N°27 I SEPTEMBRE 2022

CONDUIRE LA TRANSFORMATION NUMÉRIQUE DE L'ENTREPRISE

SMART DSI®

DOSSIER
Recruter des talents sur un marché tendu

INTERVIEW
Relever les défis de la supply chain durable

L'ETUDE A RETENIR
Comment augmenter les effectifs en cybersécurité ?

L'ŒIL SECURITE
Cyber-rançons et assurances

STRATEGIE
Challenges et perspectives sur la gestion des vulnérabilités en entreprise

L'ŒIL NUMERIQUE
Quatre piliers de la fabrication intelligente

ASSISES DE LA SECURITE 2022
L'innovation au service de la cybersécurité

Club Abonnés sur iTPro.fr

CLOUD IN ONE

www.cloud-in-one.fr

Accélérez votre transition vers le Cloud avec les experts DIB France

Simples à appréhender, évolutives et sécurisées, les Solutions Cloud In One de DIB France permettent aux Directions IT et Métiers de s'affranchir des contraintes IT pour gagner en réactivité, souplesse et sécurité.

Desktop-as-a-Service • Infrastructure-as-a-Service • Sécurité des données

Testez dès à présent les Solutions Cloud in One de DIB France sur **www.cloud-in-one.fr**

Planifier 2023 : se discipliner et se co-responsabiliser !

Entre bouleversements géopolitiques et climatiques, turbulences économiques, évolutions technologiques et tensions autour du marché de l'emploi, les priorités se modifient, les décisions s'affinent, et toujours dans un contexte de cybermenaces de plus en plus rapides, sophistiquées et percutantes.

Il faut absolument trouver le bon équilibre en 2023. Alors, comment prendre une longueur d'avance ? Quels investissements accroître et quels investissements diminuer ? Quelles technologies émergentes expérimenter ? Dans quel pari dynamique se lancer ? Et s'il était temps tout simplement de se réorganiser en mettant l'accent sur les notions de discipline et de précision ?

Les analystes Forrester en sont résolument convaincus, même si les dirigeants révèlent un excès d'optimisme, côté augmentations budgétaires sur toutes les fonctions, et dépenses pour le personnel, les compétences et technologies clés. Il leur est, toutefois, fortement conseillé de prioriser rapidement et judicieusement les investissements notamment dans les technologies améliorant l'expérience client, la sécurité, les ressources humaines, la rentabilité, la résilience, et de réduire drastiquement les dépenses qui engendrent le gaspillage, comme les contrats logiciels surchargés, l'externalisation de l'innovation, les marchés sous performants ou encore la dette technique.

Quant aux investissements, qualifiés de plus audacieux, on voit émerger l'Intelligent Edge, les agents intelligents rendant les expériences plus humaines, le métavers pour des pratiques immersives, les TuringBots écrivant du code eux-mêmes, ou les technologies de protection de la vie privée. Alors, continuez à expérimenter avec créativité et à évaluer avec sagesse ...

Mais revenons sur la sécurité ! Aucun répit pour ce secteur. En effet, face à un environnement de cybermenaces très actives, les actions 2023 devraient s'orienter vers la modernisation du Cloud, le Zero Trust mais aussi vers les contrôles et solutions de sécurité protégeant les domaines générant des revenus, et les infrastructures critiques.

Entre détermination et prudence, voici quelques pistes qui poussent décidément à la réflexion de la planification et la budgétisation pour l'année à venir ...

Très bonne lecture!

Sabine Terrey
Directrice de la Rédaction
sterrey@itpro.fr

(1) Source Budget Pulse 2022 Forrester – Juillet 2022

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°27 I SEPTEMBRE 2022

SMART DSI est un revue trimestrielle éditée par IT PROCOM
Directeur de la Publication : Sabine Terrey
Strategy Center - BP 40002 - 78104 St Germain en Laye, France.

N° ISSN : 2494-9701 - N° CPPAP : 0518 T 93059
www.smart-dsi.fr


P.58


P.38


P.22


P.26

SMARTDSI

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

Bala Amavasai, Frédéric Barthelet, Thierry Bollet, Sylvain Cortes, Didier Danse, Sabine Terrey, Laurent Teruin, Théodore-Michel Vrangos.

Régie Média & Publicité - Com4Médias
Christophe Rosset – Directeur Commercial
christophe.rosset@com4medias.com
Tél. 01 39 04 24 95

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

Conception & Réalisation
Studio C4M – Philippe Deslandes
conseil@com4medias.com

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

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

Recruter des talents
SUR UN MARCHÉ TENDU

> Par Didier Danse

La grande démission est attendue pour cet automne en France. Cette tendance à la démission s'est développée en 2021, notamment aux Etats-Unis où 90 millions de personnes ont quitté leur poste après une perte d'intérêt, une prise de conscience de l'inadéquation entre leur emploi et leurs valeurs ou encore l'absence de valeur ajoutée de cet emploi. Il faudra bien souvent remplacer les personnes sur le départ. De plus, les métiers informatiques ont évolué, notamment en réponse aux nouveaux besoins apparus durant la crise et de nouveaux postes doivent désormais être pourvus.

Le processus de recrutement n'est que la partie visible de l'attraction des talents et l'entreprise elle-même doit souvent se remettre en question au niveau de ses activités, de ses valeurs et de son fonctionnement. En parallèle, le recrutement doit évoluer, tant au travers des techniques que du contenu des postes à pourvoir afin de permettre à l'entreprise de continuer son développement et ce dans un marché tendu.

Des besoins et des attentes en forte évolution

LA SEULE CONSTANTE : L'ÉVOLUTION

Ce n'est un secret pour personne : le marché de l'emploi a fortement évolué ces dernières années, d'autant plus dans le domaine de l'informatique. Cela se ressent dès l'intitulé des annonces des postes ouverts avec des noms ronflants, trop souvent en fort décalage avec le contenu de l'offre elle-même.

A l'inverse, pour de nombreuses entreprises dont le cœur de métier n'est pas l'informatique, les titres « à l'ancienne » démontrent bien souvent la méconnaissance des métiers de l'informatique moderne. Dans les deux cas, il suffit de regarder les nombreux sujets qui sont liés à l'informatique pour se rendre compte des sujets dont il faut tenir compte au quotidien : le Cloud, le numérique responsable, les règlements dans les différentes industries, pour ne citer que ceux-ci.

De plus, la récente pandémie a provoqué des changements radicaux qu'il faut ancrer dans ce même quotidien. En effet, du jour au lendemain, le télétravail est devenu institutionnalisé et de nombreux nouveaux besoins se sont montrés de plus en plus prépondérants : l'accès à distance, le VoIP, le *learning management*, la cybersécurité. Travailler avec de nouvelles personnes permet également d'apporter une vue et des expériences différentes.

Il est nécessaire de comprendre les facteurs internes et externes qui poussent les employés à quitter leurs postes.

COMPRENDRE LES CAUSES DES DÉPARTS

Les opportunités externes ne sont pas les seules raisons des départs des employés et avant même de recruter en réponse aux départs, il est nécessaire de comprendre les facteurs internes et externes qui poussent les employés à quitter leurs postes. C'est ainsi qu'il sera possible de définir les politiques de recrutement et de développement des entreprises. Parmi les facteurs externes à l'entreprise, on peut citer entre autres : l'inflation, le coût des habitations et le coût de la vie.

Paradoxalement, ce sont aussi ces paramètres, en sus des inquiétantes perspectives de récession, qui ont également évité au phénomène de la grande démission d'être encore plus massif. Le domaine de l'informatique a également été moins impacté que d'autres, par le fait de l'absence des talents, ce qui a fait en sorte que les équipes informatiques sont souvent bien soignées.

D'autres facteurs tels que le stress et l'épuisement peuvent être classés comme facteurs internes.

Le recrutement : l'affaire de tous dans l'entreprise

UNE IMAGE COHÉRENTE

Le processus de recrutement est généralement l'affaire du département des ressources humaines. Pourtant, recruter requiert bien plus qu'initier et passer au travers du processus. Le département RH seul ne peut recruter efficacement, tout du moins sur du long terme et il s'agit de créer une marque employeur.

Pour créer cette marque employeur, l'ensemble des départements doivent aller dans un sens commun. L'image renvoyée par le marketing ou encore la lourdeur des processus tels que ceux d'achat de produit ou leur remboursement doivent être alignés avec l'approche prise par les ressources humaines. De plus, la cohérence au sein de l'entreprise doit s'étendre à ce qu'elle fait à l'extérieur ou tout du moins aux impacts sur la responsabilité sociale et sociétale de l'entreprise.

UN RETOUR AUX FONDAMENTAUX ET AUX VALEURS

Le travail doit désormais avoir un sens. Les historiens diront "avoir du sens à nouveau". Ainsi, il est critique d'être en mesure de répondre à la question "Pourquoi fais-je ce travail ?" et de savoir que son travail est une priorité pour l'entreprise. *Confiance* et *autonomie* sont les maîtres mots de l'ère postpandémique, tout du moins dans l'informatique.

En effet, durant deux ans, de nombreuses personnes dans le domaine de l'informatique ont pu se retrouver auprès de leur famille et amis. La balance entre vie privée et vie professionnelle est désormais rediscutée et fait partie intégrante des critères de choix des candidats. De manière générale, on peut dire que les employés et les candidats cherchent à se sentir mieux. Le bien-être au travail redevient une priorité pour beaucoup.

DES SUJETS ATTRAYANTS

L'informatique évolue au quotidien. Utiliser des technologies récentes n'est pas seulement un avantage technologique pouvant amener un avantage concurrentiel mais également un moyen d'attirer et de garder des talents. Si l'on tient compte du fait que maintenir des technologies obsolètes coûte cher, utiliser les technologies modernes peut alors devenir un argument financier.

Des solutions diverses

Pour attirer des talents, l'entreprise doit s'assurer que les fondamentaux établis mais aussi ceux émergeants soient pris en compte. En effet, ces points ont toujours été importants mais désormais c'est discuté et amplifié au travers des canaux de communication numériques. Ainsi, pour permettre aux futurs talents de se retrouver, de nombreuses solutions organisationnelles peuvent être mises en place :

- *Le temps partiel :* institutionalisé tel que la semaine de 4 jours ou au libre choix individuel
- *Le télétravail :* une approche en 4/1 ou 3/2 pour le présentiel par rapport au télétravail semble la plus efficace tant en termes de productivité et de dynamique de groupe, que pour éviter le risque d'isolement et le développement de troubles psychologiques

- *Les bureaux satellites :* le bureau satellite est à considérer comme une solution de télétravail et malgré la présence en dehors du domicile, l'isolement peut également survenir dans ces lieux
- *L'amélioration des conditions de travail* au travers de l'optimisation des bureaux et des espaces de travail de plus grande qualité.

Méthodes de recrutement

Lorsque l'on arrive concrètement dans le recrutement, l'adéquation entre les postes à pourvoir et les candidats ne repose pas uniquement sur les savoirs et compétences du métier mais plus généralement aux comportements et compétences dites générales, ceux-ci rendant le candidat plus apte à évoluer avec l'entreprise. Il s'agit donc d'évaluer ce type de compétences.

LA VIDÉO

La vidéoconférence s'est imposée durant la pandémie pour palier l'impossibilité de faire des entretiens en face-à-face. Cette approche ne fait qu'introduire de la technologie sans modifier l'approche de recrutement mais la vidéo permet d'aller plus loin en augmentant l'objectivité tout en profitant d'un gain conséquent de temps. En effet, la mise à disposition d'un questionnaire vidéo en ligne auquel les candidats doivent répondre en quelques minutes permet d'assurer l'équitabilité entre les candidats. L'intelligence artificielle peut directement numériser les réponses et identifier l'adéquation avec les attentes.

Une autre approche toujours basée sur la vidéo est de demander aux candidats de se présenter sans nécessairement répondre à des questions précises. Sur base des mots clés entendus, il est possible de définir un profil du candidat. L'intelligence artificielle peut d'ailleurs interpréter les intonations de la voix et même les émotions, bien que moins souvent utilisée car elle laisse place à plus de subjectivité.

Comme toujours avec ces technologies, il est important que la prise de décision reste du fait de l'humain. Ainsi, le recruteur se devra de valider la pertinence de l'intelligence artificielle de manière régulière en visionnant certaines réponses et en effectuant une évaluation par lui-même.

LE MATCHING DE L'EMPLOI

Certains sites d'emplois proposent non pas de publier classiquement des annonces et d'attendre les réponses des candidats mais plutôt de permettre à chacune des parties, tant le candidat que le potentiel employeur, de publier des listes de compétences ou de savoir-être attendus et proposés. Des tests en ligne permettent de valider ces mêmes compétences chez les candidats et ce, une et une seule fois, ce qui évite à chaque employeur potentiel de tester le candidat. Le site d'emplois joue alors l'intermédiaire entre les parties.

De plus, la recherche d'un candidat par l'entreprise permet alors d'identifier des candidats correspondant au poste sans pour autant qu'ils n'aient eu à postuler directement, pour autant qu'ils aient accepté au préalable de partager leur profil avec des entreprises sans les avoir sollicités, ou encore en tenant compte d'un niveau d'affinité calculé.

LE JEU ET LA MISE EN SITUATION

Les *serious games*, c'est-à-dire les jeux à finalité sérieuse, sont des solutions utiles pour pouvoir tester des candidats face à des situations données, tout en rendant l'activité ludique afin de libérer le candidat du stress des entretiens classiques. Ils peuvent reposer sur des technologies modernes bien que cela ne soit pas obligatoire. Une telle méthode de recrutement permet également de donner une image fort différente de l'entreprise qui propose de telles méthodes.

Dans le même ordre d'idée, les tests ludiques sont bien plus courts et ont comme intérêt de pouvoir être combinés pour tester des compétences ou des savoir-être différents. La mise en situation permet de tester les habilités du candidat tout en lui permettant de présenter le sujet qu'il traite à sa manière. La simulation permet de tester aussi bien les connaissances que les savoir-être.

Des tests courts, idéalement en lien avec les assignations du poste, permettent également de tester les candidats dans des situations très diverses sur une courte période. En combinant différents tests courts, il est alors possible de tester divers aspects du poste mais aussi de voir comment le candidat est en mesure de passer d'un sujet à un autre, de manière pratique. Enfin, les hackathons permettent d'identifier les producteurs de contenu et d'approches innovants le tout sur des périodes assez courtes, généralement un week-end.

UNE DISCUSSION OUVERTE

Pour certains postes, la discussion ouverte s'avère très intéressante pour les deux parties puisqu'elle permet d'échanger sur des sujets et d'élargir le périmètre des réponses que l'on peut obtenir lors d'une séance classique de questions / réponses, notamment avec des réponses fermées. La discussion ouverte a d'ailleurs comme avantage de mettre en avant les centres d'intérêts des uns et des autres. Elle ne requiert aucune technologie.

Confiance et autonomie sont les maîtres mots de l'ère postpandémique, tout du moins dans l'informatique.

DES CANAUX ADAPTÉS À L'AUDIENCE

Les canaux et les méthodes de communication utilisés renforcent l'image des entreprises bien au-delà du message. Ainsi, des entreprises dans le monde de la finance continueront à utiliser des canaux de communication classiques tandis que certaines entreprises ont fait le choix de partager du contenu humoristique, sans raison apparente, au travers de plateformes telles que TikTok, ce qui leur donnera un avantage certain quand ils cibleront les candidats plus jeunes.

Publier des annonces présentées sous la forme d'une fiche de poste sur www.vieuxjobboard.fr alors que les jeunes sont cibles pour des postes très dynamiques ne fait aucun sens.

D'autres solutions quand on ne peut y parvenir

Recruter n'est pas toujours simple et dans certains cas, il est nécessaire d'envisager d'autres solutions.

L'OUTSOURCING

Faire appel à des sociétés ou des indépendants a des vertus intéressantes puisqu'il s'agit de ressources temporaires, bien souvent spécialisées et qui peuvent suivre des règles différentes, notamment en termes de lieu de travail etc.

L'appel à des ressources situées dans des pays tiers peut s'avérer très tentant et peut fonctionner pour autant que la culture des uns et des autres soit compatible mais aussi que les règles de fiscalité et le RGDP soient respectés. Dans tous les cas, il est important que les employés ne se sentent pas lésés.

LE RECRUTEMENT DANS D'AUTRES RÉGIONS

Parfois, l'ouverture de bureaux satellites dans d'autres régions voire à l'étranger permet de profiter de la possibilité de profiter de règles très différentes, de réduire les coûts mais surtout de toucher de nouveaux potentiels talents.

La meilleure solution pour recruter ? Ne pas devoir recruter !

L'apport de nouvelles recrues est important pour une entreprise. C'est ainsi qu'il y a des points de vue différents et il s'agit de ne faire appel au recrutement que lorsque les autres solutions ont été envisagées. Les solutions internes, bien qu'elles coûtent de l'argent, sont parfois plus économiques que le recrutement dans le but de remplacer. En effet, si vous ne l'avez pas déjà fait, je vous suggère de faire le calcul du coût d'un recrutement : le temps passé à la recherche de candidats, les frais inhérents à organiser les entretiens, le temps passé par les personnes déjà en poste, la préparation administrative - contrats, déclarations, ... - ou encore la formation et la productivité plus faible durant plusieurs mois.

A cela s'ajoutent les coûts liés au départ de la personne remplacée, tels que la baisse de productivité directement avant son départ ou encore lors de sa recherche d'emploi.

LA MOBILITÉ ET PROMOTION INTERNE

Ainsi bien que garder ses employés semble être la solution idéale, il est force de constater que pour maintenir l'intérêt de l'employé ou de l'employée, il est nécessaire de permettre les changements de postes au sein de l'entreprise, tant au travers de la mobilité géographique lorsque cela est possible ou encore en changeant de département.

La promotion en interne permet également de combler rapidement des postes tout en testant le candidat au poste à pourvoir. Cette approche se doit cependant d'être clairement définie avec le candidat et doit être idéalement discutée avec les membres de l'équipe.

L'ACCOMPAGNEMENT DE CARRIÈRE

Il peut être intéressant de créer des nouveaux canaux de recrutement et de favoriser l'adéquation entre les candidats et les postes à pourvoir, notamment en accompagnant les formations ou encore en mettant en place des programmes de formation et d'accompagnement dans les écoles ou avec la fonction publique.

Recruter efficacement requiert de se préparer et de définir la ou les approches de recrutement.

Définir sa stratégie

Vous l'aurez compris, recruter efficacement requiert de se préparer et de définir la ou les approches de recrutement. Les recrutements internes s'avèrent une solution très efficace. De plus, il arrive qu'ajouter des ressources à une équipe coûte parfois moins que de remplacer des personnes en poste. Ainsi, avant même de penser aux remplacements, il faut réfléchir aux solutions pour maximiser l'intérêt des employés et employées.

Dans ce contexte, des solutions ne sont pas liées au recrutement mais coûtent moins chères que les recrutements : fournir du matériel adapté et de qualité, permettre le télétravail partiel – que ce soit à domicile ou dans des business centers. Dans tous les cas, il est nécessaire de s'assurer que les règles soient respectées.

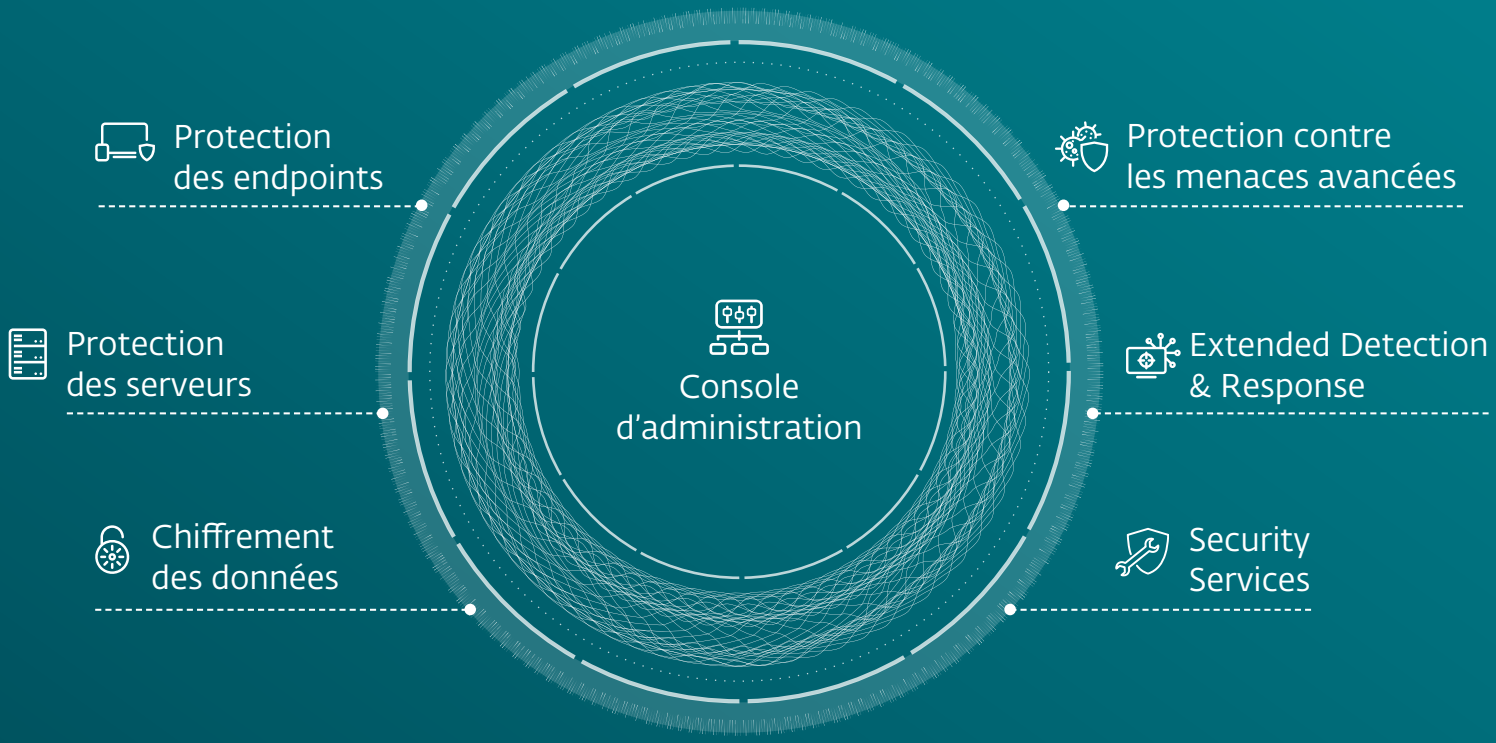
Ensuite, il est important de garantir une approche cohérente et en phase avec l'image souhaitée. Cela passe par la recherche de ressources au niveau local, la promotion dans les écoles, la non-débauche à la concurrence. Le respect des valeurs de l'entreprise est partie prenante dans la marque employeur. Enfin, l'entreprise a un impact sur la société et peut influencer le coût de la vie. Il est important d'en tenir compte !

Didier Danse - IT Manager | IT Architect | Agilist

ESET PROTECT MDR

PROTÉGEZ L'AVENIR DE VOTRE ENTREPRISE

Protection maximale de votre environnement informatique,
avec une gestion complète des cyber-risques et une expertise de nos experts



www.eset.com/fr

Special Report

METSYS

Microsoft

Metsys invite les entreprises à découvrir et adopter une sécurité moderne « Zero Trust »

Une démarche Zero Trust ne s'improvise pas. Elle se construit en adoptant une nouvelle culture de la sécurité et une multitude de briques de sécurité. C'est ce que Metsys a expliqué et démontré par la pratique un peu partout en France d'ateliers gratuits dédiés aux approches modernes de la cybersécurité et de la cyber-résilience des entreprises, au sein des Microsoft Labs.

L'approche Zero Trust, cette sécurité « sans confiance » au cœur des discussions actuelles sur la cybersécurité, ne se construit pas en un jour. Cette façon d'aborder la sécurité numérique des entreprises se construit progressivement, brique par brique, et présuppose la maîtrise d'un certain nombre de principes qui lui servent de fondation.

Comme le rappelle l'ANSSI dans son rapport sur « le modèle Zero Trust », « *cette approche demeure ardue, faute de maturité* ». D'autant qu'elle va exactement à l'inverse du principe de « *confiance implicite* » qui rythmait le modèle ancestral de défense périmétrique auquel trop d'entreprises restent encore attachées, alors qu'il n'a plus aucun sens dans un monde de travail hybride avec des collaborateurs travaillant à domicile et des données délocalisées dans le Cloud.

Le Zero Trust n'est pas une technologie. C'est un concept qui consiste à réduire la confiance accordée aux utilisateurs, aux administrateurs et aux appareils qu'ils utilisent en focalisant les efforts de sécurité sur les identités, le réseau, les accès, les applications, les données avec des contrôles permanents, granulaires et dynamiques.

Afin d'aider les entreprises à progresser sur le chemin du « Zero Trust », Metsys a animé avec Microsoft, des « Labs » dédiés à la cybersécurité moderne (format présentiel et en ligne, et disponibles également en replay). Au cours de ces « Labs 100% Cybersécurité », les interlocuteurs sont revenus sur les piliers d'une sécurité Zero Trust et sur les démarches et outils proposés par Microsoft pour adopter une posture « Zero Trust » complète, globale et pérenne.

Connaître son niveau de maturité

La démarche prônée par Metsys et Microsoft démarre par une compréhension du niveau de la maturité Cyber de chaque entreprise. « *Zero Trust is a journey* » (le Zero Trust est un voyage) » rappelle **Paul Dominjon**, directeur des solutions Cybersécurité chez Microsoft. « *Comme dans toute démarche, il est important de savoir d'où on part pour savoir quelles sont les étapes à suivre dans cette trajectoire qui vous mènera au Zero Trust. Applications des basiques de l'ANSSI, utilisation systématique du MFA, taux d'usage des applications cloud… Il est essentiel d'évaluer le niveau de maturité en matière de cybersécurité* ».

Microsoft a ainsi élaboré un questionnaire de maturité Zero Trust qui permet d'évaluer le degré d'avancement d'une entreprise sur la sécurisation des 6 piliers de la cybersécurité Zero Trust : les identités, le réseau, les accès, les applications, les données et l'infrastructure élargie au cloud.

Celui-ci en main, chaque entreprise peut mesurer les efforts à faire pour progresser sur ces 6 piliers avant d'adopter une posture « Zero Trust » à proprement parler. Des efforts qui doivent s'accompagner d'un changement de culture.

Un changement de culture…

Zero Trust est un changement de modèle de sécurité pour s'adapter aux menaces actuelles et répondre aux nouveaux besoins d'ouverture. « *C'est un changement d'état d'esprit* » explique **Paul Dominjon**. « *Le passage en travail à distance imposé par la crise pandémique a fait exploser les dernières velléités de concevoir le SI comme un château fort* ».

Les confinements successifs et l'adoption du travail hybride qui en découle aujourd'hui ont encouragé bien des entreprises à réfléchir sur la notion de confiance, « à qui » elles pouvaient faire confiance et, au final, à prendre conscience qu'il est plus simple et plus logique de choisir par défaut de ne faire confiance à personne.

Par ailleurs, avec des besoins intensifiés par la crise de prendre le contrôle à distance des infrastructures privées mais également les besoins engendrés par une adoption massive des infrastructures dans le Cloud (IaaS), « *les entreprises ont cherché des moyens de mieux contrôler l'attribution des privilèges et de gérer avec une attention accrue les comptes administrateurs en s'assurant que les privilèges nécessaires à ces accès soient fréquemment remis à jour* » ajoute **Paul Dominjon**.

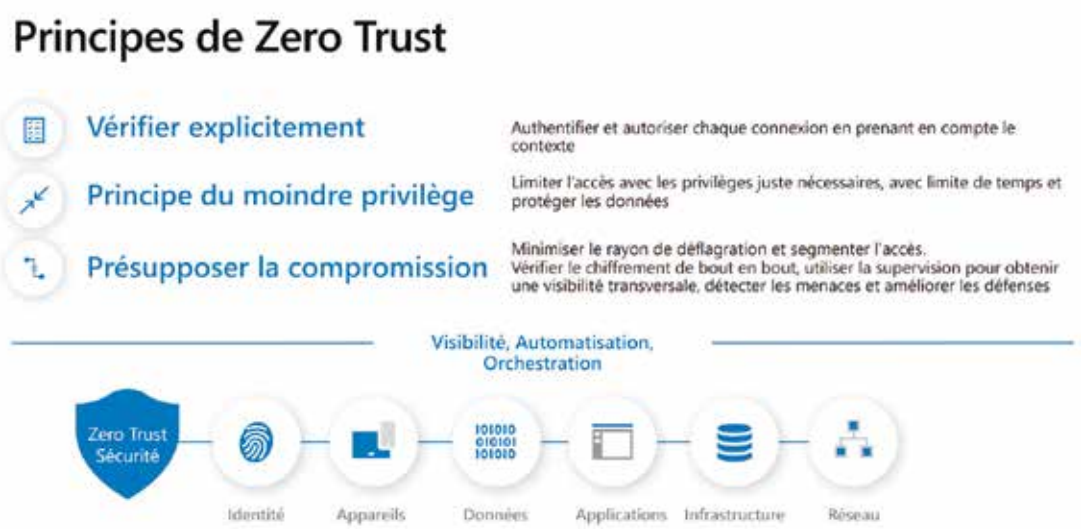
Enfin, la démarche Zero Trust est aussi marquée par un autre changement de mentalité fondamental comme l'explique **Hervé Thibault**, Chief Strategy Officer de Metsys : « *il est essentiel de présupposer que l'on est attaqué. Cela impose de savoir se projeter, de faire de la détection & réponse, et d'agir comme si le réseau était compromis* ».

… Qui nécessite un accompagnement

« *Face à un tel changement d'état d'esprit, qui demande à être expliqué, vulgarisé, assimilé, les entreprises ont besoin d'un accompagnement* » constate **Hervé Thilbault**. « *Et bien évidemment une telle approche a aussi un impact sur les outils et technologies à mettre en œuvre* ».

Microsoft propose ainsi de multiples briques permettant de couvrir l'ensemble des piliers d'une architecture Zero Trust. Ils permettent une approche progressive, éclairée par la compétence des experts cybersécurité de Metsys. « *Faire de Microsoft une fondation de sa sécurité peut encore surprendre certains responsables informatiques* » note **Hervé Thibault**. Pourtant, la division cybersécurité de l'éditeur comporte plus de 8.500 experts et réalise un chiffre d'affaires de 15 milliards de dollars, ce qui fait aujourd'hui de Microsoft l'un des tous premiers acteurs du marché de la cybersécurité.

Zero Trust est un changement de modèle de sécurité pour s'adapter aux menaces actuelles et répondre aux nouveaux besoins d'ouverture.



L'approche Zero Trust repose sur 3 principes fondamentaux et 6 piliers sur lesquels se focalisent les efforts

Construit au fil du temps, ce portfolio de solutions est l'un des plus complets et des plus matures du marché. « *Aujourd'hui, les entreprises ne s'interrogent plus sur la performance des outils ou la pertinence de Microsoft en matière de sécurité. Nous sommes désormais bien plus interrogés sur l'articulation des multiples solutions qui forment la plateforme Microsoft* » confirme ainsi **Laurent Cayatte**, Président de Metsys.

Une offre qui couvre l'intégralité des besoins

L'offre Microsoft couvre aujourd'hui les 6 piliers de la sécurité Zero Trust :

* **L'identité** avec des concepts comme le MFA, le passwordless, l'accès conditionnel, la gestion dynamique des comptes à privilèges tous pris en charge par Azure AD et renforcé par son bouclier « Microsoft Defender for Identity ».
* **Le réseau** avec cette idée qu'Internet devient le réseau de l'entreprise et qu'il faut diminuer la surface d'attaque en pratiquant une segmentation (avec Azure Networking) et en s'appuyant sur Azure Firewall, Azure WAF, Azure Security, Microsoft Sentinel et Microsoft Defender XDR.
* **Les appareils et points d'accès** avec notamment la mise en œuvre de l'accès conditionnel Azure AD, mais aussi la sécurité des appareils avec Microsoft Defender for Endpoint et Microsoft Endpoint Manager mais aussi Microsoft Defender for IoT afin de protéger les appareils dans toute leur diversité.
* **Les applications** avec la solution CASB et Microsoft Defender for Cloud Apps,
* **Les données** avec une surveillance accrue des accès mais aussi le chiffrement et le classement automatique via Microsoft Information Protection.
* **L'infrastructure élargie au Cloud** avec Azure Security et Microsoft Defender for Cloud qui s'étend au-delà du Cloud Microsoft dans une véritable approche multicloud.

> Une telle démarche réclame un accompagnement de proximité avec des experts dotés d'une véritable expérience de terrain

Progresser sur ces piliers et assembler ce puzzle en un tout cohérent à même de soutenir une démarche Zero Trust est devenu une priorité pour bien des entreprises.

« *Ce qu'on a voulu montrer au travers des 4 ateliers, c'est toute la pertinence de l'approche Microsoft et la complétude de l'offre,* explique ainsi **Laurent Cayatte**, *mais aussi l'importance pour l'entreprise de se faire accompagner face à ce qui peut sembler un énorme défi à relever.* »

Special Report

En route vers le Zero Trust

Pour les DSI, les RSSI, les responsables d'entreprises, l'approche Zero Trust a quelque chose de très marketing. Derrière, se cachent des méthodes de travail nouvelles, des modes de fonctionnement nouveaux, et de nouveaux composants défensifs. Tout ceci ne se décide pas d'un claquement de doigts, ne s'implémente pas d'un clic et ne se maîtrise pas en un jour.

« *Les outils de sécurité ne sont pas là pour combler l'absence de stratégie et de bonnes pratiques* » explique **Laurent Cayatte**. « *À l'inverse, ils sont là pour implémenter les stratégies et la posture de sécurité élaborées conjointement par les responsables de l'entreprise, les responsables métiers, la DSI et le RSSI* ».

Une telle démarche réclame un accompagnement de proximité avec des experts dotés d'une véritable expérience de terrain, habitués à insuffler les bonnes pratiques et à mettre en œuvre les outils pour servir les besoins réels des entreprises. Des experts aussi capables de soutenir au plus près les clients lorsqu'ils sont attaqués.

« *Notre métier est d'avoir désormais une approche globale dans la construction de la sécurité d'infrastructure hybride, cloud et multicloud, dans la sécurisation des applications, dans la protection des données, dans la sécurisation des identités et jusqu'à la sécurisation de tous les appareils, du PC aux smartphones en passant par les équipements connectés (imprimantes, enceintes, etc.)* » conclut **Laurent Cayatte**.

Pour aller plus loin

Cybersécurité Metsys
https://www.metsys.fr/offres/cybersecurity/

Les ateliers gratuits proposés
https://www.metsys.fr/offres/cybersecurity/nos-offres-cybersecurite#programmes-financements-ms

Le maturity model Microsoft
https://www.microsoft.com/fr-FR/security/business/zero-trust/maturity-model-assessment-tool

METSYS
www.metsys.fr

Conception éditoriale & réalisation : Agence COM4MÉDIAS www.com4medias.com - crédit photos : Shutterstock

Cyber-rançons ET ASSURANCES

Dans le monde de la cybersécurité, il y a un dicton qui dit "Il y a deux catégories d'entreprises : celles qui se sont fait hackées et celles qui ne le savent pas encore".

C'est ironique, moqueur, mais malheureusement assez proche de la réalité, celle des milliers d'entreprises qui n'investissent pas et ne sensibilisent pas leurs collaborateurs aux dangers de la cybersécurité. La très, très grande majorité d'entreprises, ce sont des PME voire des TPE. Leurs efforts sur le plan de la protection de leurs systèmes d'information et des données est faible. La CCI Occitanie a révélé que 60% des PME/PMI impactées par les cyberattaques mettaient la clé sous la porte à court terme... Par exemple, cet été, la société Clermont Pièces de Clermont-Ferrand a dû cesser son activité à cause d'une attaque informatique virulente qui a engendré la perte irréversible des données stratégiques de la société (fichiers clients, historique de production, données comptables...).

Certes, les grandes entreprises et les ETI, ainsi que de plus en plus des PME de taille moyenne investissement en cyber mais c'est la partie visible de l'iceberg. On observe, d'ailleurs, la multiplication des attaques en deux temps, d'abord passant par des PME, sous-traitants ou fournisseurs des grandes entreprises, eux mieux protégés.

Et dans ce contexte de sous-investissement et surtout de sous-formation et sensibilisation les attaques de ransomware font des ravages. Une estimation faisait apparaître un taux de paiement de 20% des demandes de paiement en provenance des entreprises françaises. Et c'est souvent la double peine : l'entreprise paie, mais ne retrouve pas ses données.

Co-sponsored by

TERRANOVA SECURITY

Microsoft

GONE PHISHING TOURNAMENT™

VOS EMPLOYÉS SONT-ILS APTES À DÉTECTER LES E-MAILS DE PHISHING ?

Découvrez-le en participant gratuitement à la plus grande simulation d'hameçonnage mondiale !

SCANNEZ LE CODE QR
ET INSCRIVEZ-VOUS
AVANT LE 7 OCTOBRE !

WWW.TERRANOVASECURITY.COM/FR-FR

Le principe d'indemnisation des rançons payées par les entreprises

En ce début du mois de septembre, le ministère de l'Économie vient d'acter le principe d'indemnisation des rançons payées par les entreprises sous réserve qu'elles portent plainte. Ou seulement qu'elles portent plainte....

Les cyberattaquants ne sont plus des personnes isolées, mais une véritable industrie, structurée et automatisée.

Comme le rapport de Bercy le soulignait, ''la loi constitue un point d'équilibre entre la volonté de ne pas financer l'écosystème des cyberattaquants et la volonté d'éviter la mort des PME et TPE touchées par une attaque.''

La réalité que beaucoup de monde ignore est que les cyberattaquants ne sont plus des personnes isolées, mais une véritable industrie, structurée et automatisée. Les attaques ne se font plus ''à la main'' sporadiquement, mais suivant une automatisation générale et systématique de toute présence sur Internet ; des scanners traquent, peignent les failles, identifient les nœuds IP vulnérables puis revendent ces cibles à d'autres groupes malveillants qui exploitent, volent et chiffrent les données, et in fine demandent les rançons. Sans se protéger en amont et entretenir régulièrement cette protection l'entreprise sera fatalement victime.

Des efforts d'investissements en cybersécurité et en sensibilisation des employés

Les pouvoirs publics avaient pris position en faveur de l'indemnisation des sinistrés par les assureurs.

Certes porter plainte est une ''démarche contraignante'' (donc filtrante) à franchir par la victime validant de facto le sérieux de l'attaque et les pertes subies, mais pourquoi on ne demande pas aux entreprises de prouver leurs investissements amont en outils et formation de leurs collaborateurs ? On indemnise ceux qui agissent préventivement en amont au même niveau que ceux qui négligent les mesures de base.

La prise en charge par les assurances des sinistres subis et du remboursement des rançons, sans demander en échange à leurs clients des efforts d'investissements en cybersécurité et en sensibilisation des employés est aux yeux des professionnels de ce domaine un chaînon manquant dans la réponse aux dangers de la cybersécurité.

Demander aux entreprises de prouver leurs investissements amont en outils et formation de leurs collaborateurs.

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

Comment augmenter les effectifs en cybersécurité ?

Les entreprises françaises sont impactées par la pénurie de talents en cybersécurité. Alors comment augmenter les effectifs ? Formation continue et diversité sont des pistes

Elargir le cercle des talents

Les chiffres sont inquiétants : selon 83 % des professionnels français, la pénurie de main-d'œuvre impacte la capacité des entreprises à sécuriser les systèmes d'information et les réseaux.

33 % travaillant dans ce domaine en France vont changer de métier à l'avenir. Les raisons indiquées :

- le Burn out lié à la pandémie
- l'émergence croissante des cybermenaces

Il est temps de changer les pratiques dans les secteurs privé et public, « *combler le déficit de talents en cybersécurité n'est pas seulement un impératif commercial, mais c'est aussi crucial pour la sécurité nationale et notre vie quotidienne. Nous devons supprimer les barrières à l'entrée, travailler activement pour inspirer les gens à faire un travail qui a du sens et s'assurer que ceux qui sont dans le domaine sont retenus.* » Bryan Palma, PDG de Trellix.

La formation continue

Certains pays (Russie et Chine) accompagnent les talents en cybersécurité au travers de formations financées par l'État, d'autres pays en sont loin.

Que retenir pour mettre en place de vraies stratégies ?

- *Diplômes universitaires*

La majorité est titulaire d'un diplôme universitaire lié aux technologies de l'information, à l'informatique et à la technologie, avec ou sans spécialisation en cybersécurité – 84%

- *Formation professionnelle*

La formation professionnelle est cruciale : si 56 % en France jugent les diplômes inutiles à la poursuite d'une carrière, la formation professionnelle (85 %) et la validation des qualifications (80%) sont des facteurs essentiels

Objectifs : *poursuivre les efforts pour promouvoir les métiers de la cybersécurité et amener les étudiants à suivre un parcours professionnel orienté STIM (sciences, technologies, ingénierie, mathématiques), et penser financements complémentaires.*

La diversité

En France, dans le milieu de la cybersécurité, la majorité sont des hommes (70%), blancs (82%) et hétérosexuels (85%).

La France est le pays où le pourcentage de femmes déclarant travailler en cybersécurité reste le plus élevé (29% contre 5% pour le Royaume-Uni et 7% pour l'Allemagne).

Objectifs : *prendre des mesures pour l'égalité des salaires, l'inclusivité homme-femme (98%) et la diversité des effectifs (97%).*

Le mentorat et l'apprentissage

D'autres mesures sont à prendre pour favoriser l'accès à la cybersécurité :

- le développement du mentorat
- les stages de longue durée
- l'apprentissage

Il est temps de considérer les parcours atypiques, dépourvus d'expérience en cybersécurité.

Un secteur évolutif et pertinent

Si les fonctions exercées sont jugées intéressantes, l'aspect constructif et porteur de sens motive les collaborateurs en cybersécurité, même si selon 38 %, aucune gratitude ne leur est témoignée pour le bien qu'ils font à la société.

Plus de la moitié (France) perçoit ce secteur progressif et évolutif et aime explorer les nouvelles tendances et es sujets stimulants. La cybersécurité gagne en pertinence.

Enfin, la cybersécurité est perçue comme un parcours professionnel avec une certaine longévité.

Source Rapport Trellix & Vanson Bourne - Professionnels de la cybersécurité en Allemagne, en Australie, au Brésil, au Canada, aux États-Unis, en France, en Inde, au Japon et au Royaume-Uni - Divers secteurs d'activité.

Codéin, l'infogérance hautes performances

Agence web open source, Codéin s'est lancée, en 2019, dans l'infogérance de serveurs Linux pour Cloud privé ou public. Cette double expertise lui permet de garantir des niveaux de performances et une qualité de service particulièrement élevés.

Les entreprises qui confient le développement et l'hébergement de leurs sites ou applications web à deux prestataires différents en ont certainement fait l'amère expérience. Au moindre bug ou baisse de performances, l'agence web et l'hébergeur se renvoient mutuellement la balle. Selon la partie interrogée, le problème vient d'un bout de code non optimisé ou, inversement, d'une infrastructure défaillante.

Agence web open source, Codéin a décidé de briser ce cercle vicieux en lançant, en 2019, son propre service d'infogérance. Un service premium qui met l'accent sur la personnalisation de l'offre, la qualité de service, le niveau de performances et la réactivité du support client.

Pour mettre fin à l'affrontement stérile entre les « dev » et les « admin », Codéin a tout d'abord généralisé l'approche DevOps. « *Plus de silos organisationnels, les échanges sont permanents entre les équipes de développement et d'hébergement* », se réjouit **Laurent Esposito**, cofondateur de Codéin.

Codéin a aussi fait des choix techniques forts pour garantir des engagements de services particulièrement élevés. Créée en 2014, la société s'est concentrée sur l'infogérance de serveurs Linux dans le cadre d'un Cloud privé ou public et pour des environnements open source de type PHP, Java, Ruby ou Node.js.

Pour répondre aux enjeux de souveraineté et se prémunir des risques juridiques, avec le principe d'extra-territorialité du droit américain qui régit le Cloud Act, Codéin a retenu deux providers français :

- La société loue des serveurs dédiés à OVHcloud. Avec ses datacenters situés à Gravelines, Roubaix et Strasbourg, le leader européen du Cloud public offre un hébergement géoredondé des données.

> **Un service premium qui met l'accent sur la personnalisation de l'offre, la qualité de service, le niveau de performances et la réactivité du support client.**

- Codéin fait également appel à 3DS Outscale et propose une interface de gestion de son cloud public (CodeOps) qui offre aux développeurs la possibilité de scaler en un clic, ou de créer des serveurs de tests temporaires à la demande pour tester une fonctionnalité. La filiale Cloud de Dassault Systèmes est le premier provider certifié SecNumCloud, visa délivré par l'Agence nationale de la sécurité des systèmes d'information (ANSSI).

UN SERVICE CLIENT TOUJOURS ACCESSIBLE

De son côté, Codéin s'est organisée en interne pour proposer une offre personnalisée. Cela passe par une compréhension fine du besoin pour concevoir et optimiser l'architecture de l'infrastructure en fonction de la nature et de la criticité des solutions hébergées. La plus-value de Codéin porte ensuite sur la qualité du monitoring et du traitement des incidents ainsi que sur la disponibilité de l'équipe support, composée d'ingénieurs systèmes.

Pas de call center à l'étranger, les clients peuvent contacter en direct leurs interlocuteurs dédiés par ticket, mail ou téléphone. Les chefs de projet ont, par ailleurs, une double compétence d'ingénieur système. *La culture DevOps permet d'abattre les murs*, constate **Laurent Esposito**. *Il n'y a pas chef de projet chez Codéin qui ne maitrise pas les fondamentaux de la gestion d'infrastructures.* »

« *Nous sommes capables de plonger dans une application web, de regarder les logs qui dépassent le cadre classique des logs purement système* » complète **Mathieu Blanc**, responsable Hosting de Codéin. Cette double expertise nous permet de donner des pistes à nos clients en leur conseillant d'aller regarder ce bout de code qui semble présenter un souci. »

Fort de ses atouts, Codéin peut contractuellement s'engager sur des garanties de temps d'intervention (GTI) ou de temps de rétablissement (GTR). « *Codéin signe avec ses clients une convention de services d'une vingtaine de pages qui détaille les opérations de surveillance, les procédures d'escalade en cas d'incident et les niveaux d'engagement de services (SLAs)* », poursuit **Mathieu Blanc**.

Dans une démarche d'amélioration continue, Codéin recommande, à partir de graphes de métrologie, différentes actions préventives. Le prestataire a aussi mis en place des procédures lui permettant d'anticiper et de limiter les conséquences d'une compromission ou d'un déni de service. Il propose, par ailleurs, un plan de reprise d'activité (PRA) adaptable en fonction de la sensibilité des données et de la fréquence des sauvegardes souhaitée.

En matière de sécurité, Codéin assure une veille permanente à partir de la liste de diffusion du CERT-FR, le Centre gouvernemental de veille, d'alerte et de réponse aux attaques informatiques, et des informations remontées par la communauté Linux. « *En faisant appel à des versions standards de Linux, nos clients bénéficient de mises à jour automatisées* » précise **Mathieu Blanc**.

RÉPONDRE AUX PICS DE CHARGE

Codéin adresse un grand nombre de cas d'usage, et gère l'hébergement et / ou l'infogérance de tout type de sites web même si le développement et la maintenance sont confiés à une autre agence.

Il peut, par exemple, héberger un site d'e-commerce à forte croissance ou aux importants pics de charge. Le groupe Sandaya est confronté à ce double enjeu. Ce réseau européen de campings 4 et 5 étoiles a fait le choix d'une politique intensive d'acquisitions tout en devant gérer la nature cyclique de son activité.

Parmi les autres références clients de Codéin, on peut citer l'Organisme Professionnel de Prévention du Bâtiment et des Travaux Publics (OPPBTP), la Fédération Française de Golf, CCI France, le groupe Delabie ou la startup Valobat.

> **Codéin peut contractuellement s'engager sur des garanties de temps d'intervention (GTI) ou de temps de rétablissement (GTR).**

Fondée par quatre ingénieurs issus de grandes ESN du marché, Codéin a réalisé 1,7 million d'euros de chiffre d'affaires en 2021. Basée à Montpellier et Strasbourg, la société emploie 28 collaborateurs dont la moitié sont certifiés Ibexa DXP, une plateforme d'expérience numérique modulaire.

Agence Codéin
www.codein.fr
contact@codein.fr
09 72 42 26 03

Kuzzle : UNE PLATEFORME AS-A-SERVICE QUI FACILITE L'UTILISATION DES APPLICATIONS IoT

Kuzzle, startup montpelliéraine, pousse les entreprises françaises à passer à l'action ! Comment ? Tout simplement avec sa nouvelle offre Kuzzle PaaS, qui est une plateforme as-a-Service dédiée à l'IoT, en service Cloud et sans engagement. Décryptage avec Jacques Le Conte, CEO de Kuzzle

Un petit mot sur l'entreprise ?

Créé en 2016, Kuzzle est un éditeur de logiciel Open Source pour l'Internet des Objets et le traitement massif temps-réel des données de l'IoT.

Conçue et développée par des ingénieurs français, la plateforme Kuzzle IoT accélère le déploiement d'applications de supervision temps réel et de pilotage pour la Smart City, le Smart Building, la Smart Industrie, la Smart Logistique et la Santé Connectée.

Kuzzle IoT est aujourd'hui adoptée et déployée par de grands groupes industriels tels que Bouygues, Eiffage, Veolia, Geodis, SNCF, La Poste, ou par des collectivités telles que la ville de Noisy-le-Grand ou les communes du Finistère.

Kuzzle PaaS est une plateforme as-a-Service dédiée à IoT, en service Cloud sans engagement.

Promodag

Promodag Reports pour Office 365 & Exchange

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

Mise en conformité avec les règles de l'entreprise

Planification simplifiée des processus de gestion

Interopérabilité avec les Systèmes RH

Optimisation des performances de la messagerie

Audit & planification de l'utilisation des e-mails

Rapports d'analyse de trafic, suivi des messages

Droit à la déconnexion et RGPD

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

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

www.promodag.fr • info@promodag.com

Pouvez-vous évoquer l'actualité, notamment avec le lancement Kuzzle Paas ?

Kuzzle PaaS est une plateforme as-a-Service dédiée à IoT, en service Cloud sans engagement, disponible depuis le mois de juin 2022. Cette offre « low code » reprend les fondamentaux de notre solution installable « on-premise », mais cette fois, activable en ligne à la demande pour tous ceux qui souhaitent déployer rapidement une application IoT sans avoir à investir dans une infrastructure technique. Les utilisateurs peuvent ainsi activer en ligne la puissance d'une plateforme Kuzzle IoT sans perdre de temps à la mise en route de leur projet et pourront désormais se concentrer pleinement sur leur cas d'usage métier.

Cette offre en ligne intègre nativement tout un ensemble de services IoT sur-mesure sur une seule et même plateforme IoT et permet de couvrir les principaux cas d'usages : gestion et monitoring des objets connectés, géolocalisation et géorepérage, configuration des règles métier, programmation des alertes, planificateur de tâches détaillées, gestion optimisée multi tenant ou encore création de rapports et de tableaux de bord avec des séries de données temporelles ou des vues cartographiques.

Kuzzle IoT est agnostique et interopérable, compatible multi-devices, multi-réseaux et multi-protocoles.

La solution en ligne « as-a-Service » peut être migrée à tout moment vers son Système d'Information existant avec une ré-installation « On-premise » sur les serveurs ou datacenters de l'entreprise, ce qui donne le contrôle total aux DSI et aux utilisateurs sur leurs services IoT et leurs données. Kuzzle IoT est agnostique et interopérable, compatible multi-devices, multi-réseaux et multi-protocoles ; le code étant entièrement ouvert en Open-Source. Une bonne façon d'accompagner le passage à l'échelle des projets IoT, bien au-delà du stade de preuve de concept (PoC) ou de preuve de valeur (PoV) des nouveaux services IoT.

Les entreprises françaises affichent un retard en matière d'IoT. Avec cette nouvelle offre, Kuzzle entend faciliter la mise en œuvre et l'utilisation des applications IoT? de quelle manière ?

Rappelons que l'Internet of Things (IoT) désigne les réseaux, les capteurs, les logiciels ou toute autre technologie embarquée collectrice de données d'objets connectés. Ce qui englobe aussi bien les appareils domestiques que les équipements industriels les plus complexes, soit plus de 13 milliards de terminaux IoT connectés à ce jour en France. Les entreprises françaises affichent un relatif retard en la matière, puisqu'elles sont 22 % à utiliser ces technologies contre 29 % en moyenne dans les autres grands pays de l'Union européenne. C'est pour inciter les entreprises françaises à passer à l'action, que nous avons lancé « Kuzzle PaaS ».

JACQUES LE CONTE

Notre plateforme as-a-Service est destinée à faciliter la mise en œuvre et l'utilisation des applications IoT. Elle vient compléter la version « installable » déjà disponible en Open-Source, afin de rendre la solution toujours plus accessible et pratique. Hébergée sur le Cloud français, elle constitue par ailleurs une alternative européenne aux géants américains du secteur, garantissant la souveraineté numérique et des données de nos entreprises nationales.

Avec notre offre PaaS, nous franchissons une nouvelle étape de notre stratégie, qui consiste à proposer une solution accessible au plus grand nombre et qui soit la plus complète et facile à utiliser. Nous continuerons à faire évoluer notre plateforme pour la rendre toujours plus performante, intuitive, intelligente et utile à nos clients.

> Par Sabine Terrey

Assises de la Sécurité 2022 :
L'INNOVATION AU SERVICE DE LA CYBERSÉCURITÉ

Dans un contexte de bouleversements économiques, sociaux, géopolitiques, climatiques, et pour faire face aux défis cyber, les Assises de la Sécurité 2022 reviennent en force du 12 au 15 octobre 2022 à Monaco. Entretien avec Florence Puybareau, Directrice de la Communication et des Contenus, DG Consultants

LA 22 LES ASSISES

« Cette édition 2022 va être une très belle édition, entre les invités, les partenaires, les experts, nous attendons 2600 participants sur les trois jours ». Un chiffre en hausse. Sans parler du *Before*, qui, année après année, s'impose comme le rendez-vous stratégique pour les décideurs du marché de la cybersécurité.

La cyber, sujet d'actualité depuis déjà longtemps, le devient de plus en plus, avec des défis à relever pour toutes les entreprises, et une mise en lumière de la mission des RSSI. « *Nous avons eu beaucoup de demandes du côté utilisateurs et fournisseurs, il y a effectivement un très fort besoin de trouver des solutions innovantes, d'échanger avec ses pairs, et de rencontrer des experts* ».

Des plénières inspirantes

Pour la conférence d'ouverture, outre l'allocution du Ministre d'Etat de la principauté de Monaco, « *on bouscule cette première plénière avec un représentant de l'OTAN qui évoquera la problématique géopolitique de la cybersécurité* ». Une analyse pertinente cyber géopolitique très attendue !

Citons la conférence, « Agir dans l'incertitude » avec Alain Bernard, double champion olympique de natation et Guillaume Schutz, pilote de chasse embarqué sur porte-avion, qui montreront que l'incertitude peut être un levier d'action.

Les nouveautés !

Le village Startup s'agrandit, « *il double en taille et en volume, la cybersécurité est particulièrement dynamique au sein des startups, notamment en France* ». Ces startups présentent l'innovation cyber d'aujourd'hui et de demain.

L'espace Meet-up se déploie ! « *En 2021, nous avions testé quelques meet up, petits ateliers pédagogiques emmenés par des RSSI. En 2022, au vu de leur succès, nous renouvelons, et 6 sujets seront abordés au sein de l'espace Meet up. Le contenu s'adapte ainsi à chaque invité, en fonction de son niveau et de sa maturité cyber* ». Les RSSI sont aux manettes !

FLORENCE PUYBAREAU

Un vent nouveau souffle sur les Keynotes, « *puisqu'après deux ans très particuliers en raison de la pandémie, les patrons US de plusieurs entreprises, SentinelOne, Darktrace, Cybereason retrouvent le sol européen et reviennent sur les Assises pour l'édition 2022* ». La Keynote « OVH, le leader du Cloud européen et souverain » avec Michel Paulin, Directeur Général OVH Cloud est attendue au regard « *des nombreuses discussions sur les stratégies Cloud actuellement* ».

Les Tables Rondes Experts

Avec des sujets percutants, savamment choisis pour répondre aux grandes problématiques actuelles! Pour ces 12 tables rondes, citons *Comment la/le RSSI doit-elle/il se former aux softskills ?* ou *La cyber assurance, quelles alternatives ? ou La sécurité des environnements industriels SI, OT/OI, La carence des talents, comment accélérer ?*

Challenges et perspectives
SUR LA GESTION DES VULNÉRABILITÉS EN ENTREPRISE

La gestion des vulnérabilités en entreprise demeure une pratique épineuse, sujet de tensions récurrentes entre les équipes du CISO et les équipes de production. Néanmoins, il s'agit sans conteste d'un des domaines les plus importants de la Cybersécurité. Les entreprises doivent connaitre leur stock de vulnérabilités, les prioriser et les corriger. L'objectif de ce dossier est de vous donner les pistes permettant d'améliorer cette pratique au sein de votre organisation.

Définition de la vulnérabilité

Comme souvent dans le monde de la Cybersécurité, il existe plusieurs définitions de la notion de vulnérabilité.

Selon la norme ISO 27005, une vulnérabilité est une « *faille dans un actif ou dans une mesure de sécurité qui peut être exploitée par une menace* » - Source : https://tinyurl.com/2s4bs8ju

Selon le NIST il s'agit d'une « faiblesse d'un système d'information, des procédures de sécurité du système, des contrôles internes ou de la mise en œuvre qui pourrait être exploitée ou déclenchée par une source de menace. » - Source : https://tinyurl.com/2p9ascze

Dans le cadre de cet article, je tenterai de donner une définition plus pragmatique pour le défenseur Cyber : « Toute CVE (Common Vulnerabilities and Exposures) non patchée ou mauvaise configuration permettant à un attaquant d'exécuter un chemin d'attaque afin d'exercer une action malicieuse au sein du système d'information ».

En effet, je rappelle ici qu'il n'existe finalement que deux moyens « d'attaquer » un système, quel qu'il soit : exploiter une CVE non patchée ou exploiter une mauvaise configuration du dit système. Ceci est applicable à toutes les composantes du système d'information : un PC sous Windows, un firewall, un téléphone IP, un annuaire, un code, etc.

Dans la suite de cet article, nous traiterons des vulnérabilités de type CVE, à savoir les failles identifiables sur les systèmes sur lesquels nous pouvons appliquer un patch pour corriger la faille. Nous ne traiterons pas ici de la partie mauvaise configuration, qui nécessiterait une encyclopédie à elle toute seule !

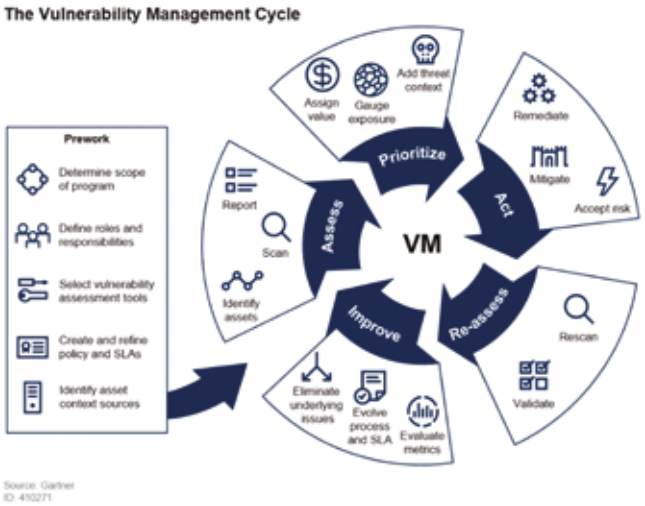
Un besoin de normalisation dans la pratique

Depuis environ une vingtaine d'années, la pratique de gestion des vulnérabilités (Vulnerability Management) s'est répandue dans la plupart des organisations souhaitant prendre en compte le risque Cyber et protéger leurs actifs des attaques. Depuis cinq ans, l'explosion des attaques par Ransomware a remis dans la lumière cette activité, car elle représente le socle fondateur pour se protéger des Malwares en tout genre.

Un travail de fond des analystes et des organismes

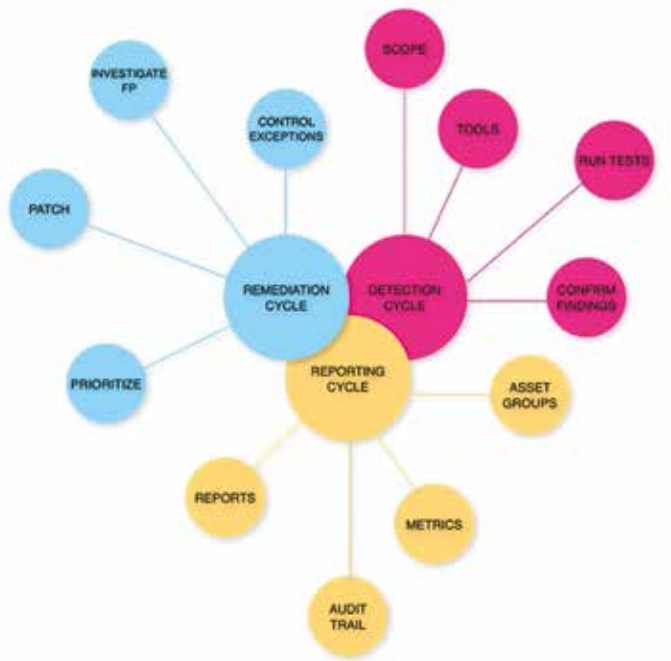
Il est notable de constater que la plupart des analystes du domaine IT se sont emparés du sujet

en proposant différents modèles permettant de formaliser la démarche en entreprise, par exemple le Gartner a publié une mise à jour de son « Vulnerability Management Guidance Framework » et a créé une série de documents décrivant la pratique, extrêmement intéressants à lire et à appliquer.



Gartner Vulnerability Management Cycle – Source: https://blogs.gartner.com/augusto-barros/2019/10/25/new-vulnerability-management-guidance-framework/

De son côté, l'OWASP publie et maintient à jour un guide de bonnes pratiques accessible sur Github : https://tinyurl.com/4up2cchu en se concentrant sur trois étapes essentielles du cycle : détection, reporting et remédiation. Ce modèle a l'avantage d'être très pragmatique et permet d'aller à l'essentiel, il est approprié pour les organisations peu matures sur le sujet.



OWASP Vulnerability Management Cycle – Source: https://owasp.org/www-project-vulnerability-management-guide/

Vous comprenez donc qu'il existe une multitude de modèles, accompagnés de leur lot d'avantages et d'inconvénients. La pratique a beau être ancienne, elle a toujours besoin de normalisation et d'évolution. La raison principale est que beaucoup de praticiens tentent d'appliquer les diverses méthodologies de gestion des risques pour modéliser leur pratique de gestion des vulnérabilités.

Gestion des risques VS Gestion des vulnérabilités

Il est important à ce stade d'expliquer quelques termes et de dissocier la gestion des risques et la gestion des vulnérabilités. Il est en effet frappant de constater deux situations extrêmement courantes :

- Beaucoup d'organisations souhaitent appliquer des méthodologies de gestion des risques à la gestion des vulnérabilités - cela peut paraitre naturel, et pour être honnête, c'est que j'ai tenté de faire également au début de ma carrière – néanmoins je considère maintenant que les pures méthodologies de gestion des risques sont difficilement transposables pour gérer efficacement les vulnérabilités.
- Il existe une multitude de termes employés, parfois à tort, dans de nombreux modèles et documents (même dans les documents officiels des organismes de normalisation !) – certains termes sont considérés par certains comme interchangeables, d'autres praticiens tentent d'utiliser les termes dans un seul contexte précis essayant d'éviter la confusion - il est donc extrêmement compliqué de s'orienter dans la jungle des différents acronymes et documents, surtout lorsque l'on tente de les comparer.

Il est important de dissocier la gestion des risques et la gestion des vulnérabilités.

Les éléments suivants sont basés sur ma propre interprétation, je ne considère pas qu'il s'agisse d'une vérité gravée dans le marbre - il s'agit plutôt du fruit de mon expérience, elle-même basée sur de la concaténation de dizaines de documents et sur l'observation de la pratique dans diverses organisations.

Voici un résumé des termes utilisés dans le cadre de la pratique de gestion des risques :

Pour le coup, la plupart des ressources documentant le sujet utilisent à priori les mêmes termes, la raison est simple, la pratique de gestion des risques existe depuis plusieurs millénaires (au sens propre) et

les praticiens ont eu le temps de s'accorder sur les termes à employer et sur leurs définitions.

Voici les termes que j'utilise dans le cadre de la gestion des vulnérabilités :

Le diable se cachant dans les détails, une nouvelle variable est apparue dans la formule, la Sévérité. Pour faire simple, chaque CVE possède un score de sévérité intrinsèque, que l'on peut évaluer, l'idée est ici d'intégrer cette variable dans le calcul du risque lié à une vulnérabilité de type CVE. Mais comme nous le verrons plus loin dans cet article, la « chose » est un peu plus compliquée que cela... De plus certains praticiens remplacent le produit Probabilité par Sévérité par le concept de Criticité. Je dois bien avouer que je suis quelque peu réticent à utiliser ce terme - autant le concept de Sévérité me parait pertinent à intégrer dans le calcul, autant la notion de Criticité est pour le coup utilisée de différentes manières selon les usages, je préfère donc ne pas y faire référence afin de gagner en cohérence.

Retenez finalement que si vous tentez de comparer la littérature de gestion des risques à celle traitant des vulnérabilités, vous rencontrerez de grandes difficultés à relier les termes utilisés dans les deux pratiques, simplement parce que leur sens profond est interprété différemment par les praticiens de ces deux disciplines.

Mesure de la sévérité d'une CVE : CVSS

Les CVEs sont donc des vulnérabilités présentes sur les systèmes, elles sont référencées selon une codification, pour faire simple chaque CVE possède un numéro unique qui lui est attribué lors de sa découverte (c'est un peu plus compliqué que cela, mais restons simples). Voici un exemple avec la CVE CVE-2022-22321 :

CVE-2022-22321 Detail – Source: https://nvd.nist.gov/vuln/detail/CVE-2022-22321

Dans cet exemple, la CVE a été publiée le 03/01/2022, c'est IBM Corporation qui a fourni les informations et son score est de 5.5 selon CVSS 3.1.

La base de données des CVEs se nomme la NVD (National Vulnerability Database), elle est gérée et maintenue par un organisme gouvernemental Américain nommé NIST (National Institute of Standards and Technology) et elle est accessible en ligne ici : https://nvd.nist.gov/

Pointons ici du doigt un paradoxe intéressant : alors que la problématique de gestion et de normalisation des CVEs est un enjeu mondial, l'organisme responsable du maintien de la base de données de référence est de fait réalisé par un organisme financé par le gouvernement Américain. Pourtant, « tout le monde » utilise cette base de données et la considère comme un « standard de fait ».

Afin de catégoriser la Sévérité d'une CVE, le NIST utilise la notation CVSS (Common Vulnerability Scoring System), la dernière version de ce modèle de catégorisation étant la 3.1. En effet, comme l'indique l'organisme FIRST (Forum of Incident Response and Security Teams) responsable du maintien de la documentation CVSS, le score CVSS mesure une sévérité et non pas un risque :

Source: https://www.first.org/cvss/v3-1/cvss-v31-user-guide_r1.pdf

Ce point est très important, le score CVSS ne mesure que la sévérité, pas la probabilité, pas l'impact et encore moins le risque. Néanmoins, comme nous le découvrirons plus loin dans cet article, le score CVSS peut fournir des recommandations pour mesurer les autres attributs, permettant finalement de se rapprocher d'une méthode classique d'évaluation du risque.

Le score CVSS attribué à une CVE s'étend sur une échelle de 0 à 10, plus le nombre est élevé, plus la sévérité est importante. Il est admis que si le score CVSS est supérieur à 7, alors la CVE est considérée comme critique, et doit donc par projection être patchée immédiatement. Comme nous le verrons plus loin dans cet article, le score CVSS a le mérite de fournir un cadre normatif mais ne permet qu'une approximation pour décider de la priorité des actions dans le cadre de la remédiation.

Pour information, le site cvedetails.com fournit des informations intéressantes concernant la répartition des scores CVSS sur l'ensemble des CVEs connues, soit au jour du 08/09/2022, 184 286 CVEs référencées !

DIB

Accélérateur de votre transformation numérique

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

Digital Workplace

Infrastructures & Réseau

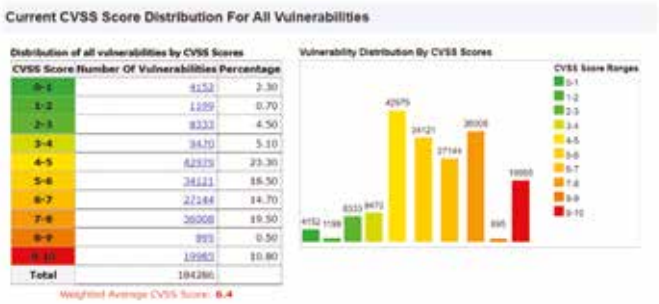
Sécurité & Stockage

Services Cloud Managés

Hewlett Packard Enterprise

www.dib-france.fr

Tél : 01 34 57 90 00



Source: https://www.cvedetails.com/

Structure du score CVSS

Comme indiqué précédemment, le score CVSS mesure la sévérité d'une CVE, dans l'objectif de prioriser les actions de remédiation. Mais il faut bien comprendre que le score CVSS global est en fait la combinaison de trois scores différents :

- **Le CVSS Base Score :** pour faire simple, il s'agit d'une caractérisation de la CVE elle-même, sans tenir compte de l'usage réel de cette CVE par les groupes d'attaquants ou de l'impact de cette CVE au sein de l'organisation. Les puristes souligneront qu'une partie du Base Score prend en compte l'impact, ce qui est vrai, mais je veux ici rester simple. Le NIST fournit donc des attributs liés à la CVE, et surtout les valeurs qui vont avec.
- **Le CVSS Temporal Score :** cette partie du Score Global prend en compte la menace réelle sous le prisme de l'exploitabilité de la CVE. Par exemple, est ce que les groupes d'attaquants utilisent réellement cette CVE, existe-t-il une preuve de l'usage de cette CVE, un code permettant effectivement d'utiliser cette CVE a-t-il été publié sur Github, etc. Il est primordial de comprendre que le NIST définit les attributs importants à suivre, mais ne fournit pas les valeurs associées, ce qui est normal puisque ces valeurs ne peuvent être fournies que par des flux de CTI (Cyber Threat Intelligence) complémentaires.

Le score CVSS ne mesure que la sévérité, pas la probabilité, pas l'impact et encore moins le risque.

- **Le CVSS Environmental Score :** il s'agit ici de prendre en compte le contexte de l'organisation afin de pondérer la menace réelle : Quels sont les critères de sécurité de l'organisation, quel est l'impact potentiel de la CVE en termes de confidentialité, intégrité et disponibilité, etc. A nouveau, le NIST définit les attributs importants à suivre, mais ne fournit pas les valeurs associées, l'organisation devra par exemple réaliser une étude de risque pour alimenter ces attributs.

Composantes du score CVSS

Pour comprendre comment le score global évolue en fonction des différentes valeurs d'attribut, le NIST propose une calculatrice en ligne accessible ici : https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator

Cet outil est très utile aux débutants afin de comprendre la structure et les équations permettant le calcul du score CVSS.

La menace liée aux CVEs est grandissante

Lorsque l'on consulte les données existantes liées aux CVEs, deux éléments sautent aux yeux immédiatement :

- **Chaque année, le nombre de CVEs découvertes augmente :** Je ne parle pas ici du nombre cumulé de CVEs qui bien sûr augmente mécaniquement chaque année, mais du nombre de CVEs que les chercheurs découvrent année après année : 4653 CVEs découvertes en 2010, 7939 CVEs découvertes en 2014, 18325 CVEs découvertes en 2020, etc.

Le score CVSS global est en fait la combinaison de trois scores différents.

- **Le nombre représentant les CVEs cumulés ne suit pas une droite mais une fonction exponentielle...** De plus les vulnérabilités les plus anciennes sont toujours les plus exploitées, il y a deux ans, plus de 80% des cyberattaques recensées utilisaient une vulnérabilité publiée avant 2017 et plus de 20% de ces attaques exploitaient même une vulnérabilité connue depuis plus de 7 ans.

Nombres des CVEs cumulées au fil des ans

A la lecture de ces indicateurs, il apparait donc évident que les organisations voient la charge de travail liée à la gestion des vulnérabilités exploser et que seule la priorisation de la remédiation peut leur permettre de gérer cette situation. Historiquement, elles s'appuient sur CVSS pour définir les priorités, malheureusement, ceci n'est plus possible aujourd'hui pour les raisons que nous allons expliquer dans le prochain chapitre.

L'enjeu majeur du traitement des vulnérabilités réside dans la priorisation de la remédiation.

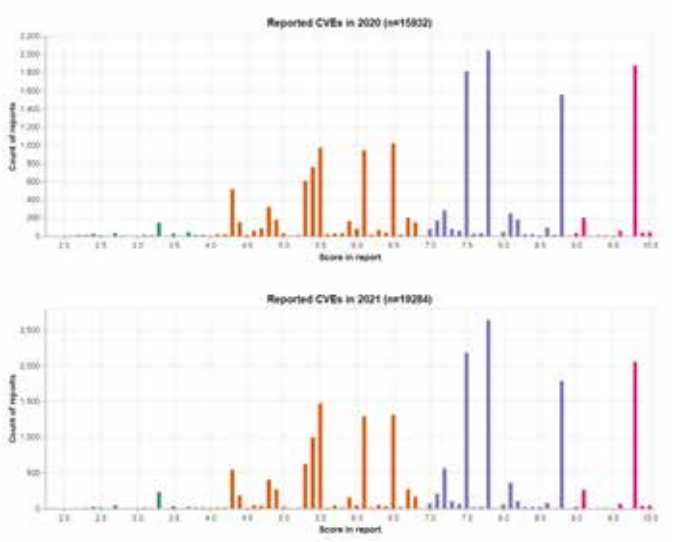
Les limites de CVSS

Si je devais me rappeler mes cours de mathématiques de l'université, je dirais que CVSS est nécessaire mais non suffisant. La pratique nous enseigne que CVSS possède de nombreux avantages : attributs normalisés, possibilités d'intégrer des concepts liés à la menace réelle et à l'organisation si on possède les sources de données adéquates, etc. Néanmoins la grande limitation de CVSS provient de son incapacité réelle à aider les organisations à la priorisation de la remédiation, c'est-à-dire définir quels sont les systèmes et CVEs à patcher en priorité pour éviter qu'une attaque ne survienne. Nous allons utiliser deux exemples pour illustrer ce fait.

Il existe trop de CVEs avec un score Critique via CVSS

La notation CVSS existe depuis une vingtaine d'années, au début de l'utilisation de cette notation l'ensemble des scores attribués aux CVEs découvertes chaque année était équilibré, au sens où il y avait une répartition des scores plus ou moins équivalente sur l'échelle allant de 0 à 10 – Globalement, il y avait donc autant de CVEs avec un score de 4.5 que de CVEs avec un score de 8. Depuis une petite dizaine d'années, un déséquilibre s'est progressivement créé sur la répartition des scores - quand on consulte les scores des trois dernières années, on se rend compte que 2/3 des scores sont supérieurs à 6.5. Cette accélération vers des scores élevés nous amène à la situation suivante : Si l'on fait la moyenne de tous les scores CVSS attribués depuis vingt ans, 1/3 des scores sont supérieurs à 7 et sont donc considérés comme critiques !

Voici deux graphiques illustrant parfaitement cette tendance de surreprésentation des scores élevés sur les deux dernières années :



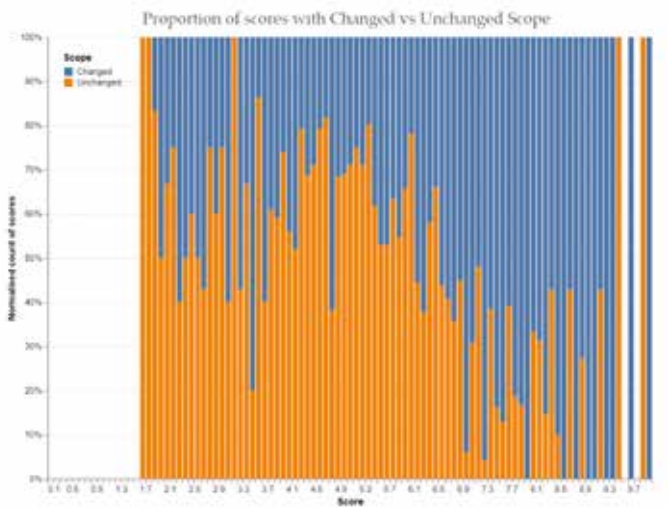
Source: https://theoryof.predictable.software/articles/a-closer-look-at-cvss-scores/

Conclusion : Du fait de la surreprésentation des scores élevés, il n'est plus possible d'utiliser CVSS pour assurer la priorisation de la remédiation.

Sans les composantes Temporal et Environmental le score CVSS est difficilement exploitable pour qualifier le risque.

Certains attributs CVSS possèdent un poids trop important dans l'algorithme

Lorsque l'on étudie l'algorithme de calcul du score CVSS afin d'appréhender la logique de notation, il apparait que certains attributs possèdent un poids surélevé dans le résultat du calcul. Par exemple, l'attribut Scope représente d'une certaine façon l'étendue de la vulnérabilité, si le Scope possède la valeur « Changed » cela signifie que la vulnérabilité peut impacter le système sur l'ensemble de ses sous-composants, si la valeur est égale à « Unchanged » les composants affectés sont limités au périmètre strict de la CVE. Bien évidemment, il s'agit d'un critère important pour évaluer le score CVSS que l'on attribue à une CVE donnée, mais lorsque nous regardons en détail il s'avère que la valeur « Changed » de l'attribut Scope est très largement surreprésentée dans les scores CVSS supérieurs à 7, donc considérés comme critiques. Le graphique suivant illustre la répartition des valeurs de l'attribut Scope en fonction du score global CVSS :



Source: https://theoryof.predictable.software/articles/a-closer-look-at-cvss-scores/

Conclusion : L'algorithme de calcul du score CVSS est déséquilibré et ne pondère pas efficacement les valeurs des différents attributs.

Stratégie pour une priorisation efficace

Comme vous l'avez compris, l'enjeu majeur du traitement des vulnérabilités réside dans la priorisation de la remédiation. Les équipes de production ne peuvent pas patcher l'ensemble des CVEs dont le score CVSS est supérieur à 7, surtout que les nouvelles CVEs découvertes sont en moyenne utilisées par les attaquants 48 heures après leur publication.

Première piste : utiliser les attributs CVSS du Temporal Score et de l'Environmental Score

Comme indiqué précédemment, le NIST fournit les valeurs accompagnant les attributs du Base Score mais ne fournit pas les valeurs pour le Temporal Score et l'Environmental Score – Pour ces deux derniers scores le NIST ne fournit que la liste des attributs importants à considérer dans le score global.

L'organisation devra donc s'abonner à des flux de CTI pour renseigner les valeurs reliées à la menace réelle (Temporal). Afin de qualifier l'impact réel de la menace dans le contexte de l'organisation (Environmental), elle devra ingérer les données provenant d'une CMDB (Configuration Management DataBase) ainsi que les données provenant d'une étude de risque.

Il est clair que sans les composantes Temporal et Environmental le score CVSS est difficilement exploitable pour qualifier le risque.

Deuxième piste : utiliser un algorithme complémentaire

Nous avons décrit plus haut les limites de l'algorithme CVSS, certaines organisations complètent le score CVSS par des algorithmes complémentaires permettant de qualifier le risque et non pas simplement la sévérité d'une CVE.

Parmi les algorithmes complémentaires, nous pouvons citer le SPR (Security Posture Rating) proposé par la société Vulcan mais celui-ci ne permet d'alimenter le score que via les valeurs présentes dans une CMDB et donc compléter les informations liées à l'impact (Environmental) – Il existe également le TRS (True Risk Score) développé par la société Hackuity qui a l'avantage d'intégrer les valeurs liées à la menace via des flux de CTI (Temporal) ainsi que les valeurs provenant de CMDBs et d'études de risques afin de qualifier l'impact réel (Environmental).

De plus, le NIST travaille activement sur une nouvelle version de CVSS, la version 4.0 – Cette nouvelle version permettra une mise à jour de l'algorithme de calcul mais ne fournira pas les valeurs associées à la menace ou à l'impact.

Troisième piste : renforcer l'automatisation

Classiquement, la pratique de gestion des vulnérabilités est une activité hautement manuelle. En effet, il est très complexe d'automatiser le déploiement de patchs sur des serveurs de production, l'impact potentiel d'un patch doit être vérifié manuellement pour assurer la continuité de service des applications importantes pour le business.

Le volume de CVEs à patcher ne cessant d'augmenter, il devient indispensable de relier les informations collectées par les scanners de vulnérabilités avec les outils de gestion de tickets (ITSM) et de permettre ainsi un échange de données bidirectionnel entre ces deux outillages. En clair, les scanners de vulnérabilités doivent alimenter la création de tickets décrivant les patchs à déployer en priorité, après application du patch le système de gestion de tickets doit pouvoir renvoyer l'information dans la base de données décrivant le stock de vulnérabilités pour indiquer que le déploiement du patch a été réalisé.

Ce lien structurant nécessite généralement un développement spécifique ou l'implémentation d'un outil dédié.

Quatrième piste : améliorer la coordination entre les équipes

Historiquement, un minimum de deux équipes différentes sont parties prenantes du cycle de gestion des vulnérabilités. Généralement les scanners de vulnérabilités sont gérés par les équipes sécurité du RSSI, de manière à obtenir une vue claire du stock de CVEs de l'organisation. Ensuite les équipes sécurité créent des tickets dans le système ITSM, ils sont attribués aux équipes de production. Ce sont classiquement les équipes de production qui déploient les patchs sur les systèmes car celles-

ci maitrisent parfaitement les différentes machines présentes dans l'organisation et sont responsables du maintien des bonnes conditions opérationnelles.

Il devient indispensable de casser les silos entre ces deux équipes et d'utiliser les outils et processus permettant d'améliorer la coordination entre tiers. Cette évolution n'est pas le seul fait d'outils supplémentaires mais nécessite une réorganisation des méthodes de travail.

Cinquième piste : intégrer les informations liées aux Pentest et au Bug Bounty

Lorsque l'on évoque la gestion des vulnérabilités on pense immédiatement aux informations présentes dans les résultats des scanners de vulnérabilités. Evidemment il s'agit d'un élément primordial, de plus, les données présentes dans ces outils ont l'avantage d'être structurées (du moins au sein d'un même éditeur !). Mais il existe un autre référentiel utile décrivant les vulnérabilités et leur exploitation réelle, il s'agit des rapports de Pentest et de Bug Bounty.

De nombreuses organisations commencent à alimenter leur cycle avec les informations présentes dans ces rapports, permettant ainsi de mieux qualifier le risque réel. Le problème est que ces rapports ne sont pas tous structurés de la même manière et demandent à être adaptés pour une gestion efficace au sein du référentiel.

Néanmoins, si l'effort de normalisation est effectué, ceci représente une avancée majeure dans le traitement des vulnérabilités.

Il existe un autre référentiel utile décrivant les vulnérabilités et leur exploitation réelle : des rapports de Pentest et de Bug Bounty.

Les ressources complémentaires pour bien appréhender la pratique

Voici une liste de ressources complémentaires qui vous permettront d'explorer en profondeur la pratique de gestion des vulnérabilités.

- Mon précédent article sur ITPro traitant de la gestion de la surface d'attaque : https://tinyurl.com/2p9ea9j3
- Le site de la National Vulnerability Database : https://nvd.nist.gov/
- La calculatrice en ligne du score CVSS : https://tinyurl.com/2bb62hxm
- Le document du FIRST décrivant les spécifications officielles du score CVSS : https://www.first.org/cvss/v3.1/specification-document
- Le site CVE Details fournissant des statistiques sur les CVEs : https://www.cvedetails.com/

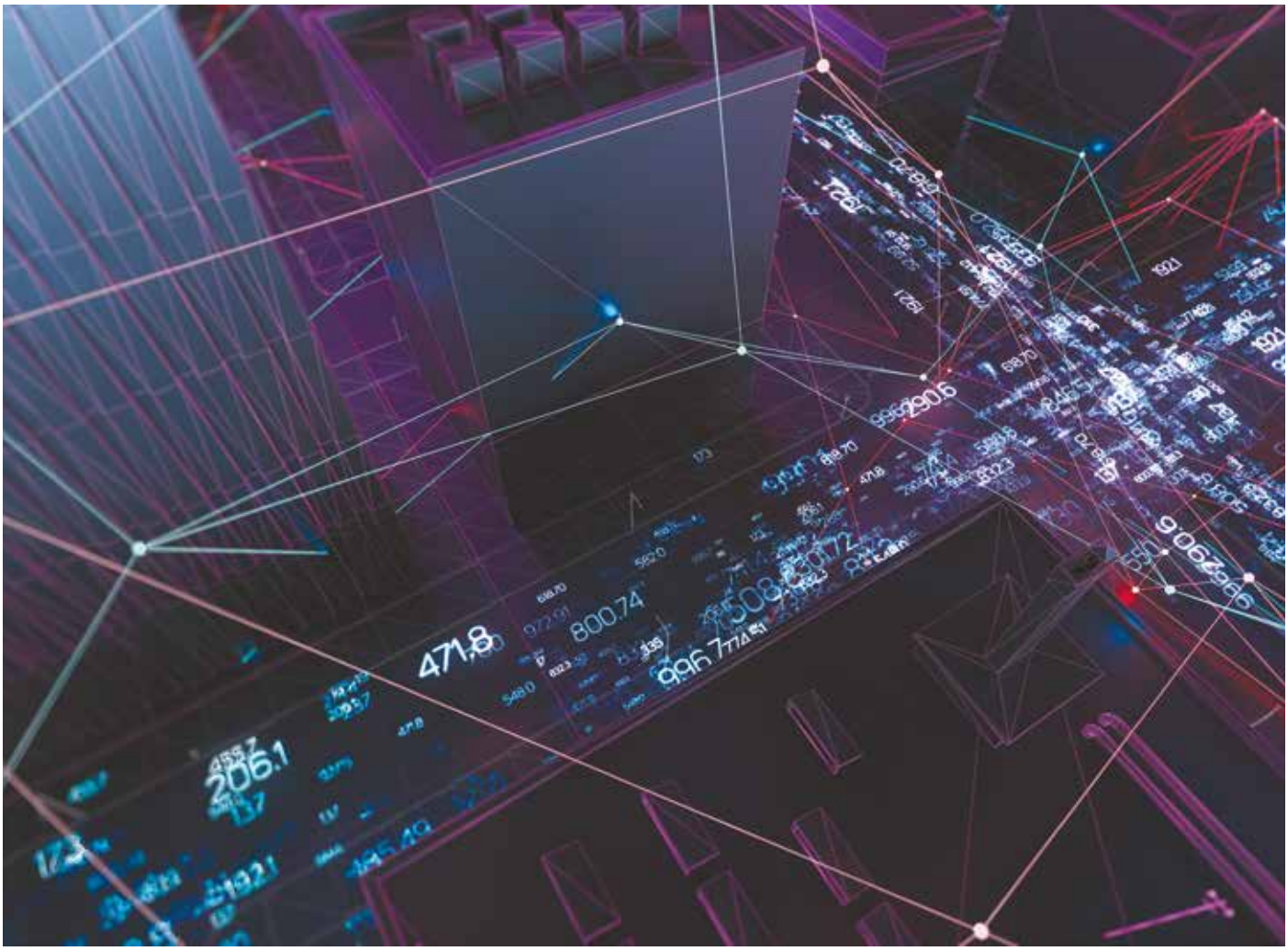
J'espère sincèrement que cet article vous aura éclairé sur la pratique de gestion des vulnérabilités et que vous avez pu trouver des pistes concrètes pour améliorer la gestion des risques au sein de votre organisation. Bien évidement votre réflexion ne doit pas s'arrêter à cet article, vous devrez chercher et comprendre par vous-même de nombreux concepts afin d'améliorer votre niveau de sécurité global.

N'hésitez pas à me suivre sur Linkedin ou à me contacter directement afin de poursuivre la conversation.

Sylvain Cortes – Microsoft MVP
Linkedin : https://www.linkedin.com/in/sylvaincortes/
sylvaincortes@hotmail.com

Azure Chaos, LE CHOIX DE LA PANNE

La crainte de la panne est une réalité pour grand nombre d'entreprise. La question est toujours la même : Mais que va-t-il se passer si telle ou telle ressource présente une panne ? Jamais facile de répondre à cette question.



Pas que les choses soient mal ou non préparées, mais plutôt qu'il n'est jamais facile de simuler une panne et encore moins un ensemble de pannes. Et pas plus facile de trouver le temps et la manière de la provoquer pour voir si tout se déroule comme cela devrait se dérouler. Et ce même sur des opérations simples comme les tests de charge ou de performance.

Il est pourtant indiscutable que le test est un élément clef pour le SI. Il est préférable d'avoir une bonne vue d'ensemble de ce qu'il va se passer en cas de dysfonctionnements et a minima d'avoir une vision claire de ce que cela peut entrainer comme indisponibilité.

Attention, l'indisponibilité d'un système ou son fonctionnement en mode dégradé n'est pas toujours synonyme de catastrophe. C'est seulement lors des simulations que l'on pourra décider de ce qui demande plus de protection (résilience, redondance...etc) et ce qui est éventuellement acceptable. Se passer temporairement d'une application ou d'un service n'est pas toujours une hérésie. Dépenser sans compter pour augmenter la fiabilité n'est pas forcément la meilleure solution. Investir 10 pour ne pas perdre 5, une bonne idée ? Pas vraiment ou pas toujours à mon avis !

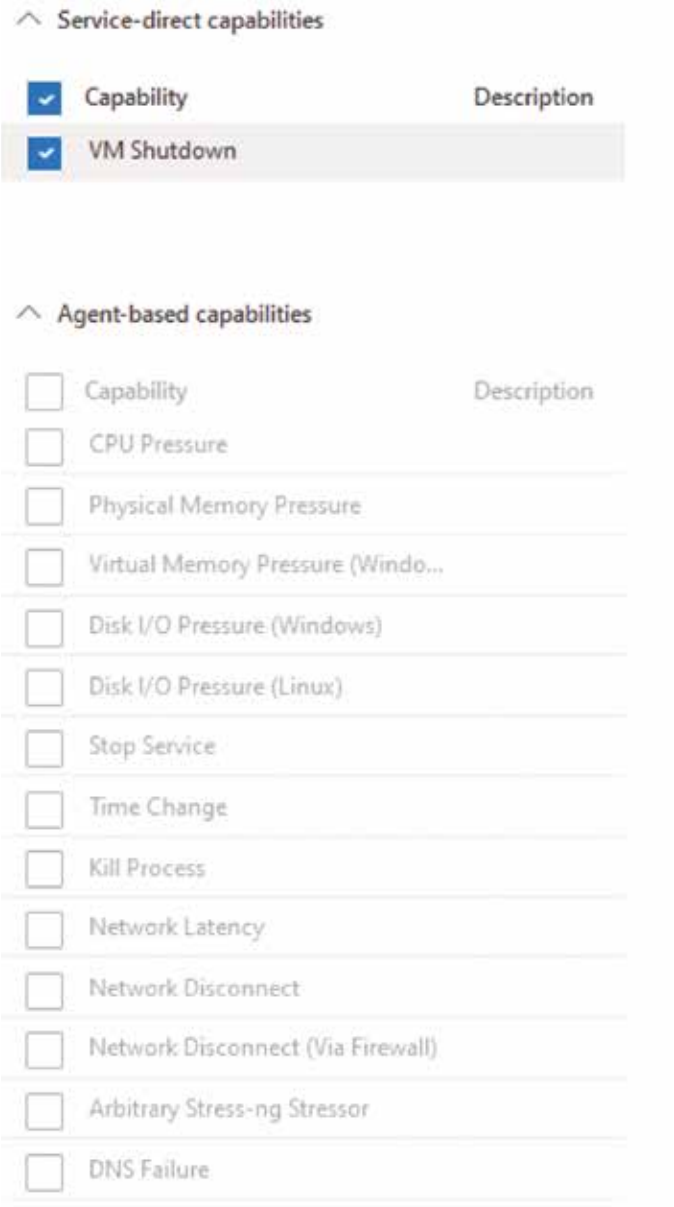
Avant de prendre la bonne décision, encore faut-il voir (simuler) ce que peut entrainer la défaillance d'un service ou d'un ensemble de services. Depuis peu, Microsoft a ajouté la fonctionnalité Azure Chaos dans le portail Azure. Elle permet de réaliser assez simplement ce genre d'opérations.

Du chaos dans le studio

Chaos Studio est un concepteur de simulation de chaos. Une console de création de scénarios de pannes ou d'indisponibilités. Cette fonctionnalité est en préversion et seules quelques régions sont pour l'instant éligibles. Pour l'Europe, North Europe et West Europe. France Central n'est pas encore déployée mais annoncée.

Présentation par l'exemple et avec quelques images de cette nouvelle possibilité.

La première opération est le choix d'une cible sur laquelle vont être simulées les pannes. Soit au travers d'un service-direct (sans agent) pour l'ensemble des ressources soit au travers d'un agent pour les ressources de type VM et VMSS (Set de machines virtuelles). Premier point, même si le service-direct est possible sur les VM, ce n'est pas le meilleur choix. Son champ d'action est restreint et présente peu d'intérêt. La liste des possibilités de simulation est bien plus importante avec l'agent comme présenté sur l'écran suivant :



Liste avec et sans agent, les possibilités sont étendues avec l'agent.

Une fois la ressource ajoutée en tant que cible, elle est éligible aux tests de pannes. Une ressource qui n'a pas été déclarée comme cible ne sera pas disponible dans la console et ne pourra être rattachée à une expérience de chaos.

Le studio est ensuite utilisé en mode expérience appelée *Chaos Studio | Experiments*. C'est ici que vont être empilées les actions. Des pannes ou des délais (*Fault* ou *Delay* dans le concepteur).

Avant d'ajouter les erreurs, il faudra parcourir la documentation éditeur que l'on retrouve dans une page « Bibliothèque d'erreurs et d'actions Chaos Studio » directement sur internet. Cette phase de documentation est indispensable. Certains tests n'ont besoin d'aucun prérequis, d'autres nécessitent l'installation d'un utilitaire complémentaire. Par exemple, l'action « Sollicitation de la mémoire physique » sur une machine Linux demande l'installation du package *Stress-ng*. Il n'y aura aucun prérequis pour ce même test sur une machine Windows. Il y a donc une phase d'étude préparatoire avant de bénéficier de l'ensemble des possibilités. Et une phase de déploiement d'outils complémentaires.

Puis viennent ensuite les paramètres de valeur des tests. Ce peut être un stress mémoire avec une sollicitation à 99%, du stress disque, un arrêt de process, une panne DNS ou même une latence ou une déconnexion réseau.

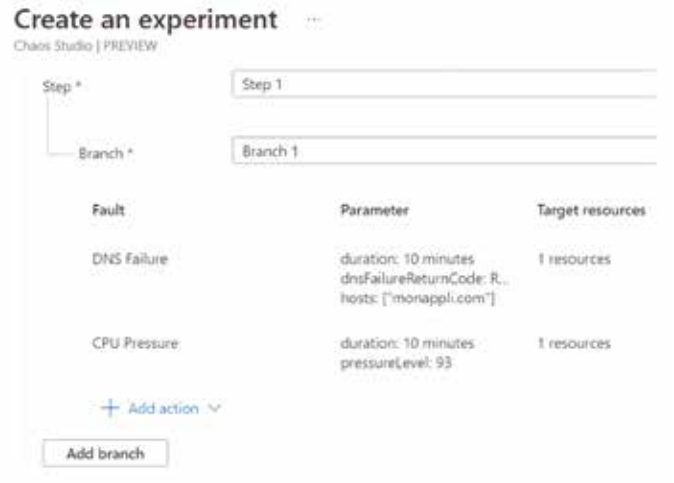
De la performance donc, avec des pics de charge, mais également de la panne. Dans le détail, on voit dans le tableau suivant que les paramètres sont assez fins en termes de valeur. Ici, pour un stress sur différents modèles de disques Azure.

Modes de pression

PressureMode	Description
PremiumStorageP10IOPS	numberOfThreads = 1 randomBlockSizeInKB = 64 randomSeed = 10 numberOfIOperThread = 25 sizeOfBlocksInKB = 8 sizeOfWriteBufferInKB = 64 fileSizeInGB = 2 percentOfWriteActions = 50
PremiumStorageP10Throttling	numberOfThreads = 2 randomBlockSizeInKB = 64 randomSeed = 10 numberOfIOperThread = 25 sizeOfBlocksInKB = 64 sizeOfWriteBufferInKB = 64 fileSizeInGB = 1 percentOfWriteActions = 50
PremiumStorageP50IOPS	numberOfThreads = 32 randomBlockSizeInKB = 64

Vue détaillée pour un test disque.

Cette phase préparatoire validée, les agents et outils installés, il ne reste qu'à créer une expérience. C'est-à-dire une suite d'actions et de pannes. Et choisir pour chaque faute la valeur des paramètres. Une durée pour une latence, un pourcentage pour un pic de charge, une non - réponse pour un service.



L'expérience, une suite de panne et de dysfonctionnement.

Il reste quelques étapes comme la création d'une identité qui aura les droits suffisants pour réaliser les opérations mais l'essentiel est là. Les différentes expériences sont réutilisables en modifiant les cibles (les ressources) qui sont à tester.

Présentée dans ce sujet sur une ressource de type machine virtuelle, la solution est bien plus complète et les ressources concernées sont variées.

De la machine virtuelle comme ce qui a été fait ci-dessus, de la base de données, de l'AKS... Etc. De quoi tirer de nombreux enseignements sur ce qu'entrainerait une panne sur un environnement Azure !

Les différentes expériences sont réutilisables en modifiant les cibles (les ressources) qui sont à tester.

En Synthèse : un bon point de départ en 3 étapes

1 / Le studio Chaos est un simulateur de pannes pour les ressources Azure.

2 / La solution est utilisable avec ou sans agent.

3 / Les différents point de panne sont détaillés dans le document « Bibliothèque d'erreurs et d'actions Chaos Studio ».

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

Insight IDC

Le nouveau lieu de travail:

Redefinir où comment et pourquoi nous travaillons

SCAN ME

Télécharger l'étude

Cohesity : UNE FORTE CYBER-RÉSILIENCE AU SERVICE DE TOUTES LES ENTREPRISES

Cohesity, fournisseur de solutions Cloud, de gestion et de protection des données, a été nommé « leader » et « ouperformer » pour la protection des données dans le Cloud hybride selon deux rapports GigaOm Radars. Un très belle performance ! Retour sur le sujet avec Tony Fanni, Senior Channel System Engineer chez Cohesity.

Un mot sur Cohesity ?

Cohesity est donc une plateforme logicielle unique et évolutive capable de couvrir différents cas d'usage (sauvegarde, NAS, archivage, cible de stockage). Elle a été reconnue leader dans son secteur par les cabinets d'analyse Gartner et GigaOm, et récemment a été nommée au classement Forbes 2022 Cloud 100.

Quant aux points clés de la solution qui la différencie, on peut citer une accélération des décisions grâce à l'IA, un accès à une Marketplace de solutions (Helios), une sécurité Zero Trust, une forte Cyber-résilience, prévention contre tout type de menaces, le data management, une simplicité pour « scale », une extensibilité aux parties tierces

C'est une solution intelligente qui, pour simplifier l'expérience utilisateur, et sans limites d'évolutivité, propose sein d'une même interface des services de BU, réplication, archivage, stockage NAS, stockages objets, isolation de données, détections d'anomalies, le tout en mode « on premise » ou SaaS.

Cohesity est donc reconnu pour sa protection des données dans le Cloud hybride pour les grandes entreprises mais aussi pour les PME. Alors que retenir des fonctionnalités clé ?

Effectivement, deux rapports, le *GigaOm Radar for Hybrid Cloud Data Protection : Large Enterprises,* et *le GigaOm Radar for Hybrid Cloud Data Protection : Small and Medium-Sized Enterprises* ont plébiscité la solution pour la protection des données dans le Cloud hybride, à la fois pour les grandes entreprises et les PME.

Que retenir ? on peut évoquer plusieurs éléments, la réduction des risques business (snapshots immuables, Multi factor authentification, Quorum, scan virus intégré), le contrôle des impacts liés aux attaques (détections des anomalies basées sur IA, notifications et alertes en temps réels via une application mobile), une réponse rapide aux incidents assurée (audit, comparaison granulaire AD, identification des failles de sécurités avant le processus de restauration), mais aussi la réduction du temps d'arrêt et de perte des données : « Instant Recovery to Scale » – pas d'arrêts de service sur les différents workload, et une visibilité globale plus détaillée (sur les objets sources affectés, recherche des données compromises).

Cohesity est également perçue comme « avant-gardiste dans la protection des données sur le cloud hybride, offrant une approche véritablement futuriste sur le marché ». Qu'est-ce que cela signifie précisément ? Qu'est-ce qui fait sa valeur ajoutée ?

On ne peut parler de ce côté avant-gardiste sans évoquer Cohesity DataGovern. Il s'agit d'un service de sécurité et de gouvernance des données qui utilise l'IA/ML pour automatiser la découverte de données sensibles et détecter les modèles d'accès et d'utilisation anormaux qui pourraient indiquer une cyberattaque en cours. En quelque sorte, c'est la clé pour contrecarrer les mauvais acteurs qui tentent d'exfiltrer ou de voler des données. Il est disponible dès maintenant pour un aperçu en accès anticipé.

Autre élément stratégique des mois à venir. Le déploiement du Project Fort Knox. C'est un service d'isolation et de récupération des données qui permettra aux clients de conserver une copie inviolable de leurs données dans un coffre-fort géré par Cohesity afin d'améliorer la résilience des données face aux attaques de ransomwares. En plus de l'immuabilité, cela offre aux clients un autre moyen de contrecarrer les attaquants qui tentent de chiffrer les données. Il est prévu pour un aperçu en accès anticipé dans les prochains trimestres.

TONY FANNI

Enfin, nous continuons de développer activement l'écosystème partenaires puisque nous avons annoncé un partenariat stratégique avec Rackspace, visant à fournir des solutions de sauvegarde et de restauration gérées multicloud aux clients de Rackspace Technology dans le monde entier.

> Par Sabine Terrey

En plus de l'immuabilité, cela offre aux clients un autre moyen de contrecarrer les attaquants qui tentent de chiffrer les données.

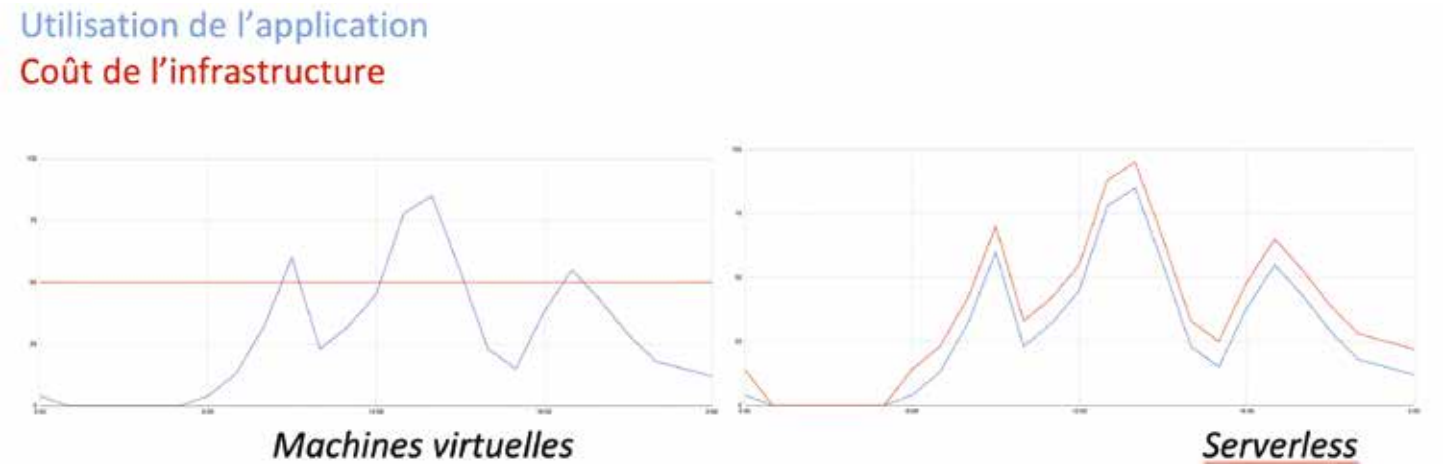
QUELS SONT LES RÉELS ATOUTS DU Serverless ?

Le serverless a le vent en poupe. Son marché devrait atteindre 21,9 milliards de dollars d'ici 2025 (selon Allied Market Research). Le serverless est une catégorie de service mise à disposition par les fournisseurs de serveur pour lesquels ce dernier abstrait entièrement les ressources physiques nécessaires (serveurs, réseau, stockage) à l'exécution d'une charge de travail.

Le Serverless, un ensemble de services spécialisés facturés à l'utilisation

Une infrastructure classique se compose traditionnellement d'un ensemble de serveurs ou machines virtuelles louées pour une période de temps moyennant un coût récurrent fixe, quelle que soit la charge des serveurs.

L'offre serverless des cloud providers tels qu'AWS, Azure ou Google Cloud vient casser ce modèle d'infrastructure, en proposant un ensemble de services spécialisés, managés, visant à remplacer les fonctions les plus courantes d'un serveur web, et facturés à l'usage. L'infrastructure sous-jacente et sa maintenance (mise à jour et de runtime pour patcher les vulnérabilités, gestion de l'espace disque disponible, sécurisation des accès) devient ainsi l'entière responsabilité du fournisseur de serveur.



LE DROIT À LA DÉCONNEXION : UN ENJEU RH

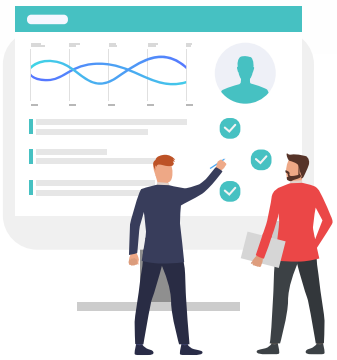
DANS UN MONDE RÉGI PAR L'IMMÉDIATETÉ,
LA DÉCONNEXION N'EST PLUS UNE OPTION, MAIS UN DROIT.

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

Ces services se scindent en 2 grandes catégories :

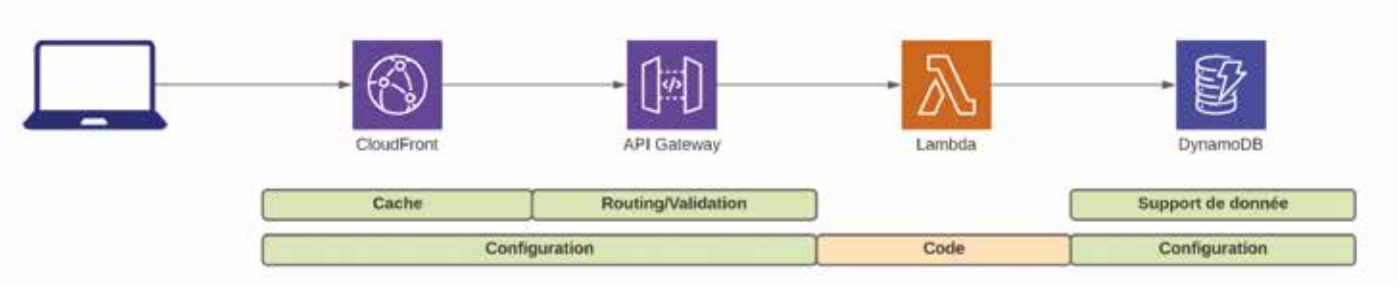
- les services FaaS, ou Fonction as a Service, responsables d'exécuter du code métier propre au business de l'application, en réponse à des évènements spécifiques (requête HTTP, fichier uploadé, utilisateur authentifié...)

- les services BaaS, ou Backend as a Service, responsables de réaliser des tâches spécifiques habituellement portées par des fonctionnalités de framework, comme le routing, l'authentification ou le stockage de fichier et qui peuvent servir d'événements déclenchant pour les FaaS.

Fonctionnant de concert pour réduire le code base

Désigner une architecture serverless, c'est combiner les bons services au bon moment et les faire interagir pour construire une application complète en écrivant seulement les lignes de code relatives à son métier, celles qui apportent le plus de valeur. Plus de code pour gérer le routing, le cache, la validation, la gestion d'erreur, l'authentification... On déporte la responsabilité du développeur d'implémenter ces fonctions supports (sans erreur) à un ensemble de services dédiés, spécialisés, maintenus et scalables.

Chez un cloud provider comme AWS, on utilisera par exemple CloudFront pour porter les certificats HTTPS d'une application web, et gérer le cache. Ce dernier sera configuré pour transférer les requêtes HTTP faites à CloudFront vers API Gateway, services de routing, de validation et d'autorisation si utilisé conjointement avec Cognito. Enfin, une Lambda contenant la logique métier propre à l'application sera invoquée par API Gateway, elle-même se reposant par exemple sur DynamoDB comme base de données.



Le Serverless, pour développer une application à faible TCO, scalable automatiquement

Le TCO (pour Total Cost of Ownership) désigne l'ensemble des coûts liés, dans notre cas, au développement d'un produit tout au long de sa durée de vie. En la matière, le paradigme serverless a du coup plusieurs avantages :

- le **coût** est calculé à l'utilisation (le nombre de requêtes HTTP API Gateway, le nombre de secondes d'exécution de Lambda). Sans utilisateur, aucune dépense.

- l'architecture est **scalable** par essence. Aucune intervention en amont d'un pic de charge prévu n'est nécessaire. C'est la responsabilité du cloud provider de s'assurer que suffisamment de ressources physiques de calcul soient disponibles pour que chaque service puisse répondre à la demande de l'ensemble de ses clients. Cette gestion nous est complètement abstraite et ne nécessite aucune configuration.

- les services sont **sécurisés** et mettent en place les bonnes pratiques nécessaires à la réduction des surfaces d'attaque d'architecture plus classique (chiffrage au repos des données, rotation des clés de chiffrement, gestion des accès aux API de provisioning et d'utilisation de chaque service en refus par défaut, permission granulaire pour chaque service). Cette sécurisation est mise en place par défaut et ne génère pas de coûts supplémentaires.

- Les **déploiements sont rapides et ciblés**. Aucune raison de mettre l'ensemble des configurations des services à jour. Le déploiement est entièrement automatisé, et laissé à la responsabilité de services dédiés, comme CloudFormation chez AWS.

Désigner une architecture serverless, c'est combiner les bons services au bon moment et les faire interagir pour construire une application complète.

FRÉDÉRIC BARTHELET

- Les compétences requises pour maintenir des applications serverless ne demandent plus une équipe dédiée ops, mais **une équipe de développement sensibilisée à des sujets d'ops**. Les développeurs configurent eux-mêmes les différents services, et sont garants de l'optimisation de leur utilisation pour réaliser telle ou telle fonctionnalité. Il n'y a plus de frontière entre infrastructure et applicatif : chaque fonctionnalité de l'application nécessite d'écrire du code et de la configuration pour provisionner les services nécessaires à son fonctionnement.

Un paradigme mature, évoluant rapidement, avec des challenges à relever

L'utilisation en production permet d'avoir du recul sur le chemin qu'il reste à parcourir. La technologie, bien que jeune, est déjà suffisamment mature car portée par de grands acteurs cloud. Elle est prête pour une utilisation en production, comme les exemples d'iRobot, de la BBC ou encore de Netflix le prouvent . Les points durs restants portent sur :

L'utilisation en production permet d'avoir du recul sur le chemin qu'il reste à parcourir.

- **l'observabilité** qui est rendue plus ardue par l'utilisation d'une architecture distribuée sur plusieurs services à chaque interaction d'un utilisateur sur une application. Certains services de monitoring comme Epsagon ou Lumigo se sont spécialisés dans la récupération des logs de chacun de ces services pour permettre de reconstruire l'enchaînement complet d'évènements et permettre ainsi de diagnostiquer plus rapidement des bugs.
- la non-coopération des différents cloud providers pour mettre en place un **catalogue unifié agnostique** pour réduire les problèmes de *vendor lock-in*. L'intégration profonde de service spécialisé dans un paradigme serverless rend toute migration plus importante que dans des paradigmes d'hébergement par machine virtuelle. Chaque migration d'un cloud à un autre, même dans un architecture plus classique représente toujours un coût important (migration de base de données, de système de gestion d'accès)
- **l'outillage** des équipes de développement, très différent de ce à quoi les développeurs sont accoutumés (en retirant entièrement le concept d'environnement de développement local virtualisé avec des outils comme Docker ou Vagrant). Le serverless nécessite un travail de **formation** important pour permettre aux équipes d'avoir une connaissance suffisante des différents services du catalogue serverless d'un cloud provider. Le cycle de développement et la maintenance de ce genre d'architecture nécessite également un accompagnement.

L'approche serverless démontre son efficacité et permet en particulier d'améliorer la capacité de production d'une équipe de développement, de livrer un produit en production plus rapidement.

Nous accompagnons nos clients pour les faire monter en compétences sur le serverless en intégrant nos experts directement avec leurs équipes de développement et en faisant de la formation notre priorité pour leur permettre une totale autonomie dans cet écosystème. Nous contribuons énormément à la communauté open-source pour rendre le serverless plus accessible et démocratiser son usage, et tous les avantages qui en découlent.

Par Frédéric Barthelet, responsable de l'unité Serverless chez Theodo

ANAPLAN RELÈVE AVEC BRIO LES DÉFIS DE LA SUPPLY CHAIN DURABLE

Volonté d'acheter des produits plus durables, de voir se déployer de plus grands efforts en matière d'approvisionnement et de production... les souhaits s'expriment plus clairement et rapidement. Et s'il était temps justement d'avoir une supply chain plus durable ? Comment les responsables de la supply chain peuvent-ils prendre en compte la durabilité dans les opérations ?

Anaplan, solution de planification, de gestion et optimisation de la supply chain pour les petites et grandes entreprises, évolue avec les nouveaux challenges de la supply chain. Entretien avec Brice Faure, DG d'Anaplan EMEA.

Pourriez-vous présenter Anaplan en quelques mots et évoquer une actualité récente ?

Anaplan est une plateforme collaborative de planification et de gestion, basée sur le cloud, qui permet l'optimisation de toutes les fonctions métiers d'une entreprise – de la finance à la supply chain en passant par le marketing, les ventes et les RH.

Les entreprises que nous accompagnons peuvent modéliser des scénarios d'hypothèses, piloter leur performance, prévoir les futures tendances et élaborer des budgets et des plans à partir de données internes de l'entreprise corrélées à des données externes. Ces données sont mises à jour automatiquement en temps réel pour refléter l'évolution des besoins de l'entreprise et de son environnement économique.

Et s'il était temps justement d'avoir une supply chain plus durable ?

LA 22

LES ASSISES

12.10.22 →→ 15.10.22

/MONACO///

→ Plus qu'un événement,
une référence, un incontournable

→ lesassisesdelacybersecurite.com

DG CONSULTANTS

COMEXPOSIUM

BRICE FAURE

Notre solution de prévision intelligente - PlanIQ - permet notamment aux clients d'exploiter l'intelligence artificielle pour créer des prévisions précises et fiables, ce qui apparaît essentiel pour faire face aux événements imprévus, tels que des événements climatiques, dont en ressortent des données extrêmement volatiles.

Nous avons, par ailleurs introduit notre nouveau moteur de calcul Anaplan Polaris™ afin que les clients français puissent tirer parti d'encore plus de puissance au sein de la plateforme Anaplan pour modéliser, analyser et résoudre les complexités qui ont un impact sur leurs opérations - des problèmes d'approvisionnement à la hausse de l'inflation.

Anaplan Polaris a la puissance et l'échelle nécessaires pour calculer les nombreuses différentes dimensions d'une grande entreprise mondiale, même celles qui dépassent les 10 millions de trillions de cellules.

Entrons dans le sujet de la supply chain durable. Comment les responsables de la supply chain peuvent-ils s'assurer que les opérations s'alignent sur les objectifs de durabilité ?

En matière de supply chain, Anaplan utilise l'informatique hyperscale pour la planification de l'offre, de la demande, du plan industriel et commercial (PIC ou S&OP). La plateforme permet de garder le contrôle avec des décisions basées sur la valeur et d'adapter les plans pour optimiser les marges et les profits. La supply chain se voit donc modélisée de façon intelligente.

Notre solution de prévision intelligente permet aux clients d'exploiter l'intelligence artificielle pour créer des prévisions précises et fiables.

Nous aidons les entreprises à briser les silos opérationnels en facilitant les échanges et le travail collaboratif des différents utilisateurs et départements en leur offrant une vue partagée des données internes et externes. Cette visibilité de chacun sur les principaux composants de la chaîne de valeur est essentielle pour garantir que les décisions commerciales ne soient pas prises à la légère, notamment en matière environnementale.

Quels conseils donneriez-vous aux dirigeants pour s'engager précisément sur cette voie de la durabilité ?

Les consommateurs orientent désormais leur pouvoir d'achat vers des produits plus durables, en choisissant des articles de marques qui mettent en avant leurs efforts en matière d'approvisionnement et de production durables.

Il faut aussi se demander si le produit est fabriqué de manière durable, ou encore si la méthode de livraison au consommateur est respectueuse.

Par conséquent, les responsables de la Supply Chain doivent réfléchir à la manière d'adapter leurs processus pour répondre à l'évolution des besoins. Pour avoir une Supply Chain durable, il ne suffit plus de considérer les fournisseurs que vous avez à bord, mais il faut aussi se demander si le produit est fabriqué de manière durable, ou encore si la méthode de livraison au consommateur est respectueuse. Plus les consommateurs auront une visibilité sur ce parcours, plus les entreprises auront des relations et des expériences clients améliorées.

> Par Sabine Terrey

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

Quatre piliers
DE LA FABRICATION INTELLIGENTE

Le secteur manufacturier a toujours évolué selon un rythme lent et naturel qui s'étalait sur des décennies, en réponse aux changements d'époque qui ont modifié progressivement les besoins de l'industrie. Toutefois, ces deux dernières années ont bouleversé ce rythme d'évolution naturel. Des vagues spectaculaires de baisses et de pics de la demande sont survenues, alors que le monde entrait et sortait de confinements à répétition, rendant ainsi les chaînes d'approvisionnement très imprévisibles. De ces turbulences, les fabricants ont appris que le numérique est essentiel. Selon une récente étude, les fabricants B2B européens qui accélèrent leur digitalisation vont investir jusqu'à 20 % de plus dans les initiatives digitales en 2022 par rapport à l'année dernière.
Bala Amavasai, Global Technical Director, Databricks, partage son expertise.

Ce fort engagement vers la numérisation ouvre la voie à l'émergence de la « fabrication intelligente ». Il s'agit principalement d'une fabrication qui fait appel à l'Internet des objets (IoT), au cloud computing, à l'analytique et au machine learning (ML) pour optimiser la façon dont les entreprises utilisent leurs actifs, en mettant l'accent sur le Retour sur Capitaux Investis (ROIC). Tout cela induit l'augmentation des compétences du personnel et l'introduction de nouveaux niveaux de connectivité pour accélérer les performances. Au cœur de tous ces changements, les fabricants sont confrontés à quatre grands défis. Toutefois, s'ils sont relevés de la bonne façon, ces défis peuvent aussi devenir les piliers d'une transformation positive.

BALA AMAVASAI

- 1 -
Combler les lacunes en matière de compétences et de production

L'essor de l'économie numérique exige un nouvel ensemble de compétences. Les cas d'usage de la fabrication intelligente entraînent une forte demande en programmeurs et techniciens en robotique, experts en cybersécurité, experts en jumeaux numériques, analystes de réseaux d'approvisionnement et personnels capables d'exploiter la data science et les algorithmes de ML. Cela signifie que l'industrie est confrontée à des défis concernant à la fois la formation et la rétention du personnel. Aux États-Unis, une étude de Deloitte révèle que si aucune solution n'est trouvée, le déficit de compétences dans le secteur manufacturier laissera plus de deux millions d'emplois vacants au cours de la prochaine décennie.

L'une des façons de relever ce défi mondial est d'améliorer les compétences des effectifs actifs et de les recycler dans les technologies émergentes essentielles à l'industrie manufacturière, telles que les systèmes collaboratifs et les outils d'automatisation avancés, plutôt que de compter uniquement sur l'arrivée de nouveaux candidats déjà formés aux nouvelles compétences requises. De nombreuses compétences des équipes en place peuvent aussi être mises à profit dans ces cas d'usage émergents. Également, les technologies open source peuvent aider les fabricants en quête de compétences à court terme, notamment en matière de données. En effet, l'esprit communautaire de l'open source permet aux entreprises de puiser dans un ensemble plus large de compétences et d'expertise basées sur la force de l'apprentissage entre pairs, ce qui allège la pression sur les équipes existantes.

- 2 -
Dompter la volatilité de la chaîne d'approvisionnement

Les effets de la pandémie ont démontré que les chaînes d'approvisionnement doivent être robustes, transparentes et résilientes. La capacité à monitorer, prévoir et réagir aux facteurs externes, tels que les catastrophes naturelles, les pénuries de matériaux et les contraintes d'expédition et de stockage, est essentielle pour réduire les risques et favoriser l'agilité. Cela dépend de la visibilité de bout en bout et à la minute près, basée sur les données, dont on dispose à toutes les étapes de la chaîne d'approvisionnement. Pourtant, de nombreuses entreprises manufacturières utilisent actuellement des architectures de données héritées complexes, telles que des data warehouses. Ces derniers se transforment souvent en silo d'informations, qui empêchent la facilité d'accès et de distribution des données. Ils sont aussi sources de données erronées qui contiennent des informations dupliquées ou périmées, susceptibles d'être partagées par inadvertance.

Un lakehouse supprime ainsi la complexité, fournit une meilleure visibilité sur les données et en facilite l'accès.

La mise en œuvre d'une architecture de données moderne et solide de type lakehouse réduit le nombre de plateformes requises. Un lakehouse supprime ainsi la complexité, fournit une meilleure visibilité sur les données et en facilite l'accès. Il permet de fournir des flux de données précises au moment opportun et de développer des cas d'usage basés sur l'IA et le ML, ce qui en fait une plateforme idéale pour produire des analyses et des informations détaillées en temps réel. Les fabricants peuvent ainsi prendre des décisions clés au fur et à mesure qu'ils reçoivent des informations, et ainsi répondre rapidement aux situations changeantes et par conséquent bien mieux faire face à la volatilité.

- 3 -
Générer de nouveaux revenus

La croissance du secteur manufacturier s'est historiquement limitée au taux de réussite du lancement de nouveaux produits ou à l'expansion dans de nouvelles zones géographiques. L'émergence de l'EaaS (Equipement-as-a-service) modifie toutefois cette dynamique. Si cette approche n'est pas nouvelle (le modèle de souscription au moteur "Power-by-the-Hour" de Rolls-Royce existe depuis 1962), elle apparaît comme un impératif pour cette industrie soumise à la demande des clients, aux progrès de l'IoT industriel et à la baisse

continue des ventes et des marges. En effet, l'EaaS offre un niveau de visibilité et de collaboration qui minimise les coûts de maintenance, les dépenses d'investissement et la gestion du capital humain.

A titre d'exemple, l'industrie aéronautique, et Rolls-Royce en particulier, utilisent des modèles basés sur le cloud non seulement pour réduire les coûts pour leurs clients, mais aussi pour créer de nouvelles sources de revenus. Rolls-Royce collecte des données générées en temps réel via la création de jumeaux numériques de ses moteurs. L'analyse de ces données basées sur l'IA et le ML repose sur l'architecture Lakehouse de Databricks. Les résultats obtenus permettent d'éviter l'immobilisation non planifiée d'avions au sol et de réduire de plusieurs millions de livres sterling le coût des pièces en stock. De plus, la plateforme de données étant dans le cloud, le fabricant ne paie que lorsqu'il exécute les modèles. Cela signifie que l'énergie n'est consommée que lorsqu'elle est nécessaire.

- 4 -
Gagner en durabilité

L'impact du changement climatique a entraîné une volatilité croissante des chaînes d'approvisionnement mondiales énormément perturbées par des conditions météorologiques extrêmes et des catastrophes naturelles. Les fabricants ne doivent donc pas se contenter de s'adapter, mais doivent être partie prenante dans la réduction de l'impact environnemental sur l'ensemble du secteur. La quête d'un développement plus durable implique de prendre en compte non seulement l'empreinte carbone de l'entreprise, mais également les émissions indirectes issues d'activités échappant à son contrôle et susceptibles de jouer un rôle essentiel.

Accroître la durabilité nécessite la refonte d'une chaîne d'approvisionnement circulaire. Cela exige une meilleure collaboration entre les fournisseurs et les éditeurs, l'optimisation des chaînes de production et du transport, et un plus grand engagement des clients pour prolonger le cycle de vie des produits. Où tout cela commence-t-il ? Par les données. Rassembler les données en un seul endroit, tel que dans un lakehouse, permet d'y accéder facilement et de les stocker pour des analyses et des cas d'usage basés sur l'IA et le ML. Cela fournit de la visibilité et de l'intelligence sur l'ensemble du réseau, ce qui permet aux fabricants de prendre des décisions clés pour gagner en efficacité. L'utilisation de logiciels open source est également essentiel pour un meilleur partage des données et une plus grande collaboration entre les fabricants, les fournisseurs et les éditeurs en amont et en aval de la chaîne d'approvisionnement.

Accroître la durabilité nécessite la refonte d'une chaîne d'approvisionnement circulaire.

Dans le monde d'aujourd'hui, les entreprises data-driven et AI-driven sont celles qui tirent leur épingle du jeu. Les fabricants qui adoptent des outils novateurs d'optimisation des processus et des produits sont en mesure de prévoir et de prendre le pouls de la demande de la chaîne d'approvisionnement. Et, plus important encore, ils peuvent créer de nouvelles formes de revenus basées sur les services plutôt que sur la seule vente de produits. Avec la bonne équipe à bord, les entreprises manufacturières qui choisissent de tirer parti des données et de l'IA bénéficient d'un modèle économique plus intelligent, plus flexible et plus compétitif que jamais.

CONGRÈS & CONFÉRENCES

CENTRE DE CONGRÈS RIVE MONTPARNASSE

Plus d'informations sur **www.metadays.fr**

METADAYS

SAVE THE DATE

LE PREMIER RENDEZ-VOUS B2B CONTENU & BUSINESS

DU MÉTAVERS EN FRANCE

29 30 NOVEMBRE 2022

500 PARTICIPANTS **80** SPEAKERS **40** PARTENAIRES **2** JOURS DE CONGRÈS

COMMENT GÉRER EFFICACEMENT vos équipes Teams

Le déploiement de la partie collaborative de Teams (canaux et partages de fichiers) s'avère relativement aisé, comparé aux défis que posent la partie téléphonie d'entreprise et plus généralement la qualité des communications.

Seulement, beaucoup d'entreprises s'interrogent sur la gouvernance qu'il convient d'appliquer vis-à-vis de ces espaces de travail. Faut-il les contrôler ? Doit-on mettre en place des stratégies afin de limiter certains usages ? Comment supprimer les équipes inactives ? Autant de questions qu'il vaut mieux se poser avant d'ouvrir le service.

Dans cet article, nous essaierons par conséquent de vous donner quelques pistes pour mieux gérer vos équipes Microsoft Teams et surtout ne pas être en face d'un environnement totalement incontrôlé voire anarchique.

Création ouverte des équipes Teams

Une des premières questions que vous devez vous poser est si vous allez laisser n'importe quel utilisateur pouvoir créer et paramétrer une équipe Teams. Car, par défaut, tous les utilisateurs ayant une licence Teams peuvent créer des équipes. Certaines entreprises choisissent ce mode de fonctionnement mais beaucoup en reviennent.

En effet, le risque de laisser n'importe qui pouvoir créer une équipe est de vous retrouver, plusieurs mois après, avec des milliers d'équipes dont la

plupart des propriétaires ont quitté l'entreprise ou ne gèrent plus du tout leur contenu. C'est également assumer le risque que ces données ou ces espaces de stockage puissent continuer à être exploités par des personnes extérieures ou invitées par l'entreprise sans que personne ne se soucie de ces accès.

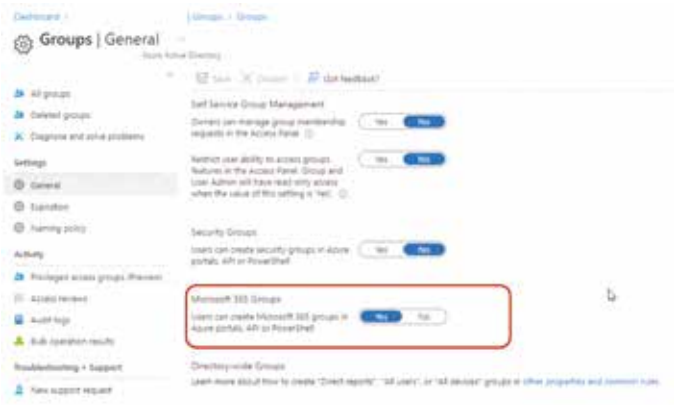
C'est aussi, risquer de vous retrouver avec des noms d'équipe comme : Pot_de_Depart_de_Gerard, MonEquipe_Laurent etc... Un peu comme à l'image de ces serveurs de fichiers, à qui on a laissé l'accès libre aux utilisateurs et qui au bout de quelques années, regorgent de données dont personne ne sait si elles sont encore utiles, sensibles et qui y a accès.

Laisser ouverte la création des équipes Teams, c'est permettre, selon les paramétrages en vigueur, aux utilisateurs de synchroniser leurs données personnelles sans véritable limite de stockage puis de les partager avec des tiers et ce sans que personne ne puisse réellement le contrôler.

C'est aussi permettre la création d'autant de « listes de distribution » dans l'environnement Exchange online que d'équipes. En effet, chaque équipe Teams (groupe Office 365) va posséder une adresse de messagerie de la sorte : Pot_de_Depart_de_Gerard 1d5c5900.montenant.fr@fr.teams.ms qui pourrait être utilisée de l'extérieur. Notez également que vos utilisateurs Exchange pourront de facto créer des groupes Office 365 depuis leurs Outlook Web Access.

Le risque est, par conséquent, de vous retrouver quelques mois après avec des milliers d'équipes totalement incontrôlées, avec des utilisateurs quelques peu désorientés, et des administrateurs du service relativement impuissants.

Vous l'avez compris, je ne suis pas un grand supporter de cette option, mais néanmoins elle existe. Pour fermer ou laisser ouverte la création des équipes à vos utilisateurs c'est extrêmement simple, il suffit d'autoriser la création des groupes Office 365 dans le portail de gestion de Azure AD comme le montre la figure suivante.



Autoriser ou non la création d'équipe à tout le monde

L'alternative à la mise en place de la création ouverte des équipes Teams, est de définir votre propre processus d'approbation via PowerApps. Pour plus d'informations, merci de vous reporter au lien suivant : https://www.sharepointnutsandbolts.com/2018/04/control-office-365-group-creation.html

Mettre en place des stratégies d'équipe

En dehors de la question d'ouvrir ou pas la création d'équipes, la première chose à faire est de mettre en place des stratégies d'équipes et surtout, de modifier la stratégie par défaut si vous laissez la création d'équipes ouverte. Ces stratégies d'équipes vont vous permettre de contrôler si vos utilisateurs pourront :

- **Créer au sein de leurs équipes des canaux privés.** En effet, les propriétaires d'équipes et les membres ayant une autorisation pourront créer des canaux privés pour un groupe spécifique d'utilisateurs dans l'organisation. Seules les personnes ajoutées au canal privé pourront par conséquent lire et écrire des messages.
- **Créer des canaux partagés.** Les propriétaires d'équipe pourront créer des canaux partagés pour les personnes à l'intérieur et à l'extérieur de votre organisation. Seules les personnes ajoutées au canal partagé pourront par conséquent lire et écrire des messages.
- **Inviter des utilisateurs externes à des canaux partagés.** En effet, si vos politiques de partage externe d'Azure AD sont configurées, les propriétaires d'un canal partagé pourront inviter des utilisateurs externes à rejoindre le canal. Notez que si le canal a été partagé avec un membre ou une équipe externe, ils continueront à avoir accès au canal, et ce même si le contrôle est désactivé par la suite.
- **Rejoindre des canaux partagés externes.** Si vos politiques de partage externe d'Azure AD sont configurées, vos utilisateurs et vos équipes pourront être invités à des canaux partagés externes. Si une équipe de votre organisation fait partie d'un canal partagé externe, les nouveaux membres de l'équipe auront accès au canal, et ce, même si le contrôle est désactivé a posteriori.

La première chose à faire est de mettre en place des stratégies d'équipes et surtout, de modifier la stratégie par défaut .

Pour modifier la stratégie des équipes rendez-vous dans le centre d'administration de Microsoft Teams comme le montre la figure suivante

Centre d'administration de Microsoft Teams - Stratégie d'équipe

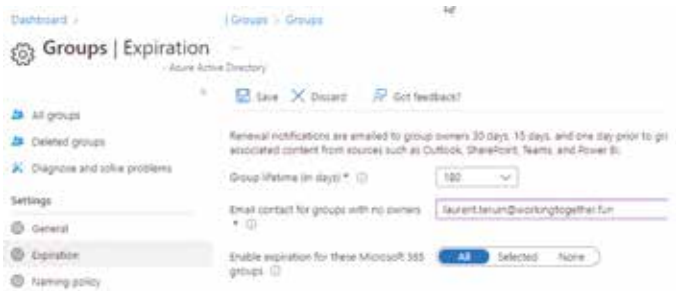
Durée de vie des équipes Teams

Une solution pour ne pas avoir à gérer des milliers d'équipes Microsoft Teams est de mettre en place une durée d'expiration. Cette option permet de fixer une durée de vie du groupe Office 365 donc des équipes Teams et de déclencher éventuellement sa suppression automatique.

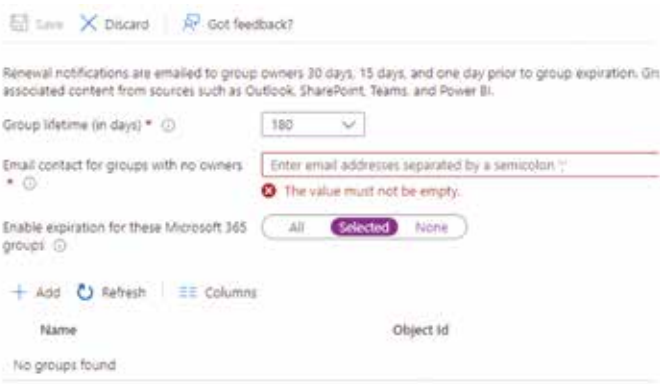
Une solution pour ne pas avoir à gérer des milliers d'équipes Microsoft Teams est de mettre en place une durée d'expiration.

Comment cela fonctionne-t-il ? Les administrateurs vont fixer une période d'expiration sur tous les groupes 0365. Les propriétaires du groupe recevront automatiquement une notification avant l'expiration, ce qui leur permettra de renouveler le groupe pour un autre intervalle d'expiration. La période d'expiration d'un groupe commence lorsque le groupe est créé ou depuis la date de son dernier renouvellement.

La figure suivante illustre ce paramétrage.



Un des problèmes lorsque vous laissez la création ouverte des équipes Teams est qu'il vous faudra positionner cette expiration de groupe pour tous les groupes Office 365. Or, pour certains groupes Office 365 générés par d'autres applications, il pourrait être souhaitable de ne pas mettre en place cette fonctionnalité. Une des solutions consiste donc à écrire un script PowerShell que vous devrez exécuter régulièrement et qui positionnera cette fonctionnalité uniquement pour les groupes Teams via l'option Selected comme le montre la figure suivante :



Expiration de la durée de vie de groupe 0365

CLOUD EXPO EUROPE PARIS 16 & 17 NOVEMBRE 2022, PARIS PORTE DE VERSAILLES.

PRÉ-INSCRIVEZ VOUS SUR : www.cloudexpoeurope.fr

Repensez les rouages de votre stratégie IT et trouvez les technologies adaptées à vos besoins et à votre organisation.

Cloud, DevOps, Cybersécurity Big Data, IA... toutes ces technologies s'imbriquent et se complètent ! Venir au salon c'est l'occasion unique de retrouver les experts de ces domaines sous un seul et même toit.

Un rendez-vous incontournable avec au programme des tables rondes passionnantes, des conférences spécialisées et des études de cas. Les meilleurs spécialistes et les leaders de l'industrie seront à vos côtés pour vous guider et vous inspirer dans cet univers toujours en mouvement.

Que vous soyez déjà spécialiste du cloud ou en pleine transformation digitale, manager d'une start up ou cadre d'une grande entreprise, le salon est l'allié de choix qui vous permettra d'affiner votre mécanique numérique !

Votre entrée gratuite vous donnera accès aux événements co-organisés : DevOps Live, Cloud & Cyber Security Expo, Big Data & AI World et Data Centre World.

CLOUD EXPO EUROPE

16-17 novembre 2022 Paris Porte de Versailles
www.cloudexpoeurope.fr

CO-ORGANISÉ AVEC

DEVOPS LIVE

CLOUD & CYBER SECURITY EXPO

BIG DATA & AI WORLD

DATA CENTRE WORLD

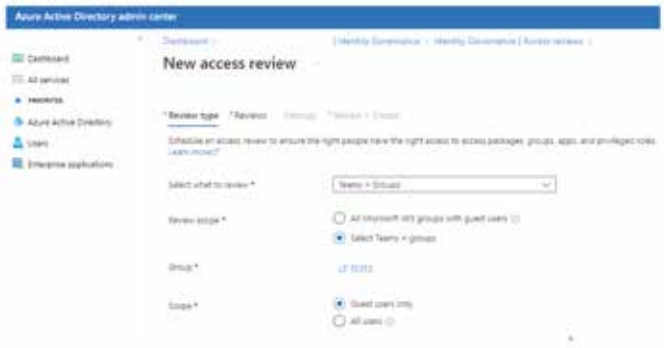
ORGANISÉ PAR

CloserStill

Mettre en place la revue des accès

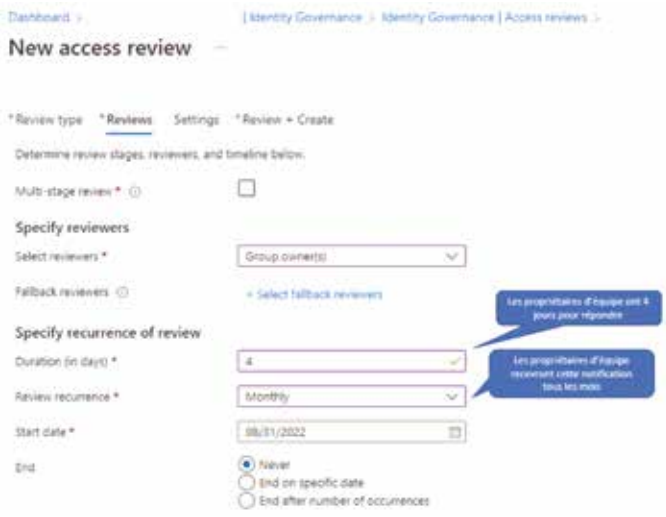
Le fait d'avoir un nombre important d'équipes incluant des partages de données avec des personnes situées à l'extérieur de l'entreprise pose une sérieux problème de gouvernance. Comment s'assurer que ces accès sont encore nécessaires après plusieurs mois ou plusieurs années ? Avec la vérification automatique des accès, les propriétaires d'équipes Teams devront valider au bout d'un délai qui sera fixé par l'administrateur, si les personnes invitées ou l'ensemble des utilisateurs doivent conserver l'accès à cette équipe.

La figure suivante illustre la création d'une revue des accès pour une équipe Teams en particulier.

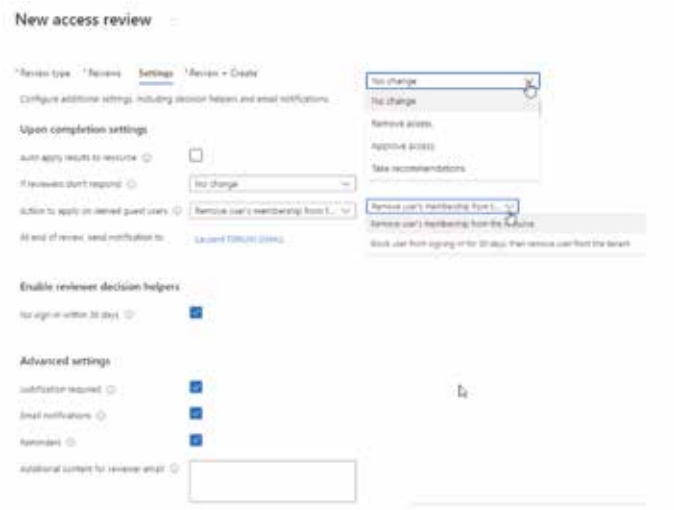


Là-aussi, si vous décidez de laisser ouverte la création des équipes et si vous voulez restreindre la revue des accès uniquement aux équipes Teams, il faudra régulièrement utiliser un script Powershell pour s'assurer que toutes les équipes Teams figurent bien dans cette revue.

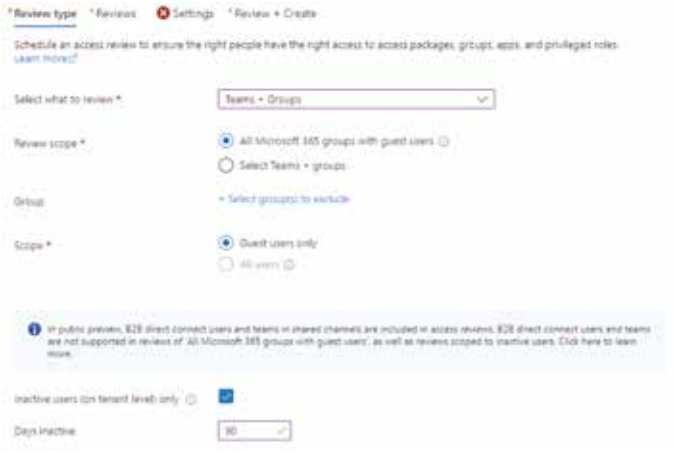
La figure ci-dessous illustre la mise en place de la fréquence des rappels et la période de grâce accordées aux propriétaires des équipes pour répondre à la revue des accès.



Si les propriétaires omettent de faire la revue des accès, Azure AD peut, soit supprimer l'accès, soit ne rien faire, soit approuver l'accès, ou enfin émettre des recommandations comme le montre la figure suivante. Tout dépend de votre stratégie.



D'une façon générale, je vous conseille de mettre en place une revue des accès pour tous les groupes Office 365, que cela soit des groupes Teams ou autres, afin de détecter les accès invités qui n'ont pas été utilisés depuis une période que vous aurez fixée. Cela est possible en utilisant l'option suivante dans la revue des accès.

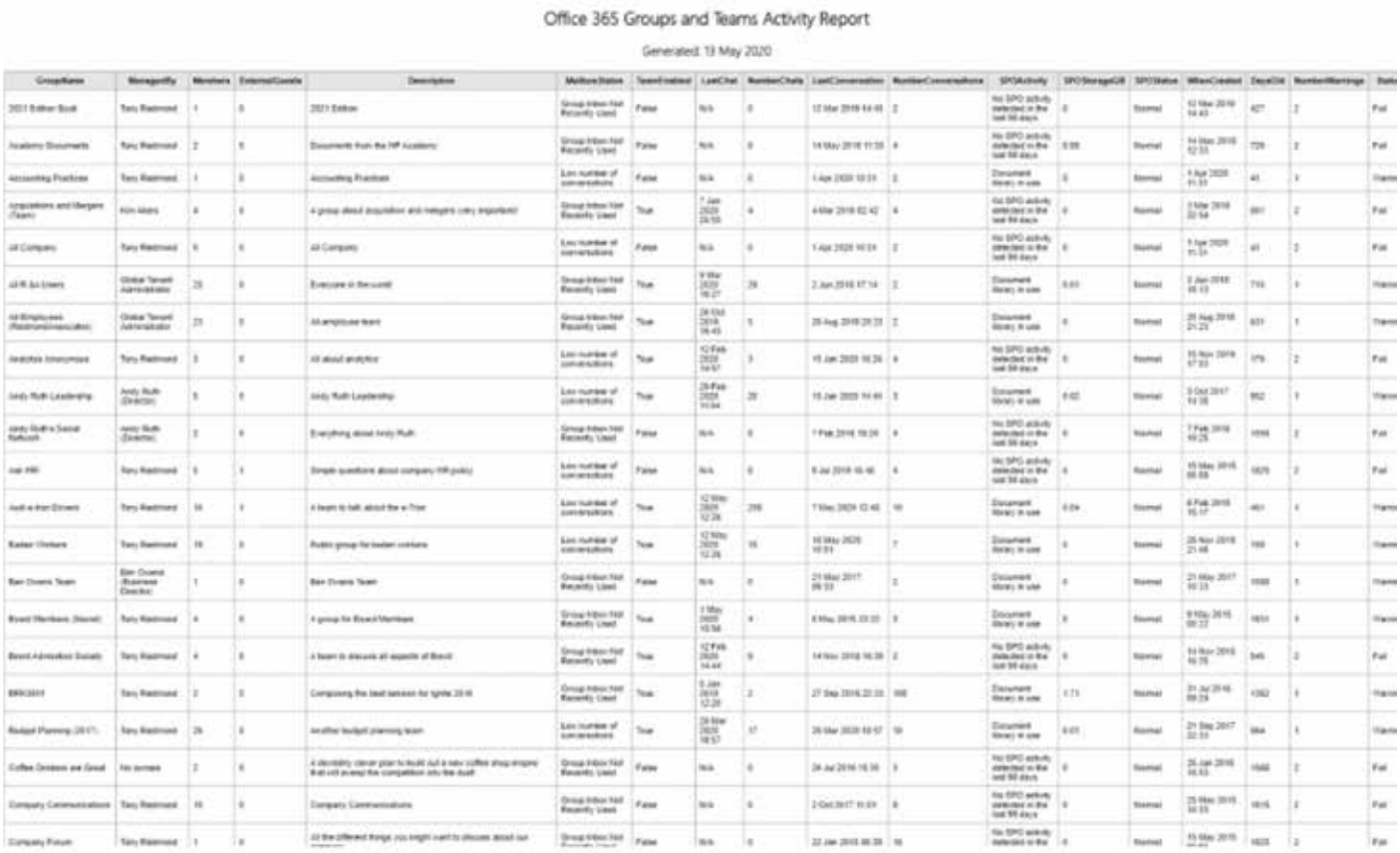


Revue des accès ; comptes invités inactifs

Utiliser un script pour analyser les usages

Une autre solution pour savoir si vos équipes sont utilisées ou pas, consiste à utiliser un script développé par Tony Redmond que vous pouvez récupérer ici : https://office365itpros.com/2020/01/14/microsoft-365-groups-teams-report/

Ce script vous donnera de précieuses informations sur tous les groupes Teams et leurs usages. Des éléments statistiques indispensables que vous ne retrouvez pas dans le portail d'administration de Teams. A consommer donc sans modération !



Office 365 Groups and Teams Activity Report

Generated: 13 May 2020

Rapport d'usage fourni par le script de Tony Redmond

Teams est une solution exceptionnelle pour le partage documentaire et la collaboration mais selon moi, demande que son usage soit encadré voire surveillé. Laisser sans aucun contrôle la solution peut faire courir un risque important de fuites de données. Aussi, avant d'ouvrir le service, je vous invite à vous positionner en tant qu'utilisateur et tester tout ce que vous êtes capable de faire une fois le client Teams en mains, puis de vérifier si cela est conforme avec la politique de sécurité de l'entreprise, comme le partage avec des invités ou les externes, le création de site SharePoint etc...

Les stratégies Microsoft disponibles dans l'environnement Azure AD, SharePoint Online et Teams sont présentes pour justement limiter certaines fonctions.

Avouez qu'il serait dommage de ne pas en profiter !

Par Laurent Teruin

CLOUD INNOVATION PARTNERS,
« POUR TOUT PROJET INFORMATIQUE EN COURS DE DÉVELOPPEMENT : NE JAMAIS PARTAGER LES DONNÉES RÉELLES AVEC LES ÉQUIPES PROJETS »

Cloud Innovation Partners (CIP) est une ESN, créée en Angleterre en 2016 par Khalid Boujdaa. En raison du Brexit puis la Covid, son fondateur revient en France et lance CIP en région Toulousaine en 2022. Projets de transformation autour de la data, solutions en mode SaaS, défis complexes de Big Data, AI/ML, Analytics, IoT... Décryptage.

Cloud Innovation Partners en quelques mots ?

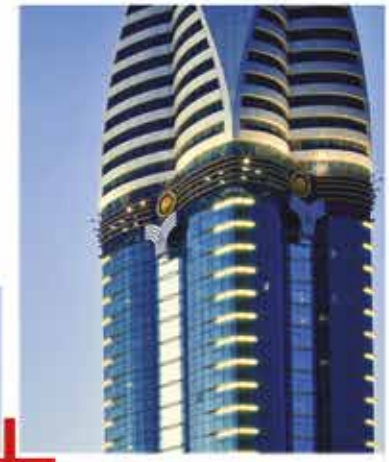
Cloud Innovation Partners, CIP est spécialisée dans la gestion des projets de transformation autour de la data. Le développement de la solution CloudTDMS a commencé au sein de CIP « Cloud Innovation Partners » en 2019 comme un accélérateur des projets internes, principalement pour automatiser la création de données synthétiques pour des défis complexes de Big Data, AI/ML, Analytics ou IoT. Compte tenu de la nature répétitive de la gestion de données de test et du manque d'outils abordables, CIP a décidé de tirer parti de ses compétences en développement Cloud et de créer une solution Cloud simple et abordable en mode SaaS. Après deux années de développement et 5 mois de « beta testing», CloudTDMS est officiellement en ligne depuis juillet 2022.

Quelles sont les valeurs qui animent CIP ?

Les valeurs qui animent Cloud Innovation Partners peuvent être résumées autour de 4 points :

- Vision : Nous créons un environnement positif où les personnes passionnées peuvent exercer leur talent et être responsabilisées et soutenues pour exceller dans leurs domaines respectifs.
- Mission : Nous contribuons aux innovations en créant des solutions en mode SaaS accessibles à tous.
- Valeurs : Nous restons connectés avec nos clients pour nous assurer que nous fournissons des solutions utiles.
- 3 Pays : Nous opérons dans 3 pays (France, Royaume-Uni et Inde).

« 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 »

Revenons sur la notion de fuite de données. Qu'est-ce qu'une fuite de données ? Quelles sont les raisons connues des fuites de données ?

Une fuite de données est un transfert de données non autorisé d'une organisation vers un tiers. Cela peut se produire de plusieurs manières, telles qu'un email, ou un accès physique non autorisé à des périphériques via des stockages dans le cloud, des ordinateurs portables ou des clés USB, ...

Les fuites de données peuvent se produire de plusieurs manières, internes ou externes, à l'exemple de ce qui suit :

- **Interne :**
  - > *Piratage interne :* en cas de divulgation délibérée des données par un employé ou un sous-traitant pour son profit personnel ou pour nuire à la réputation de l'entreprise.
  - > *Publication accidentelle :* lorsque des données sont publiées involontairement. A l'exemple d'un employé ou un sous-traitant commettant une erreur de sécurité comme l'envoi d'un e-mail contenant des informations confidentielles aux mauvais destinataires ou la publication publique des données privées.

- **Externe :**
  - > *Piratage externe :* un hacker ciblant l'infrastructure informatique d'une entreprise puis en dérobe les données.
  - > *Vol :* vol physique d'un ordinateur portable ou une clef USB.

- **Mixte interne et externe :**
  - > *Non-respect des procédures de sécurité :* une fuite de données peut également se produire lorsque des personnes ne suivent pas les procédures de sécurité appropriées. A l'exemple d'un employé qui imprime des informations sensibles et les laisse en public.
  - > *Mauvaise configuration des réseaux ou systèmes :* survient dans le cas d'un individu ou de la direction informatique qui ne configure pas correctement les réseaux ou systèmes, ce qui peut exposer des données. A l'exemple d'une base de données d'un site web insuffisamment protégée, des pirates peuvent y accéder.
  - > *Sécurité insuffisante des réseaux et systèmes :* en adoptant une sécurité traditionnelle, une fois que le hacker passe le barrage du firewall/VPN il a accès à tous les systèmes informatiques de l'organisation.

En résumé, les fuites de données se produisent le plus souvent d'une façon interne ou accidentelle. Les violations de données ouvrent une boîte de pandore de risques pour les entreprises tels que les augmentations de frais d'assurance, les poursuites judiciaires, les amendes réglementaires ou encore l'embarras avec les médias.

KHALID BOUJDAA

Analysons quelques fuites de données ?

En juillet 2022, Razer poursuit Capgemini pour une fuite de données : l'erreur à 10 millions de dollars ! Capgemini se voit poursuivi par Razer à cause d'un ancien employé de l'entreprise française qui a avoué être à l'origine de la faille de sécurité ayant provoqué une faille de sécurité en 2020, entraînant une fuite de ses données confidentielles sur ses clients et ses ventes.

En décembre 2021, la CNIL annonce la sanction de 180 000 euros à l'encontre de la société SLIMPAY pour Violation de données concernant environ 12 millions de personnes. Courant 2015, SLIMPAY effectue un projet de recherche interne, lors duquel elle utilise les données personnelles contenues dans ses bases de données. Lorsque le projet de recherche se termine en juillet 2016, les données restent stockées sur un serveur, qui ne fait pas l'objet d'une procédure de sécurité particulière et qui était librement accessible depuis Internet. Ce n'est qu'en février 2020 que la société SLIMPAY s'aperçoit de la violation de données, qui a concerné environ 12 millions de personnes.

Une fuite de données est un transfert de données non autorisé d'une organisation vers un tiers.

En juillet 2022, la base de données de la police de Shanghai est à vendre sur le dark web, ceci pourrait être la plus grande violation de données jamais enregistrée en Chine. La Chine compte environ 1,4 milliard d'habitants, ce qui signifie que la violation de données pourrait potentiellement toucher plus de 70 % de la population chinoise. En effet, des hackers inconnus ont affirmé avoir volé les données de près d'un milliard de résidents chinois après avoir piraté une base de données de la police de Shanghai. Ils vendent plus de 33 téraoctets de données volées pour 10 bitcoins (soit environ 200 000 US$). La base

de données comprend les noms, adresses, lieux de naissance, numéros de CIN, et de téléphone ainsi que des informations juridiques. Les Hackers ont affirmé que la base de données était hébergée sur le Cloud et accessible sans aucune protection.

En août 2022, deuxième fuite massive de données en 2 mois ! Les données de 800 millions de chinois exposées, Une énorme base de données chinoise stockant plus de 800 millions de visages et de plaques d'immatriculation de véhicules a été laissée exposée sur Internet pendant des mois avant de disparaître tranquillement en août. Cet incident est le deuxième après une fuite massive de données d'un milliard d'enregistrements dans une base de données de la police de Shanghai en Juin. Dans les deux cas, les données ont probablement été exposées par inadvertance et à la suite d'une erreur humaine.

Les organisation doivent rejoindre la nouvelle ère des données synthétiques (réalistes) !

Si des bases de données très sensibles ont été stockées dans le Cloud sans mesures de sécurité appropriées, cela est probablement dû au fait que des données réelles ont été utilisées pour des projets de données en cours tels que la formation d'un nouveau modèle AI/ML ou un projet big data ou Analytics.

Les experts en cybersécurité affirment qu'il n'est pas rare de trouver des bases de données ouvertes au public. Les PII (Personal Identifiable Information) non sécurisées, exposées par des fuites, des violations ou une forme d'incompétence, sont un problème de plus en plus courant auquel sont confrontés les entreprises et les gouvernements du monde entier.

Quelles sont les raisons des fuites de données ?

La cause ignorée de nombreuses fuites de données est bien évidente dans plusieurs cas : la sauvegarde locale et le partage des données réelles (de production) avec les partenaires informatiques, développeurs et testeurs pour l'avancement des projets en cours. Avec de plus en plus de travail à distance ainsi que la collaboration avec les partenaires informatiques onshore et offshore, les violations de données vont se produire plus fréquemment que jamais, aucune entreprise ne peut affirmer que cela ne lui arrivera pas !

En effet, le partage des données réelles est l'option la plus simple pour tous les membres de l'équipe d'un projet data mais c'est aussi l'option la plus dangereuse. Or ce n'est pas la seule option non plus!

Certaines entreprises pensent que le cryptage des données de production résoudra le problème, mais le diable est dans les détails ! Puisqu'il est tout simplement impossible de chiffrer tous les systèmes et toutes les données à tout moment, les données étant déchiffrées d'une manière ou d'une autre pendant le traitement des workflows (backend), il est également impossible de prouver que la sécurité du chiffrement fonctionne à tout moment. Ainsi, le chiffrement donne un faux sentiment de sécurité.

De ce fait, plusieurs entreprises ne respectent pas entièrement les politiques de confidentialité des données puisque les fichiers contenant les données sensibles sont toujours au cœur du business ainsi que l'accès à tout ou partie des données de production par les salaries et partenaires, y compris les équipes de développement et de test. Elles risquent des pénalités RGPD allant de 2 % du chiffre d'affaires annuel ou 10 millions d'euros, selon le montant le plus élevé, à 4 % ou 20 millions d'euros, selon la gravité de la violation.

Auriez-vous quelques recommandations à partager avec les entreprises pour éviter les fuites de données ?

Gartner prévoit que, d'ici 2024, 60 % des données utilisées pour le développement de projets d'IA et d'Analytics seront générées de manière synthétique.

Un conseil important de CloudTDMS.com, pour tout projet informatique en cours de développement : NE JAMAIS partager les données réelles avec les équipes projets, et cela même dans des cas aussi exceptionnels que la demande urgente d'un tableau de bord par le CEO de l'entreprise ou le besoin bloquant d'une équipe projet de données réelles pour la formation d'un nouveau modèle IA/ML, ou encore lors des phases dev/test d'un projet critique de big data.

Les organisation doivent rejoindre la nouvelle ère des données synthétiques (réalistes) ! Le nouveau carburant des Projets Data.

En d'autres termes, n'importe quelle entreprise peut rendre les données de test synthétiques/réalistes sans les extraire des plateformes de production !

> Par Sabine Terrey

Top 3 des avantages de la migration SaaS au sein de la DSI

Avec le SaaS, l'entreprise n'achète plus un produit, mais un service ! Décryptage des rythmes de déploiement, des usages, de la migration et des taux d'automatisation.

La DSI se dégage de tout ce qui est relatif à l'infrastructure et à l'administration technique, ainsi 46 % des DSI continuent à développer et maintenir plus de la moitié de leurs applications en interne.

Des applications on-premise...

Si 75 % des entreprises déploient leurs applications on-premise, 29% le font en cloud privé et cloud hybride pour 29 %, « nous constatons avec nos clients que le multi-infrastructure semble être la règle et que le cloud représente encore un potentiel important » précise Olivier Félis, ingénieur avant-vente, France et BeLux, chez Micro Focus.

Un rythme de déploiement annuel et trimestriel

Les rythmes annuels et trimestriels restent les plus prisés pour 44% des DSI. Si le rythme hebdomadaire – 21% ou mensuel- 36% est fréquent, il est moins recherché , « tout le monde parle de l'Agile et du DevOps, mais, si le DevOps peut s'appliquer largement, il ne faut pas oublier qu'une part non négligeable des applications, comme les applications legacy, ne sont pas faites pour cela. »

Top 3 des avantages de la migration SaaS !

Pour les applications critiques, le SaaS est retenu pour 51 % et des projets sont en cours pour 16 % supplémentaires en 2022. Le SaaS est donc une tendance très importante sur le marché.

Dans le Top 3 des avantages de la migration en SaaS, les réponses s'orientent ainsi :

- la maintenance système simplifiée - 63 %
- la gestion plus facile du versioning - 51 %
- la flexibilité - 46 %

Quant aux freins du SaaS, on retiendra :

- la localisation des données - 70 %
- la perte de compétences IT

Dans le Top 3 des décisions d'un passage en SaaS, on peut mentionner

- la continuité d'activité - 67 %
- la sécurité des données
- l'économie globale du projet

Focus sur les usages

Dans le Top 3 des usages des logiciels de gestion du cycle applicatif, on peut citer :

- le déploiement – 86%
- la gestion du changement/configuration
- l'intégration et la livraison continue

Dans le Top 3 des taux d'automatisation par usage, on note :

- le déploiement - 48 %
- l'intégration et la livraison continue
- Devops et Agile

Source : Observatoire du SaaS 2022 Micro Focus - Directions informatiques sur l'intégration des problématiques de migration vers le SaaS des applications stratégiques - mars et avril 2022 - 121 DSI


STORMSHIELD
Le choix européen de la cybersécurité
Partenaire de confiance
pour
sécuriser vos
infrastructures
opérationnelles
IT
OT
www.stormshield.com

METSYS

DIGITAL TRUST BUILDER

Conseil
Intégration
Services Managés