

SMART DSI®



DOSSIER

La loi sur l'Intelligence Artificielle, entre intérêts et exigences

INTERVIEW

L'IA frugale, une composante à prendre en compte

L'ETUDE A RETENIR

Top 10 des technologies émergentes

L'ŒIL DU NUMERIQUE

Panne informatique mondiale : les enseignements à tirer

INTERVIEW

Stimuler l'innovation durable

L'ŒIL SECURITE

Ralentissement économique et budgets cybersécurité

Club Abonnés sur ITPro.fr

ARRÊTER LES MENACES C'EST BIEN. LES PRÉVENIR C'EST MIEUX.



Sécurité multicouche

Des technologies exclusives qui dépassent les limites des antivirus traditionnels.



Taches des utilisateurs finaux

Processus automatisés et autres mesures de sécurité du côté du client.



Réseau sensoriel

Chasse aux menaces alimentée par le cloud et prévention avancée des menaces.



Intelligence artificielle

Apprentissage profond, apprentissage automatique et autres méthodes avancées.



Expertise humaine

Des experts hautement respectés et 13 centres de recherche et développement dans le monde.





Un leadership clair pour la cybersécurité !

En cybersécurité, aucun doute, le manque de ressources et d'adhésion de la direction est paralysant. Encore plus à l'heure où il est crucial de s'attaquer au sujet de la gestion des risques et où les impacts des cyberattaques peuvent être désastreux. Sujet qui sera évidemment porté sous les feux des projecteurs et creusé lors des prochains grands rendez-vous et salons cybersécurité en octobre et novembre 2024.

La communication entre les RSSI et la direction doit non seulement être fluide, mais elle doit reposer sur la confiance et le partage d'informations, seul moyen de renforcer la cyber résilience et de remédier aux problèmes. Les indicateurs⁽¹⁾ sont, par ailleurs, peu rassurants puisqu'au niveau mondial, seul un tiers des entreprises s'appuient sur un système de cybersécurité 24/7. Le manque de leadership et de responsabilité au plus haut niveau joue dans la balance, en d'autres termes, les directions ne perçoivent tout simplement pas la cybersécurité comme leur responsabilité selon 48% des RSSI.

Plus précisément, en France, si la quasi-totalité des RSSI sont préoccupés par la surface d'attaque, 33% s'inquiètent de la manière de découvrir, d'évaluer et d'atténuer les zones à haut risque. Pour 47%, l'attitude de leur entreprise face au cyber risque reste bien trop aléatoire...

Alors, qu'observe-t-on face aux enjeux de la cybersécurité ? Un manque de ligne directrice en matière de stratégie de cybersécurité certes, mais également un manque de ressources suffisantes, seul un quart utilise des techniques de gestion de surface d'attaque pour en mesurer le périmètre ! Et un manque de leadership éclairé des conseils d'administration qui expose cruellement les organisations.

Redoubler d'efforts pour se protéger est la priorité, cela ne se fera que si les dirigeants comprennent l'importance de la cybersécurité qui doit être appréhendée comme un objectif d'investissement stratégique.

Très bonne lecture !

(1) Source Etude Trend Micro & Sapio Research
"Underfunded and unaccountable: How a lack of corporate leadership is hurting cybersecurity"

Sabine Terrey
Directrice de la Rédaction
sterrey@itpro.fr

SMART DSI

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

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

SMARTDSI

N° 35 | SEPTEMBRE 2024

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 - 2024 IT PROCOM - Tous droits réservés
N° ISSN : 2494-9701 - N° CPPAP : 0518 T 93059
www.smart-dsi.fr

6 | DOSSIER

*La loi sur l'intelligence artificielle,
entre intérêts et exigences*

12 | L'ŒIL SECURITE

*Ralentissement économique
et budgets cybersécurité*

14 | INTERVIEW

*EasyVista accélère sa croissance en France
et à l'international*

17 | L'ETUDE A RETENIR

Top 10 des technologies émergentes

18 | EXPERT

De la visibilité par les Workbooks

24 | INTERVIEW

*Pari réussi pour Sightness
« du conseil à l'édition SaaS ! »*

27 | L'ETUDE A RETENIR

Faire comprendre le risque cyber !

28 | L'ŒIL DU FUTUR

*Industrie manufacturière: la législation
sur le droit à la réparation impose
une refonte complète de la chaîne de valeur*

31 | L'ETUDE A RETENIR

Les budgets des DSI en 2025





32 | INTERVIEW

Datascientest : l'IA frugale est une composante à prendre en compte dans le développement de l'IA

34 | L'ŒIL DU NUMÉRIQUE

Panne informatique mondiale en juillet 2024 : les enseignements à tirer

36 | EXPERT

Office 365 : 3 mesures de sécurité que vous devriez prendre

40 | INTERVIEW

Stimuler l'innovation durable grâce à la transformation numérique et aux principes ESG

SMARTDSI

Rédaction

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

Comité de rédaction associé à cette édition

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

Régie Média & Publicité - Com4Médias

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

Abonnements

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

Conception & Réalisation

Studio C4M – Philippe Deslandes
conseil@com4medias.com

© 2024 Copyright IT Procom
© Crédits Photos

IStock - Fotolia - 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.

© 2024 IT PROCOM - Tous droits réservés
N° ISSN : 2494-9701 - N° CPPAP : 0518 T 93059

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

Site officiel : www.smart-dsi.fr

La loi sur l'intelligence artificielle, ENTRE INTÉRÊTS ET EXIGENCES

> Par Didier Danse

L'essor fulgurant de l'intelligence artificielle a ouvert de nouvelles perspectives dans des domaines aussi variés que la santé, les transports, ou encore la finance. Cependant, cette technologie prometteuse soulève également des problématiques complexes qui nécessitent une attention particulière. Ainsi, elle impressionne bien des gens et en effraie bien plus.



En effet, la prolifération de systèmes d'intelligence artificielle non régulés peut engendrer des risques pour les droits fondamentaux, tels que la discrimination, la manipulation des comportements, ou encore des atteintes à la vie privée. De plus, l'absence de normes claires sur la transparence et la responsabilité pourrait compromettre la confiance

du public dans ces technologies, freinant ainsi leur adoption. C'est ainsi que des réglementations pour encadrer le développement de l'intelligence artificielle et son utilisation sont nécessaires. C'est de cette manière que se voit augmenter la collaboration entre les utilisateurs et le département informatique, en profitant de ce que chacun connaît le mieux.

Les enjeux de la loi

La mise en place de la loi sur l'intelligence artificielle représente à la fois un défi et une opportunité pour l'Europe. D'une part, le cadre réglementaire proposé vise à garantir un usage éthique et sûr des technologies d'intelligence artificielle, en établissant des normes strictes pour les applications à risque élevé, et en interdisant les pratiques jugées inacceptables. Cela pourrait renforcer la protection des citoyens contre les dérives potentielles, tout en assurant un terrain de jeu équitable pour les entreprises.

D'autre part, cette réglementation ouvre également des opportunités significatives pour l'innovation. En définissant des règles claires, la loi sur l'intelligence artificielle pourrait stimuler la confiance des consommateurs et des investisseurs, facilitant ainsi le développement de nouvelles applications d'intelligence artificielle conformes aux exigences légales.

La définition selon l'Union Européenne

La loi sur l'intelligence artificielle propose la définition suivante : « un logiciel développé à l'aide de l'une ou plusieurs des techniques et approches énumérées à l'annexe I, et qui peut, pour un ensemble donné d'objectifs définis par l'homme, générer des résultats tels que du contenu, des prédictions, des recommandations ou des décisions influençant les environnements avec lesquels il interagit. »

L'annexe I mentionnée dans la définition fait référence à des techniques spécifiques comme :

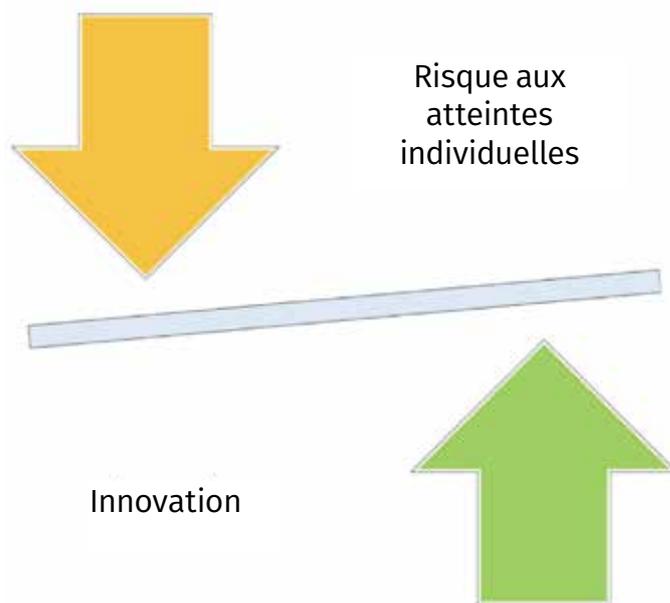
- **Apprentissage automatique** incluant l'apprentissage supervisé, non supervisé et par renforcement.
- **Logique et systèmes basés sur des connaissances**, y compris la représentation des connaissances, les moteurs de règles, les moteurs de raisonnement et la planification.
- **Méthodes statistiques et autres approches** comme les méthodes bayésiennes, les méthodes de recherche et d'optimisation.

Ainsi, la définition est suffisamment large pour couvrir bien des situations et éviter de manquer de couvrir certains systèmes.

En effet, entre la première version de la loi sur l'intelligence artificielle et le texte officiel entré en vigueur le 1^{er} août 2024, des modifications ont été nécessaires pour tenir compte de l'évolution de l'intelligence artificielle et inclure le cas de l'intelligence artificielle à usage général. Cette définition devrait permettre d'ores et déjà couvrir les utilisations futures.

Une approche basée sur le risque

La loi propose une approche basée sur le risque associé à des systèmes qui s'avèreraient défectueux ou mal utilisés. Cette approche permet de cibler les systèmes qui présentent les plus grands dangers, tout en allégeant les contraintes sur ceux qui posent peu ou pas de risques. Cette approche permet ainsi de trouver un équilibre entre confiance et capacité d'innovation. D'ailleurs, cette dernière fait l'objet d'un chapitre entier de la loi, visant à permettre la recherche et le développement sans y imposer les mêmes contraintes.



Ainsi, la loi propose de classer les intelligences artificielles en quatre catégories : les intelligences artificielles présentant des risques inacceptables, les intelligences artificielles à risque élevé, les intelligences artificielles à risque limité ou encore les intelligences artificielles à risque minimal.

Les intelligences artificielles présentant des risques inacceptables

Ce sont des systèmes d'intelligence artificielle qui posent des risques clairs pour la sécurité, les droits fondamentaux, ou les valeurs de l'Union européenne. En raison de leur dangerosité, ces systèmes sont interdits. Si vous êtes adeptes des séries télévisées, la grande majorité des sujets abordés au sein de *Black Mirror* s'avèrent être considérés comme présentant des risques inacceptables selon l'Union Européenne : Les systèmes de notation sociale des citoyens par les gouvernements, les systèmes d'intelligence artificielle utilisés pour manipuler de manière subliminale le comportement des personnes, les technologies de surveillance biométrique en temps réel dans les espaces publics.

Notons que les systèmes d'intelligence artificielle dans le contexte militaire, de la défense et de la sécurité nationale ne font pas partie du périmètre de la loi. En effet, bien que ces sujets, par définition, requièrent des données sensibles, l'utilisation aux fins ci-dessus est autorisée, tout du moins sous certaines conditions. Il est en effet critique que les autres lois soient respectées, la loi sur l'intelligence artificielle ne les remplaçant aucunement.

Les intelligences artificielles à risque élevé

Ces systèmes sont autorisés, mais soumis à des obligations strictes car ils présentent des risques élevés pour la santé, la sécurité, ou les droits fondamentaux. Ils sont souvent utilisés dans des secteurs critiques comme les infrastructures, l'éducation, la sécurité, la justice, ou les services publics.

Ainsi les systèmes d'intelligence artificielle utilisés dans les dispositifs médicaux, les logiciels d'évaluation des crédits, les systèmes de recrutement ou de gestion des ressources humaines sont autant de systèmes à risque élevé.

Les intelligences artificielles à risque limité

Ces systèmes posent des risques plus faibles mais nécessitent tout de même des exigences spécifiques pour garantir la transparence. Les utilisateurs doivent être informés qu'ils interagissent avec une intelligence artificielle.

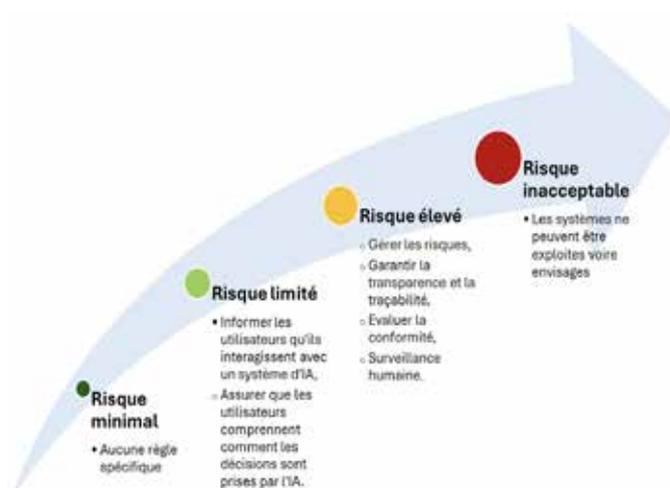
Sont attendus dans cette catégorie les chatbots ou assistants virtuels ou encore les systèmes de reconnaissance faciale sur les smartphones pour le déverrouillage.

Les utilisateurs doivent être informés qu'ils interagissent avec une intelligence artificielle.

Les intelligences artificielles à risque minimal

Ces systèmes sont considérés comme présentant des risques négligeables ou minimales pour les droits et la sécurité des utilisateurs. Ils sont exemptés de la plupart des obligations de conformité. Parmi ces systèmes, nous retrouvons les filtres de spam dans les courriels, les jeux vidéo utilisant l'intelligence artificielle ou encore les systèmes de recommandation sur les plateformes de streaming.

En fonction du niveau de risque identifié, il s'agira alors de mettre en place des mesures pour réduire le risque pour les utilisateurs et les personnes dont les données sont utilisées dans un système d'intelligence artificielle, ces points sont décrits ci-après :



Quel que soit le système, la loi impose une obligation pour les fournisseurs et ceux qui les mettent en œuvre d'être transparents. Ainsi, l'utilisation de systèmes manipulant des images, des vidéos ou encore des pistes audios se doit désormais d'être clairement indiquée. Les deepfake non explicitement notifiés sont dès lors désormais punissables explicitement au travers de cette loi.

La loi et l'intelligence artificielle générale

L'intelligence artificielle générale fait référence à un système d'intelligence artificielle capable d'exécuter n'importe quelle tâche cognitive humaine avec la même flexibilité et adaptabilité que l'esprit humain. Contrairement à l'intelligence artificielle spécialisée ou générative, qui se concentre sur des tâches ou des domaines spécifiques, l'intelligence artificielle générale pourrait théoriquement résoudre une large gamme de problèmes sans être explicitement entraînée pour chacun d'entre eux.

Les intelligences artificielles générales sont définies dans la loi sur l'intelligence artificielle comme « des systèmes d'intelligence artificielle capables de remplir des fonctions très diverses qui ne sont pas limitées à un secteur d'application spécifique. » Elles peuvent être intégrées dans des systèmes ou services plus larges, utilisés à la fois dans des environnements à risque élevé ou à risque limité. Etant donné la difficulté de clairement identifier comment seront utilisées ces intelligences artificielles étant donné leur polyvalence, il est parfois compliqué de savoir qui est responsable de quoi, bien que le bon sens pourrait répondre à cette question.

Les modèles d'intelligence artificielle générale présentent un risque systémique s'ils remplissent l'une des conditions suivantes :

- Ils ont des capacités d'impact élevées, évaluées sur la base d'outils et de méthodologies techniques appropriés, y compris des indicateurs et des critères de référence

- Sur la base d'une décision de la Commission, d'office ou à la suite d'une alerte qualifiée du groupe scientifique, il a des capacités ou un impact équivalent à ceux visés au point précédent.

Ainsi, bien que cela s'applique à tout système informatique, il est explicitement demandé de maintenir la documentation concernant les intelligences artificielles, de garantir le respect de la loi sur le copyright, de fournir de la traçabilité sur les données utilisées pour entraîner le moteur d'intelligence artificielle.

Il est peu probable que vous soyez concerné par ces exigences mais il est important d'en être conscient, notamment lorsque vous utiliserez des systèmes dont la capacité est fortement élevée.

La mise en œuvre d'une réponse adéquate

Différentes mesures s'avèrent nécessaires pour répondre aux exigences de la loi sur l'intelligence artificielle. Certaines mesures sont obligatoires tandis que d'autres sont recommandées :

- **Évaluation des risques** : Les entreprises doivent commencer par identifier et évaluer les systèmes d'intelligence artificielle qu'elles utilisent ou développent. Cela implique de déterminer le niveau de risque associé à chaque système (inacceptable, élevé, limité ou minimal) et d'adopter des mesures appropriées pour atténuer ces risques. Les systèmes à risque inacceptable ne pourront pas être utilisés.
- **Documentation et transparence** : Il est essentiel de documenter de manière détaillée la conception, le déploiement et le fonctionnement des systèmes d'intelligence artificielle. Cette documentation

doit inclure des informations sur la conformité réglementaire, les mécanismes de prévention des contenus illégaux, et les résultats des évaluations de risque. La transparence est particulièrement cruciale pour les systèmes à risque élevé, où des informations claires doivent être fournies sur leur fonctionnement et le traitement des données.

- **Mise en place d'une gouvernance de l'intelligence artificielle** : Les entreprises doivent établir une gouvernance claire autour de l'utilisation de l'intelligence artificielle. Cela peut inclure la création d'un comité d'éthique de l'intelligence artificielle, la désignation de responsables pour superviser la conformité, et le développement de processus internes pour gérer les risques associés à l'intelligence artificielle.

Différentes mesures s'avèrent nécessaires pour répondre aux exigences de la loi sur l'IA.

- **Formation et sensibilisation** : La formation du personnel est cruciale. Les employés, y compris les développeurs et les équipes de gestion, doivent être formés aux principes de la loi sur l'intelligence artificielle et sensibilisés aux enjeux éthiques et réglementaires associés à l'intelligence artificielle. Cela inclut une compréhension des risques et des moyens de maîtrise de l'intelligence artificielle.
- **Dialogue avec les régulateurs** : Engager un dialogue avec les régulateurs et les autres parties prenantes peut aider à mieux comprendre les exigences de la loi sur l'intelligence artificielle et à identifier les meilleures pratiques pour une conformité efficace.



« 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**

La collaboration avec les autorités réglementaires peut également faciliter l'adaptation aux futures évolutions de la législation.

• **Surveillance continue** : Les entreprises doivent mettre en place des mécanismes de veille pour suivre les évolutions réglementaires et les meilleures pratiques dans le domaine de l'intelligence artificielle. Cela inclut la surveillance des incidents, des jurisprudences, et des nouvelles législations pour s'assurer que leurs pratiques restent conformes aux exigences de la loi sur l'intelligence artificielle.

En adoptant ces mesures, les entreprises peuvent non seulement se conformer à la loi sur l'intelligence artificielle, mais également renforcer la confiance des consommateurs dans leurs produits d'intelligence artificielle.

Et maintenant ?

Comme nous pouvons le voir, la loi présente une vision bien plus large que la seule notion de contrainte. La présence de la notion de laboratoire s'avère fortement utile pour permettre aux différents secteurs de continuer à faire de la recherche et du développement et seule la mise en production s'avère plus contraignante.

Comprendre ce point permettra d'avoir des arguments pour favoriser la confiance des utilisateurs de vos systèmes. Dans tous les cas, les exigences se doivent d'être comprises et respectées, et ce en fonction d'un calendrier assez clair :

- 2 août 2024 : Entrée en vigueur générale de la loi sur l'intelligence artificielle.
- 2 février 2025 : Interdiction de certaines pratiques d'intelligence artificielle, comme l'exploitation des vulnérabilités.
- 2 août 2025 : Application des réglementations sur les modèles d'intelligence artificielle à usage général.
- 2 août 2026 : Application générale des règles sur les systèmes d'intelligence artificielle à risque élevé.
- 2 août 2027 : Application des règles pour les composants de sécurité classés comme systèmes à risque élevé.

Si vous prévoyez d'utiliser des systèmes d'intelligence artificielle, il est ainsi recommandé

La collaboration avec les autorités réglementaires peut également faciliter l'adaptation aux futures évolutions de la législation.

de rapidement identifier et classer ceux-ci afin de s'assurer de répondre aux exigences de la loi.

En parallèle, la lecture de la loi sur l'intelligence artificielle permettra de clarifier les exigences. Celle-ci est accessible à l'adresse : <https://artificialintelligenceact.eu/fr/ai-act-explorer/>.

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



« 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**

DECouvrez VOTRE **GUIDE D'ACHATS**
DE REFERENCE **POUR L'EQUIPEMENT**
INFORMATIQUE DE VOTRE ENTREPRISE

TPE • PME • GRANDS COMPTES



Toutes les nouveautés,
les dernières tendances IT
à découvrir dès maintenant
en scannant ce QR code.



Ralentissement économique ET BUDGETS CYBERSÉCURITÉ

La sécurité IT est devenue une composante significative des budgets des DSI. Plus la digitalisation des entreprises et des métiers avance, grâce à la numérisation des usages et pratiques en entreprise, la multiplication des applications, de l'e-commerce, du cloud sous ses différentes déclinaisons ou compréhension (mode SaaS applicatif, hébergement externalisé des données et des traitements, universalité des accès, etc.), plus les entreprises deviennent vulnérables aux attaques et incidents de cybersécurité, de continuité de services, de vols de données, etc.



Une évolution plus modeste à 8% en moyenne pour 2024

Les temps sont difficiles, le contexte économique incertain pourrait conduire les entreprises à modérer leurs investissements, et la cybersécurité pourrait être concernée également. Les contraintes budgétaires sont plus fortes mais même dans ce

climat, les budgets SSI sont en croissance. Certes à moindre niveau tel que publié dans la dernière étude annuelle du cabinet de conseil IANS, avec une évolution plus modeste à 8% en moyenne en 2024. Mais légèrement mieux qu'en 2023 quand le même cabinet indiquait 6% de croissance. C'est vrai que nous sommes bien en deçà des 16% de croissance annuelle des années 2021 et 2022.

Avoir une croissance moindre mais présente est fondamentalement sain, et suivant une tendance économique générale, plus sain pour calmer la surchauffe salariale des dernières années - à ne pas oublier que les coûts salariaux constituent le premier poste des budgets de sécurité avec 37% des dépenses.

Une stabilité des équipes

Presque la moitié des RSSI interrogés par IANS prévoit une stabilité de leurs équipes. Le secteur a aussi bénéficié de nombreuses promotions de diplômés, toute université ou école d'ingénieurs ayant mis en place des cursus de formation en cybersécurité. Certainement que le paroxysme de la crise des talents est passé, en attendant le prochain cycle tout proche, celui des départs en retraite de la première génération des RSSI et professionnels de la SSI. Il serait d'ailleurs très intéressant de se pencher sur une évaluation de ces prochains départs en retraite centrés sur 2030, plus ou moins 2 ans...

Pour les solutions et produits, le mot d'ordre est d'abord exploitons à fond, tirons profit, des solutions acquises, qui porteuses de plusieurs fonctionnalités de sécurité sont assez souvent sous-exploitées.

L'étude IANS a identifié les facteurs favorisant la hausse des budgets : les cyberattaques entraînent en moyenne une hausse de 26% des budgets, les exigences de conformité légale et réglementaires représentent une hausse moyenne de 17%.

Le binôme DSI - RSSI

Le gros moteur de croissance des budgets de cybersécurité est surtout lié à l'importance vitale de l'IT, de plus en plus vulnérable, de plus en plus critique, de plus en plus identifiée et comprise à sa juste importance par les directions générales des entreprises de toutes tailles, par les directions métier et business.

Les Comex sont fortement sensibilisés, et les DSI sont devenus les premiers porteurs des besoins et budgets en cybersécurité.

Les incidents cyber de plus en plus impactants et médiatisés, permettent aujourd'hui à un CEO ou Président d'une entreprise de comprendre vite et mieux l'importance de l'investissement en cybersécurité. Les Comex sont fortement sensibilisés, et les DSI sont devenus les premiers porteurs des besoins et budgets en cybersécurité.

Le binôme DSI - RSSI, articulation qui fonctionne mieux que jamais en entreprise, permet de corréler la valeur de l'entreprise avec les investissements cybersécurité, et est devenu un moteur performant en investissement et allocation budgétaire en cybersécurité. C'est cette réalité qui a permis la croissance de la part cybersécurité dans le budget informatique global dépassant aujourd'hui les 14%.

> Par *Théodore-Michel VRANGOS*, Cofondateur et Président d'I-TRACING



« 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 mensuel IT Pro Magazine.

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

 iTPro.fr

EasyVista ACCÉLÈRE SA CROISSANCE EN FRANCE ET À L'INTERNATIONAL

Entreprise française spécialiste de l'ITSM / ITOM, présente en Europe et aux Etats-Unis, EasyVista entend amorcer un nouveau virage et accélérer sa croissance. Stratégie, ambitions, développement, feuille de route 2024 mais aussi tendances du marché. Rencontre avec Patrice Barbedette, CEO & Président d'EasyVista pour évoquer ces sujets.



Avec plus de 35 ans d'existence, on peut dire que l'histoire d'EasyVista accompagne l'histoire de l'Informatique. Ainsi, l'entreprise offre aux Directions Informatiques et aux différents métiers des DSI (infrastructure, production, client final, support IT, opérationnel...) une plateforme intégrée pour superviser et gérer les datacenters et les infrastructures jusqu'à s'assurer de la satisfaction du end user dans son utilisation de l'informatique, « nous mesurons le ressenti du end user sur son poste de travail avant que le problème n'arrive ». La DSI déploie donc tout ou une partie de cette plateforme pour répondre aux besoins des métiers, gérer ses infrastructures et l'aider à faire du ticketing par exemple, « nous aidons l'IT à procéder plus vite dans une logique intégrée pour être plus efficace ».

Avec 400 collaborateurs environ et plus de 40 partenaires, EasyVista réalise 35% de son CA aux

Etats-Unis, un peu moins de 50% en France, et le reste dans des pays européens comme l'Angleterre, l'Espagne, l'Italie, le Portugal, « nous sommes un acteur français avec un large déploiement à l'international, et une vraie méthode de déploiement hors de France ».

Feuille de route 2024

Arrivé fin 2021 aux manettes de l'entreprise, Patrice Barbedette a pour objectif de doubler l'ARR - Annual Recurring Revenue – qui était alors de 23 millions. Objectif réussi fin 2023 avec un peu plus de 50 millions d'ARR « grâce à une croissance organique en moyenne sur les deux dernières années de plus de 25 % et trois acquisitions, Goverlan, Coservit, Itexis début 2022. Sur Coservit, nous avons fait plus de 150 % de croissance de l'ARR et sur Goverlan, plus de 70% de croissance de l'ARR sur deux ans ». Une nouvelle phase de développement s'est donc ouverte.

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



PATRICE BARBEDETTE

Un modèle d'activation d'accélération de l'activité commerciale et de satisfaction des clients est adopté à la fois pour EasyVista (partie historique) et les sociétés acquises, « nous avons augmenté notre taux de renouvellement de plus de 10 points. Ce double effet, capture de nouveaux clients et amélioration de notre relation client est essentiel. Un des objectifs était de passer d'une culture centrée produit à une culture centrée client, customer centric. De plus, on affiche un rating (Gartner Peer Insights) de 4,9/5 par nos clients, et 92% recommanderaient la solution EasyVista ».

Côté feuille de route 2024, « nous sommes sur le même modèle, et en route pour la prochaine étape qui devrait nous emmener fin 2026 à 100 millions d'euros, nous sommes bien en ligne sur cet objectif avec les mêmes leviers, la satisfaction clients pour augmenter les taux de renouvellement, la conquête de nouveaux clients et les acquisitions éventuelles ». L'entreprise affiche un bon niveau de profitabilité.

Tendances du marché

Si le marché de l'IT Service Management et de l'Enterprise Service Management est un marché établi, « en revanche, il est soumis en permanence à de gros changements, de grosses évolutions et accélérations. Bureautique, Internet, SaaS, Cloud, IA, Covid / Télétravail... pour une direction informatique, à chaque fois, ces innovations et contraintes entraînent plus de risques cyber, d'impatience, de complexité mais font évoluer ce marché ». L'IA est une opportunité, un accélérateur sur ce marché et ouvre de nouvelles perspectives.

Sur ce marché, le taux de croissance annualisé sur les 5 dernières années est de 13%, « nous sommes sur un taux de croissance plus élevé que le taux moyen du marché ».

Positionnement & Souveraineté numérique

« Dans notre positionnement, nous progressons également sur des remplacements de clients,

BMC et ServiceNow. En termes de gammes, nous parvenons ainsi à intéresser des comptes plus importants. Si notre segment idéal s'étend de 2000 – 3000 collaborateurs à 30 000 collaborateurs, nous pouvons aller au-delà de 30 000 et gagner des comptes, Aéroports de Paris par exemple ».

EasyVista se présente comme une vraie alternative, notamment dans un contexte de souveraineté numérique « au-delà des administrations, nous avons des collectivités territoriales, des OIV. Notre offre SecNumCloud coconstruite avec OutScale permet d'offrir à nos clients un environnement sécurisé et une garantie de souveraineté numérique de non extra territorialité des données ». Si l'objectif pour la France est de protéger ses administrations, EasyVista apporte une vraie réponse par rapport aux acteurs américains.

EasyVista se présente comme une vraie alternative, notamment dans un contexte de souveraineté numérique.

En effet, en réponse aux lois FISA (Foreign Intelligence Surveillance Act) des Etats-Unis, « le renforcement et le prolongement de ces lois, sous couvert de sécurité nationale, permettent de récupérer les données des clients des Tech US », l'Europe crée ce concept de souveraineté numérique, protecteur des données personnelles et encadre les entités du secteur public pour se protéger contre l'extraterritorialité des données et choisir des acteurs qui vont garantir un Cloud souverain. « Nous avons beaucoup d'acteurs dans cette sphère publique, par exemple les Ministères des Finances, de la Justice, des Affaires Sociales, des grandes métropoles de régions, des conseils départementaux, et nous constatons qu'ils portent de plus en plus d'attention à ces sujets de souveraineté numérique ».

Du côté de l'Environnement !

EasyVista s'est donné les moyens d'aider sa DSI à mesurer l'empreinte carbone de son IT. « On ne peut améliorer que ce qu'on peut mesurer, en ce sens, nous aidons nos clients à mesurer l'empreinte carbone de leur IT, charge à eux de mettre en place des plans en fonction de leurs stratégies. De notre côté, nous avons relocalisé nos datacenters sur des régions du monde où l'électricité est propre, non carbonée. Et dans notre consommation de l'informatique, sur des sujets non critiques, nous utilisons de l'IT reconditionnée ».

Avant de proposer aux clients, EasyVista entend déjà procéder pour l'entreprise « en cochant des critères ESG sur l'environnement et la diversité ».

> Par Sabine Terrey



Top 10 des technologies émergentes

L'innovation accélérée de l'IA enclenche des avancées : IA générative pour le contenu visuel, IA générative pour le langage, TuringBots et sécurité IoT.

Ces technologies fourniront le retour sur investissement le plus immédiat pour les entreprises en 2024 et au-delà. Mais quand réaliser ces investissements ? Forrester répertorie les technologies émergentes en fonction des bénéfices.

Avantages au cours des deux prochaines années

• IA générative pour le contenu visuel

Modèles avancés d'apprentissage automatique qui génèrent des images ou des vidéos à partir d'invites textuelles, audio ou vidéo, cette technologie aidera à générer du contenu visuel pour le marketing, les expériences et les produits.

• IA générative pour le langage

L'IA générative pour le langage offre déjà de la valeur dans le support client et la création de contenu, et avance à un rythme exponentiel.

• TuringBots

Accélérés par les progrès de l'IA générative pour le langage, ces robots logiciels optimisés par l'IA aident les développeurs à créer des applications qui offrent plus qu'une simple génération de code.

• Sécurité IoT

La prolifération des appareils connectés conduit à une explosion exponentielle des attaques, augmentant l'importance de la sécurité pour les appareils IoT.

Avantages au cours des deux à cinq prochaines années

• Agents IA

Le rôle des assistants de travail autonomes ou agents IA s'est étendu au-delà du back-office et de l'assistance aux employés à l'automatisation avec le client. Ces agents IA deviendront sophistiqués pour mieux comprendre et répondre aux nuances et au contexte.

• Mobilité autonome

Cette technologie accélèrera les collaborations entre les écosystèmes de transport commercial et urbain pour orchestrer des expériences de mobilité personnalisées tant pour les particuliers que pour les entreprises.

• Intelligence Artificielle en périphérie

Les capacités avancées IA en périphérie telles que l'apprentissage automatique localement sur un périphérique ne sont pas courantes, même si des éléments fondamentaux comme les modèles de fondation Apple deviennent disponibles.

• Sécurité quantique

Cette technologie révisera les systèmes de sécurité pour le calcul sur site et sur cloud, l'infrastructure de stockage et de réseau, les logiciels commerciaux prêts à l'emploi, les offres de logiciels commerciaux en tant que service et les logiciels construits en interne.

Valeur tangible dans au moins cinq ans de plus

• Réalité étendue (XR)

Seulement 8 % des adultes en ligne aux États-Unis possèdent un casque de réalité virtuelle, et seulement 16 % ont utilisé un appareil ou une application de réalité augmentée. Alors que la XR progresse dans la formation et l'intégration, les entreprises sont peu enclines à investir dans ces outils jusqu'à ce qu'elles voient une large adoption.

• Technologie Zero Trust Edge (ZTE)

La technologie ZTE protégera les télétravailleurs, les points de vente et les succursales avec une sécurité locale intégrée, peu de véritables solutions ZTE existent aujourd'hui, et les appareils existants ajoutent une complexité de gestion supplémentaire.

Source Forrester - *The Top 10 Emerging Technologies In 2024*

DE LA VISIBILITÉ PAR LES WORKBOOKS

Dans sa bonne pratique du Cloud Azure, il faut savoir exposer facilement les informations importantes. Et il faut également profiter de la facilité qu'il y a à pouvoir profiter d'un niveau d'informations très élevé.



Car s'il y a bien un secteur où le Cloud est imbattable, c'est celui de la collecte des informations de tout type et par extension, de la facilité qu'il y a à les afficher et à les consulter.

Et pour cela, il y a une ressource Azure nommée le Workbook. C'est un outil interactif qui permet de

visualiser et d'analyser les données de l'environnement en temps réel. Il offre de la flexibilité et la possibilité de créer des rapports personnalisés avec des graphiques, des tableaux et du texte, tout en combinant diverses sources de données. Idéal pour prendre des décisions éclairées ou pour avoir, en quelques tableaux, une bonne vue de ses environnements.

EX PO

img
wstore
GROUP STORE

LE RENDEZ-VOUS
DES PROFESSIONNELS DE L'IT
12^{ÈME} ÉDITION

**Venez rencontrer et échanger avec plus de 120 marques
exposantes sur les dernières nouveautés
et tendances informatiques.**

MOBILITÉ

CLOUD

SÉCURITÉ ET RÉSEAUX

INFRASTRUCTURE

SERVICES

MODERN WORKPLACE

E-PROCUREMENT

LOCATION

IMPRESSION

**RETROUVEZ-NOUS
AU PARIS EVENT CENTER
JEUDI 21 NOVEMBRE 2024**

9h30 - 18h00

**20, avenue de la Porte de la Villette
75019 Paris**

**INSCRIVEZ-VOUS
DÈS MAINTENANT**



Si la possibilité de créer des rapports personnalisés est très intéressante, elle demande un peu plus d'efforts.

Comme il existe déjà dans le portail un grand nombre de Workbooks prédéfinis, c'est-à-dire prêts à l'usage, il faut les connaître et profiter de ce qu'ils proposent. Certains sont très utiles, encore faut-il savoir les identifier.

Car si les Workbooks ont pas mal de qualités, ils restent répartis un peu partout dans le portail. Il n'y a pas d'endroit centralisé où est proposé tout ce qu'il existe. Et c'est donc pratiquement sur chaque service qu'il va falloir partir à la découverte des « pépites », c'est-à-dire de ce qui est le plus utile en termes de visualisation.

Une parenthèse avant de passer à la suite. Certains sont alimentés par défaut, comme celui présenté plus bas, le *Service Retirement (Preview)*. D'autres, pour avoir des informations à exposer, ont besoin que les diagnostics avancés soient activés sur la ressource.

Click 'Add Diagnostic setting' above to configure the collection of the following data:

- Azure Firewall Application Rule (Legacy Azure Diagnostics)
- Azure Firewall Network Rule (Legacy Azure Diagnostics)
- Azure Firewall DNS Proxy (Legacy Azure Diagnostics)
- Azure Firewall Network Rule
- Azure Firewall Application Rule
- Azure Firewall Nat Rule
- Azure Firewall Threat Intelligence
- Azure Firewall IDPS Signature
- Azure Firewall DNS query
- Azure Firewall FQDN Resolution Failure
- Azure Firewall Fat Flow Log
- Azure Firewall Flow Trace Log
- Azure Firewall Network Rule Aggregation (Policy Analytics)
- Azure Firewall Application Rule Aggregation (Policy Analytics)
- Azure Firewall Nat Rule Aggregation (Policy Analytics)
- AllMetrics

Sans cela, pas de données collectées = pas de données à exposer, et au final, un workbook inutile. Comme cela est le cas avec le *AzureFirewalls Structured Logs* également présenté ci-dessous.

A retenir donc, les workbooks sont prêts à l'emploi, mais il y a quelques prérequis pour certains d'entre eux avec l'activation des diagnostics avancés. En ayant toujours à l'esprit que l'activation des logs va entraîner un coût supplémentaire. Puisque ces informations sont majoritairement stockées dans des puits de log (logs analytics) qui sont facturés au volume d'ingestion de données.

Les workbooks sont prêts à l'emploi, mais il y a quelques prérequis pour certains d'entre eux.

C'est donc une décision réfléchie que d'activer un niveau de logs supplémentaire. Attention de bien prendre le temps de cette analyse, collecter pour ne pas afficher est une pratique coûteuse.

Les workbooks prédéfinis

Les workbooks prêts à l'usage, comme expliqué dans l'introduction, il y en a « un peu de partout ». Ce qui fait que l'on passe très facilement à côté des plus importants. Je vais présenter dans la suite de cet article un TOP de ce qui est le plus utile aux clients.

C'est un retour d'expérience qui peut donner quelques idées et quelques pistes sur l'apport que cela peut représenter en entreprise. Et qui peut faciliter la gestion de ses environnements.

Direction **Advisor** dans le portail, puis **Workbooks** dans le menu. Ici, deux workbooks. Le premier se nomme *Service Retirement (Preview)*.

Service Name	Retiring Feature	Retirement Date	Resource	Actions
Azure Service Bus	Support for Apache Spark 3.2	2024-07-08	None	Learn more
All Management	Compute Platform (v1)	2024-08-31	None	Learn more
App Service	App Service Environment (v1)	2024-08-31	None	Learn more
Azure Cache for Redis	Classic	2024-08-31	None	Learn more
Azure Logic Apps	Integration Services Environment (v1)	2024-08-31	None	Learn more
Azure Update Manager	Update Management	2024-08-31	None	Learn more
Cloud Service (Classic)	Classic	2024-08-31	None	Learn more
HDInsight	4 Series	2024-08-31	None	Learn more
Machine Learning Studio (Classic)	Classic service	2024-08-31	None	Learn more

Même si Microsoft informe régulièrement par mail ses clients des futures dépréciations, une vue agrégée sur cette partie est très intéressante. Date de retrait, type d'actions à envisager pour la remédiation, type de service, c'est parfait pour assurer le maintien en condition opérationnelle (MCO) et pour planifier les opérations d'upgrade ou de remplacement du service. Le filtre de vue vont simplifier le travail en affichant uniquement les services qui concernent vos abonnements Azure.

Le second, *Cost Optimization (Preview)*, porte bien son nom puisqu'il donne de précieuses informations sur les économies réalisables sur les environnements. Un peu de tout dans celui-là, avec également des filtres de vue avancée qui permettent la sélection de tout un tas de critères liés au coûts (et surcoûts) des services. Voilà pour ce que vous trouverez sur la page du service **Advisor**.

Dans le portail de la ressource **Backup Center**, un workbook assez différent, auquel on accède dans le menu en sélectionnant **Backup Reports**. Pour rappel, il n'y a pas un, mais deux services de Backup sur Azure. *Backup Vault* et *Recovery Service Vault*. Pouvoir centraliser l'ensemble des résultats des sauvegardes (et d'autres infos comme celles liées

aux coûts de stockage engendrés par ces backups ou aux alertes de backup) est important. Attention, il faut là aussi que les diagnostics avancés soient activés sur vos services de backup. Par défaut, ce n'est pas le cas.

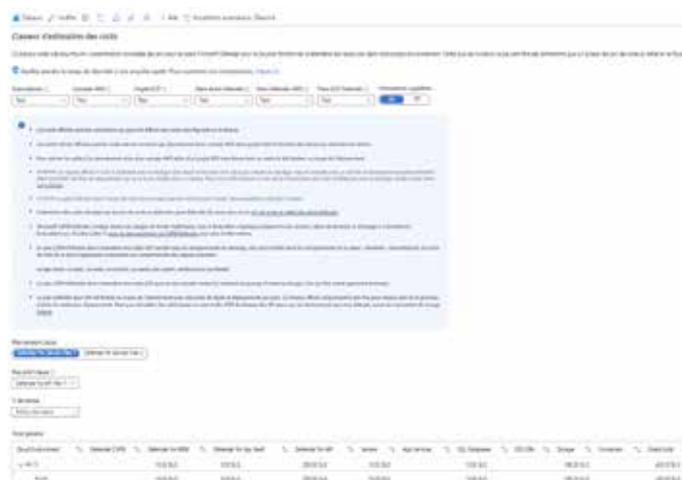
Direction maintenant la page du service **Microsoft Defender for Cloud** et le workbook *Cost Estimation*. Il est utile pour fournir une estimation consolidée des prix pour les plans Microsoft Defender pour le cloud **en fonction de la télémétrie des ressources dans votre propre environnement**.

C'est donc une projection des coûts si le service est activé, dans le contexte des ressources existantes. Autant dire que c'est une mine d'or. Il n'est jamais facile, même avec la calculatrice ou avec les pages d'informations sur le prix des ressources Azure de se projeter sur les dépenses pour l'activation d'un nouveau service.

Mais quand ces coûts sont liés à la télémétrie des ressources, c'est un peu mission impossible. Quelques exemples de prix qui rendent ce type de calcul extrêmement complexe voire impossible :

Microsoft Defender for SQL outside Azure €0.014/ Instance/vCore/hour ou *Microsoft Defender for APIs Plan 1* €0.2462 per subscription/hour up to 1 million API calls.

Autant dire que le *Cost Estimation* est une aide précieuse !



Autre élément de suivi une page dédiée aux principaux éléments des réseaux virtuels que l'on trouve dans le portail **Azure Monitor**, dans

le menu *Insights / Networks*. Sont affichées des informations sur l'état de santé des réseaux, des informations de connectivité ou de trafic. Là aussi, c'est une vue consolidée, un peu la boîte à outils de l'administrateur réseau et des équipes de support. Une seule vue, toutes les informations.



Pour finir, il y a des ajouts assez réguliers avec des nouveautés. Par exemple, toujours dans le portail **Azure Monitor**, le *Azure Monitor Migration Helper*, qui aidera sur la migration en cours et le passage au nouvel agent de machine virtuelle. Utilisation éphémère, mais qui accompagne un sujet particulier, le temps d'un déploiement, de façon plus temporaire.

Les workbooks publics

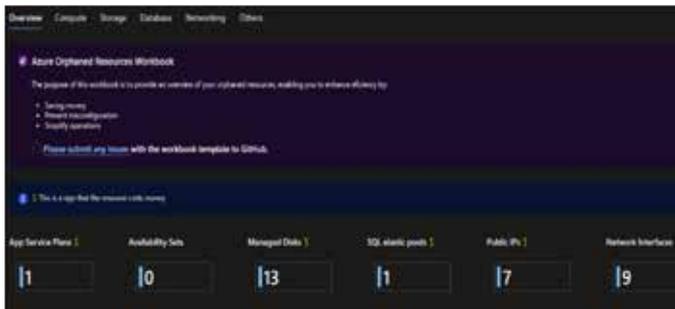
Là aussi, le choix est vaste, il faut « fouiller » un peu pour trouver des sujets complémentaires ou plus spécifiques. S'il faut en retenir un seul, c'est à mon avis l'*Azure Orphaned Resources v2.0* que l'on trouve sur Git. Il sert à identifier les ressources dites « orphelines ». Une ressource orpheline pour Azure, c'est une ressource qui n'est plus utilisée mais qui est encore présente quelque part dans l'environnement.

Certaines de ces ressources sont gratuites et le nettoyage fait partie du maintien en condition opérationnelle.

Par exemple, un disque managé qui n'est plus attaché à une machine virtuelle et qui a été oublié lors de la suppression de la machine. Un App Service Plans qui n'héberge pas de site et qui est donc très certainement inutile. Ou une adresse IP publique qui n'est plus attachée à aucune ressource.

Certaines de ces ressources sont gratuites et le nettoyage fait partie du maintien en condition opérationnelle. C'est un peu l'hygiène du Cloud. D'autres sont facturées même si elles ne sont plus utilisées car elles sont encore provisionnées et représentent un surcoût inutile.

Ce que montre parfaitement le workbook avec une petite icône \$ qui met en avant une ressource facturée. Des filtres sont présents pour mener directement sur la ressource en question et pour procéder aux opérations de nettoyage.



Voilà pour quelques-uns des workbooks les plus utiles et les plus efficaces !

Ce qu'il faut retenir, c'est au fil de l'eau que l'on découvre toutes ces pépites. Il n'y a pas (pour l'instant ?) de menu dédié à l'affichage des workbooks, de manière centralisée, c'est donc la curiosité qui poussera à découvrir ici et là les plus adaptés.

Personnaliser ses workbooks

Si tout ce qui a été présenté et tout ce qui existe sur le portail et sur le Git ne répondent pas aux besoins (ça arrive), alors il faut créer et se tourner vers les workbook personnalisés.

Les workbooks sont une source inépuisable d'information.

C'est un peu plus de travail mais c'est aussi la possibilité de déployer ce qui convient, avec de la finesse. On peut démarrer de rien, mais on peut aussi à minima s'appuyer sur une trame existante. Il en existe une que l'on trouve encore une fois dans le portail **Azure Monitor**. Elle se nomme *Resource Picker*. C'est un menu de filtrage par défaut, avec des ascenseurs de sélections de type *Abonnement*, *Groupe de ressources* et *Ressources*. Reste à passer en édition pour ajouter les requêtes KQL, les métriques et autres sources de visualisation pour habiller ce workbook avec les informations souhaitées.

Les workbooks sont une source inépuisable d'information !

Pour résumer, un bon point de départ en 3 étapes

- 1 / Le workbook est un outil interactif utilisé dans le portail Azure pour créer des rapports visuels, dynamiques et partagés sur les données de surveillance et de diagnostic. Ce sont des tableaux de bord super flexibles qui aident à mieux comprendre et gérer un environnement Azure.
- 2 / L'affichage de certaines données est lié à des collectes complémentaires qui ne sont pas activées par défaut. Il faut activer les diagnostics avancés sur la ressource afin de pouvoir exploiter pleinement les rapports.
- 3 / Il est possible avec un peu plus d'efforts de créer ses propres workbooks afin d'afficher des informations personnalisées.

> *Thierry Bollet, MVP Azure, Architecte Azure Référent – Exakis Nelite*



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

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

27-28 NOVEMBRE 2024 | PARIS, PORTE DE VERSAILLES

TECH SHOW

PARIS

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

Tech Show Paris réunit les leaders des industries Cloud, DevOps, Cyber, Data & AI, et Data Centre, avec pour objectif de s'instruire, partager, innover et générer des opportunités. Venez rencontrer vos pairs, optimiser vos coûts et votre temps, et vous informer sur les dernières tendances technologiques.

Au programme : l'IA, l'éco-responsabilité, la diversité et l'innovation seront au cœur de l'évènement !

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



RETIREZ VOTRE BADGE GRATUIT

TECH SHOW
PARIS
techshowparis.fr

REGROUPANT



CLOUD EXPO
EUROPE



DEVOPS
LIVE



CLOUD & CYBER
SECURITY EXPO



BIG DATA
& AI WORLD



DATA CENTRE
WORLD

ORGANISÉ PAR



L'ÉVÈNEMENT DÉDIÉ AUX PROFESSIONNELS DE LA TECH EN FRANCE

Pari réussi pour Sightness

« DU CONSEIL À L'ÉDITION SAAS ! »

Comment passer du conseil à l'édition SaaS ? Comment repenser son business model ? Quels sont les défis ? Autant de questions ! Entretien avec Alain Bori, Co fondateur & CEO Sightness pour évoquer ce choix stratégique non sans risque, l'anticipation du besoin du marché, le virage digital et la croissance de l'entreprise. Retour sur la transformation réussie de cette FrenchTech.



Un challenge !

Fin 2005, est créée la société bp2r, cabinet de conseil en transport de marchandises avec une vingtaine de consultants, « notre activité se trouvait effectivement sur une niche, le consulting spécialisé du transport de marchandises ».

Ayant bien conscience à l'époque que le domaine du conseil est cyclique, encore plus en période d'instabilité, la recherche d'une activité récurrente

pour limiter les risques de fluctuation est entreprise. « Si le conseil en général n'est pas un domaine où il est facile d'avoir de la visibilité, aujourd'hui l'émergence de l'Intelligence Artificielle va impacter ces métiers et la taille de l'entreprise entre en jeu, ma réflexion est forte sur ces sujets. ».

Alors, quelques années en arrière, l'idée germe, « pourquoi ne pas mettre sous contrôle les factures des transporteurs des clients pour optimiser leur organisation transport ? ».

CBC

CYBER SECURITY Business Convention

Le salon PRO de la Sécurité Numérique

JEUDI 28 NOVEMBRE 2024 TOULOUSE - MEETT



VOTRE RDV CYBER DE RÉFÉRENCE :

◆ 200 exposants

◆ + de 40 prises de parole

Conférences, masterclass, pitches, ateliers et démonstrations

◆ Thématiques variées

NIS2, sureté en aéronautique, gestion de crise cyber, données sensibles en santé, cybersécurité des programmes spatiaux, etc.

◆ Focus sur l'Intelligence Artificielle

Risques cyber et enjeux éthiques, compliances et réglementations, évaluation d'un projet face à l'IA ACT, sensibilisation aux enjeux de l'IA

MAIS AUSSI :

◆ Simulation

Cellule de crise cyber

◆ Recrutement

Animation reverse recruiting

◆ Remise de trophées Cyberstar

◆ Challenge Capture The Flag

Organisé par Devensys Cybersecurity, en partenariat avec le Commandement de l'Espace et le Comcyber



Inscrivez-vous gratuitement dès maintenant sur

cbc-convention.com

Suivez-nous  

Organisé par :

Sponsor gold :

Sponsors bronze :

Partenaires :



Le virage digital

A partir de cette idée, le pas est franchi « *comme nous maîtrisons le sujet, nous lançons notre prestation de contrôle, et pour passer à l'échelle, nous investissons sur les hommes et femmes informaticiens, jusque-là nous avons plutôt des ingénieurs généralistes* ».

Tout s'enchaîne rapidement avec une première levée de fonds de 500 000 euros auprès de Business Angels en 2017, et une levée de fonds de 5 millions en 2019 auprès de Calcium Capital, « *pour nous permettre de passer du conseil à l'édition d'une solution technologique, en structurant une équipe, recrutant des informaticiens et d'autres fonctions comme les ventes, l'accompagnement client, le customer success. Le virage se fait donc réellement en 2019* ».

Ce virage s'achève en 2023 puisque l'entreprise vend son activité historique de consulting à PwC France, « *à partir de ce moment-là, nous sommes passés d'un cabinet de conseil à une entreprise mixte conseil et tech pour aujourd'hui être une entreprise complètement transformée, nous sommes un éditeur de solution informatique en mode SaaS dans le domaine de transport de marchandises* ».

Les défis

Evidemment, modifier l'activité de l'entreprise est un défi en lui-même qui ne se fait pas sans risque d'autant que « *pendant les 10 premières années, l'entreprise avait une population d'ingénieurs généralistes, assez homogène. Nous avons donc recruté des fonctions différentes et il a fallu veiller à ce que tout se passe bien. Si l'activité conseil nous a aidés à convaincre les premiers clients, la bonne cohésion entre les équipes était essentielle* ». Le premier défi fut le recrutement, « *défi humain donc, savoir recruter des personnes ayant le même ADN, le même état d'esprit que les consultants déjà en place, des valeurs communes à celles existantes, et savoir recruter des profils nouveaux comme pour les Sales dans l'édition de logiciels* ».

Virage totalement réussi ! Retour d'expérience instructif sur ce changement de métier.

Autre défi, la distance. Si l'activité consulting a toujours été basée à Paris, l'activité édition de logiciel fut basée au début à l'île Maurice. Aujourd'hui, plus de 100 collaborateurs se répartissent entre les bureaux parisiens et ceux de l'île Maurice « *avec des équipes d'informaticiens sur les deux sites, nous avons appris à fonctionner sur deux continents* ».

Créer un business model différent est un autre défi, et non des moindres « *Pour le conseil, on parle en missions, on évalue des jours/hommes et on pilote.*



ALAIN BORI

Pour l'édition de logiciel, ce sont des fonctionnalités, des abonnements annuels, on a donc appris à tarifier et à fonctionner différemment ».

Mettre son expertise conseil au cœur de la plateforme digitale

De l'expertise de l'entreprise acquise dans le conseil à savoir l'amélioration de la performance transport des clients, sur l'optimisation des coûts, l'amélioration de la qualité et la diminution des émissions de carbone, résulte un fort savoir-faire sur ces trois domaines. « *Nous avons transformé ces compétences et notre savoir-faire conseil dans une plateforme digitale et avons repris ces trois axes de performance. Aujourd'hui, la plateforme Sightness permet aux clients de mieux maîtriser leurs coûts et les dépenses transports (avec la fonctionnalité de contrôle des transporteurs), de maîtriser la traçabilité, la qualité et la performance des transporteurs, et de maîtriser la partie carbone, en identifiant les principaux foyers d'émission pour les réduire* ».

Outre l'expertise, l'entreprise a pu s'appuyer sur une base installée de clients « *qui reconnaissant notre compétence sur le conseil, nous ont fait confiance sur la partie digitale. Ces facteurs sont fondamentaux et déterminants dans notre cheminement de devenir éditeur de logiciel SaaS* ».

Virage totalement réussi ! Retour d'expérience instructif sur ce changement de métier, « *c'est possible, même si cela reste un challenge. Autre point, cette transformation ne s'est pas faite aux dépens des salariés du conseil, puisqu'ils ont intégré un des plus grands groupes de conseil du monde, c'est une fierté en tant que chef d'entreprise et manager* ».

Si Sightness affiche aujourd'hui une croissance de 40% et compte parmi ses clients plus de 100 industriels et distributeurs du Fortune 500 à travers le monde, elle projette d'ouvrir un bureau en Asie dans les prochains mois

> Par Sabine Terrey



Faire comprendre le risque cyber !

Comprendre les risques cyber est une priorité. Et pourtant, selon 35 % des petites entreprises (Monde), les cadres supérieurs ne perçoivent pas les cyberattaques comme un risque important.

Alors, comment faire en sorte que les dirigeants soient au courant des menaces pesant sur leur entreprise ? Riaz Lakhani, CISO chez Barracuda Networks évoque trois réflexions à mener pour faire comprendre le cyber risque au sein de l'entreprise « Les RSSI doivent être des passeurs d'informations. Ils doivent être capables de sensibiliser les personnes à tous les niveaux de l'entreprise, de les aider à comprendre et à adopter des politiques de sécurité, des réponses aux incidents, etc. Le temps passé à écouter et à apprendre de ses principales parties prenantes est l'un des meilleurs investissements que l'on puisse faire ».

Trois profils de collaborateurs avec qui tout RSSI devrait discuter des sujets majeurs

- **Les collègues IT (ingénieurs, développeurs, chercheurs en sécurité)**

Dans le cadre d'une astreinte, ce sont les personnes à appeler à 2 heures du matin pour une demande urgente. Il est impératif d'établir des relations solides et de comprendre leur point de vue et perception de la sécurité.

- **Les cadres supérieurs**

La programmation de réunions régulières avec les responsables des principaux services liés à des risques critiques (service ingénierie, finance et légal) permettront d'examiner chaque situation. Elles contribueront à savoir comment évolue le paysage des menaces et de la sécurité, et ce que cela signifie pour l'entreprise, ce qu'il faut mettre en place. Ainsi, les actions à suivre pour pallier les risques encourus seront plus claires, par exemple le respect des règles de conformité.

- **Les dirigeants de l'entreprise**

Chaque conseil d'administration est différent. Il faut donc apporter le plus de connaissances possibles aux personnes présentes et s'assurer que le discours et les concepts présentés soient compréhensibles. Il faut capter leur intérêt et leur attention.

« Les responsables de service et dirigeants doivent se poser cette question : Comment pouvons-nous être résilients dans un monde où les cyber-incidents sont fréquents, imprévisibles et potentiellement destructeurs ? » Eric Heddeland, VP EMEA Southern Region chez Barracuda. « La conversation doit porter sur les principaux risques que court l'entreprise – comme au travers de la supply chain par exemple – et sur les conséquences d'une attaque réussie. Le conseil d'administration veut savoir si son RSSI a réfléchi sur la manière de repousser les acteurs malveillants, mais aussi à la façon de réagir et de se remettre d'un incident, afin que les activités puissent se poursuivre et que l'entreprise ne soit pas menacée. »

Source The CISO script: How to talk to business leaders about security risk - Barracuda Networks

Industrie manufacturière : LA LÉGISLATION SUR LE DROIT À LA RÉPARATION IMPOSE UNE REFONTE COMPLÈTE DE LA CHAÎNE DE VALEUR

Le Parlement européen a récemment adopté une directive sur le « droit à la réparation » dont l'objectif est de rendre la réparation d'articles défectueux ou cassés à la fois « plus simple et plus intéressante » pour les consommateurs. Jean-Roland Brisard, VP Solution Consulting, Infor partage son expertise sur le sujet.



Si la directive est centrée sur l'électroménager et les appareils électroniques grand public, les mêmes exigences concernent de nombreux secteurs confrontés à l'application de nouvelles réglementations, à l'évolution des préférences des consommateurs et à la nécessité de mieux gérer leurs ressources.

À mesure qu'elles remplaceront une approche linéaire de la production et de la vente par un processus de maintenance et réparation à long terme, les entreprises devront prendre d'importantes décisions stratégiques et réfléchir aux systèmes dont elles auront besoin pour soutenir leur évolution.

Faciliter et rendre plus attractive la réparation des appareils défectueux

Cette directive qui couvre un large éventail de produits — des appareils électroménagers aux smartphones et aux tablettes — oblige les fabricants à faciliter l'accès des consommateurs aux pièces détachées, aux informations sur les réparations et à la mise à jour des logiciels. En outre, elle définit clairement les services de réparation que les fabricants doivent offrir à un coût abordable et donne aux consommateurs les moyens de maintenir leurs produits en état de fonctionnement plus longtemps dans l'optique de réduire les déchets et de contribuer à la mise en place d'une économie plus circulaire et durable.

ACCÉLÉRATION.

+50 000
visiteurs

1300
exposants

400
prises
de parole

**PRIX DE
L'INNOVATION
TERRITORIALE**
avec 8 catégories
de prix

9
secteurs
d'exposition

2
salons tenus
conjointement

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

Cette édition sera tenue conjointement avec le **SALON DES SPORTS ET PARASPORTS** et accueillera un nouveau salon : le **SALON DE LA BIODIVERSITÉ ET DU GÉNIE ÉCOLOGIQUE**. Face au dérèglement climatique, les solutions par la nature sont un levier essentiel pour l'adaptation du territoire !

Alors que la fin du mandat approche, c'est le moment de finaliser les projets et programmes menés par les communes et intercommunalités. L'édition 2024 marquera donc le temps de **L'ACCÉLÉRATION**.

DÉVELOPPEMENT & ATTRACTIVITÉS TERRITORIALES | SANTÉ, SOCIAL, ENFANCE & VIVRE ENSEMBLE
NUMÉRIQUE & CONNECTIVITÉ | ÉNERGIE & CLIMAT | CULTURE, LOISIRS & ÉVÉNEMENTS
SÉCURITÉ, PRÉVENTION & PROTECTION | ENVIRONNEMENT & CADRE DE VIE | CONSTRUCTION & AMÉNAGEMENT
SPORTS & PARASPORTS | BIODIVERSITÉ & GÉNIE ÉCOLOGIQUE

19-21 NOVEMBRE 2024
Paris – Porte de Versailles
Plus d'informations sur :
www.salondesmaires.com



Pour nombre d'entreprises concernées par ce droit à la réparation, le modèle économique actuel privilégie le remplacement au détriment de la réparation — à titre d'exemple, certains fabricants annulent la garantie si l'appareil est ouvert ou impose l'utilisation de pièces exclusives.

Actuellement, la production de déchets électroniques en France demeure préoccupante. En effet, selon un rapport des Nations Unis publié en 2024, la France se classe au quatrième rang des pays générant le plus de déchets électroniques en Europe de l'Ouest.

Repenser la chaîne de valeur et développer de nouveaux services

Mais pour s'adapter à la directive sur le droit à la réparation, les fabricants vont devoir refondre leur chaîne de valeur. Les changements auront une incidence sur la quasi-totalité du processus de conception, de production et d'approvisionnement, englobant des aspects tels que la reconception de modèles existants en vue d'utiliser des pièces ordinaires pouvant être réparées et remplacées; la modification intégrale de lignes de production pour produire des produits très différents; la coordination de ces changements; et la mise en place d'une collaboration efficace avec la chaîne de fournisseurs étendue.

Le contrôle des stocks et la gestion des entrepôts ne devraient pas manquer de soulever de nouveaux défis. Actuellement, les opérations de fabrication sont conçues de manière à maintenir un niveau de stock minimale tout en conservant la capacité de produire sans interruption. Le droit à la réparation aura des répercussions importantes sur les conventions établies de longue date dans ce domaine, les entreprises réévaluant la quantité de stocks dont elles auront besoin et l'endroit où ils seront entreposés dans la mesure où elles risquent de devoir répondre à leurs propres besoins de fabrication et de réparation comme à ceux de leurs clients. Au-delà de ces mutations, les entreprises devront maintenir la production sur les bons rails tout en minimisant les coûts.

La directive relative au droit à la réparation devrait entrer en vigueur dans les États membres de l'UE vers la mi-2026.

Or, si les particuliers et les entreprises ne remplacent plus leurs appareils aussi souvent, les fabricants vont se trouver dans l'obligation de développer de nouvelles sources de revenus dans des domaines tels que les réparations, les services d'assistance en continu et la maintenance. Dans certains secteurs, nous assistons d'ores et déjà à l'émergence de services d'abonnement où, au lieu d'effectuer leurs achats dans le cadre d'une transaction unique, les entreprises comme les particuliers « louent » des appareils sur une longue période aux termes de contrats incluant l'assistance, l'entretien et la réparation.



JEAN-ROLAND BRISARD

Réussir l'adaptation au droit à la réparation

Le développement de nouvelles offres significatives de réparation, d'assistance et d'entretien, ainsi que leur bonne intégration aux activités existantes, constituera probablement un exercice important dans le parcours de transformation numérique. Comme c'est toujours le cas dans ces processus de gestion du changement, le succès dépendra des personnes, des processus et de la technologie.

S'agissant des **personnes**, les entreprises devront, au sein des activités concernées, identifier des « ambassadeurs » qui mesurent la nécessité du changement et peuvent contribuer à le mener à bien. Le succès d'un tel projet implique que la direction de l'entreprise affiche son soutien et fasse preuve d'une vision claire. En ce qui concerne les **processus**, les entreprises vont devoir automatiser les flux de travail et la circulation des données d'un bout à l'autre de la chaîne de valeur, les opérateurs humains intervenant exclusivement lorsqu'une décision doit être prise. Enfin, la **plateforme technologique** sous-jacente devra faciliter l'utilisation de méthodes de travail modernes et agiles associant des fonctions industrielles spécifiques et la capacité de s'intégrer à différents systèmes.

La directive relative au droit à la réparation devrait entrer en vigueur dans les États membres de l'UE vers la mi-2026. Compte tenu de la complexité des changements induits, ce calendrier laisse relativement peu de temps aux entreprises concernées pour déterminer comment saisir les nouvelles opportunités commerciales qu'elle leur présentera.

Mais au lieu de considérer cette situation comme un obstacle à surmonter, elles peuvent en faire un atout qui leur permettra d'être davantage respectueuses de l'environnement, une vertu que les consommateurs apprécient de plus en plus.



Les budgets des DSI en 2025

Quels sont les principaux défis pour l'année budgétaire 2025 dans un contexte d'incertitude économique et d'augmentation des enjeux de cybersécurité ?

Augmentation de budget

Ainsi, 41% des DSI prévoient une augmentation de leur budget. Qu'est-ce que cela signifie ? Abraxio livre ses derniers résultats.

Une tendance reflétant l'inflation certes, mais aussi une demande en termes de digitalisation des activités et de transformation numérique, un engagement envers la cybersécurité et l'innovation digitale.

Seulement 12% anticipent une réduction budgétaire imposée par les difficultés économiques des secteurs dans lesquels ils interviennent ou des directives strictes de coupe budgétaire (secteur public par exemple).

Enfin, si 29% maintiendront les mêmes niveaux qu'en 2024, 17% sont incertains quant à leurs prévisions.



Des discussions tendues

Les discussions avec les DAF/DG sont délicates. Ainsi, 47,5% s'attendent à des échanges difficiles, ce qui montre la pression subie par la DSI pour aligner ses ressources avec les priorités stratégiques de l'entreprise, les demandes métiers et les exigences de fonctionnement du système d'informations.

L'arbitrage budgétaire

Cet arbitrage doit être partagé entre la DSI et une décision éclairée et concertée au niveau d'un Comité de Direction.

Un cadre méthodologique pour des choix rationnels, basés sur des données concrètes et objectives peut être utilisé pour faciliter le processus. Comment alors établir le budget d'investissement ? La DSI consulte les fonctions de l'entreprise pour identifier les besoins pour l'exercice à venir. Chaque projet est étudié, macro-chiffré et évalué à l'aide d'un scoring partagé avec les métiers qui mesure sa valeur générée pour l'entreprise et ses conditions d'exécution.

Les débats stratégiques et équilibrés sont ainsi favorisés au sein des organisations et lors des réunions d'arbitrage du CODIR. Abraxio facilite ce processus d'élaboration avec une plateforme dédiée aux DSI permettant notamment de collecter, chiffrer et présenter les besoins métiers.

Top 3 des principaux défis des DSI pour 2025

Quels sont les défis majeurs identifiés par les DSI ?

- la pression budgétaire croissante (22,3%) entraînant des discussions tendues avec le DAF
- la recherche d'un alignement des priorités avec les attentes Métiers et la stratégie de l'entreprise (18,1%)
- l'enjeu d'assurer la pédagogie autour du budget (17%).

Samuel Revenu, CEO d'Abraxio souligne que "malgré ces défis, l'investissement dans le digital demeure une priorité stratégique pour les entreprises, motivant les DSI à sécuriser des ressources additionnelles notamment pour la cybersécurité et l'innovation".

Source Etude Abraxio

Datascientest : L'IA FRUGALE EST UNE COMPOSANTE À PRENDRE EN COMPTE DANS LE DÉVELOPPEMENT DE L'IA

L'IA révolutionne de nombreux secteurs, mais quelle est son empreinte carbone ? quels sont les défis énergétiques de l'IA ? qu'est-ce qu'une IA plus durable ? Les avancées technologiques comme l'IA frugale, peuvent réduire l'impact environnemental grâce à une consommation énergétique réduite. Cette approche vise à concilier innovation et décarbonation. Charles Sutton, CEO et cofondateur de DataScientest a accepté de répondre à ces questions.



Pourriez-vous présenter DataScientest ?

DataScientest, école de data science fondée en 2017 à Paris, est maintenant intégrée au groupe OMNES Education et compte plus de 15 000 apprenants formés avec succès dans des domaines variés. Nous délivrons des formations variées telles que la science des données, l'ingénierie des données,

l'analyse des données, la gestion des données, le cloud computing et DevOps. Nos partenariats officiels avec des leaders comme Microsoft, Google, AWS et Dataiku ont permis d'assurer des formations de haut niveau, reconnues par des institutions prestigieuses telles que l'Ecole des Mines Paris et l'université Paris 1 Panthéon Sorbonne.



CHARLES SUTTON

Nous avons récemment lancé de nouvelles offres telles que DST Ingénierie et le programme Tech Away pour répondre aux besoins en compétences numériques et préparer une main-d'œuvre qualifiée pour les défis technologiques à venir. Nos apprenants bénéficient d'une expérience pratique en codant directement sur notre plateforme, tout en profitant de formations en ligne dispensées par nos experts et formateurs internes.

Après sept années de croissance continue et notre acquisition par le Groupe Omnes Education en 2023, nous avons élargi notre impact avec déjà 2000 clients BtoC et 1200 clients BtoB.

Revenons sur l'IA frugale, qu'est-ce que cela signifie concrètement ? Pourriez-vous nous en dire plus ?

L'IA frugale n'est pas une innovation en tant que telle, mais plutôt une composante à prendre en compte dans le développement de l'IA. Elle vise à réduire la consommation de données et de puissance de calcul, en réponse à la forte consommation énergétique actuelle de l'IA par rapport aux moteurs de recherche traditionnels. Le progrès technologique, bien que parfois encore en phase d'immaturation, présente un potentiel considérable pour transformer notre manière de consommer l'énergie et pour réduire l'empreinte carbone à long terme.

Il existe deux visions concernant l'IA. Celle de la décroissance, dans laquelle l'innovation entraîne une augmentation des usages, et la réduction de l'empreinte carbone est compensée par une hausse du volume d'utilisation.

Ce point de vue, notamment soutenu par Jean-Marc Jancovici, suggère un retour à des modes de vie plus simples pour réduire l'impact environnemental. Pour ma part, je crois davantage à un avenir de croissance responsable où l'IA aurait nécessairement un rôle

clé. Malgré l'augmentation potentielle des usages, les avancées technologiques peuvent contribuer à une réduction significative de l'empreinte carbone à travers des solutions innovantes comme l'IA frugale, qui vise une consommation énergétique réduite.

Notre objectif chez DataScientest est d'explorer ces deux voies, en mettant en avant les avantages potentiels de l'IA frugale. Nous cherchons à jouer un rôle actif dans cette transition vers une IA plus respectueuse de l'environnement, tout en continuant à promouvoir l'innovation et le progrès technologique. 100% de nos programmes Data & IA ont une séance de sensibilisation à l'empreinte carbone.

Nous avons généralement une grosse adhésion des apprenants, qui confirment bien qu'on se dirige vers une génération d'AI Engineer sensibilisés.

L'IA pourrait réduire l'empreinte carbone, quels sont les axes envisagés ?

En tant qu'organisme de formation dans ces nouveaux métiers, nous nous devons de suivre et de nous adapter aux évolutions du secteur. Aujourd'hui, nous avons assez de recul pour prendre conscience de l'impact environnemental de l'utilisation de l'IA, ce qui fait de ce sujet un enjeu crucial à prendre en compte dans le développement de DataScientest.

Notre vision est de réduire l'impact environnemental de l'intelligence artificielle et de l'utiliser au service de l'environnement. Je crois fermement que le progrès technologique a le potentiel de transformer notre consommation d'énergie et de réduire l'empreinte carbone à long terme. Alors que seule l'UE semble actuellement suivre des recommandations strictes en matière de décarbonation, les grandes puissances comme les États-Unis et la Chine ne sont pas encore pleinement engagées dans cette démarche. Il est peu probable que ces nations suivent rapidement une politique environnementale stricte, mais cela n'exclut pas la possibilité que le progrès technologique offre des solutions globales.

Nous cherchons à jouer un rôle actif dans cette transition vers une IA plus respectueuse de l'environnement

Il y a encore un long chemin à parcourir, l'IA commençant à s'installer durablement dans notre société, dans différents secteurs d'activité, mais en utilisant correctement ces ressources, il est possible de développer des solutions qui n'auraient pas été possibles sans l'IA elle-même.

> Par Sabine Terrey

Panne informatique mondiale en juillet : LES ENSEIGNEMENTS À TIRER

Vendredi 19 juillet, une panne mondiale a provoqué l'inaccessibilité de plus de 8 millions de postes de travail sous Microsoft dans de nombreuses entreprises, aéroports, hôpitaux, gouvernements... Comment améliorer la gestion des risques ? Quels sont les enseignements à tirer ? Pauline Mendiela, Manager cybersécurité & résilience et déléguée à la protection des données du cabinet de conseil Finegan, a accepté de répondre à quelques questions



Qu'est-ce que cet événement soulève de la question de la dépendance de nos sociétés aux solutions technologiques et de la confiance sans faille (ni réelles analyses de risques) qui sont attribués aux GAFAM ?

Au-delà des conséquences économiques, de tels incidents récurrents risquent d'éroder la confiance des investisseurs et des consommateurs dans la capacité des entreprises à sécuriser leurs systèmes et les données qu'ils confient. La dépendance à un nombre limité d'acteurs pour la gestion de nos infrastructures critiques compromet notre résilience. C'est d'autant plus vrai lorsque ces services sont

centralisés entre les mains de quelques entreprises qui ne sont pas toujours contraintes au même cadre normatif. C'est notamment le cas régulièrement avec les sociétés américaines.

Aujourd'hui et de plus en plus ces dernières années, les régulateurs européens ont mis l'accent sur la nécessité de mieux connaître et encadrer les relations commerciales. Ces dispositions doivent permettre à moyen terme de mieux identifier les risques et les interdépendances entre les fournisseurs notamment les plus critiques.



PAULINE MENDIELA

En quoi cela souligne l'importance des plans de continuité d'activité (PCA) et de la nécessité d'informer rapidement et clairement les parties prenantes en cas d'incident ?

On observe depuis quelques années un changement de paradigme concernant la continuité des services. Les plans de continuité d'activité et de reprise d'activité sont d'autant plus intégrés à une stratégie plus globale de résilience opérationnelle et numérique. Cette stratégie à la fois proactive et réactive permet aux entreprises de réagir plus efficacement aux défaillances opérationnelles et technologiques, minimisant ainsi les interruptions de service et les impacts économiques.

Il est également essentiel en situation de crise de communiquer via les bons canaux et de véhiculer les informations les plus appropriées pour minimiser les impacts tant internes que externes :

- Une information rapide et transparente rassure les investisseurs et les consommateurs, maintenant leur confiance dans la capacité de l'entreprise à gérer des crises.

- La communication aide également à prévenir la désinformation et à coordonner les actions nécessaires pour résoudre le problème, renforçant ainsi la résilience globale face aux risques systémiques.

Pourquoi est-ce une nouvelle bonne raison de se conformer au plus vite au nouveau règlement européen sur la résilience opérationnelle numérique DORA qui fait la part belle aux risques liés aux Tiers technologiques ?

Cet incident a une fois de plus souligné la nécessité d'améliorer la gestion des risques liés aux Tiers.

À partir du 17 janvier 2025, le règlement DORA sera directement applicable aux établissements financiers dans l'ensemble des États membres de l'UE, introduisant pour la première fois un cadre législatif détaillé et complet sur la résilience opérationnelle numérique. Ce règlement met notamment l'accent sur la gestion des risques liés aux fournisseurs de services numériques dont ceux supportant les services les plus critiques. Ces Tiers critiques feront l'objet de diligences renforcées et de tests tant sur les aspects de sécurité que sur la continuité des services, des éléments cruciaux mis en évidence par cette panne qui a touché des millions d'utilisateurs. D'autre part, les établissements financiers devront renforcer les analyses de risques liés aux prestataires Tiers de services numériques, envisager la mise en œuvre de stratégies multifournisseurs et évaluer les risques de concentrations avant de contractualiser afin de minimiser les situations de quasi-monopole.

En se conformant à DORA, les entreprises renforceront leur capacité à anticiper, gérer et atténuer les risques technologiques, réduisant ainsi leur exposition aux menaces.



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

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



Office 365 : 3 MESURES DE SÉCURITÉ QUE VOUS DEVRIEZ PRENDRE

Si la protection des réseaux ainsi que la protection des périphériques sont largement déployées dans les entreprises, et ce, depuis plusieurs années, il reste encore un chemin important à parcourir pour protéger les accès, les données et leurs fuites.



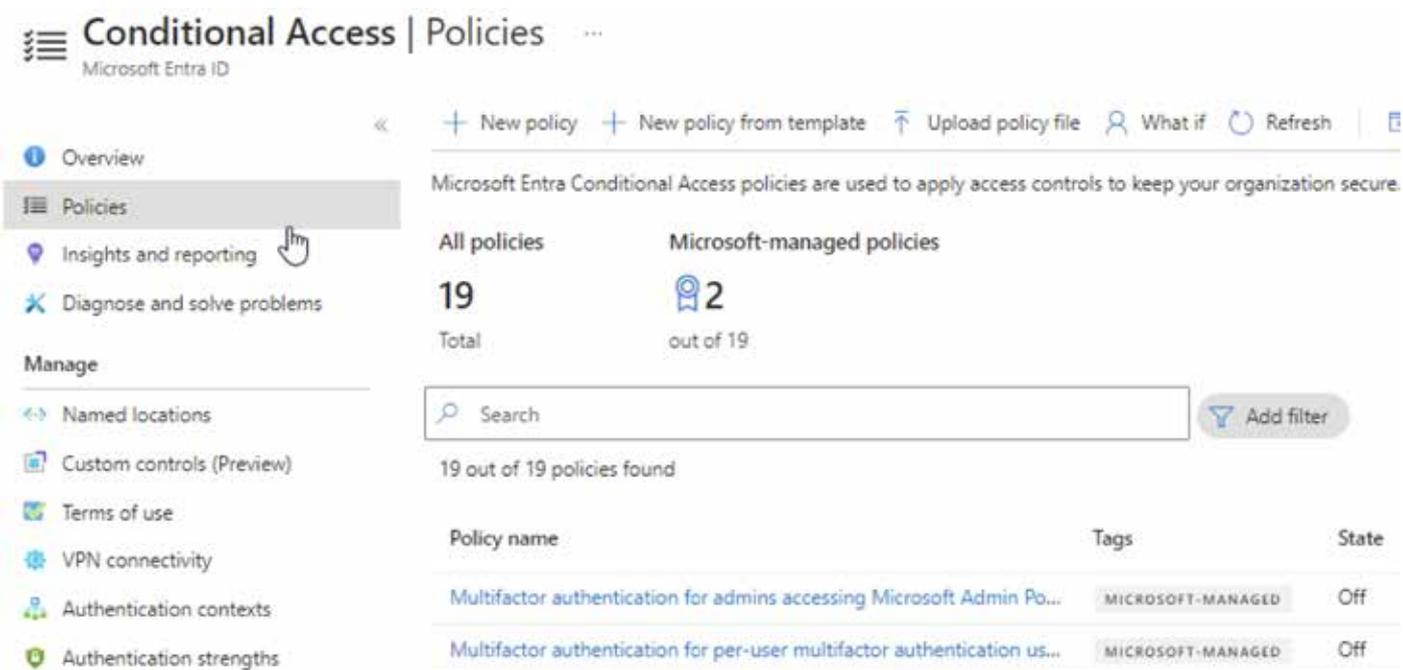
Aujourd'hui, énormément d'entreprises ont recours aux services Office 365 et pourraient être en mesure de se protéger bien au-delà de leur simple identité.

Authentification multifactorielle sans exception

Une des premières mesures que vous devriez prendre, si cela n'est pas déjà le cas, concerne la protection des accès via la généralisation pour

tous les comptes utilisateurs de l'authentification multifactorielle sans exception.

Cette authentification est de plus en plus poussée par Microsoft via des règles d'accès conditionnels qui incitent les administrateurs des tenants à la généralisation du MFA. La figure ci-dessous présente les règles d'accès conditionnels qui ont été générées par Microsoft pour la première fois cette année et poussées sur les tenants.



Il est de notoriété publique que la protection d'une identité ou d'un accès via un simple compte et un mot de passe est, depuis plusieurs années, totalement insuffisante.

D'autre part, les utilisateurs dans leur vie privée ont, d'ores et déjà intégré cette technique lorsqu'il s'agit par exemple d'accéder à leur compte bancaire en ligne, ou d'effectuer des paiements sur Internet. Cette acculturation des utilisateurs facilite grandement l'introduction de l'authentification multifactorielle au sein des entreprises, car perçue comme un gage naturel de sécurité.

Par nature, l'authentification MFA demande nécessairement un second facteur, qu'il soit physique, comme un smartphone, une clé Fido, ou virtuel comme un numéro de téléphone, une adresse de messagerie de secours, ou encore l'usage d'une application comme Microsoft Authenticator.

Comme la plupart des utilisateurs dans les entreprises ne possèdent pas de téléphone professionnel, il peut être délicat de demander à ces personnes d'utiliser leur propre matériel pour valider leurs identités professionnelles. Le recours à une adresse de messagerie de secours peut, donc, dans ce cas-là être proposé. D'un point de vue sécurité, Microsoft recommande l'usage d'une application comme Microsoft Authenticator et déconseille l'usage des SMS, jugé désormais trop fragile.

Personnellement, je vous recommande de déployer l'application Microsoft Authenticator si possible mais également de mettre en place une seconde méthode d'authentification ne dépendant pas de l'accès à cette application. En effet, en cas de perte du portable, l'utilisateur, s'il n'a pas paramétré

cette seconde méthode, sera dans l'incapacité de valider son accès. Ceci est valable pour les comptes d'entreprise, mais également à titre personnel lorsqu'il s'agit de protéger votre compte Amazon, Facebook, LinkedIn etc.

Si vous disposez par conséquent d'un ou plusieurs tenants Office 365, alors l'ensemble de vos comptes utilisateurs, et de surcroît, la totalité de vos comptes à privilèges, doivent impérativement disposer de ce mécanisme de sécurité.

Si vous disposez de comptes de récupération du tenant, qui par définition doivent être des comptes Cloud only, et ne pas dépendre d'une authentification fédérée, (@Onmicrosoft.com), alors ces derniers doivent être également protégés par du MFA.

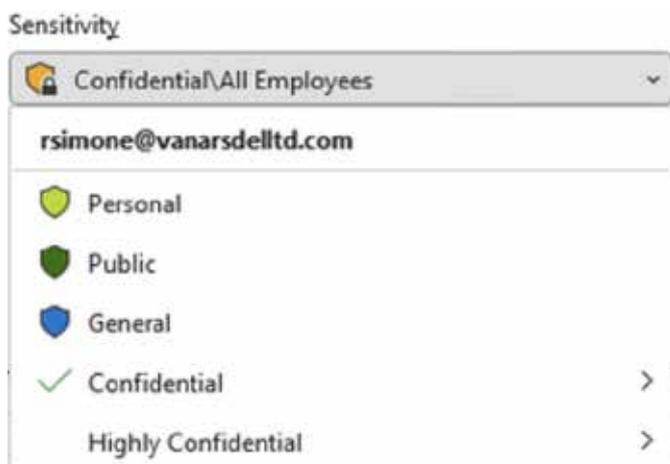
En 2004, Bill Gates annonçait déjà la fin du mot de passe comme protection des accès, il serait temps que, 20 ans après, cette information soit systématiquement prise en compte.

Protéger vos données

Les données des entreprises constituent une partie importante de leur patrimoine. Certaines peuvent se révéler très sensibles, voire totalement confidentielles. Les outils de collaboration mis à disposition des utilisateurs permettent très facilement de communiquer vers l'extérieur, bien souvent en l'absence de tout contrôle. C'est le cas notamment des messageries d'entreprise, mais c'est également le cas pour des applications collaboratives comme Microsoft Teams.

La plupart des entreprises ont des besoins métiers qui exigent régulièrement de pouvoir communiquer avec des partenaires, des fournisseurs, ou des entités ayant des relations privilégiées avec celles-ci. Elles ne peuvent tout simplement pas se couper du monde.

Les solutions Office 365 permettent facilement la mise en place des étiquettes de données qui vont renseigner d'une part les destinataires sur la nature du document, et d'autre part vont pouvoir appliquer des mécanismes de protection, comme des droits d'accès ou du chiffrement. Ainsi, un document sensible communiqué vers l'extérieur, soit par erreur soit par une volonté de nuire, pourrait être totalement illisible pour le récipiendaire. La figure suivante illustre 5 étiquettes de confidentialité possibles.



Cette classification documentaire peut être soit apportée par l'utilisateur, qui peut apposer de son propre chef une classification via ces fameuses étiquettes, ou par des stratégies qui vont être appliquées en fonction de ce que l'on pourrait découvrir dans ces documents. Ces mêmes stratégies peuvent soit inciter l'utilisateur en fonction de ce qui a été découvert dans le document à classer ce dernier, soit le faire de façon automatique et imposée.

La mise en place d'étiquettes de classification relativement simples comme :

- Données publiques
- Données internes
- Données confidentielles

Peuvent être directement activées depuis l'interface d'administration d'Office 365 et ainsi se déployer automatiquement sur toutes les suites Office des utilisateurs ciblés.

Reste naturellement à organiser la communication auprès des utilisateurs et prévoir des campagnes de sensibilisation auprès des différents métiers.

J'entends déjà des voix s'élever, alertant sur le fait qu'il faudrait systématiquement et idéalement cartographier, inventorier l'ensemble de la production documentaire de l'entreprise et qu'il s'agirait par conséquent d'un projet titanesque,

devant intégrer les métiers, la DSI, les services juridiques et un nombre trop important d'intervenants pour être mené à bien.

Malheureusement cette position attentiste, trop souvent observée, a pour conséquence de laisser vos données sensibles ou confidentielles sans protection à l'heure où les entreprises interagissent de plus en plus vers l'extérieur sans véritable protection contre la fuite de données.

Le fait de démarrer simplement, auprès d'un public restreint dans un premier temps, vous permettra de vous acculturer aux techniques de protection. Vous pourrez mesurer l'expérience utilisateur et ainsi être mieux armé pour appréhender les besoins de protection plus complexes de certains de vos départements.

Protection contre la fuite de données

La protection contre la fuite de données est effectivement la troisième mesure que vous devriez prendre en 2024. Après avoir classifié vos données et/ou mis en place des stratégies qui permettent d'inspecter le contenu de ces dernières, il est tout à fait possible d'appliquer en temps réel des contrôles sur l'usage documentaire.

La mise en place d'alertes, en cas de communication vers l'extérieur (voire de copies sur une clef USB) de documents classés ou identifiés comme étant confidentiels ou internes est alors possible.

Naturellement, selon la stratégie que vous aurez choisie, il est possible soit d'alerter l'utilisateur que cet usage n'est pas autorisé, soit simplement de ne pas permettre certains types d'opération. Enfin, il reste possible d'informer les équipes de sécurité qu'un utilisateur tente de faire sortir des documents qui par nature doivent rester au sein de l'entreprise.

La protection contre la fuite de données est effectivement la troisième mesure que vous devriez prendre en 2024.

La prise en compte du risque interne, comme le nomme Microsoft (<https://learn.microsoft.com/fr-fr/purview/insider-risk-management>), fait partie des mesures de sécurité indispensables qu'une Direction des Systèmes d'Information doit être en mesure de proposer de façon proactive en 2024.

C'est la rentrée et l'heure est aux bonnes résolutions, non ?

> Laurent TERUIN | MVP | <https://workingtogether.fun/>

ACCÉLÉRATION.

+50 000
visiteurs

1300
exposants

400
prises
de parole

**PRIX DE
L'INNOVATION
TERRITORIALE**
avec 8 catégories
de prix

9
secteurs
d'exposition

2
salons tenus
conjointement

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

Cette édition sera tenue conjointement avec le **SALON DES SPORTS ET PARASPORTS** et accueillera un nouveau salon : le **SALON DE LA BIODIVERSITÉ ET DU GÉNIE ÉCOLOGIQUE**. Face au dérèglement climatique, les solutions par la nature sont un levier essentiel pour l'adaptation du territoire !

Alors que la fin du mandat approche, c'est le moment de finaliser les projets et programmes menés par les communes et intercommunalités. L'édition 2024 marquera donc le temps de **L'ACCÉLÉRATION**.

DÉVELOPPEMENT & ATTRACTIVITÉS TERRITORIALES | SANTÉ, SOCIAL, ENFANCE & VIVRE ENSEMBLE
NUMÉRIQUE & CONNECTIVITÉ | ÉNERGIE & CLIMAT | CULTURE, LOISIRS & ÉVÉNEMENTS
SÉCURITÉ, PRÉVENTION & PROTECTION | ENVIRONNEMENT & CADRE DE VIE | CONSTRUCTION & AMÉNAGEMENT
SPORTS & PARASPORTS | BIODIVERSITÉ & GÉNIE ÉCOLOGIQUE

19-21 NOVEMBRE 2024
Paris – Porte de Versailles
Plus d'informations sur :
www.salondesmaires.com



Stimuler l'innovation durable GRÂCE À LA TRANSFORMATION NUMÉRIQUE ET AUX PRINCIPES ESG

La transformation numérique, levier pour l'innovation durable, permet aux entreprises de comprendre l'empreinte environnementale et sociale de leurs produits, facilitant la mise en place de solutions alignées avec les principes ESG. Analyse des données, opportunité pour réduire les impacts négatifs mais aussi responsabilité sociale renforcée ...Nicolas Letavernier, Directeur du développement France chez Workiva a accepté de répondre à ces questions.



Comment la transformation numérique peut-elle favoriser l'innovation des produits, services et modèles durables alignés sur les principes ESG ?

La transformation numérique et la durabilité, ou les principes ESG, peuvent aller de pair. Pour tout produit, service ou entreprise, l'innovation repose sur une mesure de base et une collaboration interfonctionnelle, facilitées par les données et la technologie. En France, par exemple, 89 % des professionnels estiment que le rapport intégré améliore la performance et offre un avantage concurrentiel, soulignant ainsi l'importance de cette approche.

Cartographier les impacts environnementaux et sociaux pertinents tout au long du cycle de vie du produit ou service est la première étape. Ce processus, souvent appelé analyse du cycle de vie (ACV), est crucial pour les biens de consommation, les produits alimentaires ou les boissons. Il est intéressant de noter que la dernière étude ESG Practitioner montre que 76 % des entreprises européennes, même celles non soumises à la directive CSRD, envisagent d'aligner leurs informations de durabilité sur ses exigences, ce qui démontre l'influence croissante de la réglementation sur les pratiques d'évaluation environnementale.

Ce processus nécessite la collecte de données de systèmes externes et de partenaires pour construire des bases de données internes et des cadres de mesure. Bien que la meilleure façon de le faire soit numériquement, il est essentiel de favoriser la collaboration et d'intégrer une réflexion durable dans toute l'organisation. La technologie est un catalyseur clé, car elle permet aux entreprises de coordonner les efforts ESG, pour que les équipes puissent travailler ensemble en temps réel pour cartographier l'empreinte de durabilité. D'après notre rapport, 84 % des Français et 81 % des Européens déclarent que l'intégration des données financières et de durabilité améliore significativement la prise de décision, ce qui montre l'impact positif de cette synergie.

Nous voyons déjà des entreprises leaders identifier des opportunités pour réduire les impacts environnementaux des produits. Par exemple, de nombreux produits alimentaires et boissons doivent gérer des risques environnementaux et de droits humains dans leur chaîne d'approvisionnement, comme avec l'huile de palme, le cacao ou le soja. Cette vue d'ensemble et la quantification des impacts sont la première étape vers l'innovation durable des produits et services. Ce processus est essentiel pour identifier les opportunités de réduire les impacts négatifs et d'améliorer les positifs en repensant les processus de sourcing, de fabrication et d'élimination. En France, 91 % des professionnels pensent que le reporting intégré aura un impact positif sur la création de valeur à long terme, une opinion partagée par 87 % des Européens, ce qui montre l'importance de ces démarches pour la durabilité.

Quels sont les avantages potentiels de l'adoption des technologies numériques en termes de réduction de l'empreinte environnementale d'une organisation et de promotion de la responsabilité sociale ?

Les technologies numériques augmentent l'efficacité, la productivité et la collaboration. Elles aident les entreprises à réduire leur empreinte environnementale et à promouvoir la responsabilité sociale. En France, environ 90 % des entreprises prévoient d'augmenter leur budget pour les technologies de développement durable au cours des trois prochaines années, ce qui témoigne de l'importance croissante de l'intégration technologique pour atteindre ces objectifs.

Par exemple, la vidéoconférence peut réduire les voyages d'affaires et les émissions de gaz à effet de serre. De même, des modes de travail plus hybrides ou numériques peuvent mieux connecter les équipes et potentiellement rendre les réunions et l'apprentissage plus inclusifs. Cependant, ces avantages ne sont pas garantis ; une entreprise



NICOLAS LETAVERNIER

doit être intentionnelle dans la poursuite de ces résultats. En effet, 92 % des professionnels français investissent dans la technologie pour améliorer la collaboration entre les équipes de reporting ESG, soulignant l'importance de cette intégration technologique pour la réussite des initiatives de durabilité.

Être 'intentionnel' signifie spécifier quel objectif une entreprise souhaite atteindre. Cela pourrait être de définir à l'avance comment un projet de digitalisation devrait réduire l'impact environnemental et promouvoir la responsabilité sociale ou l'inclusion. Dans ce cas, les entreprises devraient quantifier leur performance actuelle, estimer le résultat probable, fixer des objectifs, puis mesurer leur performance par rapport à ces objectifs. Les solutions technologiques sont essentielles pour répondre aux exigences de la CSRD et d'autres réglementations, ce qui montre l'importance de la transformation numérique pour atteindre ces objectifs de conformité et de durabilité.

Comment les organisations peuvent-elles tirer parti de la transformation numérique pour améliorer leur reporting et leur communication autour de la performance et de l'impact ESG ?

Les entreprises publient plus d'informations financières et non financières que jamais auparavant. Les organisations doivent divulguer les données ESG conformément aux réglementations et aux normes qui se multiplient, ainsi que communiquer la performance et la stratégie de durabilité aux parties prenantes de manière continue. Avoir de bons outils peut aider les dirigeants à surmonter cette complexité. En France, 86 % des professionnels estiment que certifier les données ESG augmente les chances d'atteindre les objectifs, soulignant l'importance de cette certification pour leur crédibilité.

Un moyen pour les entreprises de tirer parti de la transformation numérique est l'utilisation de plateformes de reporting sur la durabilité. Compte tenu de la dynamique des normes ESG, il est essentiel d'adopter une solution de pointe pour se conformer aux réglementations actuelles et futures. 81 % des professionnels français pensent que l'IA générative rendra les rapports de durabilité plus efficaces, ce qui est en ligne avec les opinions de 85 % des Européens, illustrant l'importance croissante de cette technologie dans le processus de reporting.

Les entreprises doivent se conformer à diverses exigences pour les rapports de durabilité, obligatoires et volontaires. Suivre ces cadres et leurs chevauchements est essentiel pour simplifier le processus. Les entreprises doivent garantir que leurs rapports ESG reposent sur des données fiables, intégrées de diverses sources comme les ERP et les outils de comptabilité carbone. Les technologies avancées centralisent ces données, facilitant la gestion des rapports et la conformité.

Il est essentiel de souligner l'impact transformateur de l'IA générative. Intégrée dans une plateforme de reporting de durabilité, elle peut grandement améliorer et accélérer les processus. Bien qu'elle ne remplace pas la collaboration humaine ni ne définisse une stratégie de durabilité, elle libère du temps pour des tâches plus complexes et à forte valeur ajoutée.

Quelles sont les considérations clés pour les organisations lorsqu'il s'agit de s'assurer que leurs initiatives de transformation numérique sont éthiques, inclusives et alignées sur leurs valeurs ESG ?

La transformation numérique a apporté des changements significatifs dans le monde, dont beaucoup sont positifs. Cependant, aucun progrès

ne vient sans certains défis qui doivent être abordés. En France, les entreprises démontrent une grande capacité d'adaptation en intégrant des pratiques de gouvernance solides pour améliorer leur transparence et leur performance ESG, illustrant leur engagement à respecter les valeurs éthiques et inclusives dans leurs projets de transformation numérique.

L'IA générative, par exemple, suscite des préoccupations environnementales, sociales et éthiques. Les entreprises doivent s'assurer que leurs employés l'utilisent correctement, avec une surveillance humaine critique. Utilisée correctement, elle est également un outil puissant pour la cybersécurité. Avec une formation adéquate et des garde-fous, l'IA peut aider à aligner l'entreprise sur ses valeurs ESG. Il est crucial de fixer des objectifs éthiques et inclusifs pour garantir une transformation numérique durable et responsable.

En plus de l'IA, une solide gouvernance est nécessaire pour aligner les projets de transformation numérique sur les valeurs ESG et les déployer de manière éthique et inclusive. Cela peut inclure la création d'un comité interfonctionnel avec le CSO, le CIO et leurs équipes pour superviser l'impact du projet. En France, la transparence et la conformité sont essentielles pour rester compétitives, soulignant l'importance de l'éthique et de l'inclusivité dans ces initiatives.

Dans cette nouvelle ère de transformation numérique, les entreprises doivent considérer l'éthique et l'inclusivité comme des valeurs fondamentales. Cela implique une gouvernance efficace et la formation des employés à mesure que les processus et les rôles évoluent avec le numérique et l'IA. L'intégration des technologies numériques doit être accompagnée de pratiques responsables pour maximiser les bénéfices environnementaux et sociaux.



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

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



STATIONS BLANCHES USB



SCAN USB



DECONTAMINATION



SECURE FILE SHARING

PROTECT BEFORE CONNECT





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

Mise en conformité avec les règles de l'entreprise

Interopérabilité avec les Systèmes RH

Audit & planification de l'utilisation des e-mails

Droit à la déconnexion et RGPD

Planification simplifiée des processus de gestion

Rapports d'analyse de trafic, suivi des messages

Optimisation des performances de la messagerie



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

Analyse, Contrôle et Reporting complet des systèmes de messageries Microsoft Office 365 et Microsoft Exchange