N°34 I JUIN 2024

CONDUIRE LA TRANSFORMATION NUMÉRIQUE DE L'ENTREPRISE

SMART DSI®

DOSSIER
L'intelligence collective dans l'ère numérique

INTERVIEW
Développer les compétences cyber sur tout le territoire

L'ETUDE A RETENIR
IA & Dirigeants : innovations et concurrence

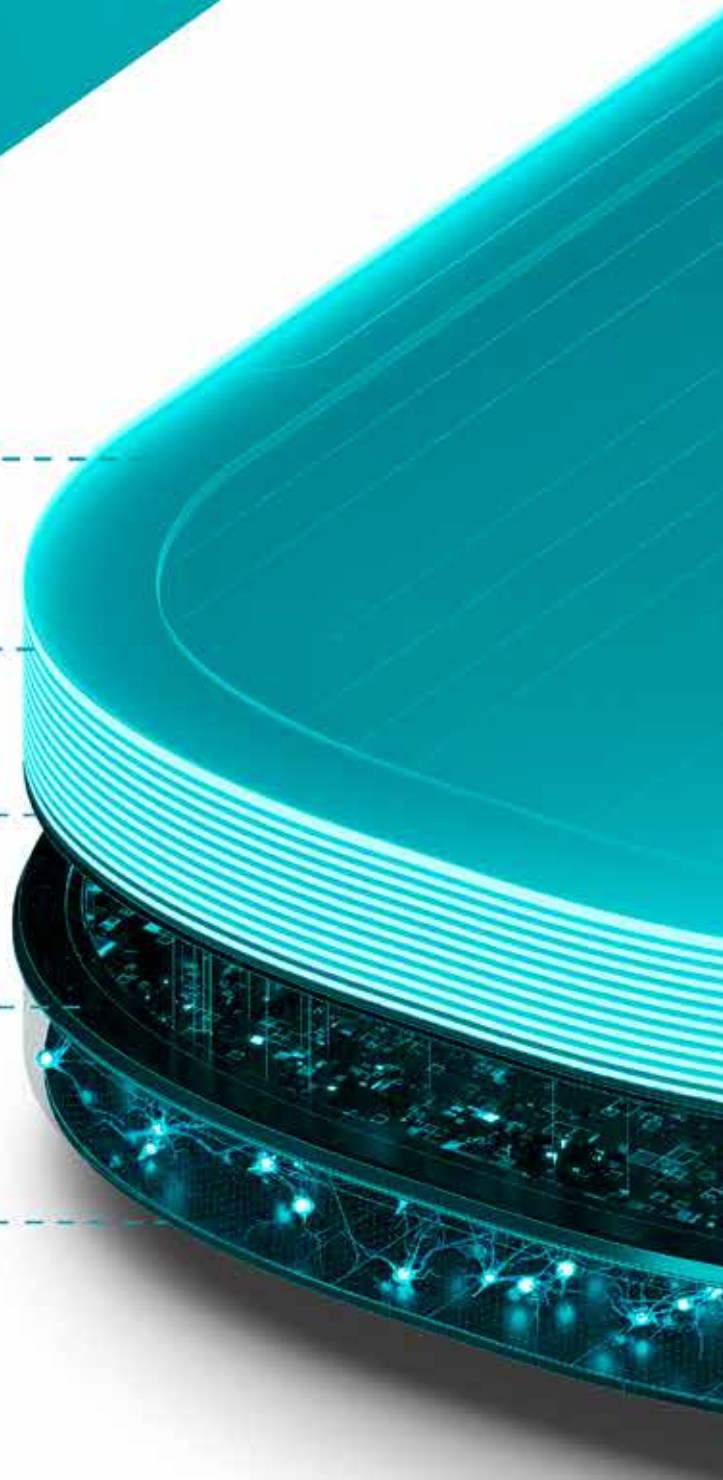
INTERVIEW
La nouvelle génération de DSI osera-t-elle innover ?

EXPERT
Supervision ou observabilité, quelles recommandations ?

PERSPECTIVES
NIS2 & CESIN : Transposition nationale de la directive européenne

Digital Security
Progress. Protected.

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



Sécurité multicouche

Des technologies exclusives qui dépassent les limites des antivirus traditionnels.

Taches des utilisateurs finaux

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

Réseau sensoriel

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

Intelligence artificielle

Apprentissage profond, apprentissage automatique et autres méthodes avancées.

Expertise humaine

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

WWW.ESET.COM/FR

Plus d'agilité ! Plus d'optimisation ! Plus de rationalisation !

A l'heure de l'engouement vers l'Intelligence Artificielle, du besoin de flexibilité, de créativité et d'ouverture mais aussi de se sentir armé et équipé pour relever les défis complexes de demain, les entreprises doutent de leurs infrastructures.

Les chiffres confortent ce constat. En effet, selon 94 % des cadres dirigeants, leur infrastructure existante est un réel frein à l'innovation, aux progrès organisationnels et tout simplement aux initiatives internes(1). Une technologie inadaptée voire obsolète augmente inévitablement les risques opérationnels. N'est-il pas temps de prendre les bonnes décisions, d'aligner son approche sur les exigences de la stratégie métier et d'améliorer les processus de gestion du cycle de vie des infrastructures ? A la clé, des avantages concurrentiels certains !

Mais, comment alors impulser plus d'agilité face aux environnements en évolution constante et aux charges de travail en progression ? Sans doute en adoptant une culture du bon sens, de l'échange et du partage des informations. A l'appui quelques indicateurs intéressants,(2) selon 93 % des cadres, les équipes pourraient atteindre leurs résultats actuels deux fois plus vite si elles collaboraient plus efficacement. Et 65 % des salariés pourraient progresser plus facilement s'ils avaient des objectifs moins nombreux et plus spécifiques.

Ainsi, si les équipes se sentent parfois bloquées avec des méthodes de travail dépassées, des objectifs bien trop variés et des réunions inutiles, optimiser les processus, définir clairement les attentes, repenser la collaboration et rendre les connaissances plus accessibles deviennent les axes prioritaires des organisations. A la clé, une productivité stimulée, un potentiel exploité et une vraie valeur créée !

De vastes chantiers certes, mais fondamentaux pour naviguer avec aisance et force face aux futurs défis.

Très bonne lecture

(1) Source Rapport Lifecycle Management Report NTT DATA.

(2) Source The State of Teams 2024 – Atlassian

Sabine Terrey
Directrice de la Rédaction
sterrey@itpro.fr

SMARTDSI *« 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

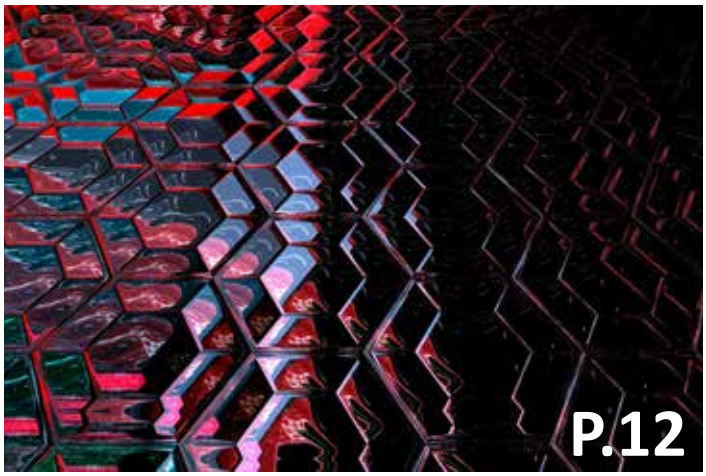
N°34 I JUIN 2024

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.6


P.26


P.12


P.40


P.38


P.34


P.31

SMART DSI

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

Thierry Bollet, Sylvain Cortes, Didier Danse, Laurent Téruin, Sabine Terrey, 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
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

L'intelligence collective
DANS L'ÈRE NUMÉRIQUE

> Par Didier Danse

Dans un monde en constante évolution, où les défis se complexifient et où les changements sont rapides, les organisations se trouvent confrontées à un défi majeur : comment tirer pleinement parti de la diversité des compétences, des expériences et des perspectives de leurs membres pour innover, s'adapter et créer de la valeur dans un environnement en mutation continue ?

Traditionnellement, les approches centralisées et hiérarchiques ont souvent entravé la capacité des organisations à exploiter pleinement le potentiel de leur capital intellectuel collectif. C'est là que l'intelligence collective fait tout son sens. En intégrant les principes de collaboration, de diversité et d'autonomie, l'intelligence collective offre des pistes pour relever ce défi et transformer les organisations en des entités agiles, innovantes et résilientes.

Des besoins croissants

La numérisation croissante des interactions humaines et des processus organisationnels a profondément transformé la manière dont les individus et les organisations communiquent, collaborent et opèrent grâce, notamment, à une interconnexion sans précédent facilitée par les technologies de l'information et de la communication. La diffusion des connaissances est rapide et massive, désormais. Les plateformes de médias sociaux, les outils de collaboration en ligne et les infrastructures de cloud computing sont devenus des éléments essentiels, rendant possibles une coordination et une coopération à grande échelle. Les barrières géographiques tendent à disparaitre, et les processus décisionnels et organisationnels s'accélèrent grâce à l'automatisation et à l'analyse des données.

La complexité croissante de ces défis contemporains nécessite des solutions innovantes et multidimensionnelles. L'intelligence collective est alors une piste importante à envisager afin de répondre à ces besoins sans cesse en augmentation.

La réponse par l'intelligence collective

L'intelligence collective prend une nouvelle dimension depuis quelques années, se nourrissant de la capacité des technologies numériques à agréger et à analyser les contributions individuelles. Les systèmes collaboratifs en ligne, les forums de discussion, les wikis et les plateformes de crowdsourcing sont autant d'outils qui facilitent l'émergence d'une intelligence collective, où les idées et les solutions sont coconstruites par des réseaux de personnes interconnectées. Cette dynamique permet d'exploiter la diversité des connaissances et des compétences, favorisant ainsi l'innovation et la résolution de problèmes complexes.

L'intelligence collective offre des pistes pour transformer les organisations en des entités agiles, innovantes et résilientes.

L'intelligence collective transcende les capacités individuelles pour exploiter le potentiel des synergies entre les personnes, les idées et les ressources et repose sur la conviction fondamentale que la somme des compétences, des expériences et des perspectives dépasse de loin celle de ses parties constitutives.

Lorsque les individus s'unissent dans un esprit de confiance, d'ouverture et de respect mutuel, ils peuvent atteindre des niveaux de performance et d'innovation qui seraient autrement inaccessibles. Chaque voix compte, chaque idée est valorisée et chaque contribution est essentielle à la réalisation de l'objectif commun.

Des opportunités multiples

Les synergies entre les personnes, les idées et les ressources ont différents intérêts, comme nous avons pu le voir au paragraphe précèdent. Il semble utile de les rassembler en une liste compréhensible, bien qu'elle ne soit certainement pas exhaustive :

- La résolution de problèmes complexes en rassemblant une diversité de perspectives, d'expériences et de compétences pour développer des solutions complètes et efficaces.
- L'innovation grâce à l'émergence de nouvelles idées, de nouvelles approches et de nouvelles technologies en encourageant le croisement des disciplines et des domaines d'expertise. Les idées nouvelles naissent de la collision d'horizons divers, et les innovations émergent lorsque les individus sortent de leurs zones de confort pour explorer de nouveaux territoires intellectuels.
- L'adaptabilité au changement pour s'adapter plus rapidement aux nouvelles réalités, répondre aux défis émergents et saisir les opportunités.
- L'amélioration de la prise de décision en réduisant ainsi les biais individuels et en augmentant la probabilité de succès.
- Le renforcement de l'engagement en favorisant un sentiment d'appartenance, de contribution et de valorisation au sein des groupes, ce qui renforce l'engagement des membres et stimule leur motivation à travailler vers des objectifs communs.
- La création de valeur économique et sociale en favorisant l'efficacité, la durabilité et l'innovation.
- La promotion de l'apprentissage continu au travers d'un environnement propice à l'apprentissage continu et à l'amélioration constante.

Les synergies entre les personnes, les idées et les ressources ont différents intérêts.

Bien que ces catégories s'avèrent assez larges et parfois même assez génériques, il n'est pas très compliqué de comprendre des gains potentiels de l'intelligence collective.

Ainsi, le proverbe « *Il y a plus d'idées dans deux têtes que dans une* » se voit démultiplier par la présence du numérique.

La technologie au service de l'intelligence collective

En effet, le numérique décuple les interactions entre les gens grâce aux outils de collaboration comme les plateformes de partage de documents, les logiciels de visioconférence, les réseaux sociaux d'entreprise et les outils de gestion de projet, qui facilitent la communication et la collaboration à distance. Mais au-delà de cette interconnexion entre les gens, de nombreux outils, technologies et méthodes permettent de supporter l'intelligence collective, notamment :

- L'intelligence artificielle pour faciliter la collaboration, notamment les chatbots pour l'assistance en ligne, les systèmes de recommandation pour le partage de contenu pertinent et les algorithmes de fouille de données pour l'identification de modèles.
- Les données massives (big data) et l'analyse de données qui peuvent être utilisées pour extraire des informations précieuses, identifier des tendances et prendre des décisions éclairées de manière collective.
- Les communautés en ligne, comme les forums de discussion, les groupes de réseaux sociaux et les plateformes de crowdsourcing, qui rassemblent des individus partageant les mêmes intérêts pour résoudre des problèmes, échanger des connaissances et stimuler l'innovation.

Combinées entre elles, il est probable que d'autres technologies de tous les jours puissent être exploitées, sans pour autant être dans la liste ci-dessus. C'est d'ailleurs tout le sujet de l'intelligence collective : permettre à des intervenants de trouver des solutions innovantes à des problèmes. Ainsi, il est probable que de nouvelles technologies utiles dans ce contexte fassent leur apparition prochainement.

Des risques

Evidemment, comme toujours, il s'agit évidemment de comprendre les risques associés à des méthodes ou même à des états d'esprit. L'intelligence collective démultiplie les intérêts. Il est évident qu'elle peut également multiplier les risques. En voici quelques-uns à tenir compte quand l'on espère en profiter pleinement…

- L'intelligence collective peut être vulnérable aux biais cognitifs et sociaux, tels que la pensée de groupe, où la pression pour parvenir à un consensus peut étouffer les idées novatrices et critiques. Cela peut conduire à des décisions suboptimales ou à la confirmation des préjugés existants.
- Lorsque les contributions individuelles ne sont pas filtrées ou vérifiées correctement, il existe un risque que des informations erronées, incomplètes ou trompeuses influencent le processus décisionnel. La gestion de la qualité de l'information est donc un défi majeur.

- La collaboration massive implique souvent le partage de données sensibles et personnelles. Si ces données ne sont pas protégées adéquatement, cela peut entraîner des violations de la confidentialité et des cyberattaques, compromettant la confiance des participants.
- Les plateformes d'intelligence collective peuvent être manipulées par des individus ou des groupes malveillants qui cherchent à influencer les résultats à leur avantage. La diffusion de désinformation peut saper la fiabilité et l'efficacité de l'intelligence collective.
- Tous les participants n'ont pas nécessairement un accès égal aux ressources numériques ou aux compétences souhaitées pour contribuer efficacement. Cela peut entraîner une représentation déséquilibrée et des décisions qui ne reflètent pas les intérêts de tous les membres du groupe.
- Une trop grande dépendance à l'égard des outils numériques et des algorithmes peut réduire la capacité humaine à penser de manière critique et autonome. Il est essentiel de maintenir un équilibre entre l'utilisation de la technologie et la valorisation de la contribution humaine.

Favoriser l'intelligence collective peut ainsi mener à des situations problématiques. Les comprendre c'est déjà minimiser les risques correspondants. Pour y parvenir, il s'agit également de s'assurer que des valeurs et des fondements soient définis...

Un cadre pour l'intelligence collective

Pour que l'intelligence collective prospère, elle exige un leadership visionnaire et inclusif qui favorise la confiance, la transparence et l'équité. Elle nécessite également des structures organisationnelles flexibles qui favorisent la communication ouverte, la prise de décision participative et l'autonomisation des individus. Dès lors, voici quelques règles qu'il s'agit de respecter :

- Créez un environnement où les membres se sentent en sécurité pour exprimer leurs idées, poser des questions et prendre des risques intellectuels. La confiance mutuelle favorise la collaboration et le partage libre d'informations.
- Rassemblez des individus aux horizons variés, ayant des compétences, des expériences et des perspectives différentes. La diversité favorise la créativité et permet d'aborder les problèmes sous différents angles.
- Encouragez tous les membres du groupe à participer activement aux discussions, aux sessions de brainstorming et aux prises de décision. Assurez-vous que chacun se sente écouté et valorisé.
- Utilisez des techniques de facilitation telles que le brainstorming, la pensée visuelle, les jeux de rôle et les discussions en petits groupes pour stimuler la créativité et l'interaction entre les membres.
- Assurez-vous que tous les membres du groupe comprennent les objectifs à atteindre et partagent une vision commune. Cela crée un sentiment d'engagement et de direction partagée.
- Mettez en place des plateformes et des outils numériques qui facilitent la communication, le partage d'informations et la collaboration à distance. Cela permet à un groupe dispersé géographiquement de travailler ensemble de manière efficace.
- Favorisez une culture où le feedback est donné et reçu de manière constructive. Cela permet aux membres du groupe de s'améliorer continuellement et de tirer des leçons des succès et des échecs passés.
- Reconnaissez et célébrez les succès obtenus grâce à la collaboration et à l'intelligence collective pour renforcer le sentiment d'appartenance et l'engagement des membres du groupe.

Pour que l'intelligence collective prospère, elle exige un leadership visionnaire et inclusif.

La ressemblance entre l'agilité et l'intelligence collective est assez flagrante car les deux partagent des valeurs. L'intelligence collective peut, en quelque sorte, être vue comme une extension de l'agilité.

L'agilité et l'intelligence collective

Oui, l'intelligence collective et l'agilité sont étroitement liées et peuvent se renforcer mutuellement dans un contexte organisationnel. Voici quelques points qui illustrent ce lien :

- L'intelligence collective repose sur la collaboration et la communication ouverte entre les membres d'un groupe ou d'une équipe. De même, l'agilité favorise une communication transparente et une collaboration étroite entre les différentes parties prenantes d'un projet ou d'une initiative.

- L'agilité est caractérisée par sa capacité à s'adapter rapidement aux changements de circonstances et aux nouvelles informations. De même, l'intelligence collective permet aux groupes de s'adapter de manière agile aux défis émergents en exploitant la diversité des perspectives et des compétences disponibles.
- Dans les approches agiles telles que la méthodologie Scrum, les équipes travaillent par itérations courtes, recevant régulièrement des retours d'information et s'adaptant en conséquence. L'intelligence collective encourage également l'apprentissage continu et l'amélioration progressive grâce au partage d'expériences et à la rétroaction constructive.
- Les équipes agiles sont souvent autonomes et responsables de la planification et de l'exécution de leur travail. De même, l'intelligence collective favorise l'autonomie des individus et des groupes, les encourageant à prendre des initiatives et à contribuer activement à la réalisation des objectifs communs.
- L'intelligence collective implique souvent une prise de décision participative, où les membres du groupe contribuent à l'élaboration et à la sélection des meilleures solutions. De même, les approches agiles encouragent une prise de décision décentralisée, où les décisions sont prises au niveau le plus approprié et le plus proche du terrain.

En combinant les principes de l'intelligence collective et de l'agilité, les organisations peuvent créer un environnement propice à l'innovation, à la résilience et à l'efficacité, leur permettant ainsi de s'adapter rapidement aux changements du marché et de relever avec succès les défis complexes auxquels elles sont confrontées.

L'intelligence collective se révèle être un outil puissant et essentiel dans la boîte à outils des organisations modernes. En favorisant la collaboration, la diversité et l'autonomie, elle permet aux organisations de naviguer avec agilité dans un monde en constante évolution. De la résolution de problèmes complexes à la prise de décisions éclairées, en passant par la stimulation de l'innovation et de la créativité, l'intelligence collective offre une approche holistique pour répondre aux défis les plus pressants et saisir les opportunités émergentes.

Pour embrasser pleinement le potentiel de l'intelligence collective, les organisations doivent cultiver une culture de confiance, d'ouverture et de collaboration, tout en adoptant des pratiques et des technologies qui favorisent le partage des connaissances et la prise de décision participative. En investissant dans l'intelligence collective, les organisations peuvent créer un avantage concurrentiel durable et s'assurer qu'elles sont prêtes à relever les défis de demain.

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

inmac wstore
GROUPE BECHTLE

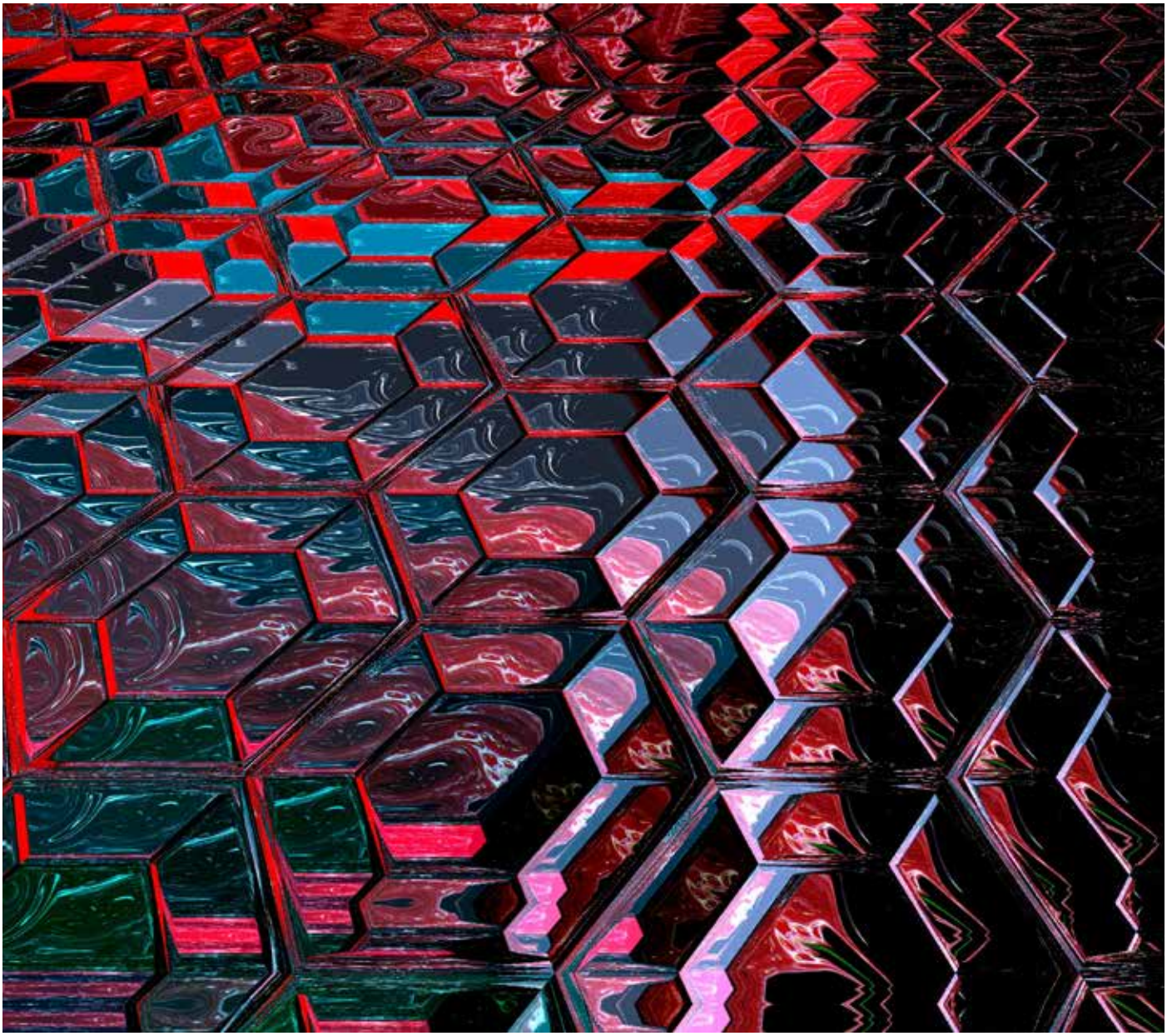
DECOUVREZ VOTRE **GUIDE D'ACHATS** DE REFERENCE **POUR L'EQUIPEMENT INFORMATIQUE** DE VOTRE ENTREPRISE

TPE • PME • GRANDS COMPTES

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

La fin D'UN CHAPITRE

Dans la cybersécurité et non pas la presque ancienne SSI (Sécurité des Systèmes d'Information) sans parler de la Sécurité Informatique, l'outillage de collecte et valorisation des logs et évènements, connu notamment par l'acronyme de SIEM est une des clés de voute de l'édifice.



Le SIEM est notamment le cœur de l'outillage utilisé quotidiennement, en 24/7 par les analystes cyber au sein d'un service de SOC et IR/CERT. Le SIEM avec ses évolutions de type datalake est la base utilisée pour la valorisation et exploitation de la sécurité, seule ou en corrélation avec d'autres outils et process tels que les flux de Threat Intelligence, les résultats des scan de vulnérabilité, les évènements en provenance d'EDR, etc.

Une vague de changements

En espace des quelques semaines, une vague de changements importants a touché les principaux éditeurs de SIEM, présage de secousses à venir pour l'ensemble du paysage de la cybersécurité.

La fin d'une histoire de la QRadar d'IBM Security qui a été cédée à Palo Alto Networks. Outil historique avec Splunk, ex Q1 Labs, un excellent produit avalé par IBM en 2007/2008, est intégré, revendu par IBM à Palo Alto Networks, et au même moment Exabeam et LogRhythm, deux autres éditeurs de SIEM fusionnent.

Ces opérations arrivent juste quelques mois après le rachat de Splunk par Cisco...

Les analystes de marché, sont eux, assez critiques concernant les implications de cet abandon par IBM de son offre cyber auprès de Palo Alto, connu pour sa solution d'orchestration XDR. Pour Forrester Research, il s'agit de la plus grande concession d'un éditeur de SIEM à un éditeur de XDR et un changement fondamental pour le marché de IR (Incident Response).

La vente par IBM de sa solution poussera les clients actuels de QRadar vers la solution Cortex XSIAM de Palo Alto. C'est de facto la mort rapide de QRadar même pas lente.

Si en plus Splunk est fusionné dans les offres intégrées de Cisco, le marché se retrouve avec deux ou trois acteurs à côté des offres SIEM de deux GAFAM investis fortement sur le marché de la cybersécurité, Microsoft et Google (Chronicle).

Les analystes de marché, sont eux, assez critiques concernant les implications de cet abandon par IBM de son offre cyber.

Quelques explications ...

Plusieurs explications, toutes valables et qui montrent les changements fondamentaux et rapides en cours.

D'une part, l'adoption des technologies cloud, auxquelles les acteurs traditionnels n'ont pas réussi au fond à s'adapter. C'est le cas notamment d'IBM qui, d'après les analystes, et malgré QRadar Log Insights et de QRadar SIEM SaaS, a échoué ces dernières années dans ses tentatives de migration de QRadar vers le cloud. Pour IBM, opérer un demi-tour et vendre QRadar à Palo Alto Networks, apparemment sans avertir tous ses clients, est choquant. Il y a certainement beaucoup de clients QRadar confus et frustrés qui cherchent des réponses à cette situation.

Manque d'innovation, inadaptation à la révolution technologique et opérationnelle du cloud, mais aussi multiplication ces dernières années d'éditeurs de solutions sur un marché complexe et concurrentiel, sur lequel, peu d'entre eux étaient financièrement autonomes et profitables....

La cybersécurité NewGen

Nous assistons à l'émergence des acteurs plateformes, Palo Alto, Microsoft, Crowdstrike, Cisco, Google. Etc. Ils s'imposent de plus en plus sur le marché de la ''cybersécurité NewGen''. Ils s'imposent face aux acteurs *best-of-breed*, qui ont été les coqueluches de CISO et RSSI pendant les quinze dernières années.

Pour les utilisateurs finaux, cela démontre plus que jamais l'importance vitale des services managés à haute valeur ajoutée, indépendants des éditeurs et constructeurs.

En fait le marché, sous la pression concurrentielle, des économies budgétaires et de la révolution du cloud, fait entrer petit à petit le marché des constructeurs et éditeurs dans la normalité des autres segments de l'IT. Celle des trois ou quatre acteurs majeurs en concurrence par segment fonctionnel, sur les marchés mondiaux. Et à cela s'ajoute l'urgence concurrentielle sur un marché chamboulé par l'ascension rapide de Microsoft avec Azure Sentinel et Google avec Chronicle.

Pour les utilisateurs finaux, cela démontre plus que jamais l'importance vitale des services managés à haute valeur ajoutée, indépendants des éditeurs et constructeurs. Des services certifiés et engageants auprès des clients, intégrant et rendant indépendants les clients des différentes briques logiciels de cybersécurité.

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

Un contexte où la gouvernance des données est de plus en plus complexe et nécessite une meilleure maîtrise

La véritable valeur d'une organisation, c'est son patrimoine data. **Cependant, saviez-vous que les informations des bases de données proviennent de données structurées, qui ne représentent que 20% de l'ensemble des données d'une organisation?** Saviez-vous également qu'un simple e-mail contenant du texte et une image est considéré comme un fichier à données non structurées? **Il est de fait inutilisable (en l'état) par l'Intelligence Artificielle ou la Business Intelligence, par exemple**. C'est regrettable, car leur utilisation devient un avantage concurrentiel indéniable, mais ils nécessitent une grande quantité de données pour être efficaces.

C'est un paradoxe, car en 2025, le monde comptera environ 175 milliards de téraoctets de données (ou 175 000 milliards de Go), mais seulement 0,5% de ces données sont actuellement utilisées. De plus, il faut tenir compte du fait que ces 0,5% comprennent des doublons, des données non-conformes, non sécurisées, non documentées ou qui ne sont même pas à jour. Autrement dit, des informations manquantes, incomplètes, erronées... **Il est donc facile de comprendre qu'il n'est pas possible de prendre des décisions éclairées, de prédire, de gouverner ou de sécuriser avec des données de mauvaise qualité et en faible quantité**.

Comment m'assurer que j'exploite bien les données à valeur ajoutée de mon organisation? **Et comment m'assurer de leur qualité dans un contexte de Cloud, de Saas, où les systèmes d'informations sont de plus en plus ouverts, interdépendants et les données de plus en plus éparpillées? Heureusement, il existe des outils permettant de répondre à cette problématique et de mettre en œuvre une stratégie de Data Quality, basée sur un catalogage des données le plus complet possible**. Cette démarche de qualité répond à de nombreux enjeux :

- **La localisation du patrimoine data**, pour une vue 360° de toutes vos données
- **Les référentiels**, pour centraliser vos données stratégiques et mieux les partager avec votre écosystème
- **L'automatisation**, pour le contrôle de cohérence de vos données avec des règles métier, et assurer la qualité par le nettoyage systématique
- **Le droit à l'information**, pour identifier les données collectées sur un collaborateur ou un client
- **L'anonymisation des données**, pour assurer la confidentialité
- **L'Intelligence Artificielle, la Business Intelligence**, pour assurer l'innovation et maintenir un niveau concurrentiel élevé

Nous allons vous expliquer dans ce guide les bases d'une stratégie de Data Quality efficiente et comment initier cette démarche grâce à la cartographie de votre patrimoine Data.

175 zettaoctets
dans le monde en 2025

1 zettaoctets
=
1Md teraoctects

0,5 %
de ces données sont actuellement analysées

80 %
sont des **données non structurées**

BLUEWAY
DATA DRIVEN SOLUTION

Éditeur d'une plateforme de gestion de données flexible et sécurisée, Blueway favorise l'automatisation des processus d'échanges d'informations pour que chaque décision, chaque processus et chaque fonctionnalité facilite le quotidien des entreprises.

Comment initier une démarche de Data Quality ?

1 Cartographie des données

Cette première étape sert à prendre connaissance de l'ensemble de son patrimoine data (systèmes et flux intersystème), prérequis nécessaire à une démarche visant la qualité.

2 Classification des données

Cette seconde étape sert à identifier les données prioritaires, les « golden sources » qui vont donner de la valeur au reporting final. Les données doivent toujours être pertinentes pour l'objectif spécifique pour lequel elles sont utilisées.

3 Catalogage des traitements

Il faut ensuite identifier les données par usage (structurées et non structurées) pour les homogénéiser, pour créer une cohérence à travers différentes sources, systèmes ou périodes de temps.

4 Analyse des données

Cette étape sert à l'analyse de la qualité des données, et ce tout au long de leur cycle de vie (de bout en bout). C'est à ce moment qu'il est nécessaire de définir les critères et les règles métiers de qualité.

5 Remédiation

C'est l'étape de correction des données qui ne répondent pas aux normes ou aux exigences de qualité définies à l'étape précédente, comme le nettoyage des données inutiles, sensibles ou interdites à la conservation, dans le but de les fiabiliser.

6 Stratégie d'amélioration

Il s'agit dans cette dernière étape de mettre en œuvre une méthodologie de correction et de prévention grâce à une vision globale et synthétique du patrimoine de données au regard de son infrastructure technique.

GUIDE PRATIQUE

Vous découvrirez dans ce guide pratique :

- Les outils pour soutenir votre démarche Data Quality
- Nos conseils pour une mise en oeuvre efficace
- Des cas d'usage à partir de retours d'expérience de nos utilisateurs
- Les points clés à retenir

Télécharger le guide

Stéphane LE LIONNAIS

Expert en gouvernance de données et co-fondateur de Dawizz

www. blueway.fr | 04 12 39 03 99

Talkspirit AIDE LES ORGANISATIONS À ÉVOLUER EN DE VÉRITABLES PLATEFORMES D'INTELLIGENCE COLLECTIVE

Nouveautés, intégration des plateformes, mais aussi alternative souveraine, enjeux du 'future of work', et défis, la stratégie de Talkspirit pour atteindre les objectifs est ambitieuse et réjouissante. Philippe Pinault Cofondateur et CEO de Talkspirit a accepté de se prêter au jeu des Questions – Réponses.

Pourriez-vous présenter Talkspirit en quelques mots ?

Avec Olivier Ricard, nous avons cofondé Talkspirit, il y a 20 ans, en 2004 (sous le nom de BlogSpirit), afin de proposer des solutions collaboratives pour les organisations en quête de transversalité, de transparence et de plus de cohésion. Nous faisions partie des pionniers des réseaux sociaux d'entreprise et, aujourd'hui, nous accompagnons plus de 1.000 entreprises et organisations, en France et à l'international, dans leur transformation digitale afin d'optimiser leur performance, mais aussi de leur rendre accessibles les enjeux du "future of work".

Nous avons acquis la conviction que, dans un monde de plus en plus complexe et incertain, les organisations qui réussiront demain sont celles qui sauront évoluer en de véritables plateformes d'intelligence collective, dont les piliers sont la transparence, la responsabilité, l'innovation, la collaboration, la diversité et l'inclusion, le sens et l'impact sociétal et environnemental.

Nos deux logiciels Talkspirit et Holaspirit répondent à cette vision, réunissant en une suite complète des applications essentielles pour répondre aux besoins des organisations en matière de communication, de collaboration ou encore de gouvernance partagée.

Luttez en continu contre tous les types de menaces

Avec une visibilité approfondie sur les cybermenaces qui ciblent votre entreprise

Threat Intelligence

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

kaspersky

PHILIPPE PINAULT

Enfin, nous sommes très fiers de notre indépendance, puisque nous sommes autofinancés à 100% ce qui nous offre une liberté d'entreprendre et d'innover qui sont de véritables moteurs pour les équipes de Talkspirit.

Les prochains mois vont être technologiquement et fonctionnellement très riches pour la plateforme. Qu'est-ce que cela signifie concrètement ?

Quoi de mieux pour fêter nos 20 ans d'existence, que de se lancer de nouveaux défis et objectifs à atteindre !

Nous travaillons à l'intégration complète de nos deux plateformes Holaspirit et Talkspirit pour apporter la meilleure expérience utilisateur à nos clients utilisant nos offres, leur offrir une suite de communication et de collaboration encore plus efficace et pertinente et émerger comme une alternative souveraine aux géants américains sur le marché européen.

Quoi de mieux pour fêter nos 20 ans d'existence, que de se lancer de nouveaux défis et objectifs à atteindre !

L'Intelligence Artificielle Générative constitue également un défi important cette année avec l'intégration de cette technologie. Qu'il s'agisse d'assister l'utilisateur dans la rédaction de contenus, la recherche d'informations ou encore l'automatisation de tâches, cette année marquera sans nul doute l'entrée dans une nouvelle ère des digital workplaces.

Enfin, nous poursuivons nos investissements en matière de recherche et de développement, notamment sur le thème des gouvernances partagées pour lequel nous avons aujourd'hui un leadership au niveau mondial, afin d'aider les organisations qui souhaitent s'engager vers de nouveaux modèles de leadership et de management.

Vous évoquez aussi votre priorité historique « l'expérience utilisateur », pourriez-vous nous en dire plus ?

L'annonce récente et brutale par Meta de fermer Workplace, son réseau social professionnel à destination des entreprises, nous encourage à continuer à investir dans l'expérience utilisateur, qui est déjà l'un de nos différenciants forts. Depuis la création de Talkspirit, nous veillons à ce que nos plateformes soient le plus ergonomique possible, et qu'elles soient simples à utiliser et à déployer pour nos clients. La technologie ne fait rien seule, c'est dans l'adoption et dans l'usage qu'il convient d'être les meilleurs !

Cette proximité, qui passe par une écoute et un dialogue permanent avec nos utilisateurs et clients, est également un élément clef de notre différenciation.

Ainsi, nous nous concentrons sur les 30 % de fonctions les plus utiles au travail quotidien, celles utilisées par 90 % des utilisateurs avec le même niveau d'excellence que les meilleurs du marché. Avec d'ores et déjà, plus d'une dizaine d'applications réunies au sein de la même suite, nous souhaitons devenir le nouvel "Operating System" des entreprises de nouvelle génération.

Notre vision de la qualité de l'expérience s'étend également à nos clients pour lesquels nous avons conçu des parcours d'onboarding et d'accompagnement uniques pour leur permettre d'atteindre leurs objectifs dans les meilleures conditions.

Cette proximité, qui passe par une écoute et un dialogue permanent avec nos utilisateurs et clients, est également un élément clef de notre différenciation.

Un dernier point à ajouter qui vous semble essentiel ?

Les signes de croissance d'une entreprise sont multiples, et il y en a un qui nous tient particulièrement à cœur chez Talkspirit, c'est l'évolution de notre équipe !

Aujourd'hui, Talkspirit c'est 45 collaborateurs, des femmes et des hommes qui veulent développer les plus efficaces et pertinents outils collaboratifs et de gouvernance à destination des organisations.

Nous avons déjà accueilli 10 nouveaux profils depuis le début de l'année et nous ambitionnons d'en recruter une autre dizaine d'ici la fin de 2024.

> Par Sabine Terrey

Top 7 du Baromètre de la cybersécurité 2023

Entre prise de conscience croissante mais hétérogène, découvrez le Top 7 de la cybersécurité 2023.

Meilleure compréhension des enjeux de la cybersécurité, niveau de résilience numérique et évolution vers une protection plus efficace, voici les objectifs du Baromètre Docaposte et Cyblex Consulting. « *Les résultats et les grands enseignements du baromètre nous permettent de mieux appréhender le degré de maturité des entreprises et organisations publiques face aux risques cyber afin de les accompagner au mieux dans le renforcement de leur cyber-résilience pour qu'elles se concentrent sur leur cœur de métier.* » explique **Olivier Vallet**, Président directeur général de Docaposte

1 entreprise sur 5 affirme avoir déjà subi une cyberattaque

On observe de fortes disparités en fonction de la taille des entreprises et des impacts hétérogènes.

Les petites et moyennes entreprises sont confrontées à des contraintes budgétaires

- 82 % des PME et 78 % des TPE accordent moins de 10 K€ par an au budget dédié à la sécurité informatique

En comparaison, 1/3 des entreprises au global affirme que celui-ci est en hausse.

31% se considèrent comme des cibles potentielles

Avec comme première crainte le vol de données, même si les efforts sur le terrain sont importants :

- renforcement de la gestion des mots de passe - 81 %
- mises à jour régulières des logiciels - 79 %
- déploiement de dispositifs de sécurisation des postes de travail - 78).

Mais l'efficacité des mesures est perçue différemment selon la taille de l'entreprise : plus elle est petite, moins elle se sent menacée.

64 % pensent faire suffisamment d'efforts pour réduire les risques cyber

Toutefois il existe de fortes disparités budgétaires en fonction de la taille des organisations.

La principale crainte est la perte des données.

62% mentionnent cet élément

Non confiance dans les mesures pour se protéger des risques cyber

1/3 n'ont pas confiance dans les mesures de protection prises par leur entreprise

L'usage de technologies souveraines, sujet important pour 1/3 seulement

On note une prise de conscience des enjeux liés à l'autonomie stratégique française et européenne. Ce sujet est assez important pour influencer l'usage de systèmes de cybersécurité souverains (français ou européen) dans le choix (deux fois plus nombreux que ceux qui le jugent peu important).

66 % n'appliquent pas les pratiques

Pour atteindre le niveau essentiel préconisé par l'ANSSI. Près de 2/3 pourraient pourtant basculer au niveau supérieur avec un bon accompagnement et une mise en perspective du degré d'importance des mesures à mettre en place.

« *Ce baromètre se positionne en complément des différentes études, sondages et rapports décrivant l'évolution ou l'état de l'art en matière de cybersécurité. L'originalité de notre indicateur réside dans la volonté d'offrir une photographie annuelle de la perception et des conditions de gestion des cyber-risques de la part des acteurs de l'économie française.* » conclut **Christophe Vendran**, Directeur général de Cyblex Consulting

Source Docaposte et Cyblex Consulting. 1ère édition du baromètre annuel de la cybersécurité - Plus de 500 décideurs français - TPE, PME, grands comptes, structures publiques et tous les secteurs d'activités.

Vulnerability Operation Center
CONCEPTS, MISE EN ŒUVRE ET EXPLOITATION

> Par Sylvain Cortes

Définition du Vulnerability Operation Center (VOC)

Une organisation, pas un outil

Un VOC est une unité spécialisée au sein d'une organisation qui sera responsable de l'identification, de l'évaluation, de la gestion et de l'atténuation des vulnérabilités dans les systèmes, les réseaux et les logiciels.

Il est important de spécifier que nous n'allons pas évoquer ici un outil, mais plutôt une organisation dans l'organisation. Le VOC est un concept, une façon de travailler et non un logiciel, bien sûr, vous aurez besoin de composants techniques pour déployer votre VOC, mais le VOC représente avant tout une méthodologie pour gagner en visibilité, en sécurité et en efficacité.

Quels sont les objectifs du VOC ?

L'objectif global du VOC est très simple : permettre une exécution professionnelle et organisée du cycle de gestion des vulnérabilités dans une organisation.

Pour ce, le VOC surveille généralement diverses sources d'information en liaison avec les failles de sécurité présentes, telles que les résultats de scan, les résultats de Pentest, les renseignements de sources ouvertes, les flux de CTI privés, les bulletins de sécurité, etc.

Dès lors, il se donne pour mission de coordonner les efforts afin de remédier efficacement les vulnérabilités présentes dans l'organisation. Sa philosophie générale est d'identifier de manière proactive les faiblesses potentielles et de prendre les mesures nécessaires pour prévenir les failles de sécurité ou en atténuer l'impact afin de garantir le niveau de sécurité nécessaire au bon fonctionnement de l'organisation.

Généralement, les organisations qui déploient un VOC le font de manière progressive, cela leur permet de se structurer petit à petit en couvrant trois besoins primaires :

(1) Centraliser toutes les informations sur les vulnérabilités présentes dans l'organisation, et ce quelle que soit la source. Il faudra alors que le VOC « aspire » des données depuis plusieurs référentiels, la source de données principale restant généralement les résultats de scan – mais ceci n'est pas exhaustif ! il sera tout à fait possible de connecter au VOC d'autres pratiques en liaison avec les vulnérabilités comme les résultats de Pentest ou même les résultats de BugBounty

(2) Une fois que toutes les données sont dans le puit de données du VOC, il sera alors possible non seulement d'évaluer l'ensemble du stock mais surtout de définir des règles pour prioriser le traitement et les mesures correctives ou dérogatoires. Cela passe généralement par une méthode d'évaluation par les risques car c'est la seule qui permettra de comparer par exemple une mauvaise configuration Active Directory, une

CVE présente dans le CISA KEV ou encore un code contenant des failles

(3) Finalement, quand les règles de priorisation seront établies et permettront de définir clairement ce qu'il faut corriger et à quelle échéance, le VOC devra synchroniser les actions entre l'équipe sécurité et les équipes en charge de la remédiation (souvent les équipes systèmes ou applicatives)

La pyramide des missions du VOC

Une prise de conscience et un virage à prendre

L'échec du SOC

Quand j'évoque avec un professionnel de la sécurité les VOCs et leurs missions, vient très souvent un « *contre argument fallacieux* » de leur part : « *Mais, ce que tu me décris, c'est la mission du SOC !* »

Et bien NON, justement, et c'est bien là le problème !

Depuis l'apparition des SOCs il y a quelques dizaines d'années, nous n'avons cessé de rajouter des sources d'information et surtout des missions au SOC ; nous atteignons maintenant un point de rupture, les équipes SOC ne peuvent plus gérer l'ensemble des tâches confiées.

Il est très simple d'en faire la preuve :

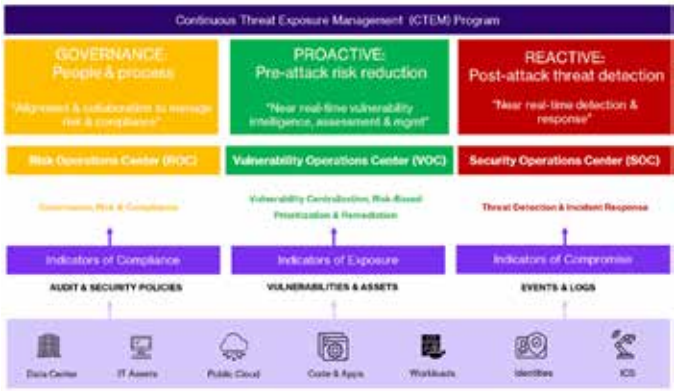
(a) Les attaques réussies se multiplient

(b) Le stock de vulnérabilités non-traitées ne cesse de grossir

(c) Demandez à une équipe SOC quel est le plan de priorisation sur la remédiation du stock de vulnérabilités ou des statistiques sur le stock global, vous entendrez les mouches voler…

En effet, nous tentons depuis des dizaines d'années de faire traiter les vulnérabilités par le SOC, mais cela ne fonctionne pas. La raison est finalement plutôt simple : ce n'est pas la mission du SOC.

Le SOC doit gérer des évènements/alertes, qui deviendront peut être des incidents – selon les organisations, le SOC assurera éventuellement la partie investigation ou passera le relais au CERT/CSIRT. Sa mission est réactive, il réagit en fonction d'un évènement ou d'une information.



Composants organisationnels d'un programme CTEM

De plus, les SOCs croulent littéralement sous les informations, faux positifs, faux négatifs et sont soumis à une pression constante. Dans ce genre de situation, la mission de prévention reste toujours en bas de la liste des choses à réaliser, c'est la raison principale de la croissance constante du stock de vulnérabilités, elles ne sont pas traitées convenablement car ce traitement n'est pas la priorité des équipes SOC.

Baromètre du CESIN

La meilleure preuve de cette prise de conscience provient des RSSI eux-mêmes, en 2023, le CESIN réalisait un sondage sur les priorités des RSSIs (Sondage OpinionWay) – le résultat est sans appel, 50% des RSSIs français déclaraient utiliser ou déployer un VOC dans leur organisation.

Sondage OpinionWay – CESIN - 2023

Le VOC, une équipe dédiée

Le déploiement d'un VOC nécessite une équipe dédiée, encore une fois, ne tentez pas d'utiliser du temps partagé avec votre équipe SOC pour remplir les missions du VOC, cela ne fonctionne pas.

De plus, les SOCs croulent littéralement sous les informations, faux positifs, faux négatifs et sont soumis à une pression constante.

Les professionnels présents au sein du VOC réaliseront principalement les tâches suivantes :

- Assurer la connexion avec les nouvelles sources de données quand elles se présentent (par exemple, parce que vous avez déployé un nouveau type de scanner de vulnérabilités)

- Analyser les vulnérabilités présentes
- Réaliser une veille en vulnérabilités
- Définir des arbres de décisions SSVC pour le tri automatique vers des stratégies de remédiation
- Créer des groupes de remédiation statiques pour des campagnes de crise (exemple Log4Shell)
- Suivre les tickets qui ont été générés automatiquement ou manuellement depuis l'outil de Cockpit VOC
- Définir et surveiller les SLAs de remédiation
- Suivre les indicateurs de régression de findings (typiquement une finding qui a été déclarée comme corrigée par l'équipe applicative mais qui est à nouveau détectée par le scanner)
- Créer des rapports statistiques sur l'évolution du stock de vulnérabilités
- Etc.

Pour exécuter les missions du VOC vous aurez donc principalement besoin d'analystes et d'une paire de managers pour orchestrer le tout. Les managers VOC recrutés devront savoir communiquer, car il faudra éduquer les différentes équipes de production sur les missions et objectifs du VOC.

Le déploiement d'un VOC nécessite une équipe dédiée.

Mise en œuvre d'un VOC

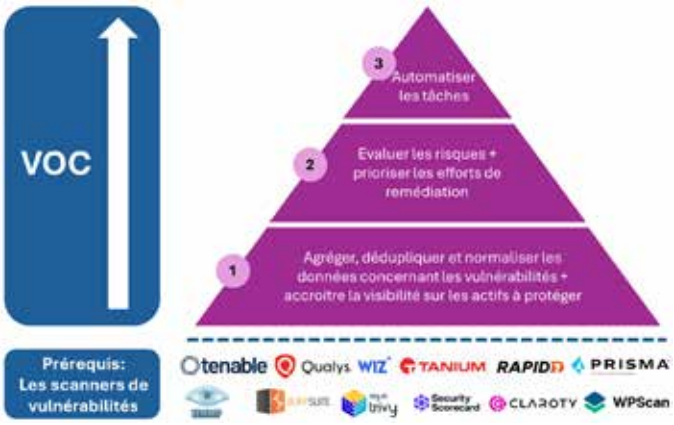
Les prérequis

Pour mettre en œuvre un VOC, vous aurez besoin absolument :

- *De scanners de vulnérabilités :* en effet, les résultats de scan sont la source première d'information pour un VOC – nulle crainte, vous pouvez aussi utiliser des scanners open-source si vous le désirez
- *D'un outil de type « Cockpit VOC »* - comme le SIEM est l'outil principal du SOC, le VOC possède son propre outillage, communément appelé « Cockpit VOC »
- *D'une source de CTI* – parfois le Cockpit VOC propose déjà une source de CTI, dans ce cas, pas besoin d'acheter les services d'un flux dédié

Certains éléments sont optionnels :

- *Informations sur les actifs à intégrer dans le cockpit* – cette partie n'est pas obligatoire, en effet, les scanners de vulnérabilités remontent de facto les informations liées aux actifs qui portent les vulnérabilités – néanmoins vous désirerez peut être enrichir ces données avec vos propres informations provenant d'une CMDB ou d'une analyse de risque
- *Des sources de CTI additionnelles* – à nouveau, un seul flux est nécessaire, mais si vous êtes mature dans votre processus de veille, peut être voudrez vous associer plusieurs sources de CTI dans votre Cockpit VOC pour améliorer votre jeu de données
- *Connexion d'un système ITSM pour attribution des tickets.* Même si cet élément est considéré comme optionnel, il peut s'avérer extrêmement important si votre objectif est d'assurer un liant efficace entre l'équipe sécurité et les équipes de remédiation



Les scanners sont un prérequis à l'implémentation d'un VOC

« Be cloud or not to be cloud ? »

Certains Cockpits VOC ne sont accessibles que sous la forme d'un service cloud. Selon vos contraintes de conformité ou de sécurité, vous ne pourrez peut-être pas envoyer les données qui concernent l'ensemble de vos vulnérabilités dans un service cloud. Dans ce cas, sélectionnez un cockpit qui peut fonctionner en mode local.

De plus, certains Cockpits VOC possèdent des capacités hybrides et peuvent fonctionner en mode service cloud mais aussi en mode local.

Exploitation

Si vous préparez bien votre projet, l'exploitation au quotidien du service de VOC ne représentera pas une tâche démesurée. Mais attention, la partie process est importante, si vous négligez cet aspect, vous ne serez efficace ni dans vos tâches de priorisation, ni dans l'automatisation des actions.

Définir un process global clair et accepté de tous

Vous devez à cette étape définir quel sera le cycle complet de traitement des vulnérabilités. Privilégiez les process simples et qui pourront être appliqués par tout le monde.

Il est important de communiquer auprès de toutes les parties prenantes et principalement auprès des équipes de production qui seront en charge des missions de remédiation. N'hésitez pas à organiser des ateliers, et à refaire une passe mensuellement pendant les six premiers mois du lancement d'un service VOC.

LE DROIT À LA DÉCONNEXION : UN ENJEU RH

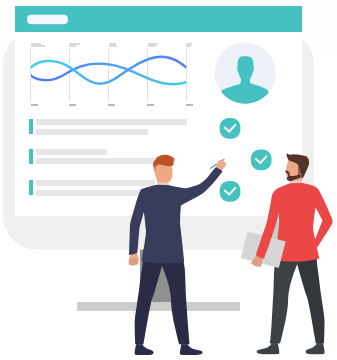
DANS UN MONDE RÉGI PAR L'IMMÉDIATETÉ,
LA DÉCONNEXION N'EST PLUS UNE OPTION, MAIS UN DROIT.

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

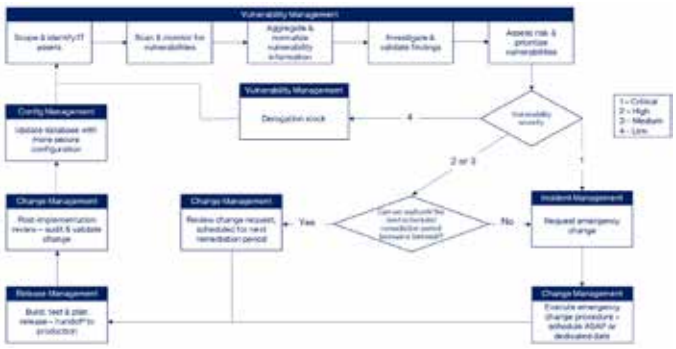
UNE SOLUTION DE SENSIBILISATION, D'ALERTE ET DE PRÉVENTION

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

Découvrez la solution Promodag Reports

Promodag

www.promodag.fr



Exemple de process global géré par un VOC

Il est primordial que chaque musicien joue sa partition, assurez-vous que chaque acteur ait bien compris sa mission au sein du cycle de gestion des vulnérabilités.

Définissez des arbres de décision SSVC

Il existe de multiples méthodologies permettant de prioriser les vulnérabilités et leur traitement. Je conseille vivement d'utiliser la méthodologie des arbres SSVC définie par le CISA (Voir : https://www.cisa.gov/stakeholder-specific-vulnerability-categorization-ssvc).

En effet, cette méthode possède l'avantage de faire un lien pragmatique entre l'évaluation des risques et vos capacités de remédiation.

Trois éléments doivent guider la création de l'arbre de décision SSVC :

1. **La capacité de traitement**, c'est-à-dire le nombre de personnes pouvant être mobilisées régulièrement pour mener des actions correctives.
2. **L'appétence de l'organisation pour le risque**, c'est-à-dire si l'organisation peut ou non prendre des risques, et à quelle échelle.
3. **Les réglementations applicables à l'organisation**, c'est-à-dire que certaines organisations sont soumises à des réglementations qui exigent un certain niveau de sécurité et que l'organisation doit fournir une capacité de traitement adéquate sous peine d'amendes ou de radiation.

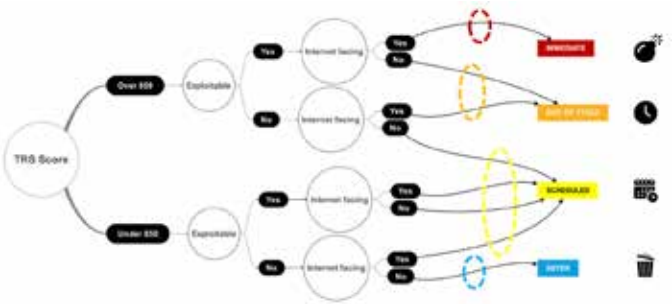
Premièrement, commencez par définir vos pools de remédiation dans lesquels vos findings viendront se ranger ; j'en conseille 4 :

- *IMMEDIATE (Sous 48 heures) :* Les findings dans ce pool sont considérées comme extrêmement dangereuses et doivent être corrigées dans un délai extrêmement court. En général, il s'agit de vulnérabilités qui peuvent être exploitées et utilisées activement par des attaquants - et le plus souvent, il s'agit de findings portées par des actifs exposés sur Internet et directement accessibles par des attaquants.
- *OUT OF CYCLE (Sous 1 à 4 semaines)* : Ces findings sont considérées comme dangereuses et le traitement ne peut pas attendre la prochaine période de remédiation planifiée. Toutefois, il n'est pas nécessaire de procéder à une correction immédiate (i.e. sous 48 heures). La planification dépend de l'urgence du traitement et de l'évaluation des risques associés, mais elle se situe généralement entre une semaine et quatre semaines à compter de la date de l'évaluation des risques.
- *SCHEDULED :* (Une à deux fois dans l'année - dates variables en fonction de l'organisation) : Une période de remédiation programmée existe dans l'organisation. Il s'agit souvent d'une période de 2 à 3 jours programmée à l'avance. La programmation de cette période dépend de l'activité de l'organisation et est généralement programmée pendant les périodes de moindre activité. Pendant cette période, les usagers savent à l'avance que les systèmes seront corrigés et que le service fourni par ces systèmes sera potentiellement perturbé.
- *DEFER :* le pool des findings qui sont mises de côté, oubliées, car ne représentent aucun risque.

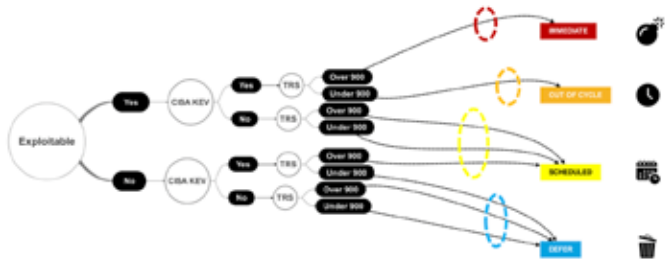
Deuxièmement, définissez vos critères d'évaluation – de nombreux critères peuvent être utilisés pour la création de vos arbres de décision, par exemple :

- Score CVSS Base (la vulnérabilité elle-même)
- Score CVSS Environnemental (prise en compte des caractéristiques de l'actif qui porte les vulnérabilités)
- Score de risque « propriétaire » (mais il faut un score applicable à tous les types de vulnérabilités) – Exemple : Hackuity TRS
- Vulnérabilité Exploitable ou pas
- Vulnérabilité exploitée ou pas par les attaquants
- Situation physique de l'actif : connecté à Internet ou pas
- La vulnérabilité fait partie du catalogue CISA KEV ou pas
- Score EPSS (évaluation de la probabilité d'exploitation par les attaquants dans les 30 prochains jours)
- Critère CIA de l'actif : niveaux attendus de Confidentialité, d'Intégrité et de Disponibilité
- Etc.

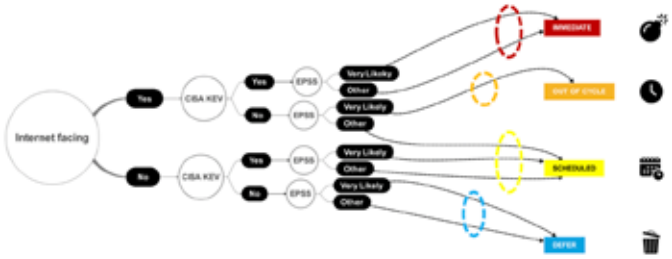
Troisièmement, créez vos arbres – chaque branche de l'arbre sert à évaluer des critères pour ranger automatiquement les vulnérabilités (en fait les findings) dans les bons pools de remédiation – voici quelques exemples :



Exemple A d'un arbre de décision SSVC



Exemple B d'un arbre de décision SSVC



Exemple C d'un arbre de décision SSVC

Rappelez-vous qu'il n'y a pas de bon ou de mauvais critère, les critères choisis dépendent de votre organisation, de ses contraintes et de ses objectifs.

Important : Les arbres peuvent évoluer avec le temps, en effet, il est envisageable que la première version de votre arbre de décision attribuera trop de findings dans le pool IMMEDIATE, et vos équipes de production ne pourront pas suivre. Il faudra alors adapter votre arbre pour qu'il soit compatible avec vos capacités de remédiation réelles et pas avec vos envies... Il est très important que les temporalités associées aux différents pools soient réalistes.

Un investissement stratégique

En conclusion, le Vulnerability Operation Center (VOC) représente un élément crucial dans la stratégie de cybersécurité des entreprises modernes. En centralisant la détection, l'analyse et la gestion des vulnérabilités, un VOC permet non seulement de réagir rapidement aux menaces, mais aussi de les anticiper et de les prévenir. Grâce à des processus rigoureux, un outillage adéquat et une équipe dédiée d'experts en vulnérabilités, le VOC assure une surveillance continue et proactive de l'environnement numérique de l'organisation.

Le VOC représente un élément crucial dans la stratégie de cybersécurité des entreprises modernes.

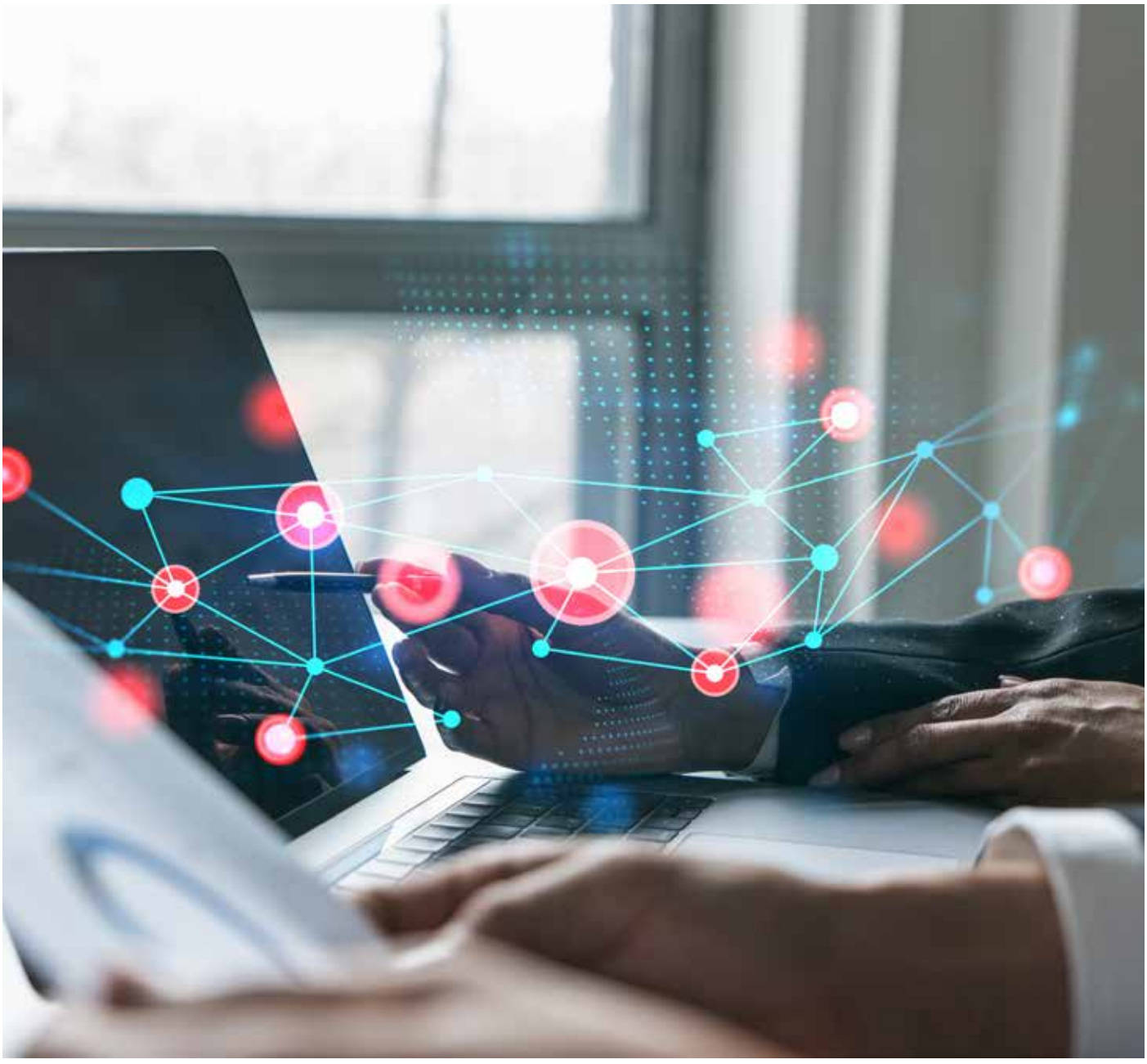
La mise en place d'un VOC constitue un investissement stratégique qui renforce la résilience de l'entreprise face aux cyberattaques. Il contribue à protéger les actifs numériques, à préserver la confiance des partenaires et à garantir la continuité des opérations.

En fin de compte, un VOC n'est pas seulement une réponse aux vulnérabilités, mais une composante essentielle d'une posture de sécurité globale et dynamique.

> Par Sylvain Cortes, MVP, co-fondateur des Identity Days

SUPERVISION OU OBSERVABILITÉ,
QUELLES RECOMMANDATIONS ?

Le pari en ce moment est d'arriver à intéresser les décideurs en ne parlant pas... d'IA.



Car oui, c'est une évolution majeure et il est difficile pour les entreprises de ne pas se poser la question de savoir ce qu'elles pourraient bien faire avec ce nouveau type de service. Les promesses sont nombreuses, et, sans que je sois expert en la matière, il me semble que les cas d'usages « utiles » sont également nombreux.

Mais, bien heureusement, il y a d'autres sujets intéressants et utiles sur le Cloud, et plus spécifiquement sur le Cloud Azure. Par exemple (et certainement qu'un jour l'IA permettra d'affiner ce sujet), l'observabilité de ses ressources.

L'observabilité ou supervision, c'est un sujet assez vaste mais indispensable.

salon des maires et des collectivités locales

ACCÉLÉRATION.

+50 000 visiteurs

1 300 exposants

400 prises de parole

PRIX DE L'INNOVATION TERRITORIALE avec 8 catégories de prix

9 secteurs d'exposition

2 salons tenus conjointement

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

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

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

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

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

Tenue conjointe avec SALON DES SPORTS — SALON DE LA BIODIVERSITÉ ET DU GÉNIE ÉCOLOGIQUE

Organisé par infoprodigital — AMF

On démarre par la collecte des informations, ce qui doit être consigné, avec quel niveau de détails et pour quels types de ressources. Puis ces données collectées sont stockées, majoritairement dans des puits de logs (log analytics), même si ce n'est pas forcément la seule destination possible.

Pour terminer, ces données sont consommées. Soit à des fins d'analyse, elles sont donc exposées dans des dashboards ou des workbooks pour visualisation. Mais sont également utilisées pour lancer des actions lorsqu'un métrique ou une information qui ne sont pas jugés conformes (par exemple, des métriques de CPU, des erreurs applicatives ...etc) deviennent une alerte. Et cette alerte va déclencher une ou plusieurs actions. D'un simple mail ou SMS pour information à une action de remédiation orchestrée par d'autres services Azure. Comme un compte d'automatisation, Azure Automation.

Pour aller un peu plus loin avec cette introduction, on peut séparer deux grandes familles dans cette notion de surveillance.

Il y a tout ce qui touche à la ressource elle-même, ses métriques, son bon fonctionnement et les dysfonctionnements éventuels. Tout ce qui est lié, à mon sens, à son cycle de vie.

Puis, il y a aussi tout ce qui va toucher un peu plus directement à la sécurité de la ressource ou du service. Ce ne sont pas exactement les mêmes tableaux de bord, pas la même urgence en cas de traitement. Et souvent, pas les mêmes équipes de support et d'analyse.

Si les concepts de base de cette observabilité sont plutôt clairs, la mise en œuvre demande réflexion. Il y a beaucoup de finesse dans l'établissement d'une architecture cohérente.

Mise en œuvre

Il faut se poser 3 questions. Enfin un peu plus, mais les trois premières vont définir les grandes lignes de ce que va être l'architecture à mettre en œuvre.

- **L'étendue générale :** elle peut être uniquement Azure ou venir intégrer des ressources On-Premises et / ou d'autres fournisseurs de Cloud.
- **L'étendue d'environnement :** c'est la définition du niveau des environnements. On n'exploite pas tous les environnements de la même manière. C'est-à-dire que l'on ne donne pas à son développement ou ses bacs à sable la même importance qu'à sa production.
- **L'étendue des responsabilités :** cette notion notamment va permettre de construire l'architecture de ses puits de logs.

Les quelques exemples et recommandations qui vont suivre vont porter sur une étendue générale Azure mais sont assez faciles à transcrire et à adapter pour des environnements hybrides ou multi fournisseurs.

L'étendue d'environnement est intéressante à travailler. Toute la réflexion doit tourner autour de ce qui doit être surveillé et ce qui ne doit pas l'être. Et plus exactement, ce que l'on souhaite ajouter comme informations selon que l'environnement soit de Développement ou de Production.

Le réflexe est souvent de se dire que tout doit être aligné et qu'il faut tout consigner parce que cela « pourrait » servir. Mais, cela ne présente que très peu d'intérêt de superviser un service de test / dev au même niveau qu'un service de production.

Intérêt faible, mais surcoût important. Car plus la collecte d'informations est étendue, plus les volumes d'ingestion dans les comptes de stockage ou les puits de logs sont importants, ce qui entraine un surcoût conséquent que je ne pense ni utile, ni nécessaire.

Une pratique courante et plus équilibrée est de conserver par défaut les logs de la plateforme Azure pour tous les environnements. Les logs de plateforme, c'est tout ce qu'il se passe côté EntraID, des logs d'abonnement qui informent sur le fonctionnement, la gestion d'un abonnement Azure et enfin, les données sur le fonctionnement d'une ressource Azure (arrêt, démarrage par exemple).

Pour les logs de ressources, il y a aussi des logs et métriques par défaut. Mais en complément, pour une supervision plus complète, d'autres logs plus granulaires qu'il est possible d'ajouter directement sur les ressources.

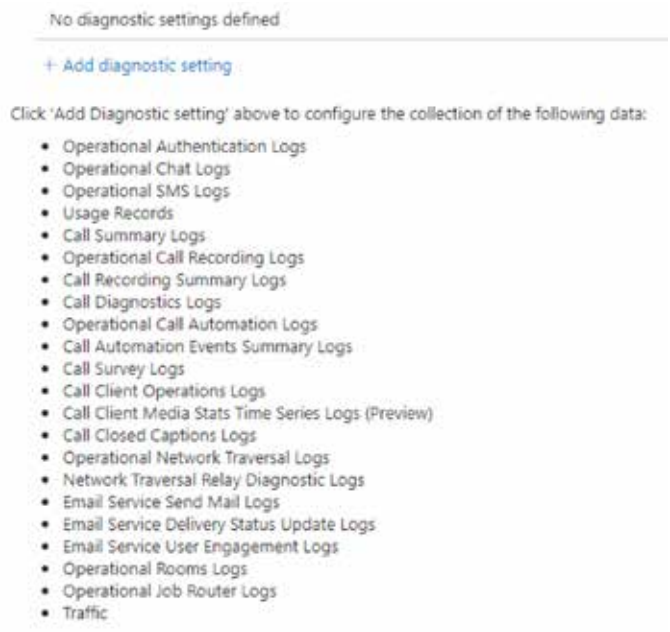
Si ces ressources sont dans des environnements de développement, on conserve les logs par défaut. Mais, il faut étendre avec l'ajout de logs plus fins pour les environnements de qualification et de production. En faisant là aussi un choix différent et en ne choisissant pas systématiquement des logs complets.

Si les concepts de base de cette observabilité sont plutôt clairs, la mise en œuvre demande réflexion.

Par exemple, quelques logs complémentaires pour les environnements de qualification et la production, et pour quelques ressources de production au cœur de l'activité de l'entreprise, les logs les plus complets possibles. Pour résumer, deux ou trois niveaux de logs selon le type d'environnement.

L'adage « qui peut le plus, peut le moins » n'est pas une bonne solution même si elle parait séduisante sur le papier.

Voilà par exemple les logs disponibles pour un service de communication. Ce sont 22 points de collectes supplémentaires que l'on peut sélectionner un à un. Tout ici ne sera pas utile selon l'environnement. C'est donc ce travail préparatoire qu'il faut réaliser.

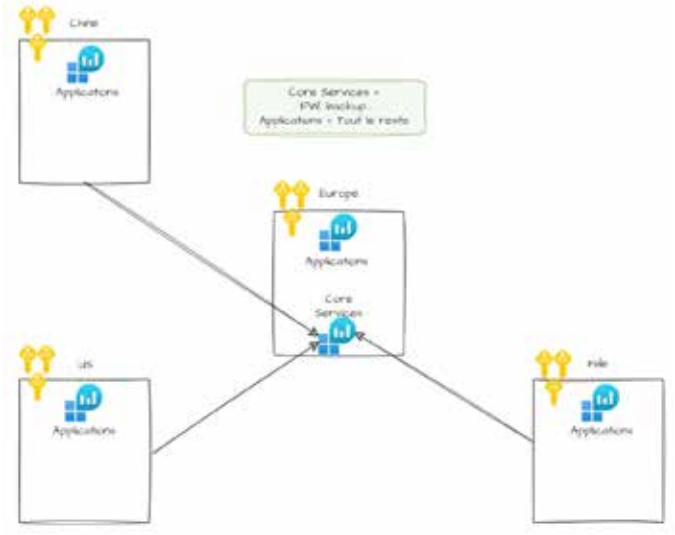


En parallèle, une réflexion est à mener sur l'étendue de responsabilités et les process d'observabilité. Cela permettra de positionner les puits de logs au mieux et de décider de la meilleure façon de les consolider. En effet, la consolidation est essentielle. Il ne faut pas « en mettre de partout ». C'est le meilleur moyen de passer à côté de ce qui est important.

Et cela devient rapidement inexploitable :

- Parce que les diagnostiques des ressources ne sont pas attachés de manière homogène si vous devez choisir entre 30 puits de logs.
- Parce que les requêtes interactives et les requêtes de workbooks vont tomber en erreur lorsqu'elles doivent croiser les données de trop de puits de logs (ou à minima, vont prendre beaucoup trop de temps).
- Parce que consolider les puits de données permet de profiter de remise tarifaire à partir d'un certain volume d'ingestion jour. 10 puits à 10 Go d'ingestion ne sont pas éligibles aux remises tarifaire, 1 puit à 100 Go va en revanche permettre d'obtenir une réduction.

Bien démarrer, c'est choisir de déployer un log analytics par paire de région ou par continent. Et toutes les ressources pointent dessus. On évite tout de même un seul analytics sur des environnements répartis sur plusieurs régions pour ne pas créer du trafic entre les régions.



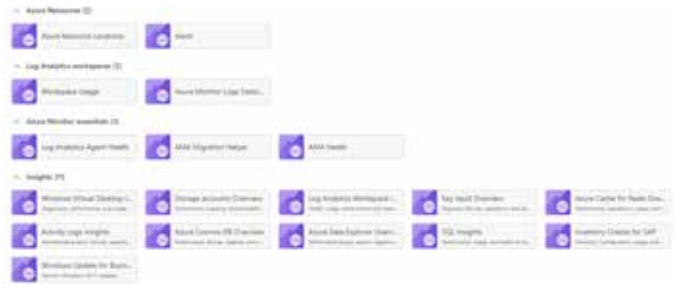
Et on complète cette architecture de base, il faut créer quelques puits dédiés comme par exemple :

- Les évènements de sécurité qui seront exploités par un plus faible nombre de personnes.
- Les évènements de type Core Azure que l'on trouve sur le schéma ci-dessus (Azure Firewall, Azure Backup ...etc.).
- Les puits de logs exploités par des sociétés partenaires mais externes à l'entreprise que l'on peut dédier au partenaire.

En parallèle, une réflexion est à mener sur l'étendue de responsabilités et les process d'observabilité.

C'est ce que je définis par le scope de responsabilité. Mais la règle de base à garder en tête est bien de limiter au maximum le nombre d'analytics.

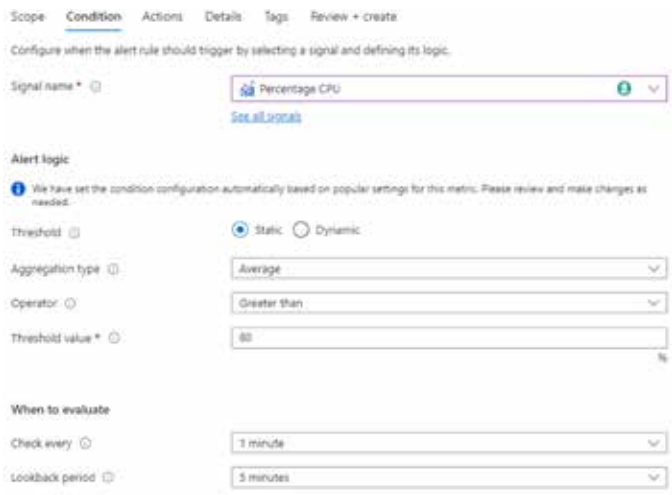
Pour la couche d'exposition des données, utilisez prioritairement les Workbooks disponibles dans le portail. Les possibilités sont plus étendues que les Dashboards. Ils sont bien cachés et se trouvent dans la partie Monitor du portail. Il y en a une trentaine, et vous en trouverez également directement sur le menu de quelques ressources.



Si vraiment les besoins de l'entreprise ne sont pas couverts, il faut écrire vos propres Workbooks.

En évitant de se lancer dans un projet trop ambitieux… Je n'ai que trop peu de « ça marche » à partager sur ce point particulier. Même si les cas d'usages sont bien définis, même si les demandes de workbooks personnalisés sont bien cadrées par les équipes, le temps passé à cette tâche est rarement récompensé.

Dernière étape une fois que les données sont collectées et qu'elles sont exposées, utilisez certaines remontées pour créer des alertes. Une alerte, c'est un métrique ou un ensemble de métriques que vous jugez comme étant anormaux et qui prédisent un dysfonctionnement applicatif.



Si cette condition est remplie, alors l'alerte peut déclencher une suite d'actions. Par exemple, des actions de remédiation automatique. Ou simplement un mail d'information, voire l'ouverture d'un ticket. Dans l'exemple ci-dessus, un % de CPU, mais ce peut être également une requête personnalisée lancée sur un puits de logs avec un ensemble de conditions.

On réserve donc alertes et remédiations aux applications pour lesquelles l'impact d'un dysfonctionnement est fort !

Et l'on reparle scope d'environnement. Avec une réflexion équivalente à celle qui a mené au choix du bon niveau de diagnostic. On n'alerte pas pour tout et dans tous les sens ! Si un environnement de production doit être en ligne 100 % du temps, quelle valeur donner à une alerte qui relancerait un service qu'un utilisateur vient de stopper volontairement dans un environnement de développement ?

Pour que cela fonctionne, derrière une alerte, il y a un process de résolution ou de remédiation. Et c'est à établir dès le départ.

Rien ne sert de tout récupérer s'il n'est pas possible de déclencher des actions dans la foulée. On réserve donc alertes et remédiations aux applications pour lesquelles l'impact d'un dysfonctionnement est fort !

Un bon point de départ en 3 étapes

1 / Même si l'idée de tout consigner pour ne manquer de rien est séduisante sur le papier, elle est loin d'être idéale dans la pratique. Elle engendre des surcoûts importants et se révèle globalement inutile sur certains environnements.

2 / Les puits de logs analytics sont des éléments centraux, qu'il faut essayer de consolider afin d'avoir un environnement homogène et facile à exploiter

3 / Une alerte = un process. Il ne sert à rien d'alerter si les actions correctives ne sont pas connues.

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

IA & Dirigeants : innovation et concurrence

La création de valeur attendue n'est pas à la hauteur des promesses de l'IA en l'absence d'une planification adéquate.

Les promesses de l'IA semblent freinées par la technologie, les processus et les compétences.

Adopter une stratégie solide

84 % des dirigeants anticipent des bénéfices organisationnels massifs de l'IA. Ils retiennent trois principaux domaines à fort impact

- l'innovation en matière de produits et de services
- l'amélioration de la disponibilité des données internes et externes
- la réduction des coûts et l'augmentation des marges

Si 90 % (82 % au global) des décideurs en France reconnaissent une forte pression pour adopter rapidement l'IA, ils restent préoccupés par le manque de planification, de mise en œuvre ou de communication.

A noter ! Un tiers des entreprises ne sont pas passées au cloud. L'entreprise n'est donc pas préparée et il est peu probable qu'elle soit en mesure d'étendre l'IA à ses activités.

Selon IFS, « *une stratégie industrielle robuste en matière d'IA nécessite une combinaison puissante de cloud, de données, de processus et de compétences* ».

Selon 90 % en France, l'absence d'approche stratégique révèle un manque de compétences en interne pour adopter l'IA avec succès. Christian Pedersen, Chief Product Officer d'IFS explique « *Il est révélateur que l'on s'attende à ce que l'IA réduise considérablement les coûts et augmente les marges, mais l'absence de stratégie solide signifie que la plupart des entreprises ne sont pas suffisamment qualifiées et préparées pour réaliser ces ambitions* ».

Planifier

Entre le déficit de compétences et le manque de stratégie claire, les entreprises hésitent. Un cinquième (global) et 13 % (France) en sont à la phase de recherche, avec des tests non contrôlés, et 5 % (3 % France) n'ont pas d'approche coordonnée.

Malgré cela, l'IA pourrait faire une différence significative pour l'entreprise d'ici un à deux ans (55 % France - 47 % global), et un quart (24 % global et 30 % France) d'ici un an.

En France, l'impact le plus important concernerait

- l'innovation

avec de nouveaux produits et services - 16 %

- la croissance et la prise de décision

en matière de modèle d'entreprise - 24 %

- l'autonomisation des personnes et la fidélisation des talents
- l'expérience et le service à la clientèle

Préparer les données

Le volume et la qualité des données sont essentiels à la réussite des applications d'IA. Quelles sont les priorités ?

- Disposer de données en temps réel pour la réussite des projets d'IA (86 % global et 95 % France)

Mais moins d'un quart ont achevé la mise en place de l'infrastructure de données.

- Disposer de données structurées et d'une partie de données non structurées.

« *Le manque de maturité au niveau de la couche de l'infrastructure des données doit être abordé dans le cadre d'une stratégie globale d'IA, sans quoi l'IA ne sera jamais la solution miracle qui permettra de dynamiser l'entreprise* » Le potentiel de l'IA est énorme « *si les dirigeants et les entreprises peuvent combiner vision, stratégie, technologie et compétences* ».

Source Etude IFS & Censuswide – Industrial AI: the new frontier for productivity, innovation and competition - 1709 décideurs/Présidents/SVP/Directeurs - Royaume-Uni, États-Unis, Canada, Allemagne, France, Émirats arabes unis, Norvège, Japon, Australie, Suède, Danemark et Finlande – Entre le 06.03.2024 et le 27.03.2024.

Développer les compétences cyber
SUR TOUT LE TERRITOIRE EST PRIORITAIRE

Stéphanie Buscayret n'est pas uniquement Chief Information Security Officer chez Latécoère, elle a aussi reçu fin 2023 le prestigieux prix Femme Professionnelle de la Cyber France lors de l'évènement Trophée de la Femme Cyber 2023 organisé par le CEFCYS (Cercle des Femmes de la Cyber Sécurité) et elle est réserviste citoyenne. Logique d'écosystème, communauté et initiatives cyber, mais aussi accompagnement cyber en région, autant de sujets qu'elle défend !

Cette experte talentueuse de la cybersécurité dans l'aéronautique nous livre sa vision de cet univers très passionnant, ses attentes et ses combats pour faire bouger les lignes !

Depuis plus de 20 ans dans cet environnement, et des débuts notamment en industrie pharmaceutique, Stéphanie Buscayret est formelle, « *en 2007, l'exercice en tant que RSSI était plutôt solitaire, car seule à porter le sujet, avec pas ou peu d'échanges entre pairs* ». Si les épisodes de ransomwares sont plutôt exceptionnels en 2009 (Conficker, malware systémique), aujourd'hui les choses ont radicalement changé « *nous sommes en permanence sous les feux des attaques* ».

Une vraie logique d'écosystème

Dès son entrée en aéronautique, la pratique change fondamentalement avec la présence de pairs « *l'industrie aéronautique ayant un mode de fonctionnement en supply chain, donneurs d'ordre et chaine de suppliers. Je côtoie alors plusieurs RSSI aux mêmes problématiques, exigences des clients, exercices de démonstration de compliance, évolution croissante de la menace non suivie de la même courbe d'évolution au niveau des ressources financières et humaines. Ainsi, avec les mêmes pressions de l'environnement, je découvre une vraie logique d'écosystème.* ».

Cette logique est bien comprise par les donneurs d'ordre subissant déjà de fortes attaques. « *En 2014, si la sécurisation de leurs SI apporte une diminution drastique des attaques, elle déplace les attaques sur leurs filiales. La sécurisation des filiales est enclenchée, mais les attaques se dirigent vers les fournisseurs moins bien armés* ».

Alors, comment sécuriser toute la supply chain en

respectant le principe de non-ingérence et avec une supply chain aéronautique rassemblant plus de 2500 fournisseurs pour l'Europe !

Maturité cyber de la supply chain aéronautique

Face à ce constat, le consortium BoostAeroSpace (joint-venture Safran Airbus, Thales, Dassault Aviation) active déjà les sujets de numérisation (dématérialisation de la chaine de commandes et de factures) et déploie des services de mise en commun numériques des flux entre les donneurs d'ordre et les fournisseurs.

Et, en 2018, sur recommandation du Conseil pour la Cybersécurité du Transport Aérien (CCTA), est lancé AirCyber (-BoostAeroSpace), programme de montée en maturité cybersécurité de la supply chain des donneurs d'ordre européens. « *Cette initiative nous permet de travailler tous ensemble à une maturité cyber croissante de toute la supply chain aéronautique, voire jusqu'au transport aérien. La meilleure approche de la cybersécurité est de faire grandir tout l'écosystème. En faisant grandir tel fournisseur, les clients en bénéficient, et vice-versa. C'est ensemble que nous y arrivons !* ».

Mutualiser, Capitaliser & Accompagner !

AirCyber édite le référentiel de maturité cyber commun à l'ensemble des donneurs d'ordre, « *ce référentiel permet notamment de remplir un seul questionnaire de maturité cyber, de faciliter les démarches cyber, d'accéder à des services de veille, de degré d'exposition, de RSSI partagés. La communauté se réunit une fois par mois pour échanger par exemple sur les nouveautés ou sur les mécanismes de financement* ».

En faisant grandir tel fournisseur, les clients en bénéficient, et vice-versa. C'est ensemble que nous y arrivons !

Cette démarche volontariste appuyée par les grands acteurs de la filière a pour ambition d'améliorer la démarche cybersécurité de nombreuses sociétés dans une logique d'écosystème pertinente. « *Nous faisons tous face à la même menace sans avoir les mêmes moyens. Mutualiser des services, capitaliser sur l'expérience et accompagner cette approche sont les trois axes clés, c'est la manière la plus efficace de répondre à des enjeux forts pour ces entreprises ne pouvant pas toutes aligner les mêmes ressources pour adresser ces enjeux* ».

En outre, cette démarche se déploie pour des sociétés situées dans toutes les régions (Nouvelle-Aquitaine, Ile-de-France, Normandie, Occitanie...) au travers de différents clusters régionaux d'industrie aéronautique.

STÉPHANIE BUSCAYRET

Mailler le territoire

Les réglementations et notamment la directive NIS2 vont étendre leurs impératifs et leurs exigences à une grand nombre d'acteurs « *pas seulement en Ile de France, mais sur tout le territoire. Nous avons donc besoin de développer des écosystèmes de formation et de communication en régions. Il n'y a pas qu'à Paris qu'on fait de la cyber, qu'il y a des talents et des besoins !* ».

Aussi, les compétences cyber doivent se développer rapidement sur tout le territoire « *l'ANSSI a, par ailleurs, commencé à donner cette direction et à mailler le territoire en finançant des CSIRT régionaux, centres de réponses aux incidents cyber* ».

Proximité, Réactivité & Expertise technique

Pas de doute pour Stéphanie Buscayret « *on connait mieux l'écosystème quand on est en local car on est au plus près des besoins. On attend la même chose des éditeurs nous accompagnant sur la cyber.* ».

La proximité sert indéniablement à développer la relation « *et cette relation apporte la confiance. Pour travailler avec des éditeurs, il faut donc développer cette confiance* ». En ce sens, la présence locale des éditeurs et intégrateurs est essentielle, d'autant que face à l'évolution de l'environnement cyber, failles critiques, crises, développement des technologies, veille active, « *il est important de nous appuyer sur nos intégrateurs locaux. Les écosystèmes de fabricants éditeurs doivent le comprendre et mailler le territoire de présences et de compétences régionales* ».

Les rencontres avec les clients sont fondamentales. « *J'insiste sur ce point, ce qu'on attend aujourd'hui d'un partenaire, c'est l'expertise technique, la réactivité et la proximité* » conclut Stéphanie Buscayret.

> Par Sabine Terrey

La nouvelle génération de DSI
OSERA-T-ELLE INNOVER ?

« Faudra-t-il attendre une crise profonde dans l'IT pour que les DSI osent vraiment innover ? La question peut paraître provocante à ceux qui croient, à tort, que l'informatique d'entreprise est un terrain d'innovation. Mais elle ne l'est pas. ».

Observateur de l'IT depuis plusieurs décennies, **Pierre Aguerreberry**, VP Sales EMEA chez DataCore constate qu'il est possible de redonner de la liberté et de l'indépendance aux services informatiques. Qu'ils peuvent se poser plus de questions, à l'instar de ces nouvelles générations en recherche de quête de sens et qui rejoignent une entreprise pour y mener une mission.

Comment et pourquoi les DSI cèdent-ils à des modes (hardware, logiciel, cloud, IA ...) ?

Le rôle d'un DSI est de s'assurer que les moyens informatiques mis en œuvre doivent répondre aux besoins des utilisateurs mais aussi tenir compte, bien évidemment, des enjeux financiers, économiques, transformationnels et évolutifs de leur société. Les différentes missions inhérentes à leurs actions nécessitent une veille technologique accrue car le monde informatique évolue sans cesse, les sociétés deviennent de plus en plus agiles, et donc leurs utilisateurs aussi. Il faut faire plus avec moins ce qui rend leur fonction très compliquée.

Afin de réduire la prise de risque, la tendance forte – notamment dans les grandes organisations – est de faire appel à des cabinets de conseils externes ou des analystes (Gartner). Cette tendance mène trop souvent à la tentation de suivre la « mode » actuelle sans se poser les questions fondamentales du type : est-ce que cela va vraiment simplifier le quotidien de mes utilisateurs tout en garantissant la sécurité de mon environnement informatique ?

Accélérateur de vos innovations
et transformations depuis 2015

#IOT #IA #ROBOTIQUE #XR

10ÈME

sido

18/19.09.2024

CITÉ INTERNATIONALE DE LYON

+ LYON CYBER EXPO by SIDO

L'événement B2B de la **cybersécurité** à destination des **PME, ETI et Grands Groupes**

1 BADGE GRATUIT
= 2 ÉVÈNEMENTS

avec le code **P-ITPSIDO24**

www.sido-lyon.com

#SIDO2024
SUIVEZ-NOUS
SUR LES RÉSEAUX

UN ÉVÉNEMENT
infoprodigital TRADE SHOWS

PIERRE AGUERREBERRY

Trop de DSI gèrent leur budget comme des allocations à dépenser et non comme des montants à allouer de manière entrepreneuriale en démontrant le retour sur investissement mais aussi la simplification des tâches utilisateurs. Si vous faites partie de ces sociétés « Hype » vous pouvez facilement « traquer » et « séduire » ces profils de DSI qui se conforteront dans l'adoption d'une technologie « innovante » et ce, sans pouvoir réellement en mesurer l'impact, puisque celle-ci est souvent trop récente.

Quelles questions se poser quand on est DSI ?

Plusieurs questions sont à se poser. Quel est le bénéfice pour mon utilisateur et ma société ? Comment faire plus de services avec moins de budget ? Quel est l'impact à moyen et long terme de mes choix ?

Les DSI ont un rôle de transformation. Même si la direction financière est devenue prépondérante dans les organisations, sans une DSI moderne intégrant ces paramètres, il est compliqué de réussir ce challenge.

Est-ce que les nouvelles générations de DSI peuvent agir différemment ?

Les nouvelles directions de DSI abordent des sujets qui sont restés longtemps des vœux pieux…La réduction de l'empreinte énergétique, la réduction de l'espace de stockage des infrastructures, l'écoute des utilisateurs qui restent les maillons de la chaine et les premiers bénéficiaires d'une infrastructure informatique bien pensée.

Le libre arbitre entre des solutions innovantes et des solutions réalistes qui répondent aux critères de l'entreprise reste essentiel.

Souhaitez-vous ajouter un point qui vous semble fondamental ?

La durée de mission d'un DSI est devenue de plus en plus réduite. On peut même parler – pour faire de la caricature – de trimestres d'ancienneté et non plus d'années. Cette transformation IT est essentielle au monde du XXI siècle et, seuls, les plus agiles et les plus innovants sauront apporter la valeur attendue.

Les nouvelles directions de DSI abordent des sujets qui sont restés longtemps des vœux pieux.

Quand on parle d'innovation, on ne parle pas forcément des dernières technologies… Cela peut être aussi repenser son informatique pour revenir à l'essentiel : la mise en place d'une solution permettant aux salariés d'être plus efficaces et aux entreprises d'être plus performantes et vertueuses.

> Par Sabine Terrey

Les développeurs ont-ils le temps d'innover ?

Comment accélérer la vitesse de déploiement des applications et offrir des expériences numériques innovantes, fiables, intuitives et sécurisées ?

Résoudre les défis de performance

Les développeurs passent 57% de leur temps à résoudre des problèmes de disponibilité et de performance d'applications, au lieu de se consacrer au développement d'applications et à la stratégie d'innovation.

Leur rôle est essentiel dans la création, le déploiement et la maintenance des applications et des services numériques. Pourtant, la pression est forte !

- Pression pour accélérer leur vitesse de production – 85% - Monde
- Pression pour offrir des expériences numériques transparentes et sécurisées – 77% Monde

Des développeurs démotivés !

Les entreprises ne disposent pas des bons outils pour leur donner la visibilité nécessaire sur les problèmes et selon 75%, le manque de visibilité et d'information sur les performances informatiques augmente les risques d'interruption de service et de perturbation des applications essentielles à l'activité.

Le moral des développeurs est touché

- Ils se sentent frustrés et démotivés – 82%
- Ils sont de plus en plus enclins à quitter leur emploi actuel – 54%

« *La plupart des services informatiques ont déployé une multitude d'outils de surveillance dans différents domaines, mais ils ne sont pas à la hauteur des environnements informatiques complexes et dynamiques d'aujourd'hui. Ce qui empêche les responsables IT de générer une vue complète et unifiée de leurs applications* » précise **Shannon McFarland,** vice-président de Cisco DevNet.

L'observabilité full-stack

Les développeurs veulent jouer un rôle plus important dans l'élaboration et le choix des solutions nécessaires. Selon eux, l'observabilité full-stack offrirait aux équipes SRE et ITOps, la visibilité unifiée sur les applications et l'infrastructure, dans les environnements cloud native et on-premises, ce qui leur permettrait de s'affranchir de la surveillance et de favoriser l'innovation – 94%.

Les équipes IT identifieraient plus rapidement les problèmes pour en comprendre les causes et mettre en œuvre les mesures de remédiation nécessaires.

L'IA pour automatiser la détection

Selon 39%, le déploiement de l'IA pour automatiser la détection et la résolution des problèmes applicatifs est crucial. Avec l'IA, les équipes informatiques peuvent analyser des volumes considérables de données, identifier les problèmes et appliquer des correctifs en temps réel.

De nouvelles méthodes de travail sont recherchées pour améliorer l'efficacité, la productivité et rationaliser la gestion des performances des applications :

- renforcer la collaboration entre les développeurs et les équipes informatiques – 57%
- mise en œuvre de méthodes de tests en amont
- adoption généralisée des méthodologies DevOps et DevSecOps

Source Etude Cisco - 500 développeurs - États-Unis (200), Royaume-Uni (100), Australie (30) et le reste du monde (170 - dont l'Allemagne, la France, l'Italie, l'Espagne, la Scandinavie, le Japon, Singapour et l'Inde). Etude menée par Insight Avenue en mars et avril 2024.

InterCERT France :
COOPÉRATION, BONNES PRATIQUES & INCUBATEUR AU SERVICE DES ORGANISATIONS

Echanges d'informations techniques, bonnes pratiques, mais aussi coopération au niveau opérationnel, partage du savoir-faire, autant de points forts pour mieux appréhender les attaques. Entretien avec Frédéric Le Bastard, président de InterCERT France, communauté d'experts en cybersécurité.

Détection et Réponse aux incidents cyber

Fondée en 2021, InterCERT France est une jeune association née de la volonté de pérenniser un réseau d'organisations ayant des activités de réponse à incident d'origine cyber, CERT (Computer Emergency Response Team, ou CSIRT, Computer Security Incident Response Team) sur le territoire français. « *Cette association s'est créée sur la base d'un groupe préexistant de 60 experts, spécialistes œuvrant dans le domaine de la détection et de la réponse aux incidents de cybersécurité. Ce sont donc des praticiens, ces hommes et ces femmes de l'ombre tentent de faire face et d'accompagner les organisations victimes d'incidents cyber* » complète le président d'InterCERT France. Des membres du premier groupe informel réunis au début des années 2000 jusqu'aux 10 équipes vers les années 2010, la croissance s'accélère ensuite « *puisque nous sommes passés de 57 membres en octobre 2021 à 107 membres aujourd'hui* ».

Le constat est simple : de plus en plus d'organisations s'intéressent activement au sujet de la détection et de la réponse aux incidents de sécurité. « *Notre raison d'être est donc de faciliter et animer la coopération entre ces équipes, notamment pour faire face à des incidents de sécurité, souvent non ciblés et opportunistes et pouvant toucher toute organisation, artisans, banques…. En effet, toute surface d'attaque peut être mise à l'épreuve par un adversaire (phishing…), aussi ceux qui en sont victimes partagent leur expérience car la question n'est pas de savoir si on risque d'être victime d'un incident de sécurité mais quand* ». L'ambition de InterCERT France est donc faciliter et limiter les effets de ces attaques.

Trois vecteurs forts de coopération

Comment InterCERT France procède-t-il concrètement ?

Le premier vecteur de coopération est un service de messagerie instantanée « *qui permet aux membres de communiquer entre eux, 24/24 7/7, 365 jours par an* ». Plus de 900 experts qualifiés, de référence et connectés sur cette plateforme de messagerie instantanée échangent sur les vulnérabilités

pouvant affecter les SI, les menaces sectorielles (énergie, finance, transport…), les faits d'actualité (JO 2024, guerre en Ukraine…). Des groupes thématiques travaillent aussi sur la sécurité des systèmes embarqués, la détection, la judiciarisation (Gendarmerie, Police nationale) et les questions opérationnelles. « *L'objectif est de partager les bonnes pratiques pour accélérer l'efficacité de la réponse à incident dans toutes ses dimensions* ».

Les séquences matinales (connectées), second vecteur, prônent le partage d'expertise et d'expérience. « *Les sujets sont divers. Un membre présente, par exemple, un retour d'expérience sur un incident qu'il a eu à traiter, une attaque qu'il a réussi à éviter, des événements d'un nouveau type observés qu'il souhaite partager avec la communauté, les feedbacks des évolutions des normes…. A noter, il n'y pas d'activité mercantile entre les membres mais des activités techniques et opérationnelles* ».

Enfin, les rencontres en présentiel appelées InterCERT Day ont lieu deux fois par an « *pour partager des informations de visu, avec la présence de divers intervenants qualifiés* ».

Un incubateur pour renforcer la maturité opérationnelle

Pour favoriser l'échange de connaissances et compétences, les membres vont partager leurs expertises et savoir-faire avec de jeunes CERTs ou en cours de constitution. Ainsi, dès le 21 mai 2024, est lancé l'incubateur d'InterCERT France pour accompagner le développement des CERTs. Un programme de formation a été élaboré par les experts et membres, et la première promotion 'Cédric Blancher' (1) pourra accueillir jusqu'à 10 équipes (sélectionnées sur dossier de candidature).

« *Cet incubateur a pour ambition de proposer une vingtaine d'ateliers animés par nos membres, à destination de personnes souhaitant devenir membres, avec des retours d'expériences opérationnels sur les volets RH, outils, techniques, processus, en mai et juin, à Paris, aux formats distanciel et présentiel pour créer un effet de groupe et de partage* ».

Autre actualité prochaine et non des moindres ! La publication de la première étude d'accidentologie en juin 2024, les membres ont ainsi partagé de manière anonymisée les incidents auxquels ils ont fait face, « *plus d'une cinquantaine d'équipes ont répondu et ont remonté plus de 220 cas d'incidents différents, ce qui montre un paysage assez complet des incidents cyber 2023, ce point de vue du terrain des praticiens est unique* ».

Le Blog, véritable manifeste

Face aux risques cyber permanents et croissants, le blog de l'InterCERT France diffuse une vision préventive de la sécurité informatique, témoigne des enjeux, et lutte contre la mésinformation et la désinformation. « *Nous avons la chance d'être autonomes dans notre fonctionnement et nous ne sommes pas sous influence d'un tiers d'où une grande liberté de parole. Aussi, les volontaires souhaitant s'exprimer et porter la voix des CERT peuvent le faire dans le Blog. Loin de se cantonner au sujet de la détection et de la réponse aux incidents, nous prenons position sur des sujets d'actualité, sur les choix faits aujourd'hui sur les SI, sur les enjeux de souveraineté, sur les décisions engageantes aux conséquences pour de nombreuses années. Par exemple, les mouvements actuels vers le Cloud poussent à confier les clés de nos SI à des acteurs internationaux, dans un contexte incertain et aux risques géopolitiques non considérés lors de ces phases de choix* ».

L'ambition de ce blog est d'éclairer les choix des organisations avec des angles non encore abordés pour faire réfléchir les lecteurs et les aider dans leur prise de décision.

Restons optimistes !

Face aux cyberattaques en hausse « *c'est parfois démoralisant certes, mais il faut s'en occuper et être optimiste. Comme Vincent Strubel, directeur général de l'ANSSI, le souligne, et je partage cette pensée, aujourd'hui, dans la perspective des JO, les acteurs qui doivent être prêts le sont, car ils se sont préparés depuis un certain temps déjà. C'est bien plus délicat pour ceux qui n'avaient pas pris conscience du sujet avant. Par contre, le niveau d'exposition va augmenter avant et pendant les JO, d'autant que la visibilité internationale va augmenter et cristalliser toute l'attention. Il faudra juste continuer sur cette dynamique de préparation et de protection dans la durée, les menaces cyber ne s'arrêteront pas* ». Il faut être lucide, car les adversaires vont profiter évidemment de ce moment.

L'ambition de ce blog est d'éclairer les choix des organisations avec des angles non encore abordés pour faire réfléchir les lecteurs et les aider dans leur prise de décision.

Les organisations sont de plus en plus préoccupées par les questions de cybersécurité, et doivent passer de l'étape de la conscience du danger et de la menace à l'étape de mise en œuvre des moyens et défenses. Toutefois, « *quand on parle d'incidents cyber en France, c'est rarement des grandes organisations, c'est bien la preuve que ces établissements ont progressé en maturité et en sécurité !* ».

(1) Hommage à l'un de ses précurseurs sur les sujets cybersécurité, Cédric Blancher

> Par Sabine Terrey

NIS2 & CESIN :
DÉBATS AUTOUR DE LA TRANSPOSITION NATIONALE DE LA DIRECTIVE EUROPÉENNE

L'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) a sollicité l'expertise du CESIN dans le cadre de la transposition nationale de la directive européenne NIS2. Retour sur les enseignements.

La consultation

Le CESIN a collecté les remarques, avis et propositions de ses membres dans le cadre de la transposition nationale de NIS2 *(Network and Information Systems Directive 2)* autour des questions et textes soumis par l'ANSSI.

Résultat : 150 membres du CESIN ont contribué à cette consultation. Le panel est constitué de membres issus d'ETI et de grandes entreprises, dont 30% ont une implantation internationale.

- 25% pensent que leur entreprise est assujettie à NIS2 en tant qu'Entreprise Essentielle (EE)
- 19% en tant qu'Entreprise Importante (EI),
- 23% pensent que leur entreprise n'est pas assujettie
- Un tiers ne sait pas déterminer si leur entreprise sera assujettie.

Les critères d'éligibilité à NIS2

Enseignement N°1, les critères d'éligibilité à NIS2 soulèvent un certain nombre de questions et le taux d'entreprises s'interrogeant est relativement élevé. Cette difficulté de positionnement ne semble pas corrélée à la taille de l'entreprise, ni à son implantation.

En matière de gestion d'incidents, les entreprises disposent d'équipes internes ou externes prêtes à prendre en charge rapidement des incidents cyber (86%) et une petite majorité d'entre elles (71% des EE, mais seulement une EI sur deux) pourraient mettre en place des dispositifs d'astreinte, à défaut de pouvoir assurer une disponibilité 24/7.

Un incident classé important

La définition d'un incident classé « important » suscite des commentaires.

Un critère simple a émergé « un incident important est un incident notifié au COMEX de l'entreprise ». En d'autres termes, un incident qui ne remonte pas au COMEX, n'est pas jugé important. La qualification de l'incident important devrait être liée au métier de l'entreprise et à la structure de son ou de ses Systèmes d'Information, notamment pour les grandes entreprises qui ont des SI et organisations plus ou moins centralisés, et pour lesquelles la notion d'incident important peut avoir des sens très différents.

En plus d'une définition formelle, le CESIN suggère que le critère d'importance d'un incident soit adaptable aux spécificités propres à chaque entreprise. Pour les autres incidents, il propose de les qualifier d'incidents « mineurs » plutôt que d'incidents « évités ». Certains incidents, bien que contenus et ayant un impact limité, sont pertinents à notifier pour comprendre les modes d'attaques et enrichir les statistiques sur les menaces.

Une stratégie de notification des incidents

Le CESIN propose une stratégie de notification des incidents qui va dans le sens d'une meilleure **connaissance globale des volumes et formes de menaces**. Les incidents importants seraient déclarables, suivant une procédure et qui ne doit pas emboliser les ressources en charge de gérer une crise.

Les incidents mineurs pourraient être déclarables de façon facultative et seraient enregistrés de façon anonymisée par le régulateur. **Alain Bouillé**, délégué général et porte-parole du CESIN, confirme : « *Nous considérons que cet anonymat est la seule possibilité de favoriser un partage réel d'information sur les menaces, leur volume et leur nature. Cela permet aussi de lever les freins à la déclaration.* »

La cartographie des entreprises et du SI

Le CESIN suggère que les entreprises ne se décrivent pas à travers leurs entités légales, mais plutôt qu'elles fournissent une vision opérationnelle de leur organisation, en lien avec leur SI. Cela implique de détailler la structure sur laquelle les mesures de prévention et de cyberdéfense sont déployées et appliquées, pour permettre notamment de mieux comprendre la surface d'attaque d'une entreprise.

Les plans d'adressage pour les actifs exposés devraient tenir compte des architectures de plus en plus tournées vers le cloud, avec un certain nombre d'IP exposées qui ne sont plus privatives, mais mutualisées ; d'autant que ces surfaces exposées publiquement évoluent constamment. Les formats et méthodes pour les transmettre à l'opérateur devront être efficaces et industrialisables pour que l'opérateur puisse avoir une cartographie à jour.

Les exigences

La phase 3 de la consultation de l'ANSSI portait sur les mesures de sécurité. Les membres du CESIN jugent que ces mesures sont claires (90%), tandis que 70% d'entre eux pressentent des difficultés pour leur mise en œuvre.

Alors qu'une EE (Entreprise Essentielle) sur deux ne pense pas pouvoir intégrer des mesures complémentaires, 71% des EI (Entreprise Importante) se disent prêtes à monter le curseur des mesures. Globalement, 82% des EE jugent les objectifs au bon niveau d'exigence, contre 61% chez les EI.

Un critère simple a émergé « un incident important est un incident notifié au COMEX de l'entreprise ».

Un quart des EI ne se prononcent pas sur le niveau d'exigence. Dans l'ensemble, les membres du CESIN jugent satisfaisant que le niveau attendu pour les EI ne soit pas trop élevé d'emblée, cela permet d'entrer progressivement dans la dynamique de cette nouvelle conformité.

Quelques réflexions complémentaires

• *Des mesures de sécurité ajustées*

Les mesures de sécurité pourraient être ajustées pour mieux intégrer l'impact croissant du cloud dans les systèmes d'information des entreprises. En particulier sur les aspects tels que la gestion des réseaux, la segmentation, l'accès, la surveillance, la protection des données et la résilience. Notamment au plan des responsabilités et des processus de gestion en cas d'incident.

• *Les risques & les dommages collatéraux*

Les risques liés aux tiers restent très centrés sur les risques en lien avec des interconnexions entre les entreprises et leurs partenaires externes. Il est important de tenir compte des dommages collatéraux, notamment les violations de données qui peuvent découler de facteurs indirects et engendrer des impacts, au-delà des seuls risques liés à la connectivité.

• *La gestion des identités et des accès & MFA*

D'autres interrogations émergent sur la gestion des identités et des accès, appelant à clarifier les aspects relatifs aux facteurs d'authentification et au multi-facteur (MFA) : quand les utiliser, et sous quelles conditions ? Le MFA lui-même doit être sécurisé, puisque de nombreux scénarios d'attaques cherchent à le contourner. Les processus de gestion des facteurs d'authentification renforcés, sur la base d'exigences plus détaillées. Des mesures spécifiques pourraient être définies pour la fédération d'identité, l'accès conditionnel et le Single-Sign-On, qui constituent des éléments structurants des nouvelles architectures d'accès.

• *Les terminaux & BYOD*

Les membres s'étonnent de ce qui peut sembler être une acceptation du BYOD pour les EI. Une posture incompatible avec d'autres règles qui demandent par exemple, des restrictions sur les droits d'administration des terminaux ou l'installation libre de composants non approuvés.

• *La détection et la surveillance*

La dimension détection et surveillance est pour le moment absente des obligations des EI. Selon **Frank Van Caenegem**, administrateur du CESIN, « *Sans un minimum de capacité à tracer et surveiller, il est considéré qu'une entreprise ne peut pas faire face à des incidents. Nous savons tous que la seule prévention ne sera jamais suffisante, et que des incidents surviendront forcément.* » Les membres du CESIN recommandent donc des mesures a minima sur ce pilier essentiel de la cybersécurité, pour permettre de détecter, contenir, investiguer, trouver les portes d'entrée et de sortie des attaques.

Le CESIN joue un rôle significatif en tant que témoin direct des défis en matière de cybersécurité auxquels font face les entreprises.

• *Des propositions adaptées au contexte*

Mylène Jarossay, Présidente du CESIN, ajoute que « *La consultation menée par l'ANSSI pour la transposition nationale de NIS2 est une opportunité pour le CESIN d'apporter des propositions concrètes et adaptées au contexte actuel des organisations et des SI en France. Le CESIN est pleinement engagé et nous sommes ravis de mobiliser notre expertise collective pour éclairer les décisions stratégiques en matière de cyberdéfense. Nous restons disponibles pour soutenir toute initiative complémentaire de l'ANSSI et continuer à œuvrer ensemble pour la sécurité de nos entreprises et de notre pays.* »

handicap international

25 ans

10 PROTÈGE-LIVRES

KIT PRÊT À L'EMPLOI

COUVRIR VOS LIVRES ET VOS CAHIERS DEVIENT UN JEU D'ENFANTS AVEC MAESTRO !

IL ÉTAIT UNE FOIS... CES DRÔLES D'OBJETS

1€ POUR LE FINANCEMENT DE NOS MISSIONS HUMANITAIRES

FABRICATION FRANÇAISE

CONDITIONNÉ PAR DES TRAVAILLEURS HANDICAPÉS

Retrouvez nos produits et de nombreuses idées cadeaux sur :
boutique.handicap-international.fr

Migrer vers Exchange 2019 -2025 SE : QUAND & POURQUOI ?

Si beaucoup d'entreprises utilisent désormais l'environnement Exchange Online, nombreuses sont celles qui ont conservé un environnement Exchange Server et utilisent de facto un environnement hybride. D'autres, au contraire, pour des raisons légales notamment, ont conservé et conserveront dans les années à venir leurs boites aux lettres On Premise.

Qu'il soit réduit à une portion congrue ou composée de plusieurs dizaines de serveurs, se pose la question de faire évoluer cet environnement vers une version plus « moderne ». C'est en tout cas ce que propose Microsoft qui recommande fortement de migrer dès à présent vers la version Exchange 2019.

Exchange Subscriber Edition (Exchange SE)...

Comme certains d'entre vous auront déjà remarqué, les équipes Exchange de Microsoft n'ont pas sorti officiellement de nouvelle version depuis 5 années. Un record si l'on regarde les anciennes versions comme Exchange 2010, 2013, 2016, 2019. Ce n'est

que 6 ans après la sortie d'Exchange 2019 que sortira officiellement la nouvelle version Exchange Subscriber Edition (Exchange SE) remplaçant enfin, la version Exchange 2019. Autant dire que le retard technologique accumulé s'est comblé à coup de Services Pack (Mises à jour) et de Security Update (SU).

Depuis 2019, Microsoft fait régulièrement évoluer sa dernière version pour lui permettre de faire face aux nouvelles menaces avec, il faut le dire, quelques effets de bord affectant parfois certaines fonctions utilisateurs. (Voir article https://techcommunity.microsoft.com/t5/exchange-team-blog/released-march-2024-exchange-server-security-updates/ba-p/4075348). L'impression générale est que le produit Exchange 2019 semble quelque peu à bout de souffle technologiquement (je ne parle même pas d'Exchange 2016 !).

Coté support, les deux versions 2016 et 2019 se termineront en même temps comme le montre la figure suivante issue de la documentation de l'éditeur.

Listing	Date de début	Date de fin du support standard	Date de fin étendue
Exchange Server 2019	22 oct. 2018	9 janv. 2024	14 oct. 2025

Listing	Date de début	Date de fin du support standard	Date de fin étendue
Exchange Server 2016	1 oct. 2015	13 oct. 2020	14 oct. 2025

La nouvelle version Exchange Subscriber Edition sortira vraisemblablement au troisième trimestre 2025 et supportera les systèmes d'exploitation Windows Server 2022 et Windows Server 2025.

Cette nouvelle version est aussi la seule à pouvoir être installée comme une mise à jour directement sur des serveurs Exchange 2019. Pour la version Exchange 2016 ,vous devrez faire une installation en parallèle et migrer, vers cette nouvelle version, vos boites aux lettres, vos services Web, vos connecteurs d'envoi et de réception, votre hybridation etc.... Bref, un vrai et beau projet que vous devriez envisager de démarrer... dès maintenant.

Si vous disposez d'Exchange 2013, *il ne sera pas possible d'installer Exchange SE dans le même environnement*. Une raison de plus pour migrer, dès à présent, vers Exchange 2019.

Vous l'avez compris, *il va falloir migrer vers Exchange 2019 et ce, sans tarder.*

Philosophiquement, la version Exchange 2019 reprend les grands principes de conception d'Exchange 2016, un point positif pour vos équipes internes niveau 3 qui auront à faire face à un environnement familier et maitrisé au quotidien. Le point négatif réside dans la charge de travail d'un tel projet, surtout pour les entreprises qui utilisent massivement le service Exchange Server.

La montée de version vers Exchange 2019 va demander de reconstruire intégralement une nouvelle infrastructure dotée de nouveaux serveurs, de nouvelles adresses virtuelles de répartition de charge, d'un nouvel espace de stockage etc.

Ce projet va demander a minima aux équipes techniques du projet de :

- *Concevoir une Documentation d'Architecture Technique précisant les points suivants*
  - > Dimensionnement du stockage
  - > Inventaires des flux réseau et connectivité Internet
  - > Dimensionnement des serveurs Exchange
  - > Définition des services de répartition de charge
  - > Exigences réseaux
  - > Sécurisation du service.
- *Concevoir et présenter une analyse des risques*
- *Définir et valider une stratégie de migration*
  - > Migration du service d'accès clients
  - > Migration des boites aux lettres et dossiers publics le cas échéant
  - > Migration de l'hybridation
  - > Migration du service SMTP.
- *Valider les solutions d'entreprise déployées sur les serveurs existants*
  - > Sauvegarde, restauration
  - > Supervision
  - > Anti-Virus, Antimalware
  - > Etc.
- *Valider la coexistence des services Exchange 2013,2016 avec Exchange 2019*
- *Référencer les dépendances applicatives du service Exchange*
  - > Flux Smtp, Imap, Pop3
  - > Flux applicatifs de type Webservices ou PowerShell.

Autant le dire franchement, le travail ne vas pas manquer.

La nouvelle version Exchange Subscriber Edition sortira vraisemblablement au troisième trimestre 2025

Se faire accompagner ?

Gérer au quotidien, le support et l'administration d'un infrastructure Exchange importante et définir une nouvelle infrastructure in extenso avec potentiellement des nouvelles contraintes ne requièrent pas les mêmes compétences. Compte tenu de l'importance du service Exchange, beaucoup d'entreprises préfèreront se faire accompagner par des intégrateurs Microsoft certifiés. La difficulté réside alors dans la disponibilité des ingénieurs ayant de réelles expertises dans ces domaines. En effet, la déferlante Cloud a massivement orienté les jeunes ingénieurs vers des compétences sur Exchange Online au dépend des environnements On Premise. Autrement dit, les compétences dans ce domaine se sont raréfiées au même titre que celles que vous pourriez demander sur des environnements Lotus Note.

Reconstruire une nouvelle infrastructure, n'implique pas obligatoirement de refaire en 2019 ce que l'entreprise avait construit à l'époque sur Exchange 2013 ou 2016.

Selon le contrat qui vous lie avec Microsoft, vous pourriez obtenir de leur part des services de conseils et de validation d'architecture. Aussi, je vous invite à vous rapprocher de votre « « *Microsoft Customer Success Account Manager* » (ça ne s'invente pas) pour connaitre les prestations auxquelles vous pourriez prétendre.

Pour les avoir utilisées, elles sont plutôt de bonnes factures mais ne couvrent pas l'intégralité des domaines que vous devrez aborder. Cela reste cependant une aide précieuse.

Suivre avec attention les publications de Scott Schnoll et de l'équipe Exchange

Scott Schnoll est " *Product Manager Exchange Online, Exchange Server, Exchange Online Protection, and Exchange Online Archiving* " chez Microsoft.

Avec l'équipe Exchange, Il communique régulièrement sur la feuille de route d'Exchange Server sur le site https://techcommunity.microsoft.com/t5/exchange-team-blog/bg-p/Exchange.

Des informations importantes et précieuses pour toute entreprise confrontée à la migration vers Exchange 2019 et Subscriber Edition. Indispensable !

Reconduire l'existant... ou pas.

Reconstruire une nouvelle infrastructure, n'implique pas obligatoirement de refaire en 2019 ce que l'entreprise avait construit à l'époque sur Exchange 2013 ou 2016. Les menaces ont changé et les besoins ont possiblement évolué.

De ce fait, le projet de migration devrait constituer le moment propice, pour questionner l'environnement actuel et bâtir le cas échéant une architecture un tant soit peu différente.

Il vous reste encore un peu plus d'une année pour tout cela. Mais comme disent les Anglais : Time flies !

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

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

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

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

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

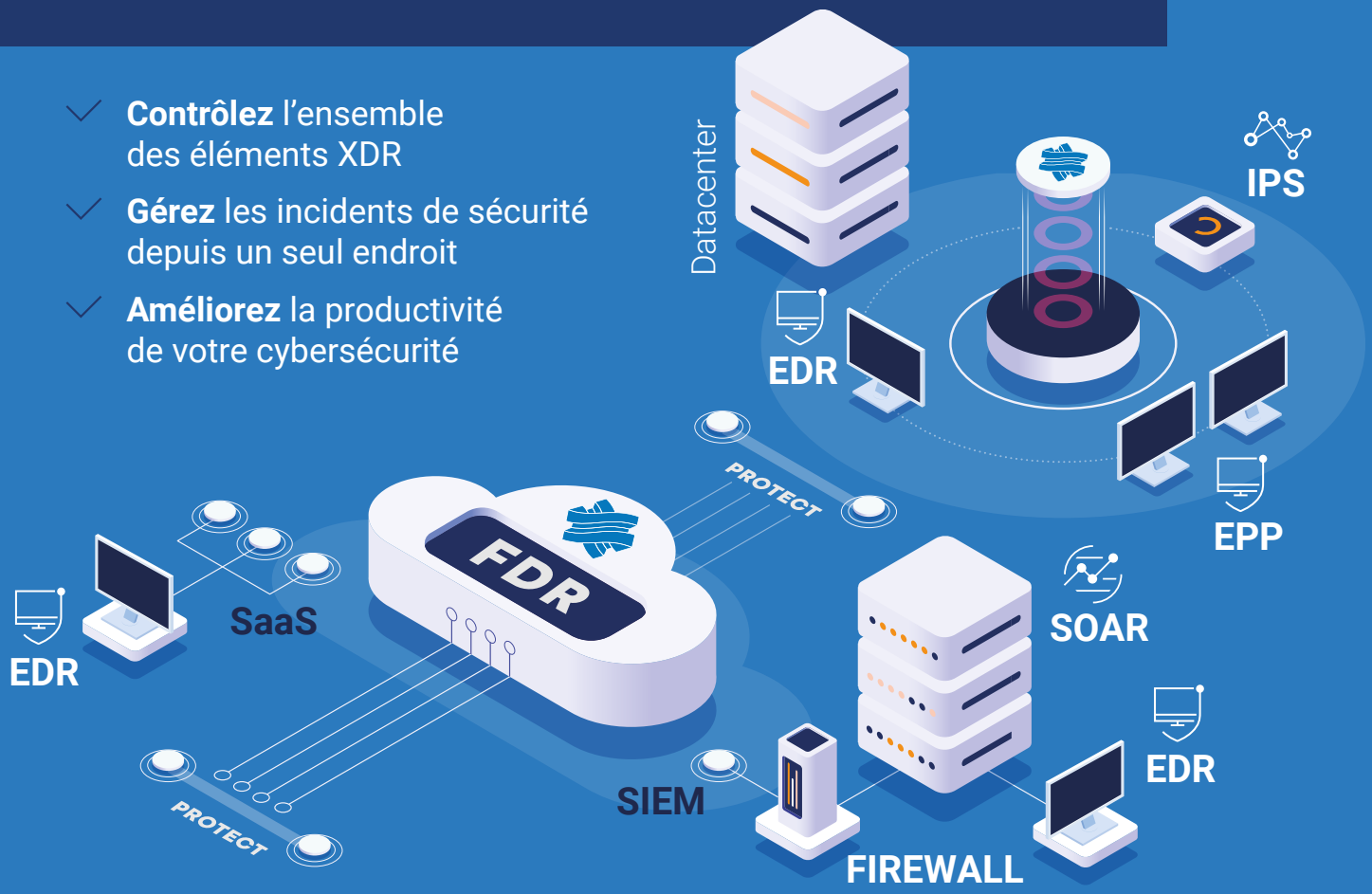
Analyse, Contrôle et Reporting complet des systèmes de messageries **Microsoft Office 365 et Microsoft Exchange**

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

Stormshield XDR

Pour améliorer l'efficacité opérationnelle cyber de votre infrastructure

- **Contrôlez** l'ensemble des éléments XDR
- **Gérez** les incidents de sécurité depuis un seul endroit
- **Améliorez** la productivité de votre cybersécurité



www.stormshield.com

Pour obtenir plus d'information sur l'offre Stormshield XDR

STORMSHIELD

Stormshield XDR est la combinaison idéale de **Stormshield Network Security** (SNS) et **Stormshield Endpoint Security Evolution** (SES) pour protéger les réseaux et sécuriser les terminaux.

L'expertise Stormshield en **Cyber Threat Intelligence** (CTI) permet d'anticiper les menaces. L'ensemble est orchestré par **Stormshield Log Supervisor** (SLS) pour vous alerter en temps réel et piloter une réponse rapide et pérenne sur le réseau et les terminaux.