N°31 I SEPTEMBRE 2023

CONDUIRE LA TRANSFORMATION NUMÉRIQUE DE L'ENTREPRISE

SMART DSI®

DOSSIER
Le no-code/low-code dans la transformation numérique

INTERVIEW
Une offre dédiée au numérique responsable pour les DSI

L'ETUDE A RETENIR
Comment faire plus vite avec moins de budget ?

STRATEGIE
CVSS4 : révolution dans la gestion des vulnérabilités ou coup d'épée dans l'eau ?

INTERVIEW
Une culture de l'innovation au service des clients

L'ŒIL SECURITE
Le Cloud, une révolution à sécuriser

Club Abonnés sur iTPro.fr

Luttez en continu contre tous les types de menaces

Avec une visibilité approfondie sur les cybermenaces qui ciblent votre entreprise

Threat Intelligence

- Kaspersky Threat Data Feeds
- Kaspersky Threat Lookup
- Kaspersky Cloud Sandbox
- Kaspersky APT Intelligence Reporting

kaspersky

Motiver & Engager les profils Tech !

De nombreux sujets préoccupent les entreprises, encore peut-être plus en cette période de rentrée où le contexte incertain fragilise les organisations ! Il en est un qui revient sans cesse et qu'il faut scruter avec attention, « la motivation et l'engagement des profils Tech ».

C'est ainsi que ces collaborateurs se démarquent par leur fort engagement au travail. Leur équilibre entre vie professionnelle et vie personnelle semble satisfait, à plus de 80%, et ils affectionnent grandement l'innovation déployée en termes de mode de travail. En ce sens, l'environnement de travail reste un critère de choix qu'il faut perpétuer, en y ajoutant les briques technologiques nécessaires à forte valeur ajoutée et le maintien de la formation et des compétences pour entreprendre des projets stimulants.

Toutefois, si les collaboratrices Tech se sentent plus engagées que la moyenne nationale, l'égalité des chances, la reconnaissance et l'évolution professionnelle demeurent des points de vigilance, et ce, encore en 2023 ! Il y a urgence à réagir !

Alors, pour aller encore plus loin, n'est-il pas temps de répondre déjà à quelques interrogations clés : Quels sont les clés de réussite de l'engagement des collaborateurs ? Comment créer des expériences positives attirant les jeunes générations ? Comment mener de front les objectifs, la performance individuelle et la confiance ?

En effet, les équipes plébiscitent la transparence des dispositifs d'accompagnement de la performance et de la carrière, le leadership inspirant et visionnaire, et bien sûr, la prise en compte des enjeux environnementaux, critère fondamental à leurs yeux. Plus de doute sur ce point, les valeurs et l'ADN RSE enthousiasment indéniablement les synergies et positionnement l'entreprise sur une bonne dynamique.

A n'en pas douter, la RSE devient aussi un des leviers pour fidéliser tous les talents !

Bonne lecture

(1) Source Etude ChooseMyCompany – 73000 salariés français – 700 entreprises – Du 1/10/2022 au 15/06/2023

Sabine Terrey
Directrice de la Rédaction
sterrey@itpro.fr

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

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

SMARTDSI

N°31 I SEPTEMBRE 2023

SMART DSI est un revue trimestrielle éditée par IT PROCOM
Directeur de la Publication : Sabine Terrey
Strategy Center - BP 40002 - 78104 St Germain en Laye, France.
© 2002 - 2023 IT PROCOM - Tous droits réservés
N° ISSN : 2494-9701 - N° CPPAP : 0518 T 93059
www.smart-dsi.fr

6 I DOSSIER
Le rôle clé du no-code/low-code dans la transformation numérique

12 I L'ŒIL SECURITE
Le Cloud, une révolution à sécuriser

16 I PERSPECTIVES
Projection sur 2023 du paysage des menaces cyber de 2022

18 I INTERVIEW
L'ESN CAPFI pose l'humain au cœur de l'activité et des projets

21 I L'ETUDE A RETENIR
Le fossé se creuse entre les équipes Sécurité et les outils de détection

22 I STRATÉGIE
CVSS 4: Révolution dans la gestion des vulnérabilités ou coup d'épée dans l'eau ?

28 I EXPERT
Azure, pile de déploiement

32 I INTERVIEW
Une offre innovante dédiée au numérique responsable pour les DSI

35 I L'ETUDE A RETENIR
Comment faire plus vite, avec moins de budget et de collaborateurs ?

36 I L'ŒIL DU FUTUR
La directive NIS2 : « un guide pour une activité durable ! »

P.6

P.12

P.48

P.41

38 I INTERVIEW
Business At Work : une culture de l'innovation au service des clients

41 I L'ETUDE A RETENIR
Les 4 révolutions impactant les équipes IT

42 I EXPERT
Retour d'expérience : Migrer « facilement » vos anciens serveurs de messagerie vers Exchange Online

48 I INTERVIEW
Datacore encourage le Datacenter « Green » pour diminuer l'impact environnemental

49 I BULLETIN D'ABONNEMENT

SMART DSI

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

Thierry Bollet, Sylvain Cortes, Didier Danse, Maggie MC Daniel, 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

© 2023 Copyright IT Procom
© Crédits Photos

IStock - Fotolia - Shutterstock

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

Toute reproduction, représentation, traduction ou adaptation, qu'elle soit intégrale ou partielle, quels qu'en soient le procédé, le support, le media, est strictement conditionnée à l'autorisation de l'Éditeur.
SMART DSI - IT PROCOM, tous droits réservés.
© 2023 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

Le rôle clé du no-code/low-code
DANS LA TRANSFORMATION NUMÉRIQUE

> Par Didier Danse

Dans un monde où il est nécessaire d'aller toujours plus vite, il est très fréquent de voir apparaitre du shadow IT, c'est-à-dire des outils non supportés par le département informatique. La raison première invoquée est la lenteur du département qui se défend en expliquant qu'il fait généralement face à un manque de ressources mais aussi de spécifications claires. Des solutions permettent l'automatisation d'actions et peuvent être implémentées par les utilisateurs eux-mêmes. Ce sont elles qui sont utilisées dans ce contexte. Une telle approche est pourtant risquée puisqu'elle peut mener à des fuites d'information.

Bien qu'elles existent depuis des décennies, ce n'est que récemment que ces outils ont émergé comme une solution à part entière, fournie, supportée mais aussi gouvernée au sein de certaines organisations. Alors que les utilisateurs de ces solutions peuvent automatiser leurs actions ou implémenter par eux-mêmes leurs propres écrans et solutions, le département informatique peut alors se concentrer sur les aspects de la gouvernance et augmenter la sécurité des données. A cela s'ajoute la possibilité pour ce dernier d'accompagner les utilisateurs dans leur quotidien et leur apporter leur expertise.

C'est de cette manière que se voit augmenter la collaboration entre les utilisateurs et le département informatique, en profitant de ce que chacun connait le mieux.

L'émergence des plateformes no-code/low-code

Plus loin, plus vite

Face au manque de ressources ayant des compétences de développement, les organisations et ses membres ont besoin d'outils pour créer des solutions bien souvent nécessaires pour apporter des avantages concurrentiels. La démocratisation de la technologie, notamment la capacité d'enregistrer des actions et de les rejouer sans nécessiter de faire du code avancé, mais aussi l'intelligence, permettent, en effet, à tout un chacun de mettre en place des solutions par lui-même.

Mais au-delà du gain pour les personnes en charge de l'opérationnel, c'est surtout l'apparition de nouvelles méthodes de travail qui change la donne. La collaboration avec les équipes qui opèreront les systèmes se voit accrue. Ces derniers peuvent ainsi faire plus qu'auparavant mais aussi plus rapidement. Le département informatique y trouve, en effet, son compte puisque son implication diminue tout en voyant augmenter le nombre de solutions implémentées.

Le Citizen Developer est une personne qui démontre un intérêt marqué pour les outils digitaux.

Grace à ces outils, il est possible de voir apparaitre des personnes faisant partie de l'opérationnel faire le lien entre ses équipes et le département informatique. Il s'agit du développeur citoyen, ou citizen developer dans la littérature qui maintient le terme anglophone. Le *Citizen Developer* est, au sein de l'organisation, une personne qui démontre un intérêt marqué pour les outils digitaux et souhaite approfondir ses compétences techniques. Le Citizen Developer n'a pas besoin de connaître un ou plusieurs langages informatiques, mais de comprendre et maîtriser les plateformes de développement no-code/low-code. Il se fait, ainsi, l'interface entre les équipes et le département informatique, connait les contraintes de sécurité et les besoins des différents collaborateurs en termes informatiques. Il s'agit d'un axe de modernisation des processus et impliquer les utilisateurs mènera à une adoption plus rapide des changements, pouvant même mener à un changement culturel dans l'organisation.

Des similarités et des différences

Nous parlons de no-code/low-code depuis un certain temps sans donner d'information sur ce qu'il s'agit exactement. Voyons, dès lors, comment les classifier:

- **Le no-code** permet d'automatiser des actions en composant des suites d'opérations au sein d'un outil de conception, généralement graphique. Il permet, aussi, de créer des écrans ou encore des solutions basées sur l'intelligence artificielle
- **Le low-code** permet de faire la grande majorité des opérations tout comme en no-code mais en permettant l'utilisation de développement, qui est alors accessible pour des actions particulières
- Enfin, **le Robotic Process Automation** (RPA), grâce à des capacités de détection et de lecture permet d'aller encore plus loin dans le no-code/low-code puisqu'il tiendra compte de ce qui est visible à l'écran.

Comme nous pouvons le voir, les trois types de plateformes proposent généralement à chacun des outils de modélisation, que ce soient des écrans ou des flux de travail. Le Citizen Developer peut effectuer des intégrations avec d'autres systèmes et automatiser des opérations plus ou moins complexes. A ces cas d'utilisation s'ajoutent des solutions simples basées sur des affichages divers : un site web ou une application ne comportant que peu de logique de calcul et bien d'autres. Parce que les cas d'utilisation sont multiples, nous pouvons voir apparaître, depuis une année ou deux, l'arrivée massive du machine learning et autres intelligences artificielles au sein même de ces plateformes. Ces nouvelles opportunités vont augmenter fortement les possibilités d'exploitation en élargissant le champ des possibilités et en rendant ces capacités accessibles à un plus grand nombre.

Le développeur classique pourra, également, profiter de tels systèmes pour compléter des solutions existantes et ce, de manière plus rapide. Le RPA permet, aussi, d'effectuer des changements sur des applications existantes puisqu'il propose des fonctionnalités de lecture visuelle et de simulation de mouvement de la souris et d'actions clavier, ce qui permet alors de répondre à des besoins complémentaires, en combinant ces capacités de lecture et de simulation aux autres fonctionnalités du no-code/low-code.

Des avantages certains... mais aussi des inconvénients

Sur base des éléments précédemment décrits, il est assez simple de comprendre que la productivité

augmente. Les études parlent de pouvoir produire des applications de 2 à 8x plus rapidement, selon les cas d'utilisation. De plus, un avantage considérable est de pouvoir travailler directement avec les utilisateurs voire de les laisser décrire leurs processus dans de tels outils. Cette collaboration, permet d'ailleurs de :

- Réduire les délais de mise en œuvre puisque la charge de travail est partagée entre plusieurs personnes
- Augmenter l'agilité en permettant à l'utilisateur de tester par lui-même les fonctionnalités et les différentes approches
- Réduire les coûts de développement puisque les spécifications des fonctionnalités sont de plus en plus précises voire déjà implémentées
- Favoriser l'adoption et l'adaptation puisque l'utilisateur est le premier concerné, son implication sera plus élevée
- Faire appel à des ressources moins expérimentées et économiser des ressources précieuses.

Du point de vue de la gouvernance, ces plateformes viennent avec des avantages considérables : en n'exposant que des capacités exposées, elles réduisent le risque et en assurent la consistance dans les méthodes de développement. Fini donc les éternelles macros dans Excel qui donnent des maux de tête dès qu'il s'agit de les maintenir.

Dans le cas du low-code, tout changement dans la plateforme elle-même nécessite de s'assurer que le code fonctionne toujours. C'est donc un point important à garder en tête dans la gestion du cycle de vie de cette plateforme et des solutions qui sont basées dessus. De plus, alors qu'un passage d'une plateforme à l'autre peut être aisé si toutes les bonnes pratiques ont été suivies, il peut être difficile voire impossible de passer d'une plateforme à l'autre dans le cas des plateformes no-code.

Cela s'appelle le *vendor lock-in*. Au-delà de ce risque, certains systèmes font appel à du code situé ailleurs. Non maitrisée, cette interconnexion peut mener à des situations complexes, puisque la gestion cohérente entre les deux plateformes est nécessaire.

Des utilisations différentes

De nombreuses utilisations peuvent être envisagées dès que l'on parle de plateformes low-code / no code.

En voici quelques-unes :

- La collecte d'informations dans le contexte des revues annuelles, le recrutement, la gestion de projets, et bien d'autres
- La circulation d'informations et la collecte d'approbations
- La visualisation de données, les rapports de données et, dans le même style, les tableaux de bord
- La manipulation de données, que ce soit la lecture, la transformation ou encore l'enregistrement des informations brutes ou transformées
- Les solutions basées sur l'intelligence artificielle telles que les chatbots
- L'extension de fonctionnalités d'applications à l'ancienne comme nous l'avons expliqué auparavant
- L'intégration entre des modules, notamment dans le domaine de l'Internet of Things.

Quelques exemples, pour ne citer que ceux-là. Pour le no-code : Shopify, Webflow, Microsoft Forms, le low-code : Wordpress, Power Platform et enfin BluePrism et UIPath pour le RPA.

Dans le cas du low-code, tout changement dans la plateforme nécessite de s'assurer que le code fonctionne toujours.

Comme nous pouvons le voir, il existe des dizaines de plateformes couvrant ces domaines. Voici quelques questions pour déterminer la plateforme adéquate pour les utilisateurs :

- Quelles sont les utilisations attendues pour ces plateformes ? Quels sont les objectifs qui y sont associés ?
- En particulier, prévoit-on de faire des intégrations avec d'autres systèmes ?
- Quelles sont les contraintes dans la gestion des déploiements des solutions ?
- Quel niveau de confidentialité des données est autorisé dans la solution ?
- En conséquence, à qui s'adressent-elles et quelles sont les compétences nécessaires pour y accéder ?

Toutes ces questions doivent être répondues préalablement au choix de la plateforme.

La gouvernance de l'information quand les plateformes sont dans les mains des utilisateurs eux-mêmes

La première étape sera de toujours bien clarifier l'utilisation de chacune des plateformes. En effet, bien que nous pourrions être tentés de mettre en place une même solution pour tous les usages, il

s'avère que les plateformes ne sont pas toutes égales et viennent avec des avantages et inconvénients forts différents comme nous l'avons vu.

Ainsi, le RPA, bien qu'il s'agisse d'une extension du low-code ou du no-code, ne sera utilisé que lorsqu'il n'est pas possible de faire autrement. Dès qu'il y a la moindre possibilité de lire ou d'interagir avec les systèmes autrement que par du « clic » ou de la lecture visuelle, il est préférable d'éviter de se créer des dépendances avec des éléments interprétables et qui peuvent régulièrement se voir modifier. Il sera, ainsi, fréquent de définir les règles d'utilisation suivantes :

- Les Citizen Developers peuvent utiliser des plateformes en no-code et uniquement celles-ci, tout du moins s'il n'y a pas de supervision de l'informatique
- Les développeurs ne peuvent utiliser que des plateformes low-code tout en respectant les règles classiques de publication d'applications (gestion des sources et des versions, respect des règles d'intégration et utilisation du déploiement continu)
- Les développeurs peuvent utiliser du RPA dans le cas où toutes les autres possibilités ont été étudiées et réfutées. Ainsi, s'il est possible de répondre au besoin en accédant à une interface applicative et non une interface graphique, cette première sera choisie.

Selon la plateforme, il se peut que les solutions développées soient transparentes pour l'utilisateur et que le moteur d'exécution soit disponible au même endroit que le designer. Dans un tel cas, il reste très important que le département informatique soit en mesure de savoir ce qui est déployé afin d'éviter des solutions fantômes. Dès que le designer et le moteur d'exécution sont des composants totalement séparés, le déploiement des solutions vers les serveurs adéquats doit rester sous le contrôle de l'informatique.

La première étape sera de toujours bien clarifier l'utilisation de chacune des plateformes.

Il en va de même pour les sources utilisées pour construire ces solutions et les packages d'installation. Il existe de nombreux cas où ces actions elles-mêmes sont source de problème, par exemple parce qu'elles permettent de copier de l'information d'un système à l'autre. Il est, ainsi, important de définir la liste des actions utilisables mais aussi de vérifier que seules ces actions soient utilisées.

Quelle que soit la plateforme, le *data management* prend toute son ampleur puisque des utilisateurs accèdent à des données et les exploitent par eux-mêmes. Celles-ci se doivent d'être sous contrôle.

La définition des sources à utiliser mais aussi des droits d'accès aux données s'avèrent critiques pour y parvenir. Le nombre élevé de sources de données qui doivent être sous contrôle peut mener à des difficultés quand il s'agit de les gérer. Des règles de gestion claires se doivent dès lors d'être définies.

Pour supporter l'ensemble, la meilleure approche est de mettre en place un centre de compétences, regroupant des compétences multiples afin de couvrir les aspects techniques mais aussi la gouvernance, l'architecture ou encore le domaine de la stratégie.

Et ensuite ?

Nous pouvons donc résumer les grandes actions à effectuer de la façon suivante:

1. Définir les objectifs et le périmètre d'utilisation
2. Définir les règles de gouvernance (cas d'utilisation, méthodes de publication des applications, etc.)
3. Mettre en place un Centre de Compétences
4. Mettre un cadre pour que la collaboration puisse s'effectuer, tout en laissant de la liberté en ce qui concerne les méthodes de cette collaboration.

Cette approche devrait définir les prémices pour apporter une démarche innovante, inclusive, le tout en mode self-service. Avec le temps, la compréhension mutuelle et l'adoption tant des solutions que des bonnes pratiques devraient fortement augmenter. Certains iront jusqu'à l'hyperautomatisation, c'est-à-dire automatiser tout ce qui est possible, notamment en combinant le no-code/low-code avec l'intelligence artificielle.

L'hyperautomatisation semble idéale mais clairement doit s'accompagner d'un changement de mentalité. Hyperautomisation ou non, le besoin de former est, comme souvent, bien présent.

Et dans ce cas, le développeur a-t-il toujours un rôle à jouer ? La réponse est évidemment oui mais son rôle évolue d'un simple rôle d'exécutant à celui de conseiller auprès du Citizen Developer. De plus, il continuera à faire des développements mais plus centrés sur la création de méthodes pour permettre les intégrations : du chargement et transformation de données au préalable mais aussi des interfaces applicatives (APIs).

L'hyperautomatisation semble idéale mais clairement doit s'accompagner d'un changement de mentalité.

Le futur du no-code/low-code est-il assuré pour autant ? Le no-code/low-code est certainement une révolution dans le quotidien des organisations. Pourtant avec l'émergence des intelligences artificielles génératives, il est probable que celles-ci prendront une place importante dans les prochaines années. Amazon a, d'ailleurs, annoncé il y a quelques jours que son service HoneyCode sera arrêté. Ce service promettait de créer des applications sans aucun code.

Est-ce la fin du no-code pour la cause ? Non, le no-code continuera d'être utilisé au travers d'outils de conception permettant de manipuler des données et bien d'autres activités de la sorte.

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

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

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

▶ iTPro.fr

agefiph

Avec le soutien du

GOUVERNEMENT
Liberté
Égalité
Fraternité

LE PROGRÈS C'EST NOUS

Martin Büchner, apprenti boulanger,
Hadda Guerchouche, coach professionnelle,
éducatrice sportive, préparateur mental
et championne paralympique,
François-Yves Guichet, opérateur logistique.

#seeph2023
Semaine européenne pour l'emploi des personnes handicapées
du 20 au 26 novembre

l'agenceverte

Pénurie de talents, difficultés de recrutement ? Grâce à l'emploi des personnes handicapées, faites vous aussi progresser la société et renforcez votre attractivité ! Rejoignez l'Agefiph et les milliers d'entreprises #activateurdeprogrès dans leur engagement sur **activateurdeproges.fr**

#activateur de progrès

EMPLOI & HANDICAP

Le Cloud, UNE RÉVOLUTION À SÉCURISER

Peut-on encore aujourd'hui, à l'heure de cette grande révolution du Cloud, ne pas fusionner dans une seule démarche d'ingénierie cohérente, les compétences et activités cybersécurité, les environnements Cloud et leur gestion « as code » de facto une imbrication forte autant dans la conception, l'ingénierie que dans l'exploitation, et le maintien dans les conditions opérationnelles et de sécurité de ces environnements ?

Compétences & Ingénieries

Renforcer les compétences et les ingénieries dans le domaine de la containerisation, est un enjeu clé, portant sur la convergence, l'automatisation et la sécurité pour établir une culture DevSecOps et permettre aux utilisateurs de mettre à profit l'innovation et le Cloud tout en maitrisant les risques de sécurité inhérents.

Car il est fort de constater que les entreprises et les administrations, dans leurs migrations vers le Cloud et le digital, rencontrent des difficultés croissantes pour maintenir la fiabilité et la sécurité des logiciels et applications hébergées au sein d'environnements Cloud complexes. Dans ces nouveaux environnements qui se généralisent à vitesse grand V, il est impératif d'avoir une approche de fédération d'expertises autant des aspects ingénierie, containerisation, CI/CD, que des problématiques de sécurité des accès, des identités, de maintien en conditions opérationnelles et de sécurité, etc.

Renforcer les compétences et les ingénieries dans le domaine de la containerisation, est un enjeu clé.

Une révolution majeure !

Le Cloud sous ses différentes formes et multiples usages, que nous parlions de monde sans limites des applications en mode SaaS, que nous parlions des architectures de hosting, ou des Cloud hybrides, que nous parlions d'intégration et de développement agile et continu et bien sûr de la containerisation tous azimuts, le Cloud est une révolution majeure.

Structurellement, la sécurité du Cloud a des implications diverses selon les différents types d'infrastructures Cloud. Les considérations relatives à la sécurité dans chacun des trois modèles populaires (Cloud public, Cloud privé et Cloud hybride) sont multiples et certaines vitales.

Cloud public, privé, hybride

Dans un Cloud public, le fournisseur de Cloud doit assumer la responsabilité de la sécurisation de l'infrastructure. Il doit fournir des outils qui permettent au client de sécuriser son activité notamment les données, en s'adaptant aux normes de conformité pertinentes. Il doit aussi garantir que toutes les activités sont enregistrées pour permettre l'audit mais aussi garantir que les configurations Cloud restent sécurisées et que toutes les nouvelles

ressources sur le Cloud sont également sécurisées, à l'aide d'outils automatisés tels que les solutions Cloud Security Posture Management (CSPM). Dans un Cloud public, les aspects niveau de service (SLA) doivent impérativement inclure les engagements de sécurité de données.

Dans un Cloud privé, le modèle permet de contrôler toutes les couches de la pile. Ces ressources ne sont généralement pas exposées à l'Internet public. Parmi les niveaux de sécurité à prendre en compte : les outils de surveillance Cloud natifs pour obtenir une visibilité sur tout comportement anormal dans les activités opérationnelles et les flux en cours d'exécution, la MCO et la surveillance des comptes, les ressources privilégiées pour détecter les activités suspectes afin de se prémunir contre les menaces internes, la sécurité et l'isolement des machines virtuelles en VLAN dédiés, les conteneurs et les systèmes d'exploitation hôtes, pour garantir que la compromission d'une VM ou d'un conteneur ne permet pas de compromettre l'ensemble de l'hôte et au-delà. Le Cloud privé est de plus en plus "en migration" vers le Cloud hybride. Cela implique la mise en place des mesures de sécurité pour garantir une migration et cohabitation avec des services de Cloud publics.

Structurellement, la sécurité du Cloud a des implications diverses selon les différents types d'infrastructures Cloud.

Dans un Cloud hybride justement, combinaison de centre de données sur site, *on-premise*, de Cloud public et de Cloud privé, les considérations de sécurité sont importantes. Il faut éviter les stratégies et outils de sécurité distincts dans chaque environnement, en adoptant un cadre de sécurité unique qui peut fournir des contrôles dans l'environnement hybride, et en identifiant tous les points d'intégration entre les environnements, devant être traités comme des composants à haut risque.

Une démarche cohérente

Sans procéder ici à une étude de sécurité Cloud, ce n'est pas l'objet de ce billet qui est plutôt de mettre en lumière la cohérence et la démarche conjointe de la sécurité des infrastructures avec celle de l'ingénierie des infras cloud, il y a un ensemble de points majeurs à prendre en compte qui sont : les comptes de services à privilèges, éléments critiques, partie prenante de la gestion des identités et des accès (IAM), les serveurs et les environnements virtualisés, les hyperviseurs (à noter que dans les Cloud publics, la sécurité de l'hyperviseur relève de la responsabilité du fournisseur de Cloud).

Sans oublier le stockage, plus souvent des pools de stockage élastiques ou des ressources virtualisées qui peuvent être provisionnées et mises à l'échelle automatiquement avec l'IAM de nouveau, élément indispensable. Notons aussi les bases de données, le réseau, et les solutions de sécurité telles que des services de pare-feu (FWaaS), les firewall d'application web (WAF) et le déploiement des outils spécifiques tel que Cloud Security Posture Management (CSPM) pour examiner automatiquement les réseaux Cloud, détecter les configurations non sécurisées ou vulnérables et y remédier. Enfin Kubernetes, avec ses composantes critiques, connus sous le nom de « 4 C » (Code, Conteneurs, Clusters et Cloud) est un environnement éminemment critique.

Plusieurs défis de conformité

La conformité aux meilleures pratiques de sécurité, aux normes et références du secteur ainsi qu'aux stratégies organisationnelles internes dans un environnement Cloud natif est également confrontée à des défis. En effet, en plus de maintenir la conformité, les organisations doivent également fournir des preuves de conformité, pour l'interne ou l'externe (certifications tiers, autorités de réglementation de marché, contraintes légales, etc.). Il est donc impératif d'ajuster la stratégie afin que l'environnement Cloud dans sa totalité (conteneurs Kubernetes, Cloud hybride, etc.) corresponde aux niveaux de conformité et de sécurité requis.

Sécuriser les Cloud est impératif, une condition de survie de l'entreprise du XXIème siècle. Cela nécessite une double expertise, dans l'ingénierie des infrastructures Cloud, dans l'automatisation "as code", dans le CI/CD, dans la containerisation des applications, et dans la sécurisation de Kubernetes et de tous les composants.

Tout cela réalisable avec une approche d'ingénierie cohérente et des équipes ingénierie Cloud et sécurité travaillant ensemble.

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

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

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

Promodag offre une vue complète de vos messageries Exchange

L'éditeur français propose une solution de reporting détaillé de l'utilisation de Microsoft Exchange, en mode on-premises ou dans le Cloud. Avec une vision unifiée de ses messageries, une entreprise protège mieux ses données sensibles, se conforme plus aisément aux contraintes réglementaires et réduit davantage son empreinte carbone.

Cela fait des années que des études prédisent la mort de l'email. A 50 ans passés, il se porte pourtant comme un charme. Il ne s'est même jamais autant échangé de courriels. Selon Statista, plus de 319 milliards d'emails ont été envoyés et reçus chaque jour dans le monde en 2021. Un chiffre qui devrait dépasser les 376,4 milliards d'ici 2025.

La crise sanitaire et la généralisation du télétravail ont encore accru le recours à la messagerie. Selon une étude d'Adobe, les cadres consacrent plus de 5 heures par jour à gérer leur messagerie. Eu égard à cet usage intensif, une entreprise se doit d'encadrer leur pratique et de s'appuyer sur des métriques fiables.

Editeur français, Promodag propose depuis 1998 une solution de reporting détaillé de l'utilisation de Microsoft Exchange en mode on-premises (Exchange Server) ou dans le Cloud (Exchange Online). Alors que le reporting proposé par Microsoft reste cantonné au niveau le plus élevé, Promodag Reports assure une granularité beaucoup plus fine, par utilisateur, service, site ou pays, en heure locale et non en heure GMT.

La solution Promodag Reports exploite pour cela les logs générés par Exchange qu'elle met en forme afin de délivrer un grand nombre d'indicateurs. Elle établit des rapports liés au trafic, au stockage et au contenu des boîtes aux lettres afin d'aider les administrateurs à simplifier et automatiser leur gestion. Il est notamment possible de rechercher des messages par mot-clé, taille, date, émetteur ou destinataire.

Conformité au RGPD et au droit à la déconnexion

Promodag Reports répond à un grand nombre de cas d'utilisation. La solution protège une organisation des fuites de données en détectant par exemple les utilisateurs indélicats qui détourneraient leur messagerie professionnelle à des fins personnelles.

Promodag Reports vérifie par ailleurs la conformité des messages au RGPD et à la politique de sécurité de l'entreprise tout en veillant au respect des permissions octroyées sur les boîtes aux lettres ou aux droits d'accès aux dossiers partagés.

La solution s'assure également de la mise en œuvre du droit à la déconnexion, instauré par la loi Travail de 2016, en mesurant la volumétrie d'emails échangés en dehors des heures de travail, le soir ou le week-end, ou durant les périodes de congés.

Promodag Reports participe enfin à l'adoption de pratiques collaboratives plus vertueuses. « *Chiffres à l'appui, une organisation peut inciter ses collaborateurs à mettre moins de personnes en copie ou à envoyer un lien pointant vers un fichier SharePoint plutôt qu'une pièce jointe* », avance **Jacques DAGOUSSET**, PDG de Promodag.

Pour réduire son empreinte carbone, une entreprise peut aussi établir un équivalent CO2 des volumes mails échangés. « *Promodag Reports l'aidera ensuite à diminuer la taille de boîtes aux lettres en répartissant les messages par ancienneté ou en mettant en évidence les corbeilles non vidées* » complète le dirigeant.

Faciliter la migration d'Exchange Server vers Echange Online

Se présentant comme un produit unique pour les environnements on-premises, Cloud ou en mode hybride, Promodag Reports facilite la migration d'Exchange Server vers Microsoft 365. La solution dressera une cartographie des messageries et des groupes à transférer.

Quel volume cela représente-t-il ? Est-il pertinent de transférer de vieux messages ? Quels sont les groupes réellement actifs ? « *En tirant profit de cette vue globale, l'entreprise n'achètera pas de licences inutiles en migrant des boîtes aux lettres non utilisées* », poursuit **Jacques DAGOUSSET**.

Se présentant comme un client lourd sous Windows, hébergé sur une machine virtuelle ou un serveur SQL dédié, Promodag Reports n'exige au plus qu'une demi-journée de déploiement.

Promodag Reports vérifie la conformité des messages au RGPD et à la politique de sécurité de l'entreprise.

« *La solution traite seulement les logs générés par Exchange et se connecte à l'annuaire LDAP pour récupérer les attributs associés* », explique **Jacques DAGOUSSET**.

L'entreprise est ensuite autonome dans la publication des rapports. Elle peut sélectionner une période, faire un regroupement par attribut et ajouter un logo pour personnaliser l'interface. Des tâches peuvent être planifiées à la fréquence souhaitée. L'export des rapports se fait au format PDF, CSV ou Excel.

80 % de l'activité à l'international

Pour tenir compte des entrées et sorties dans l'effectif, et donc de la création et la suppression de boîtes aux lettres, Promodag conseille de faire une mise à jour quotidienne ou hebdomadaire des données. « *Les données restent en local, nous n'y avons aucunement accès* », précise **Jacques DAGOUSSET**.

Editeur français, établi en France et proposant un support en français et en anglais, Promodag a pour références clients des entreprises privées employant au moins une centaine de salariés dans la banque, l'industrie, les télécoms. Promodag a aussi convaincu des acteurs publics comme des mairies ou des conseils généraux. Il réalise 80 % de son activité à l'international.

Promodag Reports, qui est proposée dans sa version 14, est un produit particulièrement mature et stable. L'éditeur l'enrichit néanmoins de nouvelles fonctionnalités comme la possibilité de sélectionner des utilisateurs par type de licence. Il travaille, aussi, en permanence sur les gains de performances. « *Quand une entreprise gère quelque 180 000 boîtes aux lettres, chaque seconde gagnée à générer un rapport a son importance* », conclut **Jacques DAGOUSSET**.

Pour aller plus loin promodag.fr

Projection sur 2023
DU PAYSAGE DES MENACES CYBER DE 2022

Sur la base d'une année de renseignements produits par ses experts de l'Insikt Group, Recorded Future analyse les événements de cybersécurité majeurs, les évolutions géopolitiques, et les divulgations de vulnérabilités, qui ont marqué 2022. De cette vision annuelle globale se dessine une projection du paysage des menaces cyber sur 2023 et au-delà, partagée par Maggie MC Daniel, VP of Insikt Group - Recorded Future.

Effets cyber et géopolitiques de la guerre en Ukraine

Le conflit physique en Ukraine encadre la discussion sur les événements importants liés aux cybermenaces et les tendances géopolitiques qui ont eu lieu en 2022. Il fait aussi émerger la convergence accrue des menaces cyber et géopolitiques. Avant et pendant l'invasion, les analystes de Recorded Future ont observé une augmentation des attaques par déni de service distribué (DDoS), de l'activité hacktiviste et du déploiement à grande échelle de malware de type « Wiper ». Tandis que l'invasion était au cœur des débats sur les opérations cinétiques et cyber-hybrides, les cyber attaquants affiliés à d'autres États-nations majeurs, en particulier l'Iran, la Chine et la Corée du Nord, ont mené des cyberattaques tout au long de l'année, guidés par un courant de tensions géopolitiques exacerbées, de concurrence et d'allégeances politiques.

MAGGIE MC DANIEL

Principales menaces géopolitiques dans le radar en 2023

Tout au long de cette année, la Corée du Nord va très probablement continuer à tester des missiles balistiques. Le renforcement de l'armée américaine dans le Pacifique occidental ainsi que l'augmentation des dépenses de défense et des dispositifs de prévention au Japon risquent d'être accueillis par des actions équivalentes de la Chine. Il y a peu de chance de voir progresser les négociations diplomatiques sur le plan d'action global conjoint (JCPOA), communément appelé l'accord sur le nucléaire iranien. Pendant ce temps, la République islamique d'Iran continue d'enrichir de l'uranium pour se doter d'une arme nucléaire. Le gouvernement israélien devrait poursuivre ses frappes cinétiques sur les éléments de la Force Al-Qods, unité d'élite du Corps des Gardiens de la révolution islamique en Iran.

Les cybermenaces dans le paysage des menaces élargi

Alors que les campagnes d'hameçonnage et les attaques par ransomware continuent d'affecter les organisations de tous secteurs et partout dans le monde, Recorded Future a identifié en 2022 une augmentation de 600 % du nombre d'identifiants vendus par le biais de malware de vol d'informations. Par rapport à l'année précédente, on constate un ciblage accru des logiciels fréquemment utilisés dans les chaînes d'approvisionnement des organisations et une évolution vers un modèle de service de plus en plus managé, les offres « as-a-service » ayant proliféré sur les places de marché du dark web et les forums clandestins. En effet, les analystes de Recorded Future ont identifié en 2022 de nouvelles offres de phishing-as-a-service (PaaS), un succès continu du modèle ransomware-as-a-service (RaaS), et l'utilisation de nouvelles souches d'offres de malware-as-a-service (MaaS). Les courtiers en accès initial (Initial Access Brokers, IAB) sont de plus en plus actifs, probablement en raison de l'utilisation accrue de malware de type « infostealer » et des opportunités de monnayer les données volées. Les logiciels open source ou propriétaires ont été ciblés avec beaucoup d'efficacité tout au long de 2022, si bien que ce type d'attaque va probablement gagner en gravité en 2023.

Les ransomware restent une menace cyber majeure

Les ransomwares ont été une menace omniprésente en 2022. Alors que certains gangs se sont dissous, d'autres n'ont pas tardé à affirmer leur domination en utilisant d'importantes ressources pour lancer des campagnes contre tout type d'organisation. Bien que les paiements de rançon aient diminué d'environ 60 % entre 2021 et 2022, probablement en raison des recommandations des gouvernements et de la vigilance accrue des compagnies d'assurance en matière de normes de cybersécurité, les ransomware demeurent une menace majeure pour les organisations. Si l'adoption de contre-mesures telles que la désactivation des macros par défaut s'est avérée très efficace, de nombreux attaquants ont également réorienté leurs opérations pour contourner les protections nouvellement développées ou mises en œuvre, soulignant ainsi la nécessité de mettre en place une stratégie de défense avancée.

Tant que toute intrusion pourra être monnayée, le ransomware restera une forme très rentable de cybermenace opportuniste.

En 2023, les marchés interconnectés du dark web vont se développer avec des offres de plus en plus sophistiquées s'orientant vers des modèles managés. Les outils de machine learning de plus en plus accessibles vont contribuer au développement accru de modèles PhaaS de meilleure qualité et de campagnes d'ingénierie sociale. L'exfiltration d'informations d'authentification par les infostealers va contraindre les organisations à mettre l'accent sur des protections d'authentification alternatives, telles l'ajout d'un MFA à l'analyse avancée du comportement des utilisateurs. Il est presque certain que les cyber criminels exploiteront les vulnérabilités *zero-day* dans les produits largement utilisés. Cependant, ils n'ont pas besoin d'investir massivement dans l'étude de ce type de vulnérabilités. Il leur suffit d'être plus rapides que la majorité des entreprises qui n'appliquent pas ou ne peuvent pas appliquer les correctifs de vulnérabilités critiques dans les mois qui suivent leur divulgation. Enfin, le ransomware demeure une menace permanente pour tout type d'organisation partout dans le monde. Tant que toute intrusion pourra être monnayée, le ransomware restera une forme très rentable de cybermenace opportuniste.

L'ESN CAPFI POSE L'HUMAIN AU CŒUR DE L'ACTIVITÉ ET DES PROJETS

Créée en 2005 et implantée à Paris, Londres et Casablanca avec plus de 200 collaborateurs, CAPFI est une ESN spécialisée dans la transformation digitale, le design d'infrastructure IT et le consulting dédié aux secteurs finance, banque et assurance, project management, cybersécurité, cloud et big data. Avec ses 5 filiales, elle répond aux diverses problématiques IT.

Entretien avec Bruno Boutet qui dirige l'une des entités, CAPFI 6è sens, offrant une expertise en sécurité, cloud et automatisation.

Pourriez-vous en quelques mots présenter CAPFI, plus précisément sa filiale CAPFI 6è sens ?

L'ESN place les relations humaines et l'innovation au cœur de chaque projet. Attachée aux valeurs d'éthique, de confiance et d'authenticité, CAPFI pose les enjeux RSE au cœur de sa dynamique. La culture d'entreprise basée sur le respect notamment apporte à tous un épanouissement personnalisé.

CAPFI 6è Sens regroupe ainsi des compétences expertes en sécurité, cloud et automatisation pour aider ses clients à lutter contre les cyber menaces et sécuriser les systèmes d'information.

L'ESN place les relations humaines et l'innovation au cœur de chaque projet.

« 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
- Boites 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.

CONCEPTION & RÉALISATION : WWW.KONTENTIOUS.COM

BRUNO BOUTET

Revenons sur les propositions et la valeur ajoutée de CAPFI 6è sens.

Alors pour être précis, l'offre de CAPFI 6è sens se divise en 2 grandes spécialités.

D'une part, le Design et Gestion d'infrastructures IT On premise & Cloud, comprenant les pôles : Architecture - Intégration et paramétrage de composants systèmes, réseaux et de sécurité - Maintien en Condition Opérationnelle et de Condition de Sécurité

D'autre part, le socle Expertise en Industrialisation et Sécurisation de système d'information, autour des pôles : Automatisation des déploiements et de l'intégration continue - Sécurisation des infrastructures IT - CyberRésilience

CAPFI 6è Sens offre ainsi un service 100% souverain. Le choix de regrouper les éditeurs français pour mieux défendre ses clients, en mettant l'accent sur la confidentialité des données est une priorité.

Enfin, nous proposons des solutions de sécurité françaises, avec des labels de confiance (France Cybersecurity, Visa de sécurité de l'ANSSI, Hexatrust, DINUM). Ce choix permet la protection et la confidentialité des données mais aussi un hébergement en France.

Comment accompagnez-vous les clients ?

L'accompagnement se fait en plusieurs étapes.

D'abord avec un Cyber SOC 100% souverain (Security Operation Center), ce qui permet une action « Anticipation, Détection et Réponse aux incidents de cybersécurité ».

Ensuite un audit d'infrastructure et de maturité en cybersécurité, comprenant un audit réseaux, un audit et durcissement AD et un audit de maturité (Vulnérabilité, conformité, bonnes pratiques...).

Nous proposons des solutions de sécurité françaises, avec des labels de confiance.

Enfin, nous proposons des actions de sensibilisation au risque Cyber, avec des campagnes de phishing et de sensibilisation utilisateurs, une recherche fuite de données et une simulation de crises & plan de réponse.

> Par Sabine Terrey

Le fossé se creuse entre les équipes Sécurité et les outils de détection

Selon 90 % des analystes SOC, les outils de détection des menaces sont efficaces mais 97 % craignent de manquer un événement de sécurité important.

La spirale vicieuse

Les équipes chargées des opérations de sécurité (SecOps) protègent des cyberattaques toujours plus sophistiquées et rapides.

Mais la surface d'attaque en expansion, l'évolution des méthodes des attaquants et l'augmentation de la charge de travail des analystes SOC, entraînent une spirale vicieuse empêchant les équipes de sécurité de sécuriser efficacement leur organisation.

Près de trois heures par jour à trier manuellement les alertes

Le triage manuel des alertes coûte aux organisations 3,3 milliards de dollars par an rien qu'aux États-Unis. Autre chiffres clés :

- La taille de leur surface d'attaque a augmenté au cours des trois dernières années – 63%
- Les équipes SOC reçoivent 4 484 alertes par jour
- Les équipes passent près de trois heures par jour à trier manuellement les alertes
- Les analystes de sécurité sont incapables de traiter 67 % des alertes quotidiennes reçues

Les surcharges d'alertes !

La combinaison d'angles morts et le volume élevé d'alertes faussement positives empêchent les équipes SOC de contenir les cyber-risques. Ainsi :

- Les analystes SOC s'inquiètent de manquer un événement de sécurité pertinent, noyé sous un flot d'alertes – 97%
- La surcharge d'alertes est la norme parce que les fournisseurs ont peur de ne pas signaler un événement qui pourrait s'avérer important – 41%
- Les outils de sécurité sont achetés pour cocher des cases et répondre aux exigences de conformité – 38%

L'épuisement des analystes

Face à la surcharge d'alertes et aux tâches répétitives, les deux tiers des analystes de sécurité envisagent ou quittent activement leur emploi. Selon 74 %, leur emploi correspond à leurs attentes, mais 67 % envisagent de le quitter ou le quittent activement.

Parmi les analystes qui envisagent de quitter ou quittent activement leur rôle : 34 % ne disposent pas des outils nécessaires pour sécuriser leur organisation.

Enfin, travailler dans le secteur de la sécurité n'est pas une option de carrière viable à long terme, selon 52%.

Source Rapport de recherche 2023 Vectra AI sur l'état de la détection des menaces
Enquête menée auprès de 2 000 analystes SecOps.

CVSS 4 : RÉVOLUTION DANS LA GESTION DES VULNÉRABILITÉS OU COUP D'ÉPÉE DANS L'EAU ?

Tous les RSSIs ou praticiens du mode de la sécurité connaissent le terme CVSS !

En effet, la gestion des vulnérabilités représente un pilier fondamental de la posture de sécurité globale de toute organisation. Comme tout élément fondamental, il nous faut des règles communes de mesure et de gestion. Le système commun d'évaluation des vulnérabilités (CVSS - Common Vulnerability Scoring System) est un cadre ouvert permettant de caractériser la sévérité des vulnérabilités (CVE), il permet donc aux organisations de caractériser les CVEs présentes et participe au processus de priorisation de la remédiation.

CVSS 3.1

La version actuelle de CVSS est la 3.1. Elle est basée sur un système constitué de trois composants permettant de « noter » les CVEs et de définir leurs caractéristiques. Un système « à tiroir » permet aussi de prendre en compte ou pas les particularités et les attentes de l'organisation. La notation CVSS 3.1 s'appuie sur trois familles d'attributs :

•Le « Base Metric »

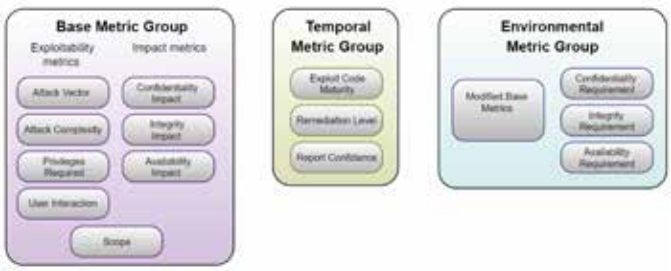
Ce composant caractérise la CVE « elle-même », les différents attributs constitutifs de ce composant permettent d'évaluer la sévérité de la CVE sans prendre en compte son usage réel par les attaquants ou les caractéristiques propres à l'organisation. Très souvent, par abus de langage, la plupart de vos interlocuteurs utilisent en fait le score du « Base Metric » comme étant la note globale CVSS – cet usage est bien sûr faux d'un point de vue sécurité mais comme cette note ne change jamais (sauf révision de la part du NVD) elle est bien pratique à utiliser

•Le « Temporal Metric »

Ce composant tente de rajouter une couleur temporelle au score CVSS. Pour faire simple, il s'agit ici de définir quel usage réel est possible de la part des groupes d'attaquants. Par nature, cette note change dans le temps, par exemple si un code permettant l'exploitation de la CVE est découvert, cette nouvelle situation va faire évoluer la note « Temporal ». Généralement, il faut avoir une équipe d'analystes et/ou un flux de CTI pour alimenter les attributs de ce composant

•Le « Environmental Metric »

Ce composant permet de définir les caractéristiques liées à l'organisation, notamment les besoins en termes de confidentialité, intégrité et disponibilité. De plus, les attributs de la catégorie « Modified Base Metrics » permettent de modifier les attributs définis dans le composant « Base Metric » afin d'aligner l'évaluation de la CVE avec les besoins de l'organisation



Les trois composants de CVSS 3.1 -
Source : https://www.first.org/cvss/v3.1/specification-document

Comme nous l'avons vu, d'un point de vue pratique, les organisations utilisent massivement la note du composant « Base Metric » mais rencontrent d'énormes difficultés à renseigner les attributs des deux autres composants. L'étude de ces difficultés dépassent le cadre de cet article, mais gardez à l'esprit qu'il n'est pas si simple de renseigner les valeurs des attributs des composants « Temporal Metric » et « Environmental Metric ».

Point extrêmement important, le composant « Base Metric » seul ne permet pas de définir un risque, il permet uniquement d'évaluer la **sévérité** d'une CVE, les organisations manipulent donc généralement des indicateurs techniques sans lien réel avec leur quotidien ou même sans corrélation avec la réalité de la menace.

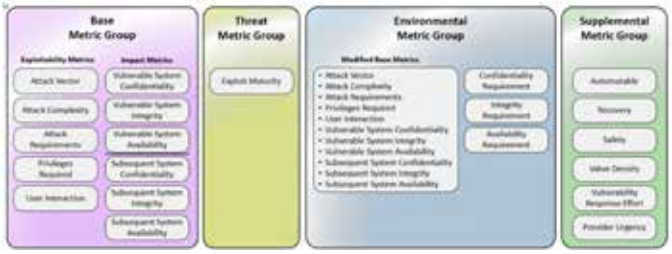
CVSS 4, pourquoi cette évolution ?

Depuis environ 6 ou 7 ans, nous avons, toutes et tous, constaté une augmentation quasi exponentielle des attaques réalisées par des groupes d'attaquants organisés. L'illustration la plus évidente de ce nouveau paradigme est représentée par l'explosion des attaques par ransomware. Or, les ransomwares utilisent des vulnérabilités pour se répandre dans les organisations, et la famille de vulnérabilités la plus connue est constituée des CVEs.

Le composant « Base Metric » seul ne permet pas de définir un risque, il permet uniquement d'évaluer la sévérité d'une CVE.

La version 3.1 de CVSS datant quelque peu, il a donc été décidé de travailler sur une nouvelle version permettant à priori de mieux évaluer la menace représentée par les CVEs. Les spécifications CVSS sont définies par le FIRST (Forum of Incident Response and Security Teams), association américaine mais dont les travaux possèdent un impact mondial.

Une version préliminaire de la version 4 de CVSS a été publiée sur le site du FIRST (voir https://www.first.org/cvss/v4-0/cvss-v40-specification.pdf), elle est publiquement accessible et devrait rentrer en application à la fin de l'année 2023 ou au début de l'année 2024. Même s'il s'agit d'une version préliminaire, nous pouvons considérer qu'il s'agit de la version « quasi » définitive des spécifications CVSS 4.



Les quatre composants de CVSS 4 -
Source : https://www.first.org/cvss/v4.0/specification-document

Quels changements dans CVSS 4 ?

Nous allons donc explorer les différents composants de CVSS 4 et mettre en lumière les changements majeurs par rapport à CVSS 3.1. Néanmoins, cet article n'a pas pour vocation de fournir l'ensemble des informations exhaustives sur ce sujet - vous devrez réaliser votre propre investigation pour comprendre comment cette évolution peut impacter vos processus d'évaluation de la menace.

•Nomenclature

CVSS 4 est constitué maintenant de 4 composants, il a donc fallu revoir la nomenclature des différents ensembles de composants. En effet, si le composant Base est par définition toujours présent, il peut être associé à un ou plusieurs des trois autres composants.

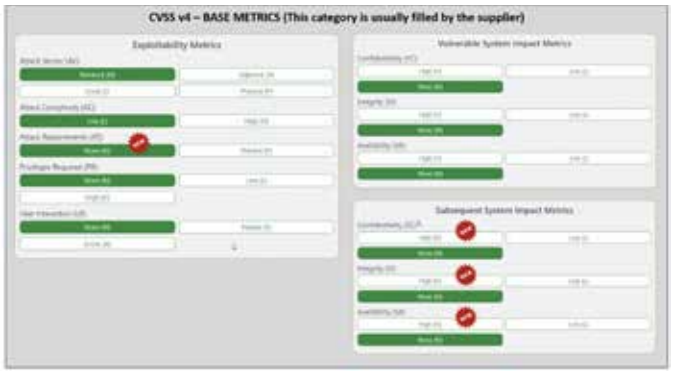
Nomenclature des composants de CVSS 4 -
Source : https://www.first.org/cvss/v4.0/specification-document

Vous avez certainement remarqué que le composant « Supplemental Metric » n'apparait pas dans les diverses combinaisons, nous y reviendrons un peu plus loin dans cet article...

CVSS 4 est constitué maintenant de 4 composants.

•Le composant « Base Metric »

Le composant « Base Metric » n'a pas subi de modifications majeures, du moins en première lecture.



Les attributs du CVSS BASE 4

- Nouvel attribut « Attack Requirements (AT) »

Cet attribut permet de déterminer les conditions de déploiement et d'exécution de l'attaque sur le système vulnérable porteur de la CVE. Ces conditions diffèrent des techniques/technologies d'amélioration de la sécurité (cf. Attack Complexity) car leur objectif premier n'est pas d'atténuer explicitement les attaques, mais plutôt d'apparaître naturellement comme une conséquence du déploiement et de l'exécution de l'attaque. Si l'attaquant ne prend pas de mesures pour surmonter ces conditions, l'attaque peut ne réussir qu'occasionnellement ou ne pas réussir du tout.

Si cet attribut contient la valeur « Present », cela signifie que la réussite de l'attaque dépend de la présence de conditions spécifiques de déploiement et d'exécution, par exemple :

- L'attaque ne peut se réaliser que dans un timing spécifique afin d'exploiter avec succès la vulnérabilité
- La réussite de l'attaque dépend de conditions d'exécution qui ne sont pas entièrement contrôlées par l'attaquant
- L'attaque peut devoir être lancée plusieurs fois contre une seule cible avant de réussir
- L'attaquant doit s'introduire dans le chemin logique du réseau entre la cible et la ressource demandée par la victime

Cet attribut semble intéressant, pourtant il semble quelque peu redondant avec l'attribut « Attack Complexity ». Néanmoins gardons ici le bénéfice du doute, nous déterminerons avec l'expérience si cet attribut sera réellement discriminant ou non.

- Nouveaux attributs « Subsequent System Impact (SC) (SI) (SA) »

La version 3.1 de CVSS comporte déjà des attributs (C, I & A) permettant d'évaluer les impacts en termes de Confidentialité, Intégrité et Disponibilité suite à une attaque réussie sur un système donné. Les codes associés à ces trois attributs sont renommés :

- Confidentiality (C) => Confidentiality (VC)
- Integrity (I) => Integrity (VI)
- Availability (A) => Availability (VA)

De plus, trois **nouveaux** attributs font leur apparition :

- Subsequent System Impact Confidentiality (SC)
- Subsequent System Impact Integrity (SI)
- Subsequent System Impact Availability (SA)

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

Sur iTPro.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 !

iTPro.fr

iTPro.fr

9 chaînes informatiques

4,200 Dossiers et Guides exclusifs
7 Flux RSS, Newsletters hebdos
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.

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

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

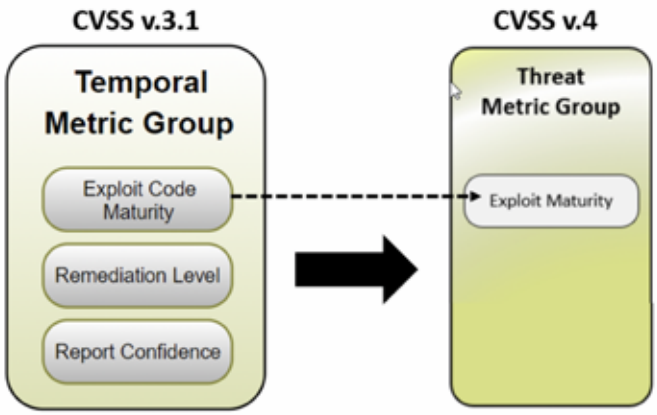
La bibliothèque éditoriale du site iTPro.fr est constituée de plus de 4200 dossiers technologiques signés par les meilleurs experts francophone et internationaux sur les thèmes de la définition, de la gestion et de l'optimisation des environnements IT basés sur les principales technologies informatiques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

L'objectif de ces trois nouveaux attributs n'est pas de définir l'impact CIA sur le système cible de l'attaque mais de définir si une compromission utilisant la CVE permettrait d'impacter **d'autres systèmes que le système cible** en termes de Confidentialité, Intégrité et Disponibilité.

Ces trois attributs sont extrêmement intéressants. Néanmoins, nous avons quelques doutes sur l'évaluation de ces trois nouveaux attributs par les fournisseurs. De plus, il faudra évaluer dans le détail comment ces nouveaux attributs seront utilisés dans la version définitive de la formule de calcul CVSS-B.

- Le composant « Temporal Metric » devient « Threat Metric »

Le composant « Temporal Metric » subit une transformation majeure, il est renommé en « Threat Metric » et deux attributs disparaissent de l'évaluation : « Remediation Level » et « Report Confidence » :



Evolution du composant Temporal Metric vers Threat Metric

Premier élément, l'attribut « Exploit Code Maturity » est renommé en « Exploit Maturity », pour l'instant pas de problème. Deuxième élément, les attributs « Remediation Level » et « Report Confidence » disparaissent de l'équation...

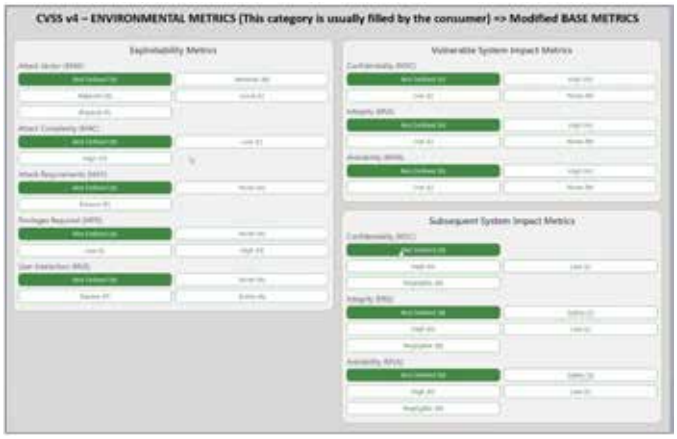
Le composant « Temporal Metric » subit une transformation majeure, il est renommé en « Threat Metric ».

Nous avons ici une interrogation, pourquoi avoir enlevé les attributs « Remediation Level » et « Report Confidence » qui nous semblent être deux attributs essentiels pour évaluer la menace réelle ? Mystère et boule de gomme... En effet, les flux de CTI modernes ont la capacité de renseigner ces informations. De plus, les valeurs de ces deux attributs ne sont pas fournies par le NVD, il appartient donc à l'organisation de les utiliser ou non.

Nous ne comprenons pas les motivations qui ont abouti à l'élimination de ces attributs, car la partie « menace » (anciennement « Temporal ») nous apparait comme un élément essentiel pour prioriser les actions de remédiation. Or, la priorisation est un élément fondamental du cycle de gestion des vulnérabilités...

- Le composant « Environmental Metric »

Pour rappel, l'objectif de ce composant est de fournir des attributs permettant de pondérer les valeurs d'attributs du « Base Metric » en injectant des données qui caractérisent l'environnement propre de l'organisation. Pas de changements majeurs de ce côté-ci.

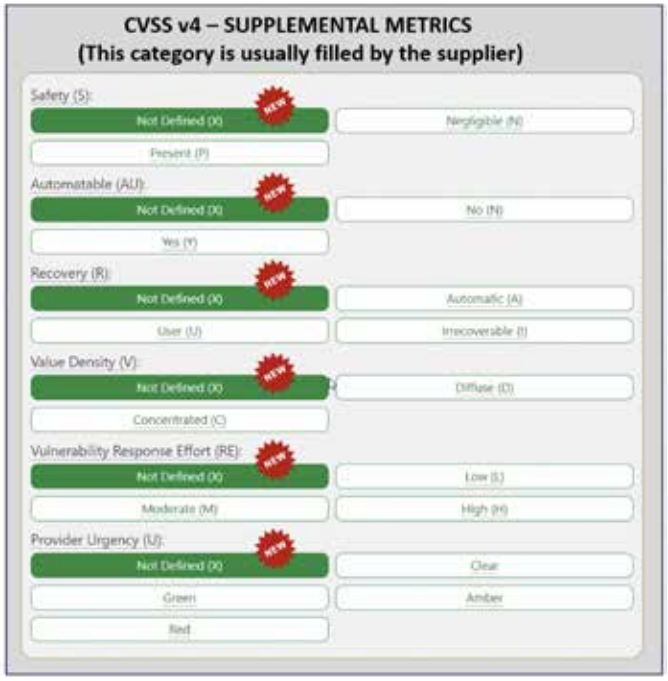


Composant Environmental Metric de CVSS 4

- Un nouveau composant : « Supplemental Metric »

Il va falloir nous habituer à cette nouvelle donne, CVSS 4 comporte maintenant quatre composants !

Un nouveau composant optionnel, appelé « Supplemental Metric », fournit une série de nouveaux attributs qui décrivent et mesurent les attributs extrinsèques supplémentaires d'une vulnérabilité. L'utilisation de chaque attribut est déterminée par le consommateur CVSS (l'organisation). Ces informations contextuelles peuvent être utilisées différemment dans l'environnement de chaque utilisateur. **Aucun attribut n'aura, dans le cadre de sa spécification, d'impact sur le score CVSS final (par exemple CVSS-B)**. Les organisations peuvent ensuite attribuer une importance et/ou un impact effectif à chaque attribut, en leur donnant plus ou moins d'effet sur l'analyse de risque finale.



Composant Supplemental Metric de CVSS 4

Vous l'avez compris, les valeurs des attributs de ce composant n'ont aucun effet sur le score CVSS global, il s'agit ici d'attributs permettant à l'organisation de réaliser une étude de risque plus poussée, et qui pourraient être utilisés en liaison avec une CMDB par exemple.

Vous pouvez consulter la version préliminaire de CVSS 4 pour une explication poussée de ces attributs : https://www.first.org/cvss/v4.0/specification-document

L'apparition du composant « Supplemental Metric » nous parait aussi utile.

Alors CVSS 4, c'est bien ou pas ?

L'étude complète des spécifications CVSS 4 nous a laissé un goût amer… En effet, nous sommes convaincus qu'il faut faire évoluer le modèle pour que les organisations puissent mieux comprendre les CVEs et surtout évaluer leurs besoins de remédiations à court, moyen et long terme.

L'évolution des attributs du composant « Base Metric » nous semble réellement intéressante. Nos projections sur la différence entre score de base CVSS 3.1 et 4 démontrent que nous obtiendrons un peu plus de finesse lors de l'évaluation de la sévérité d'une CVE.

L'apparition du composant « Supplemental Metric » nous parait aussi utile. Il est néanmoins dommage que les valeurs d'attributs ne puissent pas impacter le score global. Peut-être s'agira-t-il d'une évolution ou d'une option dans CVSS 4.1 ? Dans l'attente, ce composant vous permettra d'affiner vos études de risque, ce n'est déjà pas si mal.

La réduction à peau de chagrin du composant « Temporal Metric » est incompréhensible… Pourquoi réduire à un seul attribut la notion temporelle et l'usage réel de la CVE par les groupes d'attaquants ? Franchement, nous n'avons aucune réponse éclairée à fournir sur ce sujet, cela reste un mystère.

Nous espérons que la lecture de cet article aura pu vous fournir des informations intéressantes si vous travaillez dans le monde de la gestion des vulnérabilités.

A très vite pour de nouvelles découvertes.

> Sylvain CORTES - VP Strategy chez HACKUITY

AZURE, PILE DE DÉPLOIEMENT

Il y a de la part des fournisseurs de services Cloud tout un tas d'améliorations sur des fonctionnalités existantes mais aussi de très nombreuses fonctionnalités qui apparaissent pour couvrir des besoins qui ne le sont pas encore. Ou même parfois ... pour en créer de nouveaux.

Il faut être friand de ces nouveautés, cela fait partie de la veille technologique, cela permet de rester le plus à jour possible sur ces environnements. Mais toutes ne sont applicables. Soit parce que le client n'a pas ce besoin, soit parce que cette nouveauté ne fait pas partie du domaine d'expertise dans lequel on exerce. D'autres se chargeront de mettre en œuvre et de juger de la pertinence du sujet.

Une nouveauté

Lorsque *Deployment stacks* est arrivé du côté du portail Microsoft Azure (dans le menu des groupes de ressources), je n'ai pas immédiatement trouvé d'intérêt à ce nouveau menu.

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

IT AND CYBERSECURITY MEETINGS BY WEYOU GROUP

WWW.IT-AND-CYBERSECURITY-MEETINGS.COM

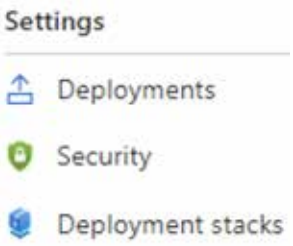
19, 20 & 21 MARS 2024

PALAIS DES FESTIVALS ET DES CONGRÈS DE CANNES

ILS SONT DÉJÀ INSCRITS

by weyou group

Professional Exhibitions and One to One Meetings Exhibitions



En passant un peu plus de temps sur ce sujet de déploiement (puisque c'est de cela qu'il s'agit), on retrouve quelques similitudes avec *Terraform*, largement utilisé pour les déploiements « As Code ». Multi fournisseurs, simple (déclaratif), il permet également de maintenir un fichier d'état. Une sorte de « sauvegarde par le code » de son infrastructure.

On retrouve également avec *Deployment stacks* une petite part des Blueprints Azure avec une notion de rationalisation, d'étendue d'application et de gestion des droits, même si c'est assez différent dans la pratique. C'est un peu de tout ça, avec quelques points propres aux piles de déploiements.

Finalement, il semble y avoir de l'intérêt à creuser un peu cette nouveauté.

Trois points attirent particulièrement l'attention dans la documentation (sources éditeur) :

- Nettoyage efficace de l'environnement en utilisant des indicateurs de suppression lors des mises à jour de la pile de déploiement.
- Empêcher les modifications indésirables des ressources managées par le biais des paramètres de refus.
- Une ressource de pile de déploiement peut être créée dans l'étendue du groupe de ressources, de l'abonnement ou du groupe d'administration. Le modèle passé dans une pile de déploiement définit les ressources à créer ou à mettre à jour dans l'étendue cible spécifiée pour le déploiement du modèle.

Utiliser Deployment stacks, c'est passer d'une logique de ressources à une logique de pile d'ensemble.

C'est encore en preview et il y a quelques limitations, mais autant se faire une idée au plus tôt sur cette nouvelle possibilité.

A noter avant d'aller plus loin, il n'est pour l'instant pas possible d'utiliser le portail pour autre chose que pour de la visualisation / détachement / suppression de pile. La création, modification se fera obligatoirement au travers de Powershell ou de l'AZ Cli. C'est une contrainte faible, la documentation est abondante et l'ensemble des commandes en fait partie. Les commandes vont utiliser des fichiers de configuration Bicep, également proposés dans la documentation. Ce qui est présenté ci-dessous est donc parfaitement et facilement reproductible.

Voici un retour d'expérience sur ce qu'amène la pile de déploiement avec quelques-uns des points les plus intéressants.

Le fonctionnement

Le principe de fonctionnement est assez simple. C'est un déploiement de ressources, dans un groupe de ressources. Mais qui forme un ensemble cohérent. Ce que Microsoft appelle « un groupe de ressources Azure en tant qu'unité atomique ». Ce regroupement de ressources, cette unité atomique, va suivre son propre cycle de vie.

En termes de création, modification et suppression. Mais ce n'est pas uniquement un cycle de vie, c'est aussi une gestion des accès. Le groupe de ressources devient en fait une ressource managée, dans son ensemble. Elle est gérée comme un tout.

C'est le premier point à bien comprendre, on passe de la gestion d'une ressource à la gestion d'un ensemble, la gestion d'une pile.

Dans la pratique, il est assez intéressant de consulter la sortie de commandes lors de la création d'un déploiement. Même sans être familier avec le code, on trouve à l'écran une projection assez clair de ce qui vient d'être mis en œuvre.

Le champ ***Id*** est l'Id qui porte le nom du déploiement *Microsoft.Resources/deploymentStacks/demoStack*

Le champ Resources est la liste des ressources qui font partie de cet ensemble. Apparaissent également les paramètres de Deny et autres paramètres de CleanUp.

Voilà bien une nouvelle façon de gérer les ressources. C'est au départ un peu dépaysant, un peu surprenant, mais c'est finalement assez rapide à adopter.

Pour aller plus loin

Au-delà des points présentés plus haut, ce qui apporte, à mon avis, le plus dans cette gestion, c'est la possibilité de définir finement les opérations de protection des ressources.

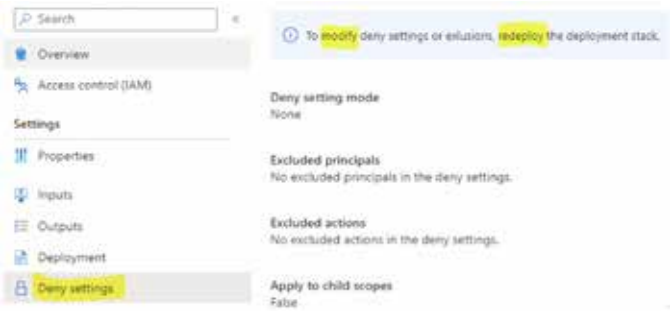
Il y a des paramètres d'opérations *DenySettingsMode* sur la ressource managée de type None, *DenyDelete* et *DenyWriteAndDelete*. Ce qui est assez proche des mécanismes de verrous (locks) existants sur Azure, même si comme expliqué un peu plus loin, c'est un verrou plus granulaire. Idem pour le mécanisme d'héritage *DenySettingsApplyToChildScopes* qui est également proche de ce qui existe déjà. Ce n'est pas de ce côté que l'on va chercher le plus de bénéfice.

Mais plutôt du côté des 2 paramètres *DenySettingsExcludedAction* et *DenySettingsExcludedPrincipal*.

Le premier va autoriser malgré le Deny quelques opérations particulières, beaucoup plus fines. Jusqu'à 200 actions, donc 200 lignes du Json qui compose les RBAC (accès en fonction du rôle Azure).

Le menu Deny Settings du portail reprend l'ensemble de ces paramètres.

Le second permet d'exclure du verrou jusqu'à 5 ID de principaux Azure AD. C'est assez nouveau, c'est un verrouillage plus souple. Le menu Deny Settings du portail reprend l'ensemble de ces paramètres. Comme indiqué sur l'image suivante, les modifier, c'est redéployer la pile.

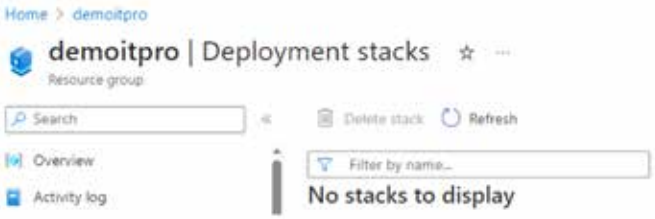


Pour poursuivre avec cette notion de souplesse, lorsque la pile de déploiement ne sert plus ou lorsqu'elle ne doit plus être vue comme une « unité atomique », elle est supprimée. Mais il y a deux notions pour cette suppression.

- La commande est lancée avec des commutateurs de type *Delete*, le tout, l'ensemble que forme la pile est supprimé.
- Elle est lancée sans, les ressources sont conservées dans le groupe de ressources mais perdent ce statut d'ensemble et deviennent des ressources « unitaires ».

Perdre ce statut, c'est aussi perdre les propriétés qui y sont attachées. Ce que l'on retrouve sur les écrans suivants. Le pile de déploiement est modifiée dans un mode *DenyDelete*. La ressource réseau virtuelle qui fait partie de ce déploiement ne peut être supprimée, message :

Les ressources de cette pile sont détachées sans commande de suppression. Le ressource groupe est conservé, mais ne contient plus de pile de déploiement.



Les ressources sont toujours présentes à la racine du groupe de ressources, mais attention, elles sont orphelines des propriétés de leur pile de déploiement, la suppression du réseau virtuel est acceptée.

Elles ne sont plus managées, plus affectées par la pile précédemment supprimée.

Reste à rapprocher les cas d'usages / nouvelles possibilités pour profiter pleinement de cette nouveauté. Je pense pour ma part qu'il y a peu d'efforts à faire pour adopter cette (nouvelle) bonne pratique.

Pour résumer, un petit rappel des points importants

1 / Utiliser Deployment stacks, c'est passer d'une logique de ressources à une logique de pile d'ensemble.

2 / Les paramètres apportent encore plus de souplesse dans la gestion des droits RBAC et la possibilité d'outrepasser les verrouillages.

3 / Les ressources déployées dans une pile peuvent être détachées / attachées à la pile. C'est-à-dire qu'elles peuvent être conservées mais deviennent « orphelines » et perdent les propriétés de leur pile.

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

Une offre innovante DÉDIÉE AU NUMÉRIQUE RESPONSABLE POUR LES DSI

L'impact de l'IT sur les émissions de gaz à effet de serre n'est plus à démontrer. Il faut désormais aborder le numérique sous un angle plus responsable, nouvel enjeu pour les DSI.
Ainsi, Lucernys et ekodev, deux cabinets experts en performance de DSI, RSE et stratégie climat, s'associent pour lancer une solution vertueuse baptisée NR 360.

Alors comment faire des DSI des acteurs de la RSE, anticipant les attentes du métier en matière de digital responsable ? Décryptage avec Christophe Dorin, directeur associé Lucernys.

Comment a germé cette idée d'offre dédiée au numérique responsable entre Lucernys et ekodev ?

Lucernys s'est engagé depuis plus de 20 ans à soutenir les DSI dans la mise en place d'une infrastructure informatique performante, répondant aux besoins des métiers. Dans cette optique, nous avons défini une approche structurée reposant sur 9 axes clés, comme par exemple l'innovation, la sécurité, la robustesse et le time to market. L'axe RSE (Responsabilité Sociale et Environnementale) est l'un de ces axes, mais il a évolué au fil du temps. Autrefois, centré sur le Green IT, il intègre désormais d'autres dimensions comme l'impact sur l'environnement ou la société.

LE DROIT À LA DÉCONNEXION : UN ENJEU RH

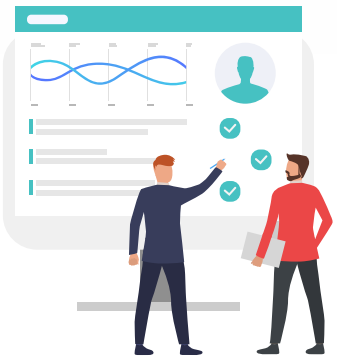
DANS UN MONDE RÉGI PAR L'IMMÉDIATETÉ,
LA DÉCONNEXION N'EST PLUS UNE OPTION, MAIS UN DROIT.

PROMODAG REPORTS PERMET LA CONFORMITÉ AVEC LE DROIT À LA DÉCONNEXION

GÉRER LA DÉPENDANCE EXCESSIVE AUX TECHNOLOGIES

LE DROIT À LA DÉCONNEXION EST UNE OBLIGATION LÉGALE

DES CHARTES DE BONNES PRATIQUES POUR LE CONFORT DES SALARIÉS



UN OUTIL AU SERVICE DES RESSOURCES HUMAINES

UNE SOLUTION DE SENSIBILISATION, D'ALERTE ET DE PRÉVENTION

PROMODAG REPORTS MAÎTRISE LE DROIT À LA DÉCONNEXION & PROTÈGE VOS SALARIÉS

Découvrez la solution Promodag Reports

Promodag

www.promodag.fr

Nous sommes tous de plus en plus sensibilisés à ces aspects, et concernant l'IT, la pandémie a contraint les entreprises à accélérer leur transition numérique, en offrant des environnements de travail accessibles depuis n'importe où. Cette accélération s'est souvent faite sans une réelle évaluation de ses impacts.

En conséquence, nos clients DSI nous ont sollicités pour les aider à définir un cadre élargi dans le domaine de la RSE. Ils souhaitent disposer de KPI pour mesurer leur situation actuelle, recevoir des recommandations à ce sujet, et suivre régulièrement l'évolution de leur performance, à l'instar des 8 autres axes que nous abordons.

Pour répondre à cette demande, nous avons collaboré avec ekodev (nous avons un actionnaire commun, le groupe EPSA), expert engagé dans la responsabilité sociétale et la transition environnementale.

Ensemble, nous avons développé l'offre NR360. Benjamin Dekester, directeur associé d'ekodev s'est basé sur le label Numérique Responsable pour établir les fondements de notre diagnostic.

La prise de conscience générale sur les impacts de nos choix sur l'environnement, la société est plus forte aujourd'hui.

L'offre NR360 a été conçue en cohérence avec ce label, lui-même inspiré de la norme ISO 26000 qui définit 7 piliers RSE principaux tels que la gouvernance, l'environnement, les achats responsables et la sécurité des données.

NR360 applique cette logique de manière plus ciblée, permettant de définir un score de performance et de formuler un premier ensemble de recommandations, telles que la mise en place d'un calcul d'empreinte carbone ou la définition de critères d'achats responsables.

Nous espérons que cette nouvelle offre répondra aux attentes de nos clients DSI et leur permettra de progresser dans leur démarche de responsabilité sociale et environnementale.

Au-delà de l'urgence de la réflexion RSE, comment allez-vous procéder pour accompagner les entreprises ?

Comme je le disais précédemment, la prise de conscience générale sur les impacts de nos choix sur l'environnement, la société est plus forte aujourd'hui.

Celle-ci n'échappe pas aux entreprises bien évidemment et elle s'organise avec des directions RSE plus présentes ou plus écoutées.

CHRISTOPHE DORIN

Ainsi, la sensibilisation RSE arrive jusqu'à l'IT, on parle de plus en plus de la déclinaison informatique de la fresque du climat, la fresque du numérique.

Il faut dire que les chiffres sont sans appel : l'IT représente aujourd'hui 4% des émissions de gaz à effet de serre dans le monde. Deux fois plus que le transport aérien. Et pour concevoir un ordinateur, il ne faut pas moins de 22 kg de produits chimiques, 240 kg de combustibles et 1,5 tonne d'eau....

Cette offre est-elle d'ores et déjà lancée ? Quelles perspectives pour 2023 ?

Oui cette offre est lancée et déjà en cours chez certains clients, mais c'est vrai que c'est le début, il faut identifier les responsables RSE IT, les sensibiliser sur l'apport qu'un cabinet IT et un expert engagé dans la responsabilité sociétale et la transition environnementale apportent à leur réflexion. Nous leur faisons gagner du temps.

On parle de plus en plus de la déclinaison informatique de la fresque du climat, la fresque du numérique.

Notre approche est structurée et basée sur des référentiels qui font foi.

Notre expérience de plus de 20 ans dans l'IT rend aussi nos recommandations applicables, car nous connaissons le contexte IT du client.

L'axe RSE n'est pas la seule métrique qui permettra de décider de telle ou telle solution IT évidemment, mais par contre, aujourd'hui, il fait partie de l'équation

> Par Sabine Terrey

Comment faire plus vite, avec moins de budget et de collaborateurs ?

L'agilité et l'autonomisation des développeurs permettront de mener des projets de transformation des applications modernes.

Les entreprises continuent d'investir dans la modernisation de l'IT et la mise en œuvre de nouveaux projets. Selon près de 60 %, le principal objectif est d'améliorer la résilience et l'efficacité face à l'évolution de l'économie mondiale.

33 millions de dollars au cours des 12 prochains mois

Les entreprises prévoient d'investir en moyenne 33 millions de dollars au cours des 12 prochains mois. Selon 78 % des dirigeants (84 % - France), les priorités ont changé au cours des trois dernières années. La transformation numérique est devenue plus réactive aux bouleversements du marché et aux préférences des clients.

Nouvelles technologies & Productivité des développeurs

Quelques constatations sont à prendre en compte.

•La pression pour les nouvelles technologies

Les responsables IT français subissent des pressions de la direction pour adopter le Cloud computing, l'edge computing et l'IoT, et les technologies low/no code.

Les équipes IT sont moins poussées à adopter des LLMs (Large Language Models) comme ChatGPT, le Web 3.0 ou la réalité augmentée ou virtuelle.

•La productivité des développeurs

La pression exercée par les développeurs pour soutenir

- le développement agile et l'innovation
- leur autonomisation pour créer plus d'applications et répondre aux besoins des clients

sont les deux principaux facteurs des projets de transformation individuels.

Dépenses IT & Retards & Attentes

•Des dépenses IT surveillées

Selon 59 % des responsables français, le directeur financier contrôle les budgets avec plus d'attention et pose davantage de questions sur les investissements IT.

Enfin, selon 30 %, la pression subie pour réaliser la transformation avec moins de budget et de ressources humaines a augmenté au cours des 12 derniers mois.

•Des difficultés et des retards

Le manque d'adhésion, l'incapacité à garantir ou à respecter les budgets, la dépendance à l'égard des technologies existantes impliquent un échec, un retard ou une annulation des projets.

70 % des entreprises françaises ont reporté leurs objectifs de transformation numérique de plus de trois mois. 44% ont reporté ou annulé un projet de transformation numérique au cours des 12 derniers mois, par crainte de l'échec.

Source Enquête Couchbase sur la transformation numérique auprès des leaders mondiaux de l'IT - 600 dirigeants IT, dont 100 issus d'entreprises françaises

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

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

La directive NIS2 :
« UN GUIDE POUR UNE ACTIVITÉ DURABLE ! »

La nouvelle directive NIS2 qui entrera en vigueur en France au deuxième semestre 2024, vise à élever le niveau de cybersécurité des entreprises européennes. Conformité, responsabilités, identité, accès, cyberhygiène ... autant de points à prendre en compte.

Entretien avec Dirk Schrader, vice-président, Security Research chez Netwrix qui nous éclaire sur le sujet.

Comment les entités concernées peuvent-elles se préparer à la mise en conformité à NIS2 ?

NIS2, comme son prédécesseur NIS, vise à élever le niveau de cybersécurité des organisations européennes en clarifiant ce que les entreprises doivent accomplir pour sécuriser leurs données. En conséquence, pour se conformer à NIS2, elles doivent évaluer en profondeur leur positionnement actuel en matière de sécurité afin d'identifier les vulnérabilités et d'y remédier.

Nous recommandons ainsi de commencer par les couches « identité » et « données », car ces dernières représentent la majeure partie des actifs informatiques, après l'infrastructure proprement dite, et ce sont généralement ces deux couches qui présentent le plus de lacunes en matière de sécurité. En s'attaquant à ces deux vecteurs d'attaque, les organisations créent donc une base solide pour le reste.

Au niveau de l'identité, il est essentiel de gérer l'accès aux systèmes, aux données et aux applications, d'appliquer des politiques de mot de passe strictes et strictement le principe du moindre privilège, ainsi que de contrôler rigoureusement les comptes à privilèges. Les solutions de gestion des identités et des accès (IAM) aident alors les organisations à mettre en œuvre ces contrôles.

Pour améliorer la sécurité au niveau des données, les organisations doivent savoir où leurs données sensibles sont stockées, avoir une visibilité sur les personnes qui y ont accès et sur les connexions qui se produisent en temps réel. C'est là que les solutions de gouvernance de l'accès aux données (DAG) entrent en jeu, en permettant aux organisations d'identifier et de s'assurer que leurs fichiers sensibles sont stockés dans des emplacements sécurisés et en offrant un audit continu pour repérer rapidement toute activité suspecte relative de ces données.

Quel sera l'impact de la directive NIS2 sur les PME et les entreprises de taille intermédiaire françaises en matière de cybersécurité ? Comment les dirigeants doivent-ils assumer leurs responsabilités ?

Une législation telle que NIS2 délivre un message très important : Chaque organisation est une cible pour les cyberattaques. Même si une entreprise ne compte que 50 employés et que son activité ne semble pas si critique, elle est un maillon d'une supply chain qui implique de plus grandes entreprises. Par conséquent, même si une PME n'est pas une cible attrayante en soi, un cybercriminel peut la cibler pour accéder ensuite à ses clients et à ses partenaires. Il est donc temps d'envisager la sécurité au-delà de sa propre organisation.

Pour assumer cette responsabilité et se conformer à NIS2, les PME et les ETI doivent passer d'une approche réactive à une approche proactive de la cybersécurité. L'atténuation des risques et la réduction de la surface d'attaque sont en effet tout aussi importantes que la détection et la réponse aux menaces.

Pour protéger correctement leurs informations, leurs identités et leurs infrastructures, les organisations doivent identifier leurs flux de données et leurs cycles de vie (génération, utilisation, destruction), mettre en œuvre l'authentification multifactorielle (MFA) pour les identités et renforcer la cyberhygiène de l'infrastructure.

En quoi la gestion des identités et des accès (IAM) et la gouvernance des identités seront-elles essentielles dans le cadre de NIS2 ?

La gestion des identités et des accès est la pierre angulaire de tout effort visant à se conformer à la directive NIS2. Il est essentiel de comprendre que si NIS2 exige l'utilisation de la MFA ou de l'authentification continue, ces mesures ne constituent pas une solution miracle pour se défendre contre les cybermenaces.

En effet, la MFA sera inefficace si l'organisation n'a pas un contrôle total sur les droits d'accès accordés et sur la manière dont l'accès est protégé. En outre, il est difficile d'imposer une authentification forte partout, et si les mesures de MFA sont trop contraignantes, les utilisateurs chercheront des moyens pour les contourner.

En outre, les organisations doivent être conscientes de l'utilisation qui est faite de leurs données sensibles, ce qui dépend fortement de la précision du processus de classification. Il est impossible de tout sécuriser, il est donc logique de se concentrer sur ce qui est vraiment important.

En résumé, les équipes de sécurité doivent être en mesure de gérer toutes les identités informatiques et de veiller à ce que seul le bon niveau d'accès soit accordé aux données, systèmes et applications sensibles, et ce uniquement pour la bonne durée. Chaque employé, sous-traitant ou fournisseur tiers doit avoir juste assez de droits pour accomplir ses tâches. Lorsque l'accès privilégié est nécessaire, il faut s'assurer de le retirer une fois le travail effectué. Une solution moderne de gestion des accès à privilèges (PAM), avec création et suppression de comptes « juste à temps », aide à automatiser ce processus.

Pensez-vous que le rôle du RSSI et du délégué à la protection des données (DPO) va changer avec cette nouvelle directive ?

Pour être honnête, je ne pense pas que ce soit le cas. Toutes les exigences de la directive NIS2 sont des bonnes pratiques fondamentales qui auraient dû être appliquées depuis longtemps, comme la cyberhygiène et la sensibilisation des employés aux cybermenaces.

Le principal changement réside dans le fait que le respect de ces exigences est désormais obligatoire pour un plus grand nombre d'organisations. Par conséquent, le seul changement dans le rôle d'un RSSI ou d'un DPO sera probablement l'ajout d'un point supplémentaire dans la description du poste, à savoir assurer la conformité à la directive NIS2.

DIRK SCHRADER

Les décisions stratégiques prises par les entreprises en matière de cybersécurité sont de plus en plus guidées par des contraintes réglementaires, plutôt que par leur propre volonté de mieux sécuriser leurs ressources et leurs données. Qu'aimeriez-vous dire à ces organisations ?

Si elles ont déjà fait le nécessaire pour sécuriser leur organisation, tant mieux pour elles. Si ces entreprises n'ont pas encore mis en œuvre les meilleures pratiques de sécurité, elles doivent s'assurer de planifier leurs activités avec soin, car le délai de mise en conformité avec NIS2 est limité. La liste des points à examiner comprend l'architecture informatique actuelle, les contrôles de sécurité, le plan de sauvegarde et de réponse aux incidents, ainsi que les stratégies de classification des données, de gestion des accès privilégiés, de gouvernance des identités et de gestion des mots de passe.

Aujourd'hui, chaque organisation est connectée à de nombreuses autres et stocke des données sensibles sur ses clients et partenaires. Des mesures de sécurité insuffisantes au sein d'une organisation affectent tous les maillons de la supply chain, comme précédemment évoqué ; avec comme exemples notoires l'attaque contre l'opérateur américain d'oléoducs Colonial Pipeline ou encore les récentes cyberattaques contre des hôpitaux en France. Nous devons commencer à traiter la sécurité de chacun de manière responsable.

Les organisations devraient considérer la directive NIS2 comme un guide pour une activité durable. Une seule violation de données peut être désastreuse pour toute organisation, entraînant une atteinte durable à la réputation et la perte de clients, en des conséquences financières immédiates.

Investir dans des mesures de cybersécurité de base nécessaires pour se conformer à la directive NIS2 se traduira *in fine* par une confiance accrue des clients et une plus grande stabilité opérationnelle.

> Par Sabine Terrey

Business At Work : UNE CULTURE DE L'INNOVATION AU SERVICE DES CLIENTS

L'ESN Business At Work a annoncé l'acquisition de Exertum, acteur de référence, spécialiste de la gestion technique des environnements SAP. Pourquoi ce rapprochement ? Quelle stratégie de développement ? Explications avec Thibault Dartevelle, Directeur Associé de Business At Work, en charge du partenariat avec SAP.

Pourriez-vous en quelques points présenter l'ESN française Business At Work ? Qu'est-ce qui vous différencie ?

Business At Work – BAW - c'est depuis près de 25 ans une aventure entrepreneuriale au service de l'amélioration de la performance opérationnelle des entreprises et des services publiques.

BAW, ce sont plus 350 femmes et hommes qui ont en commun une passion pour la transformation digitale.

BAW, c'est aussi une proposition de valeur extrêmement complète qui permet de penser la transformation, la mettre en œuvre et l'accompagner dans la durée.

#SIDO2023

L'évènement de référence
sur la convergence des technologies
IoT, IA, XR et Robotique pour concrétiser
la transformation digitale
des entreprises

LYON 9e

SIDO

IoT – AI – ROBOTICS – XR

20 & 21 Septembre 2023

Cité Internationale de Lyon

300 Exposants
60 Conférences
200 Speakers

Créer mon badge gratuit

CODE : P-SMALY23

www.sido-lyon.com

RETROUVEZ ÉGALEMENT

SIDO Paris

06 > 07 décembre 2023

Palais des Congrès | www.sido-paris.com

UN ÉVÉNEMENT

infoprodigital TRADE SHOWS

THIBAULT DARTEVELLE

Et enfin, BAW, c'est une culture de l'innovation et de la mise à disposition d'une intelligence collective au service de nos clients.

Revenons sur l'acquisition d'Exertum. Pourriez-vous évoquer les points forts de cette acquisition ?

BAW développe depuis 15 ans un partenariat très riche avec SAP. Présente sur les marchés belge et luxembourgeois, Exertum est, de son côté, un acteur reconnu pour sa maitrise des environnements techniques SAP et pour la qualité de ses services. C'est aussi une entreprise avec qui nous partageons de nombreuses valeurs.

Aujourd'hui plus que jamais, avec l'accélération du passage à S/4HANA et l'adoption de Cloud, nos clients respectifs nous demandent de les guider aussi bien sur l'adoption des nouveaux ERP, sur les trajectoires de modernisation de leurs applications SAP ou sur les enjeux technologiques associés.

C'est précisément cette complémentarité que nous allons développer avec l'acquisition d'Exertum et cela, aussi bien en France, en Belgique et au Luxembourg.

Un mot sur les perspectives d'ici fin 2023 ?

En octobre, nous nous apprêtons à retrouver nos clients à la convention annuelle de l'USF à Nantes. Cette année, nous avons particulièrement travaillé avec la commission secteur public sur les enjeux du cloud.

Pour nos clients, 2023 aura été une année riche en projets de transformation et d'amélioration de la performance. Pour beaucoup d'entre eux, c'est la préparation ou le passage à S/4HANA souvent dans le cadre RISE with SAP.

Pour les directions financières, il y une forte tendance à la digitalisation et l'automatisation des processus. On peut citer la réforme de la facturation électronique qui s'étend au secteur privé ou INFINOE le nouvel infocentre. Deux enjeux auxquels BAW répond avec des solutions innovantes.

Pour les directions supply chain, les transformations sont souvent de véritables ruptures rendues nécessaires par les besoins de performance et de résilience à combiner avec des engagements RSE de plus en plus importants. On peut citer notamment les projets de mise en œuvre sur S/4HANA des méthodes Demand Driven-MRP ou de digitalisation des entrepôts, au service de l'économie circulaire, notamment.

Enfin, pour tous les métiers, il y a des projets autour de la BTP qui répondent aux enjeux de valorisation des données et d'automatisation des processus, y compris à l'aide de l'IA.

> Par Sabine Terrey

Les 4 révolutions impactant les équipes IT

Focus sur les changements affectant les départements informatiques qui peinent à répondre aux besoins et demandes des métiers.

L'évolution des approches en matière de développement d'applications low code / no code, l'écart entre offre et demande de services informatiques et l'impact de l'automatisation et de l'intelligence artificielle sont des problématiques sous surveillance IT.

Voici les 4 principaux enseignements à prendre en compte.

La révolution de l'IA générative sur l'IT

En France, selon 77 % des responsables informatiques, le rôle de l'IA dans leur organisation est bien défini. Selon 85 %, cette technologie jouera bientôt un rôle prépondérant dans leur entreprise.

Mais 61 % sont préoccupées par la dimension éthique de l'IA générative.

Les transformations numériques en cours réduisent la capacité des services informatiques

Si 63 % des services informatiques ont du mal à satisfaire la demande des équipes métiers, 66 % s'attendent à une hausse de la demande au cours des 18 prochains mois. Ainsi, les responsables informatiques accordent de plus en plus d'attention à leur efficience opérationnelle.

La capacité de développement d'applications

Seuls 18 % des services informatiques peuvent satisfaire les demandes de développement d'applications qu'ils reçoivent.

Pour augmenter leur capacité, 70 % ont adopté des outils low-code ou no-code et 44% tirent parti de la modularité.

Une approche exhaustive en matière de sécurité

59 % des responsables informatiques français peinent à combiner les objectifs des équipes métiers et les besoins de sécurité. Ainsi, 56 % ont recours au chiffrement de données et 51 % utilisent l'authentification multifactorielle.

Source Salesforce - 28 février au 5 avril 2023 - Responsables informatiques exerçant des fonctions de directeur ou supérieures. 4 325 réponses à travers 29 pays et sur 6 continents.

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

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

Retour d'expérience : MIGRER « FACILEMENT » VOS ANCIENS SERVEURS DE MESSAGERIE VERS EXCHANGE ONLINE

Force est de constater qu'il existe encore des vieux serveurs de messagerie, fonctionnant encore avec les protocoles POP3 ou IMAP et qui parfois, doivent être migrés vers une solution nettement plus moderne : Exchange Online.

Dans cet article, nous allons donc vous expliquer les points d'attention et les outils que vous devriez utiliser pour facilement « absorber » vos anciens serveurs de messagerie. Ce contenu se base sur une récente migration en une journée d'un serveur Linux vers Exchange Online avec MigrationWiz de la société BitTitan.

Les problématiques

Accès en lecture

Dans ce cas de figure où vos anciens serveurs de messagerie n'interagissent que par un accès ou IMAP, le processus de migration doit impérativement accéder au contenu des boites aux lettres sources.

CBC

CYBER SECURITY Business Convention

Le Salon Pro de la Sécurité Numérique

JEUDI 30 NOVEMBRE 2023

MEETT - TOULOUSE

5e édition

Le RDV des experts de la cyber :

ÉCHANGER - SOURCER - S'INFORMER

AU PROGRAMME

TABLES RONDES & ATELIERS - EXPOSITION
CHALLENGE CATCH THE FLAG - RENDEZ-VOUS BUSINESS

Sécurité des informations :
données, cloud, API, EDR/XDR

Sécurité opérationnelle :
SOC, EDR/XDR

Sécurité des produits :
solutions de monitoring et alerting

Sécurité des réseaux :
pare-feu, analyse du comportement, test d'intrusion

Services :
Cyberassurances

Pour en savoir plus sur l'événement

cbc-convention.com

@CBCToulouse   @CBC - Cybersecurity Business Convention

Organisé par : DÉPÊCHE EVENTS

Partenaires média : archimag, LA DÉPÊCHE, DÉPÊCHE ÉCO, la lettre M, iTPro.fr, SMART DSI

Partenaires : ACN, AFCDP, CCI Toulouse Haute-Garonne, CESIN, CYBER'OCC, Digital113, Gendarmerie nationale, OCSSIMORE

C'est souvent délicat, car dans le cas de serveur Linux par exemple, il n'existe pas de compte de service possédant la prérogative de pouvoir visualiser l'intégralité du contenu des boites aux lettres. Il va donc falloir récupérer l'ensemble des mots de passe et des comptes de connexion pour permettre à la solution de migration de lire le contenu des boites aux lettres et de le copier vers les boites aux lettres Exchange Online de destination. C'est le côté désagréable de ce genre de migration.

Accès en écriture

Le processus de migration va devoir recevoir le droit de pouvoir écrire du contenu dans les boites aux lettres cibles, à savoir Exchange Online. La solution la plus simple est de passer par la technique de « l'impersonation ». Cette technique permet de donner un droit d'accès à un compte de service que vous renseignerez dans votre solution de migration, et qui aura les droits, sur un scope défini de boites aux lettre cibles.

La définition du scope (https://learn.microsoft.com/en-us/powershell/module/exchange/new-managementscope?view=exchange-ps) permet selon la valeur d'un attribut que vous choisirez, de circonscrire un ensemble de boites aux lettres cibles concernées. L'impersonation, ou l'usurpation d'identité signifie que le compte de service en question usurpera l'identité de chaque utilisateur de boîte aux lettres lors de la migration. D'où l'importance de définir un scope pour limiter l'étendue de l'action de ce compte de service.

Le processus de migration va devoir recevoir le droit de pouvoir écrire du contenu dans les boites aux lettres cibles.

L'annuaire

Les outils de migration et en particulier MigrationWiz de Bit Titan vont simplement migrer le contenu des boites aux lettres de façon progressive, mais ne vous seront pas d'un grand secours pour la création de l'annuaire cible. Dans notre cas de figure, avant de migrer quoi que ce soit, il va falloir, dans Exchange Online recréer l'annuaire cible. C'est-à-dire les boites aux lettres cibles avec leur alias, les listes de distribution cibles, les boites aux lettres partagées ainsi que les droits d'accès associés. Selon le nombre de boites aux lettres, ceci peut représenter une charge de travail non négligeable, mais compte tenu que le scénario de migration est de type « One shot », il faut que l'annuaire cible soit prêt avant le grand soir de la migration.

Pour cela, certains anciens serveurs de messagerie savent faire un export de la liste des boites aux lettres. Vous pouvez vous en servir pour « Scripter » la création des boites aux lettres cibles dans Exchange Online via Powershell.

Si vous intégrez un nouveau domaine de messagerie, vous pouvez tout à fait le créer dans Azure AD sans déclarer les services dans Exchange Online. Ceci vous permettra de créer les boites aux lettres cibles avec le bon domaine de messagerie sans déclarer le service dans Exchange Online. Le nouveau domaine sera identifié comme n'ayant aucun service déclaré jusqu'au jour de la migration, où vous terminerez sa configuration.

Une fois réalisé, vous pouvez même communiquer à vos utilisateurs concernés par la migration, que leur prochaine solution de messagerie est en « Avant-première ». Une fois que vous leur avez communiqué leur mot de passe pour accéder à Exchange Online, invitez-les à se connecter pour vérifier qu'ils ont accès à leur prochain environnement. Si vous avez activé l'authentification multi facteurs, cela permet de vérifier avant le jour J que tous vos utilisateurs sont en mesure d'accéder à minima à Exchange Online via le Web.

Le client Outlook ou la suite Office

Dans un scénario de migration de type POP3/IMAP vers Exchange Online, le plus compliqué n'est pas la recréation de l'annuaire dans l'environnement cible, mais bien la partie qui concerne le changement de client de messagerie. Car passer d'un simple client POP3 ou Imap4 à Outlook 365, vous en conviendrez, c'est un peu comme passer de Notepad à Word.

La première problématique que vous allez rencontrer est comment, sur des postes que vous ne maitrisez pas complètement (sauf si vous projetez de les remplacer avant la migration), déployer rapidement la suite Office.

Dans notre cas de figure, nous avons retenu d'intégrer les postes à Intune et de faire le déploiement de la suite Office 365 directement par cette solution. Ceci nous a, par ailleurs, permis de déployer Microsoft Defender et d'apporter un niveau de sécurité relatif sur des postes non maitrisés.

La seconde problématique concerne la création du profil Outlook.

Là, deux solutions s'offrent à vous. Dans la solution BitTitan, une solution de scripting est possible pour générer un profil Outlook 365.

Personnellement, nous nous sommes basés sur la seconde solution : La création du profil par l'utilisateur lorsque celui-ci lance pour la première fois Outlook.

En leur communicant un document d'accompagnement et la marche à suivre, la quasi-totalité d'entre eux ont réussi à connecter leur Outlook vers Exchange Online le jour J. Nous avons également fait de même pour les périphériques portables que nous avons intégrés à Intune, ce qui nous a permis de déployer cette fois-ci, la configuration Outlook.

La seconde problématique concerne la création du profil Outlook.

Comme à l'habitude, nous avons rencontré quelques difficultés avec les périphériques IOS et MacOs concernant l'enrôlement Intune et le déploiement de Microsoft Defender.

L'outil de migration : MigrationWiz (BitTitan)

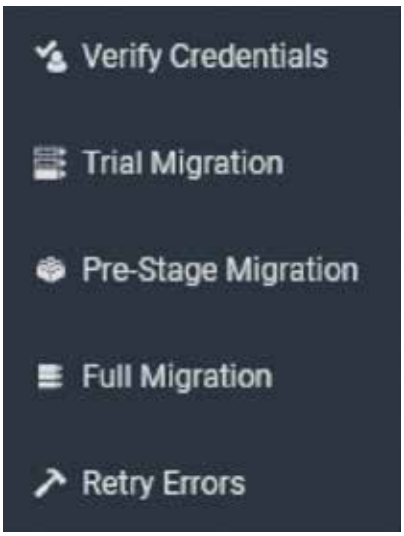
Ce n'est pas la première fois que j'utilise les solutions Bit Titan, et sans vouloir les flatter, ces solutions sont plutôt bien pensées et surtout, fonctionnent en mode SaaS.

Rien à déployer, juste de la configuration et la licence. Cela permet d'être rapide et efficace. Sachez qu'il existe une solution « gratuite » fournie par Microsoft permettant d'importer des boites aux lettres IMAP ou POP3 dont vous trouverez quelques informations ici : https://learn.microsoft.com/fr-fr/exchange/mailbox-migration/migrating-imap-mailboxes/migrate-other-types-of-imap-mailboxes. Les différents tests que nous avons menés nous ont fait choisir MigrationWiz qui s'avère beaucoup plus conviviable à l'usage et fournit en plus une migration par étapes de validation et des rapports précis.

La première étape une fois que vous avez configuré le serveur source et intégré vos fichiers de correspondance entre les boites aux lettres cibles et sources, concerne ***la validation des accès***.

Lors de cette étape, l'outil va juste vérifier qu'il peut accéder en lecture aux boites aux lettres. Naturellement, votre serveur IMAP devra être joignable depuis Internet.

La figure ci-dessous illustre la configuration du serveur source dans l'interface Bit Titan



La seconde concerne une ***migration d'essai*** où l'outil en question va migrer quelques messages depuis la source vers Exchange Online. Aucune licence n'est nécessaire pour cette étape.

La troisième étape concerne la migration dite ***prestage*** qui permet de migrer au choix entre 30 à 90 jours de message. A ce stade, une licence par boite aux lettres migrée est demandée.

Enfin, ***l'étape Full Migration*** permet de migrer la totalité des messages le jour J une fois que vous avez pris la décision de changer votre enregistrement MX et Cname, pour les faire pointer vers Exchange Online.

Nous avons en tout et pour tout, migré plus de 220 000 messages et 27 ont été reportés en erreur. Score tout à fait honorable si on l'estime en pourcentage.

L'autre intérêt de cette solution comme je l'ai précisé plus haut, est de pouvoir donner des rapports de migration précis par boite aux lettres pour connaitre de façon synthétique les utilisateurs qui n'auraient pas complétement récupérer le contenu de leurs boites aux lettres. En ayant ce type d'information, il est alors possible d'anticiper leurs appels et de voir avec eux si cela est gênant ou pas. Chose importante, MigrationWiz ne supprime rien sur le serveur source. Si des messages n'ont pas été migrés, ils restent encore disponibles sur votre ancien serveur.

L'autre intérêt de cette solution, est de pouvoir donner des rapports de migration précis par boite aux lettres

La figure ci-dessous illustre un rapport de migration sur une boite aux lettres unitaire avec quelques erreurs.

Nous avons donc migré en une journée la totalité des boites aux lettres sans véritablement rencontrer de problème majeur. Le changement de MX et la déclaration du service Exchange Online ont été faits un vendredi matin de bonne heure et les utilisateurs ont pu facilement accéder à leur nouveau client et leur nouvelle messagerie.

Si vous envisagez ce type de projet, ne sous estimez pas les tâches de préparation qui peuvent représenter plus de la moitié de la charge du projet.

Le succès de ce type de migration tient, je pense, à trois aspects :

1. La préparation,

2. La communication et l'accompagnement utilisateurs,

3. La qualité de la solution de migration qui doit vous apporter une véritable plus-value dans les opérations de migration.

Enfin dernier conseil, si vous envisagez ce type de projet, ne sous estimez pas les tâches de préparation qui peuvent représenter plus de la moitié de la charge du projet.

Une dernière chose, si vous voulez garder de bons contacts avec les équipes de sécurité, une fois le projet terminé, n'oubliez pas de supprimer le compte de service qui a servi à la migration ainsi que le scope que vous avez créé. Rappelez-vous que le compte de service possède tous les droits sur les boites aux lettres migrées désormais en production

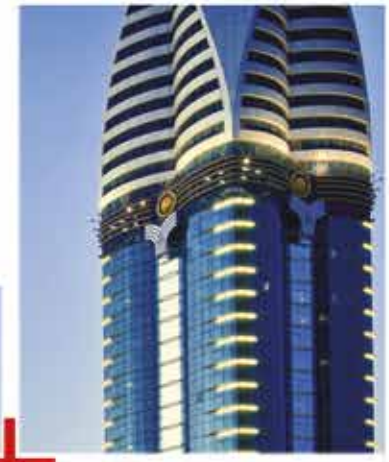
> Laurent TERUIN | https://unifiedit.wordpress.com/

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

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

▶ iTPro.fr

« 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 »

© 2020 - Conception éditoriale & graphique : Agence Com4Médias www.com4medias.com®

Datacore encourage le Datacenter « GREEN » POUR DIMINUER L'IMPACT ENVIRONNEMENTAL

Si les datacenters sont nécessaires, la question de leur impact environnemental se pose. Comment diminuer par exemple l'impact carbone du stockage des données ? Comment réduire la consommation électrique ? Entretien avec Pierre Aguerreberry, VP Sales Europe du Sud chez DataCore qui revient sur ces sujets.

La question de l'impact environnemental des datacenters se pose. Peut-on les rendre plus éco responsables ?

Tous les éditeurs et constructeurs sont conscients de l'impact environnemental des datacenters et chacun tente d'apporter sa pierre à l'édifice. Plusieurs solutions sont proposées pour réduire les consommations électriques des systèmes de refroidissement, d'empreinte au sol, d'électricité avec la mise en place de solutions photovoltaïques, d'automatisation des systèmes de sécurité afin de rendre les datacenters plus « green ». Toutes ces pistes sont adressées par de nombreuses sociétés et nous pouvons régulièrement constater les dépôts de brevets dans ce sens.

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

VOS COORDONNEES

Société .....

Nom ..... Prénom .....

Adresse de livraison.....

.....

.....

Code postal .....Ville .....

Pays .....

Tél. ..... Fax .....

email.....

Mode de règlement :

☐A réception de facture* ☐Par chèque joint

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

Indiquez votre N° TVA Intracommunautaire :

Renvoyez votre bulletin à notre service abonnements :

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

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

Au même titre que la vignette automobile, nous nous dirigeons vers une classification d'impact environnemental des datacenters qui conditionnera en partie le choix d'hébergement des clients/sociétés.

Il nous apparait important de sensibiliser les clients quant à la qualité du patrimoine de leurs données.

Du côté de DataCore Software, nous apportons des solutions de classification des données tout en nous attaquant au problème d'obsolescence, ce qui permet in fine obtenir une réduction conséquente de la consommation d'électricité.

PIERRE AGUERREBERRY

Peut-on réellement réduire leur consommation d'électricité ? Comment ?

Chaque unité de stockage consomme de l'électricité mais n'est cependant pas utilisée 24h/24h. Or, il nous apparait important de sensibiliser les clients quant à la qualité du patrimoine de leurs données.

Si nous faisons une étude rapide de notre ordinateur qui plus est des baies de stockage, nous allons observer que plus de 80% des données enregistrées le sont une fois et ne sont plus jamais accédées.

Les entreprises mais aussi les particuliers ne les détruisent jamais : nous les conservons ad vitam soit pour des raisons légales, soit par « crainte » d'une utilisation future.

Or, le maintien en ligne de ces données génère une surfacturation électrique qui n'est en rien justifiée.

Que propose DataCore en ce sens ? comment accompagnez-vous les clients ?

Notre système Swarm est une solution d'archivage active puisque nous pouvons accéder en « ligne » aux données. Swarm intègre une fonctionnalité qui va gérer l'utilisation électrique des disques : si un disque n'est pas utilisé, il est automatiquement mis en pause, ce qui implique une réduction électrique. La technologie « Darkive » permet ainsi de réduire de 30% à 50% la facture électrique des éléments de stockage. De plus, elle permet de migrer à chaud les données non utilisées du système de stockage primaire vers un système secondaire beaucoup moins énergivore.

DataCore accompagne ses partenaires et ses clients dans cette démarche en permettant de faire un mapping des données éligibles à l'archivage et de conseiller la nouvelle architecture du système de stockage des données en garantissant une forte réduction de votre facture électrique.

Outre la réduction énergétique, DataCore propose à ses clients d'augmenter la durée de vie de leurs serveurs afin de réduire l'obsolescence du matériel. Notre solution logicielle est universelle car agnostique. Si l'on prend n'importe quel serveur du marché, on constate que les composants proviennent majoritairement des mêmes fournisseurs (processeurs, caching, disques etc..). Le logiciel a donc un rôle essentiel à fournir en proposant une couche universelle de gestion, utilisable dans le temps, mais aussi en intégrant des technologies qui vont permettre de garantir des performances augmentées.

Ainsi, nous sommes non seulement capables de gérer n'importe quel type de serveur ou de matériel de stockage sans se soucier de la compatibilité matérielle mais aussi en assurant une « deuxième » vie au matériel.

Outre la réduction énergétique, DataCore propose à ses clients d'augmenter la durée de vie de leurs serveurs.

Aujourd'hui, avec plus de 2500 clients en France qui en bénéficient, la promotion du DataCenter « Green » nous laisse augurer des nouvelles références qui contribueront à diminuer l'impact environnemental des datacenters en France.

> Par Sabine Terrey

METADAYS

14 15 **novembre 2023**

Centre de congrès Rive Montparnasse

SAVE THE DATE

SALON & CONFÉRENCES

Explorez les opportunités B2B Web3 & Metaverse

800 participants
3 salles en parallèle
100 speakers et intervenants
80 sponsors & partenaires

Plus d'informations sur www.metadays.fr

Promodag | **Promodag Reports** pour Office 365 & Exchange

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

- **Mise en conformité** avec les règles de l’entreprise
- **Interopérabilité** avec les Systèmes RH
- **Audit & planification** de l’utilisation des e-mails
- **Droit à la déconnexion** et RGPD
- **Planification simplifiée** des processus de gestion
- **Rapports d’analyse** de trafic, suivi des messages
- **Optimisation des performances** de la messagerie

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

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

www.promodag.fr • +33 1 45 73 49 95 • info@promodag.com