L'IA, un facteur décisif pour renforcer la résilience numérique, découvrez l'analyse des experts ESET en page 22

N°36 I DECEMBRE 2024

CONDUIRE LA TRANSFORMATION NUMÉRIQUE DE L'ENTREPRISE

SMART DSI®

DOSSIER
DORA, explorer les risques et les tiers pour être résilient

INTERVIEW
Pour une IA responsable, pensée comme un outil au service de l'humain

L'ŒIL SECURITE
ChatGPT, 2 ans déjà, et la cyber ?

L'ETUDE A RETENIR
Actions pour un environnement de travail numérique durable

L'ŒIL DU FUTUR
Un paysage de la cybersécurité de plus en plus complexe en 2025

INTERVIEW
La cartographie du SI est un outil stratégique fondamental

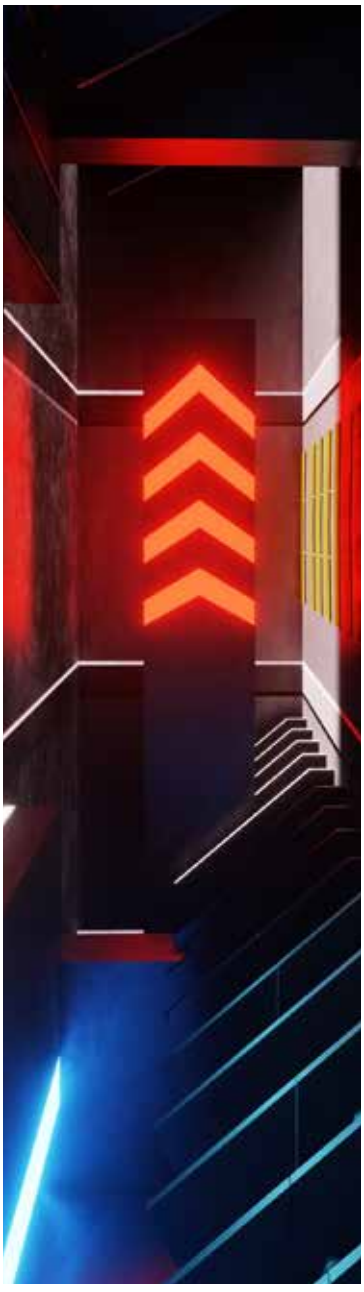
#PreventionFirst

Anticipez les cybermenaces avec une approche préventive

ESET vous accompagne depuis plus de 30 ans

ESET®

Digital Security
Progress. Protected.



Tendances 2025 : entre IA, Cyber résilience & Données !

En cette fin d'année, les sujets dédiés aux tendances 2025 explosent dans un paysage économique, politique et technologique en constante évolution, et il y en a pour tous les goûts et tous les environnements. La place occupée par l'Intelligence Artificielle se renforce, avec des axes qui s'affinent, sans oublier d'autres perspectives transformatrices et très attendues.

Si le rôle de l'IA dans la réussite des entreprises est essentiel pour atteindre les objectifs stratégiques, des facteurs peuvent encore bloquer les projets, comme le manque de compétences, de gouvernance des données, de budget, de confiance et les questions de règlementation. Toutefois, quelques évolutions de l'IA sont intéressantes à retenir [1]. Tout d'abord, l'essor de l'architecture de l'IA agentique marque une nouvelle étape avec la création d'agents IA opérant de manière autonome, communiquant en langage naturel et interagissant avec d'autres agents et des humains. Autre évolution majeure annoncée, l'IA combinée à l'informatique quantique, à la périphérie intelligente, au Zero Trust, à la 6G et aux jumeaux numériques, pour créer une dynamique d'innovation.

Autres enjeux clés pour 2025 [2], l'urgente modernisation des infrastructures dans les secteurs de la santé, de l'énergie, des télécommunications, de la production pour rester compétitif et faire face aux défis et aux risques. La cyber résilience est également une forte priorité pour toutes les industries, tout comme la simplification des processus via des plates-formes low-code / no-code, la collaboration intersectorielle pour faciliter l'adoption des solutions avancées, et la gestion intelligente des données.

Enfin, l'innovation orientée vers la durabilité prédomine, en effet, 71 % des DSI [3] sont désormais responsables de ces stratégies dans leur organisation. La réduction de la consommation d'énergie mais aussi le respect des objectifs environnementaux sont cruciaux pour rester à la pointe des avancées de la transformation numérique.

D'ailleurs, tout leader 2025 ne devrait-il pas être responsable et engagé pour l'innovation et la durabilité ?

Très belle année 2025 riche en projets et en inspiration !

Sabine Terrey
Directrice de la Rédaction

(1) Source Dell – Expertise John Roese, Global Chief Technology Officer & Chief AI Officer

(2) Source Kyndryl – Predictions 2025 Readiness Report 2024

(3) Source Colt - Rapport sur les infrastructures numériques

SMARTDSI

N°36 I DECEMBRE 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

6 I DOSSIER
DORA, explorer les risques et les tiers pour être résilient

12 I L'ŒIL SECURITE
ChatGPT, deux ans déjà, et la cyber ?

14 I INTERVIEW
Accompagner les PME pour la protection de leurs systèmes et données est une priorité

17 I L'ETUDE A RETENIR
Maturité cyber & investissements en France

18 I EXPERT
Azure Backup, de belles évolutions pour une solution clé en main

22 I PARTNER SECURITY REPORT
L'Intelligence Artificielle est-elle un facteur décisif pour renforcer la résilience numérique ?

24 I INTERVIEW
SMART TEEM « pour une IA responsable, pensée comme un outil au service de l'humain »

27 I L'ETUDE A RETENIR
Actions pour un environnement de travail numérique durable

28 I L'ŒIL DU FUTUR
Un paysage de la cybersécurité de plus en plus complexe en 2025 !

30 I INTERVIEW
Toute organisation doit évaluer le niveau de sécurité de ses partenaires

32 I EXPERT
Synchronisation Multi-Tenant : Pour quoi faire ?

36 I INTERVIEW
La cartographie du SI est un outil stratégique fondamental

SMART DSI

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

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

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

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

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

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

N° ISSN : 2494-9701 - N° CPPAP : 0518 T 93059

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

Site officiel : www.smart-dsi.fr

DORA, EXPLORER LES RISQUES ET LES TIERS POUR ÊTRE RÉSILIENT

> Par Didier Danse

Dans un monde de plus en plus interconnecté, les institutions financières dépendent fortement des technologies numériques pour offrir des services essentiels. Cette transformation digitale, bien qu'indispensable, expose le secteur à des risques croissants, tels que les cyberattaques, les pannes techniques et les défaillances des fournisseurs tiers. Ces incidents peuvent entraîner des perturbations majeures, affectant la stabilité financière et la confiance des consommateurs. Ce contexte met en lumière la nécessité d'un cadre robuste pour gérer ces vulnérabilités.

Le Digital Operational Resilience Act (DORA), adopté par l'Union européenne, répond à ce défi en établissant des règles harmonisées pour renforcer la résilience opérationnelle numérique des institutions financières. Au-delà de la conformité réglementaire, DORA offre une opportunité stratégique : celle d'adopter des pratiques exemplaires en gestion des risques numériques, de renforcer la confiance des parties prenantes et de garantir la continuité des services financiers dans un environnement incertain.

DORA, le pendant de NIS2 pour le secteur financier

Ces derniers mois, il a été fréquent de voir des articles sur NIS2, à savoir la directive européenne sur la sécurité des réseaux et des systèmes d'information, mais bien moins sur le sujet de DORA, le règlement sur la résilience opérationnelle numérique. Pourtant NIS2 et DORA reposent sur des fondements identiques visant un objectif commun : protéger les systèmes critiques contre les cybermenaces et harmoniser les règles en Europe.

DORA et NIS2 ont cependant une portée différente : NIS2 s'applique à divers secteurs critiques (énergie, santé, transport, etc.) et cible la cybersécurité des infrastructures essentielles tandis que DORA est plus spécifique au secteur financier. Il régule la gestion des risques numériques et des tiers critiques. Les entreprises financières touchées par DORA peuvent aussi être soumises à NIS2 si elles relèvent d'autres secteurs critiques.

Les grands enjeux de DORA

Le texte du règlement s'avère plutôt long à lire et très détaillé. Une lecture détaillée est évidemment recommandée mais si vous lisez cet article, certainement vous en avez entendu parler sans pour autant avoir déjà lu le règlement dans son entier. Ainsi, il est important de comprendre et retenir les enjeux :

- *Résilience face aux cyberattaques :* Réduire les risques liés aux menaces cybernétiques qui ciblent les institutions financières.
- *Sécurisation des chaînes d'approvisionnement :* Encadrer les risques associés aux fournisseurs tiers critiques, notamment les services cloud.
- *Harmonisation réglementaire :* Établir des règles uniformes au sein de l'UE pour une meilleure gestion des risques numériques.
- *Protection des données sensibles :* Garantir la confidentialité et la sécurité des informations financières et personnelles.
- *Gestion des interruptions :* Assurer la continuité des services financiers en cas de pannes ou incidents.
- *Surveillance proactive :* Renforcer la capacité des autorités à superviser et contrôler les entreprises pour prévenir les défaillances.

De quelle manière cela se traduit-il ?

Le règlement établit des exigences concernant la gestion des risques liés aux technologies de l'information et aux systèmes numériques. Voici les principaux points de DORA :

- *Gestion des risques numériques :* Les institutions financières doivent mettre en place des pratiques robustes de gestion des risques numériques, couvrant l'ensemble de leur chaîne de valeur, des services internes aux fournisseurs externes.
- *Surveillance des fournisseurs tiers :* DORA impose aux entreprises de surveiller et de gérer les risques associés à leurs fournisseurs tiers, notamment ceux qui fournissent des services cloud, des infrastructures critiques ou des solutions technologiques essentielles.
- *Résilience des systèmes informatiques :* Les entreprises doivent garantir la continuité de leurs opérations numériques et la protection des données en cas de perturbations majeures, notamment par la mise en place de plans de reprise après sinistre et des tests réguliers de leurs systèmes.
- *Notification des incidents majeurs :* DORA exige la notification rapide des incidents majeurs de cybersécurité ou des pannes informatiques aux autorités compétentes, ainsi qu'aux clients si nécessaire.
- *Tests de résistance :* Les entreprises doivent mener régulièrement des tests de résistance de leurs systèmes afin de s'assurer qu'ils peuvent faire face à des cyberattaques ou d'autres perturbations graves.
- *Gestion des données et confidentialité :* Des exigences strictes sont établies en matière de protection des données, notamment concernant les données sensibles et la gestion des informations personnelles.
- *Supervision et régulation :* Les autorités compétentes des États membres seront responsables de la supervision de la mise en œuvre des mesures DORA, avec une coopération accrue au niveau européen pour assurer la conformité.

Un focus sur le registre des tiers ou des tiers parties

Un élément clé de DORA étant l'identification et cette identification étant le point d'entrée de bien des vérifications, un registre – « encore un » diront certains – fait son apparition : *le registre des tiers* (ou registre des tiers parties).

Ce registre centralise les informations sur les tiers et fournit une base structurée pour évaluer, surveiller et gérer les risques associés. Un registre des tiers contient généralement des données telles que l'identité du fournisseur, la nature des services fournis, les contrats en vigueur, et les évaluations de risque associées.

Dans le cadre de DORA, la gestion des tiers devient une obligation. Les entreprises doivent en effet démontrer qu'elles surveillent activement les risques liés aux fournisseurs critiques, tels que les prestataires de services cloud ou de solutions

numériques. Au-delà de la conformité, cet outil est une opportunité d'améliorer la résilience globale de l'entreprise. Il favorise une meilleure prise de décision en fournissant une vue d'ensemble des interdépendances et des vulnérabilités potentielles. Par ailleurs, il contribue à renforcer la transparence et la collaboration avec les partenaires externes.

Il n'est jamais trop tard pour se mettre en conformité avec DORA

Les régulateurs locaux auront certainement une autre lecture de ce point mais à nouveau, il s'agit d'identifier les activités clés qui peuvent et doivent être couvertes. Il s'agit généralement de revoir les procédures en place pour clarifier comment les règles sont appliquées et qui sont généralement rappelées au niveau des politiques. A cela s'ajoute d'identifier plus d'éléments, comme nous avons pu le voir avec le registre des tiers. Ainsi, les grandes étapes, bien qu'en réalité nombreuses d'entre elles s'effectuent en parallèle, peuvent se présenter de la sorte :

1. Cartographier les risques numériques

L'identification des systèmes critiques et des vulnérabilités est la première étape. Elle consiste à :

- Recenser les actifs numériques (infrastructures, logiciels, données) et leur importance pour l'entreprise.
- Identifier les dépendances externes, comme les fournisseurs tiers ou les infrastructures partagées.
- Effectuer une analyse des menaces pour comprendre les risques spécifiques liés à chaque actif.

Le règlement établit des exigences concernant la gestion des risques liés aux technologies de l'information et aux systèmes numériques.

Une cartographie claire permet de prioriser les actions de sécurisation en fonction de l'importance des systèmes et des risques associés. Il y a différentes interprétations de ce qui est à faire mais, il est probable que la CMDB ait été mise à jour, ainsi que le catalogue de service et bien évidemment le registre des tiers.

Ce sera très certainement les premiers documents qui seront demandés par le régulateur en cas de contrôle puisqu'il s'agit d'identifier les éléments avant de pouvoir entrer dans l'analyse détaillée de ceux-ci.

2. Mettre en place une gouvernance des risques

Une gouvernance efficace implique la définition de processus adaptés pour gérer les risques numériques :

- Nommer des responsables dédiés à la gestion des risques opérationnels et numériques.
- Établir un cadre de gestion des risques incluant des politiques claires, des procédures, et des métriques de suivi.
- Mettre en place des comités pour examiner régulièrement l'état des risques et approuver les plans d'action.

Ainsi, il faut un *ICT Risk Officer* qui reporte soit à la direction soit à un comité dédié aux risques.

3. Surveiller les fournisseurs tiers

Les tiers, en particulier les fournisseurs critiques, doivent être évalués et surveillés :

- Mettre en place un processus d'évaluation initiale des fournisseurs pour vérifier leur résilience numérique et leur conformité.
- Inclure des clauses contractuelles spécifiques liées à la sécurité, à la notification des incidents et à la continuité des services.
- Auditer régulièrement les fournisseurs pour s'assurer qu'ils respectent les exigences de sécurité.

Pour que la surveillance soit permanente, il s'agit de faire la démarche une première fois. Définir le contenu d'une due diligence peut prendre du temps, pensez à vous y mettre tôt assez.

4. Tester la résilience

Les tests réguliers permettent de vérifier la capacité de l'organisation à faire face aux incidents :

- Réaliser des tests d'intrusion pour identifier les failles dans les systèmes.
- Simuler des scénarios d'incidents majeurs, tels que des cyberattaques, pour évaluer les temps de réponse.
- Effectuer des exercices de reprise après sinistre pour garantir la continuité des opérations.

La difficulté est d'implémenter les outils adéquats de *Static/Dynamic Application Security Testing*. A cela s'ajoute l'identification des données critiques et dont l'intégrité devra être vérifiée après chaque incident majeur.

5. Établir un plan de continuité

Un plan de continuité efficace est essentiel pour minimiser les interruptions en cas de crise :

- Définir des procédures claires pour redémarrer les systèmes critiques après un incident.
- Assurer la redondance des infrastructures, notamment en matière de sauvegarde des données et de connectivité.
- Tester régulièrement ce plan pour s'assurer qu'il est opérationnel.

Il est probable que les procédures de DRP/BCP soient déjà existantes. Une simple mise à jour avec la notion de criticité revue dans les registres et catalogues permet alors de plus facilement s'assurer que les services critiques soient restaurés au plus tôt.

6. Notifier les incidents

La rapidité et la transparence dans la gestion des incidents sont fondamentales :

- Établir un protocole clair pour identifier, classer et documenter les incidents majeurs.
- Mettre en place un processus pour notifier rapidement les autorités compétentes (conformément aux délais réglementaires) et les parties prenantes affectées.
- Analyser les incidents après coup pour en tirer des leçons et améliorer les processus.

Une cartographie claire permet de prioriser les actions de sécurisation en fonction de l'importance des systèmes et des risques associés.

Une procédure et des modèles de documents aideront en ce sens. Certains outils peuvent faciliter la communication mais assurez-vous que les personnes adéquates soient impliquées dans les étapes de notification.

7. Former le personnel

Les employés doivent être conscients des risques numériques et des obligations associées :

- Mettre en place des formations régulières sur les bonnes pratiques en cybersécurité.
- Former les équipes aux procédures de gestion des incidents et de reprise après sinistre.
- Sensibiliser au rôle de chacun dans la conformité et la résilience de l'organisation.

Bien que cela s'avère clair, s'assurer de la bonne compréhension de chacun n'est pas aise.

DORA au quotidien

Une fois la phase de transition passée, il s'agit de maintenir le niveau de conformité en effectuant des opérations régulières :

1. Surveillance continue

La surveillance continue implique l'utilisation de systèmes et d'outils pour suivre en temps réel les menaces et les vulnérabilités dans les environnements numériques. Cela inclut :

- La détection proactive des anomalies dans les systèmes via des outils de surveillance automatisés.
- Le suivi des journaux d'événements pour repérer des activités suspectes.

- L'analyse des informations sur les cybermenaces (*threat intelligence*) pour anticiper les attaques.
- La gestion des correctifs pour identifier et corriger rapidement les failles.

Les outils ne sont pas directement liés à DORA mais DORA renforce le besoin d'être à jour.

2. Mises à jour régulières

Les systèmes, logiciels et processus doivent être régulièrement mis à jour pour rester protégés face aux nouvelles menaces. Cela comprend :

- La mise en œuvre des derniers correctifs de sécurité pour éviter l'exploitation des vulnérabilités.
- L'adaptation des politiques et procédures internes pour tenir compte des évolutions réglementaires ou technologiques.

Un processus d'audit robuste permet de vérifier la conformité et de détecter les lacunes.

- L'évaluation périodique des systèmes pour identifier les besoins d'amélioration ou de modernisation.

Chaque année, une revue des procédures est importante pour s'assurer qu'elles correspondent toujours a la réalité du terrain mais aussi pour apprendre des retours acquis durant l'année.

3. Audit et reporting

Un processus d'audit robuste permet de vérifier la conformité et de détecter les lacunes, tandis que le reporting garantit la transparence. Cela implique :

- La documentation systématique des incidents de cybersécurité, y compris leur impact et les mesures prises.
- La réalisation d'audits internes et externes pour évaluer les contrôles en place.
- La préparation de rapports réguliers à destination des autorités réglementaires et des parties prenantes internes.

Ces audits s'avèrent certainement la partie la moins fun et pourtant très importante puisqu'il s'agit de comprendre les fournisseurs. Ce type de documentation sera également le point d'entrée de l'ensemble des régulateurs.

4. Formation continue

Les employés sont souvent la première ligne de défense contre les cybermenaces. Une formation continue est essentielle :

- Sensibilisation aux bonnes pratiques en cybersécurité (ex. : gestion des mots de passe, détection des tentatives de phishing).
- Programmes de formation réguliers sur les nouvelles obligations réglementaires, comme DORA.
- Simulations d'incidents pour former les équipes à réagir efficacement face à une crise.

Encore une fois, l'utilisation d'approches moins contraignantes sera favorisée. Si l'apprenant considère cette approche comme telle, il associera généralement la règlementation de la sorte, non pas pour protéger mais pour restreindre.

5. Tests fréquents

Pour garantir la résilience, les entreprises doivent effectuer des tests réguliers :

- Tests d'intrusion pour identifier les faiblesses des systèmes.
- Exercices de reprise après sinistre pour vérifier la capacité à redémarrer les opérations après une panne.
- Simulations de scénarios de cyberattaques pour évaluer la réaction des équipes et des systèmes.

Si les outils de SAST / DAST sont en place, les tests sont aisément effectués sur les données. Cependant, des tests de reprise après sinistre seront généralement encore effectués à la main, à défaut d'outils adéquats et qui ne sont généralement introduits que dans des organisations très avancées.

6. Suivi des fournisseurs

Les fournisseurs tiers, notamment ceux critiques comme les prestataires de cloud, doivent être constamment surveillés :

- Évaluation régulière de leur performance et de leur conformité aux exigences contractuelles et réglementaires.
- Suivi de leur résilience, y compris leur propre gestion des risques et leur capacité à répondre aux crises.
- Mise à jour des contrats pour inclure des clauses spécifiques à la cybersécurité et à la continuité des services.

Les due diligences et le suivi d'indicateurs clés devraient permettre de répondre à ce besoin.

Ces actions quotidiennes garantissent non seulement la conformité avec DORA mais aussi avec les buts ultimes de DORA en renforçant la capacité de l'entreprise à prévenir et gérer les crises dans un environnement numérique dynamique et complexe.

> 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.

ChatGPT, DEUX ANS DÉJÀ, ET LA CYBER ?

Il y a deux ans Sam Altman d'OpenAI annonçait le lancement et l'accès pour tous à ChatGPT, avec cette phrase "essayez de discuter avec lui" !

Cela fait quatre ans que notre monde en général et la très grande communauté IT en particulier, sont bouleversés par l'émergence de l'intelligence artificielle. Non, ce billet n'est pas le dix-millionième article (du mois) qui parle de l'impact profond, systémique, pour utiliser un mot de la crise financière des années 2010, mais qui pourrait vite revenir à la mode. Non, ce billet est en plus une vision factuelle, un angle de vue, des déclinaisons de l'IA en cybersécurité.

Récemment, j'ai assisté à une conférence aux USA dans mon domaine la cybersécurité, plus précisément les sujets liés à l'IAM les identités et leur protection constante, les identités axe d'attaque et de vols de données. L'identité est le premier point de contact digital de tout utilisateur de tout système numérique.

Managed services cyber pour la gestion des identités

Donc le sujet n'était pas l'IA, le sujet était autour de l'identité numérique, et l'orateur était le CIO d'une société d'assurance médicale et fonds de pension. L'auditoire était captivé par les sujets de *managed services cyber* appliqués à la gestion des identités, la fédération des identités, le contrôle permanent des rôles et droits, etc. etc., bref un sujet immense en cyber, et lorsqu'à la fin, l'orateur s'est rendu compte qu'en trente minutes il n'avait pas dit un seul mot d'IA. Il s'est excusé, je pensais qu'il était ironique, mais non, il ne rigolait pas en expliquant à quel point parler d'IA est devenu un automatisme pour tout sujet de conférence ou d'article.

L'impact de l'IA en cybersécurité

Cela fait quatre ans que GPT-3 a été publié sous forme d'API, point de départ pour les développeurs de son utilisation dans des nombreuses applications. Mais le coup de départ et le succès fulgurant ont été donnés il y a deux ans quand ChatGPT a été lancé à tous ! Aujourd'hui, juste deux ans plus tard, 250 millions d'utilisateurs discutent avec les chatbot AI, le robot ChatGPT et l'entreprise OpenAI est valorisée 157 milliards de dollars (pour 3 Md$ de revenus).

Mais quel impact concret de l'IA en cybersécurité ?

D'abord le fait que ChatGPT a mis en lumière la performance des modèles d'IA de très grande taille (LLM – Large Language Models tels que Gemini de Google ou GPT d'OpenAI) entrainés grâce à des quantités gigantesques de données, constitue des points de sensibilité, de fragilité de l'IT. Cela nécessite de plus en plus de puissance de calcul (et de l'énergie).

Le premier réflexe en cybersécurité est de protéger ces collecteurs de données et ces machines tournant d'algorithmes qui traitent le cœur de la donnée, du savoir-faire d'un métier, d'une entreprise, des humains.

Aujourd'hui ce sont les éditeurs et constructeurs de solutions cybersécurité tels que Crowdstrike, Google SecOps, ou Palo Alto, et bien d'autres bien sûr, qui sont les premiers à déployer de manière concrète l'IA générative dans leurs solutions de SIEM, d'EDR, *de threat intell*, de scan et analyse des vulnérabilités, etc. etc. Ce sont les éditeurs qui font profiter les analystes et autres ingénieurs cyber de ces solutions.

Démocratiser l'accès aux technologie IA auprès des CISO

Le temps est aussi venu pour les sociétés de services, les MSSP (Managed Security Services Providers) d'utiliser des fonctions d'IA dans leur travail quotidien. Nous le faisons déjà dans l'analyse des signaux faibles, nous le faisons dans la lutte contre le phishing, vecteur de propagation des attaques ransomware, nous commençons à le faire dans l'IR (Réponse Incident) et le forensic, etc. etc.

Les acteurs du service jouent aussi un rôle pour démocratiser l'accès aux technologies IA auprès des CISO.

Mais cela reste un plus, une option d'aide supplémentaire, aucunement, pour l'instant du moins, un envisageable remplacement humain. Les acteurs du service jouent aussi un rôle pour démocratiser l'accès aux technologies IA auprès des CISO, à travers des interfaces adaptées, des chatbots spécifiques, etc.

Le D comme Disponibilité du modèle fonctionnel DICP-C de la cybersécurité !

Un autre impact de l'IA est aussi au niveau de la continuité business, de la résilience des applications basées sur l'IA, car la généralisation des applications dopées à l'IA ou rendues ou devenues critiques par l'adoption rapide, nécessite une continuité d'accès, de performances réseaux, systèmes, cloud, etc. C'est justement le ''D'', comme disponibilité, du modèle fonctionnel DICP-C de la cybersécurité !

Pour les sociétés de services et d'ingénierie en cybersécurité, l'IA générative, au-delà de l'usage en tant qu'aide ou complément au mode run des MSSP, sera aussi un nouveau domaine de conseil car il faudra créer les modèles d'IA, et les interfaces d'usages.

Enfin, l'arrivée des modèles agiles, adaptés au cas précis de la cybersécurité, les modèles de taille réduite (SLM, Small Language Models) améliorent l'adoption et la diffusion car ils nécessitent moins de ressources tout en apportant une IA spécialisée.

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

Accompagner les PME
POUR LA PROTECTION DE LEURS SYSTÈMES ET DONNÉES EST UNE PRIORITÉ

A l'heure où les attaques se multiplient et les vulnérabilités technologiques sont largement exploitées, la cybersécurité reste une préoccupation pour toutes les entreprises. Toutefois, les PME, souvent moins bien équipées que les grandes entreprises, sont confrontées à des défis croissants pour protéger leurs systèmes et données. Christophe Levier Directeur Cloud & Cybersécurité de Micropole s'est prêté au jeu des questions – réponses.

Comment expliquez-vous que plus de 60 % des PME/PMI n'aient jamais réalisé d'audit de sécurité, malgré l'augmentation des cyberattaques et leur vulnérabilité croissante ?

Plusieurs explications peuvent éclairer cette situation. Malgré la forte médiatisation des cyberattaques, les efforts de communication de l'ANSSI et les dispositifs d'aides et de subventions qui se sont développés très rapidement au cours des 4 dernières années (aide «Cyber-PME » conçue par le ministère de l'Économie et des Finances, « Chèques cyber » en Île-de-France, audits proposés par BPI France ...), les PME ne disposent pas toujours d'une Direction des Systèmes d'Information (DSI) ou d'un Responsable de la Sécurité des Systèmes d'Information (RSSI).

Ainsi, dans les sociétés les mieux organisées, ces deux fonctions reposent sur la même personne. Elles vont donc nommer des cadres qui ont d'autres attributions à ces tâches. Dans la majorité des cas, il ne s'agit pas de professionnels de l'informatique, ils ne sont donc ni formés aux enjeux des risques informatiques, ni aux usages des solutions et services nécessaires à la résilience face aux cybermenaces. Le temps consacré aux opérations IT ou de sécurité est ainsi très limité.

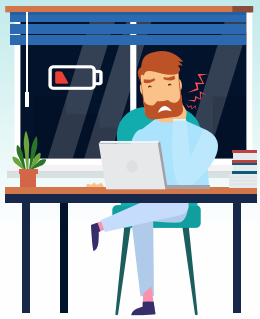
De plus, les dirigeants de PME ont très souvent le sentiment d'être à l'abri des cybermenaces car leur société n'est pas implantée à l'international, pas médiatisée, et elle dispose d'une infrastructure informatique modeste. Tant qu'un incident majeur n'a pas eu lieu, les dirigeants n'intègrent pas le

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.

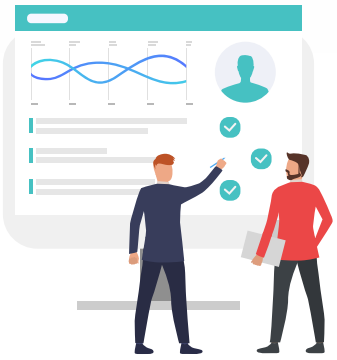
PROMODAG REPORTS PERMET LA CONFORMITÉ AVEC LE DROIT À LA DÉCONNEXION

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

CHRISTOPHE LEVIER

risque cyber dans leur gouvernance. Par ailleurs, ils ne vont pas chercher les informations sur les offres d'audit subventionnées, qui pourraient pourtant être réalisés avec un budget limité (ANSSI, BPI France, Conseil Régional...).

A noter que les budgets liés à la cybersécurité dans les PME sont souvent très restreints, voire inexistants. La sécurité devrait représenter au minimum 6% des investissements informatiques annuels. En outre, le recours à des services de RSSI à temps partagé reste très marginal en Europe comparé aux tendances que nous observons aux Etats-Unis depuis une dizaine d'années.

Les directives NIS2 et DORA vont également contraindre les PME concernées par ces réglementations européennes à passer par le processus d'audit cybersécurité pour avoir un inventaire de leurs vulnérabilités et de ses non-conformités.

Enfin, les PME souhaitant bénéficier des aides et subventions pour la cybersécurité se heurtent souvent à un parcours administratif long, complexe et décourageant.

Quels sont les principaux obstacles qui freinent les PME dans la mise à jour régulière de leurs équipements de sécurité, sachant que 80 % ne disposent pas d'équipe dédiée à la cybersécurité ?

La multiplication des équipements et logiciels de cybersécurité rend les mises à jour essentielles, mais de plus en plus complexes. Elles nécessitent du personnel qualifié capable d'administrer ces solutions et, si besoin, de déclencher des processus de réversibilité ou d'intégrer des correctifs rapidement (par exemple, la mise à jour de CrowdStrike le 19 juillet 2024 qui a généré une panne informatique mondiale).

Nous conseillons aux PME d'être accompagnées par des cabinets de conseil spécialisés en cybersécurité pour les opérations de maintien en condition opérationnelle (MCO) de leur infrastructure sécurité. Ces services restent généralement financièrement très accessibles.

Les protections standards, comme les firewalls et antivirus, ne semblent pas suffisantes pour protéger les PME. Quelles sont vos recommandations ?

En effet, les PME utilisent souvent des équipements de sécurité très basiques (firewall, antivirus, proxy), rarement mis à jour et supervisés. Dans un contexte de menaces actuelles sophistiquées, ces protections ne suffisent pas.

Les entreprises doivent mettre en place des solutions plus modernes : EDR (End Point Detection Response), NDR (Network Detection Response), XDR (Extended Detection Response), IPS (Intrusion Prevention System), IDS (Intrusion Detection System), protection DNS, solution anti-phishing, DLP (Data Loss Prevention), Firewall Applicatif (WAF) ...

De plus, les PME utilisant des services Cloud doivent impérativement mettre en œuvre des solutions de sécurité adaptées aux environnements des hyperscalers. En effet, le client reste responsable de la sécurité des environnements déployés dans un Cloud public, ce qui est souvent oublié.

A noter que les budgets liés à la cybersécurité dans les PME sont souvent très restreints, voire inexistants.

L'autre solution est de recourir à des services externes ou managés via des sociétés spécialisées, qui maîtrisent les équipements de dernière génération et ont adapté leurs services aux besoins des PME. Ces dernières peuvent ainsi profiter des mêmes solutions et services que les grandes entreprises : SOC (Security Operation Center), CSIRT (Computer Security Incident Response Team).

Enfin, il est absolument stratégique pour une PME de mettre en place un processus de gestion de crise et une solution de reprise d'activité (PRA) en cas d'incident de cybersécurité.

> Par Sabine Terrey

Maturité cyber & investissements en France

Les entreprises françaises se considèrent plutôt matures sur les questions de sécurité, malgré une inquiétude croissante ...

Le manque de connaissances et de préparation à la mise en conformité sur la réglementation cyber est préoccupant avec les échéances dépassées pour la mise en conformité (DORA, GDPR, Cybersecurity Act) ou arrivant à échéance (NIS 2).

La priorité des investissements n'est pas axée sur la conformité, mais sur la prévention des cyberattaques avec une protection sur les points terminaux de l'infrastructure : antivirus et les pare-feux (24 %), et solutions de sauvegarde (17 %).

Conformité réglementaire NIS2 & DORA

Ainsi, le manque de connaissances et de préparation lié à la réglementation doit alerter.

Si on s'arrête sur NIS 2 :

- 23 % des décideurs n'ont jamais entendu parler de NIS 2 (évolution réglementaire de la norme NIS)
- 24 % ne connaissent NIS 2 que de nom

Si on s'arrête sur DORA :

- 26 % ne connaissent pas les principes du règlement DORA
- 26 % ne connaissent que le règlement DORA pour les services financiers

Si le RGPD semble maîtrisé (48%), le Cybersecurity Act et l'AI Act, sont connus par moins d'un tiers des personnes interrogées.

Compréhension & Freins

La compréhension de ces réglementations est un facteur essentiel dans la capacité d'anticipation et de préparation à la mise en conformité :

- 34% sont assez familiers avec le règlement NIS 2
- 32% avec DORA

Côté NIS 2, 24% des entreprises sont prêtes, 45% investissent pour se mettre en conformité, 24% veulent démarrer des projets d'investissement sans calendrier mentionné.

Toutefois, 27% sont déjà prêtes à se mettre en conformité avec l'AI Act, entré en vigueur en août 2024, mais 22% des entreprises ne considèrent pas cette question comme prioritaire.

Alors quels sont les freins ? Pour NIS 2, on observe une méconnaissance des questions réglementaires (33%) et un manque de ressources humaines (33%).

Des investissements stagnants

Les entreprises françaises investissent en moyenne 38 % de leur budget informatique annuel dans les ressources de sécurité.

Les PME et ETI investissent le plus dans leur sécurité (+5 points dans le segment 250-499 salariés par rapport au segment 3 000-9 999 salariés), soit entre 41% et 60% du budget annuel total.

Coté secteur d'activité, 39 % des entreprises du secteur public investissent moins de 20 % de leur budget annuel, contre 15 % dans le secteur des nouvelles technologies et 19 % dans le secteur des services financiers.

Source Etude « État de la maturité cyber et des investissements en France » Okta & IPSOS

AZURE BACKUP, DE BELLES ÉVOLUTIONS POUR UNE SOLUTION CLÉ EN MAIN

L'évolution des services sur le Cloud Azure, que ce soit en termes de nouveautés ou d'améliorations, c'est une histoire presque sans fin. Les évolutions sont constantes. Ce qui n'existait pas il y a quelques semaines peut apparaitre, ce qui existe déjà est mis à jour en continu, pour faire évoluer des fonctionnalités existantes ou en proposer de nouvelles.

Un très bon exemple est la fonctionnalité de sauvegarde, qui ajoute au fil des mois des fonctionnalités complémentaires et surtout, ajoute des possibilités de backup pour des services non couverts au départ. Ce service de backup a été présenté il y a un peu plus de 2 ans dans cette même revue, mais il y a depuis beaucoup de nouveautés...

La suite Azure Backup est donc de plus en plus complète. On peut parler de suite puisqu'exploiter les sauvegardes Azure, c'est exploiter *Backup Vaults, Recovery Services Vaults* et *Business Continuity Center.*

Il reste encore, à mon sens un petit point dur avec deux services de backup qui n'adressent pas les mêmes ressources, mais c'est un détail qui ne doit empêcher l'adoption d'une solution de backup managé.

Ces services viennent donc d'évoluer et ce n'est pas terminé. La console de gestion unifiée vient également de connaitre une évolution et même un changement de nom puisque Backup Center devient *Business Continuity Center*.

De nombreuses informations sont à connaitre avant de se lancer dans un projet de sauvegarde complètement managé par les services Azure. Lorsque l'on parle d'une infrastructure de sauvegarde complètement managée par Azure, c'est une infrastructure qui permet de sauvegarder les services (IaaS, PaaS) Azure.

Mais il est aussi possible, même si c'est une solution que l'on rencontre assez peu, d'étendre cela à ses ressources On-Premises. Je ne développerai pas cette partie que je connais peu, mais sachez qu'il est possible d'avoir une seule solution On-premises / Azure directement depuis Azure.

Voici quelques informations importantes pour se mettre à jour et pour ajouter une couche d'automatisation à ses sauvegardes, garantissant ainsi homogénéité, cohérence et performance.

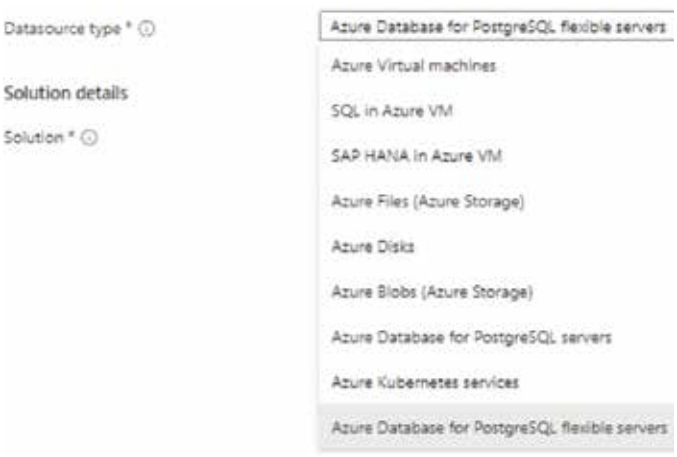
Les dernières nouveautés pour les backups

Petite contrainte dont il a été question ci-dessus avec Azure Backup, la présence de deux services différents. Cette contrainte est partiellement gommée si l'on utilise la console unifiée *Business Continuity Center*.

Je crois qu'il faut définitivement que ce soit le point d'entrée pour les sauvegardes. Elle est pensée pour simplifier l'exploitation, il faut en profiter !

Lorsque l'on choisit de lancer une sauvegarde par le menu *Protectable resources / Configure protection*, on trouve la liste de tout ce qu'il est possible de traiter comme services.

Avec l'arrivée récente des services *Azure Blobs (Azure Storage)*, *Azure Kubernetes services* et *Azure Database for PostgreSQL flexible servers*, il ne manque plus grand-chose et cette liste est pratiquement exhaustive.



Il faut noter que certains choix comme la sauvegarde *Azure Storage* sont traités différemment dans la console. Et c'est la raison principale pour laquelle il faut utiliser *Business Continuity Center*.

Pourquoi cette séparation ? Parce qu'Azure Storage dépend d'un *Recovery Service Vaults* pour les *Files* et d'un *Backup Vaults* pour les *Blobs*. La console « gomme » un peu cette complexité. C'est une philosophie qui part du besoin et qui va à la cible qui couvre ce besoin. Sans cela, il faut connaitre son point d'entrée : *Recovery Service Vaults* ou *Backup Vaults*.

La suite Azure Backup est donc de plus en plus complète.

Comme on retrouve également dans cette console la gestion des stratégies de Backup et les rapports de Backup, on peut se contenter de cela (et c'est même un conseil) pour assurer toute sa gestion. Petite parenthèse sur le sujet des rapports, on trouve du rapport journalier, ce qui facilite l'exploitation sous la forme d'un workbook. Simple, lisible, complet.

On y trouve les ressources protégées, un niveau de sécurité ou un détail des alertes sur les 24 dernières heures.

Mais on peut aller beaucoup plus loin avec un menu dédié à la création de rapports détaillés. Pour récupérer l'historique de sauvegardes sur une plus grande durée ou pour analyser le volume de stockage par instance sauvegardée. Utile par exemple s'il faut une analyse fine des coûts engendrés par les services Azure backup.

Ces rapports sont interactifs pour une analyse depuis la console ou sont envoyés automatiquement et à intervalles réguliers sur une boite mail.

Gestion automatique

Maintenant, avec tout ce que peut Azure Backup, comment peut-on gérer ses sauvegardes de manière encore plus industrielle ?

Si une gestion manuelle est possible au départ à petite échelle, ce n'est pas une solution viable sur la durée et à plus grande échelle.

Et bien la réponse est : par de l'automatisation. Et même par une automatisation managée. Automatiser n'est pas uniquement scripter. C'est une solution envisageable, mais qui demande de l'investissement en temps.

Il y a parfois plus simple et c'est du côté des Azure Policy que l'on va trouver de quoi améliorer (fortement) la gestion automatique de ses backups. La policy Azure est vue avant tout comme un contrôle contraignant de ses ressources. Par exemple au travers des effets *Deny* qui interdisent telle ou telle sorte de déploiements et de comportements. Ou telle ou telle sorte de paramètres. C'est un fait, on interdit par policy.

Azure policy, c'est surtout un puissant outil de gouvernance. Au sens large.

C'est-à-dire que l'on peut aussi, au travers de l'effet *DeployIfNotExists* faire du déploiement ou au travers des effets *Audit* / *AuditIfNotExists* vérifier que les prérequis à la sauvegarde d'un composant sont bien déployés.

Et la catégorie des policy dédiées au Backup est particulièrement fournie !

Ce ne sont que quelques exemples. Cet ensemble permet de faire du Backup automatisé de bout en bout. Ou presque. Mais ce qu'il faut retenir, c'est que cette catégorie évolue très régulièrement en ce moment et propose de plus en plus de possibilités.

De nombreux nouveaux paramètres sont encore en preview. Mais, si je ne déploie jamais une fonctionnalité en preview, je le fais (exceptionnellement) pour les policy. Une raison à cela ?

Ne pas déployer en preview, c'est souvent le faire parce que ce qui est déployé n'est pas couvert par les SLA Azure (*Azure Service Level Agreement).*

Dans le cas des policy, je ne vois pas de risque à le faire, c'est un peu à part, le SLA n'est pas une donnée palpable pour la policy.

Pour s'y retrouver, puisque la liste est longue, il y a dans ces différents choix *quatre grandes familles permettant de préparer ses sauvegardes*.

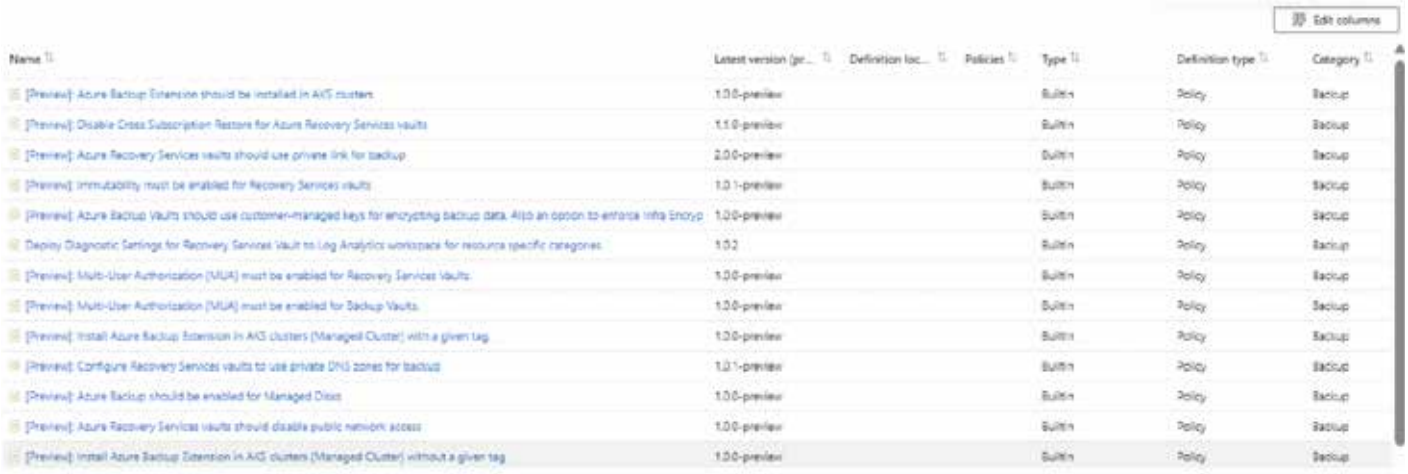
1 / L'identification

Par exemple, pour une sauvegarde AKS, l'audit de contrôle pour l'extension des backups, *[Preview]: Azure Backup Extension should be installed in AKS clusters*. Sans la présence de cette extension, les prérequis ne sont pas couverts.

2 / La remédiation

En partant de l'exemple précédent, une policy qui viendra automatiquement déployer cette extension manquante, *[Preview]: Install Azure Backup Extension in AKS clusters (Managed Cluster) with a given tag*. Avec en complément un filtre au tag qui permettra d'affiner les déploiements.

Azure Backup est maintenant totalement adapté à la sauvegarde d'environnements Cloud complexes et variés.



3 / L'ajout automatique du service (IaaS, PaaS) à un coffre de backup

Si cela n'est pas encore possible pour AKS (il faudra pour l'instant se contenter de l'audit de l'extension puis son ajout), les dernières policy ajoutées en preview le font pour les blobs, les disques managés en plus de machines virtuelles qui sont dans ce scope depuis bien longtemps.

4 / Dernier point, pas le moins important, en complément des sauvegardes, une liste de policy qui traitent de la conformité des coffres de sauvegardes

Plus exactement de la conformité des options / fonctionnalités portées par le coffre.

Quelques exemples particulièrement intéressants avec l'audit de conformité de l'option d'immuabilité du coffre, *[Preview]: Immutability must be enabled for backup vaults*. Ou, autre exemple intéressant, la vérification de l'option Soft Delete (elle conserve pour une durée donnée d'un effacement accidentel) avec la policy *[Preview]: Soft delete must be enabled for Recovery Services Vaults*.

Conclusion

Azure Backup est maintenant totalement adapté à la sauvegarde d'environnements Cloud complexes et variés, par la diversité des services couverts, par sa console de gestion unifiée et par l'ajout de policy Azure qui vont simplifier l'automatisation des sauvegardes.

La liste des services IaaS / PaaS couverts est de plus en plus large et devient presque exhaustive.

Un bon point de départ en 3 étapes

1 / La liste des services IaaS / PaaS couverts est de plus en plus large et devient presque exhaustive.

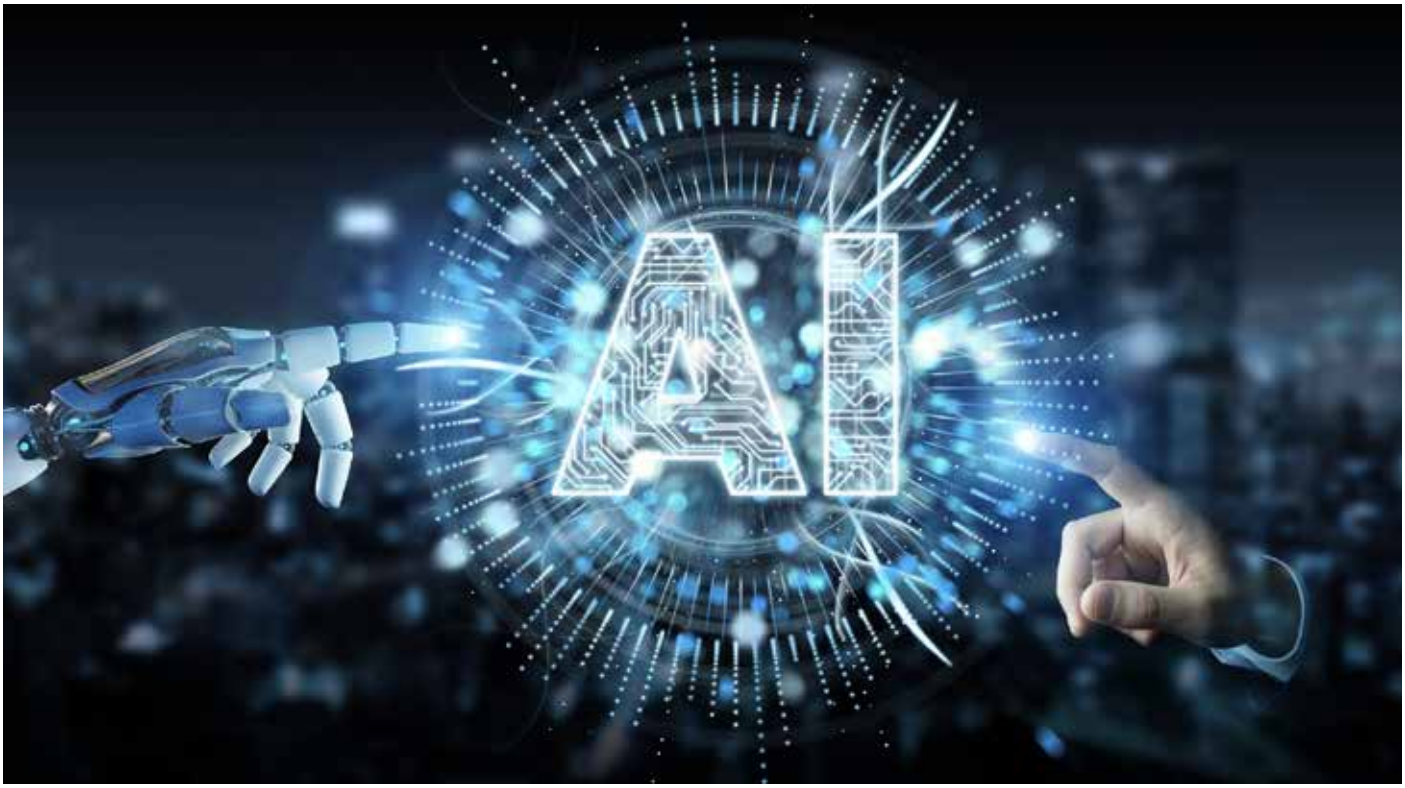
2 / L'utilisation de la console de gestion est conseillée, elle simplifie grandement l'exploitation des sauvegardes Azure. C'est un outil de préparation des sauvegardes, de préparation des stratégies de sauvegarde (maintenant appelées Protection policies) et de visualisation et création de rapports

3 / Les Azure policy sont de plus en plus intégrées aux services de backup et permettent d'automatiser en grande partie ses sauvegardes.

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

L'INTELLIGENCE ARTIFICIELLE EST-ELLE UN FACTEUR DÉCISIF POUR RENFORCER LA RÉSILIENCE NUMÉRIQUE ?

L'Intelligence Artificielle s'invite dans le domaine de la protection des systèmes d'information. Ou plutôt, les intelligences artificielles (ou les différents algorithmes), permettent des analyses prédictives rapides, des identifications précises des menaces et des réponses automatisées.



La promesse, garantir une protection dynamique des infrastructures et des données et augmenter sa robustesse face aux aléas. Car au-delà de la simple protection, la résilience vise la continuité opérationnelle malgré une cyberattaque. L'intelligence artificielle étant une notion générique, voyons précisément ce sur quoi les solutions de détection par IA doivent s'appuyer.

Pour débuter dans l'optique de prévenir, c'est la fondation de la détection, ces solutions doivent comporter une surveillance en temps réel et multi modale. Doivent être analysés en continu le réseau, les systèmes et les comportements utilisateurs, pour y repérer des anomalies subtiles. L'objectif est de révéler les signes précoces d'une violation de sécurité, comme des connexions inhabituelles ou des transferts de données suspects. Adossée à cette analyse en temps réel, l'IA doit exploiter les données collectées pour anticiper les menaces potentielles, détecter des schémas répétitifs de tentatives d'accès et identifier des vulnérabilités logicielles avant leur exploitation. Cependant et contrairement aux systèmes traditionnels, les solutions d'IA améliorent continuellement la précision de leur détection, presque automatiquement. En affinant constamment leurs modèles, elles réduisent significativement les alertes inutiles. Cette optimisation permet aux équipes de sécurité de se concentrer sur les véritables menaces sans être submergées par des fausses alertes. Néanmoins, pour permettre cette amélioration continue, la supervision humaine, chez l'éditeur, est indispensable.

Si la détection précoce d'un incident est préférable, les systèmes à base d'IA peuvent réagir quasiment instantanément lors de la détection d'une menace. Dès lors, des actions automatisées peuvent et doivent être définies en amont : isolation des systèmes infectés, blocage d'adresses IP malveillantes et alerte immédiate des équipes de sécurité. Cette réactivité rapide est essentielle pour minimiser l'impact des attaques et maintenir la continuité opérationnelle. La qualité et la pertinence des réponses dépendront de la préparation de scénarios par les équipes terrain et celle du CSIRT.

L'intégration de l'IA dans la cybersécurité offre des avantages significatifs, mais ne constitue pas une solution ultime. Une stratégie globale doit combiner l'IA avec des pratiques complémentaires, comme la formation des employés, des contrôles d'accès stricts et des évaluations régulières des vulnérabilités. Ces éléments clefs se retrouvent dans les nombreuses règlementations, normes et état de l'art (Guide d'hygiène de l'ANSSI, ISO 27001 et NIS2).

SMART TEEM

« POUR UNE IA RESPONSABLE, PENSÉE COMME UN OUTIL AU SERVICE DE L'HUMAIN »

Si l'intelligence artificielle transforme la manière de travailler, il est essentiel de maitriser les données et proposer des solutions sur mesure. C'est ce que SMART TEEM entend faire en alliant puissance analytique, confidentialité, éthique et transparence pour des décisions éclairées. Entretien avec Mohammed Lahlou, CEO de SMART TEEM.

Pourriez-vous en quelques mots présenter SMART TEEM ?

SMART TEEM, cabinet spécialisé en Data & AI, allie conseil et solutions pour accompagner ses clients dans la mise en œuvre des projets de transformation Data & IA (dès la phase de PoC jusqu'à la mise en service). Depuis sa création en 2018, SMART TEEM s'engage auprès de ses clients à relever leurs défis stratégiques par une approche Data (Data-Driven) et par le développement des solutions Analytics & AI, sur-mesure, performantes répondants aux besoins spécifiques de ses clients.

L'expertise de SMART TEEM couvre l'ensemble du cycle de vie des données : Accompagnement métier / Modélisation & Architecture des données /BI & Reporting / Data Gouvernance / Machine Learning & GenAI ...

Vous évoquez votre positionnement en proposant des offres sur mesure. Pourriez- vous nous en dire plus ?

Chez SMART TEEM, nous plaçons les besoins spécifiques de chaque client au cœur de notre démarche. Notre positionnement repose sur la création d'offres d'accompagnement sur mesure, adaptées aux enjeux stratégiques et opérationnels de nos clients, qu'il s'agisse des projets BI, Analytics, AI ou Move To Cloud ...

Comment accompagnez-vous les clients ?

Notre approche d'accompagnement se base sur 4 points, à savoir le Diagnostic / Audit personnalisé. Nous débutons chaque collaboration par une

+120
exposants

+3000
participants

CYBER SHOW PARIS

29 ET 30 JANVIER 2025

+500
rendez-vous d'affaires 1to1

+100
interventions

À CHAQUE TAILLE D'ORGANISATION, SES SOLUTIONS EN CYBERSÉCURITÉ

L'ESPACE CHAMPERRET
6 rue Jean Oestreicher
75017 Paris

TICKET

> S'INSCRIRE À L'EVENT
CYBERSHOWPARIS.FR

phase d'écoute active et d'analyse approfondie de l'écosystème existant (outils, infrastructures, compétences) pour identifier les besoins et les opportunités.

En second, la Co-construction des solutions. Nous travaillons main dans la main avec nos clients pour concevoir des solutions adaptées, en nous appuyant sur les meilleures technologies du marché (Teradata, Informatica, Power BI, Tableau, Databricks, Dataiku, BigQuery (GCP), Snowflake ..) et en prenant en compte leurs contraintes techniques, budgétaires et organisationnelles.

Puis la mise en œuvre agile. Nos consultants-expert adoptent une approche agile pour garantir des résultats rapides et alignés sur les attentes.

Enfin, la formation et prise en main des solutions. Nous proposons des sessions de formation et d'up-skilling pour les équipes internes afin de les rendre autonomes dans l'utilisation et l'exploitation des solutions mises en place.

La maîtrise des données est le socle de toute IA performante.

En alliant expertise technique, méthodologie éprouvée et écoute client, SMART TEEM transforme les données en un véritable levier de performance et de prise de décision.

MOHAMMED LAHLOU

Revenons sur la maitrise des données. Comment doit être entrainée l'IA selon vous, avec quelles données ? Quelle place donner à l'IA éthique ?

La maîtrise des données est le socle de toute IA performante. Pour l'entraîner, il faut des données de qualité, représentatives et diversifiées, afin d'éviter les biais et de garantir des prédictions fiables. L'éthique, quant à elle, est essentielle : elle impose des modèles transparents, équitables et respectueux des droits des individus.

Chez SMART TEEM, nous croyons en une IA responsable, pensée comme un outil au service de l'humain, et non l'inverse. Nous intégrons dès la conception des mécanismes d'audit et de supervision, pour allier innovation, performance et valeurs fondamentales. Une IA utile et éthique, voilà notre engagement.

> Par Sabine Terrey

Actions pour un environnement de travail numérique durable

Doubler la durée de vie des équipements IT et maintenir un haut niveau de satisfaction chez les utilisateurs est tout à fait possible. Découvrons les actions à adopter pour une démarche positive et durable.

57 % des émissions de carbone du secteur des TIC proviennent des équipements et espaces de travail. Découvrez les informations et recommandations pour améliorer la prise de décision en matière d'informatique et les stratégies de responsabilité sociale d'entreprise (RSE).

Allonger le cycle de vie

On observe des niveaux élevés de gaspillage endémique dans l'industrie informatique. A noter que 79 % de l'empreinte carbone d'un ordinateur portable est produite lors de sa fabrication et que chaque nouvel appareil génère environ 338 kg d'équivalent CO2 avant même d'être utilisé. Allonger le cycle de vie est donc une priorité.

Les cycles de vie des appareils peuvent être prolongés sans compromettre la satisfaction de l'utilisateur : ainsi en augmentant le cycle de renouvellement standard de 3 à 4 ans, les entreprises peuvent réduire de 25 % les émissions de l'appareil sans en dégrader les performances ni affecter l'expérience de l'utilisateur.

Reconditionner

Le rafraîchissement des appareils en fonction des données de l'état de fonctionnement, combiné au reconditionnement, peut permettre d'atteindre une durée de vie de 8 à 10 ans.

Ainsi, 76 % des ordinateurs portables des grandes entreprises peuvent être reconditionnés. Les 24 % restants peuvent faire l'objet d'une mise à jour plus légère ou être recyclés et contribuer à l'économie circulaire.

Impliquer les employés

Il ne faut pas sous-estimer le rôle des employés dans la durabilité de l'informatique : 75% sont prêts à conserver leurs appareils plus longtemps s'ils sont au courant des bénéfices environnementaux d'une telle pratique.

Mais 16 % des appareils restent allumés en permanence. Sensibiliser les employés aux pratiques d'économie d'énergie est un autre priorité.

Informer pour une meilleure efficacité énergétique

L'intensité carbone peut fluctuer jusqu'à 2,3 fois au cours de la journée. Informer les utilisateurs des meilleurs moments pour utiliser le réseau électrique et passer à l'alimentation par batterie est essentiel pour une meilleure efficacité énergétique.

Une gestion durable de l'environnement de travail avec processus et bonnes pratiques n'est ni longue ni coûteuse. Selon Atos, il est important d'accéder à des données exhaustives et en temps réel pour progresser dans la tenue des objectifs environnementaux.

Source : Etude Atos « Accroître la durabilité de l'environnement de travail numérique : une stratégie fondée sur les données pour progresser collectivement » - Atos a analysé avec ses partenaires Nexthink, Tier1 et Circular Computing, 28,5 millions d'appareils utilisés par de grandes entreprises et des entreprises de taille moyenne

Un paysage de la cybersécurité
DE PLUS EN PLUS COMPLEXE EN 2025 !

Les menaces existantes s'intensifient et les vecteurs d'attaques se multiplient.

Face à cela, l'IA joue évidemment un rôle prépondérant, à la fois côté attaque mais aussi côté défense.

Aussi, pour anticiper les prochaines évolutions et aider les organisations à se préparer, découvrons les prédictions des experts Proofpoint qui éclairent sur les tendances clés en matière de cybersécurité pour 2025.

Entre gestion des identités numériques, environnements multicloud, stratégies de données et conformité aux nouvelles règlementations, la mise en place des outils appropriés pour sécuriser les données à travers un éventail d'applications et d'environnements sera une priorité pour les équipes de sécurité.

Les 5 grandes tendances à prendre en compte

• Manipulation des données privées
L'intégration croissante d'agents IA semi-autonomes aux flux de travail va créer de nouvelles vulnérabilités. Les acteurs malveillants n'hésiteront pas à manipuler l'IA en contaminant les données privées utilisées par les LLM, tels que les emails ou documents de travail, avec des informations fausses ou trompeuses.

• Arbitrage entre IA et gestion des risques
Déjà au cœur des réflexions stratégiques des entreprises, l'IA sera bientôt partie intégrante de leur fonctionnement, même si elle reste perçue comme un risque. Les RSSI doivent comprendre comment les employés utilisent les outils d'IA afin d'identifier les potentielles fuites d'informations, tout en maîtrisant les risques associés. Une plus grande transparence sur le fonctionnement des outils d'IA et leur sécurisation est nécessaire.

• Géopolitique, un nouveau champ de bataille
Le cyber espionnage étatique sera toujours étroitement lié aux tensions géopolitiques et ne se limitera plus aux grandes nations. Les opérations des groupes APT refléteront les conflits mondiaux et régionaux. Ces attaques serviront également des objectifs financiers et de propagande, en exploitant la balkanisation des nations pour propager des charges utiles.

Les RSSI doivent comprendre comment les employés utilisent les outils d'IA afin d'identifier les potentielles fuites d'informations

• Augmentation des attaques sur mobile
L'utilisation d'images et de vidéos dans les attaques de smishing sera croissante. Au même titre que pour les SMS, les cybercriminels intègrent des liens malveillants dans des messages multimédias en usurpant l'identité d'organisations légitimes pour inciter les utilisateurs à divulguer des informations sensibles. La similarité avec les SMS classiques et le manque de sensibilisation des utilisateurs à ce vecteur d'attaque contribuent à son efficacité.

• Evolution du rôle du RSSI
Si l'influence du RSSI croît au sein des conseils d'administration, avec une responsabilité accrue en matière d'évaluation et de communication des risques cyber, leur implication opérationnelle en est par conséquent réduite. Une division qui, selon les cas, aura pour conséquence de réduire ou d'élargir le rôle des RSSI, venant complexifier davantage la gouvernance et la question de responsabilité.

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

SMARTDSI

www.smart-dsi.fr

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

Toute organisation DOIT ÉVALUER LE NIVEAU DE SÉCURITÉ DE SES PARTENAIRES

Plusieurs incidents récents, notamment la cyberattaque de Sofinco, filiale du Crédit Agricole, ayant exposé des données bancaires sensibles, montrent qu'il est temps de renforcer la posture de sécurité des entreprises en intégrant des solutions couvrant l'ensemble de leur écosystème. Quelles sont les mesures à adopter pour minimiser les risques et garantir une meilleure sécurité des infrastructures numériques ? Entretien avec Marc-Andre Tanguay, Head of Nerds chez N-able

Pourriez-vous nous présenter N-able ?

N-able est l'un des acteurs historiques du secteur des fournisseurs de services managés (Managed Service Providers, MSP), ayant commencé son activité dès l'an 2000. Nous avons participé à la mise en place du modèle MSP en Amérique du Nord et avons évolué pour accompagner nos partenaires à l'échelle mondiale. Notre objectif est d'aider ces derniers à apporter la valeur de leurs services à un éventail croissant d'entreprises, quelle que soit leur taille ou quel que soit leur secteur, et qui ont besoin de solutions efficaces de gestion des risques cyber en plus des services informatiques traditionnels.

En tant que fournisseur de premier plan en gestion informatique et en cybersécurité, N-able offre aux MSP les outils nécessaires pour fournir des services IT de grande qualité aux petites et moyennes entreprises (PME) du monde entier. En simplifiant les défis complexes liés aux infrastructures IT et à la sécurité, nous proposons une gamme complète de solutions conçues pour renforcer la sécurité, optimiser les opérations et accroître l'efficacité.

Notre portefeuille inclut des plateformes de gestion à distance telles que N-central et N-sight, des solutions de sécurité des endpoints développées avec SentinelOne, des outils de sauvegarde et de récupération des données pour les endpoints et Microsoft 365 grâce à Cove Data Protection, des services de gestion des événements de sécurité (SIEM) avec un SOC 24/7 via notre solution MDR, ainsi que des outils pour la gestion des mots de passe et de la documentation avec Passportal et la protection des emails avec Mail Assure. Ces solutions sont spécifiquement conçues pour permettre aux MSP de protéger leurs clients face à des cybermenaces en constante évolution, tout en facilitant l'extension et l'amélioration de leurs services.

Par ailleurs, nous accompagnons nos partenaires au-delà des outils techniques, en leur offrant des supports de formation, des bootcamps et des sessions dirigées par nos experts internes, les "Head Nerds". Grâce à notre plateforme MarketBuilder, nous aidons également nos partenaires à réussir non seulement dans l'exécution technique de leurs services IT et de cybersécurité, mais aussi dans la gestion et la croissance de leur entreprise.

MARC-ANDRE TANGUAY

Pensez-vous que les cyberattaques ciblant les partenaires sont en hausse ? Les approches de gestion des risques doivent-elles être réévaluées ?

Les MSP sont depuis longtemps des cibles privilégiées des cybercriminels, ce qui oblige à repenser les approches de gestion des risques pour eux-mêmes et leurs clients. Les cybercriminels comprennent l'intérêt stratégique de cibler les MSP, car ces derniers jouent un rôle clé en tant que passerelles vers plusieurs réseaux clients. En attaquant un MSP, ils peuvent potentiellement compromettre un grand nombre d'entreprises clientes.

De plus, les attaquants exploitent la confiance existante entre les partenaires et leurs clients, rendant les activités malveillantes plus difficiles à détecter dans un premier temps. L'augmentation des vulnérabilités dans les chaînes d'approvisionnement, combinée à des tactiques sophistiquées d'ingénierie sociale, a encore renforcé ces risques.

Dans ce contexte en constante évolution, la gestion des risques doit s'élargir pour inclure les relations avec les tiers et les vulnérabilités de la chaîne d'approvisionnement. La sécurité ne peut plus être confinée aux seules opérations internes ; elle devient une responsabilité partagée qui inclut partenaires, fournisseurs et autres parties prenantes externes. Chaque organisation doit évaluer le niveau de sécurité de ses partenaires et intégrer ces informations dans une stratégie globale de gestion des risques.

Quelles recommandations donneriez-vous ? Quelles mesures devraient être prises pour minimiser ces risques ?

Pour faire face à la montée des cybermenaces et au risque commercial que représente un retard dans l'adoption de solutions adaptées, les MSP doivent intégrer la gestion des risques au cœur de leurs services. Cela nécessite une approche globale qui combine les dimensions humaines, procédurales et technologiques.

Un modèle de sécurité "Zero Trust" est fortement recommandé : il repose sur le principe qu'aucun appareil, individu ou système ne doit être considéré comme digne de confiance par défaut, avec une vérification continue des droits d'accès. Une gestion rigoureuse des identités et des accès (IAM), incluant des mécanismes d'authentification multi-facteurs et des politiques limitant les accès au strict nécessaire, constitue une base essentielle pour renforcer la résilience.

La segmentation des réseaux permet de contenir les incidents en cas de violation, tandis que des solutions de gestion des correctifs, telles que notre moteur de Patch Management, garantissent que tous les appareils disposent des dernières mises à jour de sécurité. L'erreur humaine demeurant une vulnérabilité majeure, il est crucial de sensibiliser les employés et les partenaires aux tactiques de phishing et aux techniques d'ingénierie sociale. Des audits réguliers et des évaluations des risques, y compris au niveau des chaînes d'approvisionnement, permettent d'identifier et de corriger les faiblesses avant qu'elles ne soient exploitées par des attaquants.

Historiquement, la mise en œuvre de ces capacités représentait un obstacle financier majeur pour de nombreux MSP, en raison des coûts liés à la création d'opérations de sécurité 24/7. Les solutions proposées par N-able permettent désormais aux MSP de toutes tailles de surmonter ces obstacles en leur fournissant des capacités avancées et des opérations continues, sans nécessiter de lourds investissements en recrutement.

Enfin, l'entrée en vigueur de la directive NIS 2 souligne l'importance d'une gestion rigoureuse des risques en matière de cybersécurité. Cette directive élargit les obligations des entreprises en matière de sécurité, incitant un plus grand nombre de secteurs à adopter des normes cohérentes et robustes.

En intégrant des stratégies globales de gestion des risques et en respectant les directives évolutives telles que NIS 2, les MSP peuvent réduire leur exposition aux menaces, renforcer la résilience de leur entreprise et répondre à la demande croissante des entreprises en quête de conformité réglementaire et de solutions de cybersécurité avancées.

> Par Sabine Terrey

Synchronisation Multi-Tenant :
POUR QUOI FAIRE ?

On ne compte pas le nombre d'entreprises ou d'organismes qui tous les jours travaillent sur des projets transverses et qui ont, la nécessité de partager des documents, de se réunir voire de communiquer plus largement. L'environnement Office 365 offre, il est vrai, un environnement de travail confortable car intégré, mais qui accusait certaines limites fonctionnelles dès lors que l'on sortait du cadre d'un simple tenant.

Autrement dit, au sein d'un même et unique tenant l'expérience fonctionnelle des utilisateurs est homogène, mais si l'entreprise a la nécessité de travailler avec ses filiales ou ses partenaires de façon plus intégrée, l'expérience multi-tenant devenait compliquée.

Posséder plusieurs tenants et offrir la même expérience applicative a été une demande prégnante des entreprises et ce, depuis plusieurs années. Elle semble être en passe d'être désormais couverte avec la synchronisation multi-tenant.

Principes généraux

Dans la quasi-totalité des projets, une des problématiques de départ se concentre sur l'identité. Dans l'environnement « Cross Tenant Synchronisation », il est désormais possible de synchroniser des identités d'un tenant A vers un tenant B et inversement. Cette synchronisation est déclarative et monodirectionnelle.

Autrement dit, la synchronisation entre tenant est configurée comme une synchronisation d'égal à égal à sens unique, ce qui signifie que la synchronisation est configurée entre un tenant source et un tenant cible.

Son mode de fonctionnement peut être manuel voire automatique (toutes les 40 minutes) et peut adresser soit la totalité des identités, soit être limité à un groupe d'individus ou à des utilisateurs désignés par l'administrateur.

Microsoft 365 Copilot.

Révolutionnez votre façon de travailler.

65%

Passent trop de temps à chercher des informations lors d'une journée de travail.

70%

Des personnes délégueraient autant que possible à l'IA pour réduire leur charge de travail.

2x

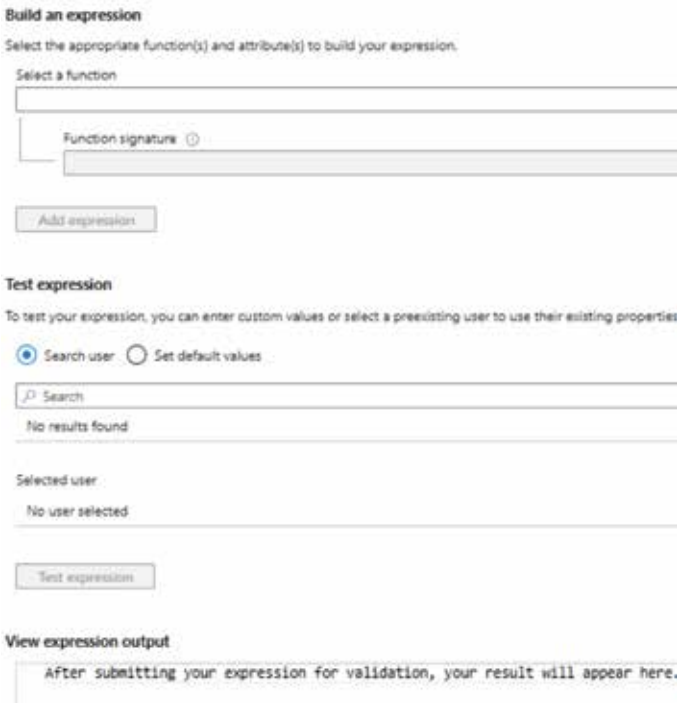
Probabilité qu'un dirigeant affirme que l'IA apportera de la valeur en augmentant la productivité plutôt qu'en réduisant les effectifs.

Révolutionnez votre façon de travailler avec Microsoft 365 Copilot.

Avec nous, vous découvrirez comment intégrer de manière transparente cette technologie révolutionnaire dans votre organisation. Nous pouvons également vous accompagner sur tous les projets d'IA générative et les offres Copilot. Alors pourquoi attendre ? Améliorez les performances de votre équipe, rationalisez vos processus et préparez-vous à la transformation numérique ultime.

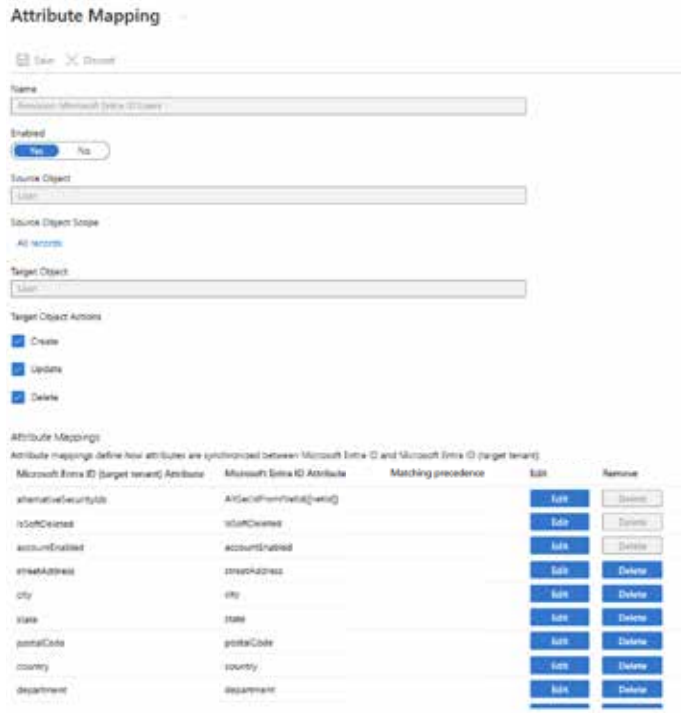
Insight

Un système de requête permettant de filtrer les utilisateurs est également disponible comme le montre la figure suivante.



Par ailleurs, on notera que les comptes invités sont exclus de la synchronisation.

La synchronisation cross tenant permet également de limiter le nombre d'attributs que l'on souhaite synchroniser dans le tenant de destination. La figure suivante illustre la configuration du « mappage d'attributs » d'une synchronisation mono directionnelle.



Ainsi, les entreprises pourront d'une part, isoler les identités à ne pas synchroniser vers le tenant cible et d'autre part, ne faire apparaitre que les valeurs d'attributs qu'elles souhaitent synchroniser.

Quelles licences ?

Comme vous le savez dans l'environnement Office 365, tout est affaire de licence. Pour mettre en place la synchronisation multi-tenant ou Multi-tenant Organisation, aucune licence complémentaire ne vous sera demandée. Autrement dit, avec de simples licences Entra ID P1 ou P2 vous pourrez activer cette fonctionnalité, mais ne vous réjouissez pas trop vite car comme on le verra par la suite, il se pourrait bien qu'il faille acquérir des licences complémentaires.

Les avantages

Un des premiers avantages concerne le cycle de vie des identités. Si un utilisateur quitte l'organisation du tenant A, son identité sera supprimée au prochain cycle dans le tenant B et inversement si les deux organisations partagent leurs annuaires de façon bidirectionnelle.

Le second avantage est de pouvoir distinguer au niveau de Entra ID des personnes véritablement externes à l'entreprise (Compte invité) et des comptes synchronisés (Compte Membre). Cette distinction permettra potentiellement d'accorder selon la nature de l'identité des prérogatives différentes sur l'annuaire de destination.

Et le dernier mais pas le moindre est de permettre de faciliter « applicativement » la vie des utilisateurs. Prenons quelques exemples démontrant la prise en compte de cette synchronisation Cross Tenant par certaines applications Office 365 comme

- Exchange Online
- Microsoft Teams
- Viva Engage

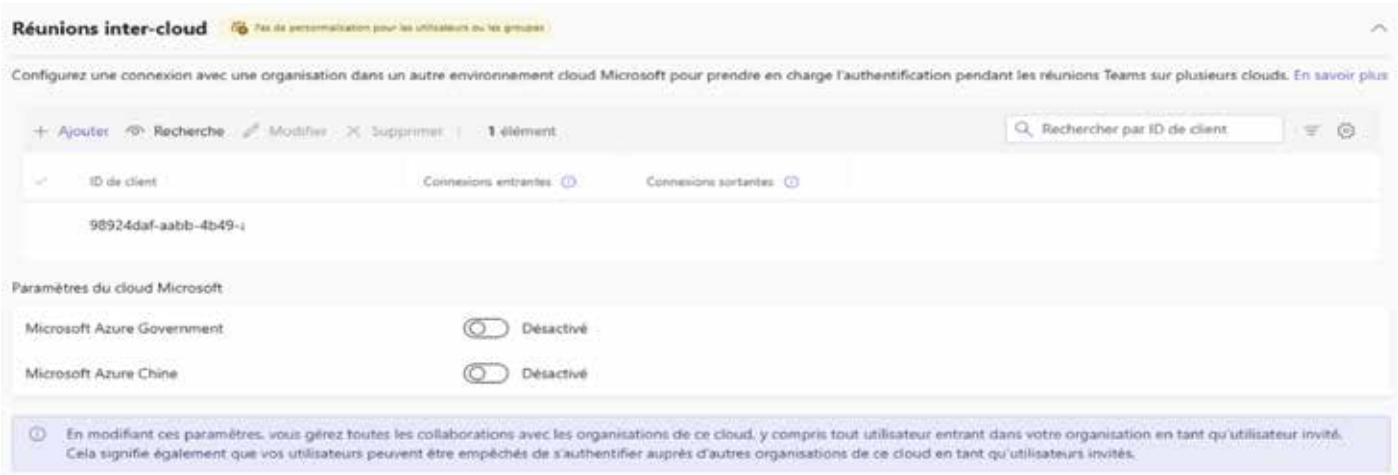
Exchange Online

La conséquence directe de l'application d'une synchronisation cross tenant est que les utilisateurs vont pouvoir « Voir » dans l'annuaire de l'entreprise du tenant A les utilisateurs synchronisés du tenant B. Ils pourront par conséquent résoudre leurs noms et les visualiser dans l'annuaire de l'entreprise de la même façon que leurs collègues. D'un point de vue « expérience » c'est totalement transparent pour les utilisateurs, qui sont certains de disposer d'un annuaire à jour.

On notera que le fait de mettre en place une organisation MTO entre deux tenants ne permet pas de visualiser les plages libres et occupées des utilisateurs placés dans un autre tenant. Ceci est possible mais cela n'est pas lié à un environnement MTO.

Microsoft Teams

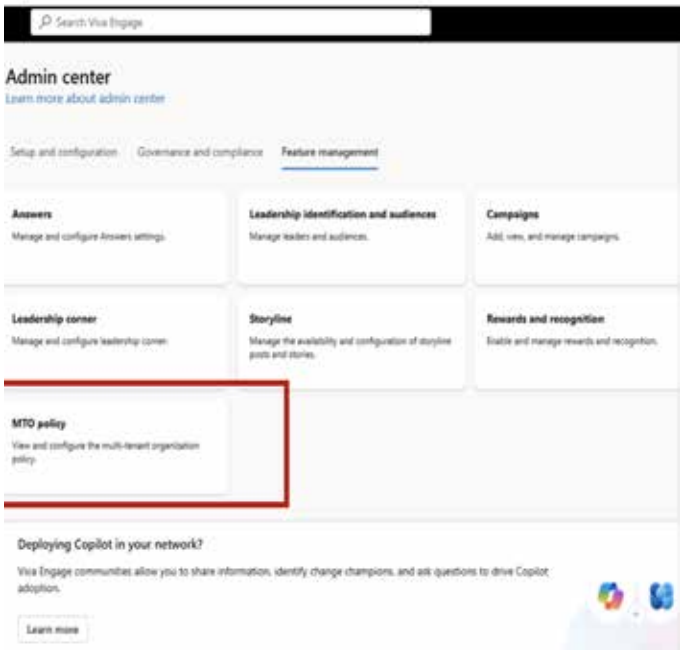
Avec le nouveau client Teams, il est de plus en plus facile de naviguer entre deux tenants et si vous n'avez pas restreint les domaines externes dans votre environnement Teams alors les utilisateurs n'y verront pas de grandes améliorations. Cependant, l'environnement d'administration Teams permet de configurer une authentification Inter-cloud entre les différents participants d'une même réunion mais provenant de tenants différents. Ainsi, les utilisateurs d'un tenant source participant à une réunion organisée par un utilisateur d'un tenant cible pourront s'authentifier plutôt que d'être considérés comme des utilisateurs anonymes. La figure suivante illustre cette possibilité dans l'administration Microsoft Teams



Note : Des problématiques de partage de fichiers entre différents utilisateurs de différents tenants nous ont été récemment remontés à travers le nouveau client Teams Desktop. Par conséquent, prenez soin de bien vérifier que l'application se comporte correctement dans un scénario de MTO.

Viva Engage

Le cas de Viva Engage est un peu différent. Prenons le cas où une maison mère qui veut déployer Viva Engage pour 2 de ses filiales. Le scénario qui devrait s'imposer est de synchroniser tous les annuaires des différents tenants et d'ouvrir le service sur le tenant de la maison mère de façon à ne pouvoir bénéficier que d'une seule organisation Viva Engage dans laquelle tous les utilisateurs puissent se retrouver. La figure suivante issue de l'administration de Viva Engage illustre cette prise en compte.



Nous vous invitons à bien tester les scénarios d'usage si vous envisagez de mettre en place cette solution prometteuse.

Ce scénario est donc possible car Viva Engage sait désormais prendre en compte l'environnement multi-tenant (MTO) mais à certaines conditions détaillées ici : https://learn.microsoft.com/en-us/viva/engage/mto-setup et plus particulièrement si ….

Une licence *Microsoft Viva Suite ou Communications et Communautés* est attribuée à tous les utilisateurs des tenants concernés. Rappelez-vous : tout est affaire de licence !

Cela étant dit, la synchronisation multi-tenant est assez récente et la prise en compte de ces nouvelles fonctionnalités par les applications 0365 est encore plus récente. Aussi, nous vous invitons à bien tester les scénarios d'usage si vous envisagez de mettre en place cette solution prometteuse qui devrait considérablement simplifier les problèmes de gestion des identités.

Pour cela, faites vous accompagner par une société spécialisée, installez un environnement de préproduction, et utilisez les services Fastrack de Microsoft si vous en avez la possibilité.

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

La cartographie du SI
EST UN OUTIL STRATÉGIQUE FONDAMENTAL

La cartographie du Système d'Information est essentielle pour les entreprises souhaitant avoir un inventaire global, optimiser les processus et piloter les projets avec agilité. C'est pourquoi le fondateur de Cartographit, David Bougearel a accepté de répondre à quelques questions pour mieux appréhender cette démarche.

Qu'est-ce que la cartographie du SI ? Pourquoi est-elle essentielle ?

La cartographie du système d'information (SI) est une modélisation visuelle et structurée de l'ensemble des composantes d'un SI, incluant les applications, les serveurs, les réseaux, les flux de données, ainsi que les interactions internes et externes. Elle permet une documentation exhaustive de chaque composant du SI, facilitant ainsi sa gestion, son optimisation et sa gouvernance.

En intégrant des perspectives métiers, applicatives et techniques, la cartographie permet une compréhension holistique et un contrôle accru d'un SI dont la complexité ne cesse de croître.

La cartographie est essentielle pour assurer une maîtrise complète du SI, et ses bénéfices se manifestent de plusieurs manières :

- **Sécurité et gestion des risques :** Elle permet d'identifier les systèmes critiques ainsi que les vulnérabilités potentielles, ce qui favorise une approche proactive de la gestion des risques.

- **Optimisation des ressources :** En dévoilant les redondances et les sous-utilisations, elle favorise une meilleure allocation des ressources et permet des réductions de coûts substantielles.

- **Conformité et gouvernance :** La cartographie organise de manière systématique les informations du SI, facilitant les audits et assurant la conformité aux normes en vigueur, telles que le RGPD et ISO 27001.

- **Outil de compréhension, de découverte et de communication :** La cartographie simplifie la représentation d'un système complexe, offrant une vue claire et accessible.

Elle facilite l'analyse, la planification et la communication entre les différentes parties prenantes. En intégrant les perspectives métiers, applicatives et techniques, elle crée un lien entre les pôles souvent isolés, favorisant la collaboration et le partage des connaissances. Cela améliore la synergie entre les équipes IT, métiers et gouvernance, renforçant ainsi la cohésion et l'alignement des objectifs.

La cartographie renforce la cybersécurité du SI. Pouvez-vous nous en dire plus ?

En matière de cybersécurité, la cartographie du SI est un outil stratégique fondamental. Elle permet aux organisations de visualiser les composants sensibles de leur infrastructure et les interconnexions entre systèmes. En cas d'incident de sécurité, cette représentation précise est cruciale pour identifier les points d'impact, évaluer l'étendue des dommages, et établir rapidement un plan de réponse approprié. La cartographie contribue également à anticiper les trajectoires d'attaque potentielles, renforçant ainsi la surveillance des points critiques et facilitant la planification de mesures de défense efficaces.

Elle facilite l'analyse, la planification et la communication entre les différentes parties prenantes.

De surcroît, la cartographie facilite l'adoption de stratégies de sécurité modernes, telles que l'approche "Zero Trust", et permet de centraliser l'inventaire des actifs informatiques, offrant ainsi une vision intégrée et à jour. Elle s'impose donc comme un outil incontournable pour améliorer la résilience organisationnelle et répondre de manière proactive aux menaces émergentes.

En fournissant une compréhension claire et structurée des systèmes en place, la cartographie des SI permet de simplifier les processus d'audit et d'accélérer l'obtention de certifications critiques telles que SOC2, ISO 27001, RGPD, NIS2, DORA, assurant ainsi la conformité et la sécurité de vos opérations.

***" Outil indispensable à la maîtrise de son système d'information (SI) et obligatoire pour les Opérateurs d'importance vitale (OIV), la cartographie du SI permet de connaître l'ensemble des éléments qui le constituent pour en obtenir une meilleure lisibilité, et donc un meilleur contrôle. Elle s'intègre dans une démarche globale de gestion des risques."* précise l'ANSSI**

DAVID BOUGEAREL

Si vous deviez donner des conseils pour se lancer, quels seraient-ils ?

Mon premier conseil est de ne pas trop attendre si vous n'avez de vision globale de votre SI. La cartographie constitue la première étape indispensable pour renforcer la cybersécurité de son entreprise. Il est crucial d'adopter une approche proactive et anticipative, non seulement pour se préparer à d'éventuelles attaques, mais aussi pour réduire la surface d'exposition aux menaces. Cette anticipation permet de détecter et de corriger les vulnérabilités avant qu'elles ne soient exploitées, assurant ainsi une posture de sécurité plus robuste.

Mon deuxième conseil est de suivre une méthode et de ne pas vouloir tout faire d'un coup. Pour se lancer dans la cartographie du SI, voici quelques recommandations :

1. **Définir un périmètre clair et impliquer les parties prenantes :** Il est essentiel de commencer par identifier les systèmes critiques et les données sensibles à cartographier. Impliquer les parties prenantes, notamment les responsables métiers, techniques, et de la sécurité, dès le début garantit une vision partagée et exhaustive.

2. **Adopter une démarche progressive et itérative :** La construction d'une cartographie du SI ne doit pas être une tâche unique et massive, mais un processus continu et évolutif. En optant pour une approche progressive, les équipes peuvent enrichir et détailler la cartographie au fur et à mesure, ce qui permet de maintenir une dynamique de projet positive et évite la surcharge. Cela réduit aussi le risque d'erreurs et de lacunes en rendant les mises à jour plus faciles à gérer.

3. **Choisir des outils adaptés :** Opter pour une solution de cartographie qui facilite la mise à jour des données, propose une visualisation intuitive et permet un partage efficace des informations. Un bon outil doit être suffisamment flexible pour s'adapter aux évolutions constantes du SI, intégrer des fonctionnalités d'automatisation pour réduire la charge manuelle, et offrir des capacités de collaboration qui favorisent la participation des différentes équipes impliquées.

4. **Assurer une mise à jour régulière de la cartographie :** Une cartographie n'a de valeur que si elle reflète fidèlement l'état actuel du SI. Pour garantir la fiabilité des données, il est impératif de mettre en place des processus de mise à jour réguliers, qu'il s'agisse de mises à jour déclaratives, d'importation automatisée ou via des connecteurs. Cela garantit que la cartographie reste pertinente, même lorsque le SI évolue, et assure ainsi une vision précise et en temps réel.

Mon troisième conseil est de choisir le bon outil. Forts de notre expérience en tant qu'architectes et experts en cybersécurité, nous avons développé une solution qui répond à cette problématique majeure des entreprises.

Cartographit se démarque par son interface utilisateur intuitive, qui est conçue pour être accessible aux équipes techniques qu'aux responsables métiers.

Pouvez-vous nous présenter Cartographit ?

Cartographit est une solution collaborative et innovante qui facilite la cartographie du SI pour les entreprises de toutes tailles. Elle se distingue par sa capacité à fournir une représentation dynamique et détaillée des différentes couches du SI (écosystème, métier, applicative, conteneur, infrastructure logique et physique), offrant ainsi une vue complète et compréhensible.

Cartographit se démarque également par son interface utilisateur intuitive, qui est conçue pour être accessible aussi bien aux équipes techniques qu'aux responsables métiers. Cette convivialité favorise une adoption rapide au sein des organisations, garantissant une collaboration fluide entre les différents départements.

Basé sur le guide de l'ANSSI, son modèle de données est capable de s'adapter aux spécificités des SI les plus complexes, tout en restant aligné sur les standards de cybersécurité et de conformité actuels.

Cartographit a été sélectionnée comme solution innovante par le dispositif France 2030, nous sommes donc soutenus par BPI France, la Région Occitanie et France 2030.

Si vous souhaitez entreprendre une démarche de sécurisation et de cartographie de votre SI, vous pouvez demander une démonstration de l'outil Cartographit.

> Par Sabine Terrey

HOGO.eu

STATIONS BLANCHES USB

SCAN USB

DECONTAMINATION

SECURE FILE SHARING

PROTECT BEFORE CONNECT

hello@hogo.eu

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