tel qu'on peut le voir ci-dessous au travers de ces cinq grands groupes d'activités qui font partie de la gestion de portefeuille :

- *Gestion des demandes* : choisir les sujets en lien avec les initiatives stratégiques.

- *Planification de portefeuille* : analyser et définir des plans multiples pour maximiser les bénéfices, en tenant compte des contraintes, des dépendances et des ressources disponibles.
- *Optimisation du portefeuille* : choisir le plan le plus efficace et revoir régulièrement le plan pour tenir compte des nouveaux éléments.
- *Gestion des programmes et des projets* : fournir le support nécessaire aux équipes d'implémentation en monitorant les performances classiques des projets et des liens divers.
- *Gestion des déploiements* : gérer les livraisons mais aussi les fournisseurs.

Afin d'être concret, on peut présenter une série de livrables issus de la gestion de portefeuille et leurs objectifs :

- *Proposition de changement* : communiquer un changement et évaluer les risques, les impacts et la faisabilité.
- *Charte de projet* : description de haut-niveau tels que les livrables, les ressources nécessaires et une estimation du plan projet. C'est sur cette base que se fait le design de la solution et du projet.
- *Modèle de service* : description de la structure de service, les composants et les interactions entre ceux-ci.
- *Portefeuille de services* : le service identifié à l'étape précédente doit explicitement être ajouté au portefeuille en même temps que l'ensemble des requêtes de service, c'est à dire tout ce qui peut être demandé par rapport à ce service.
- *Rapport de revue du portefeuille* : analyse régulière de l'ensemble des éléments du portefeuille afin d'identifier les besoins en termes de changements et les opportunités offertes par la rationalisation.

La gestion de portefeuille fait partie intégrante de la gouvernance informatique.

Structurer la démarche

Pour parvenir à fournir les différents rapports et autres documents, la gestion de portefeuille doit être structurée en une série d'activités que l'on peut rassembler en flux de travail et qui sont reliés entre eux, formant un cycle :

La collecte d'informations et l'étalonnage

- *Lister l'ensemble des projets et des idées* : obtenir l'information sur les projets, leurs fondements, la charge de travail potentielle mais aussi les coûts, les risques et les bénéfices.

- *S'assurer que le besoin est aligné (business case) :* en tenant compte des besoins métiers et de leur alignement avec la stratégie, il s'agit de s'assurer que l'initiative crée de la valeur.
- *Valider les informations :* recevoir des informations est assez simple, encore faut-il qu'elles soient justes. Il faut donc vérifier les différentes informations et les différents scénarios.

L'analyse stratégique

- *Maximiser la valeur du portefeuille :* le sujet est large. Il s'agit en effet d'optimiser et de revoir les différents portefeuilles en cherchant à exploiter les différents contrats, en se focalisant sur les plus importants mais aussi en évitant les doublons. Puisque le passé ne peut pas être changé, on veillera à se focaliser sur le futur et le consommable. De nouveaux projets support aux autres pourraient également apparaître à cette étape.
- *Aligner et prioriser :* en identifiant les points d'améliorations et les opportunités, il est ainsi possible de prioriser les investissements en fonction du retour attendu.
- *Balancer l'offre et la demande :* à tout moment, il est nécessaire d'identifier comment aligner au mieux l'offre et la demande de services.

La prise de décision

- *Finaliser la proposition de portefeuille :* il existe de nombreux portefeuilles et sous-portefeuilles. Les projets d'un portefeuille partagent des objectifs et des paramètres. Pour chacun des sous-portefeuilles tel que la création d'un nouveau département, d'une usine ou simplement l'amélioration du niveau de cyber sécurité, une proposition doit permettre de maximiser les résultats, en tenant compte des facteurs coûts et temps.
- *Autoriser des projets :* les projets ne font sens que s'ils créent de la valeur. Dans ce contexte, il est nécessaire de s'assurer que les projets mais aussi les attentes qui y sont liées soient en phase avec les objectifs et les critères du portefeuille tout en étant initiés au moment opportun.
- *Autoriser des ressources :* cette activité requiert de définir les plans et les besoins en termes de ressources en tenant compte de l'organisation des projets.

Pour parvenir à fournir les différents rapports et autres documents, la gestion de portefeuille doit être structurée en une série d'activités.



AXEL
définit autrement la technologie
du Client Léger

Prêt gratuit
pour évaluation

www.axel.fr

The advertisement features a dark background with a glowing green and yellow light effect. In the foreground, there is a small, dark grey rectangular device with a USB port and a green indicator light. In the background, a larger server rack unit is visible, also with a glowing light effect. The text is overlaid on this background.

L'élaboration de chartes

- **Communiquer les décisions** : cette activité s'avère critique afin de s'assurer que l'ensemble des intervenants, notamment les membres des équipes projets, puisse prendre connaissance des dernières informations et décisions. La formalisation de la communication facilitera l'adoption de celles-ci.
- **Réallouer les ressources** : les ressources principales, c'est-à-dire celles critiques pour l'exécution des différents projets, doivent être gérées au niveau

du portefeuille. L'équipe en charge du portefeuille étant responsable de créer de la valeur s'assure ainsi que les ressources sont allouées aux projets créant le plus de valeur à un moment précis.

- **Créer ou modifier la charte des projets** : le contexte dans lequel s'exécutent les projets varie au quotidien et de nombreuses nouvelles informations sont identifiées durant la vie du projet. Il s'avère alors nécessaire de revoir, après chaque phase de projet, la charte du projet et d'ajuster ce qui s'avère nécessaire pour tenir compte des nouveautés.

Par où démarrer ?

Au travers de ce papier nous avons pu voir qu'il existe de nombreux éléments à tenir compte pour créer de la valeur de manière efficace et que de nombreuses actions requièrent de la gouvernance au quotidien.

Ainsi, le plus simple sera de revenir aux fondamentaux et de connaître votre propre activité. Cela semble évident pour beaucoup mais quelques questions simples permettront d'identifier des axes d'amélioration rapides à mettre en place :

- **Ai-je une liste exhaustive des licences ? Quels sont les services Cloud qui coûtent le plus chaque mois ? Une liste exhaustive sera très utile mais on veillera à se concentrer sur les plus coûteux.**
- **Ai-je connaissance du catalogue de service et quelles sont les capacités de chacun de ces services ?**
- **De même, quelles sont les applications dans le giron ? Certains sont-ils en doublon ?**
- **Enfin, à quel point chacun des éléments ci-dessus sont-ils utilisés ?**

Avec les réponses à ces questions, il est alors possible de rationaliser les différents catalogues en s'assurant que les composants clés sont effectivement utilisés. Lors de l'optimisation, il convient de commencer avec ce qui n'est pas encore payé.

Si le contrat est d'ores et déjà payé, il n'est pas possible de le changer et l'effort fourni sera alors nul ou presque. Dans certains cas, il suffit de réduire le nombre de

composants pour réduire immédiatement les coûts. Parfois il sera possible de réduire les redondances en se posant quelques questions :

- **Deux entreprises fournissent les mêmes services. Est-ce nécessaire ?**
- **Migrer une solution vers une autre permet-elle de réduire le besoin en support (par exemple avoir 1 expert au lieu de 2) ?**
- **Et si un service venait à être indisponible, quel en serait l'impact pour les utilisateurs ? Est-ce que je peux envisager de le supprimer ?**

Une fois ce premier nettoyage effectué, assurez-vous de mettre en place une gouvernance, somme toute basique mais suffisante, pour garder le contrôle sur les services, les applications et les projets.

De manière régulière, interrogez-vous sur la pertinence des services et l'efficacité des fournisseurs. Cela permettra de connaître la stratégie à adopter lorsque le contrat arrivera à échéance. En fonction de cette stratégie, il faudra alors se donner du temps pour effectuer les démarches adéquates.

Ne sous-estimez pas le temps nécessaire pour y parvenir, l'effort est considérable mais le résultat en sera d'autant plus grand.

Et si vous souhaitez en savoir plus sur la gestion de portefeuille, il peut être utile de parcourir la littérature dans plusieurs ouvrages de référence tels qu'ITIL et COBIT ou encore PMI.

> Par Didier Danse
IT Manager - Collaborative Platforms and IT Tools



CLOUD PRIVÉ HÉBERGÉ DE LA CPEM

Souveraineté, transparence et sécurité
au service des PME et TPE



**UNE ÉQUIPE À
TAILLE HUMAINE**



**UN CLOUD
SUR MESURE**



**UNE OFFRE
SOUVERAINE**

Découvrez toutes nos solutions cloud de confiance

www.cpem.com - contact@cpem.fr

MFT :

DATA3V PROPOSE UNE OFFRE SOUVERAINE D'ÉCHANGES SÉCURISÉS DE DONNÉES

Intégrateur de solutions MFT, Data3V a fait le choix d'ajouter à son catalogue Primeur, un éditeur européen, proposant la plateforme Data One® répondant aux standards du marché. Découvrez la valeur ajoutée de l'offre de Data3V.



Engagées dans leur transformation numérique, les entreprises sont conduites à partager un nombre croissant de fichiers avec leurs clients, partenaires et fournisseurs. Ces fichiers contenant des informations sensibles, elles doivent prendre toutes les mesures de protection pour prévenir une fuite de données et répondre aux exigences de conformité du RGPD.

Dans ce contexte, les méthodes classiques de transfert de fichiers reposant sur les protocoles FTP ou HTTP montrent rapidement leurs limites. Seule une solution de MFT (Managed File Transfer) permet de sécuriser les fichiers en transit ou au repos en faisant appel à des algorithmes de chiffrement. Elle comprend aussi différents modules pour transformer les fichiers, automatiser leurs transferts en nombre ou générer un reporting.

"Les établissements bancaires ou les industries doivent échanger avec une multitude de partenaires évoluant dans des environnements informatiques très différents » observe **Ashok Sundaram** fondateur et directeur général de Data3V, société de services experte en solutions MFT. Il faut assurer les échanges sécurisés des données, appliquer des modifications aux fichiers en maîtrisant leur compatibilité, les crypter en entrée et les décrypter en sortie."

Créée il y a six ans par des professionnels bénéficiant chacun de plus vingt ans d'expérience, Data3V, s'adresse aux PME et grands comptes de l'industrie, de l'automobile, du secteur bancaire, de la logistique, du transport et de la grande distribution. Parmi ses références, on peut citer ArcelorMittal, le cimentier Vicat ou encore le réseau des caisses Congés Intempéries BTP (CIBTP) et plusieurs établissements publics.

Exposition au Cloud Act

Les entreprises utilisatrices sont toutefois exposées à la réduction du nombre de spécialistes du MFT. Des éditeurs historiques comme File Catalyst, GoAnywhere ou Globalscape sont à présent dans le giron d'un même groupe. "Ce quasi-monopole fait peser un risque de dépendance technologique et d'enfermement propriétaire, estime **Ashok Sundaram**. Sur le plan tarifaire, une entreprise captive peut aussi se voir imposer une hausse subite des coûts de maintenance."

Le mouvement de bascule du mode on-premise vers le Cloud pose, par ailleurs, un enjeu de souveraineté. Selon le principe d'extraterritorialité propre au droit états-unien, un acteur américain est, en effet, soumis au Cloud Act même s'il héberge sa solution sur le sol européen.

Le mouvement de bascule du mode on-premise vers le Cloud pose, par ailleurs, un enjeu de souveraineté.

Pour toutes ces raisons, Data3V complète à présent son offre en solutions MFT avec l'éditeur indépendant italien Primeur, dont il assure le support et l'intégration pour la France.

Primeur est le seul éditeur européen à proposer une solution complète intégrant nativement les protocoles spécifiques PeSIT, EBICS, AS2, employés pour des échanges de fichiers entre des systèmes informatiques bancaires.

Un module RGPD natif

Baptisée Data One, la plateforme de Primeur comprend quatre modules.

Data Mover, est le module qui gère les protocoles sécurisés pour les transferts de fichiers. Il planifie, gère et contrôle l'intégration des flux de données de bout en bout. "Une entreprise peut échanger des centaines de milliers de fichiers par jour, entre utilisateurs ou partenaires, mais aussi d'application à application sans intervention humaine", illustre **Ashok Sundaram**.

Data Shaper, va, lui, transformer les fichiers afin de les rendre compatibles parmi différents types de plateformes, "Un serveur sous Windows ou une machine Linux, un AS/400 hébergent des fichiers à des formats totalement différents", poursuit-il.

Baptisée Data One, la plateforme de Primeur comprend quatre modules.

Autre module, *Data Watcher* permet de constituer des tableaux de bord pour l'analyse et le reporting afin de signaler des fichiers bloqués ou un serveur hors service.

Enfin, *Data Privacy* garantit la qualité des données et leur conformité au RGPD. "Peu d'éditeurs ont intégré nativement un module RGPD aussi performant, remarque **Ashok Sundaram**. Il permet de s'assurer du bon respect du traitement des données personnelles, principes du RGPD, comme le recueil de consentements, les notions de finalité d'utilisation, de l'anonymisation des données ou les délais de conservation. Ce module peut fonctionner indépendamment de la solution MFT."

Data One de Primeur est également la première plateforme basée sur un modèle dit COA (Contract-Oriented Architecture). Cette architecture orientée contrats permet d'organiser les flux de données selon des règles et des contraintes prédéfinies, contrats de service. "Il est ainsi possible de programmer l'envoi à 8h d'un flux de X fichiers à destination de tel serveur à tel format selon tel protocole d'échange et faisant appel à tel algorithme de chiffrement", conclut **Ashok Sundaram**.

Pour aller plus loin :

<https://data3v.com/> - contact@data3v.com

Envahissement de l'Ukraine par la Russie

LA CYBERSÉCURITÉ EN DEUXIÈME LIGNE ET LES SOC EN ALERTE MAXIMALE

Alors que la guerre, avec ses drames et ses injustices, est malheureusement revenue sur notre continent, la cybersécurité et les SOC (Security Operations Centers) Français sont en état d'alerte maximale.



Dès le début des attaques militaires et de l'envahissement de l'Ukraine par la Russie, précédant les opérations militaires russes, des sites de banques et de ministères ukrainiens ont été visés par des cyberattaques. Les Etats-Unis et l'Union Européenne, alliés de l'Ukraine, s'attendent à de nouvelles attaques informatiques du fait des sanctions prononcées contre la Russie. Et les alliés s'attendent à des attaques au-delà de l'Ukraine, mais sur nos propres infrastructures, nos propres hôpitaux, agences gouvernementales, entreprises prestigieuses, etc, en représailles aux soutiens au peuple Ukrainien.

Différents types de cyberattaques

Attaques sur les Active Directory, nouveau malware HermeticWiper, à code quasi nouveau, attaques en déni de service distribué (DDoS), faux sites officiels rendus injoignables ou abritant des mécanismes de distribution de maliciel, les attaques d'origine russe, centrées pour l'instant sur l'Ukraine, sont surveillées de très près dans la crainte de cyber-représailles sur les entreprises et administrations françaises et européennes.



STORMSHIELD

Le choix européen de la cybersécurité

Partenaire de confiance
pour

sécuriser vos infrastructures opérationnelles



www.stormshield.com

Deux types de cyberattaques ont touché l'Ukraine : d'une part, des attaques par déni de service distribué (DDoS) d'intensité moyenne, d'autre part, des offensives destructives (wipers) qui exploitent une faille et suppriment le contenu des ordinateurs ciblés avant de les bloquer.

Avant l'entrée des troupes russes en Ukraine, banques et administrations locales ont été confrontées à la distribution d'un maliciel, en amenant les internautes à se tourner vers un potentiel cheval de Troie.

Les groupes de hackers s'expriment

Cela dit pour le moment la situation sur le terrain de la cyber-guerre est un peu chaotique : d'une part chaque pays et chaque grande entreprise ont placé en alerte leurs unités de cyberdéfense et leurs SOC, d'autre part partout dans le monde, les groupes de hackers et gangs de ransomwares s'expriment parfois très ouvertement sur les réseaux sociaux pour annoncer leur allégeance à tel ou tel camp.

Les "Anonymous" sont officiellement en « cyber guerre » contre le gouvernement russe. Ghostsec s'est également prononcé en support du peuple ukrainien et bien évidemment UNC1151 (basé à Minsk, cela veut tout dire...), the Red Bandits et SandWorm ont pris position en faveur de la Russie et ouvertement menacé tous ceux qui tenteraient des cyberattaques contre les instances et les entreprises russes.

Les war-room des SOC

Depuis plusieurs années les grandes entreprises françaises et européennes, à l'instar de leurs confrères américains ou canadiens, se sont dotées des services permanents, souvent externalisés de SOC (Security Operations Center) et CERT 5 (Computer Emergency Response Team). Aujourd'hui, ce sont les ETI qui constituent la vague des demandeurs de services de SOC et CERT sans oublier les grandes entreprises et administrations qui, dans le sillage de leurs expériences d'utilisateurs de SOC depuis plusieurs années, augmentent, améliorent, redéfinissent les services attendus de leurs opérations de 2^{ème} voire 3^{ème} génération.

Au début les SOC, composés d'analystes et ingénieurs, d'outils et des processus d'analyse, d'actions d'ingénierie et remédiation, de reporting, étaient centrés sur l'exploitation des logs des nœuds IP (infrastructures, réseaux, serveurs, puis applicatifs, apps mobiles, etc...).

Les "Anonymous" sont officiellement en « cyber guerre » contre le gouvernement russe.

Ces SIEM ont été complétés par les outils EDR (Endpoint Detection Response), anti-virus de nouvelle génération, enrichis par des résultats des scans de vulnérabilités autant infra qu'applicatifs, des input des threat intelligence en provenance des éditeurs spécialisés, qui approfondissent les alertes en fonction des métiers et business, des zones géographiques, des usages, etc.

Ce sont donc des véritables war-room chapeautés par des outils SOAR d'orchestration, d'automatisation et de réponse aux incidents de sécurité qui apportent aux responsables de la sécurité des capacités temps réel tournant en permanence, 24/7 pour les périmètres IT sans cesse en développement, que les SOC gèrent. Ce sont des véritables big Data Cyber avec en plus une capacité d'actions et de réponses. Car ce que caractérise un Big Data ou Mégadonnées sont les trois axes fondamentaux, les « EV » : volume, variété et vélocité.

Ce sont des véritables big Data Cyber avec en plus une capacité d'actions et de réponses.

Par temps de guerre ...

C'est exactement ce dont le SOC, en plus par temps de guerre, doit apporter à ces utilisateurs et clients. Ce sont eux qui sont en première ligne dans ces moments troubles de tensions géopolitique et de guerre.

Détection préventive des signaux faibles d'attaques, corrélation avancée des logs et des flux de Cyber Threat Intelligence en provenance de nos partenaires éditeurs, liens actifs avec ANSSI et le CERT-FR, la mobilisation 24/7 des cyber-analystes doit être forte et la vigilance accrue.

La cyber est importante, mais il faut aussi, malheureusement relativiser, car le drame qui se joue avec les tirs de missiles qui frappent la population civile ukrainienne est une horrible réalité. Le Monde rapporte que, sollicité par Associated Press pour savoir si les attaques par DDoS se poursuivaient sur les sites officiels, un responsable de la cyberdéfense ukrainienne a répondu par SMS : « Vous êtes sérieux ? Il y a des missiles balistiques qui tombent, ici. »

> Propos de Théodore-Michel Vrangos, cofondateur et CEO de I-TRACING Group, recueillis en exclusivité pour Smart DSI



5 axes pour exploiter les données en 2022

Les organisations doivent être prudentes quant à la manière d'intégrer et gérer les données qui sont distribuées, accessibles, fiables et gouvernées.

Comment exploiter efficacement les données ? Voici 5 pistes dévoilées par Denodo.

La data fabric = fondement de l'entreprise distribuée

Activités numériques, canaux de vente en ligne, travail à distance offrent un écosystème diversifié de dispositifs, d'applications et d'infrastructures de données.

En 2022, les entreprises créeront une data fabric pour piloter les données et l'analytique à l'échelle de l'entreprise et automatiser des tâches d'exploration, d'ingestion, d'intégration et de préparation des données. Ces data fabrics réduiront les délais de livraison et deviendront une approche de gestion des données privilégiée.

Selon Forrester, « la technologie Data Fabric fait franchir une étape supplémentaire à la virtualisation des données en automatisant les fonctions de gestion des données à l'aide de l'intelligence artificielle/machine learning et en fournissant des capacités sémantiques supplémentaires grâce au catalogue de données, à la préparation des données et à la modélisation des données. »

L'intelligence décisionnelle = aide à la décision d'entreprise

Les tableaux de bord habituels et les plateformes de BI sont complétés par des systèmes d'aide à la décision basés sur l'IA et le machine learning.

L'intelligence décisionnelle accélère les évaluations en 2022. Mais les machines n'ont toujours pas de conscience et ne comprennent pas les implications du résultat de la décision : les entreprises vont intégrer l'intelligence décisionnelle dans leur stack BI pour mesurer le résultat et éviter les conséquences involontaires en ajustant les paramètres de décision en fonction.

L'attraction des architectures de data mesh

Les équipes traitent avec des unités fonctionnelles et consommateurs de données associés. Comment comprendre les besoins en données des équipes inter-fonctionnelles ? Le data mesh, nouvelle approche d'architecture de données décentralisée pour l'analyse de données, supprime les goulets d'étranglement et rapproche les décisions relatives aux données de ceux qui les comprennent.

Le data mesh créera une infrastructure unifiée permettant aux domaines de créer et de partager des produits de données tout en appliquant des normes d'interopérabilité, de qualité, de gouvernance et de sécurité.

Les données et l'analytique = augmenter les capacités des consommateurs de données

Les entreprises internationales gèrent des données distribuées à travers des clouds et data centers dans le monde entier. L'architecture de données composable apporte l'agilité à l'infrastructure de données. L'infrastructure de gestion des données est diversifiée et, chaque entreprise utilise des systèmes ou modules qui constituent son environnement de gestion des données.

En 2022, les entreprises accéléreront la mise en place d'environnements composables pour les données et l'analytique, pour bénéficier d'une grande souplesse pour composer le stack d'infrastructure de données qui répond à leurs besoins.

L'analyse des données à petite et grande échelle

L'IA et le machine learning transforment le mode de fonctionnement des organisations, mais leur réussite repose sur le Big Data.

En 2022, les entreprises tireront parti de l'analyse des petites données pour créer des expériences client hyper-personnalisées et comprendre les préférences des clients à l'instant T. Si l'analyse des données étendues (données structurées, non structurées et semi-structurées) est un concept nouveau non adopté à grande échelle, on peut s'attendre à ce que l'analyse des données à petite et à grande échelle gagne du terrain dans les entreprises en 2022.

Source Denodo

L'avenir de la fonction finance

POST PANDÉMIE

Dans un contexte de pandémie jusqu'à la relance post-récession, comment va se façonner le futur pour les entreprises et pour tous ? Comment va évoluer la fonction finance ?



Un nouveau rôle se dessine, c'est certain. Loin des activités pures « finance » et des savoir-faire traditionnels et transactionnels, le conseil, l'analyse, la planification prennent le pas, les compétences se modifient, le recrutement et la rétention des talents aussi !

En ce sens, BlackLine a voulu examiner les savoir-faire technologiques et les expertises clés pour assurer la croissance de demain, dans son baromètre, et a souhaité poursuivre la réflexion avec **Emmanuel Millard**, Directeur de la DFCG, Association Nationale des Directeurs Financiers et de Contrôle de Gestion, **Éric Lamarque**, Directeur de l'IAE Paris Sorbonne Business School et de son Master Finance, expert en stratégie, gouvernance, organisation et performance des institutions financières et formateur pour First Finance, **Anne-Claude Tessier**, Associée KPMG, spécialisée dans les projets de transformation de la fonction finance.

La défiance envers les données financières

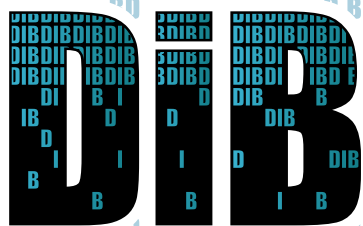
On relève une « confiance érodée » des professionnels de la finance et des cadres dirigeants envers l'exactitude des données financières. En 2018,

75% avaient totalement confiance envers les chiffres de leur entreprise (21% relativement confiance). Si en septembre 2020, on tombe à 47%, en septembre 2021, 11% seulement ont totalement confiance envers l'exactitude de leurs données financières, et 41% relativement confiance. A noter ! 19% ne leur font pas confiance du tout !

Pourquoi ? La non-reconnaissance des compétences des personnes ayant manipulé les données, le manque de contrôles et de vérifications automatisés par rapport à la quantité de données, la dépendance du service aux tableurs et procédés dépassés, le trop grand nombre de sources de données... « On constate que la confiance intégrale envers les données financières diminue au profit de la généralisation d'une confiance plus mitigée » décrypte **Lucie Bordelais**, Directrice développement EMEA de BlackLine.

Toutefois, face à cette défiance et cette complexité de prédiction, **Anne-Claude Tessier**, Associée KPMG, souligne « pour ces enjeux de transformation finance, nous allons désormais plus vers la mise en place de solutions digitales d'automatisation des contrôles des chiffres, de sécurisation des contrôles, nous adaptons nos méthodologies ».

DIDDIBDIBDIBDIBDIBDIBDIB
D DDIBDIBDIBDI DIBD BDIBDIB
DIDDIBDIB IBDIBDI DIBDIBDIB
DI DIB IBDIBD BDIBDIB IB IB
DIBDIBDIBDIBDIB IBD BDIBDIB
D BDIBDIB IBDIBDI DIBDIBDIB
DIBD BDI DIBDI DIBDIB IBDIB



DID IBDIBDIBD BDIBDI DIBD B
D DDIBDIB IBDIBDI DIBDI DIB
DID IBD BDIB IB IBD BDIBD B
IDDIB IB IBDIBDI DIBD BDIB
DID IBD BD BDI DIBDI DIB IB
D DDIB IB IB IBDI DIBD BDIB
DIBD DIBD BDIB IBD B DB
IBDIB I DIB IBDI DIBDI DIB
D BD BD B IBDIB IBD BD BDI
DIB I DIBD B IBDIB IBDI DIB
DIBD B BDIBDI DIBDI BDIB
I DIBDIB DIB I IBDIB IB
DIB DIBDIB DI DIBDIB B
D BD DIBD DIB DI DIB
DIB D I I B



1992



1

équipe d'experts
à votre écoute



+20%
de croissance
en 2019



31 millions
d'euros de chiffre d'affaires
réalisé en 2019

DIB France vous facilite l'IT



SOLUTIONS WORKPLACE
INFRASTRUCTURES & SECURITE
SERVICES & INTEGRATION

Depuis plus de 30 ans DIB France s'est développée sur des valeurs fortes autour de l'écoute, la proximité et la satisfaction client, ces valeurs guident notre stratégie au quotidien et accompagnent vos projets de transformation numérique.



www.dib-france.fr
DIBD BDI DIBDI DIBDIB IBDIB
D BDIBDIB IBDIBDI DIBDIBDIB
DIBDIBDIBDIBDIB IBD BDIBDIB
DI DIB IBDIBD BDIBDIB IB IB
DIDDIBDIB IBDIBDI DIBDIBDIB
D DDIBDIBDIBDI DIBD BDIBDIB
Tél : 01 34 57 90 00
DIDDIBDIBDIBDIBDIBDIBDIBDIB

En complément, on peut relever d'autres points importants, en effet « *la RSE irrigue complètement les métiers du dirigeant financier, tout comme la transformation digitale et celle de l'entreprise. En 2 ans, de pandémie il s'est déjà passé beaucoup de choses. Enfin, les talents et les compétences sont un vrai sujet qui nous préoccupe et qui nous tient à cœur* » alerte **Emmanuel Millard**, Directeur de la DFCG, Association Nationale des Directeurs Financiers et de Contrôle de Gestion.

Dynamiser la fonction comptable : un souffle de modernité

La crise sanitaire a créé une nouvelle normalité. Il faut s'adapter rapidement car ne pas proposer de travail hybride peut décourager les candidats selon 33%, tout comme utiliser des technologies et processus dépassés et le manque d'attractivité des conditions de travail. Le « nouveau » financier est multi compétent et devient un conseiller multi facettes. Ainsi, **Éric Lamarque**, Directeur de l'IAE Paris Sorbonne Business School et de son Master Finance, expert en stratégie, gouvernance, organisation et performance des institutions financières et formateur pour First Finance, souligne « *aujourd'hui, le métier tend à se scinder en deux, avec ceux en charge de la constitution et de la qualité des datas et ceux en charge du pan analyse et connexion avec le reste de l'entreprise* ».

Côté rétention des talents, il faut agir vite et prendre en compte l'apprentissage de nouvelles compétences, l'évolutivité des carrières, le manque de collaboration avec d'autres domaines de l'entreprise, les options de travail flexible, la nature répétitive des tâches, la sous-estimation du département financier, le stress du contrôle accru et des réglementations strictes.

En outre, **Eric Lamarque** complète « *il y a un attrait aujourd'hui pour les questions et formations Finance. Toutefois, côté diplômes académiques, on note parfois un décalage. Les étudiants en alternance par exemple montrent une très bonne adaptation. Enfin, face aux étudiants en quête de sens et d'implication, il faut que l'entreprise soit vigilante et laisse place à leur esprit critique et leurs besoins de débat* ». Sans oublier les soft skills !

Data – Automatisation – Intelligence Artificielle

Si les diplômés académiques actuels ne préparent pas convenablement au travail quotidien effectif de la fonction financière, les candidats s'attendent à ce que le département comptable et finance soit plus compétent dans le numérique, et que les cours se concentrent plus sur les compétences technologiques.

Métier stratégique avec une grande capacité d'agilité, ce qui augure des changements positifs

La transformation de la fonction doit se baser sur la data, en effet, en plus des qualifications traditionnellement requises, il faut des connaissances technologiques en intégration des systèmes financiers, en automatisation robotisée des processus, en solutions d'automatisation des finances et d'Intelligence Artificielle. Selon **Lucie Bordelais**, « *la donnée est existentielle pour l'avenir du métier : il faut la ressembler et l'identifier, apprendre à l'utiliser, et lui donner du sens.* »

Collaborer avec les autres fonctions

Si la fonction comptable et financière permet d'évoluer vers des fonctions plus stratégiques, quelles sont les compétences des futurs chefs financiers ?

- une grande compréhension de la gestion des risques - 39%
- des bonnes pratiques financières
- des bonnes pratiques des données
- l'analyse des données
- la collaboration
- une capacité à penser de façon stratégique

Le métier du financier bouge et va encore bouger très vite. Un futur passionnant donc. « *Métier stratégique avec une grande capacité d'agilité, ce qui augure des changements positifs* » ajoute **Emmanuel Millard**.

Enfin, « *la fonction comptable et financière peut servir de tremplin vers des fonctions plus stratégiques de l'entreprise. Encore faut-il que les dirigeants placent la collaboration inter-départements au cœur de leurs priorités, notamment sur les sujets sociétales de RSE (Responsabilité Sociétale des Entreprises). Actuellement, cela ne semble pas être le cas — mais demain ?* » conclut **Lucie Bordelais**.

Source BlackLine & Censurwide - 1150 cadres dirigeants et professionnels de la finance - Monde - 150 en France

> Par Sabine Terrey



Biométrie, Data Science et Durabilité bouleversent la sécurité en 2022

Pénuries de la chaîne d'approvisionnement, durabilité, travail hybride, biométrie sans contact, et bien d'autres. Autant d'axes qui remodelent la sécurité en 2022 selon HID Global. Retour sur les innovations, développements et accélérations au sein des entreprises.

Découvrons les 7 tendances qui vont secouer la sécurité en 2022.

• Problèmes de chaîne d'approvisionnement

La sécurité devra faire preuve de créativité car les pénuries de semi-conducteurs, les goulots d'étranglement logistiques mondiaux et les augmentations de coûts impacteront les lecteurs et panneaux de contrôle jusqu'aux capteurs et détecteurs.

• Durabilité

La durabilité augmentera, les fournisseurs devront se concentrer sur les solutions numériques, jusqu'aux technologies mobiles et multi-applications de bout en bout réduisant l'empreinte de l'industrie.

• Identités fournies par SaaS

Au-delà des déploiements et modèles de service dans le cloud gérant le contrôle d'accès pour les applications, actifs physiques et données, de l'authentification fiable, les identités fournies par SaaS deviendront la norme et la perspective.

• Identifiants numériques

Face aux nouvelles fonctionnalités d'identification dans les applications, nouvelles infrastructures pour les transactions numériques, les identifiants numériques dépasseront les identifiants physiques, et la servitisation numérique deviendra clé.

• Avenir du travail

Avec le travail hybride, la sécurité Zero Trust domine la sécurité en 2022. Au-delà des environnements sûrs au bureau, de la gestion sécurisée des identités et accès pour ceux à distance, des meilleures pratiques, des solutions sans contact, de la protection des données et gestion des visiteurs, l'accent est mis sur les solutions d'authentification multi facteurs pour les applications distantes.

• Biométrie sans contact

La biométrie liée à des solutions de gestion d'identité basées sur le cloud alimentera une croissance rapide. La sécurité au sein d'une technologie biométrique permet une authentification sécurisée et protège la confidentialité des données

• Data Science

Technologies IoT, cloud et mobiles transforment déjà l'industrie de la sécurité. L'intelligence artificielle et le machine Learning intégreront les solutions d'identité de confiance dans le continuum physique et numérique, automatisant les performances, la précision, la sûreté et la sécurité. Tirer parti des innovations en matière de solutions et services pour un niveau de sécurité plus élevé dans les domaines physique et numérique est une priorité.

Source Prédictions 2022 d'HID Global

Wasabi Technologies

REND LE PROCESSUS DE STOCKAGE PLUS SIMPLE ET INTUITIF

A l'heure où les entreprises se tournent indéniablement vers le Cloud pour stocker les données ou faire fonctionner les applications, la question cruciale de la souveraineté demeure...



Qu'il s'agisse d'exigences en matière de stockage ou de protection, le traitement des données est plus que jamais en jeu. **Richard Czech**, Directeur EMEA chez Wasabi Technologies a accepté de répondre à quelques questions.

Pourriez-vous nous présenter Wasabi Technologies, l'entreprise, son développement et son actualité 2022 ?

Wasabi Technologies s'est fixé pour objectif de transformer le secteur du stockage cloud en proposant le « hot cloud storage », prévisible et abordable pour les clients du monde entier. Avec Wasabi, les entreprises peuvent stocker et accéder instantanément à une quantité illimitée de données à 1/5^e du prix des hyperscalers, sans paliers ni frais pour les demandes de sortie ou d'API. Avec

leurs données conservées "à chaud", elles sont accessibles facilement en quelques millisecondes.

Depuis notre création en 2017, nous connaissons une forte croissance, en particulier en Europe, avec une forte demande pour le hot cloud storage de Wasabi. Nous avons commencé notre déploiement mondial à Amsterdam avant de nous lancer à Londres, et plus récemment à Paris et Francfort prochainement. Au fur et à mesure que notre base s'élargit, nous nous engageons à répondre aux demandes de stockage de chaque utilisateur et à soutenir leurs opérations avec un service de stockage rentable, de haute performance et au plus près de chez eux. Nous avons également assisté à l'expansion de notre réseau de partenaires européens, qui comprend des réseaux exclusifs ainsi qu'un réseau de revendeurs et de MSP qui nous accompagnent afin de fournir un stockage cloud performant à travers l'Europe.



Azure Virtual Desktop et l'expertise Insight, pour une expérience de bureau à distance agile, moderne et sécurisée

Azure Virtual Desktop est une plateforme VDI (Virtual Desktop Infrastructure) cloud flexible qui offre en toute sécurité des bureaux virtuels et des applications distantes avec un maximum de contrôle.

Pour en savoir plus, rendez-vous sur : <https://fr.insight.com>





RICHARD CZECH

Nous allons poursuivre notre hypercroissance dans la région, en nous concentrant uniquement sur l'aide à apporter à nos clients pour qu'ils tirent le meilleur parti de leurs données en leur fournissant une solution de stockage rentable et performante à proximité de chez eux.

Pourquoi le stockage des données est-il plus crucial que jamais aujourd'hui ?

Les données ne sont plus un sous-produit de l'entreprise, elles en sont l'élément vital. Les entreprises ne peuvent tout simplement pas exister sans avoir accès à une énorme quantité de données. Auparavant, les coûts de stockage et la confusion des niveaux obligeaient les entreprises à faire un choix entre les données à conserver ou non, et pour combien de temps, en renonçant éventuellement à des renseignements commerciaux essentiels. C'est là que Wasabi entre en jeu.

Wasabi croit en l'économie du stockage "bottomless cloud" dans lequel les clients conservent toutes les données dont ils ont besoin pour alimenter leurs entreprises et ont la possibilité d'y accéder exactement au moment où ils en ont besoin. L'accès instantané et facile, sans frais supplémentaires pour les requêtes de sortie ou d'API, élimine une grande partie des frictions auxquelles les entreprises sont confrontées. Cela rend finalement le processus de stockage plus simple et beaucoup plus intuitif pour les organisations, afin qu'elles puissent se concentrer sur les résultats commerciaux, plutôt que sur la complexité du stockage des données.

Wasabi Technologies a ouvert un site en France, en région parisienne. Un mot sur cette ouverture ?

Nous avons ouvert notre site parisien en janvier 2022 dans le cadre de notre stratégie d'expansion mondiale. Diverses réglementations en matière de protection et de souveraineté des données ont forcé

les organisations européennes à réévaluer la manière dont elles stockent les données, et par conséquent, elles souhaitent de plus en plus stocker leurs données dans le pays dans lequel elles opèrent.

L'ouverture d'une unité de stockage Wasabi à Paris nous aide à répondre efficacement à la demande de stockage Cloud en France tout en atténuant ces préoccupations de souveraineté des données et en renforçant notre performance en Europe.

Un mot sur votre positionnement par rapport aux exigences européennes en matière de souveraineté des données ?

Quoi qu'il arrive avec les différentes réglementations en vigueur en Europe, nous savons que nos clients et partenaires souhaitent simplement que leurs données soient stockées dans le pays où ils opèrent. Répondre à cette priorité est la pierre angulaire de notre stratégie d'expansion européenne.

Wasabi croit en l'économie du stockage "bottomless cloud" dans lequel les clients conservent toutes les données dont ils ont besoin.

Wasabi poursuivra son expansion en Europe tout au long de l'année 2022, avec notamment un nouveau site en Allemagne, à Francfort (mars). Nous continuerons à nous développer là où les entreprises ont besoin de nous.

En fin de compte, nous sommes fiers de fournir hot cloud storage qui est abordable, évolutif, sécurisé et accessible au moment où les données sont nécessaires, ce qui signifie qu'il n'y a pas de délais de latence basés sur les niveaux. Les données doivent se trouver exactement là où les gens en ont besoin.

> Par Sabine Terrey



Actualités, chroniques et dossiers informatiques experts pour les Professionnels IT.

Nouveau sur ITPro.fr : les chaînes Enjeux DSI et Vidéos IT !



Le difficile défi de rétention des équipes IT

Entre accélération du rythme de la transformation digitale et rétention du personnel technique, comment procéder au mieux ?

Forte charge de travail & Attentes irréalistes !

Les départements IT sont essentiels pour la croissance et la stratégie commerciale de l'entreprise selon 61 %. Il faut tenir le cap et le rythme de la transformation digitale et bien entendu conserver le personnel technique. Ce n'est pas si simple.

72 % annoncent perdre du personnel. Mais quelles sont plus précisément les causes du départ des membres de l'équipe ?

- La forte charge de travail
- Les attentes irréalistes envers l'équipe
- Le manque de soutien de la direction
- L'impossibilité de télétravailler
- L'équipe de direction peu encline à adopter l'automatisation
- L'absence des technologies indispensables pour travailler efficacement

Déconnexion entre VP et managers

Le constat est sans appel : on note une réelle déconnexion entre les hauts responsables/VP et les managers/directeurs.

Les managers et directeurs signalent que le département IT est considéré seulement comme un centre de coûts (27 %), contre 19 % des hauts responsables/VP.

De plus, 32 % pensent que l'équipe de direction associe le département IT uniquement au dépannage du matériel et des logiciels.

Avec le passage rapide au télétravail, on relève une accélération des plans ou une augmentation du taux d'adoption des offres de services IT automatisés.

Everywhere Workplace

Les collaborateurs veulent désormais se connecter sur différents périphériques pour accéder aux réseaux, données et services de l'entreprise.

Garantir la connexion continue de ces périphériques et services, met une forte pression sur les membres de l'équipe IT.

Selon 55% des décideurs, le département IT gagne 1-8 heures par demande de service grâce à l'automatisation des processus. Dans les entreprises où plus de 50 % des services IT sont automatisés :

- le gain de temps atteint plus de 16 heures par demande de service.

L'automatisation, indicateur clé de croissance

Là où 50 % des services IT sont automatisés, le département IT est perçu comme essentiel pour la croissance et la stratégie commerciale - 74 %. En effet, l'automatisation fluidifie la gestion des environnements hybrides en automatisant l'infrastructure, le Cloud et les processus d'espace de travail.

Enfin, les tâches manuelles de routine consomment des ressources IT et ne permettent pas aux équipes de se consacrer aux projets stratégiques et à l'innovation.

Source Ivanti - 250 professionnels de l'IT d'entreprise en Amérique du Nord, et en régions APAC et EMEA – Entre août et octobre 2021.

Réaliser une croissance à deux chiffres GRÂCE AUX DONNÉES ZERO PARTY

Au cours des quinze dernières années, le marketing personnalisé s'est construit sur la « traque » des consommateurs. Les cookies de tiers, les listes et données de tiers étaient la norme, même si les marketeurs savaient que ces informations non vérifiées étaient biaisées et intrusives. Aujourd'hui, la collecte de données pour la personnalisation du marketing évolue rapidement. Grâce à un contrôle de la réglementation accru et à l'accent mis depuis longtemps sur la création d'une relation de confiance avec les clients, le harcèlement n'est plus de mise. La tendance est aux données auto-attestées, telle que chez ASICS par exemple. Depuis 2017, son équipe omnicanale a mis en place un impressionnant programme de marketing personnalisé qui dynamise considérablement l'acquisition de clients et la CLV (Customer Lifetime Value).



François Rychlewski, VP of Sales EMEA chez SheerID explique ainsi comment les données Zero-party sont la nouvelle clé de voûte des entreprises pour repenser leur marketing digital et gagner de façon durable la confiance des consommateurs.

Un changement radical s'opère dans la personnalisation

Les préoccupations relatives à la protection de la vie privée poussent les marques à repenser le marketing personnalisé. Des plateformes technologiques comme Google et Apple éliminent progressivement les cookies et les identifiants d'appareils, ouvrant ainsi la voie à un « avenir sans cookies ». Les équipes marketing quant à elles adoptent de nouvelles stratégies pour atteindre les consommateurs.

Selon une récente enquête du CMO Club auprès des directeurs marketing (CMO) de différents secteurs : 84 % des CMO considèrent qu'il est très important de s'éloigner des sources de données tierces en raison des problèmes de confidentialité. Plus de

73 % augmentent leurs investissements dans des programmes communautaires et de contenu axés sur les consommateurs. 80 % investissent davantage dans la publicité organique.

Les données Zero-party, nouvelle clé de voûte de la personnalisation

Les données Zero-party sont des informations personnelles qu'un consommateur choisit de fournir volontairement, généralement pour bénéficier d'une offre, d'un avantage de la part d'une marque. Il s'agit des données au plus fort potentiel qu'une marque peut collecter. Elles sont auto-attestées et vérifiées, signalent une intention élevée du consommateur et reflètent un échange de valeur réciproque, qui donne des résultats. En d'autres termes, les consommateurs sont prêts à fournir des données personnelles, si une marque est transparente quant à la manière dont elle utilisera ces données et si elle leur offre une expérience à valeur ajoutée en échange de ces données.



FRANÇOIS RYCHLEWSKI

C'est ainsi que ASICS a commencé à développer son programme de fidélisation OneASICS conçu à l'origine pour offrir des avantages exclusifs, comme la livraison gratuite, aux clients réguliers. Puis, la marque a intégré les données collectées dans son écosystème numérique élargi et les a utilisées pour étendre ses initiatives de marketing personnalisé. Aujourd'hui, ces données Zero-party permettent à ASICS de se démarquer de ses concurrents et de stimuler sa croissance en accentuant son objectif d'établir des relations solides et durables avec ses clients, en fournissant une vue à 360 degrés des clients sur tous les canaux et plateformes de vente directe, et en offrant des expériences de contenu personnalisées aux clients connectés à son site Web ou à son application mobile.

Exploiter les données pour célébrer l'identité des clients

Il est alors possible d'offrir une personnalisation adéquate en collectant et en exploitant les trois types de données suivants.

Les données sur l'historique d'achat : recueillies par l'équipe omnicanale d'une marque lorsque les clients sont connectés ou utilisent leur compte de fidélité. Ces informations sont aussi utilisées pour proposer un contenu pertinent sur tous les canaux.

Les données d'usage : en plus d'un site web, les clients peuvent utiliser une ou plusieurs applications d'une marque, offrant ainsi à l'équipe omnicanale de la marque de quoi intégrer des points de données comportementales à ses campagnes de personnalisation.

Les données d'auto identification : grâce aux offres basées sur la vérification digitale d'identité, les marques peuvent s'adresser à des communautés spécifiques de clients en fonction de leur profession ou de leurs affiliations, et ainsi offrir des remises aux étudiants, aux soignants ou aux seniors. La vérification digitale de ces clients facilite l'auto identification d'acheteurs potentiels, en tant que

membres de la communauté ciblée et leur permet de bénéficier de leur réduction. Ces données précieuses et auto-attestées permettent aux marques non seulement de personnaliser davantage les expériences et de renforcer la confiance, mais aussi d'atteindre de nouveaux clients.

Trois conseils pour collecter et tirer parti des données Zero-party

1. Se développer avec la vérification digitale

Grâce à une vérification d'identité automatisée, les marques se protègent contre la fraude et l'abus de coupons, et s'épargnent des centaines d'heures de traitement manuel par semaine. Elles assurent l'exclusivité de leur offre, ce qui la rend plus attrayante et augmentent ainsi considérablement leur taux de conversion.

2. Être patient et flexible

Les marketeurs doivent fixer des attentes, des objectifs et des délais réalistes. Le marketing basé sur la vérification d'identité ne se fait pas du jour au lendemain. Il faut faire des essais, avoir beaucoup de patience et aussi la volonté de s'adapter continuellement en fonction de l'évolution des réglementations et des attentes des consommateurs."

Les marketeurs doivent fixer des attentes, des objectifs et des délais réalistes.

3. Rester à l'écoute des consommateurs

Il est impératif de constamment demander l'avis des clients, que ce soit par le biais de groupes de discussion, d'enquêtes ou du service client interne. Rester à l'écoute et apprendre des clients permet de comprendre ce qu'ils veulent et de faire évoluer les programmes en conséquence.

Les offres spéciales proposées par de nombreuses marques aux personnels de première ligne, aux soignants, et aux autres groupes les plus touchés par la pandémie sont un bon exemple de programme pour gagner la confiance des consommateurs.

Ces offres ont suscité une attention considérable et représentent une tendance qui perdurera. Aujourd'hui, les consommateurs sont ultra-sollicités. Utiliser des moyens respectueux de la vie privée pour leur offrir une valeur ajoutée substantielle renforcera la confiance dans une marque, créera des liens émotionnels et les encouragera à fournir à une marque des données personnelles qu'elle pourra utiliser pour les engager durant de nombreuses années.

Azure ARC, HYBRIDE ET MULTI-CLOUD

Annoncé lors de la conférence Ignite 2019, Azure Arc est arrivé un peu comme un OVNI dans l'environnement des fournisseurs de Cloud. Lors de cette annonce se posait une multitude de questions.



ARC est-il une nouvelle console de gestion, une sortie de Windows Admin Center pour le Cloud Azure ? Est-ce un complément pour les produits hybrides Azure Stack ?

Il semble y avoir la possibilité de connecter d'autres fournisseurs de Cloud pour utiliser un outil de gestion unifié ?

Arrivés en même temps que cette annonce, les premiers schémas de présentation donnent une idée de ce que va permettre le produit.

- On premises, on retrouve deux versions de l'Azure Stack installées sur des datacenter OnPrem. Mais également du matériel hors Stack symbolisé sur le schéma par des baies serveurs « Any Hardware ».
- Du Multi-Cloud
- Enfin, sur la partie Edge, la version dite portable de l'Azure Stack qui est un élément un peu à part.

Puis on trouve sur le reste du schéma quelques références à l'Azure Active Directory (l'annuaire Azure), des éléments de sécurité avec Microsoft Defender dans le Cloud, des références aux pratiques Devops (de plus en plus courantes dans l'exploitation d'un environnement Cloud Azure) et au centre, une référence Azure Data Services and Management, que l'on peut traduire par, Console de gestion du portail Azure.

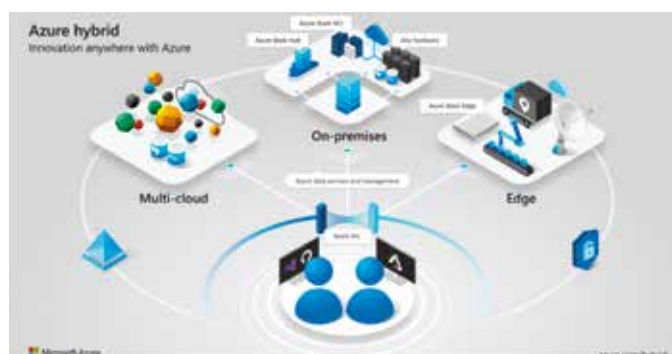
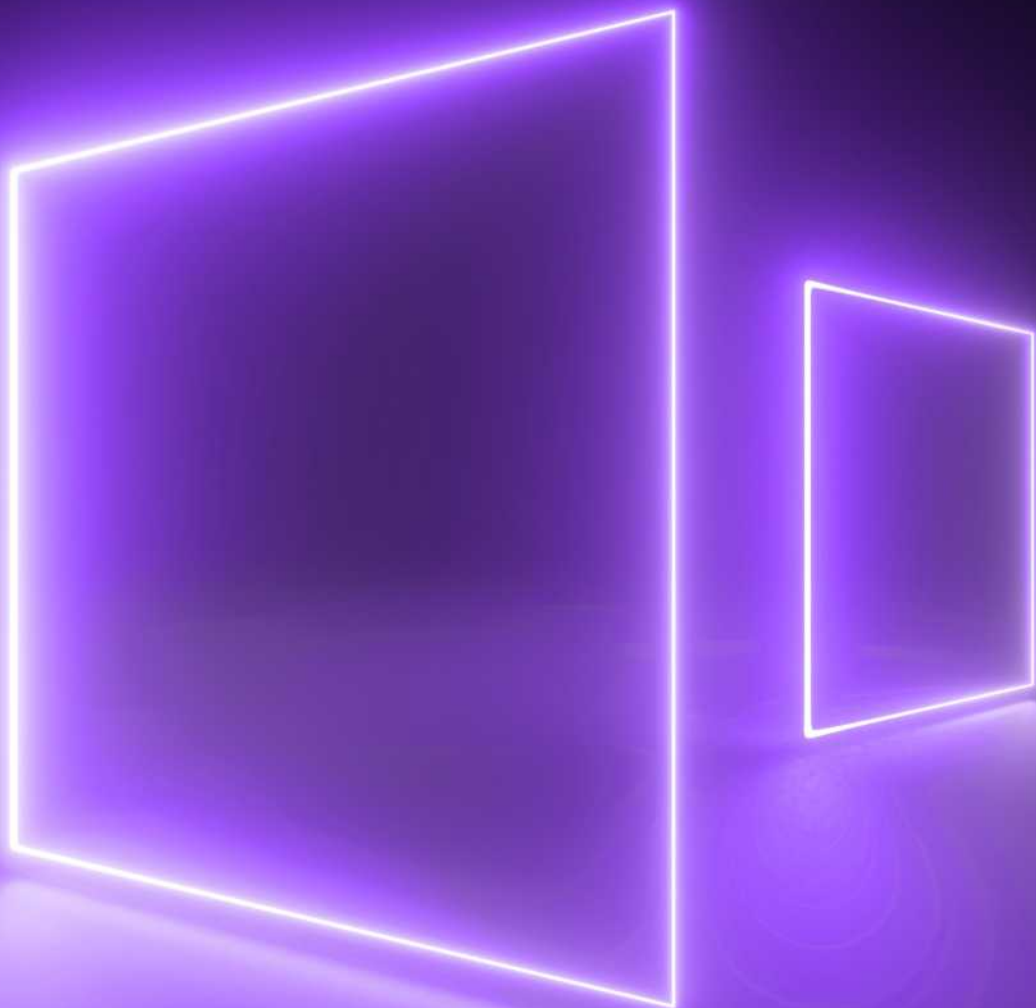


Schéma de présentation pour Azure ARC. Image éditeur.

CARBONITE® + WEBROOT®

— opentext™ companies —



**Microsoft 365
ne sauvegarde pas
tous vos fichiers.**

Nous, oui

Pour en savoir plus :

<https://www.carbonite.com/cp/intl/fr/microsoft-365-backup>

Ou contactez-nous au +33 (0)1 47 96 55 41

ou par email france-smbc@opentext.com

Si ce schéma est un bon résumé des capacités du produit, j'aime compléter cette vue par une courte explication et par une vue logique, plus « excitante » et plus directe.

Si l'on oublie un instant l'emplacement des machines « hors Cloud Azure », on trouve d'un côté, le portail de gestion Azure, de l'autre, des machines physiques ou virtuelles de type Windows ou Linux. Point !

Que ces machines se trouvent chez un autre fournisseur de Cloud autre qu'Azure, qu'elles se trouvent physiquement sur votre Datacenter ou même qu'elles soient virtualisées dans votre Datacenter, elles sont éligibles à la connexion Azure Arc. Avec même un gros plus qui n'apparaît pas sur l'image précédente, la possibilité de connecter des clusters Kubernetes locaux ou hébergés chez d'autres. Voilà pour cette vue pragmatique et rapide.

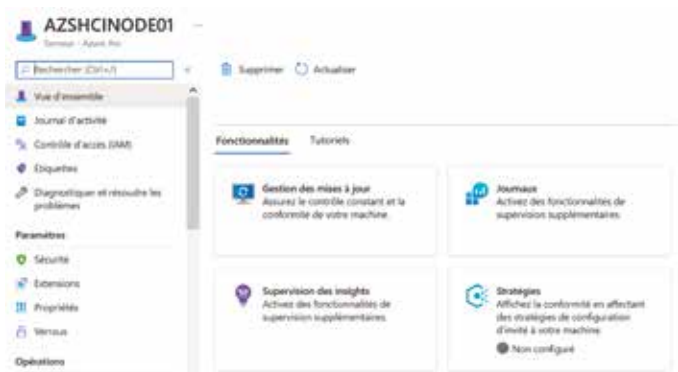
Quelles fonctionnalités ?

Ce qui intéresse, maintenant que la portée d'utilisation du produit est un peu plus claire, c'est ce que rend possible cette intégration, et quels sont les bénéfices à en tirer.

Connecter la machine à ARC, c'est simplement installer un agent appelé *Azure Connected Machine*. Voilà pour résumer la phase d'intégration. Il y a très peu à faire pour cette partie.

A partir de cet instant, les principaux outils de gestion, de configuration et d'administration Azure sont disponibles sur ces machines intégrées.

C'est ici que l'on découvre que l'agent n'est pas simplement utilisé pour consulter l'état d'une machine, c'est-à-dire pour la lecture d'informations, mais qu'une majorité des outils de gestions Azure sont ajoutés pour cette machine. Ce n'est pas uniquement comme on l'entend parfois un outil de supervision ou de visualisation, c'est beaucoup plus que cela.



Un serveur Azure ARC dans le portail Azure.

Connecter la machine à ARC, c'est simplement installer un agent appelé Azure Connected Machine.

Il faut connaître la charte graphique utilisée par les composants ARC (le demi-cercle bleu qui souligne l'icône du serveur) pour identifier rapidement que cette machine n'est pas une machine Cloud Azure. Tout dans le menu laisse à penser que c'est un serveur classique comme ce que l'on retrouve sur le portail pour les machines Cloud.

Nom	Type
AZSHCINODE01	Serveur - Azure Arc
ptbtwin0001	Machine virtuelle
ptbtwin0003	Machine virtuelle

Entouré de noir, le cercle bleu des ressources ARC.

Profiter des outils de gestion Azure, c'est profiter d'une liste de fonctionnalités des plus intéressantes. De la mise à jour, en passant par la consolidation des journaux ou la possibilité d'utiliser les stratégies (ou Policy) Azure.

La liste des possibles est mise à jour régulièrement mais on retrouve quelques-unes des fonctionnalités Cloud les plus importantes.

La présentation suivante est incomplète mais ce sont certaines des possibilités les plus intéressantes.

- De la gouvernance avec Azure Policy (en mode audit), les étiquettes ou tags Azure et le support des accès basés sur les rôles.

Si une seule des fonctionnalités devait être mise en avant, ce devrait être celle-là. Gouverner son IT est assez complexe, le faire avec cet ajout de fonctionnalité est un très beau progrès !

- Les journaux, c'est-à-dire l'intégration à log Analytics et sa capacité d'ingestion de données couplée au langage de requêtes Kusto pour l'analyse de ces données.

Cette fonctionnalité est également utilisée pour la surveillance et l'affichage de métriques d'utilisation et de consommation.

- Les outils de mise à jour comme Update Management, ainsi que des compléments comme l'inventaire.

En plus de ces quelques fonctionnalités majeures, une machine intégrée peut être enrichie de quelques extensions (que l'on peut voir comme des plugins ou de petites applications complémentaires) qui vont encore faciliter et améliorer la gestion des machines. On trouve par exemple dans cette liste la fonctionnalité Powershell DSC qui assure le maintien en condition opérationnelle des machines et un mécanisme d'auto remédiation. Ce n'est pas un spécifique Azure, mais c'est une possibilité qui s'intégrera facilement au travers des extensions.

Choisir Azure ARC, c'est moderniser son informatique, mais c'est surtout uniformiser, unifier sa gestion.

Choisir Azure ARC, c'est moderniser son informatique, mais c'est surtout uniformiser, unifier sa gestion. Un même outil, complet et cohérent pour simplifier son exploitation. Pour une entreprise déjà utilisatrice des services Azure et qui exploite également son propre Datacenter avec ses propres ressources, c'est une évolution logique et naturelle.

Porter peu à peu les ressources éligibles sur ARC permet à court terme de reconduire tous les « ça marche » de son Azure existant sur des ressources hébergées par d'autres.

Dernier point de ce sujet, la tarification. Les informations précises sont à consulter sur ce lien <https://azure.microsoft.com/fr-fr/pricing/details/azure-arc/>. Ici, tout sera affaire de choix. Intégrer une machine, ce n'est pas obligatoirement activer toutes les fonctionnalités. Ici, ce n'est pas très différent de ce que propose une machine Cloud Azure.

Il faudra bien réfléchir ses dépenses et adapter fonctionnalités et extensions aux usages.

	Ressource Azure	Ressource Azure Arc
Fonctionnalité du plan de contrôle Azure	Gratuit	Gratuit
Configuration invité Azure Policy (inclut le suivi des modifications Azure Automation, l'inventaire, la configuration de l'État)	Gratuit	\$6/Service/Mois

Exemple de prix pour un service ARC.

Pour résumer, un rappel des points importants

- 1 / Intégrer une machine à Azure ARC, c'est lui ajouter tout un tas d'outils de gestion parfaitement intégrés au portail Azure.
- 2 / Intégrer une machine, c'est uniformiser et faciliter l'exploitabilité de son parc, c'est profiter d'une console de gestion centrale.
- 3 / Azure ARC est granulaire, intégrer une machine, ce n'est pas lui ajouter toutes les fonctionnalités. La calculatrice Azure permettra d'adapter finement son besoin et son ratio usage / coût.

Thierry Bollet, MVP Azure, travaille chez Capgemini. Auteur aux Editions ENI, il est passionné aussi de Powershell et d'automatisation



Sur iPro.fr, 9 chaînes d'informations et de formations des meilleurs experts en technologies informatiques d'entreprise, par les éditeurs du mensuel IT Pro Magazine.

Bénéficiez d'une richesse éditoriale incomparable... connectez-vous !



S!MPL : L'INTELLIGENCE ARTIFICIELLE PROACTIVE AU SEIN DE SIMPLE CRM

Simple CRM, logiciel de travail collaboratif, architecturé autour d'une intelligence artificielle, nommée HaPPi, a été le premier logiciel de gestion à embarquer une IA et ce, depuis 2015. Revenons sur la technologie, la création de la pépite franco-belge mais aussi la stratégie et les perspectives avec Brice Cornet, CEO de S!MPL.



Brice Cornet, et les deux cofondateurs historiques, **Vladimir Cousew**, CTO et **Elena Popa**, COO, ont construit dès 2012 un modèle fonctionnel basé sur des analyses de terrain pratiques, des modélisations issues du milieu universitaire et les résultats des travaux de recherche du CEO. C'est ainsi qu'en se basant sur les besoins pragmatiques des entreprises, la nécessité d'introduire l'intelligence artificielle dans la conception du CRM et de l'ERP s'impose.

Mais qui est S!MPL ? pourriez-vous nous en dire plus ?

S!MPL, éditeur de logiciel, établi à Verviers en Belgique et à Bergerac en France, est éditeur de Simple CRM, logiciel CRM dont la qualité est saluée par les professionnels du secteur.

En 2005, **Brice Cornet** lance E-DIABOX, un groupware dédié au milieu automobile qui se mue dès 2008, en CRM dédié aux Universités et Hautes Ecoles, pour se transformer en Simple CRM, en 2012. L'idée est de construire la solution de gestion sur base de la réalité du terrain.

Un mot sur la stratégie et sur HaPPi ?

La croisement Jarvis de Iron Man + Siride Apple fit réfléchir **Brice Cornet** au futur de Simple CRM : les outils SIMPL devaient être construits autour d'une intelligence artificielle qui soit pro-active pour renverser l'échelle de valeur. Que se passerait-il si le logiciel venait vers les utilisateurs avec des données potentiellement intéressantes ? si le logiciel analysait les données, détectait des problèmes potentiels et proposait des solutions ? C'est sur la base de cette vision que naquit HaPPi, l'IA maison.

LE DROIT À LA DÉCONNEXION : UN ENJEU RH

DANS UN MONDE RÉGI PAR L'IMMÉDIATÉTÉ,
LA DÉCONNEXION N'EST PLUS UNE OPTION, MAIS UN DROIT.

**PROMODAG REPORTS PERMET LA CONFORMITÉ
AVEC LE DROIT À LA DÉCONNEXION**

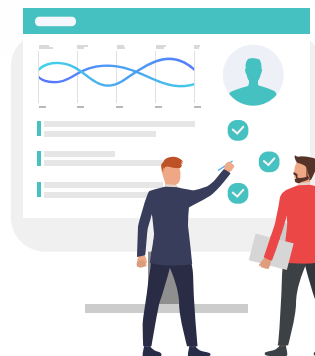
**GÉRER LA DÉPENDANCE EXCESSIVE
AUX TECHNOLOGIES**



**LE DROIT À LA DÉCONNEXION EST
UNE OBLIGATION LÉGALE**



**DES CHARTES DE
BONNES PRATIQUES POUR LE
CONFORT DES SALARIÉS**



**UN OUTIL AU SERVICE DES
RESSOURCES HUMAINES**



**UNE SOLUTION DE SENSIBILISATION,
D'ALERTE ET DE PRÉVENTION**



**PROMODAG REPORTS MAÎTRISE LE DROIT À LA
DÉCONNEXION & PROTÈGE VOS SALARIÉS**
Découvrez la solution Promodag Reports



Promodag

www.promodag.fr

La première tâche de HaPPi fut de rendre la totalité des fonctionnalités de Simple CRM accessibles à tous et toutes.

La road map de développement des solutions est, ainsi dès 2020, axée sur l'Intelligence Artificielle

Quelques dates clés

Dès 2015, les utilisateurs ont la possibilité de poser des questions simples ou complexes à HaPPi : "HaPPi où est mon calendrier ?", "HaPPi donne-moi la liste de mes clients peu rentables." Plusieurs expérimentations ont été réalisées. En 2016, une fonction phare apparaît : la possibilité pour HaPPi de proposer des clients potentiels. Dès 2017, HaPPi est dotée d'un cerveau mémoire pointant les forces, faiblesses, opportunités et menaces gravitant dans et autour des entreprises. Le but est de réaliser des analyses faciles et complexes.

Enfin, en 2019, HaPPi peut analyser les avis publiés sur Internet, pour mesurer le branding d'un produit ou la marque employeur.

Puis via le chat d'entreprise Simple Messenger, HaPPi devient capable de communiquer des analyses, des idées, des stratégies, des solutions, tout en animant les équipes au travers d'une gamification de l'activité.

La capacité d'HaPPi à conseiller et accompagner est la priorité.

Dans la version 10 de Simple CRM, on parle d'évolutions majeures, quelles sont-elles ?

Après avoir intégré, en 2014 la reconnaissance vocale (vous parlez et le CRM écrit), en 2015 les ordres vocaux (vous dictez une tâche et le CRM le réalise) et en 2016 la détection de client potentiel (l'IA détecte des clients potentiels à contacter qu'elle transmet aux commerciaux), le nouveau Simple CRM version 10 est équipé de la première IA qui sera une réelle assistante proactive pour chacun des collaborateurs de l'entreprise.

L'intelligence artificielle et l'ouverture sont majeures car en s'ouvrant aux autres Systèmes d'informations et en intégrant leurs données dans Simple CRM, on nourrit l'IA.

C'est donc un portage indirecte de notre IA sur les dates des autres SI !

C'est un moyen détourné de lui offrir plus de données à analyser et de facto, plus de puissance. La stratégie d'ouverture permettra à l'intelligence artificielle de Simple CRM version 10, d'analyser des données venant d'autres SI. L'IA de Simple CRM pourra être portée, de façon indirecte, sur d'autres logiciels, de par le patrimoine de données, issu des synchronisations : un avantage stratégique énorme pour les entreprises.



BRICE CORNET

Vous évoquez la "première IA généraliste fournie sur étagère" ou encore "la première IA 100% francophone" ?

Actuellement, la relation avec un CRM est mono directionnelle : ce sont des utilisateurs qui vont vers le CRM pour y saisir et y consulter des données. Avec Simple CRM version 10, c'est le CRM qui va aller vers l'utilisateur en proposant du contenu, des analyses et des pistes de travail pertinentes. Et le tout, sans implémentation ou réglage spécifique : c'est l'IA qui fait réellement tout le travail.

Le défi est de taille : en 8 mois, cette IA sur étagère sera capable de comprendre le métier de chacun des collaborateurs afin de fournir des conseils pertinents qui allégeront la charge mentale des équipes et faciliteront réellement leur quotidien. C'est un changement total de paradigme !

Un mot sur l'année 2022 ?

Pour nous 2022, c'est avant tout livrer le fruit de 10 ans de travail, avec la première IA généraliste. Ce sera à partir de septembre, un énorme travail d'écoute de nos clients pour intégrer leurs feedbacks et leurs usages par rapport à cette IA.

A partir de la fin d'année, ce sera la création d'un plan stratégique pour communiquer clairement la valeur ajoutée de la techno.

Côté croissance, nous restons prudents dans nos prévisions car avec une Covid qui redistribue non-stop les cartes, il est complexe de poser les bons axes. On anticipe donc une croissance sereine de 22% par rapport à 2021.

> Par Sabine Terrey

SMARTDSI®

DOSSIER
La gestion de portefeuille pour créer de la valeur

INTERVIEW
Rendre le processus de stockage plus simple et intuitif

L'ETUDE A RETENIR
Biométrie, Data Science et Durabilité au cœur de la sécurité en 2022

INTERVIEW
Tout le monde peut avoir la chance de comprendre l'Intelligence Artificielle

EXPERT
La confidentialité de vos réunions!

L'OEIL DU FUTUR
Innovation SIRH : quels changements la crise sanitaire a-t-elle pu faire émerger?

Club Abonnés sur ITPro.fr

« Comprendre les enjeux, évaluer les perspectives et conduire la transformation numérique de l'entreprise »

ABONNEZ-VOUS MAINTENANT !

SMARTDSI

Oui, je profite de votre offre d'abonnement pour recevoir les 4 prochaines éditions du magazine SMART DSI au tarif de 120 € ttc*

Tarif d'abonnement pour la France métropolitaine, pour les abonnés hors de France métropolitaine, l'offre d'abonnement est au tarif de 140 € ht*

*Taux de TVA 2,1 %

** Taux de TVA du pays destinataire, surtaxe postale incluse soit 20 € par abonnement

Date + signature

Mode de règlement :

A réception de facture* Par chèque joint

*réservé aux sociétés en France - Belgique - Luxembourg & Suisse.

Indiquez votre N° TVA Intracommunautaire :

VOS COORDONNEES

Société.....

Nom Prénom

Adresse de livraison

.....

.....

Code postal Ville

Pays

Tél. Fax

email.....

Renvoyez votre bulletin à notre service abonnements :

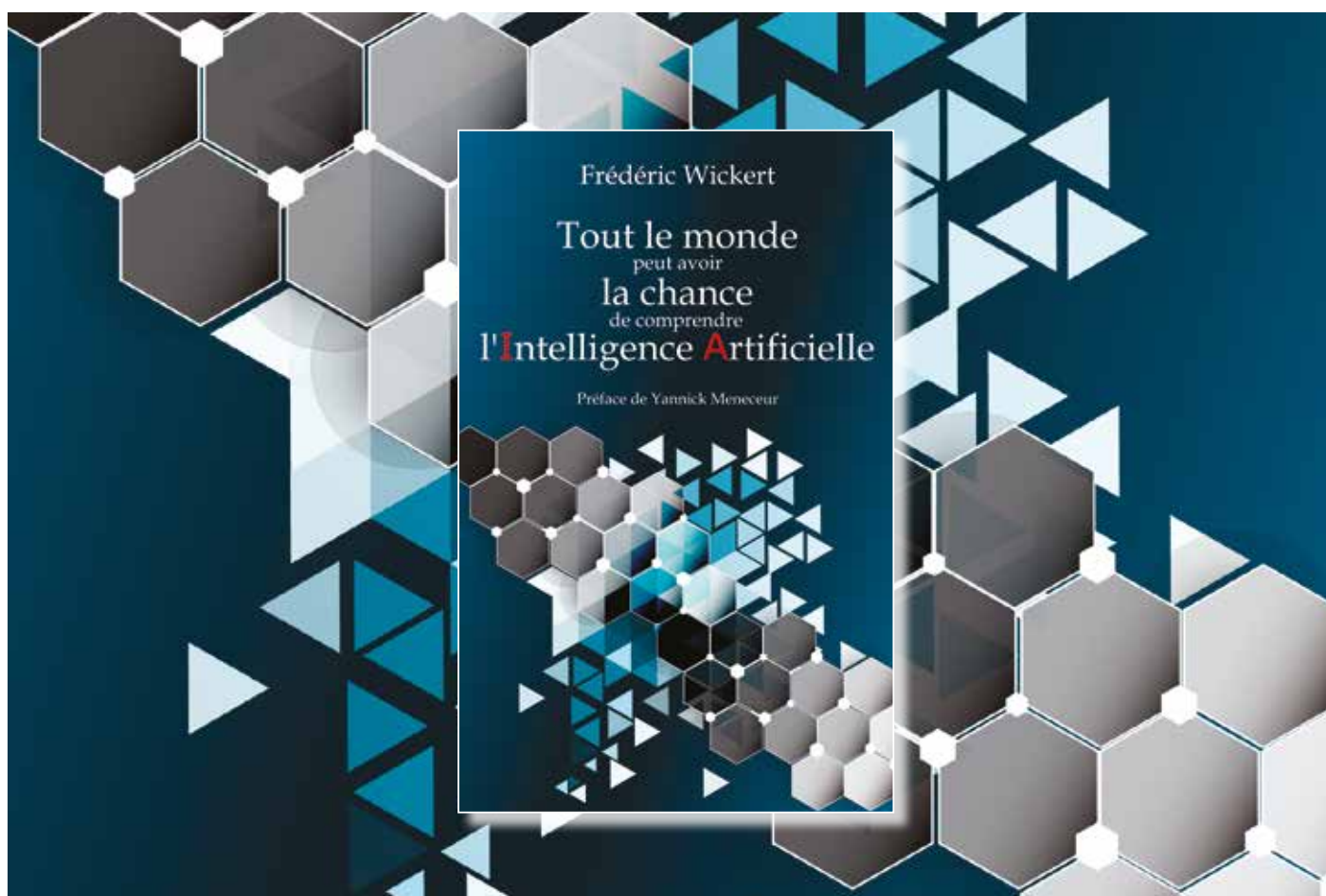
SMART DSI - ABOSIRIS - Service des abonnements
BP 53 - 91540 Mennecy - France

Fax. +33 1 55 04 94 01 - e-mail : abonnement@smart-dsi.fr

TOUT LE MONDE PEUT AVOIR LA CHANCE DE COMPRENDRE L'INTELLIGENCE ARTIFICIELLE

Comprendre la substantifique moelle de l'IA et s'en faire sa propre idée, c'est désormais possible grâce au livre de Frédéric Wickert qui s'attache, avec pédagogie et humour, à démocratiser et à clarifier l'Intelligence Artificielle.

De l'historique à la construction d'une définition, en passant par des explications très complètes sur les algorithmes, tout est passé en revue. Retour sur le sujet avec l'auteur, Frédéric Wickert qui se définit comme « un artisan » dans son métier et a accepté de répondre à quelques questions.



Conférencier, formateur et consultant en Intelligence Artificielle et en développement d'applications innovantes, il a animé de nombreuses conférences et ateliers sur l'Intelligence Artificielle dans l'objectif de la démocratiser et en apporter du sens. Également co-auteur du rapport sur les "Enjeux de la reconnaissance faciale" pour le Conseil de l'Europe, **Frédéric Wickert** jouit d'une expérience de 20 ans dans le numérique.

Passionné par son métier technique, il ne conçoit pas, « dans notre petit passage sur notre belle planète, de ne pas transférer les compétences acquises à ceux qui vont nous succéder ».

Sa « baseline » pourrait être : « Dispenser son savoir et transmettre sa passion ».



FRÉDÉRIC WICKERT

Il est important que tout le monde puisse élever son niveau de conscience sur ce sujet pour prendre des décisions en connaissance de cause.

Pourquoi avoir voulu écrire un livre sur le sujet ?

J'ai animé des centaines de conférences et ateliers sur ce sujet. Je voulais que toutes les personnes qui n'avaient pas encore eu la chance d'y participer puissent également saisir l'importance de l'Intelligence Artificielle dans nos vies. Et que tout le monde ait un ouvrage sur lequel s'appuyer que vous soyez étudiant, dirigeant, cadre, entrepreneur ou simplement un citoyen.

Mais au fait, c'est quoi pour vous l'Intelligence Artificielle ?

Il a fallu un livre pour expliquer ce que j'entendais par Intelligence Artificielle, compliqué de le résumer en quelques lignes. L'IA répond à des besoins que nous ne pouvons pas combler avec des algorithmes classiques et déterministes.

L'un des moyens d'y arriver serait, oui, je reste conditionnel, de « simuler l'intelligence humaine » avec un « ensemble de concepts et de technologies ». L'intelligence Artificielle sera ce que nous en ferons ! Mais pour une définition et comprendre vraiment, je vous conseille évidemment la lecture du livre.

Quel message avez-vous voulu faire passer dans ce livre ?

Le message est que « tout le monde » peut comprendre l'Intelligence Artificielle. Beaucoup trop de messages et de littératures tournent autour de la technique ou de la science-fiction. Les ouvrages clarifiant ce qu'est l'IA ne sont pas légions et plongent rapidement dans la technique ou dans l'apport de l'IA dans un métier particulier.

Il est important que tout le monde puisse élever son niveau de conscience sur ce sujet pour prendre des décisions en connaissance de cause. Notre avenir est certainement en jeu.

Si on devait garder en tête 5 points clés du livre ?

Le livre est structuré autour d'un triptyque basé sur le cercle d'Or :

Pourquoi en aurait-on besoin ?

Comment elle fonctionne ?

Que peut-on faire avec concrètement ?

Alors les 5 points clés pourraient être :

- Démocratisation, Clarification et non simplification
- Humour
- Exemples concrets
- A la portée de tous
- Les limites de l'IA

Avez-vous un dernier point à partager avec les lecteurs, un point qui vous tient particulièrement à cœur ?

Oui, l'Intelligence Artificielle n'est qu'un outil parmi tant d'autres. Certes puissant. Mais c'est à nous tous d'en faire quelque chose qui nous permet d'avancer dans l'idée de progrès.

Je dis souvent qu'il y a deux manières de craindre l'IA : Craindre qu'elle soit, souvent par méconnaissance mais également par crainte de perdre son emploi ou son libre arbitre. Et craindre qu'elle ne soit pas au vu des défis que nous avons tous à relever. Je fais partie de cette seconde catégorie.

Je le répète, il est important que nous élevions tous notre niveau de conscience sur différents sujets. L'IA en fait partie...

Je continuerai à créer des livres de « clarification » (je préfère ce mot à vulgarisation) pour aider chacun à cet objectif d'élévation.

J'ai encore foi en l'humanité.

> Par Sabine Terrey

Les utilisateurs cloud, VICTIMES PRIVILÉGIÉES DES RANSOMWARES

Selon le 7^{ème} baromètre du CESIN, publié le 17 janvier 2022, 1 entreprise française sur 5 a subi une attaque ransomware au cours de l'année 2021. De plus, pour 86 % des RSSI, la sécurisation des données stockées dans le cloud nécessite encore la mise en place d'outils spécifiques. Dans ce contexte émerge le ransomcloud, un nouveau vecteur d'attaque ransomware. Amir Landau, Malware Research Team Leader, au CyberArk Labs nous livre son analyse.



Qu'est-ce que le ransomcloud et comment cette attaque fonctionne-t-elle ?

Le ransomcloud est une attaque de ransomware qui cible les clients des services cloud, mais pas le fournisseur lui-même. Le chiffrement doit être initié sur le cloud et non sur une machine locale - en d'autres termes, le cybercriminel doit disposer d'identifiants de compte utilisateur cloud valides et avoir accès à tous les fichiers et ressources autorisés pour ce compte. Il peut alors utiliser le phishing, une fuite de données connue, une mauvaise configuration du cloud, un malware, des attaques DDoS ou tout autre moyen de prendre le contrôle du compte cloud de l'utilisateur. Une fois à l'intérieur, le hacker peut déployer un rançongiciel qui chiffre et vole les informations de la victime.

Qui est le plus exposé aux ransomcloud et quelles en sont les conséquences ?

Les entreprises disposant d'un compte cloud multi-utilisateurs avec accès aux fichiers et aux ressources autorisées sont les plus exposées. En effet, le principal vecteur pour ce type d'attaques est le phishing car il offre au cybercriminel une plus grande surface d'attaque du fait des comptes multi-utilisateurs.

Les autres groupes d'utilisateurs à risque sont ceux qui réutilisent leurs mots de passe. Les conséquences d'un tel comportement peuvent inclure une double extorsion, c'est-à-dire la perte de tous leurs fichiers et une demande d'extorsion sous menace de divulguer leurs informations privées.

EXPOSITION - TABLES RONDES
ATELIERS - RENDEZ-VOUS BUSINESS

SYMPOSIUM • CONFERENCES • WORKSHOPS •
USE CASES • RENCONTRES ONE TO ONE

IoT+MtoM Embedded

CLOUD DATA CENTER +INFRA

#MtoM / IIoT #Embedded

#Objets connectés

#Réseaux (pan, Lan, LPWAN, 5G, ...)

#Plateformes

#DATA (Edge Computing, Big Data, IA...)

#Cybersécurité



www.salon-iot-mtom.com



#Cloud Hybride

#Open Source

#Cybersecurity

#Plateformes

#Supervision

#Stockage Cloud

#Green IT

www.datacenter-cloud.com

29 et 30 juin 2022

PARIS EXPO- PORTE DE VERSAILLES



@IoTWorldParis1



@salonMtoM



Groupe Cloud et Datacenter Management

Comment les cybergangs développent-ils et déploient-ils de plus en plus d'outils de logiciels malveillants pour cibler le cloud ?

Il existe quatre méthodes courantes utilisées par les attaquants pour cibler le cloud. Premièrement, ils exploitent souvent la synchronisation des machines avec le cloud. En chiffrant les données localement, puis en synchronisant l'appareil avec le cloud, les données qui y sont stockées sont également chiffrées.

Les campagnes de phishing ordinaires sont une seconde méthode que les cybercriminels utilisent avec beaucoup de succès. Grâce à elles, les hackers peuvent obtenir les identifiants de leurs cibles et les utiliser pour accéder au cloud. Dans la même optique, une autre méthode à haut rendement consiste à cibler les fournisseurs de cloud eux-mêmes. Cela peut permettre aux acteurs malveillants d'accéder à plusieurs victimes, qui utilisent toutes le cloud. Enfin, ils profitent également de la technologie cloud configurée de manière non sécurisée pour y accéder.

En plus du ransomcloud, les cybergangs utilisent également des cryptomineurs ordinaires dans des environnements cloud, afin de tirer parti de la puissance du cloud computing. Par exemple, les pirates informatiques derrière le ransomware Maze ont noté que les sauvegardes dans le cloud peuvent servir d'arme à double tranchant. Elles facilitent en effet la recherche de données sensibles, car ces dernières sont généralement sauvegardées. De plus, l'extraction des données du cloud pour les attaques de double extorsion est moins susceptible de déclencher des contrôles de prévention des pertes de données (DLP).

Comment les entreprises peuvent-elles éviter la menace des rançongiciels cloud ? Quelles mesures peuvent-elles prendre ?

Le plus important est de comprendre qu'il existe une responsabilité partagée pour la sécurité des données entre les organisations et le fournisseur de cloud. Afin d'éviter la menace, les entreprises doivent d'abord demander à leur fournisseur de cloud de planifier des stratégies afin de se remettre d'une attaque de ransomware et d'autres types de pannes. Ils doivent également réfléchir aux mesures de sécurité qu'ils ont mises en place pour se protéger contre les attaques de cette nature, tout en s'assurant qu'ils utilisent une authentification à deux facteurs, et n'accordent des autorisations pour les ressources cloud qu'aux comptes d'utilisateurs qui en ont effectivement besoin - autrement connu sous le nom de principe du moindre privilège.

Il est également important pour les entreprises d'utiliser des outils anti-phishing et de s'assurer que les employés suivent une formation de sensibilisation à la sécurité. Dans ce cadre, l'importance d'utiliser un mot de passe compliqué comprenant des lettres, des chiffres et des caractères spéciaux doit être établie, en précisant que les mots de passe ne doivent pas être réutilisés dans tous les services. Les organisations doivent également imposer des changements de mot de passe à des intervalles appropriés. Enfin, les sauvegardes sont vitales. Les entreprises doivent stocker leurs informations à plusieurs endroits tout en effectuant des restaurations de test pour évaluer la résilience.



AMIR LANDAU

Le plus important est de comprendre qu'il existe une responsabilité partagée pour la sécurité des données entre les organisations et le fournisseur de cloud.

*« COMPRENDRE LES ENJEUX, ÉVALUER
LES PERSPECTIVES ET CONDUIRE
LA TRANSFORMATION NUMÉRIQUE
DE L'ENTREPRISE »*



SMARTDSI

www.smart-dsi.fr

« Analyses, dossiers, chroniques pour conduire la transformation numérique de l'entreprise »

Teams

LA CONFIDENTIALITÉ DE VOS RÉUNIONS !

Le travail à distance et le fait de se réunir systématiquement à travers Microsoft Teams n'empêche pas de s'interroger sur les stratégies de confidentialité des réunions. Plusieurs entreprises mal préparées, voire trop permissives, en ont fait les frais.

Dans cet article nous allons passer en revue tout ce que vous devriez savoir pour sécuriser vos réunions et autres webinaires.



L'ACCÈS EXTERNE

Par définition, une réunion Teams dans la plupart des cas, permet d'inviter n'importe quelle personne, qu'elle appartienne à l'entreprise ou pas. Dans ce scénario, on distinguera trois types de population :

- les personnes externes,
- les personnes invitées
- les anonymes.

La première population est constituée de personnes d'une autre organisation qui utilisent Microsoft Teams depuis leurs tenants. Dans ce cas, vous êtes à peu près certains que la personne externe que vous avez invitée, est bien celle qui va participer à la réunion. Sauf usurpation de son compte bien sûr.

La seconde population est constituée de comptes appartenant à votre organisation mais qui vont être utilisés par des personnes extérieures à celle-ci et qui n'ont pas l'usage de Teams. Avec l'accès invité, votre organisation fournit un compte d'accès à ces personnes auprès de votre Azure Active Directory leur permettant de s'authentifier et, in fine, participer à la réunion. Là aussi, vous êtes à peu près sûr que c'est la bonne personne qui va se joindre à votre réunion.

La troisième population est composée de personnes anonymes qui vont pouvoir accéder à votre réunion sans pour cela s'authentifier. Autrement dit, toute personne qui possède le lien de la réunion va de facto pouvoir rentrer dans la réunion. Certes, vous pouvez, avec les stratégies bloquer ces dernières, mais force est de constater que cette fonctionnalité est très utilisée dans les entreprises, justement pour inviter des personnes totalement externes à l'entreprise. Il est donc difficile de totalement bannir cette possibilité.

LES STRATÉGIE DE RÉUNION ET LEURS OPTIONS

La capture d'écran suivante illustre par conséquent une stratégie relativement permissive qui permet à n'importe qui de rejoindre une réunion mais qui limite malgré tout certaines fonctionnalités

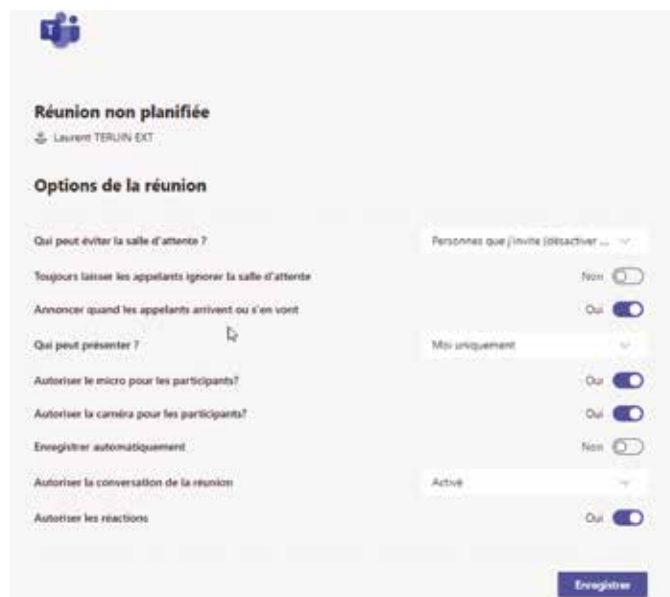


Une des premières choses à faire est de ne pas laisser la possibilité aux personnes non authentifiées de démarrer la réunion. Sans quoi, n'importe qui peut utiliser votre service de réunion. Le paramètre « *Let anonymous people join a meeting* » doit être positionné sur « *On* » mais le suivant, « *Let anonymous people start a meeting* » sur « *Off* » impérativement

Concernant l'accès au rôle présentateur je vous conseille plutôt de laisser la valeur suivante « *Organizers, but user can override* » ce qui signifie que par défaut, seul l'organisateur possède le rôle présentateur mais que les utilisateurs peuvent éventuellement changer cette option lorsqu'ils organisent des réunions. Comment le font-ils ? Par le biais du bouton ci-dessous présent dans leur Outlook



ou par le biais du lien Hypertexte de la réunion qui vous amènera à cette page de configuration



Attention, si vous changez certaines options, ces changements ne vont s'appliquer que sur votre réunion et non sur vos futures réunions. Par défaut, pour chaque nouvelle réunion, le client Teams appliquera la stratégie de réunion décidée par l'administrateur.

La troisième population est composée de personnes anonymes qui vont pouvoir accéder à votre réunion sans pour cela s'authentifier.

LES 2 ERREURS CLASSIQUES

Erreur 1 : Si vous planifiez une réunion dont vous êtes l'organisateur et par conséquent l'unique présentateur et que vous décidez d'inviter des personnes extérieures qui devront patienter dans la salle d'attente, et qu'au dernier moment vous décidez de rejoindre cette réunion par le pont de conférence audio téléphonique sans authentification, alors... vous serez vous aussi placé dans la salle d'attente. Sauf, si bien avant, vous avez pris le soin de prendre connaissance de votre code d'accès personnel en cliquant sur le lien suivant « *Réinitialiser le code confidentiel* ». ce que peu de personnes font.

Réunion Microsoft Teams

Rejoindre sur votre ordinateur ou application mobile

[Cliquez ici pour participer à la réunion](#)

Ou composer le numéro (audio seulement)

+33 1 73 24 00 20,83463 France, Beaumont-Sur-Oise

ID Conférence Téléphone: 834 633

[Rechercher un numéro local](#) | [Réinitialiser le code confidentiel](#) |

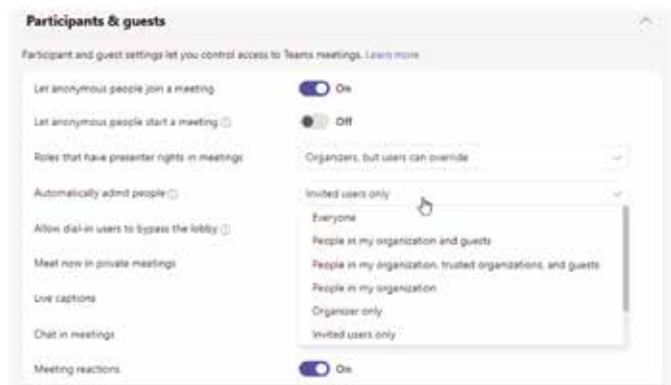
[Pour en savoir plus](#) | [Options de réunion](#)

Erreur 2 : Si vous planifiez une réunion dont vous êtes l'organisateur et par conséquent l'unique présentateur et si vous ne pouvez pas y participer, seule les personnes de votre organisation pourront accéder à la réunion mais ne pourront rien partager. Quant aux personnes anonymes elles resteront cantonnées dans la salle d'attente.

CHOISISSEZ QUI VOUS DÉSIREZ FAIRE RENTRER

Le paramètre « *Automatically admit people* » est dans notre cas positionné sur « *Invited Users Only* » ce qui signifie que seules les personnes ayant la possibilité de s'authentifier vont être automatiquement admises à rentrer dans la réunion.

Personnellement je ne suis pas un grand adepte de ce mode de fonctionnement et je recommande souvent de positionner cette valeur sur « *People in my Organization* » pour des questions de confidentialité. Dans ce mode, les personnes extérieures à l'organisation patienteront dans une salle d'attente le temps que les personnes internes coordonnent leurs messages par exemple.



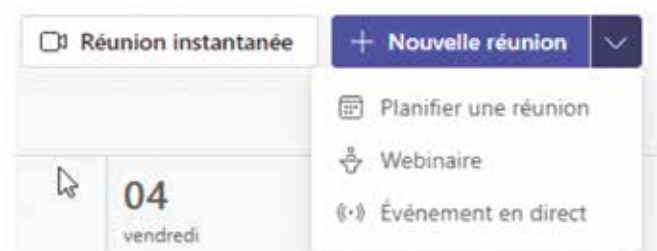
Il en va de même pour les personnes qui rejoignent la réunion avec leur téléphone portable via le pont de conférence téléphonique, et qui par définition ne sont pas authentifiées. Même traitement que les personnes extérieures, direction la salle d'attente.

BLOQUEZ L'ENREGISTREMENT DES RÉUNIONS

Comme vous le savez, les réunions Teams peuvent être enregistrées. C'est d'ailleurs une option que vous pouvez choisir de désactiver grâce à l'option « *Cloud recording* ». Notez que vous pouvez fixer désormais une date d'expiration de l'enregistrement. Passé cette date, l'enregistrement ne sera plus disponible. Pratique !

Voilà pour les réunions mais ce n'est pas encore tout à fait terminé.

La seconde partie concerne les webinaires, ces réunions organisées permettant d'inviter plus de 1000 utilisateurs simultanément et 1000 utilisateurs en plus sans interaction possible (audio et vidéo).



Avant de laisser la possibilité à tous vos utilisateurs d'organiser ces événements, vérifiez l'impact sur la bande passante internet, surtout si vos utilisateurs sont connectés sur les réseaux internes. Notez que le problème est identique avec les événements en direct.

Comme vous le savez, les réunions Teams peuvent être enregistrées.

CONGRÈS & CONFÉRENCES
MERCREDI 23 ET JEUDI 24 MARS 2022
RIVE MONTPARNASSE • PARIS

CAP IT

| BANQUE | ASSURANCE | FINANCE |

SAVE THE DATE

L'ÉVÉNEMENT IT 360 À DESTINATION DE LA BANQUE, L'ASSURANCE ET LA FINANCE

500 donneurs d'ordre attendus
sur deux jours

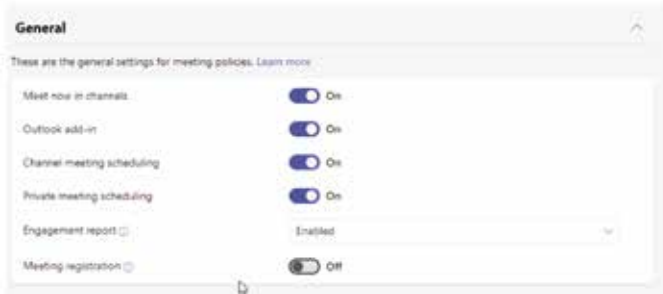
48h de débats et contenu spécialisé à haute
valeur ajoutée

80 speakers experts en conférences et salles
ateliers métier

40 sponsors & partenaires acteurs clés

Réservez votre badge sur www.cap-it.fr

Les webinaires permettent par définition des accès anonymes à vos réunions. Certaines entreprises désactivent donc cette fonctionnalité pour la plupart des utilisateurs qui doivent alors en faire expressément la demande. Pour ce faire, positionnez l'option « Meeting registration » à Off comme le montre la figure suivante, l'option Webinaire disparaîtra des clients Microsoft Teams.



Vous croyez en avoir terminé ?... pas tout à fait il reste encore les événements en directs

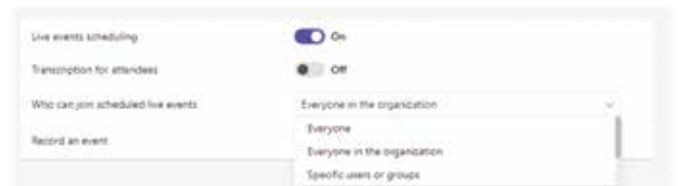
Les webinaires permettent par définition des accès anonymes à vos réunions.

ÉVÈNEMENTS EN DIRECT OU LIVE EVENT

Les événements en direct permettent d'organiser des événements de plusieurs dizaines de milliers de personnes et tout cela avec des personnes non authentifiées (ou pas). Vous voyez où je veux en venir ?

Sachant qu'une personne regardant un événement en direct consomme 1,7 Mbs seconde en download depuis internet, si 300 personnes d'un même site font la même chose en même temps, la consommation de bande passante internet frôlera les 510 Mb/s. Autant vous dire que les Live Event ou événements en direct sont bien souvent désactivés pour la plupart des utilisateurs. D'autant plus que ceux-ci doivent être organisés et animés par des personnes expérimentées.

Là-aussi, soyez prudent car selon la stratégie en place (voir ci-dessous) les événements en direct vont permettre (ou pas) la connexion de personnes anonymes. Quiconque possédant le lien de l'évènement en direct pourra y assister



Voilà, vous ne savez pas tout sur les réunions mais vous devriez en savoir un peu plus sur les bonnes options à positionner.

En attendant, je vous souhaite d'excellents meetings sur Teams !

Laurent TERUIN / <http://Workingtogether.fun>



« SUR ITPRO.FR, NOS EXPERTS VOUS ACCOMPAGNENT AU QUOTIDIEN POUR VOUS AIDER À TIRER LE MEILLEUR PROFIT DE VOS ENVIRONNEMENTS IT... »

Sur iPro.fr, 7 chaînes d'informations et de formations des meilleurs experts en technologies informatiques d'entreprise, par les éditeurs de la revue SMART DSI.

Un savoir technologique unique, une base de connaissances exclusive pour vous accompagner dans la gestion et l'optimisation de vos environnements IT Professionnels.

Bénéficiez d'une richesse éditoriale incomparable... connectez-vous !

► **iPro.fr**



Suivez-nous sur **Twitter** : @iProFR



Partagez sur **Facebook** : www.iPro.fr

► **iPro.fr** **9 chaînes informatiques**

4,200 Dossiers et Guides exclusifs
7 Flux RSS, Newsletters hebdomadaires
Videos & Webcasts
Fil d'actualités



Des ressources exclusives

Enjeux DSI
Cloud Computing
Collaboration & mobilité
Exchange Server
IBM i



Un Club Abonnés

Des services réservés aux abonnés de la revue, en complément des dossiers publiés dans SMART DSI.

La bibliothèque éditoriale du site iPro.fr est constituée de plus de 4200 dossiers technologiques signés par les meilleurs experts francophone et internationaux sur les thèmes de la définition, de la gestion et de l'optimisation des environnements IT basés sur les principales technologies informatiques d'entreprise en terme d'infrastructure serveurs, réseaux, plate forme de collaboration, mobilité d'entreprise et de virtualisation.

AIDER LES ENTREPRISES À ANTICIPER ET GÉRER LES VIOLATIONS DE DONNÉES : L'OBJECTIF DES LIGNES DIRECTRICES PUBLIÉES PAR LE CEPD

Le 3 février 2022, le Comité Européen de la Protection des Données (CEPD) a publié des lignes directrices destinées à aider les responsables de traitement à répondre à leurs obligations et à déployer les réactions adaptées en fonction de chaque situation. Simon de Charentenay, CEO de MonJuridique.Infogreffe nous livre son expertise sur le sujet.



Aider les organismes à traiter les violations de données et à identifier les facteurs à prendre en compte lors de l'évaluation des risques, tel est l'objectif des lignes directrices qui viennent d'être publiées par le Comité européen de la protection des données (CEPD).

En effet, si des lignes directrices avaient déjà été publiées fin 2017 (G29 WP250 rev.1, 6 February 2018, Guidelines on Personal data breach notification under Regulation 2016/679 - endorsed by the EDPB), le besoin s'est fait sentir de disposer d'informations davantage orientées vers la pratique et basées réellement sur des cas concrets. C'est donc l'objectif de ces lignes directrices. En tout et de manière didactique, dix-huit cas pratiques ont ainsi été recensés.



SIMON DE CHARENTENAY

Comment résumer ces 18 cas ?

Savoir s'il faut ou non notifier une violation à la CNIL laisse parfois perplexes les entreprises. Pas toujours simple, en effet, de déterminer quels sont les bons critères pour évaluer les violations de sécurité et les risques auxquels ils exposent une société.

Pour le Comité européen de la protection des données, les entreprises peuvent concrètement se retrouver face à six types de risques :

- **rançongiciel** (sans exfiltration de données et avec sauvegarde ; sans sauvegarde ; dans un hôpital ; avec exfiltration et sans sauvegarde)
- **exfiltration de données** (exfiltration de données de candidature à des offres d'emploi ; exfiltration de mots de passe hachés ; bourrage d'identifiants sur un site bancaire)
- **action d'un salarié, volontaire ou non** (sortie de données de l'entreprise par un employé ; transmission accidentelle à un tiers)
- **perte/vol d'appareils/documents papier** (matériel volé stockant des données personnelles chiffrées ; matériel volé stockant des données personnelles non chiffrées ; documents papier volés contenant des données sensibles)
- **Erreur d'envoi** (erreur d'envoi postal de factures d'achat en ligne ; données personnelles hautement confidentielle envoyées par courriel par erreur ; données personnelles envoyées par courriel par erreur ; erreur d'envoi postal de documents d'assurance)
- **ingénierie sociale** (vol d'identité ; exfiltration de courriels)

Les entreprises peuvent concrètement se retrouver face à six types de risques.

Quels changements concrets vont-ils permettre ?

Ces lignes directrices présentent de manière pédagogique les principales hypothèses rencontrées en pratique. Bien que les cas présentés soient fictifs, ils sont basés sur l'expérience collective des autorités de régulation en matière de notification des violations de données.

Les violations de données sont des problèmes en soi, mais elles peuvent aussi être les symptômes d'un régime de sécurité des données vulnérable, voire obsolète, et indiquer des faiblesses du système auxquelles il faut remédier.

Elles ont donc d'abord vocation « à servir de point de contrôle des processus internes afin de se prémunir contre des attaques mais aussi à servir d'illustration pour modéliser des simulations afin de mieux préparer les salariés à adopter les bonnes attitudes ». En outre, dans une perspective plus curative, elles ont pour objectif d'aider les entreprises à mieux réagir si une attaque se produit.

D'autant qu'il n'est pas toujours simple de déterminer précisément à quel moment le responsable de traitement doit notifier l'autorité de contrôle. Parfois, le responsable du traitement est en mesure d'identifier que l'incident est susceptible d'entraîner un risque et qu'il doit donc être notifié. Mais dans d'autres cas, la notification n'a pas besoin d'être reportée jusqu'à ce que le risque et l'impact entourant la violation ont été pleinement évalués. L'évaluation complète des risques peut en effet avoir lieu parallèlement à la notification, et les informations ainsi obtenues peuvent être fournies à la CNIL par étapes.

Quels outils juridiques pourraient mieux protéger les entreprises face à la violation de données ?

C'est presque une lapalissade, mais la première des règles de sécurité, c'est de stocker les données des entreprises sur un cloud certifié sans intrusion possible, répondant aux normes AFNOR NF Z42-013 ET NF Z42-020. Pour autant, c'est encore loin d'être pratique courante dans toutes les entreprises françaises.

En plus d'offrir la possibilité de paramétrer les accès par profil de poste ou fonction, ce type de cloud offre pourtant en pratique une sécurité accrue et une confidentialité optimale des documents (statutaires, bancaires, registres sociaux, contrats, convocation aux assemblées générales, etc.), dans des formats évitant toute altération.

> Par Sabine Terrey

Comment résister AU RAZ-DE-MARÉE DE LA CYBERCRIMINALITÉ EN 2022 ?

L'impact et la visibilité des cyberattaques augmentent d'année en année, et 2021 n'a pas fait exception à la règle.

Pierre-Yves Popihn, Director Security Consulting, Infrastructure, Cloud & OT EU Practices pour NTT Ltd livre ses recommandations aux entreprises pour lutter face à la vague de cybercrimes qu'elles vont subir en 2022.



Pour la première fois, les cyberattaques ont un impact direct sur le monde physique à l'image de celle qui a touché l'oléoduc Colonial Pipeline, et qui eut pour conséquence directe des pénuries d'essence et des empoignades dans les stations-service. De plus, les ransomwares, cyber ennemi public n°1, ont connu une évolution considérable avec la création de deux types de ransomwares : ceux à double extorsion et ceux disponibles sous forme de service (RaaS). Malheureusement, il faut s'attendre à voir ce phénomène continuer à se développer et à évoluer en 2022.

La tâche pour lutter contre cette cybercriminalité croissante peut sembler colossale pour les professionnels de la sécurité, en particulier au vu des forces qui se liguent contre eux. Cependant, les entreprises peuvent renforcer certaines mesures de contrôle identifiables pour faciliter la défense contre la montée des menaces en 2022.

Sécuriser les technologies opérationnelles

Face à la montée des attaques contre les infrastructures critiques, il est nécessaire de prêter attention à la sécurité des technologies opérationnelles (OT). La sécurité des technologies opérationnelles fait de plus en plus partie de la stratégie cyber des entreprises, puisqu'elles élargissent progressivement leurs programmes de sécurité afin d'y intégrer celles-ci. Elles ont compris qu'en raison de la nature des systèmes en jeu, ces dernières ne peuvent pas se contenter de leur appliquer les outils et concepts classiques de sécurité informatique. En effet, en effectuant un scan de port réseau avec leurs techniques habituelles, elles risquent de paralyser des machines. Heureusement, les entreprises s'équipent en nombre et en qualité d'outils dédiés à la sécurité des équipements OT et IoT (Internet des objets).

A luxurious room with deep red floral wallpaper and gold trim. On the wall are taxidermy mounts of a rhinoceros, a gazelle, a zebra, a tiger, and a bear. In the center, a man's head is mounted on a plaque, holding a camera. A leopard is on a leopard-print sofa, and a lioness sits on the left. A fireplace is in the background.

ARRÊTONS LA CHASSE AUX JOURNALISTES

En 10 ans, plus de 900 journalistes ont été tués dans le monde.

FAITES UN DON SUR [RSF.ORG](https://www.rsf.org)

RSF REPORTERS
SANS FRONTIÈRES

Sécuriser les applications

Les incidents Kaseya et Solarwinds sont venus rappeler au marché la nécessité de renforcer la sécurité des applications. Des bugs dans le code se transforment en vulnérabilités risquant d'être exploitées par des pirates.

En investissant dans un programme DevSecOps, les entreprises peuvent aider à prévenir la prochaine attaque Solarwinds.

Le cadre DevSecOps (développement, sécurité, opérations) permet ainsi d'intégrer la sécurité dans le cycle de développement de produits. En incorporant des outils de sécurisation des applications dans le processus de développement, les équipes de développeurs peuvent repérer plus rapidement les failles dans leur code et les corriger avant sa livraison aux clients. Il est également essentiel de procéder régulièrement à un contrôle des applications, à la recherche de nouvelles vulnérabilités. En investissant dans un programme DevSecOps, les entreprises peuvent aider à prévenir la prochaine attaque Solarwinds.

Pouvoir compter sur des sauvegardes

Bien entendu, toutes les suggestions précédentes ne rendront pas le réseau invulnérable, c'est pourquoi il est indispensable de réfléchir également au moyen de récupérer ses données critiques en cas d'attaque.

La mise en place d'une infrastructure robuste de sauvegarde réduira considérablement la durée de l'interruption d'activité après une attaque. Même si une entreprise choisit de payer une rançon pour obtenir le déverrouillage d'un système frappé par un ransomware, tous les auteurs d'attaques ne redonnent pas systématiquement l'accès à leurs données. De plus, les entreprises ne peuvent jamais avoir la certitude qu'un malware ne reste pas tapi dans leur système, attendant de récidiver (la plupart des entreprises ayant cédé au chantage subissent une nouvelle attaque). Avoir un plan de reprise après sinistre qui prévoit la restauration des données à partir de sauvegardes fiables est donc nécessaire.

Isoler le premier système infecté

Il s'agit de l'étape suivante dans l'évolution de la sécurité. Les entreprises peuvent faire progresser les concepts d'auto-isolément de l'EDR (Endpoint Detection & Response) et étendre ainsi leurs capacités de détection pour y inclure des outils de sécurité tels que des firewalls, des passerelles web et les technologies associées.

Avoir un plan de reprise après sinistre qui prévoit la restauration des données à partir de sauvegardes fiables est donc nécessaire.





« Sur itPro.fr, nos experts vous accompagnent au quotidien pour vous aider à tirer le meilleur profit de vos environnements IT ... »

En ligne sur itPro.fr, 9 chaînes d'information et de formation des experts en technologies informatiques d'entreprise, par les éditeurs de la revue SMART DSI.

Une bibliothèque de ressources éditoriales exclusive pour vous accompagner dans la gestion et l'optimisation de vos environnements IT Professionnels.

- Chaînes thématiques
- + 2800 Dossiers IT
- Guides exclusifs
- 7 Flux RSS
- Newsletters hebdos
- Videos & Webcasts
- Cloud
- Data
- Mobilité
- Sécurité
- IoT
- Enjeux IT
- Tech
- Boîtes à Outils
- Trucs & Astuces
- Hub éditoriaux
- Hors-Série
- Livres blancs...

Bénéficiez d'une richesse éditoriale incomparable ... [connectez-vous !](#)

Suivez-nous sur [Twitter](https://twitter.com/itprofr) : [www.twitter.com/itprofr](https://twitter.com/itprofr) 

Partagez sur [Facebook](https://www.facebook.com/www.itpro.fr) : www.facebook.com/www.itpro.fr 

 **itPro.fr**

La bibliothèque éditoriale du site itPro.fr est constituée de plus de 2800 dossiers technologiques signés par les meilleurs experts francophones et internationaux sur les thèmes de la définition, de la gestion et de l'optimisation des environnements IT Professionnels.

L'extension de ces fonctions peut constituer un moyen d'améliorer considérablement les temps de réponse et de réduire la capacité des malwares à se propager sur leur réseau. Alors que les attaques sont de plus en plus médiatisées, les entreprises prennent conscience que le coût d'un faux positif est nettement inférieur à celui d'une attaque, et elles sont de plus en plus disposées à faire appel à des technologies d'isolement actif et défensives.

Prenons l'exemple de Colonial Pipeline : la compagnie a isolé son environnement informatique de son environnement opérationnel afin de prévenir la propagation du ransomware. XDR permet de porter cette défense à un niveau encore plus précis. Plutôt que d'isoler un réseau entier, pourquoi ne pas isoler le premier système infecté afin d'empêcher la contamination des autres ?

Faire de la sensibilisation

Une fois, un collègue a demandé à un client : « Combien de collaborateurs compte votre entreprise ? » Réponse : « 22 531. » Puis il a demandé : « Et votre équipe de sécurité ? » Réponse « 22 531. » Cette anecdote illustre parfaitement l'importance de la sensibilisation à la sécurité. Lorsque les entreprises remontent au vecteur initial de la plupart des attaques, c'est généralement « quelqu'un qui a cliqué sur quelque chose qu'il ne fallait pas. » Les entreprises dotées d'un programme actif de sensibilisation à la sécurité peuvent considérablement réduire leur surface d'attaque. Cela peut être aussi simple que des quiz réguliers concernant le phishing, ou des webinaires mensuels de formation organisés par l'équipe de



PIERRE-YVES POPIHN

sécurité. Tout ce qui amène les collaborateurs à se poser des questions telles que « Dois-je ouvrir cette pièce jointe ? » ou « Dois-je cliquer sur ce lien ? » renforcera la sécurité des entreprises par rapport à la situation antérieure au lancement du programme. Nul besoin d'apprendre à chacun à devenir un expert en sécurité, mais simplement à accomplir son travail en toute sécurité.

Les entreprises doivent ainsi prêter une attention étroite à l'évolution du paysage des menaces. Un examen des tendances historiques dans ce domaine pour ensuite les comparer avec les défenses mises en place peut les aider à se préparer pour les prochains grands dangers qui se profilent à l'horizon.

> Par Pierre-Yves Popihn



Sur iTPro.fr, 9 chaînes d'informations et de formations des meilleurs experts en technologies informatiques d'entreprise, par les éditeurs du mensuel IT Pro Magazine.

Bénéficiez d'une richesse éditoriale incomparable...
connectez-vous !





La culture data en 2022 au sein des organisations

Des enjeux « data » de demain jusqu'aux équipes data, en passant par l'engagement des collaborateurs et le Chief Data Officer, les interrogations sont nombreuses. Des éléments de réponse sont évoqués au sein de l'Observatoire 2021 de la Maturité Data des entreprises de Datasulting.

Parmi plus de 500 TPE, PME et ETI, 14% ont mis en place des actions de sensibilisation valorisant l'usage des données pour les métiers.

L'Observatoire 2021 de la Maturité Data des entreprises

Dans une étude inédite, l'Observatoire 2021 de la Maturité Data des entreprises en Île de France, Auvergne-Rhône-Alpes et Occitanie, Datasulting livre des résultats autour de 5 axes : potentiel data, stratégie data, gouvernance, compétence et culture data.

Selon Gael Philippe, Président et co-fondateur du cabinet, il faut « démystifier l'usage des données en entreprise, identifier les freins et le niveau de culture data ». 53% ont un niveau très faible niveau de connaissance des possibilités offertes par l'exploitation des données.

Big Data - Intelligence Artificielle - Décisionnel

Le sujet de la data à savoir Big Data, Intelligence Artificielle, BI / Décisionnel... est connu par seulement 43%. Ainsi :

7% ont intégré la data dans toutes leurs réflexions et structuré la culture data en interne

14% ont mis en place des actions de sensibilisation valorisant l'usage des données pour leurs métiers

14% ont formé leurs collaborateurs autour des usages et/ou des outils en lien avec les données.

Les collaborateurs ont un niveau faible de sensibilisation aux sujets data – 61%.

Acculturation à la data

La culture data des collaborateurs, enjeu majeur dans la course à la valorisation des données de l'entreprise, doit passer par l'implication du management et de la gouvernance d'entreprise pour

- instaurer un climat de confiance
- sensibiliser les collaborateurs
- obtenir l'alignement des valeurs

Un travail d'acculturation à la data doit être mené à deux niveaux

- 1^{er} niveau - *Décideurs*

Les décideurs définissent la stratégie de l'entreprise et impulsent la démarche data.

- 2^{ème} niveau - *Collaborateurs*

Les collaborateurs doivent s'engager dans les projets data, afin que l'entreprise ne se retrouve pas face à des résistances, mauvais usages des outils, problèmes de qualité des données.

Attention donc au déficit de culture data qui peut impacter les décisions initiales (technologie, choix de partenaires, dimension du projet, budget...) et la mise en œuvre des projets, ou ralentir la performance des actions.

Source Datasulting, cabinet de conseil spécialisé dans la valorisation des données

Innovation SIRH : QUELS CHANGEMENTS LA CRISE SANITAIRE A-T-ELLE PU FAIRE ÉMERGER ?

Quand on parle d'innovation, on pense souvent à « révolution ». Une nouvelle organisation, un nouvel outil, une nouvelle technologie, qui va complètement réinventer l'approche d'un sujet et qui implique une amélioration fondamentale des performances. Force est de constater que les évolutions des technologies dans l'industrie et les sciences sont plus souvent issues d'une innovation incrémentale que de rupture. François Bouchery, Directeur Conseil & Delivery Digital Experience chez Umanis partage son expertise.



Souvent les Directeurs IT, Directeurs Digitaux, les DRH et autres fonctions métier, sollicitent les experts et consultants avec cette question : quelles sont les solutions et technologies innovantes ? Pour y répondre, les experts et consultants conseil ont indirectement cette pression de devoir mettre en avant la nouvelle innovation de rupture que personne ne connaît, seul moyen de se démarquer des confrères qui eux aussi essaient de démontrer toute leur expertise et valeur ajoutée.

Les innovations incrémentales majeures

Les directions des ressources humaines ont vécu 2 années intenses et passionnantes. Les contraintes administratives et opérationnelles multiples, ont amené les entreprises à trouver de nouvelles organisations, accélérer la mise en place d'outils digitaux, mais aussi à aider les organisations auxquelles elles appartiennent à gagner en maturité sur l'organisation du travail. Les experts s'accordent à dire d'ailleurs que nous avons gagné 10 années en maturité digitale.

*« COMPRENDRE LES ENJEUX, ÉVALUER
LES PERSPECTIVES ET CONDUIRE
LA TRANSFORMATION NUMÉRIQUE
DE L'ENTREPRISE »*



SMARTDSI

www.smart-dsi.fr

« Analyses, dossiers, chroniques pour conduire la transformation numérique de l'entreprise »



FRANÇOIS BOUCHERY

Quels sont donc les outils et technologies qui vont permettre aux DRH de continuer à améliorer les services rendus aux collaborateurs, managers, sous-traitants, partenaires et candidats en recrutement ?

• L'Intelligence Artificielle

Le mot clef est dit ! Les fonctions RH peuvent bénéficier de la capacité d'analyse de gros volumes de données afin d'améliorer des sujets tels que la gestion des référentiels de compétences et d'emploi, la recommandation personnalisée de parcours de carrière et de formation par exemple. Ces sujets gagnent en maturité, et de plus en plus d'éditeurs proposent des fonctionnalités basées sur l'analyse de gros volumes de données. On développe ici le self-service et on améliore les outils à disposition des fonctions RH travaillant sur la GPEC et le parcours collaborateur.

• L'utilisation de la data

On observe de plus en plus de maturité dans l'utilisation des données RH. Rien de nouveau ici, mais encore une fois on constate un gain de maturité des outils packagés presque prêts à l'emploi. Cela permet de réduire les coûts et d'accélérer la mise en œuvre des projets. Pour exemple, la mise en place des applications de Bilan Social ou de Bilan Social Individuel s'effectue en moins d'un mois, ce qui n'est pas négligeable dans une période de remise en question de choix de vie par les collaborateurs. Grâce à ces outils self-service, les RH rendent leurs collaborateurs acteurs de leur évolution professionnelle.

On observe de plus en plus de maturité dans l'utilisation des données RH.

• Les réseaux sociaux

Pour le recrutement, pour la marque employeur, de nouveaux acteurs proposent de cibler des individus sur la base de leurs centres d'intérêts, de leurs réactions à des publications des entreprises. Ce nouveau levier de recrutement dans un contexte extrêmement concurrentiel s'applique à tous les métiers.

• Les outils collaboratifs

Tout le monde a eu l'occasion de tester voire de benchmarker Zoom, Google Meet, Teams ces derniers mois. Si ces outils permettent d'accélérer et de faciliter la collaboration des équipes, ils représentent un véritable enjeu pour les DSI ET pour les DRH. Ces outils permettent la localisation des données personnelles, la sécurisation du SI, le maintien d'une politique d'entreprise et de ses valeurs et enfin le management du changement. Ils permettent également d'accompagner les collaborateurs et les managers dans la nouvelle organisation du travail. Sans oublier les outils de formation, webinaire, conférence qui prennent encore plus d'importance pour favoriser cette évolution.

Actuellement l'agilité est une démarche omniprésente dans les entreprises.

• Les méthodes de travail

Actuellement l'agilité est une démarche omniprésente dans les entreprises. Les DRH, notamment, en ont fait preuve ces derniers mois ! Pour aller au bout de la démarche ils ont dû appréhender le concept d'agilité, se familiariser aux méthodes et aux outils proposés. En raison de la multitude de méthodes et organisations agiles, les DRH doivent trouver celles qui correspondent à l'entreprise, sachant qu'elles peuvent être différentes selon les projets ou les entités. En définitive les équipes improvisent souvent leur organisation agile alors qu'un simple coaching de quelques semaines ou mois leur permettrait de gagner en efficacité et en maîtrise.

2022 sera probablement l'année au cours de laquelle les DRH pourront normaliser l'utilisation de ses nouveaux outils, s'appuyer sur le retour d'expérience pour industrialiser leurs processus, valider certaines expérimentations ou au contraire mettre de côté des outils ou méthodes qui ne leur correspondent plus.



Promodag

Promodag Reports pour

Office 365



Promodag Reports est un outil puissant conçu pour l'analyse, le contrôle et le reporting complet des systèmes de messageries Microsoft Office 365 & Microsoft Exchange

Mise en conformité
avec les règles de l'entreprise

Planification simplifiée
des processus de gestion

Interopérabilité
avec les Systèmes RH

Optimisation
des performances
de la messagerie

Audit & planification
de l'utilisation des e-mails

Rapports d'analyse
de trafic, suivi des messages

Droit à la déconnexion
et RGPD

“ **OPTIMISEZ VOS USAGES COLLABORATIFS & RÉGLEMENTAIRES À L'HEURE DE LA DIGITAL WORKPLACE GÉNÉRALISÉE** ”

Rendez-vous sur www.promodag.fr pour télécharger gratuitement une version entièrement fonctionnelle ou contactez nous pour bénéficier d'une démonstration complète avec l'un de nos experts.

Libérez-vous de la gestion de votre cybersécurité et de vos environnements cloud !



Centre Opérationnel de Cybersécurité

Optez pour un dispositif organisationnel et technique afin d'assurer la supervision de la sécurité informatique de votre entreprise et de garantir une intervention rapide en cas d'incident ou d'attaque.



Services Managés Cloud

Externalisez vos services d'infrastructure, d'infogérance et de support. Bénéficiez d'une écoute 24/7/365 et d'une garantie de transparence sur les prestations tout en maîtrisant votre budget.

— Faites appel à nos experts —
contact@metsys.fr