

SMART DSI®



DOSSIER

Définir une stratégie informatique pour les 3 - 5 ans à venir

BONNES

PRATIQUES 2022

Six domaines clés à évaluer pour adopter le DevSecOps

INTERVIEW

La cyber-résilience basée sur l'identité au service des entreprises

L'ETUDE A RETENIR

Top 3 des changements stratégiques des responsables IT

INTERVIEW

Orchestrer l'intelligence collective en entreprise

CYBERSECURITE

Prédictions pour 2022 et au-delà



En route vers le DaaS augmenté avec DIB-France®

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


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

Simplicité de mise en œuvre



Sécurité renforcée



Infrastructure Cloud



Flexibilité & Souplesse





De nouvelles compétences pour des environnements innovants !

Après ces longs mois de pandémie et d'incertitudes, les cartes sont totalement rebattues et une certaine prise de conscience émerge. L'autonomie et la flexibilité au travail deviennent des facteurs tout aussi importants que le salaire pour les collaborateurs. Mais ce n'est pas tout, le travail hybride s'impose pour les salariés français qui considèrent que si la vie sociale et la collaboration ont lieu « au bureau », les tâches individuelles se passent « à l'extérieur ». Certains pensent même que le bureau sera perçu comme un avantage, et non plus comme un lieu de travail obligatoire⁽¹⁾.

Face à ce constat, les entreprises s'empressent de repenser leurs espaces de travail pour être en phase avec les nouvelles aspirations, et réfléchissent à des mesures pour un environnement hybride sain et réussi, en s'éloignant des politiques traditionnelles. L'objectif est de recréer des environnements de confiance, d'ouverture, de principes certes, mais aussi d'authenticité, d'épanouissement, de flexibilité sous couvert de technologies adaptées aux besoins.

Et pour poursuivre en ce sens, un autre changement radical se prépare du côté des directions informatiques. Une refonte profonde s'amorce et les cinq prochaines années seront essentielles pour apporter plus de valeur stratégique aux organisations.

Alors quelles sont les évolutions à venir ?⁽²⁾ Les directions informatiques comptent s'appuyer sur la décentralisation pour répartir les tâches et travailler avec les autres départements, mais elles entendent aussi accentuer les compétences relationnelles, l'empathie, le leadership et les technologies collaboratives renforçant l'autonomie et les responsabilités. Deux autres priorités s'imposent, d'une part accélérer la formation continue pour ne pas se spécialiser dans une seule technologie et avoir un impact majeur transformationnel, et d'autre part, anticiper la charge de travail attendue. Enfin, favoriser la diversité, l'égalité et l'inclusion permettra de s'entourer de nouveaux talents et d'équipes innovantes et créatrices.

Des pistes qui assurément donnent aux entreprises les moyens de répondre aux bouleversements du monde du travail de manière durable.

Très belle année 2022 !

Sabine Terrey
Directrice de la Rédaction
sterrey@itpro.fr

(1) Jabra Hybrid Ways of Working 2021 - 1800 salariés en France
(2) Source Pega & cabinet iResearch - 750 responsables
(vice-présidents, directeurs et managers)

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 ».

SMART DSI

N°24 | DECEMBRE 2021

6 | DOSSIER

Définir une stratégie informatique pour les 3 – 5 ans à venir



P.6

12 | L'ŒIL SECURITE

Réflexions et stratégies de sécurité des Clouds managés



P.28

14 | PERSPECTIVES

Cybersécurité : Prédications pour 2022 et au-delà !

17 | L'ETUDE A RETENIR

Envolée des besoins en calcul, stockage et connectivité

18 | INTERVIEW

Semperis : la cyber-résilience basée sur l'identité au service des entreprises

21 | L'ETUDE A RETENIR

Rançongiciels : les 3 recommandations pour se protéger

22 | EXPERT

Azure Stratégie, brique essentielle de la gouvernance



P.12

27 | L'ETUDE A RETENIR

Top 3 des changements stratégiques des responsables IT pour 2022

28 | INTERVIEW

Paessler : le rôle clé de la supervision dans la réduction de consommation des ressources naturelles

31 | L'ETUDE A RETENIR

Les DSI progressistes pilotent la fonction Finance en 3 étapes

32 | BONNES PRATIQUES 2022

Six domaines clés à évaluer pour adopter la culture DevSecOps



P.38



38 | EXPERT

Comment développer une application de recherche de contenu avec Apache Lucene ? - Partie 1

44 | INTERVIEW

Orchestrer l'intelligence collective en entreprise !

45 | BULLETIN D'ABONNEMENT

48 | EXPERT

Les indispensables stratégies d'accès conditionnel

56 | INTERVIEW

Nua.ge simplifie l'adoption du IaaS

SMARTDSI

Rédaction

Pour joindre les membres de la rédaction
redaction@smart-dsi.fr
Comité de rédaction associé à cette édition

Thierry Bollet, Juvénal Chokogoue, 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

© 2021 Copyright IT Procom
© Crédits Photos

AdobeStock - Istock - Shutterstock

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

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

SMART DSI - IT PROCOM, tous droits réservés.

© 2021 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

Définir une stratégie informatique POUR LES 3 – 5 ANS À VENIR

> Par Didier Danse

Les technologies de l'information font partie intégrante du quotidien de chacun. Celles-ci sont ainsi passées du statut d'élément de support à celui de différenciateur pour les entreprises. Celles qui ont intégré les technologies de l'information dans leur propre stratégie ont pu améliorer leur positionnement sur leurs marchés respectifs et améliorer les conditions de travail par la même occasion.



Transformer son département informatique pour que celui-ci devient un vecteur d'évolution de l'entreprise peut cependant s'avérer complexe. Ainsi, il n'est pas rare de voir d'excellents responsables informatiques avoir des difficultés à y parvenir, créant parfois des situations difficiles à gérer.

Dans les grandes entreprises, le poste de gestionnaire informatique est de plus en plus fréquemment pris en charge par une personne dite « à vocation métier » et qui a d'ores et déjà des compétences diverses dans la définition d'une stratégie et son exécution, la partie technique étant déléguée à des responsables techniques. Dans des entreprises à taille humaine, le coût financier et humain s'avère important avec cette formule et il est préférable d'avoir une personne technique

à ce poste. Malgré la difficulté, il ou elle pourra s'épanouir au mieux et transformer un centre de coûts en un différenciateur compétitif au quotidien.

Pour cela, il est nécessaire d'aborder les fondamentaux de la stratégie.

La stratégie, qu'est-ce que c'est ?

Le positionnement de la stratégie dans l'organisation

Michael Porter, spécialiste dans le domaine de la stratégie a défini celle-ci comme suit :

« La Stratégie, c'est la réalisation des choix d'allocation de ressources (financières, humaines, technologiques, etc.) qui engagent l'entreprise

dans le long terme et la dotent d'un avantage concurrentiel durable, décisif et défendable ».

Tout chef d'entreprise ou tout gestionnaire d'équipe, à minima, se doit d'avoir une vision claire de ce que doit être son organisation dans le futur. Ayant cela en tête, il est possible de formaliser la mission, c'est à dire comment la vision sera réalisée. Ceux qui en disposent savent ce à quoi ils veulent parvenir sur du très long terme, ce qui leur permet de réfléchir aux attentes et priorités pour les 3 ou les 5 ans à venir, au travers de la stratégie.

La stratégie c'est la réponse aux opportunités, menaces, forces et faiblesses de l'organisation pour défendre ses avantages concurrentiels. Vous aurez reconnu l'analyse SWOT comme méthode pour identifier les éléments de la stratégie même si certaines organisations feront le choix d'utiliser des approches plus complexes pour identifier les objectifs et finalement définir les actions qui en découlent. Notons que la notion de stratégie est souvent confondue avec les aspects tactiques ou encore avec l'opérationnel. La tactique c'est ce qui va être fait sur du moyen terme, soit de quelques mois à un an tout au plus tandis que l'opérationnel est comment cela va être fait.

Avoir une stratégie claire permet donc de clarifier le chemin à prendre pour atteindre la vision afin que l'interprétation ne prenne une place trop importante au quotidien. Définir et maintenir une stratégie s'avère d'autant plus compliqué que le monde

est en perpétuelle évolution. C'est pour cela que, régulièrement, une évaluation doit être faite pour réaligner la stratégie avec l'environnement dans lequel est placée l'organisation.

Bien que l'on parle de « la stratégie », il s'avère qu'il y en a plusieurs. En effet, la stratégie peut s'appliquer à différents niveaux : l'organisation (l'ensemble des domaines), un domaine ou encore une fonction. Les stratégies peuvent être en réponse à des événements tels que l'apparition d'opportunités sur le marché (l'apparition du Covid a clairement été favorable à bien des industries) ou anticiper des événements tels que le lancement d'un produit ou le souhait de développer des produits dits disruptifs. Parfois, la stratégie est simplement subie, c'est à dire qu'elle est nécessaire en réponse à des événements pour lesquels des décisions ont manqué.

Quel que soit le niveau auquel s'appliquent la stratégie et le fondement de celle-ci, la plupart des stratégies peuvent être regroupées dans une des catégories suivantes :

- la domination par les coûts ou par l'innovation et la technologie
- la différenciation
- la coopération au travers de l'utilisation d'une licence, de la sous-traitance, d'une franchise ou encore d'une concession.

AXEL
définit autrement la technologie
du Client Léger

Prêt gratuit
pour évaluation

www.axel.fr

"Start with why"

Simon Sinek a présenté son modèle "Golden circle" dans son livre "Start with Why" et pour faire simple, il y indique qu'avant d'envisager de définir ce que vous allez faire, il s'agit de définir le pourquoi vous allez le faire, c'est à dire le but ultime. Ayant cet élément en tête, il est alors possible de définir le comment y arriver (les objectifs) avant finalement de parler des activités à réaliser dans ce but.



Je vous encourage d'ailleurs à prendre 20 minutes pour regarder sa présentation TED "Comment les grands leaders inspirent l'action" de 2014.

Ce que couvre de la stratégie

Afin d'être le plus concret possible, parcourons quelques approches stratégiques qui peuvent être prises en compte lors de la définition d'une stratégie :

1. L'amélioration des processus et des techniques (faire plus avec moins)
2. L'amélioration de la capacité des équipes métier à créer de la valeur facilement et rapidement (évolution technologique)
3. L'amélioration de la prédictivité (mettre en place des outils de reporting et de prévisionnel)
4. L'amélioration de la qualité des données pour que celles-ci puissent être utilisées au mieux
5. La réaffectation des moyens dans le but de délivrer le maximum de valeur
6. L'utilisation de ressources externes spécialisées
7. Et beaucoup plus encore...

Définir les axes d'une stratégie informatique

De la même manière que la stratégie est inhérente à la mission de l'entreprise, la stratégie informatique se voit héritée de la stratégie de l'entreprise. La stratégie informatique doit permettre de clarifier le positionnement du digital dans l'entreprise : le pourquoi, les avantages attendus et bien plus. Ainsi, si la stratégie d'entreprise est « d'être réactif », il est nécessaire de s'assurer d'avoir du personnel et du matériel en suffisance ainsi que des processus de validation rapide.

Il est alors nécessaire de définir le modèle d'exploitation cible informatique et d'évaluer l'état actuel des technologies de l'information : la capacité actuelle, la maturité des processus, l'analyse du portefeuille, la méthodologie et la gouvernance et bien d'autres tels que la sécurité ou encore l'infrastructure en place. Ce à quoi s'ajoute l'ensemble des facteurs externes et le niveau de la concurrence sur des éléments tels que la robotisation et les tendances technologiques (standards).

En connaissant la situation actuelle et la cible, il s'agit d'analyser les écarts et de créer le plan du directeur informatique. Un tel plan peut nécessiter de nombreux changements tels que :

- l'énoncé de mission,
- l'introduction de nouvelles technologies,
- la revue du futur modèle opérationnel informatique,
- l'adoption de nouveaux outils et méthodologies,
- la modification de processus informatiques,
- une revue de l'approche concernant gestion des fournisseurs,
- de même pour la gouvernance.

La stratégie c'est la réponse aux opportunités, menaces, forces et faiblesses de l'organisation pour défendre ses avantages concurrentiels.

Ce plan sera explicité au travers des initiatives nécessaires pour atteindre la cible en tenant compte de plusieurs facteurs : la valeur, la complexité, les coûts et la main d'œuvre nécessaire.

Une fois les priorités identifiées, il s'agit de les décrire en fournissant les informations suivantes : une description de l'initiative et les hypothèses, les buts et objectifs ainsi que le périmètre, l'approche, les coûts, une estimation du calendrier, les risques et dépendances, les indicateurs de performance clés (KPI).

Communiquer la stratégie

Avoir une stratégie est évidemment important mais la communiquer efficacement s'avère critique au risque de se perdre dans l'orientation prise par les uns et les autres. Pour cela, le message doit être court, simple, clair et explicite et doit donner une description explicite de ce que l'on imagine afin de permettre de se projeter.

La documentation se fait au travers d'un document d'environ 35 pages à destination du Comité de Direction et du Conseil d'Administration avant tout, avant même les collaborateurs. Il s'agit de dire ce que l'on va entreprendre, pas du comment s'y prendre.

Certaines entreprises profitent de la définition de la stratégie pour revisiter la mission de celle-ci et éviter une différence notable dans la compréhension des uns et des autres. Encore une fois, il s'agit d'aligner la vision, la mission et la stratégie pour y arriver. Pour être comprise, la stratégie doit être ambitieuse mais réalisable et avec un objectif temporel notamment. Vous l'aurez certainement compris, les objectifs doivent respecter l'acronyme « SMART ».

Une fois la stratégie clarifiée, il s'agit d'informer l'ensemble des intervenants, notamment des objectifs à atteindre et dans quelle temporalité, mais aussi les moyens qui y seront dédiés.

Exécuter et mesurer l'efficacité de la stratégie

La conduite de changement est un enjeu important, d'autant plus critique que la stratégie couvre des sujets de grande envergure. La conduite de changement s'opère au travers de la mise à disposition d'informations mais aussi de formations.

Différentes méthodes existent mais toutes suivent un schéma similaire, issu du modèle « ADKAR » qui décrit les grandes étapes de la conduite de changement :

- 1. Awareness :** Faire prendre conscience des raisons et objectifs (de la stratégie)
- 2. Desire :** Donner le désir d'opérer le changement
- 3. Knowledge :** Permettre l'apprentissage ou la formalisation de la manière de faire le changement
- 4. Ability :** Se donner les moyens de parvenir au changement et l'exécuter
- 5. Reinforcement :** S'assurer que le changement soit durable dans le temps.

Se donner les moyens, c'est notamment s'assurer que le portfolio contenant les programmes et les projets soit en adéquation avec la stratégie. Ensuite, ces projets se doivent d'être suivis efficacement,

notamment au travers d'un tableau de bord permettant d'identifier les progrès de ces projets mais surtout l'efficacité de la stratégie au travers de mesure de performance en adéquation avec les enjeux de la stratégie.

Une stratégie étant l'expression d'enjeux et d'activités qui seront effectuées sur plusieurs années, il est important d'envisager une réévaluation annuelle. La remise en question régulière permet de tenir compte de l'évolution de l'environnement de l'entreprise.

Enfin, il importe à nouveau de gérer de façon professionnelle les changements qui découlent de ces évolutions comme présenté ci-dessus.

Comment démarrer ?

Tout d'abord, il est important de rappeler qu'une stratégie ne se définit pas d'un jour à l'autre. Evidemment, il est possible de démarrer « en l'état » mais toute information collectée au préalable permettra d'être d'autant plus efficace pour la préparation de la stratégie. Ainsi, il s'agit de mettre en place des mécanismes permettant cette collecte d'informations au quotidien, informations qui seront utilisées pour étudier l'écart entre la situation actuelle et la situation attendue.

De plus, la stratégie ne peut être définie au sein du département informatique uniquement. La stratégie informatique doit être alignée avec les autres départements sans quoi il y aura un décalage entre les attentes des uns et des autres et surtout entre les objectifs de chaque département. Ainsi, si le département financier souhaite réduire le montant des frais ou que le département RH veut externaliser certaines activités alors que vous souhaitez engager abondamment, on peut vite se rendre compte que la stratégie définie ne pourra fonctionner. C'est pour cela que la stratégie se doit d'être préparée avec le Comité de Direction.

Pour être comprise, la stratégie doit être ambitieuse mais réalisable et avec un objectif temporel.

Ce dernier devra valider la stratégie afin de s'assurer de l'adéquation à tous les niveaux. Cet accord servira également comme support à la mise en place à venir. La collaboration entre les différents départements permet notamment d'identifier les questions auxquelles il faut répondre et s'assurer que les 3 axes classiques sont couverts : finances (rentabiliser), marketing (adéquation entre offre et demande) et organisationnel (efficacité, synergies et flexibilité interne).

Pour cela, COBIT, le référentiel des bonnes pratiques au niveau gouvernance, fournit une matrice RACI des plus utiles pour identifier les parties prenantes :

AP002 RACI Chart																										
Key Management Practice	Board	Chief Executive Officer	Chief Financial Officer	Chief Operating Officer	Business Executives	Business Process Owners	Strategy Executive Committee	Steering (Programmes/Projects) Committee	Project Management Office	Value Management Office	Chief Risk Officer	Chief Information Security Officer	Architecture Board	Enterprise Risk Committee	Head Human Resources	Compliance	Audit	Chief Information Officer	Head Architect	Head Development	Head IT Operations	Head IT Administration	Service Manager	Information Security Manager	Business Continuity Manager	Privacy Officer
AP002.01 Understand enterprise direction.		C	C	C	A	C	C				C	C	C					R	C	R	R		R	R	R	
AP002.02 Assess the current environment, capabilities and performance.		C	C	C	R	C	C				C					C	C	A	R	R	R	C	C	C	C	C
AP002.03 Define the target IT capabilities.		A	C	C	C	I	R	I			C	C			C	C	R	C	C	C	C	C	C	C	C	C
AP002.04 Conduct a gap analysis.					R	R	C				C				C	R	R	A	R	R	R	R	R	R	R	C
AP002.05 Define the strategic plan and road map.		C	I	C	C		C	R			C	C				C	C	A	C	C	C	C	C	C	C	C
AP002.06 Communicate the IT strategy and direction.	I	R	I	I	R	I	A	I	I	I	I	I	I	I	I	I	I	R	I	I	I	I	I	I	I	I

Il est évident que de nombreuses actions décrites précédemment s'avèrent importantes et nécessaires mais d'ores et déjà avoir les bonnes personnes permettra de poser les bonnes questions, de s'assurer une vision commune et de valider l'approche.

L'appel à un facilitateur peut être d'une grande aide. D'autres outils peuvent être utiles : le SWOT dont nous avons parlé mais aussi le PESTEL, les 5 forces de Porter et bien d'autres.

Enfin, attention à ne pas confondre plan stratégique et business plan. Le premier décrit la feuille de route à prendre tandis que le second décrit le fonctionnement de l'organisation.

La remise en question régulière permet de tenir compte de l'évolution de l'environnement de l'entreprise.



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

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



Inmac wstore vous accompagne dans l'achat de vos équipements et solutions IT



Notre approche conseil de proximité repose sur une organisation complète et un accompagnement par des spécialistes expérimentés :

- Une équipe de plus de 200 commerciaux & spécialistes
- Plus de 100 certifications
- Centre de prestations techniques de 2 500 m² certifié ESD
- Une offre de produits globale de 80 000 références actives
- Un stock de 9 500 m²
- Une livraison en 48h en France
- Plus de 2 000 commandes livrées par jour

Découvrez toutes les solutions IT pour collaborer en toute simplicité grâce au guide du travail hybride inmac wstore



Retrouvez toutes nos solutions sur www.inmac-wstore.com

Réflexions et stratégies DE SÉCURITÉ DES CLOUDS MANAGÉS

La face visible de la cybersécurité tourne actuellement majoritairement autour des attaques de phishing porteuses des ransomwares. C'est un sujet critique, les attaques aux rançons se multiplient et causent des graves sinistres aux entreprises de tout segment économique. Ces thématiques et surtout ces incidents réels ont développé des indispensables services de Détection d'attaques et de Réponse/Résolution.



Un autre sujet moins visible mais tout aussi critique anime les réflexions et les plans d'action des RSSI et le quotidien des ingénieurs et consultants en cybersécurité.

La sécurité des SI et des données externalisés dans le Cloud

Il s'agit de la sécurité des SI et données dorénavant externalisés dans le Cloud. Déjà quand on parle sécurité Cloud, il y a plusieurs compréhensions et

facettes couvertes, que nous citons : l'hébergement et l'accès aux données, que nous visons : les applications en mode SaaS, dont nous parlons : des cycles agiles de DevOps, etc. etc.

Le code devient donc la zone à protéger.

Mais revenons à notre sujet stratégique lié à la sécurité des Clouds. Les enjeux de cybersécurité de nouvelle génération partent de la notion des services exposés et les vecteurs de compromission, définissent les cloisonnements nécessaires pour que les compromissions ne se propagent pas et abordent la gestion des identités et des droits.

Nous constatons clairement que la sécurité de demain, vraiment demain voire déjà aujourd'hui, est une articulation entre la gestion des identités et des droits (identités compromises, élévation de privilèges, etc.), la sécurité des codes voire de l'infra as code avec son corollaire immédiat portant sur la gestion du risque applicatif (l'analyse amont) du code, avant son déploiement.

Le code devient donc la zone à protéger. Exit la stratégie de cybersécurité consistant à sécuriser les accès au périmètre de l'entreprise, la vieille approche citadelle, exit donc cela, en faveur ou plutôt devant la nécessité de protéger la donnée, le code et l'appli la manipulant, transformant, l'hébergeant. Cela a généré les outils de sécurité des conteneurs, et cela devient un sujet type appsec avec audit du code en amont du déploiement, etc.

Et le DevOps devint SecDevOps!

Dans les entrailles de la sécurité du Cloud, on retrouve donc ces plaques tectoniques autour de l'IAM, de la SecDevOps, de la surveillance permanente, véritable tour de contrôle des interactions Cloud.

Un management via le code (changement du code) implique la gestion des risques autour de ces opérations de management : le contrôle et la maîtrise des outils de gestion du code (git, pipelines CI/CD, outils de déploiement comme Ansible ou Terraform, etc.).

De par la gestion fine des privilèges et proactive des identités, certaines surexposées et compromises, IAM est plus que jamais au cœur d'une démarche cohérente de cybersécurité. Combiné d'une part à la sécurité des applications et d'autre part, aux opérations de surveillance et de contrôle permanent de la sécurité du SI à travers des organisations opérationnelles, souvent 24/7, de type SOC, la sécurité d'une organisation doit aujourd'hui accorder une place prioritaire aux problématiques IAM et sécurité des applications, car là se trouve le cœur de l'entreprise.

Un management via le code implique la gestion des risques autour de ces opérations de management.

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



« 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



Progress fournit les meilleures technologies pour **développer**, **déployer** et **superviser** des applications métier critiques.

Enable your technology team to **do more, faster.**

 **Progress**[®]

Prédiction #5

Des compromissions de la chaîne d'approvisionnement

En 2022, les attaques contre la chaîne d'approvisionnement vont encore gagner en maturité, en portée et en sophistication. Il est à parier que beaucoup plus de solutions tierces et de pratiques de développement communes seront visées.

Prédiction #6

La fin des contrats de cyberassurance

On craint un tsunami d'annulations des cyberassurances et une course effrénée des entreprises pour obtenir une nouvelle couverture, potentiellement à des taux beaucoup plus élevés. Pour obtenir une couverture et s'assurer les meilleurs tarifs, les entreprises devront faire preuve d'une hygiène de cybersécurité élevée exigée par les souscripteurs de cyberassurance.

Prédiction #7

La fin de la liberté des réseaux sociaux

Il faut s'attendre à des contrôles plus stricts du contenu diffusé sur les plateformes sociales, à une attestation fiable de la source du matériel et, éventuellement, à un accès aux données pour les autorités.

Prédiction #8

Des détections toujours plus longues

L'année prochaine, le délai moyen entre l'intrusion et la détection augmentera, ce qui donnera aux attaquants plus de temps pour effectuer des reconnaissances et causer des dommages sur les systèmes. Ainsi, de nombreux pirates pourraient se frayer un chemin dans les systèmes et y établir des résidences à long terme.

Nous nous préparons à une panne d'envergure ou à un événement de type perte massive de données dans les cinq prochaines années.

Prédiction #9

De nouveaux records dont on se serait bien passé

Le nombre d'attaques fructueuses continuera d'augmenter, le coût moyen assumé par une entreprise victime et par attaque va également progresser, et le schéma va se répéter. Happés par toutes les nouvelles technologies attrayantes émergentes, les utilisateurs ont tendance à oublier les bases de la sécurité informatique.

AU-DELÀ DE 2022, DANS LES CINQ ANS A VENIR...

Prédiction #10

Le cataclysme

Nous nous préparons à une panne d'envergure ou à un événement de type perte massive de données dans les cinq prochaines années.

Prédiction #11

La résurrection digitale

À notre mort, les ressources digitales seront orphelines et non gérées, et les amis et membres de la famille ne connaîtront peut-être pas les mots de passe permettant de récupérer des informations inestimables. Aussi pourraient apparaître de nouvelles entreprises capables d'accéder à la présence digitale d'une personne après sa mort et de la préserver.

Prédiction #12

L'IoT, nouvelle poubelle de l'espace

Tout comme les débris spatiaux posent problème aux nouveaux satellites, les projets IoT abandonnés et les systèmes non pris en charge constitueront des cibles idéales pour les attaquants, ce qui sera amplifié par une connectivité 5G plus rapide.

Prédiction #13

Des zones libres de connectivité

Certaines populations vont vouloir s'opposer à ce que leur mode de vie traditionnel soit bouleversé par le tout connecté et créer des « zones libres de connectivité » dépourvues de technologie cellulaire et Wi-Fi, telles que des cinémas, des lieux de culte, etc.

Prédiction #14

Un avenir sans mot de passe ?

La disparition du mot de passe semble enfin gagner du terrain. Mais avec moins de points d'accès verrouillés par des mots de passe, les attaquants vont de plus en plus se concentrer sur l'exploitation des utilisateurs et des applications pour accéder aux données et aux privilèges.

Les graines de la mise en œuvre précipitée du travail à distance et de la transformation digitale ont porté leurs fruits sous la forme de brèches qui ne se produisent qu'une fois par décennie, comme celles de SolarWinds, Colonial Pipeline et d'autres qui semblaient se produire tous les mois. Regarder vers l'avenir nous permet d'anticiper vers où les acteurs de cybermenaces se dirigeront lorsqu'ils chercheront à tirer parti de ce changement de paradigme.

Source *BeyondTrust*



Envolée des besoins en calcul, stockage et connectivité

Quel est l'avenir des réseaux de communication ? A cette question, Huawei dévoile son rapport Global Industry Vision : Communications Network 2030. L'avènement de l'IoT entrainera une augmentation des besoins en calcul, stockage et connectivité que les réseaux traditionnels ne pourront fournir...

Une nouvelle ère de connectivité entre les personnes, machines et objets s'ouvre et les réseaux devront supporter les usages domestiques, les nouveaux services industriels intelligents et innovants, transformant la société (chirurgie médicale à distance, conduite autonome, villes intelligentes). De grandes quantités de ressources de calcul et de mise en réseau vont donc être indispensables...

D'ici 2030, quelles sont les prévisions ?

- 1 yettaoctet

Le monde générera 1 yettaoctet (1 000 milliard de téraoctets) de données par an, soit 23 fois plus qu'en 2020

- Connexions mondiales : 200 milliards

C'est le nombre total de connexions mondiales, dont 100 milliards de connexions sans fil (y compris les connexions cellulaires passives) et environ 100 milliards de connexions filaires, Wi-Fi et à courte portée

- Ressources informatiques multi-niveaux

Les utilisateurs seront connectés à des ressources informatiques multi-niveaux : une latence de 1 ms sera garantie pour la transmission des données dans les villes, 10 ms dans les agglomérations urbaines et 100 ms dans les réseaux très haut débit / optiques. Les réseaux offriront une disponibilité supérieure à 99,999 %

- Consommation mensuelle moyenne : 600 Go

La consommation mensuelle moyenne de données par personne sur les réseaux cellulaires sans fil sera multipliée par 40 pour atteindre 600 Go

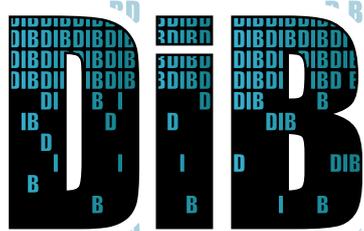
- Consommation par foyer : 1,3 To

La consommation mensuelle moyenne de données sur les réseaux fixes par foyer devrait être multipliée par 8 pour atteindre 1,3 To.

« En 2030, les réseaux de communication seront amenés à connecter des centaines de milliards d'objets et devront relever de nombreux défis. Tout d'abord, la complexité des infrastructures IoT rendra indispensable la construction de réseaux plus intelligents. Ensuite, les nouveaux usages industriels et agricoles mais aussi les véhicules autonomes exigeront des opérateurs qu'ils améliorent la couverture, la qualité, la sécurité et la fiabilité de leurs réseaux. Sans les réseaux, l'innovation numérique est impossible » Weiliang Shi, président de Huawei France.

Source - Huawei Intelligent World 2030 Forum - Rapport Global Industry Vision (GIV)

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



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



1992



1

équipe d'experts
à votre écoute



+20%

de croissance
en 2019



31 millions

d'euros de chiffre d'affaires
réalisé en 2019

DIB France vous facilite l'IT



**SOLUTIONS WORKPLACE
INFRASTRUCTURES & SECURITE
SERVICES & INTEGRATION**

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



www.dib-france.fr

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

Tél : 01 34 57 90 00

DIDDIBDIBDIBDIBDIBDIBDIBDIB

à une situation stable et sécurisée. Il s'agit de sonder l'environnement Active Directory, identifier les failles, erreurs de configuration dangereuses et autres faiblesses que les cyberattaquants pourraient exploiter pour voler des données ou installer des logiciels malveillants. En août 2021, nous avons réalisé une mise à jour de cet outil pour le marché français, en intégrant les recommandations de l'ANSSI concernant les points de contrôle.

En août 2021, nous avons réalisé une mise à jour de cet outil pour le marché français, en intégrant les recommandations de l'ANSSI.

L'autre annonce concerne l'ouverture vers les solutions Cloud de Microsoft, Azure Active Directory, afin de proposer des fonctionnalités de protection, monitoring et récupération après incident. La dernière version de DSP (Directory Services Protector) donne ainsi une vue d'ensemble de l'exposition aux risques dans les environnements hybrides et crée une vue unifiée des cyber-menaces provenant de l'Active Directory et d'Azure Active Directory.

Les nouvelles fonctionnalités de DSP dédiées à la détection et la remédiation des risques de sécurité des environnements d'identité hybride permettent de faire face aux attaques qui visent l'AD sur site pour pénétrer dans l'entreprise, puis se propagent sur le cloud, ou inversement. Dans les environnements AD hybrides, DSP unifie la présentation des indicateurs de sécurité, aussi bien pour l'AD que pour Azure AD.

De plus, nous voulons fournir à plus long terme des solutions liées à l'identité, et ce quel que soit le référentiel d'identité.



Matthieu Trivier

Un mot sur votre dernier rapport semestriel publié récemment. Pouvez-vous revenir sur les lacunes mises en évidence ?

Semperis a, en effet, publié son premier rapport semestriel sur la sécurité de l'Active Directory. Ce rapport traite du déferlement d'attaques visant l'identité et les vulnérabilités...

Rien que cet été, deux grandes vulnérabilités ont été relevées. Nous mettons ainsi en lumière de nombreuses erreurs de configuration réalisées bien trop souvent rapidement, un manque d'attention autour d'AD (serveurs non mis à jour, environnements vulnérables...), il faut vraiment réaliser en temps et en heure les mises à jour ! Enfin, nous voulons aussi alerter sur la gestion des privilèges, trop de privilèges ont été donnés pendant des années sans vérification faite ensuite.

Il faut repenser et renforcer la position de sécurité de l'identité qui s'est érodée après des années d'erreurs de configuration ou compétences inadaptées.

Et les perspectives 2022 ?

Après une expansion massive en 2021 côté effectifs, une ouverture en Asie (Singapour) et un renforcement du marché français (acteurs du CAC 40), nous allons poursuivre sur cette lancée.

Côté Cybersécurité, je dirais qu'il faut agir et rester en alerte ! Je reprendrai ainsi les propos marquants de Guillaume Poupard de l'ANSSI, « en 2019, nous avons fait 50 interventions, en 2020, nous en avons fait 200, et cela augmente sans cesse... ».

Mais j'espère un réel soubresaut dans cette prise de conscience de protection ! Restons confiants et agissons ensemble !

> Par Sabine Terrey



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

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



Rançongiciels : les 3 recommandations pour se protéger

Les cybercriminels mettent en œuvre de nouvelles techniques d'extorsion, des outils de piratage améliorés et des modèles économiques affinés.

Des opérations lucratives !

Pour preuve, le montant moyen des demandes de rançons est passé à 5,3 M\$ au premier semestre 2021, + 518 % par rapport à 2020 : 847 000 \$ en moyenne.

La rançon moyenne versée s'élève à 570 000 \$, + 82 % par rapport à 2020. La crise des ransomwares s'intensifie et les entreprises criminelles investissent dans des opérations lucratives basées sur des rançongiciels.

La quadruple extorsion

La tendance est identifiée par les consultants d'Unit42 : les exploitants de rançongiciels combinent jusqu'à quatre techniques pour pousser les victimes à payer.

- Chiffrement

Les victimes paient pour retrouver l'accès à leurs données brouillées et systèmes informatiques compromis qui ne fonctionnent plus à cause du chiffrement de certains fichiers clés

- Vol de données

Les pirates dévoilent des informations sensibles si la rançon n'est pas payée

- Déni de service (DoS)

Les gangs de rançongiciels lancent des attaques par déni de service qui font tomber les sites Web publics des victimes

- Harcèlement

Les cybercriminels contactent les clients, les partenaires commerciaux, les employés et les médias pour les informer du piratage de l'organisation.

Les 3 conseils pour se protéger

Découvrons quelques conseils de Jen Miller-Osborn, Directrice adjointe de l'Unit42, pour se prémunir de ces attaques.

Les pirates, en chiffrant les données, peuvent désactiver des systèmes informatiques stratégiques (centres d'appels d'urgence, fonctionnement des gazoducs, urgences des hôpitaux...).

Les rançongiciels posent un risque énorme pour la sécurité nationale, les grands groupes, les États et les petites entreprises. Il faut informer les collaborateurs des risques.

- Méfiez-vous des emails d'hameçonnage : si vous pensez en avoir reçu un, signalez-le

Les rançongiciels se diffusent principalement par le biais d'emails d'hameçonnage contenant des pièces jointes malveillantes. Le courriel frauduleux pousse le destinataire à répondre en l'incitant à cliquer sur un lien, à ouvrir une pièce jointe ou à fournir directement des informations sensibles. Il existe aussi des kits d'hameçonnage comprenant des logiciels de développement de site Web, du code, des logiciels de spam et du contenu qui peuvent être utilisés pour créer des sites Web et des emails convaincants.

- Mettez à jour vos appareils en leur appliquant les derniers correctifs logiciels

Les pirates exploitent souvent les failles logicielles pour propager leurs rançongiciels.

Un correctif logiciel va résoudre les failles de sécurité d'un logiciel afin de les rendre inexploitable par un pirate. Sinon, vous devez installer manuellement un correctif logiciel : assurez-vous de disposer des plus récents.

- Restaurez les fichiers chiffrés à l'aide de vos sauvegardes

Si vous êtes victime d'une attaque par rançongiciel, regardez si vous avez sauvegardé vos fichiers. Si c'est le cas, restaurez-les à partir de la dernière version. Si vous ne les aviez pas sauvegardés, vous pouvez considérer qu'ils sont perdus.

A la question « **Devons-nous payer la rançon ?** » toutes les victimes des attaques par rançongiciel sont confrontées à des décisions difficiles. Les professionnels peuvent vous conseiller. Mais préparez-vous : il existe des outils et des technologies de sécurité qui peuvent empêcher une telle attaque et vous éviter de devoir prendre cette décision difficile.

Rapport sur les menaces de ransomwares de l'Unit 42 Palo Alto Networks - 1^{er} semestre 2021

Azure Stratégie, BRIQUE ESSENTIELLE DE LA GOUVERNANCE

La gouvernance dans le Cloud c'est la garantie de profiter au mieux de ses ressources. C'est-à-dire dans les grandes lignes : auditer, gérer, optimiser et contrôler.

Lorsqu'il est question de Cloud Azure, la bonne pratique, voire la meilleure des pratiques est de s'appuyer sur les stratégies Azure (ou Azure Policy).



C'est un élément, une brique essentielle pour garantir la conformité et l'unicité des ressources déployées. Ressource est ici un terme global puisqu'il s'agit tout à la fois de IaaS, de PaaS mais aussi par exemple de personnalisation de portail.

Mais que se cache-t-il exactement derrière cette appellation de stratégie ? A quoi cela sert-il vraiment ?

C'est tout à la fois un outil d'audit, de bon usage, de contrôle des coûts ou de respect de la conformité. Mais aussi un outil de contrôle de déploiement, qui ne permettra pas de déployer tel ou tel composant ou qui imposera tel ou tel modèle. Et même dans certains cas, un outil de remédiation qui va "réaligner" et corriger les ressources.

Il ne faut pas sous-estimer les possibilités des stratégies, elles sont immenses et pratiquement infinies.

Présentation théorique

Une stratégie est composée de deux parties bien distinctes. Une règle de sélection ou condition, une action. Puis, cette stratégie est ensuite positionnée sur un scope pour être appliquée. Règle et scope sont deux choses différentes.

Les ressources de type machines virtuelles dont le nom commence par *windows*, voilà une règle.

L'attachement de cette stratégie sur un abonnement *monabo0001*, voilà le scope. Ainsi, une machine nommée *mamachine0001* n'est pas concernée par la règle. Même si elle est présente dans l'abonnement *monabo0001*.

Si cette machine est nommée *windows0001*, elle est concernée par la règle. Mais (il y a un mais), la stratégie ne s'applique que si cette machine virtuelle est dans l'abonnement *monabo0001*.

Vient ensuite l'action ou effet. Ces effets sont au nombre de 7. De l'audit à la modification en passant par l'interdiction. Un exemple d'effet sera présenté dans la partie pratique.

Sans aller trop loin dans le code, dans le fichier JSON ci-dessous apparaissent clairement la notion de règle (balise « *policyRule* ») et la notion d'effet (balise « *effect* »).

```
JSON
{
  "properties": {
    "displayName": "<displayName>",
    "description": "<description>",
    "mode": "<mode>",
    "parameters": {
      <parameters>
    },
    "policyRule": {
      "if": {
        <rule>
      },
      "then": {
        "effect": "<effect>"
      }
    }
  }
}
```

Une connaissance approfondie du code ne sera nécessaire que lorsqu'il s'agira de créer ses propres stratégies. Mais, il y a déjà beaucoup à faire avec les stratégies par défaut disponibles dans la console.



À la découverte de l'offre «M365 as your Digital Platform» d'Insight

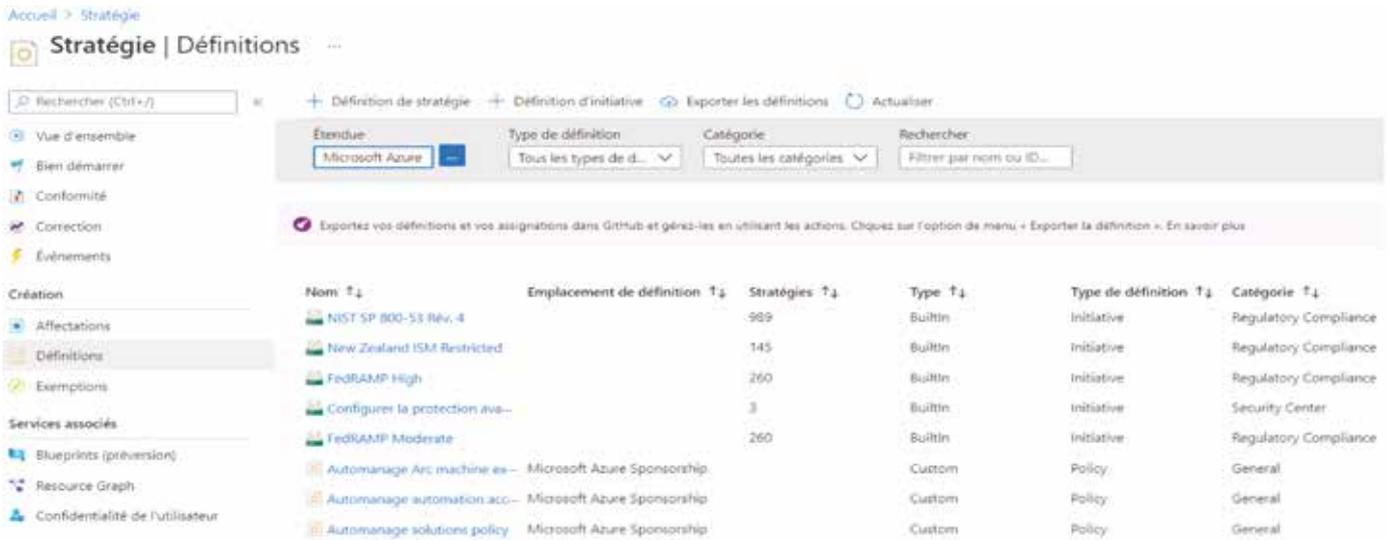
Découvrez une offre de conseil innovante et originale pour optimiser les coûts, favoriser l'adoption des outils et créer de la valeur métier en vous appuyant sur le potentiel de Microsoft 365.

Pour en savoir plus, rendez-vous sur fr.insight.com/solve/connected-workforce ou flashez ce code



Dans la pratique

Comme la fonctionnalité est très complète, elle a une console dédiée sur le portail.



Tout commence par le menu **Définitions** où se trouvent deux types de définition. Les **Policy** (le terme n'est pas traduit dans la console) et les Initiatives. Une initiative est en fait un regroupement de stratégies sur un même thème. On voit clairement dans l'écran précédent qu'une initiative peut porter deux stratégies, mais aussi... 989. On trouve également dans le menu des catégories comme **General, Security Center** ou **Backup**. Il est de cette façon plus facile de sélectionner un thème particulier.

Dans cette console, tout commence par la définition car c'est ici que condition et effet sont choisis. Dans l'exemple suivant, la stratégie se nomme **Configurer une sauvegarde sur des machines virtuelles sans étiquette donnée dans un coffre Recovery Services existant dans la même localisation**.

Voilà une règle de gouvernance élémentaire et indispensable lorsqu'il s'agit de machine de production.

Pour résumer, les conditions sont :

une machine virtuelle qui n'a pas d'étiquette (appelée également tags ou balises).

Une fois cette stratégie sélectionnée, il faut l'affecter.

Et lors de cette affectation (le scope ou cible de déploiement), il faut choisir l'un de effets proposés par la stratégie. On retrouve dans l'image suivante quelques-uns des points listés.

Dans cette console, tout commence par la définition car c'est ici que condition et effet sont choisis.

Il est intéressant de noter que cette stratégie possède plusieurs effets : *deployIfNotExists*, *auditIfNotExists*, *disabled*. L'affectation se fait enfin sur une étendue (Groupe de management, Abonnement, groupe de ressources). Dernière subtilité, si l'effet choisi est de type déploiement (*deployIfNotExists*) et que le choix de l'administrateur est de créer une tâche de remédiation lors de l'affectation, la console propose de créer automatiquement une identité managée pour effectuer les actions. Si cette identité est de type système, elle est attachée au cycle de vie de l'affectation. Cela signifie que dès que l'affectation est retirée, l'identité liée est automatiquement supprimée.

Si cette identité est de type système, elle est attachée au cycle de vie de l'affectation.

Configurer une sauvegarde sur des ma

Définition de stratégie

Affecter Modifier la définition Dupliquer la définition

Bases

Nom
Configurer une sauvegarde sur des machines virtuelles sans étiquette...

Description
Appliquez une sauvegarde à toutes les machines virtuelles en les s...

Effets disponibles
deployIfNotExists, auditIfNotExists, disabled

Catégorie
Backup

Comme elle est affectée, cette définition est maintenant visible dans la console dans le sous menu **Affectations**. Au bout de quelques minutes, le temps de la vérification de l'état et des conditions, la stratégie affiche un pourcentage de **Conformité**. C'est un écran très utile à l'échelle d'une entreprise ou l'on retrouve des dizaines de stratégies avec leur niveau de conformité.

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

CAP IT

| BANQUE | ASSURANCE | FINANCE |

SAVE THE DATE

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

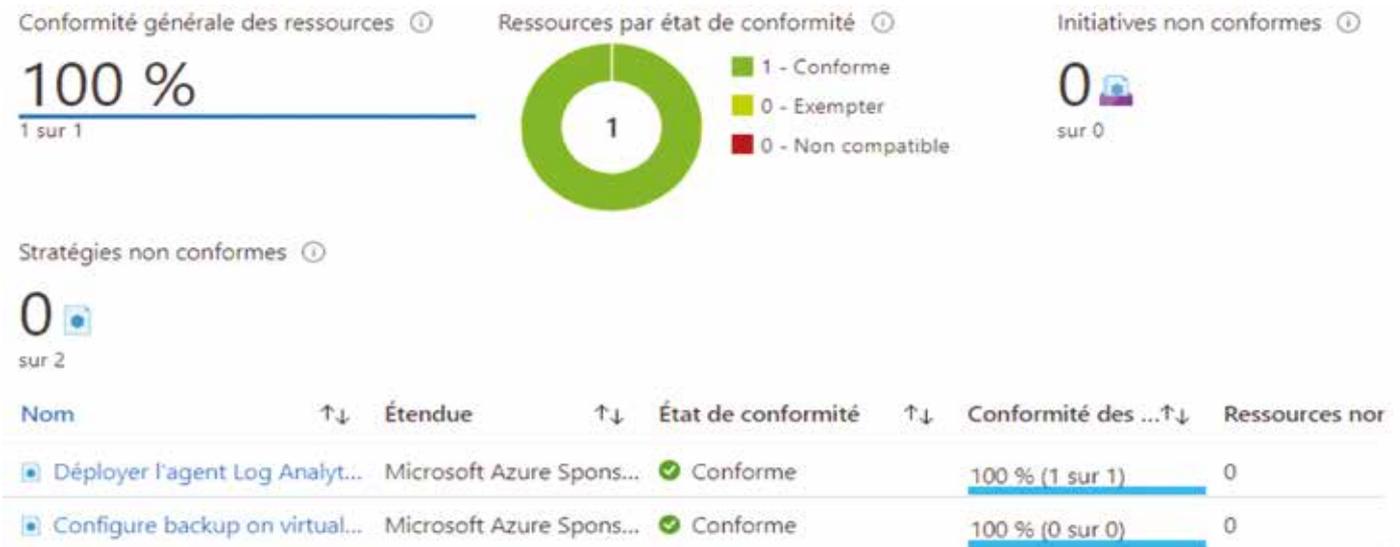
500 donneurs d'ordre attendus
sur deux jours

48h de débats et contenu spécialisé à haute
valeur ajoutée

80 speakers experts en conférences et salles
ateliers métier

40 sponsors & partenaires acteurs clés

Réservez votre badge sur www.cap-it.fr



Voilà un tableau de suivi qui offre une vue synthétique et expose un taux global puis le taux pour chaque stratégie.

Enfin, si l'effet est de type `deployIfNotExists` (ce n'est pas le seul effet qui va effectuer de la remédiation), c'est le sous menu **Correction** qui va afficher le statut des remédiations.

Ce cycle Définitions => Affectations => Conformité => Correction (facultatif) est bien le meilleur moyen de « gouverner » son Cloud Azure. Et d'assurer automatiquement que ce qui est décidé est bien appliqué.

Présenter cette belle mécanique en quelques pages est impossible, mais comprendre la philosophie du produit est important. Enfin, se lancer dans ce mode de gouvernance est certainement une très bonne idée pour simplifier la gestion de ses ressources Azure.

En synthèse, un rappel des points importants :

- 1 / La gouvernance est au centre des préoccupations pour qui veut optimiser et contrôler la bonne utilisation de ses ressources.
- 2 / Les stratégies sont des conditions et des effets positionnés sur une cible, un scope.
- 3 / Les effets vont du simple audit à la remédiation des ressources dont la conformité n'est pas valide.

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



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 !





Top 3 des changements stratégiques des responsables IT pour 2022

Valeur ajoutée, continuité des opérations, innovation, agilité, la pandémie bouleverse la donne. Les responsables IT affichent leurs motivations, préoccupations, priorités et perspectives d'évolution.

Changement de cap

Les responsables IT français se concentreront sur le développement de leurs compétences : la cyber-résilience - 51 %, la réflexion et la vision stratégique - 47 %, les méthodologies expérimentales/agiles - 42 %, au cours de l'année à venir.

Ils veulent privilégier de solides partenariats avec les autres dirigeants : plus de la moitié avec le directeur financier, 38 % avec le directeur des opérations, et 35 % avec le directeur produit.

Enfin, 1 responsable informatique sur 5 en France est réellement motivé par la technologie, les priorités portent sur les perspectives d'évolution et sur l'augmentation du retour sur investissement.

Le rôle des données

Si les données sont essentielles dans la réussite de l'entreprise, les responsables IT français - 74% sont fiers de leur rôle au cours de l'année dernière.

Ils veulent contribuer à la transformation numérique, aux efforts de changement mis en œuvre, aider et accompagner leurs collaborateurs dans leur carrière informatique, leur nouveau rôle stratégique.

Les défis métiers

Les responsables IT sont bien plus en accord avec les dirigeants métier, avec un alignement des besoins respectifs à 61 %. Les responsables IT sont conscients de l'importance de leur contribution au niveau de l'infrastructure technologique en place, de l'agilité des méthodes de travail et de la culture informatique.

Quelques mécontentements toutefois à noter pour plus de 1 sur 3 sur la non reconnaissance des résultats obtenus, mais aussi sur la concurrence des priorités, la gestion réactive et non proactive des urgences, la pression constante d'innover tout en réduisant les coûts.

Santé mentale, Ecologie, Diversité & Inclusion

Pour 2022, les responsables IT concentreront leurs efforts sur les 3 objectifs stratégiques :

- La santé mentale de leur personnel - 43%

- Le programme écologique

42 % indiquent que la durabilité sera une de leurs préoccupations majeures

- La diversité et l'inclusion

38 % souhaitent travailler sur les questions de diversité et d'inclusion.

Les 4 priorités

Voici les 4 grandes priorités des spécialistes technologiques pour les 12 mois à venir, à savoir :

- L'agilité

Incorporer et accélérer l'agilité dans l'entreprise - 87 %

- Les coûts

Optimiser les coûts/réajuster le service informatique - 82 %

- Les clients

Améliorer l'expérience numérique/optimiser le parcours du client - 81 %

- Le travail à distance

Améliorer l'expérience numérique pour un avenir tourné vers le travail à distance ou des approches hybrides - 77 %

Source Etude PureStorage & Insight Avenue - 504 responsables informatiques - Organisations européennes de plus de 500 employés, dont 100 en France - avril/mai 2021 au Royaume-Uni, en Allemagne, en France, en Espagne, en Italie, aux Pays-Bas et en Suisse.

Paessler : LE RÔLE CLÉ DE LA SUPERVISION DANS LA RÉDUCTION DE CONSOMMATION DES RESSOURCES NATURELLES

De l'orientation stratégique innovante vers la supervision des environnements industriels jusqu'aux dernières annonces, l'actualité est riche chez Paessler. Rencontre avec Fabien Pereira Vaz, Technical Sales Manager EMEA.



Découvrez pourquoi Paessler est convaincu du rôle clé de la supervision dans la réduction de consommation des ressources naturelles de la planète.

Pouvez-vous nous expliquer l'orientation stratégique prise par l'entreprise ?

Paessler qui est entreprise spécialisée dans la supervision des réseaux, a la volonté aujourd'hui de réduire activement l'empreinte de l'homme sur son environnement, en s'appuyant sur le monitoring et la supervision des ressources.

Pour mener à bien cette mission, Paessler se donne donc les moyens et développe plusieurs axes. Nous allons continuer à faire de la supervision dans le monde de l'infrastructure informatique classique,

certes, mais nous allons également développer plus amplement notre offre déjà initiée, par le biais d'un écosystème de partenariats dans le domaine de l'OT (Technologies Opérationnelles dans l'industrie) afin que notre solution puisse s'ouvrir et superviser les objets connectés dans l'industrie. Enfin, nous souhaitons poursuivre dans des environnements plus commerciaux c'est-à-dire la ville ou les bâtiments.

Dans le cadre de ce troisième axe, nous avons lancé Paessler Building Monitor, qui est un produit indépendant de notre solution initiale qu'est PRTG. Nous le voulons indépendant car il s'adresse à des gestionnaires d'installations et propriétaires de bâtiments pour optimiser l'évolution des bâtiments et leur consommation en énergie. Ce logiciel SaaS assure une supervision numérique 24h/24 de l'état des immeubles.

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



www.promodag.fr

Pouvez-vous préciser les contours de cette offre ?

Aujourd'hui dans les bâtiments, face à une faible adoption du digital, il en résulte une collecte manuelle des données. Le statut des objets est bien loin d'être établi en temps réel car les données ne sont pas actualisées.

Nous allons donc donner la possibilité avec Paessler Building Monitor d'interagir avec des objets IoT exploités via un réseau (technologie LPWAN). Le but de notre applicatif est de pouvoir s'intégrer sur ces objets, de récupérer les données en temps réel, de les afficher sous forme de tableaux de bord et de notifier les gestionnaires d'immeubles des changements survenus. Bien sûr, le bénéfice attendu est de détecter en amont les anomalies et d'anticiper les dommages liés à la désuétude, fuites de gaz, d'eau, moisissure, climatisation ...On parle ici de maintenance préventive.

Ce logiciel SaaS assure une supervision numérique 24h/24 de l'état des immeubles.

Nous pouvons aussi donner des informations factuelles pour réduire l'empreinte énergétique, et nous aligner avec les directives et correspondre aux exigences gouvernementales de plus en plus fortes. Avec les éléments récoltés, les informations sont tangibles et permettent d'agir concrètement.

Le produit s'adapte donc aux besoins spécifiques ?

Absolument. Un premier partenariat lancé en Allemagne (avec Rehnig) a débouché sur une réalisation : nous avons donc des modèles, des KPI significatifs à disposition qui s'adapteront en fonction des besoins spécifiques de chaque bâtiment. La solution est donc totalement personnalisable.

Pour assurer la récupération des données en temps réel, nous voulons nous assurer que les objets des bâtiments répondent aussi à des normes de sécurisation (compteurs intelligents, caméra de surveillance ...) et notre produit supervise ces éléments pour renforcer la sécurité.

Pour ce produit, vous évoquez « une supervision facile, sans compétence particulière » pouvez-vous nous en dire plus ?

Effectivement, c'est un point fort du produit. Nous mettons en place des cas d'usage préconfigurés, en nous appuyant sur des modèles qui comprennent des limites de valeur par défaut pour faciliter la mise en œuvre (moisissure, qualité de l'air, statut des lumières,



Fabien Pereira Vaz

accès au secours, circuits de chauffage...), avec un tableau de bord structuré et intuitif qui convertit les données en informations utiles pour l'utilisateur.

Cette solution de supervision à distance est facile à mettre en place et à utiliser, et ne nécessite aucune compétence et connaissance en programmation.

Un assistant intuitif connecte les appareils IoT du bâtiment au logiciel de supervision et les modèles de cas d'utilisation permettent aux utilisateurs de commencer immédiatement leur supervision.

Nous mettons ainsi notre expertise dans la supervision à disposition et nous l'appliquons aux bâtiments.

Un mot sur les perspectives pour l'année 2022 ?

Nous allons poursuivre le développement des capteurs qui vont aider nos clients (Cloud, supervision des environnements virtualisés), car notre solution PRTG facilite l'import de capteurs dans le domaine de l'IT, et c'est un pilier de notre stratégie.

Cette solution de supervision à distance est facile à mettre en place et à utiliser, et ne nécessite aucune compétence et connaissance en programmation.

La volonté de l'entreprise est de s'émanciper de la solution mono plate-forme en la déclinant dans l'IT classique et le monde de l'industrie. Avec Paessler Building Monitor, on initie un nouveau mouvement et on diversifie notre portefeuille. Notre axe de développement futur touche ainsi tout ce qui concerne le Smart Monitoring.

> Par Sabine Terrey



Les DSI progressistes pilotent la fonction Finance en 3 étapes

La pandémie a accéléré d'au moins un an la transformation de la fonction Finance, selon les DSI.

Mais les pressions sont fortes, il faut adapter les stratégies de transformation numérique, sans perturber les activités critiques. Les DSI progressistes pilotent cette transformation avec une approche plus stratégique, collaborative et basée sur les données. En effet, la modernisation des opérations financières est cruciale pour l'entreprise.

L'accélération numérique impacte les pratiques des DSI

Les DSI sont actifs dans la transformation de la fonction Finance et des stratégies mises en place pour faire face à l'évolution des besoins métiers et technologiques :

- 70 % des DSI auraient accéléré d'au moins un an la transformation de la fonction Finance.

Les DSI progressistes ont mis en place des partenariats stratégiques au sein de leur organisation :

- le service IT est bien plus aligné avec les autres fonctions et services de l'entreprise qu'il y a un an, selon 90%

Ainsi « DSI progressistes se concentrent sur la collaboration entre services informatique et financier, l'exécution l'agile et le bon usage des données. Ils s'efforcent de fournir aux équipes financières les outils nécessaires pour accélérer leur transformation et obtenir des résultats stratégiques » souligne Sheri Rhodes, Chief Information Officer de Workday.

La fonction Finance pilotée par les DSI progressistes en 3 axes

Les DSI progressistes se distinguent par leur approche en matière de transformation financière en termes de stratégie, de collaboration, et de choix technologiques, et ils soutiennent la transformation de la fonction Finance selon 3 axes :

- L'exploitation des données = faciliter la prise de décision

Les DSI progressistes priorisent le rapprochement et la gestion des données et comprennent l'importance d'une utilisation efficace des informations. Selon 92%, la priorité est l'agrégation des données financières en une source unique de données.

- La collaboration avec la fonction Finance = piloter la transformation

83 % des DSI progressistes s'attendent à "ne pas atteindre leurs objectifs de croissance si les services informatique et financier ne collaborent pas plus étroitement."

- L'adoption d'une approche Cloud agile et progressive = se transformer

Plus de la moitié des DSI progressistes (37 % échantillon total) déploieront en continu de nouvelles fonctionnalités dans le cadre d'une stratégie Cloud, pour moderniser les ERP, minimiser les perturbations, mener des initiatives numériques avancées.

Source Workday & Deloitte Global - A More Effective CIO-CFO Partnership - 600 cadres d'entreprise du monde entier. Les plus performants, les "DSI progressistes", ne représenteraient que 8 % de cet échantillon.



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

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

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

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

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

Suivez-nous sur **Twitter** : www.twitter.com/itprofr



Partagez sur **Facebook** : www.facebook.com/www.itpro.fr



 **iTPro.fr**

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



Il se base sur la connaissance que Datadog a pu construire en observant la façon dont de nombreuses entreprises gèrent la sécurité de leurs applications et définit un ensemble de compétences-clés pour évaluer ses progrès dans l'adoption des pratiques DevSecOps.

Les processus de sécurité des entreprises d'aujourd'hui

Avec plus de 10 ans d'accompagnement auprès de 15 000+ entreprises dans leur adoption des pratiques DevOps (et maintenant DevSecOps), Datadog a pu observer des entreprises à tous les stades de leur maturité DevSecOps et en tire les conclusions suivantes :

Les équipes DevOps avancent plus vite que la sécurité. La sécurité peut rapidement devenir un goulot d'étranglement dans le processus de delivery (livraison), si elle ne met pas en place les bons processus pour suivre le rythme. C'est pourquoi les dirigeants sont conscients qu'il est nécessaire d'ajouter de meilleurs contrôles de sécurité directement au niveau du développement pour accélérer la delivery des logiciels et réduire les risques de vulnérabilité applicatives.

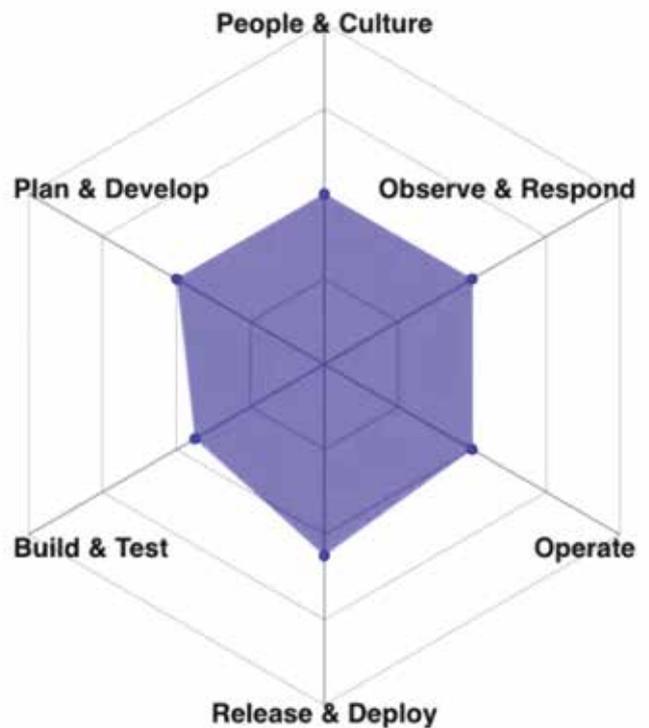
La sécurité est une pratique trop souvent silotée. Les équipes sécurité utilisent souvent des outils, des processus et une terminologie différents de ceux des DevOps, ce qui rend plus difficile l'intégration des pratiques de sécurité dans les workflows de développement existants.

Les entreprises se préoccupent de la sécurité de plus en plus tôt au cours du cycle de développement. Les équipes DevOps prennent de plus en plus de responsabilités en matière de sécurité, et les équipes sécurité elles-mêmes interviennent de plus en plus tôt au cours du cycle de développement. Cette évolution nécessite des changements substantiels dans toute l'entreprise pour une adoption réussie de la culture DevSecOps.

L'adoption de la méthodologie DevSecOps est plus rapide pour les entreprises avec une culture DevOps bien implantée. Cependant, même les entreprises matures constatent des lacunes importantes dans l'observabilité de la sécurité des applications, telles que l'absence de métriques de sécurité bien définies et visibles par toutes les équipes.

Six champs de compétences clés à évaluer pour mettre en place une culture DevSecOps

Datadog a identifié six compétences essentielles à la mise en place de processus DevSecOps au sein des entreprises. Comprendre la façon dont ces compétences impactent les entreprises et leur SDLC permet de clarifier le concept parfois abstrait de DevSecOps et d'identifier les étapes requises pour progresser dans l'adoption de cette méthodologie.



Culture

La culture de votre organisation est clé dans la construction de processus DevSecOps matures. Quatre domaines sont à examiner pour donner la priorité à la sécurité des applications à toutes les étapes du SDLC, depuis la planification et le développement de la fonctionnalité au monitoring applicatif post release :

- *Communication* : supprimer les silos entre les équipes impliquées et promouvoir une communication régulière.
- *Onboarding* : permettre aux nouveaux membres des équipes de se familiariser rapidement avec les processus de développement.

- **Responsabilisation** : encourager la transparence des équipes et leur prise de décisions dans les développements.
- **Bonne santé des équipes** : bâtir un environnement propice à la bonne santé et à la productivité des équipes.

Planification et développement

La prise en compte des aspects de sécurité dès les étapes de planification et de développement du SDLC permet aux équipes d'avoir suffisamment de temps pour mettre en œuvre des mesures de sécurité adéquates et ainsi diminuer le risque d'introduire des vulnérabilités pour les clients. Plus difficiles à corriger dans les dernières étapes du cycle de développement, les vulnérabilités de sécurité nécessitent en effet souvent de modifier fondamentalement l'architecture d'une application alors que le temps presse.

Le modèle de maturité Datadog comprend quatre points de mesure pour aider les entreprises à évaluer leurs pratiques DevSecOps au stade de la planification et du développement :

- **Évaluation des risques** : créer des évaluations complètes des risques et des modèles de menaces lors de la conception de nouvelles fonctionnalités.
- **Gestion de la dette technique** : prendre des décisions de conception qui minimisent la dette technique.
- **Priorisation** : mettre en place des processus pour prioriser les fonctionnalités et les bugs.
- **Validation du code** : tester régulièrement la qualité et la sécurité du nouveau code à l'aide de tests de validation intégrés au processus de développement.

Conception et test

Les phases de conception et de test de nouvelles fonctionnalités peuvent prendre du temps. Elles permettent aux équipes de mettre au point leur code pour en corriger les bugs et éventuels problèmes d'utilisation. L'ajout de pratiques DevSecOps à ces étapes permet aux équipes d'ingénierie de traiter et prioriser les vulnérabilités de sécurité de la même façon que pourraient l'être des bugs ou problèmes de conception.

Le modèle de maturité Datadog met en évidence les aspects du SDLC où un monitoring performant permet aux entreprises d'identifier automatiquement les problèmes de l'application et

ainsi d'éviter de construire des fonctionnalités qui pourraient représenter une menace pour les clients finaux :

- **Quality assurance et automatisation des tests** : exécuter régulièrement différents types de tests automatisés pour vérifier les fonctionnalités des applications.
- **Scan de code** : effectuer des scans réguliers pour détecter de potentielles vulnérabilités et autres problèmes connexes.
- **Validation des builds** : utiliser des tests pour vérifier que les nouveaux builds sont conformes aux politiques de sécurité et de développement.

Release & déploiement

Les stratégies de déploiement doivent aider les entreprises à livrer du code avec aussi peu d'incidents ou erreurs de configuration que possible, tout en leur permettant de répondre rapidement à tout problème survenant à cette étape. Le modèle de maturité DevSecOps encourage les entreprises à examiner les domaines suivants pour déterminer si leurs équipes sont en mesure de déployer de nouvelles fonctionnalités de manière stable :

- **Automatisation des déploiements** : déployer automatiquement le code dans les différents environnements pour minimiser les erreurs utilisateurs et les mauvaises configurations.
- **Validation des déploiements** : exécuter des contrôles de validation et de sécurité avant tout nouveau déploiement.
- **Remédiation des déploiements** : mettre en place des roll backs automatiques en cas de modification du code qui altère la fonctionnalité ou expose une vulnérabilité de sécurité.



Pierre Bétouin

Exploitation

L'infrastructure sous-jacente à une application est essentielle à la création d'applications sécurisées et doit devenir une priorité à mesure que les processus DevSecOps de l'entreprise mûrissent. Datadog recommande aux entreprises d'évaluer les domaines suivants pour s'assurer qu'elles bâtissent une infrastructure avec des mesures de sécurité appropriées, capables de supporter des applications à haute disponibilité et de rapidement se remettre d'incidents critiques :

- *Gestion de la plateforme* : tirer parti de "l'infrastructure as code" pour gérer automatiquement les configurations et les ressources de sécurité.
- *Planification des ressources* : baser ses ressources sur les besoins quotidiens et la croissance saisonnière.
- *Scaling* : adapter automatiquement les ressources à la demande pour mieux absorber les attaques.
- *Fiabilité* : distribuer les ressources d'infrastructure dans plusieurs régions et zones de disponibilité.
- *Tests de résilience* : tester régulièrement la résilience de l'infrastructure en implémentant du chaos engineering.
- *Correctifs* : automatiser les processus d'identification et de correction des vulnérabilités.
- *Disaster recovery* : définir un plan de reprise complet pour récupérer les ressources de l'infrastructure en cas de sinistre, et ce, y compris en cas d'incident lié à la sécurité.

Observabilité et résolution

Après un déploiement en production, il est nécessaire pour les entreprises de pouvoir détecter et traiter toute nouvelle vulnérabilité ou menace qui pourrait compromettre leurs applications. Encore une fois, Datadog a identifié plusieurs domaines auxquels les entreprises doivent prêter attention pour s'assurer qu'elles sont en mesure de les monitorer proactivement.

- *Service Level Objectives (SLOs)* : utiliser des SLOs et des budgets d'erreurs pour orienter les décisions d'ingénierie et mesurer la fiabilité du service.
- *Scanning* : effectuer régulièrement des scans d'infrastructure pour détecter de potentielles vulnérabilités et erreurs de configurations des services.
- *Security monitoring* : définir et collecter des KPIs (indicateurs clés de performance) de sécurité mesurables à travers l'ensemble des services.

- *Données centralisées* : utiliser une plateforme centralisée pour monitorer les performances et l'expérience utilisateur des applications.
- *Gestion d'incidents et post mortems* : encourager des analyses exhaustives de la "root cause" (raison première) avec des runbooks détaillés sur la gestion d'incidents.

Soutenir la culture DevSecOps

Ce modèle de maturité a été développé par Datadog afin d'apporter aux entreprises de la visibilité sur les pratiques à adopter pour mettre en place une culture orientée DevSecOps au sein des équipes d'ingénierie et ainsi évoluer vers des applications plus résilientes et sécurisées. Évaluer la situation actuelle de son entreprise à travers ce prisme donne des clés de compréhension pour mieux envisager la transition des méthodologies DevOps classiques vers des pratiques DevSecOps plus matures. Après avoir identifié les compétences les plus importantes pour elle, l'entreprise est en mesure d'élaborer les plans d'amélioration dans chacune : introduction de nouveaux outils, de nouvelles formations et de nouvelles équipes afin de soutenir la transition.

Évaluer la situation actuelle de son entreprise à travers ce prisme donne des clés de compréhension.

A mesure que ces pratiques s'implantent au sein de l'entreprise, les équipes en ressentent les bienfaits sur toutes les problématiques de sécurité de l'entreprise et voient les cycles de développement produit s'accélérer. Cela se matérialise finalement par un produit à plus forte valeur ajoutée, et des applications plus fiables et sécurisées pour les utilisateurs finaux.



**DÈS MAINTENANT
SUR ITPRO.FR**

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

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

Le monde tourne avec des logiciels.

Nous nous assurons que ça fonctionne.

Parfaitement.

Se transformer plus rapidement
avec une observabilité
et une automatisation intelligentes



Essayez notre plateforme
maintenant et gratuitement : >
dynatrace.fr/trial

 **dynatrace**

Comment développer UNE APPLICATION DE RECHERCHE DE CONTENU AVEC APACHE LUCENE ? - PARTIE 1

La donnée est le carburant de l'économie Numérique. Elle a toujours été le support de toute prise de décision efficace. Dans le *Data Mining*, l'augmentation du volume de données permet d'accroître la précision des informations et d'éclairer d'avantage les prises de décision.



Cependant, en Interne, beaucoup d'entreprises souffrent de l'incapacité qu'ont leurs employés à retrouver du contenu dans leurs fichiers. Avec la quantité phénoménale des données qui prévaut actuellement, l'indexation de contenu est la technique principale utilisée pour rechercher de façon efficace du contenu.

L'indexation de contenu permet de réaliser les recherches en se basant d'une part sur un index et d'autre part sur un score de similarité qui attribue un niveau d'importance à chaque fichier. Beaucoup d'outils qui implémentent ces techniques d'indexation de contenu ont été développés. Pour la recherche à large échelle certains de ces outils sont distribués et scalables. La fondation Apache dispose actuellement de trois outils de recherche de contenu : Apache Lucene, Apache Lucy et Apache Solr.

Dans ce tutoriel complet, nous allons vous montrer comment développer une application de recherche

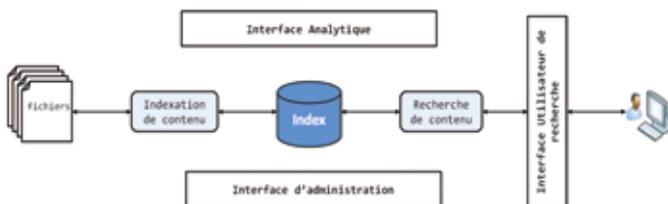
de contenu avec Apache Lucene. Le but n'est pas de faire de vous des experts sur Lucene, mais de vous montrer les étapes de développement, les illustrer par des modèles de code et vous inspirer quant à la façon dont vous pouvez l'utiliser pour développer des applications de recherche de contenu.

1. LES ÉTAPES DU DÉVELOPPEMENT D'UNE APPLICATION DE RECHERCHE DE CONTENU

Avant d'entrer dans le développement proprement dit d'Apache Lucene, et même de tout moteur d'indexation de contenu, il est critique que vous soyez au point sur l'architecture et la méthodologie de développement d'une application de recherche de contenu. Celles-ci sont indépendantes des outils de recherche de contenu et vous permettent de séparer la structure de vos applications de la technologie dans laquelle elles sont implémentées.

1.1 Architecture d'une application de recherche de contenu

Il est très courant de confondre *une application de recherche de contenu avec un moteur de recherche de contenu*. En réalité, ces deux choses, bien que similaires en apparence, sont totalement distinctes. Le moteur de recherche de contenu fait référence à un moteur NoSQL d'indexation de contenu. C'est une application dont le but est d'indexer et de retrouver du contenu sur la base des critères fournis par l'utilisateur. Une application de recherche de contenu quant à elle fait référence à une application (métier) à laquelle a été intégré un moteur d'indexation de contenu ou des fonctionnalités d'un moteur d'indexation de contenu. Par exemple, vous pouvez développer une application Web de gestion de tickets de cinéma, ensuite décider d'y intégrer les fonctionnalités d'indexation et de recherche de contenu d'un moteur de recherche pour faciliter la recherche de contenu aux internautes. Le développement d'une application de recherche de contenu se fait toujours selon l'architecture suivante :



Architecture d'une application de recherche de contenu

Toute application de recherche de contenu est constituée de 6 composants. En d'autres termes, développer une application de recherche de contenu va vous demander le développement de 6 composants : un index, une interface de recherche utilisateur, un module de recherche de contenu, un module d'indexation de contenu, une interface analytique et une interface d'administration.

- **L'index** : au départ de l'application, vous avez une large base de fichiers, de documents ou de données que vous voulez interroger. Supposons que vous souhaitez rechercher dans cette base tous les documents qui contiennent certaines expressions ou certaines phrases. Par exemple : « la liste des livres publiés il y'a 8 mois sur le sujet «Big Data» qui contiennent en première de couverture le mot «Hadoop» ». Pour traiter une telle requête, une approche naïve consisterait à scanner séquentiellement tous les documents à la recherche de chaque mot. Même si cette approche fonctionnerait, elle ne serait pas appropriée à cause du volume de données et du temps nécessaire pour exécuter avec succès la requête. La meilleure

approche pour résoudre ce problème consiste à construire un index, c'est-à-dire à regrouper dans une liste tous les mots qui apparaissent dans l'ensemble des documents, et pour chaque mot, l'ensemble des identifiants des documents dans lesquels il apparaît. Cet index sera ensuite stocké soit en mémoire, soit sur le disque dur et servira de socle à tous les autres modules de l'application de recherche de contenu. Il élimine la latence liée à l'accès séquentiel des fichiers et permet de rechercher du contenu exactement comme l'index d'un livre le permet. Ainsi, la première des choses à faire lors du développement de votre application de recherche consiste à identifier les fichiers que vous allez utiliser et les indexer. Le processus et les techniques d'indexation varient en fonction des moteurs ;

- **Le module d'indexation de contenu** : le développeur s'appuie sur une classe ou une fonctionnalité offerte par le moteur pour développer un module d'indexation de contenu. Ce module a pour vocation de construire l'index et de le mettre à jour au fur et à mesure de l'ajout de nouveaux documents. C'est dans ce module que les techniques d'amélioration de la qualité du dictionnaire de l'index telles que le N-Gram, l'extraction d'entité, le stemming ou encore la recherche de proximité peuvent être utilisées. Le développeur également va s'appuyer sur des modèles de calcul distribués tels que le MapReduce pour lancer la construction et la mise à jour de son index à des moments précis ;

- **Le module de recherche de contenu** : Pour rappel, la recherche de contenu est un processus qui consiste à chercher des termes dans un index pour retrouver les documents dans lesquels ils apparaissent. Le développeur s'appuie également sur une classe ou une fonctionnalité offerte par le moteur d'indexation de contenu pour développer son algorithme de recherche. Cet algorithme varie en fonction du cas d'utilisation. Le développeur peut implémenter l'un des 6 types de recherche que nous avons vus dans le chapitre précédent à savoir la recherche de texte intégrale, la recherche vectorielle, la recherche géographique, la recherche réseau, la recherche facettée et la recherche N-Gram. Par exemple, si l'utilisateur développe une application de géolocalisation, il peut utiliser un moteur d'indexation de contenu pour y implémenter la recherche géographique. C'est aussi dans ce module que le développeur implémente la métrique de mesure de similarité qui indique le niveau d'importance de chaque document et la pertinence de la recherche des utilisateurs ;

- **L'interface utilisateur de la recherche** : l'interface utilisateur est l'interface que voit l'utilisateur et qui lui permet d'interagir avec l'application. Généralement, elle se présente comme une page dans un navigateur Web, une application

de bureau, une application mobile. Bien que ce composant soit le plus simple, il est le plus important car plus il est difficile à utiliser et moins l'application sera utilisée. Nous verrons plus bas ce qui peut rendre une interface utilisateur difficile à utiliser. Rendez l'interface très simple à utiliser, dans l'idéal il faudrait qu'elle soit similaire à Google et qu'elle permette à l'utilisateur de directement entrer sa requête sans aucun processus supplémentaire ;

- L'interface analytique : c'est une couche qui ajoute de l'intelligence dans vos applications de recherche de contenu. Elle s'exécute souvent dans une machine séparée sur un moteur de Reporting. Elle génère des rapports sur l'utilisation de l'application de recherche de contenu qui peuvent être utilisés pour améliorer les prises de décision. Dans un site e-commerce par exemple, des modules analytiques fournissent un rapport sur les recherches qui ont été effectuées sur le site et qui n'ont pas fourni des résultats satisfaisants, les liens de résultats sur lesquels les utilisateurs ont cliqué, les achats qui surviennent ou pas après les recherches, ce qui permet de faire des offres ciblées à l'utilisateur et d'améliorer son expérience d'utilisation. Les moteurs d'indexation de contenu comme Lucene offrent des métriques analytiques telles que le type de recherche effectué, les requêtes de faible précision, les requêtes sur lesquelles les utilisateurs n'ont cliqué sur aucun résultat, etc. ;

- L'interface administrateur : une application de recherche de contenu est un assemblage de plusieurs modules complexes qui ont besoin d'être configurés de façon particulière. L'interface administrateur permet de gérer l'infrastructure de l'application (démarrage et stoppage des machines, gestion des pannes, gestion de la santé globale du système, restauration du système, scalabilité du système, configuration du système) et ses aspects sécuritaires.

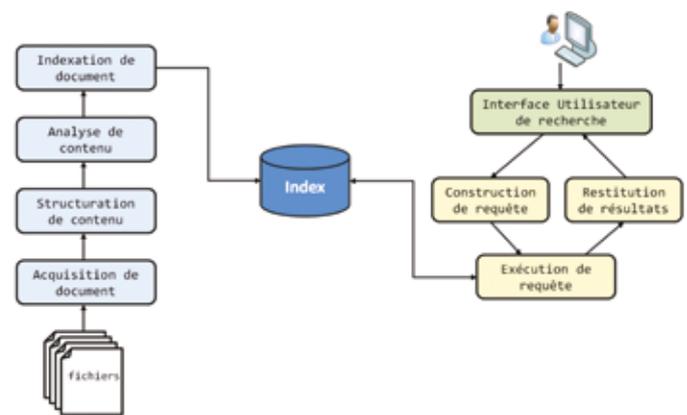
Toute application de recherche de contenu est développée suivant cette architecture et contient presque toujours ces 6 couches. Les fonctions de ces 6 couches sont réparties entre l'application et le moteur d'indexation de contenu. Retenez bien cela car beaucoup de professionnels ont tendance à confondre l'application avec le moteur d'indexation de contenu et croient à tort que le moteur d'indexation de contenu est l'application d'indexation de contenu.

En fait celui-ci en est le support. Pour que vous compreniez la relation entre ces deux éléments, nous allons prendre l'exemple du développement des bases de données relationnelles. Dans une base de données relationnelle, le SGBDR est le support de stockage de la base de données, tandis que

les applications métiers exploitent cette base de données à travers d'une part les classes fournies par un Framework de programmation (.NET, JEE, etc.) et les API fournies par le SGBDR. Dans le cas de la recherche de contenu, le moteur d'indexation de contenu joue le rôle du SGBDR, tandis que l'application de recherche de contenu joue le rôle de l'application métier. Dans le point suivant, nous allons vous donner les étapes systématiques de développement d'une application de recherche de contenu.

1.2. Etapes de développement d'une application de recherche de contenu

Le développement d'une application de recherche de contenu suit 8 étapes que nous pouvons répartir en trois phases : la phase de construction de l'index, la phase de construction du module de recherche et la phase de construction de l'interface utilisateur. La figure suivante illustre ces 8 étapes. Dans la figure, la couleur bleu-ciel représente les étapes de construction de l'index, la couleur jaune représente les étapes de construction du module de recherche et la couleur verte représente la construction de l'interface. Ces étapes peuvent vous servir de guide systématique pour le développement de vos applications de recherches. Elles ont l'avantage d'être indépendantes de la technologie (le moteur d'indexation de contenu) que vous allez utiliser.



Etapes de construction d'une application de recherche de contenu

1.2.1. La construction de l'index

La première phase dans le développement de toute application de recherche de contenu est le développement du module de construction et de mise à jour de l'index. Cette phase se déroule en 4 étapes : l'acquisition de documents, la structuration de contenu, l'analyse de contenu et l'indexation de document.

• L'acquisition de documents

La première étape dans la construction de l'index consiste à acquérir les documents, plus précisément le contenu, puisque la recherche commence avec un ensemble de documents ou de fichiers ou de données stockées dans un répertoire centralisé telle qu'une base de données relationnelle ou un moteur NoSQL. Cette étape consiste à se connecter à la source de données et récupérer le contenu nécessaire pour la construction de l'index (du dictionnaire de l'index). Le contenu dont nous parlons ici ce sont les termes uniques contenus dans les documents de la base. Lorsque la recherche va porter sur des documents non-structurés (ce qui est très souvent le cas) comme le XML, JSON, les pages HTML, l'acquisition de contenu se fait par le développement de **crawler ou scrapper**, des robots qui récupèrent le contenu spécifique d'un document. Par exemple, supposons que l'ensemble des documents qui vont être utilisés pour la recherche soient des pages HTML. Pour construire le dictionnaire de l'index, on peut avoir besoin de récupérer les données de balises précises. Des bibliothèques de programmation comme **BeautifulSoup** et **Selenium** vous permettent de développer des crawler pour cette tâche. Voici un exemple de crawler développé en python à l'aide de ces deux bibliothèques.

```
browser = webdriver.PhantomJS()

agent_scrapper = {'User-agent': 'Mozilla/5.0
(Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/37.0.2062.120 Safari/537.36'})

contenu = browser.get('http://juvenaljvc.acndirect.
com', headers = agent_scrapper)

soup = BeautifulSoup(contenu.page_source)

browser.close()

product_title = soup.select('#productTitle')[0].
getText()

prix_promo = soup.select('#priceblock_dealprice')

prix_normal = soup.select('#priceblock_ourprice')
[0].getText()

date_expiration = soup.select('#deal_expiry_
timer_7e1665d8')[0].getText()

caracteristiques = soup.select('#feature-bullets')
```

Sans rentrer dans les détails techniques, le code précédent est extrait de la page Web d'URL <http://juvenaljvc.acndirect.com> le contenu des balises HTML `#productTitle`, `#priceblock_dealprice`, `#priceblock_ourprice`, `#deal_expiry_timer_7e1665d8` et `#feature-bullets`. Ces balises représentent dans l'exemple respectivement le titre du produit, le prix de promotion, le prix normal, la date d'expiration du produit, et les caractéristiques du produit.

Pour plus de détails sur BeautifulSoup et Selenium, rendez-vous sur leurs sites web respectifs (fournis dans la liste des références de l'ouvrage). Les bibliothèques de Crawling varient en fonction du format de fichier. BeautifulSoup est spécialisé sur le Crawling des fichiers au format HTML. Si vos fichiers sont au format XML par exemple, vous pourrez utiliser la bibliothèque LXML ou les bibliothèques DOM (Document Object Model) pour extraire le contenu des balises XML particulières dans le fichier XML. En dehors du développement personnalisé des crawlers, vous pouvez également utiliser des logiciels de Crawling ou des logiciels qui incluent des crawlers tels qu'Apache Solr, Nutch, Grub ou Aperture. Comme vous avez pu le constater, les modules d'acquisition de contenu ne sont pas nécessairement fournis par le moteur d'indexation de contenu (Apache Lucene par exemple ne fournit pas de modules de Crawling), ça sera donc à vous de le développer manuellement et de l'inclure dans votre application de recherche de contenu dans la plupart des cas.

• La structuration de contenu

Une fois que vous avez acquis le contenu des différents documents qui doivent être indexés, la seconde étape consiste à traduire ce contenu en **unités** qui vont être utilisées par le moteur d'indexation de contenu. Souvenez-vous que l'indexation se fait sur une copie séparée de la base de fichiers. C'est l'ensemble des fichiers de la base de cette copie qu'on appelle techniquement des unités. Comme leur format peut être différent d'un fichier à l'autre, il faut nécessairement les restructurer pour les rendre adéquat à l'indexation de contenu. C'est dans cette étape que vous allez structurer le contenu que vous avez récupéré en fichier indexable. La structure du fichier que vous allez utiliser dépend du type de contenu. Un exemple de structure serait *document -> champs -> valeur*. Un autre serait *page -> en-tête -> corps*. Les moteurs d'indexation de contenu ne fournissent pas nécessairement les outils pour réaliser cette opération. Auquel cas, vous le ferez manuellement avec beaucoup de prudence, car c'est cette structure qui sera utilisée par le moteur d'indexation de contenu pour automatiser la construction de l'index. Si la structure n'est pas bien définie, certains mots (documents par ricochet) risquent de ne pas apparaître dans les résultats de recherche et ainsi baisser leur précision¹. Apache Lucene fournit une API pour vous assister dans ce travail, mais ne fournit pas la logique de structuration pour construire le document (ceci est fonction de l'application de recherche de contenu et ne peut donc pas être automatisé). Si par exemple les fichiers à indexer sont dans une base de données relationnelle, vous pourrez passer par des outils tels que Hibernate Search, LuSQL, ou Compass pour

indexer et faire de la recherche de contenu dans les tables de la base de données. A ce stade, l'index ne peut pas encore être construit, car le contenu textuel doit être analysé et traité.

• L'Analyse de contenu

Une fois que la copie de la base de données a été structurée de façon appropriée, la troisième étape consiste à analyser le contenu (ce qu'on appelle dans le jargon le parsing de texte). Cette phase est nécessaire car le texte qui a été récupéré par les crawlers doit passer par une analyse sémantique. Aucun moteur d'indexation de contenu ne crée d'index sur du contenu textuel directement. Le texte doit être soit fragmenté en morceaux atomiques appelés des **jetons** (*tokens* en anglais). Dans cette étape, le contenu textuel de tous les documents à indexer est fragmenté en jetons qui sont ensuite analysés selon les règles orthographiques et grammaticales d'une ou de plusieurs langues. C'est dans cette étape qu'il faut déterminer le sens des mots, décider si le synonyme d'un mot est égal à ce mot, par exemple : si une recherche est faite sur le mot « *laptop* », est ce que le moteur doit également renvoyer « *notebook* » ? Doit-on respecter la casse ? Est-ce que « *Dossier* » = « *dossier* » ? En quelle langue doit-on évaluer les mots ? Doit-on proposer des correcteurs orthographiques type « *vouliez-vous dire ?* » ? Comment détecter la langue dans laquelle un mot est écrit ? Vous pouvez utiliser dans cette étape l'ensemble des méthodes que nous avons vu dans le chapitre précédent pour améliorer la qualité du dictionnaire de l'index à savoir : le N-Gram, l'extraction d'entité, le stemming, ou encore la recherche de proximité. Le moteur d'indexation de contenu peut également vous aider à cette étape en fournissant une bibliothèque de fonctions d'analyse qui réalise l'analyse sémantique, grammaticale, orthographique et linguistique de vos contenus textuels. Apache Lucene par exemple possède des **Analizers** pour cela. Nous allons y revenir dans la partie suivante.

• L'indexation des documents

A ce stade, tout est fin prêt pour la construction de l'index. Tous les éléments sont réunis pour construire le dictionnaire et la liste des valeurs qui constituent l'index. Cette étape est entièrement prise en charge par le moteur d'indexation de contenu. Pendant celle-ci, les termes qui ont été précédemment traités sont ajoutés au dictionnaire de l'index, les documents sont indexés et le programme s'actualise à une période déterminée par le développeur pour mettre à jour l'index. Pour rappel, la structure d'index utilisée ici est l'index inversé.

1.2.2. La construction du module de recherche

Dans le point précédent, vous avez vu en détail comment construire un index. Aussi complexe et intimidant qu'il paraît, la valeur de l'index n'est visible que par les recherches qu'il supporte. La deuxième phase dans le développement de l'application de recherche de contenu est le développement du module de recherche de contenu. Ce module est le cœur de l'application car il détermine les recherches qui pourront être effectuées par l'application, et donc son efficacité. La construction du module de recherche se fait en trois étapes : la construction des requêtes de recherche, la recherche et la restitution des résultats.

• La construction des requêtes de recherche

La première étape dans la construction du module de recherche est de définir les modèles des requêtes qui vont pouvoir être faits sur votre application. L'utilisateur saisit une requête de recherche sur l'interface graphique offerte par votre application, celle-ci est transmise à votre application et traduite en objet de recherche dans le moteur d'indexation de contenu. Généralement, vous n'avez pas à développer l'objet de recherche, il est fourni par le moteur d'indexation de contenu. Apache Lucene par exemple fournit une bibliothèque appelée « *QueryParser* » qui traduit le texte de l'utilisateur en objet de recherche. Vous devez définir la façon dont le texte saisi doit être traité. Par exemple, est ce que le moteur doit interpréter les caractères génériques tels que *, ?, %, + comme des opérateurs de recherche ou simplement comme des textes ? La recherche porte-elle sur des phrases ou sur des termes ? Comment sont traitées les requêtes suivantes : `%juvenal +Hadoop -Apache, Pierre+feuille+cisceau, pierre feuille:cisceau` ? Même si ce n'est pas vous qui développez le module de transformation du texte de requête en objet de recherche de contenu, vous devez quand même préciser la façon dont il sera traité.

• La recherche de contenu

Une fois que le texte a été transformé en objet de recherche de contenu, le moteur d'indexation de contenu va consulter l'index, chercher les documents qui correspondent aux critères de recherche et les classer par ordre d'importance. Cette étape est exclusivement faite par le moteur d'indexation de contenu, la recherche est réalisée sans que vous n'en sachiez le comment. Par contre, vous pouvez décider du type de recherche qui va être réalisé

et peut-être de la métrique qui va être utilisée pour mesurer l'importance des résultats. Mais généralement, les moteurs d'indexation de contenu possèdent déjà leur propre métrique de mesure de pertinence des résultats et ne laissent pas la possibilité de définir et d'utiliser sa propre métrique. Pour rappel, 6 types de recherches peuvent être effectués, ces types sont disponibles ou pas dans les moteurs d'indexation de contenu, il s'agit de : la recherche textuelle intégrale (full text Search), la recherche géographique, la recherche réseau, la recherche facettée, la recherche vectorielle et la recherche N-Gram. Vous sélectionnez celle que vous voulez que votre moteur implémente, et le moteur s'occupe de la recherche sans que vous ne sachiez les détails de l'algorithme de recherche ;

• Le renvoi des résultats

Une fois que la recherche a été exécutée, que les documents correspondant aux critères de recherche ont été renvoyés et triés par ordre de pertinence, l'application doit les restituer via l'interface utilisateur. Cette restitution doit se faire de façon intuitive et l'interface utilisateur devrait offrir un chemin clair sur les actions à suivre pour consommer ces résultats (par exemple le clic sur le lien ou l'image du résultat). De plus, il faudrait que l'interface permette à l'utilisateur de pouvoir raffiner ses recherches ou trouver des résultats similaires à l'un des critères de recherche.

1.2.3. Le développement des interfaces

La dernière phase dans le développement d'une application de recherche de contenu est le développement des interfaces. Comme nous l'avons mentionné plus haut dans l'étude de l'architecture des applications de recherche de contenu, les interfaces, spécialement l'interface utilisateur est la porte d'entrée à l'application. Il faut donc veiller à ce qu'elle soit très simple et très intuitive. Certains experts recommandent de ne pas présenter d'options avancées à la première page, de rester sur le modèle de Google, c'est-à-dire une barre de texte et un bouton de recherche. Une seule étape doit être nécessaire à la fois pour saisir ses requêtes de recherche que pour consulter les résultats. Si possible, ajoutez des options de corrections orthographiques, implémentez des fonctionnalités de remplissage semi-automatique. Tous ces éléments amélioreront l'expérience utilisateur. Au-delà de l'interface utilisateur, cette phase permet également d'implémenter les interfaces analytiques et administrateur nécessaires respectivement pour le Reporting et l'administration de l'application.

Un autre aspect annexe du développement des applications de recherche de contenu c'est la **scalabilité**. Beaucoup d'applications de recherche utilisées en interne n'ont pas suffisamment de trafic de requêtes pour poser les problèmes de passage à l'échelle au-delà d'un ordinateur. Dans le cas contraire, le passage à l'échelle peut se faire sur deux dimensions : la quantité de contenu à indexer et le débit des requêtes.

- Si l'application doit gérer un volume important de contenu, alors il faut le diviser en partitions (on parle de "shards") et les distribuer sur plusieurs machines. Dans ce cas de figure, une machine cliente redirige chaque requête à toutes les machines contenant les partitions, celles-ci y exécutent la recherche et renvoient leurs résultats qui sont agrégés par la machine cliente. Le principe est très similaire à celui de l'interrogation des bases de données parallèles que nous avons vu au chapitre 5 ;
- Si l'application rencontre un débit élevé de requêtes (comme c'est le cas pendant des heures de pointe), alors l'index devra être répliqué à travers plusieurs machines. Une machine qui fait office d'équilibreur de charge (on parle techniquement de *load balancer*) envoie les requêtes à la machine la plus disponible en termes de ressources ;
- Si vous devez combiner les deux dimensions, alors les approches distribuées utilisées par les moteurs tels que Google que nous avons étudiées dans le chapitre précédent pourront être utilisées. Apache Lucene, Elasticsearch et les autres moteurs d'indexation de contenu que nous avons évoqués jusqu'à présent sont des moteurs distribués, ils s'adaptent très bien à la recherche de contenu à large échelle.

A présent, vous savez comment développer des applications de recherche de contenu. Notez que ces principes s'appliquent indépendamment du moteur d'indexation de contenu que vous choisirez. Nous allons maintenant passer à l'étude concrète d'Apache Lucene dans une prochaine partie.

Nous aidons les professionnels à se reconvertir dans le métier de Data Engineer. Si vous souhaitez vous réorienter vers ce métier, vous pouvez nous contacter à l'adresse suivante : <https://www.data-transitionnumerique.com/>

> Par Juvénal Chokogue

¹ La précision est la métrique utilisée pour mesurer le degré d'efficacité d'une requête de recherche de contenu. Plus le moteur renvoie des résultats correspondant à l'intention de l'utilisateur et aux mots-clés qu'il a saisi, plus on dira que le module de recherche de contenu est précis.

ORCHESTRER L'INTELLIGENCE COLLECTIVE EN ENTREPRISE !

Des univers éthiques, attractifs, performants, ça vous parle ? Vous voulez en savoir plus sur tous les mécanismes et les bénéfices de l'intelligence collective ? Alors, plongez-vous au cœur de cet ouvrage qui va inscrire votre entreprise dans un avenir durable et confiant.



Rencontre avec Charlotte du Payrat, qui s'est appuyée sur son expérience professionnelle mais aussi ses observations et ses passions, pour évoquer les défis à surmonter et les réflexions à nourrir afin d'orchestrer l'intelligence collective en entreprise.

Pourriez-vous vous présenter en quelques lignes ?

Consultante, j'accompagne les entreprises dans le changement afin de renforcer leur dynamique collective via du coaching d'équipe, du coaching de dirigeants. Je les aide à travailler sur la culture managériale et la culture collaborative, propose des formations, des ateliers... Mon approche est basée sur une logique d'« empowerment ». C'est-à-dire que

SMARTDSI®



DOSSIER
Définir une stratégie informatique pour les 3 - 5 ans à venir

BONNES PRATIQUES 2022
Six domaines clés à évaluer pour adopter le DevSecOps

INTERVIEW
La cyber-résilience basée sur l'identité au service des entreprises

L'ETUDE A RETENIR
Top 3 des changements stratégiques des responsables IT

INTERVIEW
Orchestrer l'intelligence collective en entreprise

CYBERSECURITE
Prédictions pour 2022 et au-delà

Club Abonnés sur ITPro.fr

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

ABONNEZ-VOUS MAINTENANT !

SMARTDSI

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

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

*Taux de TVA 2,1 %

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

Date + signature

Mode de règlement :

A réception de facture* Par chèque joint

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

Indiquez votre N° TVA Intracommunautaire :

VOS COORDONNEES

Société

Nom Prénom

Adresse de livraison

.....

.....

Code postal Ville

Pays

Tél. Fax

email.....

Renvoyez votre bulletin à notre service abonnements :

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

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



Charlotte Du Payrat

je suis dans la co-construction avec mes clients et je m'interdis de leur apporter des solutions toutes faites. Cependant, je les aide à prendre du recul, à identifier les éléments clés, à effectuer des prises de conscience, à renforcer leurs synergies, etc. C'est un travail très exigeant, centrée sur la notion de confiance et de libre arbitre, et une approche différente du consultant classique.

"Orchestrer l'intelligence Collective", mais pourquoi traiter ce sujet, d'où est venue cette idée ?

Ma manière d'appréhender la réalité de l'entreprise est avant tout globale et systémique avec une grande attention au vécu des collaborateurs. Afin d'ouvrir mon regard, je m'efforce en permanence d'écouter des angles de vue différents des miens. J'ai retrouvé cet état d'esprit dans le modèle de l'entreprise apprenante (- proposé par Peter Senge, il y a 30 ans -) dont la clé est l'intelligence collective. A partir du moment où l'on adopte une démarche pragmatique avec une structuration via la chaîne managériale, je suis convaincue que c'est un modèle d'avenir. Cependant, c'est un modèle exigeant qui nécessite de cheminer avec vigilance et attention pour éviter les écueils.

L'intelligence collective c'est le fait de travailler les interactions entre les personnes.

D'après les retours lecteurs que je reçois, des managers retrouvent dans le livre un style de management systémique et centré sur le vécu des collaborateurs qu'ils adoptent naturellement sans en prendre conscience - ce qui est peu surprenant.

Il se donnent cette exigence en supplément des objectifs plus explicites donnés par l'entreprise - ce qui est parfois fatigant - car ils savent intuitivement que cela génère de l'esprit d'équipe et de la performance long terme.

Implicite pour une partie des managers, je pense que cette vision systémique gagnerait à faire l'objet d'une véritable réflexion explicite dans l'entreprise alors qu'elle est particulièrement adaptée à la complexité actuelle.

Pouvez-vous donner une définition de l'Intelligence Collective. Alors, c'est quoi l'Intelligence Collective ?

Ma définition est la suivante : l'intelligence collective c'est le fait de travailler les interactions entre les personnes. Un certain nombre de personnes pensent que c'est simple parce cela semble être du bon sens ou pensent que cela devrait se faire tout seul. Nous sommes aussi tentés de réduire ce champ à des outils ou des méthodes.

Or, si celles-ci peuvent être un point d'appui, l'humain est souvent beaucoup plus complexe et subtil. Nous sommes avant tout dans une démarche, un état d'esprit à bien comprendre...

Vous évoquez le fait de réinventer la façon de travailler, de manager, de sortir des schémas classiques. Comment faut-il s'y prendre ? Y a-t-il urgence ? On sent que le besoin est là après la crise sanitaire vécue par tous ...

Le monde dans lequel nous évoluons aujourd'hui est devenu complexe et incertain. Les modèles qui marchaient hier ne correspondent plus aux besoins d'aujourd'hui. Il y a un changement de paradigme, une nécessité de réinventer nos manières de travailler ensemble : travailler la logique de collaboration, renforcer l'engagement des collaborateurs, écouter les signaux faibles, etc.

Nous sommes de plus en plus conscients que cette crise sanitaire va bien au-delà d'une crise liée à un virus. Pour s'en convaincre, il suffit d'écouter les conclusions du rapport du GIEC¹ - groupement d'experts - publié le 9 août qui alerte sur le dérèglement climatique qui va menacer la vie humaine sur terre (canicules, inondations...). Les entreprises et la société sont face à de nombreux défis pour lesquels il va falloir jouer collectif : l'obsolescence des compétences, l'hyperconnexion qui génère de la fatigue chez les collaborateurs, la perte de sens...

Nous n'avons plus le choix, nous devons avancer ensemble et trouver de nouvelles voies... !! Nous sommes dans le même bateau... !

Cependant, malgré l'urgence, la résistance au changement reste une réalité, elle est inhérente à notre nature humaine (et notamment au biais cognitif de statut quo) : changer ses habitudes demande beaucoup d'énergie, du temps et de l'accompagnement... ! Est-ce que nous accompagnons suffisamment ces changements d'habitude, de culture, de schémas de pensée en temps et en budget ? L'accompagnement humain est tout aussi important que la transformation digitale, davantage investie.

L'entreprise du futur, c'est donc pour vous, recentrer l'humain et impulser une dynamique collective. Alors quels conseils donner aux dirigeants, RH, managers pour y arriver ?

Lire « Orchestrer l'Intelligence Collective »... ! Il m'est difficile de retranscrire tout le contenu du livre en quelques lignes. C'est un livre dense, riche, clair d'après les retours lecteurs. Et c'est justement la « raison d'être » de proposer une démarche pragmatique et méthodologique, d'en comprendre les tenants et les aboutissants.

Le livre permet au lecteur (manager, DRH, dirigeant ou collaborateur) de « cheminer » à partir d'anecdotes, d'illustrations, d'analyses, de réflexions... L'écriture de ce livre est partie d'une intuition et d'une volonté de partage : donner des repères dans une époque bousculée, aider à passer d'une rive à l'autre... Et un livre se prête très bien à un exercice de réflexion active tout en respectant le rythme du lecteur et permettant la compréhension du changement actuel. Son édition a été un vrai parcours du combattant. Cependant, le succès est au rendez vous avec des articles dans les Echos (en mai) et Echos Entrepreneurs (août) qui en ont mis en avant à la fois la qualité et l'actualité.

L'accompagnement humain est tout aussi important que la transformation digitale, davantage investie.

Un certain nombre de grands groupes ont acheté le livre pour le distribuer à des collaborateurs comme L'Oréal, Malakoff Humanis, La Poste, Engie, Le groupe Nutriset... Le Groupe l'Oréal a ainsi acheté et distribué 100 livres à ses DRH. Malakoff Humanis l'a distribué à 100 top managers. Voilà une manière simple et efficace d'avancer... !

D'autre part, comme évoqué précédemment, selon moi, un accompagnement est utile pour favoriser des prises de conscience. En tant que consultante, outre quelques outils connus, j'ai créé, pour justement accompagner les dirigeants, RH et managers, un certain nombre de démarches, un modèle, des formations. Je suis optimiste car je sais qu'il y a des solutions pour l'avenir... !

Un dernier point à partager avec les lecteurs et qui vous tient particulièrement à cœur ?

L'entreprise apprenante nous invite à accorder davantage d'importance à la réflexivité, à la connaissance, au dialogue. Pourtant c'est un champ qui, avec l'arrivée d'internet, a été particulièrement dévalorisé sur le plan financier ces dernières années. Par exemple, le chiffre d'affaires du marché de la presse a été divisé par moitié en vingt ans... !

L'entreprise apprenante nous invite à accorder davantage d'importance à la réflexivité, à la connaissance, au dialogue.

Or plus que jamais nous avons besoin de personnes capables de produire des réflexions, d'inciter à prendre du recul, d'imaginer... J'avais écrit un article dans Harvard Business Review <https://www.hbrfrance.fr/chroniques-experts/2020/09/31368-quand-le-gratuit-de-lun-devient-la-valeur-de-l'autre-sur-ce-sujet>.

Il me tient à cœur car j'ai un grand respect pour les « inspireurs » qui au lieu de copier et reproduire l'existant créent de nouvelles voies à partir d'une page blanche (écrivains, artistes, consultants mais aussi entrepreneurs, créateurs...). Or, ce travail est plus exigeant et demande du temps... Dans cette période, où nous avons besoin d'innovateurs pour avancer, il est indispensable de valoriser cette création parallèlement à la valorisation des découvertes digitales... !

(1) <https://www.lesechos.fr/monde/enjeux-internationaux/climat-les-6-chiffres-alarmants-du-dernier-rapport-du-giec-1337701>

> Par Sabine Terrey



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

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

Les indispensables stratégies D'ACCÈS CONDITIONNEL

L'utilisation d'Office 365, si elle permet des gains de productivité importants, doit nécessairement faire l'objet d'un niveau de sécurisation élevé. L'usage de l'application Microsoft Teams, de One Drive et in fine, de SharePoint Online, peut rapidement exposer vos données confidentielles si vous n'avez pas pris en compte les menaces qui pèsent sur les processus d'authentification de toute solution SaaS.



Comme recommandé par Microsoft et par la plupart des entreprises œuvrant dans la sécurité, il est fortement conseillé, entre autres, de mettre en place des stratégies de sécurité afin de renforcer l'authentification utilisateur et notamment de déployer ce que l'on appelle les **stratégies d'accès conditionnel**.

Comme vous devez le savoir, aucune entreprise n'est à ce jour à l'abri des nombreuses menaces présentes sur Internet. Si vous n'êtes pas convaincu de la nécessité de protéger vos accès, je vous invite à lire le dernier rapport d'Octobre 2021 de Microsoft

portant sur la protection numérique disponible sur le lien suivant <https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RWMFii>

Ou encore celui du département IC3 du FBI.

https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf Edifiant !

Pour rappel en 2019, Microsoft a bloqué plus de 13 milliards de courriers malveillants et suspects, dont plus **d'un milliard** étaient des URL mises en place dans le but explicite de lancer une attaque par **hameçonnage de comptes utilisateurs**.

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



SMARTDSI

www.smart-dsi.fr

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

Cet article présente donc les concepts de base que vous devez intégrer avant de vous lancer corps et âme dans la sécurisation de vos comptes utilisateurs et autres comptes à privilèges.

Avant de rentrer dans le vif du sujet, sachez que les stratégies d'accès conditionnel Microsoft sont des fonctionnalités relativement puissantes qui peuvent réduire de façon significative votre exposition aux menaces d'usurpation d'identité. Elles doivent cependant être mises en place avec précaution, en particulier si vous voulez éviter des blocages abusifs pour vos utilisateurs.

Notez d'ores et déjà que celles-ci bénéficient d'un mode appelé « rapport uniquement » qui vous permettra, avant de les mettre en action, d'évaluer leurs impacts sur les utilisateurs. Une vérification indispensable.

Activer une stratégie



Naturellement, je vous engage à mettre en place ces stratégies d'accès conditionnel pour les comptes utilisateurs et encore plus pour les comptes ayant des privilèges sur votre tenant Office 365.

Rappelons que l'accès conditionnel est généralement fourni dans les licences E1 E3 E5 et le niveau de licence minimal est Azure AD premium P1. Avouez que cela serait dommage de ne pas les utiliser.

Le principe de l'accès conditionnel est de prendre en compte des informations (signaux) qui vont être captés par vos stratégies, qui à leur tour, vont accorder, refuser ou demander une validation complémentaire des accès (MFA : authentification Multi Factorielle). La figure ci-dessous issue la documentation Microsoft illustre relativement bien le principe général.

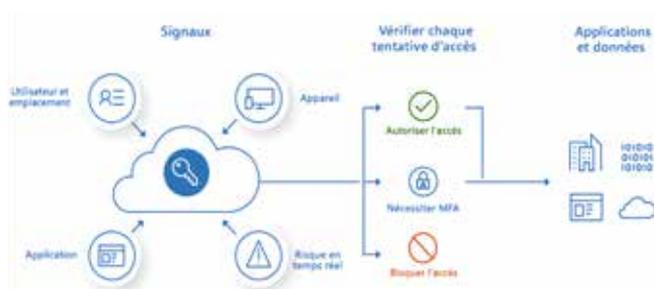


Figure 1 : Stratégie d'accès conditionnel - Principes de base (Source Microsoft)

Naturellement, selon vos propres contraintes de sécurité, et selon vos catégories d'utilisateurs, les stratégies d'accès conditionnel peuvent être plus ou moins complexes. Dans cet article, nous allons simplement présenter quelques mesures de base que toute entreprise quelle que soit sa taille et son activité, devrait, selon moi mettre en place.

LA LOCALISATION DES ACCÈS OU EMPLACEMENTS NOMMÉS

Dans l'environnement Azure AD, il est possible de définir des localisations de confiance (Emplacements nommés). Ainsi, une entreprise française dont les employés sont censés se connecter depuis chez eux (sur le territoire national), va définir deux régions de confiance que sont : La France et le réseau interne de l'entreprise. Ainsi, toute tentative de connexion et ce, même si la personne rentre correctement ses informations de connexion, sera refusée en dehors de ces deux emplacements.

Naturellement l'inverse est possible, à savoir autoriser les connexions depuis tous les pays du monde sauf quelques-uns (pas totalement au hasard... Russie, Corée du Nord, Iran etc.).

Attacks by country of origin (July 2020-June 2021)

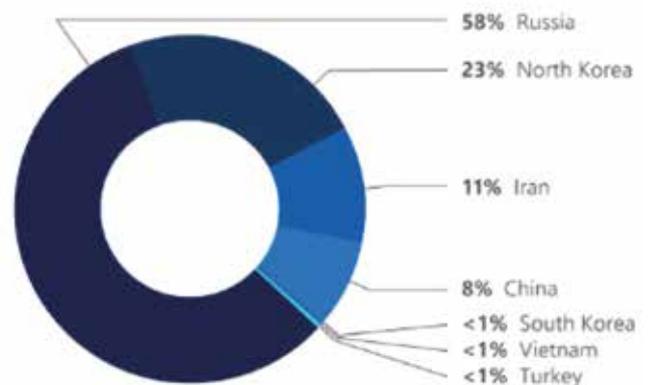


Figure 2 : Attaques par pays d'origine (juillet 2020-juin 2021) : Source Microsoft Digital Defense Report | Octobre 2021

Les stratégies d'accès conditionnel peuvent être de natures différentes et ciblent traditionnellement des groupes d'utilisateurs. Elles peuvent donc autoriser certaines personnes de l'entreprise, comme des frontaliers, à se connecter depuis un pays limitrophe en plus du territoire national par exemple.

Les stratégies d'accès conditionnel peuvent être de natures différentes et ciblent traditionnellement des groupes d'utilisateurs.

La figure suivante illustre la création de régions de confiance permettant aux utilisateurs de se connecter. En quelques clics, vous allez pouvoir réduire votre exposition.

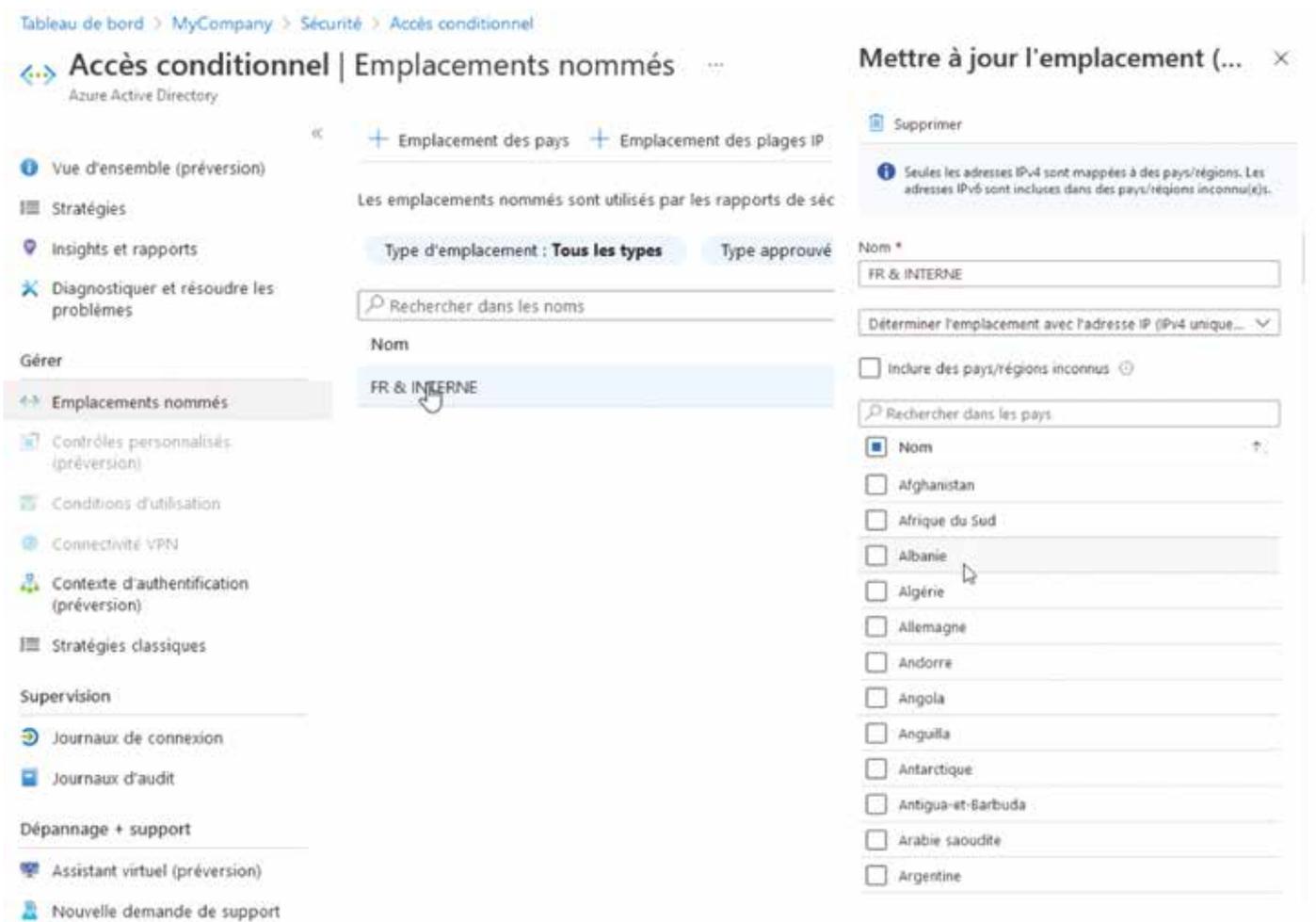


Figure 3 : Emplacements de confiance

Certes, cette mesure de restriction par localisation est simple, rapide mais ne découragera pas longtemps des hackers avisés qui utiliseront soit un VPN, soit des machines de rebond pour tenter de se connecter directement sur votre Tenant. Il va donc falloir aller plus loin.

POSTE DE TRAVAIL MAÎTRISÉ

La seconde solution consiste à restreindre l'accès aux ressources O365 via des postes que l'entreprise maîtrise c'est-à-dire qu'elle sécurise, et qu'elle met à jour régulièrement.

Le concept est assez simple. Il consiste à synchroniser depuis vos différents Active Directory, vos postes de travail dans l'environnement Azure Active Directory. Cette synchronisation est effectuée directement par le processus Azure Ad Connect que vous installerez sur site.

Le concept est assez simple. Il consiste à synchroniser depuis vos différents Active Directory, vos postes de travail dans l'environnement Azure Active Directory. Cette synchronisation est effectuée directement par le processus Azure Ad Connect que vous installerez sur site. Si vous disposez d'ores et déjà d'un environnement Exchange Hybride vous voyez sûrement à quoi je fais référence.

L'Azure AD connect va donc "remonter" vos postes de travail (Windows 10 ou Windows 11) dans l'environnement Azure Active Directory pour vous permettre de les adresser directement dans vos stratégies d'accès conditionnel. Ainsi, vous serez en mesure d'interdire tout accès à votre environnement O365 depuis un poste qui n'est pas référencé dans votre environnement.

La figure ci-dessous illustre la configuration de la stratégie qui s'applique à tous les utilisateurs du Tenant sauf quelques comptes d'Administration (qui eux feront l'objet d'une stratégie spécifique)

Postes Maitrisés

Stratégie d'accès conditionnel

Supprimer

plus des invités externes. [En savoir plus](#)

Nom *
Postes Maitrisés

Affectations
Utilisateurs ou identités de charge de travail
Tous les utilisateurs inclus et utilisateurs spécifiques exclus

Applications ou actions cloud
Aucun(e) application cloud, action ou contexte d'authentification sélectionné(e)

Conditions
3 conditions sélectionnées

Contrôles d'accès
Océroyer
2 contrôles sélectionnés

Session
0 contrôles sélectionnés

À quoi cette stratégie s'applique-t-elle ?
Utilisateurs et groupes

Inclure Exclure

Aucun
 Tous les utilisateurs
 Sélectionner des utilisateurs et des groupes

Tous les utilisateurs invités et externes
 Rôles d'annuaire
 Utilisateurs et groupes

À quoi cette stratégie s'applique-t-elle ?
Utilisateurs et groupes

Inclure **Exclure**

Sélectionner les utilisateurs et groupes à exclure de la stratégie

Tous les utilisateurs invités et externes
 Rôles d'annuaire
 Utilisateurs et groupes

Sélectionner les utilisateurs exclus
2 utilisateurs

- admin admin@clo ...
- Laurent TERUIN lteruin@c ...

⚠ Ne bloquez pas votre accès ! Cette stratégie aura une incidence sur tous vos utilisateurs. Nous vous recommandons d'appliquer d'abord une stratégie à un petit ensemble d'utilisateurs pour vérifier qu'elle se comporte comme prévu.

Figure 4 : Poste Maitrisé : Configuration des utilisateurs

« 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

IL EST PAS FRAIS MON ALBUM ?



Un poster
offert !

9,90 €

À l'occasion de la sortie d'*Astérix et le Griffon*,
RSF célèbre la résistance joyeuse avec les irréductibles Gaulois.

RSF REPORTERS
SANS FRONTIERES

La seconde figure présente la condition pour accorder l'accès à l'environnement Office 365. Dans cet exemple, le poste en question doit être enregistré dans l'Azure AD en tant que Poste hybride Azure AD join (HADJ). Les stratégies applicatives que vous apercevez dans la figure ci-dessous servent à restreindre fonctionnellement certaines applications notamment sur le périphérique mobile.

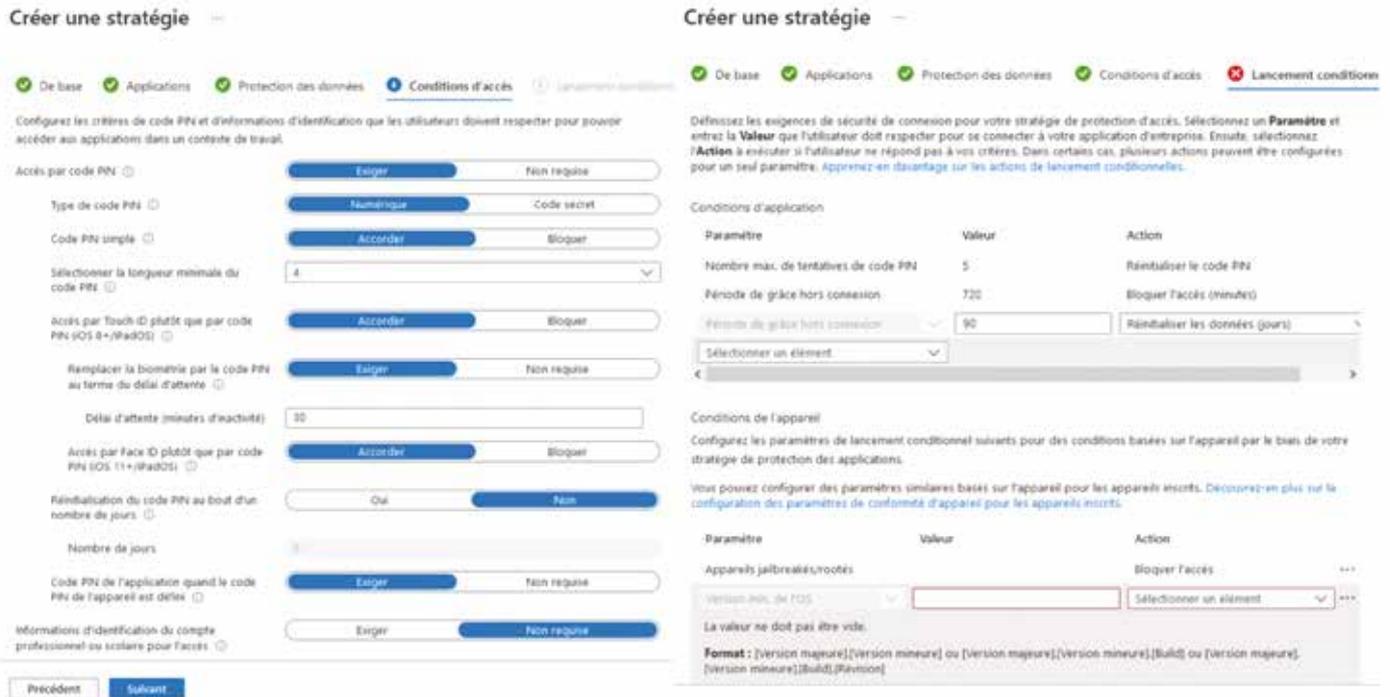
Maintenant que l'on a dit ça ou que vous l'avez mis en place, reste à adresser les fameux périphériques mobiles. J'ai nommé, smartphones, et autres tablettes, bref, tout ce qui n'est pas Windows 10 ou Windows 11 mais plutôt IOS ou Android voire Windows Phone.

MAÎTRISE DES PÉRIPHÉRIQUES MOBILES

A ce niveau deux grands choix sont possibles. Le premier que je vous conseille consiste à interdire tout accès aux ressources Office 365 depuis un périphérique

mobile non géré. On comprendra par périphérique non géré, tout périphérique Android ou IOS possédant une version logicielle récente qui n'est pas « enrôlée » dans votre organisation. Cela comprend naturellement les périphériques mobiles de l'entreprise, mais également les périphériques mobiles personnels : BYOD. Cet enrôlement va donc nécessiter d'installer sur le périphérique une application qui va « contrôler » l'état de ce dernier et conditionner son accès à diverses conditions (Version du système d'exploitation, chiffrement du périphérique, présence de code d'accès pour le déverrouillage etc..).

Cet enrôlement va également vous permettre de contrôler ou de limiter certaines fonctions des applications Office 365 présentes sur le périphérique. On parle alors de stratégies applicatives. La figure ci-dessous vous donne un rapide aperçu de ce que l'on est capable de paramétrer comme restrictions fonctionnelles.



Le second choix que je qualifierais de moins raisonnable est de permettre l'accès aux ressources de votre Tenant depuis n'importe quel périphérique Android et IOS, quel que soit son état, tout en appliquant ces fameuses stratégies applicatives.

Naturellement, vous pourrez toujours conditionner l'accès de ces périphériques au fait qu'ils se connectent depuis des emplacements géographiques approuvés. L'estimation et l'acceptation du risque vous revenant de droit, c'est à vous de voir.

GESTION DES UTILISATEURS EXTERNES / INVITÉS

L'utilisation d'un Tenant Office 365 comprend également la possibilité de partager avec des utilisateurs externes à votre entreprise certaines données SharePoint, Teams etc.

Ces utilisateurs externes naturellement ne doivent pas être oubliés, et ce n'est pas parce qu'ils font partie d'une autre organisation que vous ne devez pas contrôler la façon dont ces derniers s'authentifient chez vous.

Là aussi, je vous invite à renforcer leur mode d'authentification et à ne pas laisser un simple compte / mot de passe permettre l'accès à vos données. L'utilisation à minima d'un MFA, qu'il soit géré par l'application Mobile Microsoft Authenticator, ou par SMS, me semble être aujourd'hui, un prérequis indispensable.

DÉTECTION DES RISQUES EN TEMPS RÉEL

L'intégration de signaux à Azure AD Identity Protection permettant aux stratégies d'accès conditionnel d'identifier des comportements déviants, (lieu de connexion inhabituel, voyage impossible, par exemple) vous permettra d'exiger des facteurs d'authentification complémentaires voire de refuser l'accès aux ressources. A vous de définir le niveau de sécurisation que vous envisagez de mettre en place.

Vous l'aurez compris, les stratégies d'accès conditionnel constituent un outil indispensable parmi tout le catalogue sécurité proposé par Microsoft, pour protéger l'accès à vos ressources Office 365.

Les stratégies d'accès conditionnel constituent un outil indispensable, pour protéger l'accès à vos ressources Office 365.

Par leur souplesse et leur exhaustivité, elles sauront répondre aux nombreux cas de figures qui ne manqueront pas de se poser. C'est une solution indispensable que vous devez déployer pour limiter votre exposition et reprendre le contrôle de vos accès.

Laurent TERUIN / <https://www.workingtogether.fun/>

NUA.GE SIMPLIFIE L'ADOPTION DU IAAS

Oxeva lance Nua.ge, nouvel acteur français du cloud public, qui simplifie l'usage et l'adoption du IaaS, et réduit ses coûts sans entamer la performance. Ce cloud public de type IaaS (Infrastructure as a Service) made in France, s'adresse principalement aux startups, aux développeurs, ops, métiers et aux agences web. Décryptage avec Gabriel Barazer, CTO et cofondateur de Nua.ge.



Pouvons-nous en savoir plus sur ce nouvel acteur, Nua.ge ? Qui sont les fondateurs ?

Nua.ge est un cloud public de type IaaS conçu par la société Oxeva, spécialisée dans l'hébergement infogéré et haute disponibilité depuis 2005. Oxeva et Nua.ge ont été fondées par Vincent Harmin, Olivier Doucet et moi-même, Gabriel Barazer.

D'ailleurs, on remarque que le marché du IaaS a augmenté de 40,7 % en 2020 pour atteindre 64,3 milliards de dollars, contre 45,7 milliards de dollars en 2019, selon Gartner, Inc.). La pandémie et ses effets ont accéléré la transformation numérique des entreprises et le recours massif au Cloud.

Que permet Nua.ge plus précisément ?

Nous avons fait le constat que le Cloud était devenu de plus en plus complexe, que ce soit dans son usage mais aussi dans la prévisibilité des coûts et des consommations réelles.

Nous portons la simplification des usages au cœur de nos valeurs, valeurs qui nous ont guidés lors de la construction de Nua.ge et qui resteront un fil conducteur constant et fondamental dans son évolution.

Nua.ge a pour vocation de proposer de l'infrastructure Cloud de la façon la plus standard et sécurisée possible, avec une petite révolution ergonomique dans la manière de consommer le Cloud.

Notre objectif est que les utilisateurs se sentent sécurisés, en permanence en contrôle de leurs ressources et de leurs dépenses, en leur permettant de créer des instances en un clic tout en gardant une visibilité des coûts en temps réel.

Nua.ge permet donc à ses utilisateurs de créer, le plus simplement possible, des instances avec du stockage et un réseau performant, pour y déployer du code et héberger des sites web ou tous types d'applications.

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

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

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

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

► **iPro.fr**



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



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

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

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



Des ressources exclusives

Enjeux DSI
Cloud Computing
Collaboration & mobilité
Exchange Server
IBM i



Un Club Abonnés

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

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



Gabriel Barazer



Olivier Doucet



Vincent Harmin

Quelles sont les spécificités techniques?

Nua.ge repose sur une architecture OpenStack, base performante et robuste mais complexe à utiliser. Sur le papier, c'est contre-intuitif avec notre promesse de simplicité. C'est pourquoi nous avons pris le parti de développer notre propre API et application web et ainsi permettre aux utilisateurs de pouvoir utiliser un Cloud performant dans la plus grande simplicité et efficacité.

Sous le capot, nous avons aussi voulu simplifier des mécaniques et composants couramment utilisés dans les installations OpenStack classiques afin de faciliter le travail de nos équipes techniques et concentrer les efforts sur des spécificités rares dans un service de cloud public comme l'accélération matérielle de toutes les fonctions de routage et de sécurisation des flux réseau.

Côté infrastructures, nous avons opté pour du matériel sur mesure, haut de gamme, permettant les plus hautes densités de ressources du marché.

Côté infrastructures, nous avons opté pour du matériel sur mesure, haut de gamme, permettant les plus hautes densités de ressources du marché afin de pouvoir répondre rapidement à la demande croissante, prolonger la durée d'utilisation et maîtriser au mieux notre empreinte énergétique.

Nous avons confiance dans la qualité et la performance du service, c'est d'ailleurs la raison pour laquelle nos environnements de développement et de production, basés sur la technologie Kubernetes, fonctionnent eux-mêmes sur Nua.ge !

S'il fallait retenir 5 points clés, côté bénéfices ?

On peut tout à fait retenir ceux-ci, c'est-à-dire, qu'il est possible de

- Créer un cloud simple d'utilisation pour offrir une alternative française aux usines à gaz
- Faciliter la prévisibilité des dépenses
- Améliorer la visibilité sur les consommations
- Garantir la conformité RGPD
- Offrir un Cloud "de tous les jours" aux développeurs, startups, CTO et agences web

Souhaitez-vous évoquer les perspectives 2022 ?

Nous sommes toujours en phase de lancement, et nous avons à cœur d'écouter et répondre aux attentes de nos utilisateurs : nous attendons donc de recueillir leurs premiers retours pour prioriser les chantiers à mener. À court terme, nous souhaitons mettre en place une roadmap collaborative, sur laquelle nos utilisateurs pourront suivre les sujets sur lesquels nous travaillons et nous en suggérer de nouveaux. Nous allons aussi étendre notre offre en matière de choix de systèmes d'exploitation à la création des instances, du stockage objet, des options de performance et des architectures matérielles multiples.

À plus long terme, nous souhaitons compléter notre offre IaaS avec des services PaaS tels que la gestion et le stockage de conteneurs applicatifs avec la même démarche permanente de simplification des usages et transparence des coûts.

> Par Sabine Terrey

Expertise & Richesse fonctionnelle
Interopérabilité avec les Systèmes RH
Sécurité & Conformité réglementaire



Promodag



PROMODAG est le spécialiste du contrôle de votre système de messagerie **Microsoft Exchange** en local ou dans **Office 365**. Sa gamme complète et polyvalente de rapports d'analyse de trafic, de suivi des messages et de planification simplifiée et automatise le **processus de gestion de l'utilisation des e-mails**, vous assurant ainsi la **conformité et l'optimisation** des performances des systèmes de messagerie critiques.

“ Optimisez vos usages collaboratifs et réglementaires à l'heure du télétravail généralisé ”

Sur www.promodag.fr téléchargez une version d'évaluation gratuite et entièrement fonctionnelle ou demandez une démonstration avec l'un de nos experts



CLOUD OFFICE SECURITY

PROTECTION PRÉVENTIVE DES APPLICATIONS MICROSOFT 365[®]

Protégez les fichiers et les données de vos clients stockés dans le Cloud,
en moins de 5 minutes, sans interruption de services.



EXCHANGE
ONLINE



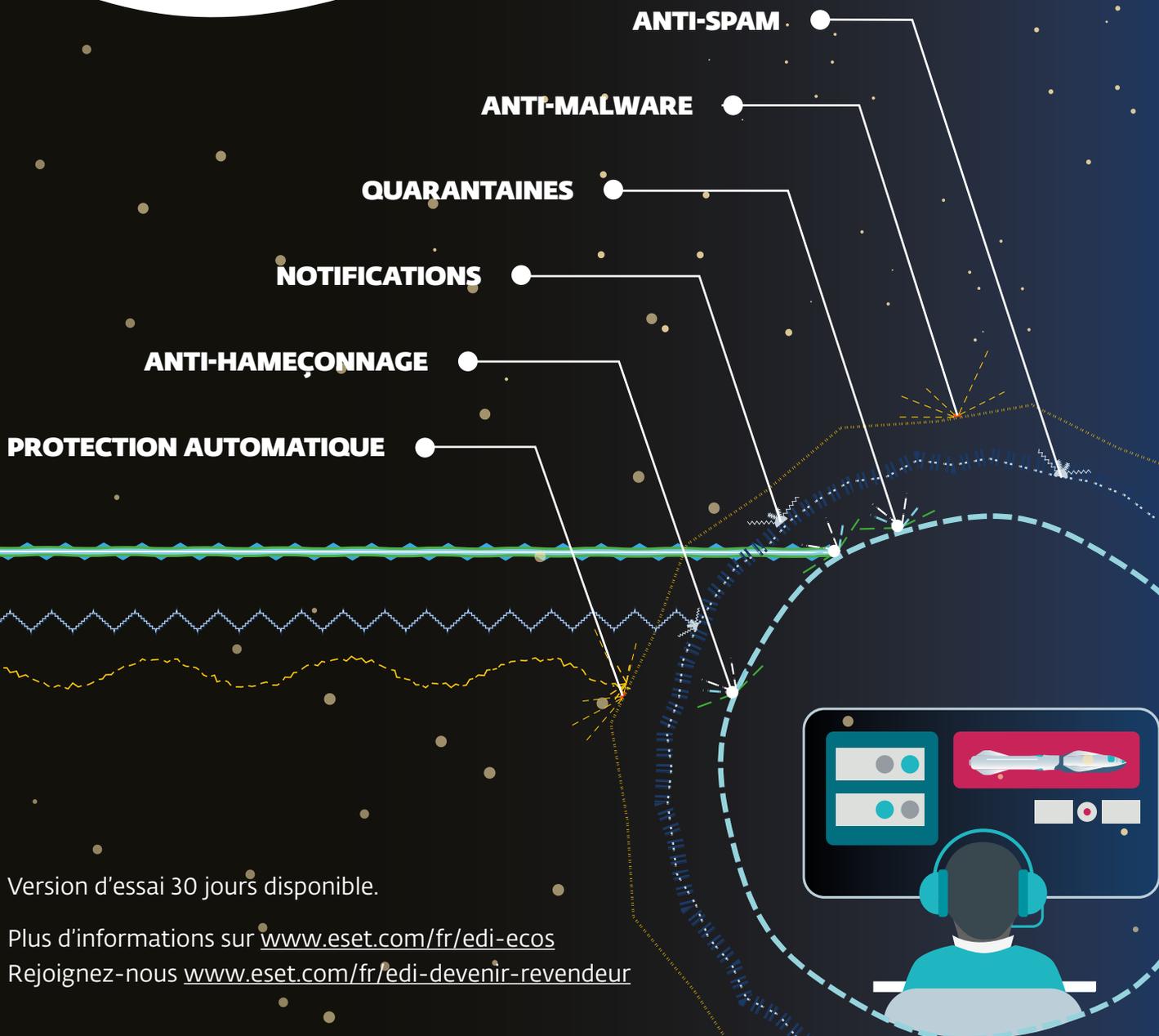
ONEDRIVE



TEAMS



SHAREPOINT
ONLINE



Version d'essai 30 jours disponible.

Plus d'informations sur www.eset.com/fr/edi-ecos

Rejoignez-nous www.eset.com/fr/edi-devenir-revendeur

Copyright © 1992 – 2021 ESET, spol. s r. o. ESET, logo ESET et/ou d'autres produits mentionnés d'ESET, spol. s r. o., sont enregistrés marque déposée d'ESET, spol. s r. o. Microsoft ou les produits mentionnés ici peuvent être des marques enregistrées de leurs propriétaires.