

SMART DSI[®]

DOSSIER

L'agilité dans un monde où l'on veut tout contrôler

INTERVIEW

Adopter la Feedback Intelligence est vital

L'ŒIL SECURITE

Cyberattaques en hausse
- Investissements en baisse

L'ETUDE A RETENIR

Les 3 défis du Cloud hybride

ANALYSE

Le recours à l'IA et aux robots dans l'industrie : opportunité ou menace?

STRATEGIE

5 choses que les DSI devraient faire en 2023

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

SAMSUNG | econocom



Galaxy Book2 Series

**La légèreté et la puissance
au service de la mobilité**



Plus proche de ce que vous aimez.



Les couleurs peuvent varier selon les pays.

Des PC portables conçus pour vous suivre partout

Galaxy Book2 Series



13,3" | 11,2 mm | 0,87 kg

Avec un design ultra mobile et robuste, le Galaxy Book2 Pro et le Galaxy Book2 Business ont été conçus pour vous suivre partout dans vos déplacements.



Une très grande autonomie

Déplacez-vous sans inquiétude avec la batterie longue durée du Galaxy Book2 Pro.

Avec une autonomie pouvant aller jusqu'à 21 heures en lecture vidéo, le Galaxy Book2 Pro vous offre une mobilité ultime sans se soucier de la batterie.



Galaxy Book2 Pro

- 13,3" FHD Amoled
- Intel Core i5 12^e génération
- 8 Go RAM
- 256 Go SSD

Existe également en 15,6"



Galaxy Book2 Business

- 14" FHD LCD
- Intel Core i5 12^e génération
- 8 Go RAM
- 256 Go SSD
- Sécurisé par Knox Security

Vous voulez en savoir plus ? Complétez ce formulaire pour que notre équipe commerciale Econocom puisse répondre à votre demande en [cliquant ici](#) ou en scannant ce QR Code.



L'écosystème Samsung

Tout votre téléphone désormais sur votre PC

Transférez vos applications mobiles sur votre Galaxy Book2. L'application Mobile Connecté a été optimisée pour les utilisateurs de l'écosystème Galaxy avec Lien vers Windows³. Elle offre une expérience inter-appareils parfaitement fluide pour plus de productivité. La fonction Applications récentes⁴ vous permet de continuer d'utiliser une application ouverte sur votre smartphone, directement sur votre PC.



Doublez votre écran, démultipliez votre productivité



Transformez votre Galaxy Tab S en deuxième écran. Comme pour tout moniteur externe, vous pouvez dupliquer, étendre et travailler simultanément

Un écosystème riche et sécurisé

La fonctionnalité Quick Share¹ est un moyen pratique d'envoyer des fichiers en sans fil entre les appareils Samsung Galaxy. Dans la continuité, Private Share² offre une protection plus poussée en chiffrant les fichiers à l'aide de la technologie blockchain.



DAS Galaxy Book2 Pro 13" : Tronc : 0.406 W/Kg ; Membres : 0.406 W/Kg
DAS Galaxy Book2 Business : Tronc : 0.268 W/Kg ; Membre : 0.268 W/Kg

¹Disponible sur les appareils Galaxy avec One UI 2.1 ou une version ultérieure installée. La fonctionnalité Quick Share nécessite que le Bluetooth Low Energy et le Wi-Fi soit activé sur les deux appareils durant le partage.

²Private Share ne peut être pris en charge que sur les téléphones mobiles Galaxy dotés du système d'exploitation Android P ou supérieur. Le type, le nombre, la capacité et la date d'expiration des fichiers transférables ainsi que le nombre de partages de fichiers simultanés dans Private Share peuvent être limités.

³Link to Windows (Lien avec Windows) est pris en charge sur les modèles des séries S, Z et N dotés de la version One UI 3.1.1 ou ultérieure et les PC Windows 10 20H1 (2004) ou ultérieur. Les caractéristiques et la disponibilité de l'application peuvent varier selon les pays. Certaines fonctionnalités peuvent nécessiter que le smartphone et la tablette soient connectés au même réseau Wi-Fi. Windows, le logo Windows, Votre Téléphone, Office, Excel, Word et PowerPoint sont des marques déposées de Microsoft, Inc. ou de ses filiales.

⁴Applications récentes est uniquement disponible pour les appareils Samsung Galaxy avec One UI 3.1.1 ou ultérieur (Samsung Galaxy S, Note, Z Fold, Z Flip) avec les versions des application suivantes minimales : Your Phone (1.21092.145.0), Your Phone Companion (1.21083.49.0), Link to Windows (2.3 ou version ultérieure). Recent Apps est disponible à partir du 14 février 2022. La disponibilité des fonctionnalités peut varier selon les applications.



Une année 2023 sous haute résilience et innovation !

Face à une année 2022 oscillant entre une forte incertitude économique et géopolitique, et la complexité des environnements technologiques, les entreprises n'ont pas d'autres choix que de mettre en place une approche 2023 audacieuse et teintée de résilience, axe de valeur⁽¹⁾ et impératif stratégique.

Alors comment garder plus précisément une longueur d'avance ? Loin de céder au fatalisme et pour relever le défi des diverses turbulences actuelles, le dynamisme des organisations sera crucial. Elles articuleront la convergence des données et des outils et devront faire preuve d'agilité en se basant sur l'observabilité, accélérateur de la transformation digitale et de l'expérience numérique, mais aussi sur l'automatisation, différentiateur incontestable.

Pas de répit pour la cybersécurité avec une surface d'attaque qui ne cesse de s'élargir ! Une vigilance toute particulière sera portée, entre autres, sur l'arrivée de la nouvelle génération de ransomware, les risques de menaces dans le Cloud et contre les chaînes d'approvisionnement, le danger d'une cyberattaque de grande ampleur, sans oublier les difficultés d'indemnisations des cyber assurances, et la pénurie continue des talents. Parmi les pistes, la détection des anomalies, la modélisation comportementale, les technologies prédictives et la cryptographie quantique seront des axes à suivre de très près.

Enfin, en 2023, plus que jamais, place aux collaborateurs, ressources et piliers de la créativité et de la valeur ajoutée de l'entreprise. Il sera indispensable de continuer à les informer, les former, les impliquer dans tout projet pour recueillir leur adhésion et identifier leurs attentes. En ce sens, l'innovation s'accélère et devient l'assurance d'un avenir plus inclusif, avec le travail hybride où des expériences équitables amélioreront le bien-être, et avec une Intelligence Artificielle plus responsable et éthique pour réduire les atteintes potentielles et favoriser la réussite. De vastes chantiers pour un futur plus engageant ...

Nous vous souhaitons une très belle année 2023 avec la réalisation de tous vos projets !

Sabine Terrey
Directrice de la Rédaction
sterrey@itpro.fr

(1) Source Splunk – Prévisions 2023 pour les leaders et les technologies émergentes

SMARTDSI

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%

« SMARTDSI 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°28 | DÉCEMBRE 2022

SMART DSI est une 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

L'agilité dans un monde où l'on veut tout contrôler

12 | L'ŒIL SECURITE

Cyberattaques en hausse – investissements en baisse...

16 | PERSPECTIVES 2023

Budgets, conformité et périphérie : les tendances qui vont façonner le marché IT en 2023

18 | INTERVIEW

Supermood : « Adopter la Feedback Intelligence, c'est un besoin vital aujourd'hui »

21 | L'ETUDE A RETENIR

Les 3 défis du Cloud hybride !

22 | STRATEGIE CYBERSECURITE 2023

Tendances cybersécurité 2023 pour l'Europe

25 | L'ETUDE A RETENIR

La cybersécurité perçue par les conseils d'administration

26 | ANALYSE

Le recours à l'IA et aux robots dans l'industrie : opportunité ou menace ?

29 | L'ETUDE A RETENIR

Le rôle clé du Directeur Financier et Administratif dans la transformation digitale

30 | EXPERT

Du Finops à toutes les sauces

35 | BULLETIN D'ABONNEMENT





36 | INTERVIEW

Patrowl élève fortement le niveau de sécurité des systèmes d'information

38 | STRATEGIE

Cinq choses que les DSI devraient faire en 2023

40 | INTERVIEW

A3BC : des solutions d'identité numérique universelle et sécurisée pour tous

44 | L'ŒIL NUMERIQUE

Plongée au cœur de la DevX !

46 | EXPERT

L'ECDN : la solution indispensable pour des live events réussis

50 | L'ETUDE A RETENIR

La valeur stratégique des entreprises déployée grâce à l'IA et les données

SMARTDSI

Rédaction

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

Comité de rédaction associé à cette édition

Thierry Bollet, Didier Danse, Massimo Guarnieri,
Sabine Terrey, Laurent Teruin, Théodore-Michel Vrangos,
Tobias Wölk.

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

IStock - Shutterstock

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

L'agilité DANS UN MONDE OÙ L'ON VEUT TOUT CONTRÔLER

> Par Didier Danse

Le terme agilité est utilisé à tort et à travers. La grande majorité des organisations annoncent être agiles ou tout du moins vouloir l'être, mais la réalité est souvent fort différente. Cela se ressent notamment dans les relations internes et l'absence d'agilité est d'autant plus visible lorsqu'il s'agit de faire appel à des intervenants externes, où il est nécessaire de contractualiser la relation. D'autant que l'organisation faisant appel souhaite généralement être totalement en contrôle sur l'exécution du projet tout en déportant le risque sur le prestataire.



Pourtant agilité et contractualisation ne sont pas antinomiques. Il est tout à fait possible de fonctionner de manière agile avec des intervenants externes, tout en gardant un certain contrôle sur le résultat à atteindre mais aussi sur la manière de l'atteindre. Une telle approche permet d'ailleurs de minimiser les risques et les coûts associés à la réalisation, quelque part entre le projet forfaitaire et la régie, tout en étant bénéfique pour le prestataire. Une approche gagnant-gagnant est en effet possible, la clé est de placer la création de valeur et la collaboration active au centre de l'équation.

Le forfait ou la régie, les approches les plus courantes

De manière classique, on retrouve deux types de relations. Lorsque le périmètre est identifié, alors le commanditaire fait généralement appel au forfait, à savoir le paiement d'une somme définie pour un périmètre explicite et immuable. Il arrive régulièrement que cette approche soit choisie alors que le périmètre s'avère très large, augmentant fortement le risque pour le prestataire. Pour les autres situations, la mise à disposition de ressources en régie, c'est-à-dire en fonction du temps passé et des moyens mis en œuvre, est choisie. Dans ce cas, c'est le client qui supporte le risque dans sa globalité.

La régie est souvent perçue comme étant plus adaptée face à l'inconnu. Le forfait est plus adapté à des situations fortement maîtrisées.

Un petit rappel sur l'agilité

L'agilité est bien plus large que la régie. Il est dès lors important de rappeler ce qu'est l'agilité : c'est s'adapter rapidement face à des événements, tant à la suite de difficultés que pour répondre à de nouveaux besoins et opportunités. Pour y arriver, il est nécessaire de respecter 4 principes : des interactions, un produit fonctionnel, de la collaboration, et de la réactivité.

Les méthodes agiles permettent de respecter les principes d'agilité en définissant des cycles de création de valeur courts, ou inversement selon le point de vue. En effet, le tout forme un ensemble où les causes et les conséquences ne font qu'un. On retiendra l'aspect de cycle de vie itératif, incrémental et adaptatif basé sur du pragmatisme et de la réactivité pour tenir compte de besoins en évolution. L'agilité, c'est donc la capacité à accompagner la maturation des besoins et intégrer des changements de périmètre à tout moment. Intégrer la maturité projet dans la démarche permet de favoriser la capacité d'exécution et de maximiser la valeur produite en utilisant le produit au plus tôt.

Pour y parvenir, il existe de nombreux cadres de développement : *Scrum*, *Extreme Programming*, *Development Lean*, et de nombreux autres bien moins connus. Des méthodes issues du développement ou des approches spécifiques s'appliquent également à des projets d'infrastructure.

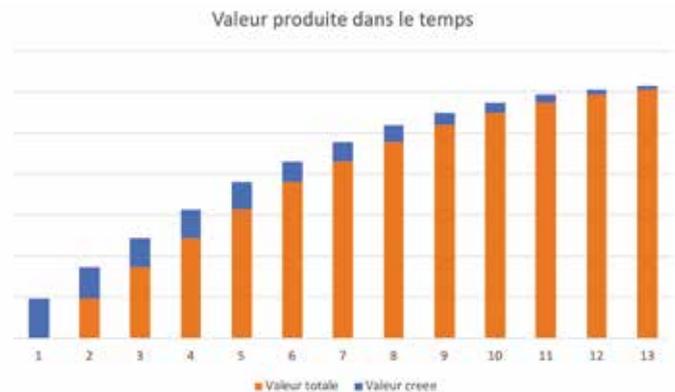
Avec un tel cadre de travail, il est possible de définir un contrat hybride, il est possible pour le demandeur de garder le contrôle, en s'assurant de la bonne collaboration et de l'engagement de l'ensemble des intervenants tout en créant de la valeur de manière régulière, permettant de s'arrêter à tout instant tout en profitant de la valeur créée jusque-là. Nous verrons un peu plus tard que le prestataire partage le bénéfice issu de cette méthode de travail avec le commanditaire, notamment dans la réalisation au quotidien mais aussi financièrement.

Ainsi, l'engagement porte sur la méthode et non sur un résultat.

Comment réussir en étant agile ?

Tout d'abord, il s'agit d'avoir la vision produit et un *backlog*, c'est-à-dire une liste ordonnancée, de fonctionnalités à implémenter. Cette liste se doit d'être organisée en tenant compte tant de la valeur attendue de la réalisation, que de l'effort à produire pour obtenir cette valeur. Cette liste de fonctionnalités peut être modifiée à tout moment ou presque.

L'ordre est généralement orienté de sorte à avoir les fonctionnalités nécessaires en premier avant de mettre en place les fonctionnalités donnant un avantage compétitif pour finalement terminer avec les fonctionnalités considérées comme non nécessaires mais apportant un plus aux utilisateurs. De ce fait, la valeur ajoutée diminue généralement itération après itération :



La valeur à chaque itération diminue tandis que l'effort fourni durant une itération donnée est censé rester stable. Ainsi à un moment, par exemple après l'itération 8, il peut être nécessaire de s'arrêter, avant que l'effort à fournir pour créer de la valeur n'augmente de trop.

Concrètement, la valeur créée est estimée par le commanditaire tandis que l'effort sera convenu de manière concertée entre le demandeur et les personnes en charge de l'implémentation, du déploiement et de la maintenance de la fonctionnalité. L'effort se mesure en *Story point*, qui s'avère propre à chaque équipe. La lecture du guide *Scrum*¹ devrait donner quelques pistes intéressantes, que vous ayez de l'expérience ou non avec *Scrum* ou les autres méthodes agiles.

Dans ce contexte, on notera que l'on vise à ne mettre en place qu'un et un seul contrat régissant la relation. Attention donc aux contrats faussement agiles avec des accords signés sur le périmètre de chaque itération, ce qui en fait une série de contrats au forfait et non une approche forfaitaire agile.

Comment mettre en place de l'agilité en quelques étapes

Le périmètre n'étant plus fixe, le forfait est-il possible ? Presque. Le contrat agile porte sur un budget sous contrôle et pour lequel le risque financier n'est pas inexistant mais s'avère minimisé tandis que le périmètre sera réévalué régulièrement.

Ainsi, l'engagement porte sur la méthode et non sur un résultat bien que la notion de création de valeur soit l'élément clé de ce type de contrat. Pour y parvenir, il s'agit de mettre en place un travail commun avec le client avec revue régulière.

Par l'approche coopérative, il est nécessaire de construire la relation au travers de plusieurs phases :

1. **Lancement** : élaboration d'un Plan Qualité de Service, c'est-à-dire des indicateurs qui seront suivis tout au long de la relation
2. **Mise en place de la collaboration** : durant quelques sprints, ajustement de la vision, du backlog, mais aussi estimation de l'effort d'implémentation des fonctionnalités du haut de la liste. On notera que malgré qu'on soit en phase de mise en place, il est d'ores et déjà attendu d'avoir des livrables à chaque itération
3. **Implémentation** : les itérations continuent, en utilisant les bases mises en place à l'étape 2, notamment autour de l'estimation de l'effort à produire
4. **Clôture** : formation des intervenants et transfert de connaissance.

Dans certaines situations, il peut être intéressant de contractualiser après la 2^{ème} étape, ou tout du moins de laisser de la marge dans le temps pour l'estimation.

Ce qui doit être livré à chaque livraison

Pour les adeptes de Scrum, pas ou peu de surprises dans ce paragraphe. Il reste cependant intéressant d'énumérer ce qui est attendu après chaque itération. Chacun des éléments permet la couverture d'un des points importants à tenir compte lors de toute implémentation :

- **Le besoin couvert** : les exigences sous forme de *user stories*,
- **La réponse au besoin** : le code, dans sa version actuelle,
- **La qualité** : l'ensemble des tests portant sur le code ou les fonctionnalités et les rapports d'exécution de ceux-ci,
- **Le déploiement** : les scripts de compilation et de déploiement,

L'idéal est que cette documentation ne soit pas « externe » au package mais totalement intégrée dans le processus de livraison et accessible via les outils en place. Malheureusement, il s'avère que les clients sont souvent peu outillés pour cela et que les fournisseurs ne peuvent éternellement donner accès aux clients. Dans ce cas, il reste nécessaire de faire des livraisons incluant de l'information sous forme de documents.

La gouvernance autour des projets agiles

Quelle que soit la méthode de contractualisation, les projets agiles requièrent certains intervenants avec principalement un *product owner* (qui sera donc côté client) et un *scrum master*, bien souvent issus du fournisseur. L'ensemble des intervenants se rencontrent de manière même cyclique et chaque

rencontre a des objectifs particuliers :

- Le *daily standup* permet quotidiennement de faire le point d'avancement et d'échanger en quelques minutes sur les difficultés rencontrées par rapport aux sujets en cours,
- Le *backlog refinement* permet de revoir les éléments du backlog et de s'assurer de leur bonne compréhension,
- Le *sprint planning* durant lequel les éléments du backlog sont évalués en termes de points, correspondant à la difficulté de produire la valeur espérée,
- Le *sprint review* dont le but est d'obtenir des retours d'informations sur les nouvelles fonctionnalités,
- Et enfin la *rétrospective* qui s'avère clé dans ce contexte puisqu'il permet à chacun d'exprimer sur la période qui vient de s'achever.

Pour plus d'informations sur ces cérémonies, je vous renvoie vers le Scrum guide dont nous avons parlé précédemment.

Par l'aspect contractuel, il est également nécessaire de mettre en place un comité de pilotage portant sur la vie du projet en tant que tel, durant lequel les indicateurs présentés au paragraphe suivant seront présentés, en autres choses. Plusieurs profils sont importants au travers des cérémonies : le *Product Owner*, le *Scrum Master*. A ceux-ci s'ajoutent des profils qui ne sont pas directement liés à l'opérationnel : le gestionnaire du projet et le directeur de projet ou le sponsor.

Par l'aspect contractuel, il est également nécessaire de mettre en place un comité de pilotage.

Le pilotage par les indicateurs

La croyance populaire voudrait que le succès ne se mesure qu'au travers du succès de l'appli ou non. Bien que ce fondement fasse du sens puisqu'il s'agit de l'objectif final, il est utile de suivre un certain nombre d'indicateurs, tant dans le quantitatif que le qualitatif au travers du temps pour s'assurer que la collaboration est la plus efficace possible.

On regardera ainsi 4 indicateurs quantitatifs, ayant pour objectif de promouvoir la pérennité des fonctionnalités livrées et de donner un aperçu sur le niveau de contrôle du projet. Pour ce qui est du code en tant que tel, on mesurera la qualité technique (la couverture de code, la complexité du code, etc.) mais aussi la qualité fonctionnelle (le nombre d'anomalies et de régressions par exemple).

En plus de la qualité, 2 indicateurs de prédictibilité et de productivité seront présents. Le premier permet d'évaluer la cohérence entre ce qui est livré et ce

qui était planifié, notamment grâce à la vélocité. La productivité est fonction du nombre de points délivrés par rapport à un nombre d'intervenants, de toutes les parties.

Le niveau qualitatif portera généralement sur l'implication et la satisfaction des parties. L'implication se base sur les contributions à tout moment, tant durant les estimations que les rétrospectives, pour ne citer que ces moments. La satisfaction, bien plus classique, permet de valoriser un sentiment de satisfaction.

Ces indicateurs peuvent d'ailleurs servir de base contractuelle afin de favoriser une relation collaborative ou même permettre aux parties de quitter ladite relation.

L'impact sur la responsabilité

L'approche agile et itérative permet de faire en sorte que chaque cycle génère un produit directement utile. Une telle approche basée sur des retours dynamiques et en temps réel s'avère très utile pour le projet. La responsabilité partagée est, dès lors, clé du succès de tel projet.

Avec le niveau collaboration induit lié au changement d'approche, la responsabilité d'un échec ne peut être imputée exclusivement au prestataire. La responsabilité est alors partagée entre les intervenants. La responsabilité en cas de succès l'est également, ce qui s'avère bien plus

intéressant. D'ailleurs le modèle participatif et actif du client dans le projet est alors une opportunité de transformer une gageure en une opportunité.

L'aspect financier

L'aspect financier des projets s'avère plutôt important pour les différents intervenants. Le coût pour l'un correspond aux rentrées pour l'autre et de ce fait il est fréquent de penser à mettre en concurrence des organisations qui doivent pourtant collaborer pour le bien être des projets. La collaboration nécessaire à l'agilité doit permettre à l'ensemble des parties de trouver un terrain d'entente dans un but commun : maximiser le retour sur investissement.

L'approche agile et itérative permet de faire en sorte que chaque cycle génère un produit directement utile.

Pour se faire, nous l'avons vu, le projet peut s'arrêter après chaque itération en tenant compte de la période de préavis. Dans un tel contexte, il s'agit alors de trouver un modèle de facturation tenant compte du second facteur « valeur produite », le premier étant le coût. Différentes approches sont alors possibles pour établir le coût d'une fonctionnalité ou d'un ensemble de fonctionnalités. La facturation peut se

AXEL
définit autrement la technologie
du Client Léger

Prêt gratuit
pour évaluation

www.axel.fr

faire par exemple sur base d'un mix entre taux horaire et nombre de points (ex : 35€/h + 200€/point). On se rappellera que la notion de point est définie dans les premiers sprints, la notion de coût associée est ainsi variable d'un projet à l'autre et d'une équipe à l'autre. C'est pour cela que chaque partie doit pouvoir sortir de la relation si le product backlog n'est pas acceptable par toutes les parties.

L'approche basée sur un taux fixe et un taux variable a plusieurs vertus positives. Le fait de livrer la même qualité en un temps moindre est économiquement plus intéressant que de miser sur la même livraison plus tard, tant pour le prestataire que le client.

Le manifeste précise d'ailleurs que la collaboration est à préférer à la négociation contractuelle.

Enfin, en clôturant le projet plus tôt, le client peut faire le choix d'interrompre les investissements s'il estime que ceux-ci ne produisent plus la valeur suffisante. Pour éviter un impact trop important pour le fournisseur, il souvent prévu de payer une indemnité équivalente à un certain nombre d'itérations calculées sur la partie fixe. Le nombre d'itérations couvertes est bien souvent défini sur base d'un pourcentage du temps qui était initialement planifié. A l'inverse, en cas de dépassement du planning initial, le tarif journalier peut être revu à

la baisse, pouvant même descendre jusqu'à 50% de celui-ci. Dans un tel cas, le calcul n'est pas intéressant ni pour le fournisseur qui verra fondre sa marge sur le projet ni pour le client qui continue à payer pour des fonctionnalités qui étaient initialement prévues pour un moindre coût, c'est ce qui motivera l'ensemble à délivrer le nécessaire et s'arrêter à temps.

En résumé

Selon le manifeste, l'agilité repose sur les individus et leurs interactions, un logiciel fonctionnel, l'adaptation au changement et la collaboration avec les clients. Pour ce dernier, le manifeste précise d'ailleurs que la collaboration est à préférer à la négociation contractuelle.

Pourtant le contrat est nécessaire selon la loi. Ce qu'il faut retenir c'est que la contractualisation doit alors porter sur l'approche, la mesure et les responsabilités de chacun. Une fois ce cadre contractuel en place et en s'assurant de la collaboration, l'agilité peut alors s'exprimer et de la valeur est créée à chaque itération.

1 <https://scrumguides.org/docs/scrumguide/v2020/2020-Scrum-Guide-French.pdf>

> Par Didier Danse - IT Manager | IT Architect | Agilist





Distributeur IT depuis plus de 35 ans,
nous vous accompagnons
dans votre **TRANSFORMATION DIGITALE**

Passionnés d'IT nous mettons l'humain au cœur
de toutes nos activités avec un seul objectif :
devenir l'architecte IT des entreprises



Scannez ce QR code et découvrez
toutes nos solutions sur inmac wstore



BECHTLE

Cyberattaques en hausse – INVESTISSEMENTS EN BAISSÉ...

La nouvelle est tombée durant le premier week-end de décembre : cyberattaque contre l'hôpital André Mignot du Centre Hospitalier de Versailles. Mais cela n'est malheureusement pas un fait rare, d'autres hôpitaux ont subi des attaques de type ransomware, avec vol des données et chantage, mais aussi destruction des postes contaminés et nécessité de les remplacer.



Les investissements en cybersécurité vue par l'ENISA

Le sujet est gravissime, parce qu'il touche le monde de la santé globalement, mais aussi parce qu'il préfigure ce qui peut se passer au niveau d'autres services de santé tel que les centres de radiothérapie, de dialyse, etc. mais aussi d'autres services publics tels que les transports, bref, il fait froid au dos !

Au même moment, l'ENISA (European Union Agency for Cybersecurity) publiait son étude régulière NIS Investments 2022, une excellente étude, gratuite de surcroît, qui synthétise les budgets,

les investissements en cybersécurité en 2021 et présente des axes techniques par secteur d'activité économique d'investissements en cybersécurité. Et le tout au niveau des 27 pays de l'EU.

Ce qui est particulièrement inquiétant pour nous tous citoyens, pas uniquement en tant que professionnels de la cybersécurité, est que le pourcentage moyen de la part des budgets IT alloués à la cybersécurité est de 6,7%, en baisse d'un point par rapport aux chiffres de l'année dernière. Cette diminution est expliquée par un certain atterrissage en 2021 d'investissements en cyber du secteur de la banque et la finance.

Le manque de fonctions stream Cyber Threat Intelligence

Pour revenir à la dernière attaque de l'hôpital André Mignot, tant que les budgets alloués à la sécurité des systèmes d'information seront en moyenne à 6,9% du budget IT pour un établissement de santé en Europe, quand les professionnels de sécurité des SI, estiment qu'il faudrait qu'il soit à minimum 15%, on aura de très graves cyber-incidents dans l'avenir.

Le coût direct d'un incident de sécurité est en moyenne de 200 000 euros.

Car dans ces chiffres, nous retrouvons la totalité des coûts : CAPEX et OPEX, les salaires des personnels, les outils, les maintenances, etc. etc.

L'étude ENISA, qui a porté sur des données de 2021 couvrant 1080 opérateurs de services essentiels ainsi que des providers de services digitaux (marketplace, moteurs de recherches, cloud providers) nous enseigne aussi que le coût direct d'un incident de sécurité est en moyenne de 200 000 euros, le double de l'année précédente en Europe et que les secteurs de la santé et de la banque sont les premiers en termes de coûts subis.

Donc d'un côté les budgets moyens ont baissé de 1% et de l'autre côté les coûts des sinistres ont doublé, sachant que 37% des opérateurs de services sensibles en Europe ne possèdent pas de SOC !

Et dans ce contexte, beaucoup de sociétés ne possèdent pas de fonctions stream CTI (Cyber Threat Intelligence), composante indispensable dans le quotidien des ingénieurs, qui couplée à une organisation de SOC composée de cyber-analystes, permet d'identifier les signaux faibles, de savoir où chercher, suivant des patterns d'attaques, et in fine d'éviter des cyberattaques.

La sensibilisation ...

Dernier élément pour finir de comprendre pourquoi les établissements de santé sont la cible fréquente des attaques : l'étude ENISA indique qu'en 2021 seulement 27% des établissements de santé surveillés possédaient un programme de protection contre les rançongiciels et la majorité n'avait pas d'outils ou de programme de sensibilisation des personnels non-informaticiens.

Le chemin est long mais aussi vital, comme leur mission, pour les hôpitaux et autres opérateurs de services sensibles de s'équiper et d'opérer ces services de cyber protection.

Beaucoup de sociétés ne possèdent pas de fonctions stream CTI (Cyber Threat Intelligence).

> Par Théodore-Michel Vrangos, cofondateur de I-TRACING Group



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

Sur iPro.fr, 9 chaînes d'informations et de formations des meilleurs experts en technologies informatiques d'entreprise, par les éditeurs du trimestriel SMART DSI.

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

▶ **iPro.fr**

Codéops permet d'automatiser, de faciliter et de sécuriser vos déploiements et la gestion de vos applications sur le cloud de confiance Outscale tout en confiant le monitoring de votre infrastructure aux experts systèmes Codéin.

**PERSONNALISATION**

Vous bénéficiez d'un build sur mesure qui s'appuie sur vos propres procédures.

**FLEXIBILITÉ & SIMPLICITÉ**

Testez, déployez, scalez en un clic ! De plus, Codéops supporte toutes les technologies !

**FIABILITÉ ET SÉCURITÉ**

Les processus de déploiements respectent les bonnes pratiques avec retour arrière possible.

**SOUVERAINETÉ**

Le cloud d'Outscale associe haute performance et souveraineté des données.

**LISIBILITÉ TARIFAIRE**

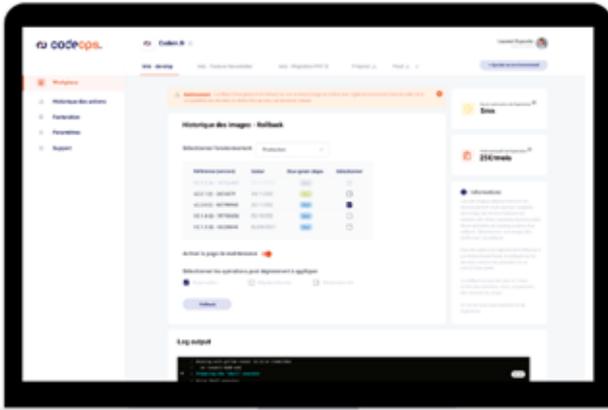
Une politique tarifaire basée sur une configuration hardware et non sur une consommation de ressources qui ne peut être que prédictive !

**INFOGÉRANCE &
SUPPORT INCLUS**

Nos experts systèmes gèrent votre infrastructure et sont joignables par téléphone.

- ✓ Automatisez vos déploiements
- ✓ Adaptez votre infrastructure aux pics de charge grâce au scaling en un clic !
- ✓ Créez des environnements de tests temporaires à la demande basés sur la branche applicative de votre choix
- ✓ Optimisez vos diagnostics grâce à la centralisation des logs et des métriques

**POSEZ TOUTES VOS QUESTIONS ET/OU
RÉSERVEZ UNE DÉMO : hosting@codein.fr**

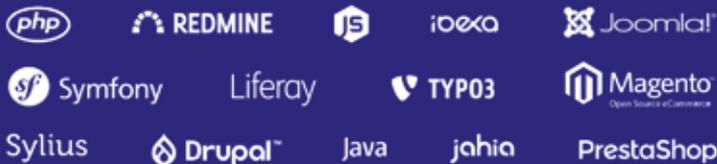


codéops.

La solution de gestion clé en main de votre applicatif sur cloud public

Vos écrans de monitoring entièrement personnalisés pour un suivi en temps réel !

Peu importe vos choix technologiques, Codéops convient à tous vos environnements



La solution de déploiement avec infogérance intégrée !

- ✓ Suivi des périodes de support des composants systèmes
- ✓ Gestion des attaques et des failles de sécurité
- ✓ Sauvegardes
- ✓ Déploiements
- ✓ Supervision
- ✓ Logs et graphes de monitoring
- ✓ Configuration des serveurs
- ✓ Support (HO)
- ✓ Astreinte 24/7 (option)



“

Contraints d'utiliser des solutions PaaS pour nos clients, nous avons constaté que le prix était souvent élevé au regard des prestations proposées, un manque de disponibilité et de qualification des interlocuteurs ainsi qu'un manque de flexibilité des plateformes qui vous imposent des contraintes applicatives (question de compatibilité), alors que ceci devrait être l'inverse !

Nous avons donc décidé de créer notre propre plateforme

Laurent Esposito,
Co-fondateur de Codéin



Avec **Codéin**, vous bénéficiez culture Devops et d' une vraie disponibilité !

POSEZ TOUTES VOS QUESTIONS ET/OU RÉSERVEZ UNE DÉMO : hosting@codein.fr

Budgets, conformité et périphérie

LES TENDANCES QUI VONT FAÇONNER LE MARCHÉ IT EN 2023

Des incertitudes pèsent sur le marché IT et continueront d'imprimer leur marque en 2023. Toutefois, dans ce contexte de changements, parfois colossaux, les entreprises cherchent plus de résilience et à tirer parti du multicloud pour augmenter leur compétitivité et limiter leurs coûts.



Voici les tendances observées, elles sont primordiales pour comprendre ce que sera l'informatique professionnelle en 2023. **Jean-Pierre Boushira**, VP South EMEA, Benelux & Nordics chez Veritas Technologies les partage.

1. Les budgets consacrés au cloud seront scrutés

Une récente étude a révélé que 94% des entreprises françaises seraient particulièrement dépensières en matière de cloud ; 43% d'entre elles dépasseraient même les budgets initialement alloués. Alors que les volumes de données continuent de croître chaque année - tout comme leurs coûts de stockage dans le cloud - ces budgets seront sans doute de plus en plus scrutés avec des justifications à apporter en termes de retour sur investissement.

Les responsables IT subiront une pression supplémentaire. Ils devront non seulement justifier leurs budgets cloud mais aussi identifier de nouvelles façons de réduire les volumes de données en adoptant des approches plus modernes et plus drastiques telles que la déduplication systématique.

2. Le mouvement *low code/no code* se heurtera à des problématiques de conformité

Le *low code/no code* a contribué à la démocratisation du développement d'applications au sein des entreprises. En 2023, l'utilisation d'applications *low code/no code* deviendra courante, et chaque employé (même les non-experts IT) aura la possibilité de créer sa propre application simple. Bien que cela allège considérablement la charge qui pèse sur les équipes IT, cela créera également un risque de conformité important pour les entreprises. Étant donné que ces « développeurs en herbe » n'ont pas la même expérience en matière de mise en œuvre de la sécurité et de la confidentialité, la plupart de ces applications ne seront pas protégées correctement, et les politiques risquent d'être mal appliquées car méconnues. Non seulement les entreprises pourraient être confrontées à des problèmes de conformité, mais leurs applications risqueraient de créer de nouvelles vulnérabilités que des cybercriminels pourront exploiter.



JEAN-PIERRE BOUSHIRA

3. La pénurie au sein de la *supply chain* mettra la pression sur les fournisseurs de logiciels

Cette année, les fournisseurs de logiciels auront encore une fois fait preuve d'innovation et auront apporté de nouvelles solutions aux entreprises. Toutefois, le déficit en matériel (qui devrait encore se faire sentir en 2023) ne sera pas en faveur de cette tendance pour les mois à venir. Les restrictions géopolitiques et les pénuries de puces ont gravement affecté la *supply chain* de matériel informatique. Les clients ont eu du mal à implémenter simultanément les logiciels et le matériel de sorte de créer des solutions fonctionnelles. Pour contrer ces problèmes, les clients adopteront certainement des solutions et des appareils basés sur le cloud avec du matériel et des logiciels déjà intégrés, plutôt que d'avoir à gérer de multiples relations fournisseurs et à attendre que le matériel n'arrive.

4. La mobilité des données inter-cloud se généralisera

Plus de 75 % des entreprises utilisent actuellement plusieurs services de cloud public. Si les avantages d'une stratégie multi-cloud sont notables, l'interopérabilité reste un défi pour les gestionnaires de données. Non seulement il est coûteux de déplacer les données d'un cloud à l'autre, mais des cloud qui ne fonctionnent pas ensemble de manière intégrée favorisent la création de silos et l'introduction de nouvelles vulnérabilités. Pour suivre le rythme des offres de cloud et atteindre les objectifs orientés métier, les entreprises vont commencer à tirer parti de l'IA/ML et des solutions autonomes plus systématiquement. Ces technologies les aideront à faire face aux défis des charges de travail cloisonnées et à améliorer l'interopérabilité du cloud via la portabilité des données. Alors que les entreprises s'efforcent de relever les défis d'interopérabilité pour obtenir plus de contrôle dans le cloud, la mobilité des données inter-cloud sera plus répandue en 2023.

5. Plus de dispositifs en périphérie induit plus de vulnérabilités

Gartner prévoit que plus de 50 % des données gérées par les entreprises seront créées et traitées en dehors des datacenters ou du cloud d'ici à 2025. Plus le traitement des données se déplace vers la périphérie, plus l'architecture informatique se complexifie, et plus la surface d'attaque augmente. Par ailleurs, les entreprises n'appliquent généralement pas le même niveau de protection à la périphérie qu'au datacenter ou au cloud - en raison d'un manque de compétences et/ou d'experts. Pour protéger pleinement l'entreprise, chaque dispositif en périphérie doit être protégé et faire l'objet d'une sauvegarde. En outre, les entreprises doivent déterminer quelles données sont critiques et celles qui ne le sont pas. À terme, cela permettra aux entreprises de mieux gérer les coûts liés au stockage et à la protection des données, ainsi que de comprendre l'origine de cette nouvelle pression exercée sur leurs budgets informatiques.

6. Kubernetes devient critique

Au cours des 24 derniers mois, la technologie Kubernetes s'est généralisée. Les conteneurs sont désormais adoptés dans les environnements critiques, impliquant alors que l'environnement applicatif ainsi que ses données sous-jacentes devraient désormais être protégés. Or, la propriété de ces conteneurs et leurs protections sont devenues plus complexes, en écho à la création de différents silos. De ces aspects résulte une certaine confusion en matière de responsabilité : la personne en charge est-elle l'administrateur de sauvegarde ou l'administrateur DevOps ? Dans le même temps, les entreprises ont du mal à identifier les conteneurs à sauvegarder et la manière de le faire. Par conséquent, elles investiront davantage dans la formation pour combler le déficit de compétences pour la gestion de Kubernetes. En 2023, les services IT continueront certainement de naviguer à vue sur la façon de protéger et de sauvegarder adéquatement leurs environnements Kubernetes.

Les entreprises et les professionnels de l'IT doivent s'interroger sur le degré de maturité de leurs projets, notamment au regard de ces différents éléments. En effet, en matière de données, la protection, l'organisation, le stockage, la gestion des coûts sont aussi importants que l'exploitation des données brutes. Ainsi, en fonction de ce qui est actuellement mis en place, d'éventuels dysfonctionnements, des points d'amélioration, voire de potentiels projets en construction, l'année 2023 pourra être un nouveau tournant pour l'entreprise et son évolution. C'est dans cette logique d'évolution et d'anticipation que les entreprises pourront se préparer à différents cas de figures et plus facilement s'adapter aux innovations et menaces à venir.

Supermood :

« ADOPTER LA FEEDBACK INTELLIGENCE, C'EST UN BESOIN VITAL AUJOURD'HUI »

Les DSI doivent s'emparer de nouveaux outils qui remettent les collaborateurs au cœur du processus de transformation, et notamment de la Feedback Intelligence. L'impact du recours à la Feedback Intelligence est rapide et percutant. Creusons le sujet avec Kevin Bourgeois, Président et co-fondateur de Supermood.



Un mot sur Supermood ?

Créée en 2015, Supermood, est la première plateforme tout-en-un de Feedback Intelligence, au service de la performance et de l'engagement des entreprises. Notre solution permet de créer des conversations internes autour des sujets majeurs de l'entreprise, puis transforme les retours collaborateurs en données objectives temps réel.

Elle est utilisée par les décideurs et managers (un tiers du CAC40) qui pilotent leurs transformations avec précision, et mettent en place des actions concrètes pour améliorer performance et expérience interne.

La Feedback Intelligence, désigne les moyens de collecter, de traiter et d'analyser les remontées des collaborateurs.

Vous parlez de "Feedback Intelligence" pour une vraie culture de la performance. Qu'est-ce que la Feedback Intelligence ? pourquoi y recourir ?

La Feedback Intelligence, abrégée en "FI", désigne les moyens de collecter, de traiter et d'analyser les remontées (les feedbacks) des collaborateurs. Le but de la FI est de servir de support à la décision et la résolution de problèmes. Elle agit comme un levier d'amélioration continue en mettant en lumière les points forts et les points faibles internes de l'entreprise. La FI est une approche orientée données qui s'inscrit dans une démarche d'amélioration continue et qui fait partie intégrante du management par la qualité, en particulier du PDCA (Plan-Do-Check-Act), qui est une boucle itérative permettant d'atteindre un objectif en agissant sur les causes, et non sur les effets.

kaspersky



Threat hunting proactive. Détection en continu. Réponse automatisée.

Confiez la gestion de votre
cybersécurité à un expert.



Kaspersky
Optimum
Security



Alors que la majorité des informations suivies par les dirigeants sont des données externes (satisfaction client, dynamique du marché, ...) ou "froides" (marges, augmentation du CA, ...), la FI se concentre quant à elle sur des signaux "vivants" de ce qui se passe en interne en collectant les feedbacks de manière régulière et confidentielle grâce à des sondages courts et précis. Autrefois l'apanage du département RH, les collaborateurs sont aujourd'hui sollicités sur tous les pans de l'entreprise : humain, stratégique et métier. L'objectif est ainsi plus vaste, celui d'avoir une vue 360° des leviers sur lesquels les décideurs peuvent agir immédiatement.

L'adoption de la FI aujourd'hui n'est plus un avantage compétitif mais un besoin vital. A l'heure où les marchés changent plus vite que jamais et que les talents sont de plus en plus exigeants, il est indispensable pour les entreprises de ne plus avancer dans le noir. Il leur faut donc sans cesse se remettre en question, être à l'affût du moindre signal faible qui permet d'anticiper un risque ou au contraire de capitaliser sur une opportunité difficile à déceler.

Est-il possible d'évoquer un ou deux cas d'applications ?

Les cas d'utilisation historiques sont ceux centrés autour de l'amélioration de la QVT. En instituant un dialogue plus régulier avec les collaborateurs, nos clients gagnent en moyenne +20 points d'engagement dans l'année, ce qui est énorme. Le secret : identifier les petits cailloux qui bloquent les salariés au quotidien.

Au-delà de la QVT, de nombreux cas "business" existent. Un client dans l'énergie a ainsi mesuré précisément l'adhésion à la stratégie globale de l'entreprise à un rythme mensuel. Il a détecté que si le top-management et les salariés étaient en accord avec la direction donnée, le middle-management quant à lui était fortement réfractaire. En creusant via des micro-enquêtes ciblées, l'entreprise s'est rendu compte que la défiance était hétérogène et dépendait de la nature des entités au sein de l'entreprise. Un "plan d'adhésion" a pu être développé afin de "convertir" les entités neutres en ambassadrices à un horizon de 12 mois,

et de travailler sur les plus réfractaires à un horizon 36 mois. Grâce à la Feedback Intelligence, le top-management a pu améliorer l'adhésion à la stratégie de 70% en 18 mois, tout en ayant des certitudes tout au long du déploiement du plan de transformation, grâce à des mesures régulières.

L'adoption de la FI aujourd'hui n'est plus un avantage compétitif mais un besoin vital.

Côté SI, de nombreux exemples tournent autour de l'amélioration des processus et de la qualité des livrables. La FI permet souvent dans un premier temps de mettre en place des métriques de suivi internes : satisfaction des salariés quant aux interactions inter-équipes, fierté du travail produit, etc. Les DSI peuvent ainsi avoir des discussions basées sur des faits objectifs : si les métriques n'ont pas augmenté d'un trimestre à l'autre, il faut repenser sa façon de faire. Vient ensuite un travail d'audit plus précis.

Les questions posées sont orientées sur les dimensions métiers : qualité du code, outillage, etc. Un client s'est ainsi rendu compte que malgré l'engagement de ses équipes, la mise en production finale était toujours une source de stress intense. Quelques enquêtes plus tard, celui-ci a identifié que les facteurs de stress étaient multiples : mauvaise communication, manque de planification, et une préproduction inefficace. Des questions ouvertes avaient également pour objectif d'impliquer chaque personne dans la résolution des problèmes. Grâce à chaque idée partagée, ce sont plus de 35 initiatives qui ont pu être mises en place avec la pleine adhésion des collaborateurs.

Résultat : un stress réduit de 90% et une satisfaction globale qui triple !

> Par Sabine Terrey



KEVIN BOURGEOIS



Les 3 défis du Cloud hybride !

Sécurité, Compétences, Conformité. Il est actuellement difficile d'assurer la conformité dans le Cloud et le manque de talents entrave les objectifs.

Comment aider les entreprises à cartographier leur transformation Cloud et leur permettre d'auto-évaluer leurs progrès ? IBM évoque quelques pistes pour identifier les domaines d'opportunités et de croissance..

Une solide stratégie de Cloud hybride

Si les entreprises adoptent l'approche Cloud hybride pour la transformation numérique, la complexité de faire fonctionner les environnements Cloud est au cœur des débats.

Il s'avère difficile de réaliser le plein potentiel d'une transformation numérique sans avoir mis en place une solide stratégie de Cloud hybride – 71% Monde – 68% France.

Seuls 27 % - Monde possèdent les caractéristiques clés pour être considérés comme « avancés » dans leur transformation.

Trois obstacles à ne pas sous-estimer

Comment gérer les environnements Cloud hybride à l'heure où les entreprises sont confrontées à des freins en matière de compétences, de sécurité et de conformité ? Retenons quelques indicateurs :

• La conformité

Assurer la conformité dans le Cloud est compliqué au moment où l'application des exigences réglementaires et de conformité s'intensifie

• La sécurité

Il faut gérer au quotidien les diverses techniques de sécurité pour sécuriser les applications dans le Cloud

• Les compétences

Face à la pénurie de talents, comment mettre en œuvre une stratégie holistique de Cloud hybride ?

L'indice de transformation d'IBM 2022 sur l'État du Cloud

Cet indice révèle ces 3 points clés en détail.

Le manque de compétences

Pour la gestion des applications Cloud, selon 69 % - Monde et 65 % - France, leur équipe ne dispose pas des compétences nécessaires pour être performante.

En outre, le manque de compétences techniques empêche les entreprises d'intégrer un écosystème de partenaires dans les environnements Cloud.

Les cybermenaces

Qu'est-ce qui empêche les organisations de favoriser l'innovation ?

- La sécurité est l'obstacle N° 1 à l'intégration des applications dans les environnements et les problèmes de sécurité sont un obstacle à la réalisation des objectifs métier grâce au Cloud (32 % - Monde et 34% - France)

Quels sont les principaux défis à relever pour intégrer pleinement l'écosystème commercial dans le Cloud ?

- la gouvernance des données
- la cybersécurité

Les exigences en matière de réglementation et de conformité

Selon 53% Monde et France, garantir la conformité dans le Cloud est très difficile. Les problèmes de conformité réglementaire sont un obstacle majeur à l'intégration des applications dans les environnements informatiques privés et publics.

Source Etude IBM & The Harris Poll - États-Unis, Canada, Royaume-Uni, Allemagne, France, Inde, Japon, Chine, Brésil, Espagne, Singapour, Australie - Du 8 juin 2022 au 17 juillet 2022 - 3 014 professionnels de l'informatique et métier (252 en France) -

IBM va rendre public l'outil « indice de transformation d'IBM sur l'Etat du Cloud » dans les mois à venir, pour fournir aux chefs d'entreprise des informations de comparaison pouvant leurs stratégies de Cloud hybride.

Tendances cybersécurité 2023 POUR L'EUROPE

L'Europe est de plus en plus touchée par les cybermenaces. Si les attaquants changent leurs tactiques et techniques, les défenseurs doivent s'adapter s'ils veulent rester à la hauteur. Parmi les prévisions pour lutter contre les cyber adversaires en 2023, que retenir ?



L'Europe pourrait devenir la région la plus ciblée par les ransomwares

Les États-Unis sont le pays le plus visé par les attaques par ransomware, mais quelques signaux montrent que l'activité des ransomwares est en baisse aux États-Unis et en hausse dans d'autres pays. En Europe, le nombre de victimes augmente, et si cette augmentation se poursuit, l'Europe deviendra probablement la région la plus ciblée en 2023. Les États-Unis ont fait preuve d'une grande franchise en matière de politiques, sanctions et le potentiel d'une réponse dans le domaine cybernétique concernant les ransomware et autres attaques.

La Cyber Russie

L'invasion de l'Ukraine par la Russie a créé des circonstances sans précédent pour les cybermenaces. La Russie mène des attaques perturbatrices, du cyber espionnage et des opérations d'information en même temps que des opérations militaires cinétiques de grande envergure. De futures attaques perturbatrices en Ukraine sont à prévoir, accompagnées d'opérations de désinformation. La volonté de la Russie de recourir à des tactiques perturbatrices, de faux fronts hacktivistes ou fronts cooptés, devrait s'étendre en dehors de l'Ukraine et de l'Europe.

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 bénéficiez d'une démonstration complète avec l'un de nos experts.

Les opérations d'information s'appuieront sur des organisations tierces

Les OI ont toujours été motivées politiquement et parrainées par des États (cf les élections américaines de 2016). Depuis, on note une grande externalisation du travail des OI par des acteurs étatiques. Cette tendance pourrait s'accroître en 2023, car les engagements de type « hack-for-hire » deviennent plus courants. Cette observation est étayée par une coïncidence, Meta a témoigné d'une augmentation de l'embauche de sociétés de marketing ou de relations publiques dans les campagnes d'OI, afin d'abaisser la barrière d'entrée pour certains hackers et d'obscurcir les identités de ceux qui sont plus sophistiqués.

Vers l'authentification sans mot de passe

Le vol d'identifiants d'entreprise reste l'un des principaux moyens utilisés par les cybercriminels. Apple, Google et Microsoft se sont engagés à mettre en place des ressources sans mot de passe basées sur les normes de l'alliance FIDO et du World Wide Web Consortium. Le déploiement initial de ces technologies se concentrera sur les ressources sans mot de passe pour le consommateur, mais les RSSI exigeront des plates-formes d'identité d'entreprise pour étendre le passwordless au marché des entreprises.

L'identité des utilisateurs volée

Les hackers trouveront de nouveaux moyens de voler les identités des utilisateurs en utilisant une combinaison d'ingénierie sociale, de vol d'informations de base et de collecte d'informations à partir de sources de données internes après la compromission. Ils combineront les informations d'identification volées avec de nouvelles techniques pour contourner le MFA et abuser des systèmes de gestion des identités et des accès.

La cyber assurance plus difficile à obtenir

Les entreprises recourent à la cyber assurance pour couvrir les cyber risques, les responsables sont conscients des risques de cybersécurité. Mais, les demandes d'indemnisation ont explosé, obligeant les compagnies d'assurance à réévaluer leur goût pour le risque et réduire leur couverture en conséquence. De nombreuses entreprises tentant de renouveler leur cyber assurance pourraient avoir du mal à obtenir la couverture souhaitée.

La Russie cible l'Europe

En 2023, la Russie pourrait étendre ses cyber-opérations à toute l'Europe. Si les mois d'hiver peuvent ralentir le rythme du conflit physique, les acteurs russes disposeront de plus d'espace.

La Russie pourrait utiliser davantage ses compétences cyber perturbatrices contre les organisations européennes, notamment les fournisseurs d'énergie et de matériel militaire, les entreprises de logistique participant à l'approvisionnement de l'Ukraine et les organisations participant à l'introduction et à l'implantation de matériel de guerre.

Les préoccupations énergétiques européennes dans le cyberspace

Les préoccupations relatives à l'approvisionnement et au prix de l'énergie en Europe pourraient se manifester sous forme de cyber-opérations malveillantes. Les entreprises européennes du secteur de l'énergie pourraient être plus ciblées au cours des mois d'hiver à venir.

Les organisations du monde entier doivent être prêtes à faire face à une augmentation des tentatives d'extorsion.

Les fournisseurs d'énergie européens sont la cible de hackers parrainés par l'État russe. La disponibilité du pétrole et du gaz, les mouvements de prix planifiés par les organisations, et les politiques énergétiques des gouvernements en développement deviendront des cibles de collecte plus importantes pour les agences de renseignement des États.

Les organisations du monde entier doivent être prêtes à faire face à une augmentation des tentatives d'extorsion.

Source Rapport prédictif Mandiant Cyber Security Forecast 2023



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

[Nouveau sur iTPro.fr : les chaînes Enjeux DSI et Vidéos IT !](#)



La cybersécurité perçue par les conseils d'administration

Une question : la cybersécurité est-elle réellement au cœur des réflexions des conseils d'administration ? Penchons-nous sur les défis et risques auxquels ils sont confrontés.

Un membre de conseil d'administration sur deux n'est pas prêt à gérer une cyberattaque

La cybersécurité est une priorité absolue pour le conseil d'administration (77%), et les discussions sur le sujet ont lieu au moins une fois par mois (76%), mais certains n'en discutent qu'occasionnellement (24%).

Ainsi, le conseil d'administration comprend clairement les risques systémiques auxquels l'organisation est confrontée et des investissements adéquats ont été réalisés.

Toutefois, si selon 65% des membres de conseils d'administration, leur organisation risque de subir une cyberattaque importante au cours des 12 prochains mois, selon la moitié, leur organisation n'est pas préparée à faire face à une attaque ciblée.

Que retenir pour la France ?

Quelques indicateurs révèlent l'état d'esprit au sein des conseils d'administration français.

- *Alignement entre les conseils d'administration et RSSI français*

Selon les membres des conseils d'administration français, leur organisation risque de subir une cyberattaque importante au cours des 12 prochains mois (78%)

- *Préoccupations semblables*

Les membres du conseil d'administration ont classé la fraude par email/compromission d'emails professionnels, les attaques de la chaîne logistique (42 %), et les ransomwares (40 %) comme principales préoccupations

- *Désaccord sur les conséquences d'un incident cyber*

L'atteinte à la réputation est en tête de liste des préoccupations des conseils d'administration, les RSSI s'inquiètent de l'impact sur la valorisation des entreprises

- *Etat de préparation*

Le conseil d'administration comprend le risque systémique et selon 72 %, ils ont investi suffisamment. Mais discuter de la cybersécurité au moins une fois par mois est insuffisant

- *Erreur humaine*

Selon les membres de conseils d'administration français, l'erreur humaine est la plus grande vulnérabilité

- *Vision commune*

Selon 67 %, ils ont une vision commune avec leur RSSI, et 64 % des RSSI pensent de même

- *Surveillance réglementaire*

Selon 84 %, les organisations devraient être tenues de signaler une cyberattaque importante aux autorités de réglementation dans un délai raisonnable

Source Rapport Proofpoint & Cybersecurity at MIT Sloan - Cybersecurity : Board Perspective 2022 – Auprès de 600 membres de conseils d'administration d'organisations comptant 5 000 employés ou plus - Différents secteurs d'activité - Août 2022 - France, États-Unis, Canada, Royaume-Uni, Allemagne, Italie, Espagne, Australie, Singapour, Japon, Brésil et Mexique.

Le recours à l'IA et aux robots dans l'industrie : OPPORTUNITÉ OU MENACE ?

Les robots, véritables assistants mécaniques, sont désormais omniprésents dans l'industrie française, en particulier dans le domaine de la production, où leur Intelligence artificielle permet d'atteindre un niveau d'efficacité bien supérieur. Néanmoins, des réserves persistent face à cette technologie.

Tobias Wölk, Product Management Automation Technology chez reichelt elektronik partage son expertise.

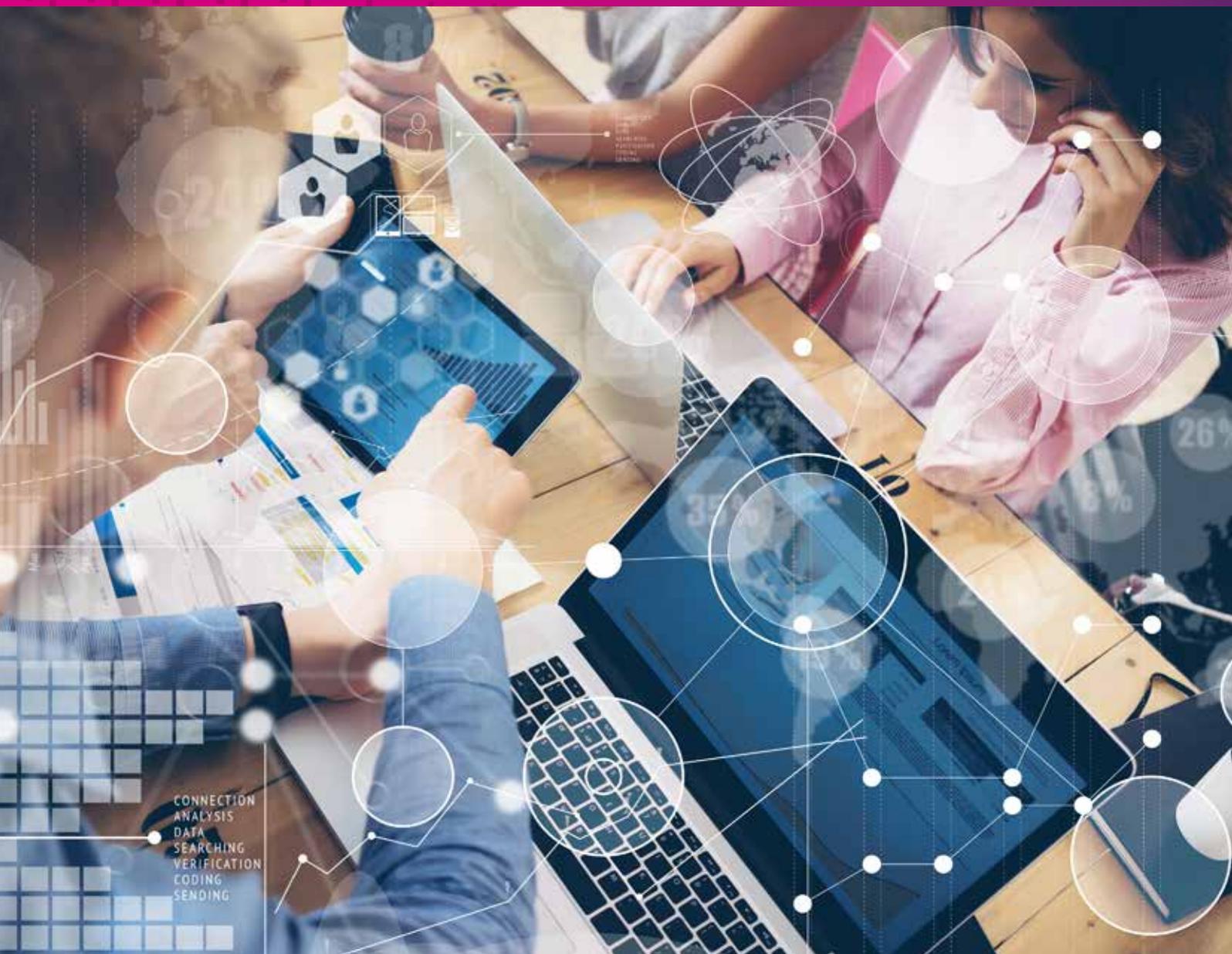


Les robots sont-ils des voleurs d'emplois ?

Évoquer simplement la pénurie de personnel qualifié ne suffit pas à décrire l'ampleur du problème ; il s'agit plutôt d'une pénurie de main-d'œuvre à l'échelle nationale. Il n'est donc pas surprenant que l'industrie se tourne de plus en plus vers la robotisation. Toutefois, cela ne signifie pas pour autant que les robots rendront le travail humain superflu ou qu'ils occuperont nos emplois à moyen ou long terme. Dans les prochaines années, les activités concernées par la robotisation seront celles qui exigent un haut degré de reproductibilité, ainsi qu'un taux d'erreur très faible, telles que la production ou la logistique de stockage.

Dans le secteur de la production, les robots collaboratifs (dits cobots), ces robots de petite taille vont venir assister principalement les êtres humains en agissant comme un bras supplémentaire. Contrairement à leurs « grands frères », les robots industriels, les cobots ne sont pas cantonnés derrière une barrière de sécurité, mais peuvent travailler main dans la main avec des spécialistes ayant reçu une formation appropriée.

Les activités concernées par la robotisation seront celles qui exigent un haut degré de reproductibilité.



Accompagner la transformation digitale avec One Call, Cloud Care et les Services Managés

Découvrez comment les offres de support, d'accompagnement et de services managés d'Insight vous guident sur la route de l'agilité, la sécurité et la résilience de vos environnements Cloud.



Pour en savoir plus et contacter nos experts, rendez-vous sur : fr.insight.com



TOBIAS WÖLK

Si les entreprises parviennent à former leur personnel de manière adéquate, les robots ne nous voleront pas nos emplois, bien au contraire, puisque ces processus homme-machine éprouvés permettent déjà de gagner en efficacité et en productivité.

A n'en pas douter, d'ici à cinq ans environ, l'utilisation de l'IA deviendra la norme dans l'industrie.

Le rôle de l'intelligence artificielle ?

Autre facteur pouvant conduire à une amélioration de la productivité, l'utilisation ciblée de l'IA. Dans la production française, les projets s'appuyant sur l'IA visent principalement à optimiser les processus. Il est souvent question de Machine Learning (ML) : sur la base des données collectées, les algorithmes sont adaptés ou développés par l'IA. De cette façon, les robots peuvent se familiariser avec le fonctionnement logiciel au cours du processus et se transforment progressivement en assistants intelligents, capables de prendre en charge de plus en plus de tâches habituellement. En contrepartie, le collaborateur peut alors se consacrer à des tâches à plus forte valeur ajoutée. A n'en pas douter, d'ici à cinq ans environ, l'utilisation de l'IA deviendra la norme dans l'industrie.

Jusqu'où irons-nous ?

Face à la situation actuelle du marché du travail, il est tout à fait réaliste de prédire que le nombre de robots et de cobots utilisés dans les entreprises continuera d'augmenter. De plus, la courbe d'apprentissage des machines est bien plus rapide, notamment grâce au ML.

Les collaborateurs ont besoin d'être impliqués le plus tôt possible pour abattre les craintes.

L'utilisation de l'IA ne peut être porteuse de promesses que si elle s'accompagne d'une stratégie élaborée qui s'appuie sur le personnel de l'entreprise dès le début du projet. Pour pouvoir surmonter les craintes et les préjugés liés à l'IA, les collaborateurs ont besoin d'être impliqués le plus tôt possible pour abattre les craintes et les méfiances encore répandues aujourd'hui face à cette technologie. En effet, savoir utiliser l'IA et la robotique constitue une véritable opportunité, à condition que les salariés soient formés en conséquence. Si ces derniers doivent suivre une formation une fois le projet mis en place, le processus est généralement plus long et plus coûteux.

Si les entreprises parviennent à mettre stratégiquement en place la robotique et l'IA au sein de leurs processus, les bénéfices tirés ne seront pas visibles seulement sur le chiffre d'affaires. Les êtres humains et les machines peuvent apprendre les uns des autres et rendre ainsi la production plus efficace sur le long terme. Le trésor de données auquel l'IA a accès est une source d'informations quasiment inépuisable, qu'il s'agit d'utiliser à bon escient. Si les entreprises prennent conscience de leurs besoins et n'utilisent pas la technologie uniquement pour se faire plaisir en se cantonnant à des innovations technologiques de surface, elles sortiront également renforcées de la crise liée à la pénurie de main-d'œuvre. Les robots ne sont pas là pour se substituer à nos emplois ; au contraire, ils peuvent nous aider à améliorer notre manière de travailler.





Le rôle clé du Directeur Financier et Administratif dans la transformation digitale

Analysons la perception de la fonction Finance par les responsables et directeurs de directions administratives et financières.

Comment perçoivent-ils leur rôle dans le développement du chiffre d'affaires et dans la conduite de la transformation digitale ?

Un rôle incontournable

Quand 71% des DAF pensent jouer un rôle incontournable dans la transformation digitale de leur entreprise, 33% perçoivent leur fonction comme essentielle.

Plus de la moitié ont le sentiment d'avoir développé et acquis de nouvelles compétences : Grandes entreprises - 57% / Secteur des services - 62%.

Leur travail est valorisé par les dirigeants – 91% et par les salariés – 87%. Enfin, selon 81%, leur rôle est central en situation de crise.

Charge de travail & Stress

Toutefois, un DAF sur deux éprouve du stress au travail (58% secteur des services - 63% grandes entreprises).

Ce stress s'explique par une charge de travail trop importante, et par le sentiment de devoir réaliser au quotidien des tâches chronophages, répétitives et à faible valeur ajoutée.

Automatisation

L'automatisation possible par l'innovation technologique est une opportunité pour leur fonction, notamment dans le secteur industriel - 49% et dans les grandes entreprises - 48%.

Les solutions d'automatisation libéreraient du temps pour :

- effectuer des tâches à valeur ajoutée – 85%,
- améliorer leur employabilité grâce à la formation
- réduire le risque d'erreur humaine
- mieux gérer l'écosystème de l'entreprise

Côté RH, ce gain de temps leur permettrait de se consacrer davantage à la fidélisation et au recrutement des talents (51%).

Un accompagnement au changement

L'accompagnement est la condition de l'appropriation de ces solutions technologiques. Ce besoin suppose la mise en place de groupes de travail pour identifier les besoins des salariés (88%), puis la diffusion aux salariés d'explications claires des bénéfices (87%), et par la mise en place de formation (89%).

Source Etude Esker& OpinionWay - L'évolution de la fonction finance en entreprise » - 334 directeurs ou responsables des affaires financières d'entreprises de 50 salariés et plus - Du 18 juillet au 5 août 2022.

Du Finops À TOUTES LES SAUCES

Que le terme choisi soit **Finops**, plan d'optimisation des coûts ou optimisation financière, difficile d'échapper au sujet du coût de son informatique. Et c'est une bonne nouvelle.



Voire une très bonne nouvelle lorsque son informatique est pour tout ou partie hébergée chez un fournisseur de Cloud. Puisque le principe fondateur est de ne payer que ce qui est utilisé, il faut pour répondre à ce besoin que tous les aspects soient parfaitement couverts. C'est-à-dire simplement et abondamment outillés.

Le client doit pouvoir :

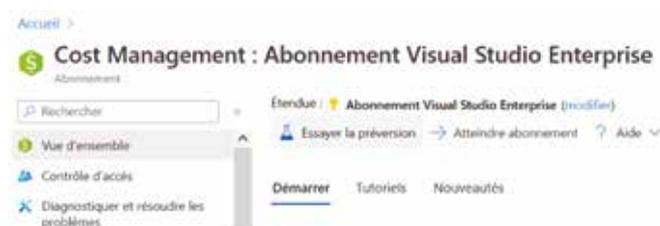
- Trouver facilement et rapidement ses informations de facturation
- Manipuler des tableaux de bord directement dans le portail
- Avoir une information exhaustive
- Analyser très finement ses coûts
- Être aidé dans le contrôle de ses dépenses
- Être alerté en cas de débordement
- Lancer des actions automatiques et correctives dès qu'un seuil d'alerte est atteint
- Et depuis peu, s'appuyer sur un algorithme de Deep Learning pour ses anomalies de dépenses

Direction le portail pour découvrir ou redécouvrir l'ensemble de ces menus dans leurs dernières évolutions en préversion. Et pour parler plus spécifiquement de la nouveauté la plus marquante (anomalies de dépenses) et des différentes manières existantes pour que les alertes déclenchent des actions.

Les outils du portail

Travailler les coûts Azure peut se faire depuis plusieurs endroits sur le portail. Mais l'entrée la plus adaptée pour une gestion centralisée est le menu central **Cost Management**. Même si ce menu est décliné sur d'autres écrans (Groupe de ressources, abonnements ...etc.).

Tous les éléments présentés ici sont issus de la préversion du portail qu'il faut lancer spécifiquement dans le menu (Essayer la préversion).



Essayer la préversion

C'est ici que sont regroupées les vues et les différentes options les plus récentes. La vue de départ est **Analyse des coûts (préversion)**. Pour qui a déjà travaillé avec le portail des coûts, cette nouvelle vue est surprenante et paraît moins complète que la vue habituelle (basée sur des graphs) que l'on retrouve toujours dans le sous menu **Analyse des coûts**.

CONGRÈS & CONFÉRENCES • 2^E ÉDITION
MARDI 21 ET MERCREDI 22 MARS 2023
RIVE MONTPARNASSE • PARIS

CAP IT

| BANQUE | ASSURANCE | FINANCE |

SAVE THE DATE

L'ÉVÉNEMENT DÉDIÉ À LA TRANSFORMATION DIGITALE
EN BANCASSURANCE ET FINANCE

500 décideurs de la filière attendus
sur deux jours

80 speakers et intervenants

500 rendez-vous d'affaires attendus

60 sponsors & partenaires acteurs
spécialistes

48 heures de débats, retours d'expériences,
projets, travaux et résultats d'études

Réservez votre badge sur www.cap-it.fr

Pourtant, elle offre un supplément de détails avec une vue que je nomme « Services / Ressources ». Il faut expliquer cette notion.

Certains services sont composés de plusieurs ressources. Par exemple, un coffre de sauvegarde **Recovery Services vault**, c'est un service facturé pour sa ressource **Azure VM Protected Instances** que l'on peut considérer comme le service en lui-même. Mais aussi pour mon cas pour sa ressource **RA-GRS Data Stored** qui est le compte de stockage sous-jacent attaché au service. Ce que l'on retrouve sur l'écran suivant.



Décomposition des coûts

Cette décomposition est extrêmement utile lorsqu'il s'agit de travailler finement les coûts. RA-GRS est une version de stockage coûteuse mais qui couvre parfaitement mon besoin. Mais cette vérification est à faire de temps en temps et il faut confirmer que ce choix :

- Est volontaire ?
- Est toujours adapté ?

Si cette nouvelle vue paraît finalement assez banale, il n'y avait pas d'autres choix auparavant que de naviguer dans les menus des services, en afficher les propriétés et récupérer les informations de configuration (même si ces extractions pouvaient se faire au travers des API Azure). Encore fallait-il connaître précisément la composition d'un coffre de sauvegarde pour connaître cette subtilité.

Autre sous menu, **Alertes de coût** et **Budgets**. Je ne vais parler ici que de la partie **Alertes de coût** qui permet de fixer des alertes et qui reprend intégralement les options du menu... **Budgets**. Il y aura peut-être à terme une fusion pour ce doublon.

La vue appelée **Prévision** est un autre moyen de connaître les coûts engagés.

Avant d'aborder cette partie, un rappel sur l'existant en termes de vue et une présentation de la nouveauté, les anomalies.

Lorsque l'on expose son budget, on peut vouloir retrouver des informations de dépenses sur une période donnée. Savoir ce qu'a coûté l'environnement du 1^{er} au 30 du mois. Cette vue est appelée **Coût réel**. Elle est utile mais elle ne permet pas d'engager d'actions de remédiation sur les dépenses engagées sur cette période. On regarde en

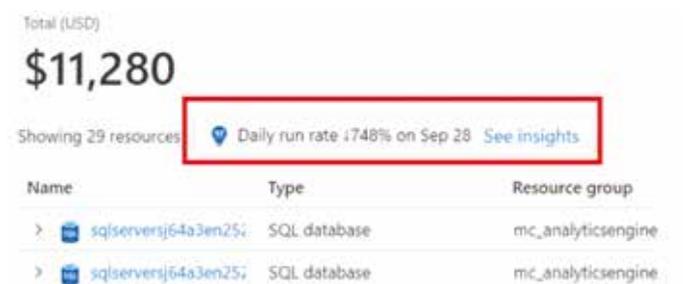
arrière et on constate.

La vue appelée **Prévision** est un autre moyen de connaître les coûts engagés. Mais cette fois, c'est une projection de ce qu'il va se passer. Je peux par exemple le 10 du mois en cours savoir combien va me coûter l'environnement sur la base des services déployés. En clair, si je ne modifie pas mon environnement (ajouts / retraits / réajustement de ressources), voilà ce que va coûter l'ensemble du 1^{er} au 30. La différence est énorme en termes d'actions de remédiation. Je peux engager des actions pour agir sur ma facture. Je regarde en avant, j'agis.

Mais ... il manquait jusqu'à ce jour une option pour être encore plus efficace. Les **Anomalies**. Présentées de cette manière par Microsoft :

« Le modèle de détection d'anomalie est une série chronologique univariée, une prédiction non supervisée et un modèle basé sur la reconstruction qui utilise 60 jours d'utilisation historique pour la formation, puis prévoit l'utilisation attendue pour le jour. »

Mes dépenses sont-elles au niveau de ce qu'elles devraient être. Et si elles ne le sont pas, je peux retrouver une information claire dans le portail.



Daily run rate = - 748 % (image éditeur).

Les options du menu amènent ensuite sur une vue détaillée où il devient assez facile d'identifier les différents types d'anomalies.

Pour mettre plus en valeur toute cette belle mécanique, les alertes sont indispensables. Alerter, c'est décider de piloter ses coûts à l'aide de l'une ou plusieurs des options présentées ci-dessus et d'y attacher des alertes.

Quelques « ça marche » pour que ces alertes aient de la valeur.

- Utiliser des alertes basées sur les prévisions (plutôt que sur les budgets) pour pouvoir engager des actions de remédiation AVANT de trop déborder sur les dépenses.
 - Par de l'alerting mail / SMS. Prévenir les propriétaires de l'environnement d'un possible débordement des coûts. Il doit agir.
 - Par de l'automatisation. Agir directement sur les ressources. Cette méthode est évidemment la plus efficace, mais elle doit être acceptée...

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

- Activer l'alerte d'anomalies. C'est une alerte quotidienne si nécessaire.
- Comme pour toute alerte, quelques alertes de qualités valent mieux qu'une multitude d'alertes.

Une courte parenthèse sur l'automatisation et quelques pistes de mise en œuvre (si ces actions sont acceptables en environnement de test ou de maquette, elles sont aussi transposables en partie pour des environnements de production).

- Stopper les ressources qui peuvent être stoppées.
- Verrouiller le groupe de ressources pour empêcher de nouvelles créations.
- Réduire les performances d'une ressource.

Reste deux sous menus toujours très utiles et complémentaires des précédents.

Advisor recommendations, qui entre autres possibilités, expose une vue des recommandations liées aux coûts. C'est une aide importante, qui propose des pistes d'optimisation sur les services déjà déployés. Pas besoin ici de présentation détaillée, le produit est tellement bien fait qu'il suffit de se laisser guider et de lire et / ou d'appliquer ce qui est suggéré. C'est à mon sens la meilleure option pour qui ne peut pas consacrer trop de temps à l'optimisation de ses coûts.

Une question peut se poser, pourquoi ne pas se baser uniquement sur ces recommandations et pourquoi passer plus de temps sur son optimisation financière ? Et bien parce que pour reprendre l'exemple du coffre de sauvegarde, **Advisor** peut vous conseiller de réduire la taille d'une machine virtuelle qui est utilisée à 2 % de ses possibilités depuis 3 semaines. Mais il ne peut pas « décider » si votre coffre de sauvegarde en RA-GRS répond bien à un besoin ou si c'est une erreur de déploiement.

Advisor recommendations expose une vue des recommandations liées aux coûts.

Dernier point, le sous menu **Reservations + Hybrid Benefit**.

Pour les réservations, il est question d'acheter des ressources ou du volume sur la durée. Une machine virtuelle pour 3 ans ou une capacité de réserve de stockage pour 1 Po. Cet engagement à moyen long terme permet de bénéficier de réduction sur la facture.

Pour l'Hybrid Benefit, c'est une répartition des licences existantes, la possibilité d'utiliser des licences locales compatibles dans le Cloud.

Ce sous menu permet de retrouver toutes ces informations.

En résumé

Voilà une très belle panoplie de services pour l'optimisation de ses coûts. Ses outils sont natifs et complémentaires. Ils sont exhaustifs et clairs.

Ils sont étendus par les alertes et les actions. La prise en main est rapide, les données sont exportables dans la majorité des cas pour pouvoir être utilisées par les outils de BI.

Avec ces dernières nouveautés, il ne manque plus de vues ou fonctionnalités pour pouvoir travailler efficacement le Finops !

En synthèse, un bon point de départ en 3 étapes

- 1 /** Le portail est nativement outillé pour traiter finement du sujet des coûts Azure.
- 2 /** Les dernières nouveautés offrent 3 niveaux d'informations.
 - Ce qu'il s'est passé, le coût réel.
 - Ce qu'il va se passer, la prévision.
 - Ce qui ne se passe pas bien en rapport avec mon historique récent, les anomalies.
- 3 /** Alerter, c'est informer, mais c'est aussi agir par l'automatisation.

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



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

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

Codéops, la solution de gestion clé en main de votre applicatif sur cloud public souverain, rdv en page 14

N°28 | DÉCEMBRE 2022 CONDUIRE LA TRANSFORMATION NUMÉRIQUE DE L'ENTREPRISE

SMART DSI®

DOSSIER
L'agilité dans un monde où l'on veut tout contrôler

INTERVIEW
Adopter la Feedback Intelligence est vital

L'ŒIL SECURITE
Cyberattaques en hausse - Investissements en baisse

L'ETUDE A RETENIR
Les 3 défis du Cloud hybride

ANALYSE
Le recours à l'IA et aux robots dans l'industrie : opportunité ou menace?

STRATEGIE
5 choses que les DSI devraient faire en 2023

Club Abonnés sur ITPro.fr

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

ABONNEZ-VOUS MAINTENANT !

SMART DSI

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 Mennecey - France

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

Patrowl ÉLÈVE FORTEMENT LE NIVEAU DE SÉCURITÉ DES SYSTÈMES D'INFORMATION

Évaluer la sécurité des actifs extérieurs en permanence est une priorité pour Patrowl, startup française, éditrice de la solution d'Offensive Security as a Service éponyme. Revenons sur l'actualité de l'entreprise avec Vladimir Kolla COO de Patrowl.



Un mot sur votre start up ?

Patrowl est la solution leader de la sécurité Offensive as-a-Service permettant de protéger la surface d'attaque externe des entreprises, c'est-à-dire tout ce qui est exposé sur Internet. Patrowl identifie les vulnérabilités à corriger avant toute attaque.

Pour cela, Patrowl opère une cartographie de ce que détient et expose l'entreprise sur Internet, teste ses actifs en continu, identifie les vulnérabilités et propose un plan de remédiation et le contrôle des corrections appliquées. Aujourd'hui, plus de la moitié des piratages provient d'une exposition sur Internet mal contrôlée, un partage d'accès distant, un mail, un site Internet, etc.

C'est une solution simple d'usage, accessible aux non experts, qui a vocation à élever fortement le niveau de sécurité des systèmes d'information. La cartographie ou EASM selon le Gartner fait partie des technologies que le cabinet conseille aujourd'hui. De notre côté, nous pensons que l'EASM n'est efficace que lorsqu'elle s'accompagne d'une parfaite lisibilité des informations et d'accompagnement à la remédiation, l'objet de Patrowl.

Patrowl, c'est également la société qui porte la solution. Fondée en 2020 par Nicolas Mattioco, Florent Montel et Vladimir Kolla, elle compte aujourd'hui une vingtaine de collaborateurs. Patrowl est née du constat que les tests d'intrusion, trop ponctuels, sont devenus inefficaces au regard des méthodes de développement continu appliquées en entreprise. Il faut aujourd'hui être capable d'évaluer la sécurité des actifs extérieurs en permanence.

Que retenir des dernières actualités de l'entreprise ?

En premier lieu, je citerai notre levée de fonds de 2 millions € auprès du fonds d'entrepreneurs Cyber Impact Ventures, porté par la société de gestion Auriga Partners, de la banque d'investissement Bpifrance et de la région Île-de-France. C'est pour nous une reconnaissance de la pertinence de notre solution dédiée à des organisations, publiques et privées, de plus en plus attaquées.

Ces fonds nous permettront d'une part de renforcer notre communication et notre marketing, un exercice auquel les entreprises françaises ne sont pas

toujours bien rompues. D'autre part, ils viendront soutenir notre recrutement. Il faut enfin souligner le précieux conseil que nous délivre Cyber Impact Ventures, grâce auquel nous pouvons conforter notre position de leader français du Pentest en continu et accélérer notre croissance commerciale.

En participant au FIC Montréal au début du mois de novembre, nous voulions mieux connaître le fonctionnement du marché Nord-américain de la cybersécurité. Ce fut l'occasion de rencontrer de probables partenaires locaux et d'évaluer les opportunités notamment canadiennes et états-uniennes.

Nous poursuivons le développement de nouvelles fonctionnalités pour Patrowl, à travers le renforcement de l'automatisation des tâches et la simplification des étapes de remédiation.

Nous tenons en premier lieu à répondre rapidement aux demandes des entreprises utilisatrices. Ainsi, certaines évolutions, notamment l'intégration du Single Sign-On (SSO permettant d'utiliser le référentiel d'identité de nos clients pour les accès), l'interconnexion avec les outils de gestion de tickets du marché, la connexion aux infrastructures Cloud, la refonte graphique de l'interface..., sont issues des requêtes de nos clients.

Il faut aujourd'hui être capable d'évaluer la sécurité des actifs extérieurs en permanence.

Dans cet objectif, nous avons lancé nos User Squad début novembre afin d'échanger avec eux, de leur présenter notre feuille de route et surtout d'être à l'écoute de leurs attentes pour les évolutions à venir. Une expérience que nous renouvellerons tous les 6 mois.



VLADIMIR KOLLA

Quelles perspectives pour 2023 ?

Les rencontres avec les entreprises et partenaires américains lors de notre présence au FIC Montréal nous ont confortés dans notre intention de nous développer en Amérique du Nord.

Nous préparons d'ailleurs une levée de fonds en série A en 2023 pour accompagner notre développement à l'international.

En parallèle de ce projet, nous prévoyons de renforcer notre programme partenaire, initié cette année, pour développer un circuit de vente indirecte complémentaire.

Et bien sûr, nous recrutons des ingénieurs, juniors/seniors, H/F pour accompagner le développement de notre activité. Une appétence pour la cybersécurité est évidemment un plus !

> Par Sabine Terrey

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

Sur iTPro.fr, 9 chaînes d'informations et de formations des meilleurs experts en technologies informatiques d'entreprise, par les éditeurs du trimestriel SMART DSI.

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

▶ iTPro.fr

CINQ CHOSES QUE LES DSI DEVRAIENT FAIRE EN 2023

Difficile à croire, mais 2023 arrive à grand pas. Après avoir fait face à la crise sanitaire en 2020, l'attention générale s'est portée sur la nouvelle année à venir avec pour espoir qu'elle soit celle d'un « nouveau normal ».

Massimo Guarnieri, Global Lead for "X on Azure", Avanade livre ses prédictions.



Ce qu'aucun d'entre nous ne savait alors, mais que nous acceptons pleinement aujourd'hui, c'est que cette nouvelle normalité continue d'être marquée par une forte instabilité mondiale. Outre l'incertitude économique et politique persistante, celle-ci est également alimentée par l'adoption du télétravail, la fréquence croissante des cyberattaques ou encore les réglementations de plus en plus complexes en matière de sécurité, de finance et d'ESG.

S'il ne fait aucun doute que l'objectif initial de nombreux DSI, en réponse à ces problématiques, sera d'assurer la survie et la conformité de l'entreprise à court terme, il est vital de ne pas perdre de vue les objectifs à long terme : la transformation numérique. Aussi chaque DSI devrait se pencher en 2023 sur cinq points essentiels :

1. Investir dans la résilience et la flexibilité pour faire face à l'imprévu

Si l'année dernière nous a enseigné une leçon importante c'est que la capacité à s'adapter rapidement au changement est la clé de la réussite en période de crise. Il est évidemment beaucoup plus facile d'y parvenir avec une stratégie de type "cloud first", pourtant, deux tiers des charges de travail informatiques restent sur site. Bien sûr, cela est compréhensible : garder ses informations sur un ordinateur central donne le sentiment de mieux les contrôler, ce qui est d'autant plus important lorsque l'on opère dans des environnements hautement réglementés. Néanmoins, le changement et l'innovation menés par les mainframes prennent des mois, dans un monde où chaque seconde compte.

Il est également extrêmement coûteux d'évoluer vers des technologies comme l'Intelligence Artificielle et le Machine Learning qui permettront à l'entreprise non seulement de réagir, mais aussi de prévoir et d'anticiper. C'est pourquoi Gartner prévoit que d'ici 2027, environ la moitié des entreprises utiliseront des plateformes de cloud industriel pour accélérer plus de 50 % de leurs initiatives commerciales clés. L'année dernière, ce chiffre était inférieur à 10 %. En 2023, tous les DSI devront investir dans des solutions de cloud sécurisées dans lesquelles ils pourront avoir confiance. Il faudra être en mesure de s'adapter et d'évoluer plus rapidement qu'auparavant.

2. Préparer les talents de demain

Avec la pression exercée sur les entreprises pour qu'elles performant plus efficacement, tout en répondant à des demandes de plus en plus complexes de la part des clients, la guerre des talents est loin d'être terminée. Il n'est donc pas surprenant que 94 % des cadres supérieurs de la tech affirment que la recherche et la rétention de talents sont des tâches devenues de plus en plus importantes dans leur quotidien. Alors que le marché des profils tech est plus hyperconcurrentiel que jamais, attirer et retenir les talents est aujourd'hui un facteur clé pour les entreprises souhaitant prospérer l'année prochaine. Malheureusement, pour ceux qui dépendent encore largement des mainframes, souvent construits sur un langage hérité des années 1950 et 1960, ce problème est encore plus important. La vieille garde qui parle ces langages COBOL est bien avancée dans sa retraite, et les jeunes développeurs choisissent plutôt de se concentrer sur des technologies plus récentes, plus



MASSIMO GUARNIERI

attrayantes et plus innovantes. Plutôt que d'essayer de recruter des profils formés à des technologies vieillissantes, il faut investir dans le futur et passer à Azure. La bonne nouvelle, c'est que si les grands acteurs du marché continuent à se débarrasser discrètement de leurs talents dans une tentative désespérée de réduire les coûts, une foison de profils formés et talentueux seront disponibles.

Attirer et retenir les talents est aujourd'hui un facteur clé pour les entreprises souhaitant prospérer l'année prochaine.

3. Réduire les coûts sans compromettre la continuité

Il va sans dire qu'en période d'incertitude, cette phrase fait partie de presque toutes les conversations. Alors que les DSI s'attendent à ce que les budgets informatiques augmentent de 5,1 % en moyenne en 2023, cela reste inférieur au taux d'inflation prévu de 6,5 % et il sera donc important de dépenser efficacement, tout en fournissant de la valeur. C'est ce que disent de nombreuses entreprises, qui parlent également de la pression qu'elles subissent pour réduire les coûts sans pour autant réduire les services ou les engagements stratégiques, c'est-à-dire faire plus avec moins. Il existe bien sûr de nombreuses façons d'y parvenir : réévaluer les contrats des fournisseurs, retarder les achats de technologies et réduire les embauches. Cependant, il est aussi judicieux de mettre hors service des infrastructures obsolètes et redondantes, comme des ordinateurs centraux coûteux, et transférer les activités vers le cloud, où vous pouvez garantir une réduction des coûts d'au moins 50 %. Un chiffre qui ferait sourire n'importe quel PDG.

4. Continuer à abattre les silos pour innover plus efficacement

Les directeurs de la technologie et des systèmes d'information sont formels et unanimes : c'est toujours une priorité absolue. Bien sûr, le niveau d'innovation dépendra de votre organisation et du secteur dans lequel vous travaillez, mais une expérience client prédictive, immersive et en temps réel transcende à peu près tout. Quel que soit le degré de maturité de l'entreprise, il sera essentiel d'investir dans les Superapps, l'IA adaptative et la préparation au Metaverse, autant d'éléments que Gartner a cité dans son top 10 des tendances technologiques stratégiques pour 2023. Les recherches montrent que la plupart des entreprises consacreront une part importante de leur budget informatique à ces technologies, les investissements en logiciels devant augmenter de 11,3 %, contre seulement 3,4 % pour les systèmes de centres de données. Les chiffres parlent d'eux-mêmes, si la R&D va dans une direction, pourquoi aller dans l'autre - c'est de la folie. Rester focalisé sur une stratégie imaginée autour de l'ordinateur central, sur site, c'est choisir de freiner la transformation de l'entreprise, son agilité et la réduction des coûts.

5. Prendre part aux conversations autour de l'ESG

La durabilité environnementale continue de grimper dans les rangs des priorités stratégiques des PDG. Le cabinet Gartner la place désormais au huitième rang, contre le treizième en 2020. Les DSI ont un rôle évident à jouer dans ce domaine, car la capacité d'accéder à des données transparentes et fiables est essentielle pour mesurer les progrès accomplis dans la réalisation de ses objectifs. L'informatique est donc vitale au succès de toute stratégie ESG. Il est également important pour les DSI de s'assurer que la stratégie informatique globale de l'entreprise tienne bien compte de son propre impact environnemental et tente de le réduire autant que possible, lorsque cela est possible. La meilleure façon de prendre place à la table ESG est de s'assurer que vos données se trouvent dans un environnement permettant de fournir ces informations en temps réel, en utilisant le moins d'énergie et de ressources possible.

Si les dernières années d'instabilité nous ont appris quelque chose, c'est que ceux capables de réagir plus rapidement sont ceux qui s'en sortent le mieux dans des crises. Avec au moins 12 à 18 mois supplémentaires de chaos à l'horizon, il est temps pour les dirigeants d'être honnêtes avec eux-mêmes et de prendre des mesures définitives en matière de recrutement, d'agilité, de réduction des coûts, d'innovation et de durabilité. Ceux qui ne le feront pas auront peu de chances de s'en sortir.

A3BC : DES SOLUTIONS D'IDENTITÉ NUMÉRIQUE UNIVERSELLE ET SÉCURISÉE POUR TOUS

Fondée en 2018, la société A3BC (Anything, Anytime, Anywhere Biometric Connections), acteur privé de la French Tech, vient compléter les initiatives de l'État en matière de numérique. Dinesh Ujoodah, CEO d'A3BC, s'est prêté au jeu des questions – réponses.



Un petit mot de présentation de votre start-up et votre technologie ?

La technologie développée par A3BC permet d'offrir aux entreprises privées et aux particuliers des solutions d'identité numérique universelle et sécurisée avec l'ambition de devenir un tiers de confiance reconnu en France et en Europe.

A3BC a conçu, breveté et déployé une plateforme de confiance numérique, délivrant et gérant une identité numérique couplée à une authentification forte. Les produits et services d'A3BC mettent en œuvre un protocole de protection des données, hautement sécurisé, ayant nécessité deux ans de recherches et développement. Ce protocole a été breveté et appartient à A3BC. Ce brevet décrit un procédé de transaction sans support physique, ni identifiant de sécurité ni jeton, sécurisé par le découplage structurel des identifiants personnels et de transaction. La

sécurité est obtenue en répartissant dans différentes bases de données les différentes composantes des informations personnelles, c'est-à-dire les données biométriques, les données personnelles et les données de paiement, sans aucun moyen de les réconcilier facilement.

Notre plateforme permet d'optimiser l'expérience client et de renforcer le contrat de confiance, en ligne et également en face-à-face en particulier grâce entre autres à l'usage de la biométrie.

Notre plateforme repose sur 3 piliers fondamentaux que sont l'identité numérique qui gère les attributs de la personne physique (nom, prénom, numéro de mobile, adresse email, vérifie l'authenticité de sa pièce d'identité ou son passeport), un Wallet qui permet de vérifier et ajouter des documents supplémentaires, les méthodes d'authentification forte qui sont la connaissance, la possession et la biométrie.

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



WWW.IT-AND-CYBERSECURITY-MEETINGS.COM

**21, 22 & 23
MARS 2023**

PALAIS DES FESTIVALS ET DES CONGRÈS DE CANNES

ILS SONT DÉJÀ INSCRITS



A3BC accompagné par Alain Bensoussan, avocat spécialisé en droit numérique, a conçu et déployé l'application mobile TrustMe, entièrement conforme à la réglementation RGPD. A3BC garantit que les données des utilisateurs leur appartiennent et ne seront jamais exploitées à des fins commerciales ou publicitaires. De plus, dans un souci permanent de protection des utilisateurs et de leurs données, A3BC a breveté un protocole de stockage de données.

L'application TrustMe est en cours de certification eIDAS identité numérique niveau substantiel auprès de l'ANSSI et a déjà franchi les deux premiers jalons de cette certification. Le règlement eIDAS a pour ambition d'accroître la confiance dans les transactions électroniques. Il établit un socle commun pour les interactions électroniques sécurisées entre les citoyens, les entreprises et les autorités publiques.

En 2023, A3BC prévoit de finaliser et obtenir la certification eIDAS identité numérique niveau substantiel pour confirmer notre position en tant qu'acteur majeur de confiance numérique. A3BC compte également étendre son offre commerciale en proposant sa plateforme en marque blanche pour les entreprises privées qui veulent se doter d'une solution clé en main d'identité numérique certifiée. Enfin, nous prévoyons de mettre en œuvre les concepts SSI (Self Sovereign Identity) pour renforcer le contrôle total des données personnelles par l'utilisateur.

A3BC garantit que les données des utilisateurs leur appartiennent et ne seront jamais exploitées à des fins commerciales ou publicitaires.

Si on revenait sur l'usurpation d'identité, pourquoi et comment protéger son identité sur internet ?

La récente pandémie a accéléré de manière incroyable la transition numérique et nos usages digitaux. Plus que jamais, nous devons retrouver dans le monde digital et les interactions à distance la confiance que nous avons dans le monde réel pour réaliser les actes et transactions de tous les jours.

Pour définir l'identité numérique, il faut rappeler les fondamentaux. L'identité est un l'ensemble d'éléments qui, aux termes de la loi, concourent à l'identification d'une personne physique (dans la société, au regard de l'état civil) : nom, prénom, date de naissance, filiation, etc. L'identité numérique est l'extension de cette définition dans le monde numérique. Elle représente l'ensemble des éléments qui permettent d'identifier un individu physique ou moral en ligne et en face à face.



DINESH UJOODAH

La digitalisation qui s'invite désormais dans toutes les sphères de notre vie fait naître de nouvelles problématiques : comment être certain que notre interlocuteur est bien celui qu'il prétend être ? Comment s'assurer de l'authenticité des données nécessaires pour effectuer une opération financière ? Face aux nouveaux défis digitaux, la question de l'identité numérique est plus que jamais d'actualité.

Aujourd'hui, plus que jamais, la question de la confiance et de la sécurité est devenue centrale, notamment grâce à une prise de conscience collective face aux fuites de données et cyberattaques massives de ces dernières années. En effet en 2020, dans le monde, le nombre de données personnelles compromises - parmi lesquelles noms, identifiants et mots de passe - s'est élevé à 36 milliards contre 15,1 milliards en 2019 soit plus du double. Par ailleurs, en 2019, les pertes liées aux usurpations d'identité se sont élevées à 502,5 milliards de dollars aux Etats Unis et ont atteint 712,4 milliards de dollars en 2020.

Assurer la véracité de l'identité numérique est vital ! Elle constitue la clé d'accès à des services de plus en plus essentiels où la confiance est au cœur de la relation : services automatisés d'enrôlement et de vérification d'identité (KYC/KYB), services personnalisés et pertinents de santé, accès à des processus administratifs, notariaux, de succession, d'éducation, de mobilité. L'identité numérique constitue finalement la base de notre liberté et est la clé de voûte du nouveau monde digital.

Dans tous les métiers de confiance, la réglementation fixe les exigences qui permettent de gagner cette confiance. Dans le cas de l'identité numérique, RGPD et eIDAS sont les deux réglementations fondamentales.

Le RGPD, Règlement général sur la protection des données adopté en 2016 par le Parlement européen, soumet les organismes recueillant des données personnelles numériques à certaines obligations afin de garantir la protection des données recueillies.

L'identité numérique constitue finalement la base de notre liberté et est la clé de voûte du nouveau monde digital.

Le Règlement « eIDAS » n°910/2014 du 23 juillet 2014 a pour objectif d'accroître la confiance dans les transactions électroniques au sein du marché intérieur. La révision de celui-ci prévoit la mise en œuvre de portefeuilles européens d'identité numérique, dits « EUDIW ». Selon la proposition législative, les portefeuilles d'identité numérique devraient garantir le niveau de sécurité le plus élevé possible pour les données à caractère personnel utilisées pour l'authentification, que ces données soient stockées localement ou à l'aide de solutions en cloud, en tenant compte des différents niveaux de risque. Le recours à l'authentification biométrique est ainsi l'une des méthodes d'identification offrant un niveau de confiance élevé, en particulier lorsqu'elle est utilisée en combinaison avec d'autres éléments d'authentification

Par conséquent, les solutions d'identité numérique ont besoin de garantir la sécurité des données personnelles tout en garantissant une expérience utilisateur fluide. L'application d'identité numérique TrustMe développée par A3BC permet de réconcilier ces deux tendances à travers un processus simple de vérification d'identité, des moyens d'authentification fiable, sécurisée et préservant la confidentialité des données personnelles et un protocole breveté de stockage sécurisé.

Comment les entreprises peuvent se protéger contre ce type de fraude ?

Afin de se protéger contre ce type de fraude, les entreprises doivent s'appuyer sur des solutions d'identité numériques fiables, sécurisées et qui ont fait l'objet d'une certification de niveau substantiel ou élevé fournie par l'ANSSI.

La plateforme d'identité numérique de A3BC permet de répondre à ces enjeux au travers d'une culture reconnue en matière de cybersécurité, le recours à des fournisseurs labellisés par l'ANSSI et le respect strict du cadre réglementaire tels que le RGPD et eIDAS.

De plus, A3BC prend les aspects de sécurité et privacy dès la phase de conception (security and privacy by design) de façon à ce qu'ils soient mis en œuvre selon le principe de défense en profondeur. Et bien évidemment, nous faisons appel à des cabinets d'audit en cybersécurité et des programmes de type bug bounty pour évaluer régulièrement notre solution d'identité numériques.

Par conséquent, les solutions d'identité numérique ont besoin de garantir la sécurité des données personnelles tout en garantissant une expérience utilisateur fluide.

> Par Sabine Terrey



PLONGÉE AU CŒUR DE LA DevX !

La DevX, c'est mettre le développeur au cœur de son entreprise. Mais plus précisément, comment se lancer dans une démarche DevX ? Clément David, CEO et cofondateur de Padok, a accepté de répondre à quelques questions.



DevX (Xpérience du développeur) mais qu'est-ce que c'est précisément ? y a-t-il plusieurs définitions ou visions du sujet ?

L'expérience DevX est une philosophie au carrefour du développement, du *management*, du *business*, des RH : Il existe de multiples définitions de la devX (expérience du développeur) mais elles se rejoignent toutes sur deux grands axes : la satisfaction des développeurs et leur efficacité/productivité.

La DevX, c'est en quelque sorte, mettre le développeur au cœur de son entreprise.

Lorsqu'une entreprise met en place une démarche DevX au sein de son organisation, l'objectif est de trouver des solutions pour que les développeurs puissent exercer leur métier dans les meilleures conditions, avec les meilleurs outils. La DevX, c'est en quelque sorte, mettre le développeur au cœur de son entreprise. Autrefois perçu comme un exécutant parmi tant d'autres, peu d'attention lui était portée. "Mais ça, c'était avant", comme dit l'expression. Aujourd'hui, les développeurs sont la pierre angulaire, les catalyseurs de l'innovation des entreprises. Dans un contexte où la guerre des talents fait rage, mettre ses développeurs dans les meilleures conditions pour produire du code de qualité, le plus rapidement possible, est un facteur clé de rétention et un avantage concurrentiel non négligeable.

Les définitions de la DevX dépendent aussi et surtout du contexte du développeur et de la taille de l'entreprise. Par exemple, dans certaines scale up, la problématique majeure sera de pouvoir tester une nouvelle fonctionnalité dans tout l'écosystème technique de l'entreprise, ce qui n'est pas forcément possible en local quand il existe une trentaine d'applications qui communiquent entre elles et c'est à ce moment-là que les environnements de développement à la volée arrivent sur la table notamment. Tandis que d'autres entreprises auront davantage de problématiques autour de leur CI/CD (l'intégration continue) car si pour tester dans un environnement Cloud, un développeur doit attendre 30 min pour tester une fonctionnalité, il sera à la fois inefficace et frustré par cette lenteur.

Et la DevX concerne tous les domaines ?

Oui, cela concerne tous les domaines de la tech. Cela peut aller du développeur web pour qu'il puisse implémenter de nouvelles fonctionnalités sur un site web rapidement de manière sereine jusqu'au data engineer qui lui, va avoir besoin d'un workflow efficace pour tester ces processus d'analyse de données qui sont assez lourds en général.

C'est un des enjeux clés du métier de DevOps : mettre les développeurs dans les meilleures conditions pour produire vite du code de qualité. Le développeur est considéré comme un utilisateur, dont on écoute les retours et avec qui on met en place une démarche d'amélioration continue.



CLÉMENT DAVID

Dans une grande structure, les enjeux de validation ou de gestion des données critiques rendent forcément l'expérience de développement plus lourde, il devient alors essentiel d'avoir une démarche consciente pour faciliter le travail des équipes techniques au quotidien. Toute la problématique est d'optimiser cette expérience en fonction du contexte de l'entreprise.

Alors, finalement la DevX, c'est prendre soin des développeurs. Pourquoi est-ce un sujet crucial aujourd'hui pour vous ?

En 2022, les missions "DevX" représentent un quart des projets, un chiffre en forte progression par rapport à 2021. Start up comme grands groupes sont en recherche de solutions pour améliorer les conditions de travail techniques des développeurs. En tant que DevOps c'est notre mission car ce sont les premiers utilisateurs d'une infrastructure Cloud. Nous devons alors échanger avec les développeurs pour voir ce qui les bloque ou les ralentit.

S'il faut deux jours pour générer un environnement de test afin que le développeur puisse tester une fonctionnalité, c'est extrêmement pesant pour lui car il a deux options : attendre longtemps et faire exploser son projet, ou prendre le risque de mettre en production sans tester son code et donc faire bugger son application. La génération automatisée d'environnements de test est alors une solution envisageable pour débloquer la situation. Autre exemple, nous allons souvent déployer des composants comme des bases de données que nous mettrons à disposition des développeurs pour qu'ils puissent faire leurs tests avec tous les composants nécessaires au bon fonctionnement de leur application. Dans ce cas, les devs seront forcément plus sereins que s'ils ne pouvaient pas tester avec toutes les dépendances externes de leur application.

C'est une démarche sur-mesure, car chaque équipe technique a ses propres contraintes et ses propres process.

Le conseil que je donnerais à une entreprise qui souhaite se lancer dans une démarche DevX : il ne faut pas se lancer dans une grande liste au Père Noël des meilleures pratiques DevX. C'est une démarche sur-mesure, car chaque équipe technique a ses propres contraintes et ses propres process.

Pour démarrer, il faut créer une coopération entre "utilisateurs" (développeurs) et fournisseurs (DevOps), définir les points bloquant pour les développeurs, et établir une stratégie étape par étape qui lève les points bloquants des développeurs.

Plusieurs petits chantiers successifs fonctionnent toujours mieux qu'un grand "big bang DevX".

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

Sur iPro.fr, 9 chaînes d'informations et de formations des meilleurs experts en technologies informatiques d'entreprise, par les éditeurs du trimestriel SMART DSI.

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

iPro.fr

L'ECDN : LA SOLUTION INDISPENSABLE POUR DES LIVE EVENTS RÉUSSIS

Il y a quelque temps, j'ai testé et mis en place la solution Collective qui, pour être tout à fait honnête, est une solution très bien pensée et optimisée. La relation commerciale mais aussi technique avec les équipes de Collective nous a beaucoup aidés à l'époque pour comprendre les mécanismes d'optimisation des flux live Event entre les postes de travail, la technologie utilisée et les différents problèmes qu'il convient d'éviter.



Il semblerait donc, que Microsoft ait compris l'importance de ce type de solution pour les entreprises. En effet, on ne transforme pas les réseaux d'entreprise conçus principalement pour des données, en autoroutes pour flux vidéo. Les solutions ECDN (Enterprise Content Delivery Network) sont donc indispensables pour cela. Je vais vous expliquer pourquoi.

Les live Events

En regardant de plus près les deux solutions, celle de Collective et celle de Microsoft, le principe de fonctionnement est identique. Au lieu que tous les utilisateurs téléchargent la même chose en

même temps, ces derniers s'échangent le contenu localement, via des connexions point à point évitant la saturation des liens internet qu'ils utilisent.

Cette solution ne concerne pas les utilisateurs travaillant depuis leur domicile, car la bande passante internet qu'ils utilisent est naturellement leur propre bande passante. La dernière fois que j'ai fait des relevés avec Collective, nous étions partis sur une consommation de 1,7 Mb/s par client regardant un live Event. Si l'on considère une agence ayant 200 utilisateurs avec une bande passante de 500 mb/s utilisée en moyenne à 50% et si 80% d'entre eux regardent le même évènement, alors, le calcul est vite fait ($200 \times 0,8 \times 1,7 = 272$ MB/s).

Autant dire que le live Event va

- Saturer les interconnexions Internet
- Rendre l'expérience utilisateur extrêmement dégradée.

Comment je le sais ? Je l'ai vécu, l'entreprise pour laquelle je travaillais à l'époque a essayé et ce fut un désastre. Routeurs saturés, plus de possibilité d'envoyer et de recevoir des messages de l'extérieur, impossibilité de surfer sur internet, etc... quant à l'image de la DSI... je vous laisse imaginer.

Les bonnes questions à se poser

Par conséquent, si vous activez ces fonctions de live Meeting vous ne devez pas faire l'économie d'une étude préalable.

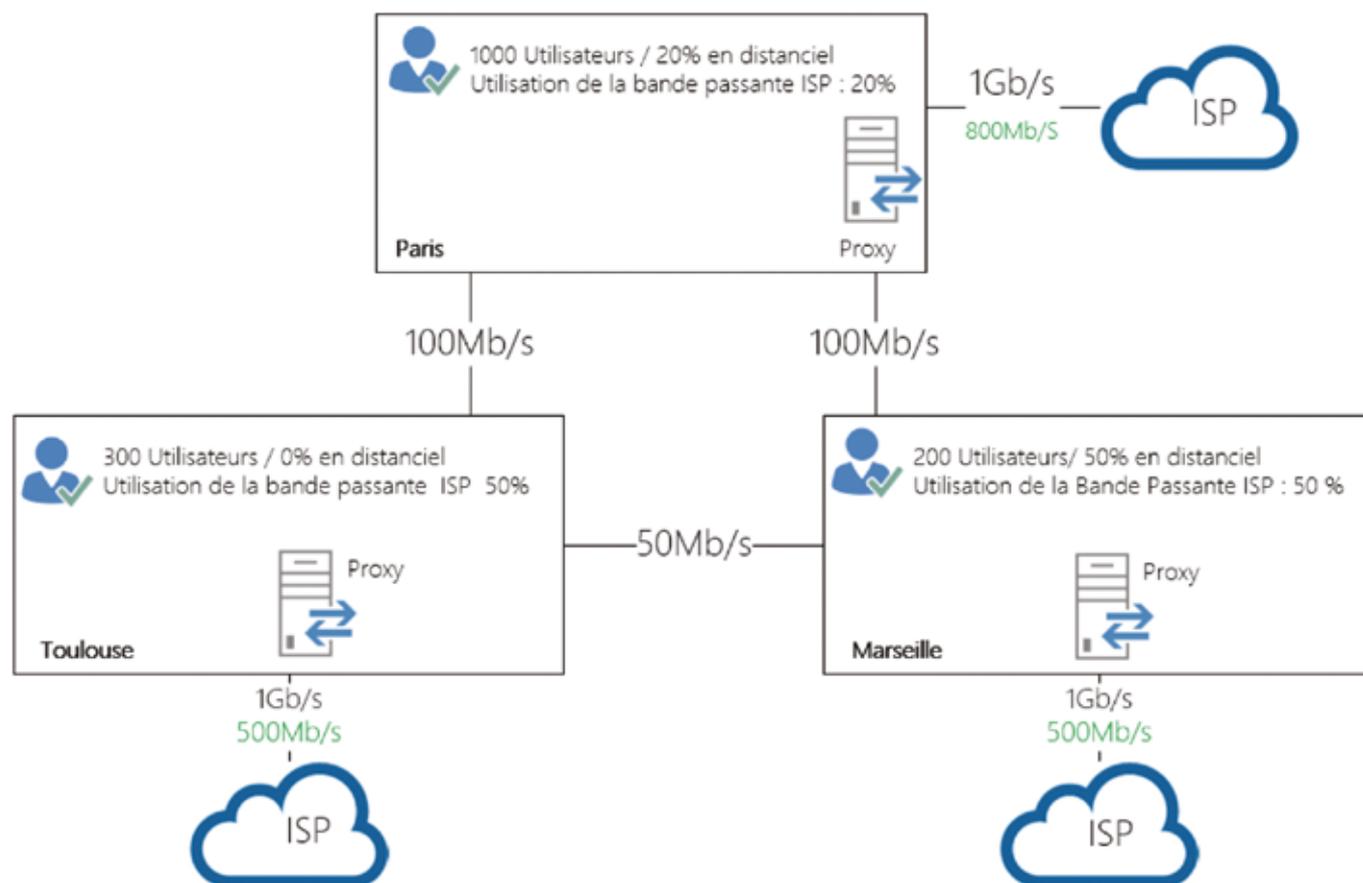
Et là-dessus il y a des quelques questions importantes à se poser.

1. Est-ce que tous les sites de mon entreprise doivent être optimisés et si non, comment indiquer aux services ECDN que certains sites ne doivent pas l'être ?
2. De combien de licences dois-je disposer pour une optimisation efficace ?
3. Dois-je acquérir autant de licences que d'utilisateurs alors même que certains travaillent à 90 % à distance ?
4. Est-ce que la solution ECDN est disponible quel que soit l'endroit où mes utilisateurs se trouvent ?
5. Qu'est ce que cela implique de faire du partage de flux en point à point ?
6. Est-ce que la solution fonctionne avec les différents systèmes ?
7. Comment valider la solution ?
8. Que suis-je en droit d'attendre d'une solution ECDN ?

Est-ce que tous les sites de mon entreprise doivent être optimisés et si non, comment indiquer aux services ECDN que certains sites ne doivent pas l'être ?

Certains sites en France comme dans le monde possèdent suffisamment de bande passante pour supporter les flux vidéo sans être optimisés.

La figure suivante illustre le réseau de l'entreprise Lamda.com comprenant 3 agences interconnectées entre elles.



Si l'on prend par exemple un site à Marseille comportant 200 utilisateurs dont 50% travaillent habituellement en distanciel, avec une bande passante internet de 1 Gb/s même utilisée à 50 %, il est certain que vous n'avez pas besoin d'acquérir des licences pour ces utilisateurs. Si l'on considère que 100% des utilisateurs regarderont le même live event la bande passante consommée sera de 1,7mb/s * 100 soit 170 Mbs. Pas de quoi trembler.

Si vous activez ces fonctions de live Meeting vous ne devez pas faire l'économie d'une étude préalable.

Autrement dit les sites concernés (sites critiques) sont ceux dont le nombre d'utilisateurs locaux est important et où la bande passante restant libre, demeure faible. Vous devez donc en faire l'inventaire.

De combien de licences dois-je disposer pour une optimisation efficace ?

Pour les sites critiques il faudra calculer le nombre d'utilisateurs locaux qui doivent être optimisés pour que la consommation de bande passante lors d'un live Meeting soit acceptable au regard de la bande passante du site concerné. Il n'est donc pas forcément nécessaire d'acquérir des licences pour la totalité des utilisateurs de site critique mais suffisamment de licences pour ne pas saturer le lien internet. Encore un petit calcul que vous devrez entreprendre.

Comment les clients se découvrent-ils ?

Chez Collective, les clients se découvrent grâce à l'agent qui se connecte sur les services cloud (une solution sans agent existe également). Les clients Collective reçoivent les adresses IP des autres clients qui leur sont proches via la notion de site IP. La notion de site IP est importante car elle permet d'éviter que certains client Live Event se connectent entre eux.

Dans notre exemple, il faudra éviter que les clients de Toulouse et de Marseille s'échangent leur contenu car s'ils le font, il est probable qu'ils risquent de saturer la bande passante de 50 Mb/s reliant les deux sites.

Dois-je acquérir autant de licences que d'utilisateurs alors même que certains travaillent à 90 % à distance ?

Certainement pas, car encore une fois les utilisateurs qui travaillent à distance devraient utiliser leur propre bande passante Internet, sauf si la configuration mise en place encapsule le flux Teams

dans la solution VPN qui connecte la station de travail au site de l'entreprise. Cette configuration fortement déconseillée, doit être alors modifiée pour permettre aux stations de travail à distance de sortir directement sur Internet sans passer par un site de l'entreprise. Dans ce cas, l'utilisation en home Office n'a nullement besoin d'être optimisée par l'ECDN.

Est-ce que la solution ECDN est disponible quel que soit l'endroit où mes utilisateurs se trouvent ?

Il est possible que certaines régions ne soient pas optimisables, je pense à la Chine par exemple. Avant de vous lancer dans la validation de ces deux solutions, vérifiez bien cette information.

Qu'est-ce que cela implique de faire du partage de flux en point à point ?

Tous vos postes de travail, je l'espère pour vous, ont un firewall. Le partage point à point des flux live Event va nécessairement entraîner l'ouverture de port de communication entrant – sortant depuis, vers les postes de travail. Est que la communication entre les stations de travail est sécurisée ? de mémoire la Solution Microsoft utilise (le protocole SCTP plutôt que UDP, chiffré par DTLS) et quels sont les ports de communication utilisés ? Faites-vous vérifier l'information.

Réaliser un Live Event et mesurer le taux d'audience ainsi que l'expérience utilisateur sont deux choses différentes.

Est-ce que la solution fonctionne avec les différents systèmes ?

Des clients Teams il y en a beaucoup. Il y a le client Teams desktop, le client Web, les applications mobiles Android & iOS. La solution ECDN que vous envisagez de choisir sait-elle toutes les optimiser ?

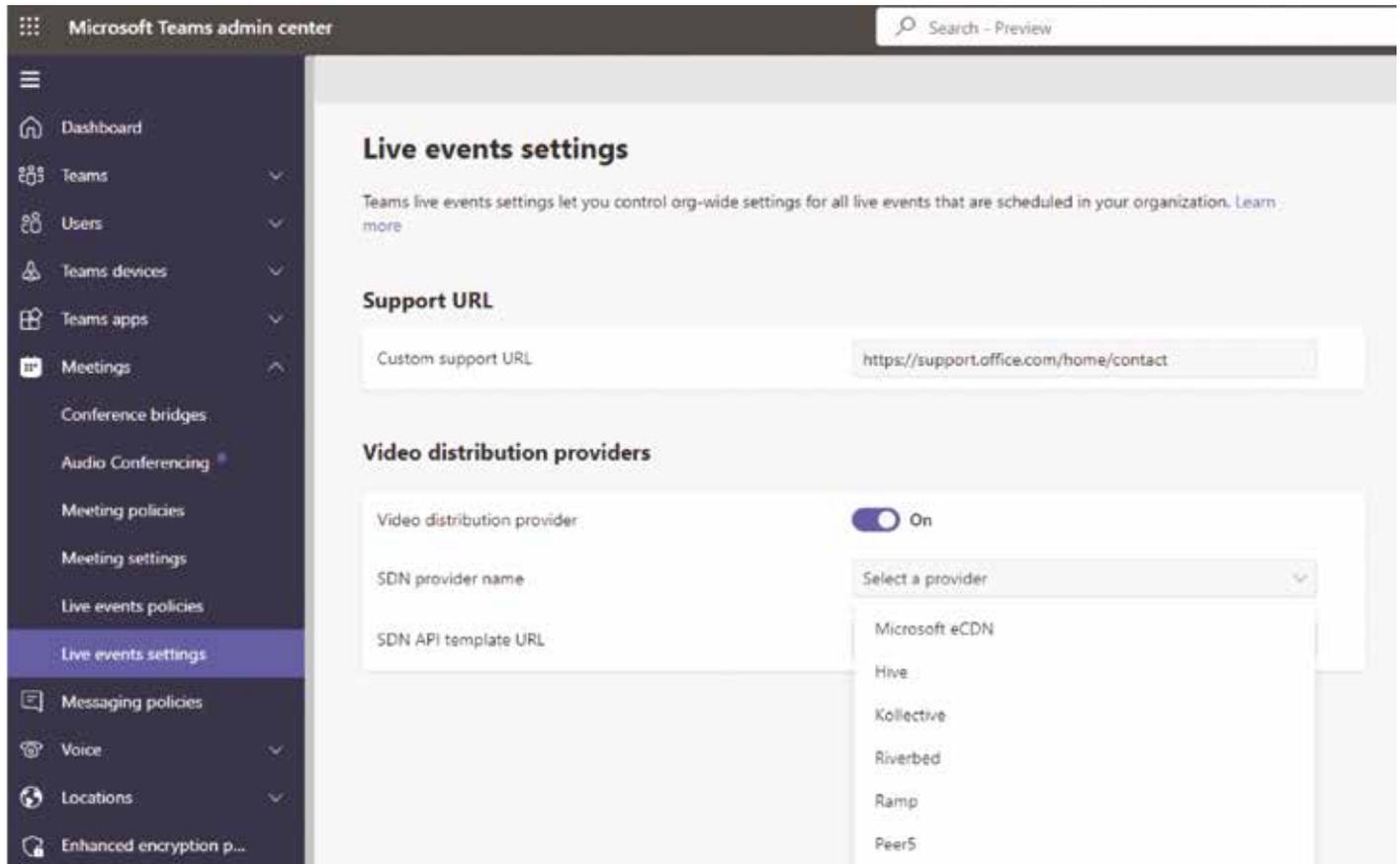


Actualités, chroniques et dossiers informatiques experts pour les Professionnels IT.

[Nouveau sur ITPro.fr : les chaînes Enjeux DSI et Vidéos IT !](#)

Comment valider la solution ?

Rien de plus simple, prenez contact avec votre CSAM Microsoft ou avec Kollektive , et rendez-vous dans votre tenant 0365 pour activer la solution comme le montre la capture d' écran suivante.



Note : de mémoire la solution Riverbed revend en marque blanche la solution Kollektive

Que suis-je en droit d'attendre d'une solution ECDN ?

La première chose que l'on est en droit d'attendre d'une solution ECDN est qu'elle optimise les flux Live Event en toute sécurité. Je suis assez confiant sur le fait que toutes savent le faire.

La seconde chose qui sera fort utile va tourner autour des outils statistiques, post production ou temps réel que la solution va offrir.

Réaliser un Live Event et mesurer le taux d'audience ainsi que l'expérience utilisateur sont deux choses différentes. Les outils de statistiques par exemple devraient vous permettre a posteriori, voire en temps réel, de valider le taux d'optimisation de chaque site distant et de mettre en évidence la qualité de l'expérience utilisateur.

Nul doute que si le top management de votre entreprise s'adresse à l'ensemble des collaborateurs, ces derniers vous demanderont des statistiques sur la qualité de l'évènement : combien de personnes se

sont connectées, quelles sont les personnes qui ont eu des problèmes de déconnexion ou une mauvaise qualité audio ...

Sans vouloir nécessairement promouvoir la solution Kollektive, il est vrai que sa mise en place a donné d'excellents résultats. Je suis certain que la solution ECDN de Microsoft saura également optimiser drastiquement les bandes passantes.

Je suis donc extrêmement curieux de la comparer car la différence risque de ne pas se jouer sur les capacités d'optimisation mais plutôt sur le service global que la solution devrait apporter aux Directions des Services Informatiques.

A suivre donc !

> Par Laurent Teruin, MVP



La valeur stratégique des entreprises déployée grâce à l'IA et les données

Les entreprises pourraient générer des bénéfices supplémentaires à trois conditions : améliorer les pratiques en matière de données, remettre de la confiance à l'IA avancée et intégrer l'IA aux opérations commerciales.

Convertir la data science en véritable valeur commerciale

Les entreprises veulent exploiter l'IA au sein des activités, mais 81 % ont déployé leur premier système d'IA seulement ces quatre dernières années et 50 % au cours des deux dernières.

Les difficultés, en matière de vérification des données, de pratiques et stratégies associées, persistent et 26 % seulement sont très satisfaits de leurs données et de leurs outils d'IA.

Une approche « IA + Données » pour créer de la valeur

Découvrons une démarche qui se concentre sur 3 domaines pour augmenter l'utilisation de l'IA, libérer sa valeur et améliorer l'expérience humaine.

- *Transformer la gestion des données en partage des données*

Les entreprises qui adoptent l'économie du partage des données tirent une plus grande valeur des données. Les données prennent de la valeur lorsqu'elles sont traitées comme de la monnaie et circulent à travers des modèles de gestion de données en étoile. Les entreprises qui rafraîchissent les données avec une faible latence génèrent plus de bénéfices, de revenus et de mesures subjectives de la valeur.

- *Passer de la Data Compliance au Data Trust*

Les entreprises très satisfaites de leur projet IA détiennent des pratiques de données éthiques, responsables et dignes de confiance. Ces conditions permettent de relever les défis de la vérification, de la partialité des données et d'instaurer la confiance.

- *Étendre l'équipe d'IA au-delà des data scientists*

Les entreprises qui appliquent la data science à des exigences pratiques créent de la valeur. L'intégration entreprise-data science accélère les gains d'efficacité et l'extraction de valeur.

« Les entreprises qui se base sur la fiabilité et le partage de leurs données sont plus agiles et font évoluer leur IA au rythme de leurs besoins. Les entreprises qui doutent de leurs données risquent un cercle vicieux de "purgatoire des pilotes" et utilisent les données et l'IA pour résoudre uniquement des problèmes de petite envergure. La gestion des données combinée à la confiance dans l'IA augmentent très clairement les capacités de l'entreprise et les performances financières » conclut **Satish H.C.**, EVP and Co-Head Delivery, Infosys

Source Etude Infosys Knowledge Institute « Infosys Data+AI : Faire de l'IA une réalité » - 2 500 dirigeants et cadres supérieurs du secteur technologique dans treize industries - États-Unis, Royaume-Uni, France, Allemagne, Australie, Nouvelle-Zélande

ENTREPRISE ET CYBERSÉCURITÉ

CYBER-SÉRÉNISEZ VOTRE ACTIVITÉ



© Studio Orkidées 2022

À l'ère de la transformation numérique et à l'heure des questions de souveraineté numérique, **cyber-séréniser vos activités devient vital face aux impacts financiers des cyberattaques.**

Protection des réseaux, des données, des postes et serveurs ; choisir les solutions Stormshield, c'est faire appel à un acteur de cybersécurité de confiance.



STORMSHIELD

www.stormshield.com



DIGITAL TRUST BUILDER

Conseil
Intégration
Services Managés

www.metsys.fr

Paris - Rennes - Nantes - Tours - Bordeaux - Toulouse - Aix-en-Provence - Lyon - Strasbourg - Lille