La fin de l'année 2023 augure des tendances 2024, découvrez l'analyse complète des experts ESET en page 22

N°33 I MARS 2024

CONDUIRE LA TRANSFORMATION NUMÉRIQUE DE L'ENTREPRISE

SMART DSI®

DOSSIER
La complexité des Systèmes d'Information

INTERVIEW
Un DSI de transition prêt à affronter toutes les situations critiques

L'ETUDE A RETENIR
Priorités des investissements des entreprises en 2024

L'ŒIL SECURITE
Lockbit semble décapité mais le hacker de demain est l'IA

STRATEGIE
Identité numérique : partager ses données de manière sélective et sécurisée

L'ŒIL DU NUMERIQUE
DORA : DSI, coopérez avec la Direction des Risques

Digital Security
Progress. Protected.

Ne rien faire coûte plus cher que de protéger votre entreprise

Optez pour les services de Managed Detection & Response (MDR) ESET

RENFORCER LE NIVEAU DE SÉCURITÉ

Accélérez vos capacités de détection des menaces, d'investigation et de réponse grâce à l'expertise d'ESET.

PERSPECTIVES INTERSECTORIELLES

Accédez à une bibliothèque prédéfinie et personnalisable de modèles de comportement de détection qui vous aide à élaborer un nouvel ensemble de règles de comportement.

EXPERTS EN THREAT HUNTING

Votre entreprise est protégée 24 heures sur 24 et 7 jours sur 7 par des experts humains.

Arrêter les menaces c'est bien. Les prévenir, c'est mieux.

eset.com/fr/business/services

Intelligence Artificielle : Ethique, Leadership et Diversité

L'année 2024 est lancée avec son lot de défis pour les dirigeants ! Cybersécurité, Cloud, Intelligence Artificielle, Données, Automatisation... Des domaines étroitement liés puisque la maturité du Cloud et des plates-formes de données augmente le potentiel de l'IA qui transforme les entreprises, les économies et les sociétés.

Si son essor n'est plus à démontrer, l'IA générative bouleverse profondément le quotidien dans tous les domaines et oblige à repenser la façon de travailler et communiquer, et les stratégies. Plus de doute, la GenAI devient une réponse redoutablement efficace pour les objectifs de productivité.

Alors, entre compétitivité et risques, il est urgent d'ajuster au mieux un subtil équilibre. Dans ce cas, les choix technologiques des organisations devront prendre en compte les capacités mais aussi gérer la sécurité, l'éthique, les compétences et l'humain. En effet, pour les nombreux usages actuels et à venir de l'IA, les entreprises doivent intégrer la gestion et l'utilisation des données, à savoir la gouvernance, la conformité, la confidentialité, la souveraineté et l'éthique(1).

Enfin, il reste un point d'extrême vigilance à surveiller pour l'impact positif de l'IA. Son leadership ! Celui-ci doit refléter toute la société, et absolument embarquer les femmes dirigeantes, c'est fondamental. Mais les indicateurs(2) ne sont pas optimistes en France, les niveaux de représentation et de confiance des femmes dirigeantes sont inférieurs à ceux des autres pays de la région EMEA. Et pourtant ! Si l'IA apprend des développeurs et utilisateurs, la participation des femmes reste essentielle pour diminuer le risque de biais inconscients. Certes, des initiatives sont lancées, mais il en faut bien plus : mentorat, augmentation de la représentation au niveau de la direction et des cadres intermédiaires, investissements dans les entreprises d'IA fondées par des femmes. La diversité, l'égalité et l'inclusion sont décisives pour le succès à long terme de l'IA et le futur de l'innovation.

Impulser des démarches responsables pour un avenir technologique avancé et socialement acceptable pour tous est une priorité.

Très bonne lecture

Sabine Terrey
Directrice de la Rédaction
sterrey@itpro.fr

(1) Source 3ème édition du Tech Radar de Devoteam

(2) Source Etude IBM - Female Leadership in the age of AI

SMARTDSI

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

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

SMART DSI

N°33 I MARS 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
La complexité des systèmes d'information

12 I L'ŒIL SECURITE
Lockbit semble décapité mais le hacker de demain est... l'IA !

14 I STRATEGIE
Identité numérique : partager ses données de manière sélective et sécurisée

17 I L'ETUDE A RETENIR
Les investisseurs priorisent les critères ESG

18 I INTERVIEW
La start-up Tenacy accélère son développement au service des clients

22 I PARTNER SECURITY REPORT
La fin de l'année 2023 augure des tendances 2024

24 I EXPERT
Zone d'atterrissage Azure

30 I INTERVIEW
Open Lake Technology s'engage pour la conformité et la supervision de votre téléphonie unifiée

33 I L'ETUDE A RETENIR
Priorités des investissements des entreprises en 2024

34 I L'ŒIL DU NUMERIQUE
Règlement DORA : DSI, coopérez avec la Direction des Risques

38 I PERSPECTIVES
AI Act : Quel encadrement des systèmes d'IA par l'UE ?

41 I L'ETUDE A RETENIR
Changements sociétaux : 5 tendances à surveiller par les entreprises

42 I INTERVIEW
Consol Connect : une seule plateforme automatisée pour gérer sa connectivité avec souplesse et rapidité


P.34


P.24


P.38

45 I L'ETUDE A RETENIR
Paysage des cybermenaces mondiales

46 I L'ŒIL DU FUTUR
Inclusion et IA générative au cœur des décisions des dirigeants et des tendances RH

50 I STRATEGIE
L'Open Source Intelligence : un outil nécessaire de cyberdéfense

52 I EXPERT
Nouveautés dans la gestion des identités externes

53 I BULLETIN D'ABONNEMENT

56 I INTERVIEW
Infortive prône un DSI de transition prêt à affronter toutes les situations critiques

SMARTDSI

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

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

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

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

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

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

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

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

Site officiel : www.smart-dsi.fr

La complexité
DES SYSTÈMES D'INFORMATION

> Par Didier Danse

Le système d'information comprend tellement de composants qu'il est naturel de rencontrer des difficultés au quotidien. Le dynamisme des interactions entre les composants technologiques, les processus métier et les utilisateurs peut mener à des défis multiples, que ce soit la maintenance, la sécurité des données, la gestion des risques et bien d'autres. Toutes ces difficultés peuvent mener à des systèmes non pertinents ou non fonctionnels.

Même si aucun système n'est parfait, et à priori aucun ne le sera jamais, comprendre ce qu'est un système d'information dans son ensemble est déjà une (r)évolution en soi. Le facteur le plus compliqué à gérer est sans nul doute la présence de l'humain dans les rouages du système. C'est pourtant ce même humain qui pourra permettre de faire évoluer le système et créer de la valeur, agissant à la fois en tant qu'utilisateur final, concepteur, développeur, gestionnaire et décideur.

Tout d'abord quand on parle de système, il est important de définir quelques concepts, notamment ce qu'est un système informatique et un système d'information. Comprendre la différence entre les deux s'avère déjà un avantage certain dans l'implémentation, la maintenance et l'amélioration de ceux-ci. Pour faire simple, un système informatique se concentre principalement sur l'aspect technique de l'informatique. En effet, un système informatique fait référence à l'ensemble des composants matériels et logiciels qui interagissent pour traiter, stocker et transmettre des données dans un environnement informatique.

Un système d'information, d'autre part, est un concept plus large qui inclut non seulement les composants techniques, mais aussi les processus, les personnes et les données qui travaillent ensemble pour collecter, traiter, stocker et distribuer des informations dans une organisation ou un environnement particulier. Ceci repose notamment sur les politiques organisationnelles, les structures hiérarchiques et les objectifs stratégiques d'une organisation.

Les composants d'un système d'information

Les systèmes d'information représentent l'épine dorsale de notre société moderne pour traiter, stocker et transmettre des informations de manière efficace et fiable. Ces systèmes sont omniprésents, touchant presque tous les aspects de notre vie quotidienne, de la communication à la gestion des données, en passant par le divertissement, la recherche et bien plus encore. Il existe de nombreuses composants dont les principaux sont listés ci-dessous :

- Le **matériel** informatique constitue la composante physique des systèmes, comprenant les ordinateurs, les serveurs, les périphériques de stockage (disques durs, SSD), les périphériques d'entrée (claviers, souris, scanners), les périphériques de sortie (moniteurs, imprimantes, haut-parleurs), ainsi que les réseaux de communication (routeurs, commutateurs, câbles).
- Le **logiciel** englobe les programmes informatiques, les systèmes d'exploitation, les applications et les outils qui permettent aux utilisateurs d'accomplir différentes tâches sur les ordinateurs et les périphériques. Les systèmes d'exploitation (Windows, macOS, Linux) fournissent une interface entre le matériel et les logiciels applicatifs, tandis que les applications logicielles (bureautique, navigateurs web, jeux) offrent des fonctionnalités spécifiques aux utilisateurs.

Les systèmes d'information représentent l'épine dorsale de notre société moderne pour traiter, stocker et transmettre des informations.

- Les **données** représentent l'information brute traitée et stockée par les systèmes informatiques. Elles peuvent prendre diverses formes, y compris du texte, des images, des vidéos, des fichiers audio, des bases de données et bien plus encore. La gestion efficace des données est essentielle pour assurer l'intégrité, la sécurité et la disponibilité des informations.

- Les **utilisateurs** sont les personnes qui interagissent avec les systèmes informatiques, qu'il s'agisse d'utilisateurs finaux, de programmeurs, d'administrateurs systèmes, de concepteurs d'interfaces utilisateurs ou d'autres parties prenantes. La conception centrée sur l'utilisateur vise à optimiser l'expérience utilisateur et à rendre les systèmes plus conviviaux et accessibles.
- Les **processus** décrivent les méthodes et les règles utilisées pour collecter, stocker, traiter, et distribuer les données dans le système d'information. Cela inclut les workflows, les procédures opérationnelles, les politiques de sécurité, et les stratégies de gestion des données.
- Les **réseaux** permettent la connexion et la communication entre les différents composants du système d'information. Cela inclut les réseaux locaux (LAN), les réseaux étendus (WAN), les connexions sans fil, et les technologies de communication comme Internet et les intranets.

Alors que la liste est assez limitée, nous pouvons d'ores et déjà voir qu'un système peut être composé de dizaines de composants, voire plus.

Les interactions au sein des systèmes informatiques

Revenons aux systèmes informatiques. Les interactions en son sein suivent un processus généralisé, comprenant plusieurs étapes interdépendantes qui peuvent se résumer de la manière suivante.

- ***Entrée***

Les données et les instructions sont introduites dans le système informatique via des périphériques d'entrée tels que les claviers, les souris, les scanners, les microphones, les caméras, les capteurs et autres dispositifs d'acquisition.

- ***Traitement***

Le processeur (CPU) et d'autres composants matériels exécutent des instructions pour traiter les données entrantes en fonction du logiciel et des algorithmes appropriés. Ce processus implique la manipulation, la transformation et l'analyse des données pour produire des résultats significatifs.

- ***Stockage***

Les données sont stockées dans la mémoire vive (RAM) pour un accès rapide et temporaire, ainsi que dans des périphériques de stockage à plus long terme tels que les disques durs, les SSD, les cartes mémoire et les serveurs. La gestion du stockage vise à optimiser l'utilisation des ressources tout en assurant la disponibilité et la redondance des données.

- ***Sortie***

Les résultats du traitement sont renvoyés à l'utilisateur via des périphériques de sortie tels que les moniteurs, les imprimantes, les haut-parleurs, les écrans tactiles et les dispositifs haptiques. L'interface utilisateur joue un rôle crucial dans la présentation des informations de manière claire, intuitive et attrayante.

- ***Communication***

Les systèmes informatiques peuvent communiquer entre eux via des réseaux de communication, permettant le partage de données, la collaboration en temps réel, l'accès à des ressources distantes et la synchronisation des informations. Les protocoles de communication, tels que TCP/IP, HTTP, FTP, SMTP, facilitent l'échange d'informations dans des environnements réseau.

Les systèmes informatiques sont la partie émergée et la plus simple à gérer au quotidien, jusqu'à pouvoir rendre ces systèmes totalement autonomes, ce qui est un avantage certain quand on souhaite gérer un système d'information dans son ensemble. Il sera alors possible de s'occuper exclusivement des aspects qui se basent purement sur l'humain et ses constructions, que ce soient les règlements ou les structures hiérarchiques.

La gestion efficace des données est essentielle pour assurer l'intégrité, la sécurité et la disponibilité des informations.

Quelques exemples de systèmes informatiques

Dans les organisations, les systèmes informatiques sont omniprésents, que l'on s'en rende compte ou non. C'est d'ailleurs pour cela qu'ils sont présentés dans ce paragraphe. Les systèmes informatiques peuvent être classés en plusieurs catégories en fonction de leur portée, de leur fonctionnalité et de leur domaine d'application:

- **Les systèmes d'exploitation** (Windows, macOS, Linux, Android, iOS) fournissent une interface entre le matériel et les logiciels applicatifs, facilitant la gestion des ressources système, la gestion des fichiers, la sécurité et la prise en charge du matériel.
- ***Les réseaux informatiques*** permettent la communication et le partage de ressources entre plusieurs ordinateurs et périphériques. Les topologies de réseau (étoile, anneau, maillé) et les technologies de communication (Ethernet, Wi-Fi, Bluetooth) jouent un rôle clé dans la conception et la mise en œuvre des réseaux.
- ***Les Systèmes de Gestion de Base de Données*** (SGBD, tels que MySQL, PostgreSQL, Oracle, ou

encore Microsoft SQL Server) stockent, organisent et permettent l'accès aux données de manière efficace et sécurisée. Les langages de requête (SQL) permettent d'interroger, de manipuler et de gérer les bases de données relationnelles.

- ***Les systèmes embarqués*** sont intégrés dans des dispositifs spécifiques pour effectuer des tâches dédiées telles que le contrôle industriel, l'automobile, les appareils électroniques grand public, les dispositifs médicaux et les systèmes embarqués.
- ***Les systèmes de gestion*** capturent, traitent et distribuent des informations pour soutenir les opérations et la prise de décision au sein des organisations. Ils comprennent les systèmes ERP (Enterprise Resource Planning), les systèmes CRM (Customer Relationship Management) et les systèmes de BI (Business Intelligence).

Nous l'avons vu et répété, tous ces systèmes informatiques ne font pas directement partie d'un système d'information mais y contribue, que ce soit en fournissant les fondements à ces derniers ou étant un composant à part entière de ce même système d'information.

Un système bien connu comme exemple : la voiture

La place de la voiture dans le présent et dans notre futur est très certainement l'exemple le plus concret et le plus connu d'un système, bien que peu de gens seront en mesure d'identifier plus de six ou sept des composants alors que le système repose certainement sur plusieurs dizaines de composants. Ce sujet est discuté très régulièrement, au bureau ou à la maison. Les avis divergent et même s'opposent. Il est fort probable qu'il y a une partie de vrai dans chacun d'eux. Sans chercher à faire un procès à ces idées, voyons plutôt la complexité du système dans son ensemble.

Les technologies sont là. Certes il y a encore des améliorations à apporter mais la voiture est aujourd'hui capable de conduire seule et offre de nombreuses opportunités. Associée à la capacité d'interconnecter les véhicules tant entre eux et avec des centres de données, la technologie permet dès lors d'envisager de prévoir les déplacements et de désengorger les villes. Les voitures pourraient aller se garer seules voire se recharger, ou même faire le plein grâce aux robots pompistes qui sont actifs notamment en Asie. Donc au lieu de tourner plusieurs minutes avec vous en conducteur, consommer du carburant ou de l'énergie, la voiture vous dépose au plus proche de votre lieu de destination et optimise son trajet pour réduire le temps sur la route. Cette même voiture pourrait même, à l'inverse, augmenter son temps sur la route afin de ne pas surcharger l'une ou l'autre route si cela s'avérait positif pour l'ensemble des utilisateurs.

Technologiquement, il suffit d'un effort relativement minime pour atteindre un niveau de maturité encore plus élevé. Pourtant, le sujet n'évolue que très peu, malgré l'accélération de l'adoption du véhicule électrique, notamment par notre attachement à la voiture. De nombreux défis sont directement visibles, notamment:

- L'infrastructure n'est pas en mesure de supporter toutes ces nouvelles utilisations: que ce soient les systèmes de recharge ou encore le réseau de transmission des données, ils ne sont pas encore entièrement prêts et la volonté d'y parvenir est très souvent limitée aux sociétés commerciales. Il sera donc nécessaire de faire en sorte que l'ensemble fonctionne avec un objectif commun y compris lorsque la concurrence est présente.
- Les modèles de fourniture des biens ne sont pas adaptés au partage : la fourniture des véhicules actuels est basée sur la vente, y compris pour les leasers, bien que le système de location tende à apparaitre chez les constructeurs. Pour un futur efficace, il s'agira très certainement de proposer des systèmes d'abonnements ou de paiement à l'utilisation.
- La coexistence avec des technologies d'une génération précédente : l'incapacité de faire interagir des technologies différentes peut empêcher une implémentation efficace voire des dangers puisqu'un véhicule qui ne récupèrera pas l'information des voitures sans les technologies modernes pourrait prendre une décision incohérente. Le risque devra donc être géré au mieux, jusque dans le véhicule lui-même.
- Les règlementations et politiques inadaptées : dans ce cas, celles qui imposent de physiquement avoir les mains sur le volant et ce en permanence, pour ne citer que ces points. La taxation des véhicules, des carburants et de l'énergie et la fiscalité en entreprise font qu'il est parfois peu intéressant d'adopter des systèmes particuliers.

- Les aspects juridiques: qui est responsable en cas d'accident avec une voiture autonome ?
- Les aspects éthiques: quand la voiture est face à 2 personnes et que l'accident est inévitable, laquelle de ces personnes doit être sauvée, pour ne pas dire que l'autre se verra sacrifiée ?
- Les aspects financiers: est-on prêt à payer pour la recherche de nouvelles technologies ? Comment paie-t-on le prix le plus juste ? Comment les organisations impliquées peuvent continuer à exister dans ce contexte ?
- Et surtout, la culture: êtes-vous réellement prêts à envisager à ne plus avoir votre voiture mais plutôt d'utiliser une voiture partagée ? Comment garde-t-on la personnalisation des voitures qui nous importe tant ?

Alors qu'il s'agit d'un enjeu national voire mondial, cet exemple est très représentatif de ce qu'il se passe dans une organisation de plus petite taille, généralement l'entreprise. Un système doit, en effet, tenir compte de l'ensemble des facteurs, pas uniquement de la technologie. Si le système ne respecte pas les facteurs externes, il est voué à l'extinction. Et si même il coche toutes les cases, il reste un élément important: **l'humain dans le système**. L'adoption est critique.

Dans l'organisation, cette adoption peut s'avérer très compliquée. L'intelligence artificielle, par exemple, fait peur à bien des gens, même les proches des technologies.

Comment mettre en place un système d'information efficient ?

Le système informatique, tout autant que tout autre système, se doit dès lors d'être pensé dans son ensemble, en tenant compte de chaque facteur et principalement le facteur humain. En effet, nous l'avons vu, l'humain est partout. Même si la perception est que le tout est automatisé, seuls les systèmes informatiques peuvent vraiment l'être. Les systèmes d'information quant à eux continuent à exister grâce aux personnes, avec leur culture au sein de l'organisation, mais aussi toutes les composantes qui font du système ce qu'il est, notamment les règlements.

Ainsi, comprendre les besoins réels, pas uniquement ceux qui sont émis par les utilisateurs des systèmes informatiques potentiels, est une tâche ardue. Il s'agira très certainement de faire appel à des persona, c'est à dire des profils types de personnes. Ces profils seront généralement définis sur base d'interviews ou même de simples analyses des retours, qu'il faudra faire valider tôt ou tard. Pour cela, on pourra utiliser des techniques issues du design *thinking* notamment.

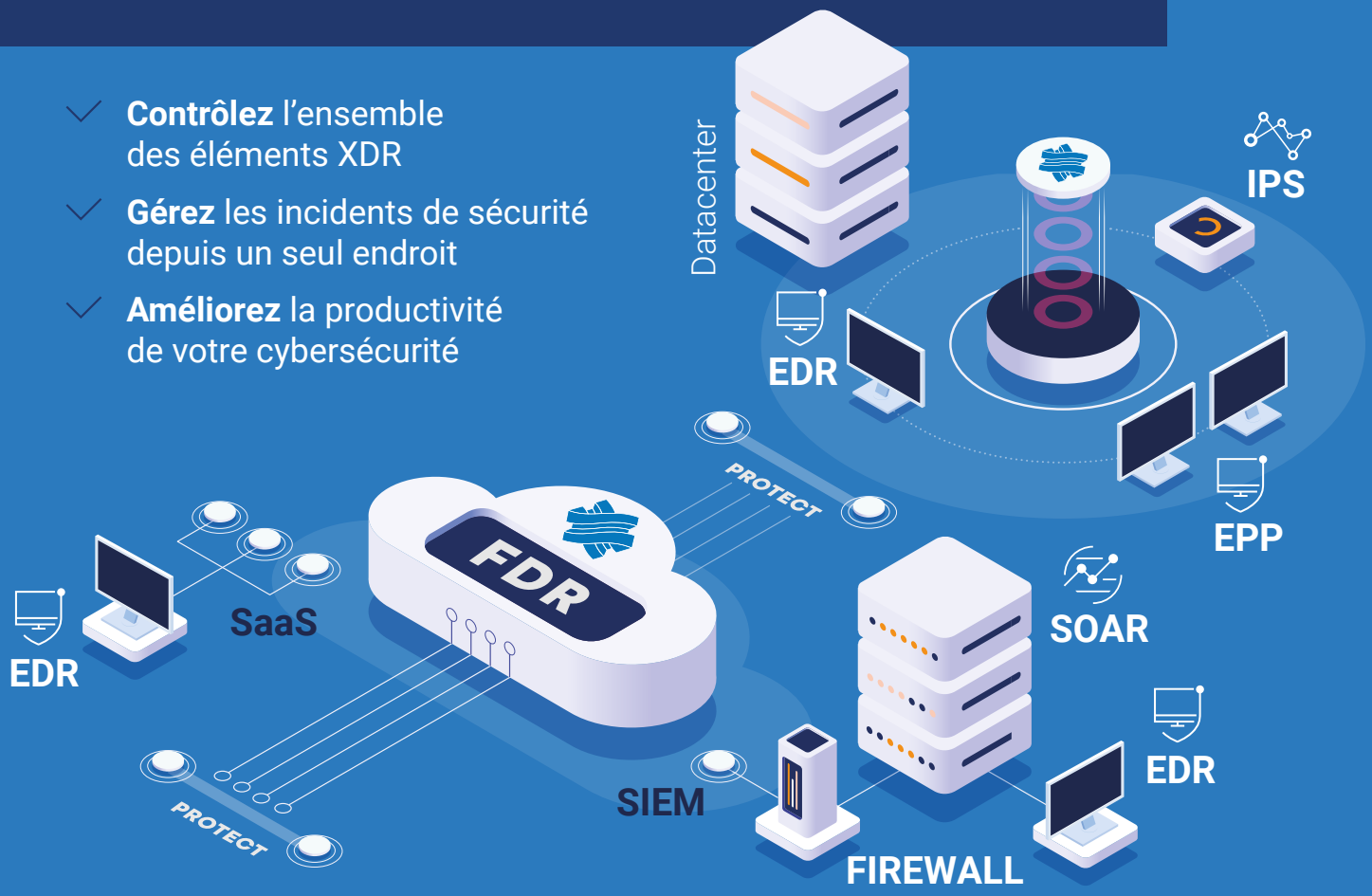
Dans tous les cas, la difficulté restera de gérer la relation avec des parties externes, sur lesquelles vous n'avez que peu de contrôle et de faire adopter le système dans son ensemble à un maximum de personnes, sachant qu'ils font eux-mêmes partie de ce système.

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

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 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.

STORMSHIELD

LOCKBIT SEMBLE DÉCAPITÉ MAIS LE HACKER DE DEMAIN EST... l'IA !

Bonne nouvelle sur le front de la cybersécurité : Lockbit, le groupe de hackers considéré comme "le plus nuisible au monde", a été la cible, lundi 19 février, lors de l'opération Cronos d'une action cyber policière coordonnée dans dix pays, notamment par la Gendarmerie Nationale, le FBI et Europol.

L'opération Cronos a porté un coup très dur à ce réseau de hackers, qui a émergé en 2019 et qui a donné son nom à Lockbit 3, son ransomware, l'un de ces logiciels qui pénètrent un réseau informatique grâce à une faille technique, humaine, mais souvent les deux, et le paralysent, dans l'attente du paiement d'une rançon. Rançon souvent payée inutilement, car la récupération des environnements chiffrés se fait difficilement, et souvent des données sont volées et revendues sur le darkweb.

En cinq ans, on parle d'au moins 100 millions d'euros extorqués, et de plusieurs milliards de dollars de dégâts causés, plus de 200 entreprises et administrations attaquées, comme les hôpitaux de Corbeil-Essonnes et de Versailles, la Poste Mobile, Voyageurs du Monde ou les cosmétiques Nuxe.

L'argent, la motivation principale

L'argent est la motivation principale des hackers Lockbit, même si la structure a aussi été décrédibilisée. Les autorités ont même pris le contrôle du propre site de Lockbit, pour afficher les visages des hackers, les mandats d'arrêt, les comptes de cryptomonnaies saisis, et les antidotes informatiques, un site destiné aux clients de Lockbit, qui utilisaient le logiciel pour leurs propres méfaits, contre une commission reversée à l'organisation, estimée à 20%.

Enfin, selon l'éditeur de solutions cybersécurité Trend Micro, le groupe de pirates informatiques travaillait sur le développement d'une nouvelle variante. Un Lockbit 4.0 serait en cours de développement par les hackers russophones.

L'infrastructure technique est – certes – entre les mains des forces de l'ordre mais, a priori, la tête pensante de l'organisation qui se fait appeler LockbitSupp, court toujours, tout comme plusieurs ressortissants russes qui ne risquent probablement rien en Russie.

L'IA générative...

Ce sont de beaux succès mais à moyen terme, il faudra se préparer : les pirates vont utiliser de plus en plus l'IA générative. Au revoir le phishing avec des fautes grossières, bienvenue aux messages hautement personnalisés, riches en contenus, en contenus adaptés...

Cette utilisation commencera par toucher la planification et l'orchestration des attaques. Aujourd'hui, encore, la préparation d'une attaque contre une entreprise peut prendre des semaines, impliquer des compétences différentes. Avec des IA connectées au Web, les pirates accèdent en temps réel et en masse de données aux informations d'entreprises ciblées, aux vulnérabilités, aux *threats* identifiés, etc. La planification est presque instantanée et adaptable facilement.

La révolution des cyber attaques *AI-driven !*

Pour comprendre ou imaginer la révolution AI appliquée à la cybersécurité, il faut juste se remémorer les années 2000. Au milieu des années 2000, le premier iPhone 2G sortait. A cette époque, toutes les data étaient stockées dans les datacenters de l'entreprise et 90% de la protection était on-*premise*. Le Cloud a changé tout cela pour le bien ou pour le pire. Le Cloud a permis la collecte, le stockage et la valorisation des quantités énormes de données et l'émergence des nombreuses entreprises exploitant, valorisant ces données dans tous les domaines de la vie. Mais les cybercriminels veulent, aussi, cette mine d'or et, finalement, la quasi-totalité des attaques portent sur l'accès et le vol des données. Avec l'émergence exponentielle de l'usage par les entreprises de multiples apps et technologies, la surface d'attaque a cru exponentiellement.

Il faudra se préparer : les pirates vont utiliser de plus en plus l'IA générative.

La sécurité des environnements Cloud est, actuellement, de mieux en mieux prise en compte par les entreprises, mais nous sommes toutefois loin de la cible.

Et voilà qu'à la révolution du Cloud de ces quinze dernières années, nous entrons d'un coup, dans la révolution des cyber attaques *AI-driven* !

Allons-nous, par exemple, vers l'*IA Gen-as-a-service* appliquée au hacking après l'ère du *ransomware-as-a-service* qui elle se ''limitait'' à fournir sur abonnement des outils logiciels malveillants aux hackers?

L'avenir proche nous le dira. En attendant, préparons-nous !

> Théodore-Michel VRANGOS, Cofondateur et Président d'I-TRACING

Identité numérique : PARTAGER SES DONNÉES DE MANIÈRE SÉLECTIVE ET SÉCURISÉE

Nom, date de naissance, adresse, email, numéro de mobile, diplômes, documents fiscaux ou fiche de paie – autant de documents ou données personnelles que les particuliers doivent fournir pour accéder à des services numériques plus ou moins complexes. Et par conséquent, autant de données personnelles stockées et centralisées par les entreprises dans d'énormes bases de données. Stéphane Mavel, en charge de la stratégie Identité Numérique d'IDnow revient sur le sujet.

Bien que les entreprises soient de plus en plus sensibilisées et tentent de sécuriser leurs systèmes d'information, la centralisation des données personnelles augmente le risque de cyberattaques, comme nous le rappelle régulièrement l'actualité, en relatant des exemples de vols de données personnelles, parfois par millions. Une seule attaque, ou piratage ciblé, met en danger toutes les

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

données contenues dans un système centralisé. Par ailleurs, et malgré le cadre imposé par le Règlement Général de la Protection des Données (RGPD) et autres réglementations, le stockage de données personnelles centralisé accroît le risque de leur utilisation à des fins commerciales sans avoir effectué au préalable le consentement de l'utilisateur.

Identité numérique : le moyen de ne fournir que les données nécessaires au service

Pour reprendre le contrôle de la diffusion de ses données personnelles, il est possible d'utiliser la divulgation sélective. Grâce à ce système, l'utilisateur ne partage qu'une partie de ses données, celles strictement nécessaires au service demandé. Ainsi, pour accéder à un site de paris sportifs en ligne (interdit aux mineurs), l'utilisateur n'aura plus besoin de fournir sa pièce d'identité complète, ni même sa date de naissance exacte pour prouver qu'il a plus de 18 ans. Il pourra partager la donnée 'majorité' de son identité numérique, car cette information aura déjà été vérifiée par ailleurs.

Encore plus loin vers une identité auto-souveraine grâce aux portefeuilles d'identité numérique

L'identité auto-souveraine (*Self Sovereign Identity, SSI*) permet de donner à l'utilisateur le contrôle de ses propres données, sans qu'elles puissent être manipulées, dupliquées ou volées. Le portefeuille d'identité numérique (*Digital Identity Wallet*), souhaité par l'Union européenne, constituera un élément central de ce futur paradigme. Il permettra à chaque citoyen de contrôler sa propre identité numérique, et de maitriser la manière dont celle-ci est utilisée.

L'identité auto-souveraine permet de donner à l'utilisateur le contrôle de ses propres données.

Cette divulgation sélective sera donc intégrée à la technologie du portefeuille d'identité numérique avec le concept de « preuve de zéro connaissance » (*Zero-Knowledge-Proof, ZKP*). Ce protocole de sécurité cryptographique permettra de prouver l'authenticité d'un attribut concernant une personne (la majorité par exemple). La vérification de l'authenticité pourra être effectuée sans avoir à révéler la valeur réelle des données, comme la date de naissance. Si un vol de données dans l'entreprise a lieu, celle-ci ne les ayant jamais eues en sa possession, aucune donnée personnelle ne pourra être usurpée.

STÉPHANE MAVEL

Le protocole ZKP compte parmi les plus sûrs au monde en matière de protection de la vie privée des utilisateurs de services en ligne. En y ayant recours, l'utilisation des données d'identité personnelles peut être considérablement limitée. Et le modèle va bien au-delà du principe de minimisation des données qui, jusqu'à présent, a souvent été difficile à respecter dans la pratique.

Souveraineté des données grâce au stockage décentralisé

Aujourd'hui stockées dans d'immenses bases de données privées et publiques, les données personnelles de chaque citoyen seront décentralisées demain avec le wallet. Chaque citoyen européen pourra les gérer individuellement depuis son propre smartphone et deviendra ainsi souverain de ses données afin de les transmettre en toute connaissance de cause, sans craindre qu'elles ne tombent entre de mauvaises mains. Il reprendra ainsi le contrôle de sa vie numérique, de ses données personnelles et de leur diffusion.

Même si l'utilisation du portefeuille d'identité numérique ne sera pas obligatoire, l'UE espère que tous les citoyens se laisseront convaincre par cet outil simple et facile à utiliser. Le concept de preuve de zéro connaissance jouera un rôle central.

Les investisseurs priorisent les critères ESG

La dimension ESG (Environnementale, Sociale et de Gouvernance) a un véritable impact sur la dynamique des transactions. Explications en 3 points clés.

Avant, l'intégration de l'ESG dans le métier d'investisseur était motivée par la gestion des risques. Aujourd'hui, la gestion des critères ESG contribue à la protection et la création de valeur pour les entreprises et actifs en portefeuille.

N° 1 - L'ESG : un catalyseur de valeur pour les fonds d'investissement

La création de valeur liée aux critères ESG est le moteur des activités ESG des fonds d'investissement selon deux tiers. Selon un tiers, plus de la moitié des transactions intègre l'ESG comme principal moteur d'investissement.

L'un des principaux avantages est d'améliorer la réputation de la marque. En France, cette tendance est encore plus marquée, avec une mise en avant significative des enjeux d'attraction et de fidélisation des clients.

Divergence de la perception des avantages ESG

Selon 78%, la prise en compte de la performance ESG d'un investissement potentiel est en phase avec la recherche de rendement de l'entreprise ou fonds d'investissement.

Mais on note des divergences de perception des avantages de l'ESG selon le montant des actifs sous gestion : ce chiffre monte à 90% pour les répondants disposant de plus de 10,1 milliards de dollars d'actifs sous gestion et descend à 67% pour ceux disposant de 200 millions de dollars ou moins.

N° 2 - Les facteurs importants de l'ESG pour les fonds de capital-investissement

Des mesures ciblant les problèmes de gouvernance sont prises ainsi que des dispositions pour prévenir la corruption.

Quels sont les sujets environnementaux, sociaux et de gouvernance identifiés comme importants ? Les émissions de gaz à effet de serre, les sujets environnementaux et la biodiversité.

Côté social, la prise en compte des droits de l'homme et les relations de travail, les talents de l'entreprise et l'attractivité, suivis par le monde du travail de demain, l'automatisation.

Concernant la gouvernance, l'éthique, les valeurs et la culture d'entreprise sont des éléments différenciants, seulement 27% prennent en compte la transparence fiscale et les reportings.

France : les préoccupations ESG du capital-investissement

Les préoccupations du capital-investissement s'orientent vers les données, les technologies émergentes et la cybersécurité. Les défis nécessitent une compréhension technologique approfondie et des protocoles de sécurité complexes.

L'inquiétude à l'égard de la biodiversité est plus élevée que la moyenne mondiale - 56% contre 39%. Cette variation peut être attribuée au cadre réglementaire strict (Loi Énergie Climat et la réglementation CSRD - Corporate Sustainability Reporting Directive).

Côté lutte contre les émissions de gaz à effet de serre, la France est en avance sur la tendance mondiale, 75% ont ainsi déjà mis en œuvre des stratégies à cet égard, contre 69% pour les répondants monde.

N° 3 - Les critères ESG dans les étapes du processus de transaction

Les considérations ESG sont maintenant initiées avant le début du cycle d'investissement, dès la recherche d'opportunités.

La diminution du nombre d'investisseurs renonçant à des opportunités d'investissement en raison de considérations ESG peut être attribuée à un changement d'approche.

France : approfondir l'intégration de l'ESG

L'investissement responsable prend une place importante dans le private equity. Durant la phase de pré-acquisition, 62% prennent systématiquement en compte les considérations ESG, 78% considèrent la performance ESG des investissements potentiels comme étant en phase avec la recherche de rendement au moment de la décision d'investissement. Pendant la période de détention, ils intègrent les considérations ESG dans le suivi de leurs sociétés de portefeuille.

Source Enquête PwC – Global Private Equity Responsible Investment Survey 2023 - Points de vue des dirigeants et professionnels seniors de l'investissement et du développement durable au sein des sociétés de capital-investissement. 166 répondants issus de 22 pays et territoires dans le monde, 27% basés en France- Premier semestre 2023.

La start-up Tenacy
ACCÉLÈRE SON DÉVELOPPEMENT AU SERVICE DES CLIENTS

Créée en 2019 par deux entrepreneurs du secteur, Cyril Guillet et Julien Coulet, Tenacy, plateforme SaaS de pilotage de la cybersécurité et de la conformité, a une actualité riche en ce début d'année 2024 ! Levée de fonds de six millions d'euros, développement sur le territoire français, extension sur le marché européen, en commençant par le Benelux et l'Espagne. Echange avec Cyril Guillet, PDG et co-fondateur de Tenacy.

En 2023, selon 53%[1] des organisations, il est difficile de respecter les exigences cyber et 88 % ont des problèmes liés à la pénurie de talents en cybersécurité. Les difficultés de recrutement et la recrudescence des cyberattaques entrainent notamment l'épuisement professionnel.

Notre innovation réside dans notre interconnexion et notre modèle de données.

Parlons de Tenacy.
Un mot sur sa création et sa mission ?

Tenacy a pour mission de pérenniser les organisations grâce à un usage plus efficace des ressources de cybersécurité. Grâce à notre plateforme SaaS tout-en-un à destination des RSSI, nous consolidons et simplifions le pilotage de la cybersécurité et de la conformité pour les transformer en accélérateurs du business.

HOGO.eu

STATIONS BLANCHES USB

Retrouvez nous au Forum InCyber STAND H21

SCAN USB

DECONTAMINATION

SECURE FILE SHARING

PROTECT BEFORE CONNECT

in hello@hogo.eu

CYRIL GUILLET ET JULIEN COULET

Leader en France, nous comptons plus de 150 clients, 3 000 utilisateurs et 50 collaborateurs. Fondée en 2019 et basée à Lyon, Tenacy a levé 6 millions d'euros en série A en décembre 2023.

Mais alors, qu'est-ce qui vous différencie ?

Notre innovation réside dans notre interconnexion et notre modèle de données. Manager sa cyber dans Excel, c'est prendre le risque de données dédoublées, altérées, indexées différemment.

Grâce à 30+ connecteurs, Tenacy se branche à l'ensemble de l'écosystème IT et cyber des clients. Cela permet de centraliser les KPIs de sécurité, consolider les anomalies et renforcer la collaboration des équipes.

Avec notre modèle de données, nous lions également l'ensemble des processus de pilotage de la cyber entre eux.

Si on devait retenir les points clés de votre plateforme ?

Tenacy s'adapte aux spécificités des organisations, de l'ETI aux grands comptes. Nos clients peuvent modéliser leur organisation et gérer ainsi la granularité de leurs objectifs de sécurité. Ces capacités de modélisation sont une de nos grandes forces.

Tenacy est un allié de poids face au défi de la multi-conformité. Nous avons construit un catalogue de 40+ référentiels français et européens, avec leurs mesures de sécurité, indicateurs, tâches de contrôle et risques associés. Cela assure une gestion cyber efficace et cohérente.

Enfin, la centralisation des données est un élément crucial pour simplifier le pilotage cyber. Nous avons déjà développé 30+ connecteurs, pour collecter automatiquement les données des écosystèmes IT / SSI. L'avantage pour nos clients est double : gagner du temps dans la consolidation du reporting et faciliter la prise de décision des équipes cyber.

Dans le cadre de France 2030, votre entreprise participe au projet "Attack Path Monitoring" mené par Hackuity. Qu'est-ce que cela signifie concrètement ?

Le projet "Attack Path Monitoring" représente une innovation importante : nous changeons le paradigme de gestion des vulnérabilités, en nous concentrant sur leurs chemins de propagation. À partir d'un point d'entrée, nous pourrons identifier le point d'attaque suivant le plus probable. Ce projet permet donc de prioriser la gestion des vulnérabilités et d'identifier les nœuds critiques dans les systèmes d'information.

Tenacy joue un rôle crucial, car les scores de sécurité que nous produisons pour nos clients vont permettre de pondérer les chemins d'attaque. Les organisations utilisant à la fois Hackuity et Tenacy pourront ainsi passer d'une stratégie de gestion des vulnérabilités basée sur le point de vue des défenseurs, à une stratégie basée sur le point de vue des adversaires, avec la surveillance des chemins d'attaque.

Outre la levée de fonds en ce début d'année, que dire pour 2024 ?

Cette levée de fonds ouvre une nouvelle phase de croissance pour Tenacy, réaffirme la pertinence de notre solution "All your cyber in one place" et de notre business model. Elle va permettre d'exécuter notre mission qui est de pérenniser les organisations grâce à un usage plus efficace des ressources en cybersécurité.

L'avantage pour nos clients est double : gagner du temps dans la consolidation du reporting et faciliter la prise de décision des équipes cyber.

En 2024, nous nous étendons à l'international, en commençant par l'Europe francophone (Belgique, Suisse, Luxembourg) et l'Espagne.

2024 marquera aussi l'entrée en vigueur de NIS 2, que nous percevons comme une opportunité pour accélérer notre développement commercial et confirmer notre position de leader.

1 - Etat de la cybersécurité en 2023 – Splunk

> Par Sabine Terrey

Au-delà de l'hypothèse

Comprendre les véritables possibilités de l'IA générative

92%

des dirigeants d'entreprise estiment que l'IA générative peut améliorer de nombreux emplois.

72%

des dirigeants d'entreprise européens ont déclaré que leur entreprise avait déjà établi, ou est en train de développer, des politiques internes pour l'IA générative.

Top 3 des préoccupations concernant la mise en place de l'IA générative

Sécurité et fiabilité

Europe 49%

- Royaume-Uni **52%**
- Pays-Bas **51%**
- Allemagne **46%**
- France **48%**

Qualité et contrôle

Europe 43%

- Royaume-Uni **45%**
- Pays-Bas **47%**
- Allemagne **46%**
- France **32%**

Conformité légale et réglementaire

Europe 37%

- Royaume-Uni **34%**
- Pays-Bas **45%**
- Allemagne **41%**
- France **30%**

Comprendre l'IA générative

Nous avons interrogé des centaines de dirigeants sur leurs projets et leurs progrès en matière d'adoption de l'IA générative. Consultez les résultats complets de l'enquête et découvrez comment des organisations comme la vôtre intègrent l'IA générative dans leur activité.

Insight

LA FIN DE L'ANNÉE 2023 AUGURE DES TENDANCES 2024

Fort de plus d'un milliard d'internautes protégés à travers le monde, ESET édite semestriellement un rapport d'observation. Ce rapport s'appuie sur les données issues de notre télémétrie d'une part et d'autre part propose les analyses de nos chercheurs sur les groupes d'attaquants APT et cybercriminels. Il concerne le paysage des menaces de juin 2023 à novembre 2023.

Voici trois sujets clefs extraits du rapport, dont vous pouvez consulter l'intégralité en scannant le QR code ci-contre ou en vous rendant sur notre blog www.welivesecurity.com.

Dans le rapport complet, vous trouverez d'autres sujets qui ne sont pas couverts ci-dessous, tels que la recrudescence d'attaques de rançongiciels menées par le groupe Cl0p, s'appuyant sur le hack « MoveIT », le déploiement de logiciels espions visant Android et pour terminer l'importance des campagnes d'infostealers (logiciels exfiltrant les login et mots de passe et toutes autres informations sensibles des machines).

Chiffres clefs de notre télémétrie

La plupart des statistiques suivantes sont issues de notre télémétrie en France, montrant une augmentation des attaques. Le phishing reste en tête, visant principalement à voler les identifiants pour Office, Outlook et d'autres services en ligne, et constitue environ un quart de toutes les menaces identifiées par ESET. Les JavaScripts nuisibles, en particulier JS/Agent, qui est passé de la cinquième à la deuxième place des menaces, représentent maintenant 10 % du total. En France, les cas de sextorsion par email continuent d'augmenter de 32 %, bien que moins rapidement qu'auparavant.

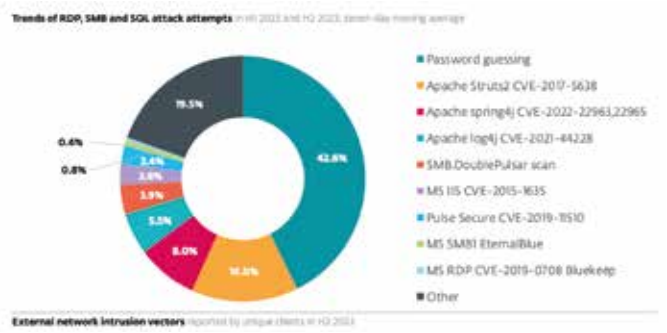
Spam, hameçonnage, tendance des attaques sur les messageries

Le volume des menaces véhiculées par les courriers électroniques ne faiblit pas, il est marqué par une légère hausse au cours de l'année.

Les scripts et les documents PDF malicieux sont majoritaires et représentent près de 75% des contenus malveillants attachés aux messages. Ils sont suivis par les documents MS Office, des éléments à surveiller de près lors du filtrage : les premières places du classement regroupent les messages malveillants qui visent à récupérer les identifiants MS Office ainsi que ceux des applications populaires. A l'exception de la seconde place tenue par des messages de sextorsion. (spécifiquement en France).

Tendances des exploitations des services RDP et SMB (France)

Durant la seconde moitié de 2023, les attaques contre les services RDP et SMB sont restées constantes, avec la France parmi les nations les plus visées. La méthode d'attaque la plus courante consiste à tenter de deviner les mots de passe, ciblant tant les services RDP que SMB. Il est vivement recommandé d'adopter une authentification multi-facteurs et de limiter le nombre de tentatives de connexion pour ces services.



La chasse aux utilisateurs ChatGPT est ouverte

Au cours du 2e semestre 2023, nous avons bloqué plus de 650 000 tentatives d'accès à des domaines malveillants dont les noms comprenaient la chaîne « chapgpt » ou un texte similaire. Si la plupart des blocages ont eu lieu en juin, les mois suivants ont vu un flux constant de nouveaux domaines malveillants prétendant offrir des services liés à ChatGPT.

En dehors de ces applications Web, presque tous les noms de domaine chatgpt malveillants étaient liés à des extensions Chrome malveillantes - détectées comme JS/Chromex.Agent.BZ.

Ce que leurs créateurs promettent aux victimes, c'est une fenêtre de recherche dans leur navigateur, qui combine la puissance de la recherche Google et de ChatGPT. Cependant, le serveur de l'attaquant peut envoyer une URL en réponse et l'extension peut l'afficher dans un nouvel onglet du navigateur. Cette fonctionnalité, non divulguée par le développeur, pourrait conduire la victime vers des pages Web malveillantes. Notons que d'autres campagnes menées sur le thème de l'IA visent à récupérer les clefs API d'utilisateurs. Ainsi les cyber criminels peuvent utiliser avec un anonymat certain et sans frais les outils leur permettant d'améliorer leurs campagnes.

Quels enseignements tirer du rapport ESET ?

Sans surprise l'humain reste au cœur des préoccupations pour renforcer la sécurité globale des SI. Les menaces véhiculées par emails sont en constante évolution, tant en quantité qu'en qualité. L'IA générative apporte une pierre de taille à l'édifice, tant par son attractivité et les escroqueries qui y sont liées, que par l'apport technique qu'elle apporte aux attaquants.

Par ailleurs et comme le montrent les statistiques des attaques sur les protocoles SMB et RDP, toutes les parties prenantes doivent être sensibilisées et accompagnées. Qu'il s'agisse de shadow IT ou de déploiement régulier, les ressources doivent faire l'objet d'un traitement sous l'angle de la cyber sécurité, pour ne pas servir de porte d'entrée au SI. L'humain est tout autant une force et une ressource rare. Pour se protéger la surveillance du SI doit être constante, ne faiblissant pas à l'aune du weekend ou des congés. C'est à partir de ce constat qu'ESET propose un service de MDR adossé à ses solutions logicielles. Nos experts épaulent les équipes IT et sécurité à la recherche des intrusions et comportements suspects en tirant parti des solutions composant notre XDR (EPP, EDR, sandbox cloud, filtrag ail et plus largement Office 365 ou Google workplace).

Venez à notre rencontre

Les équipes d'ESET présenteront leurs recherches à la conférence https://www.botconf.eu/ en avril 2024. Cet événement regroupe les chercheurs du monde entier qui luttent contre les multiples menaces. Notre dernière intervention démontrait les efforts des attaquants à pénétrer les réseaux isolés (air gap) sur plus de 15 ans.

Nous serons également présents aux événements suivants :

- IT Meetings (19, 20 et 21 mars 2024)
- Forum In Cyber (26 et 27 mars 2024)

A propos des données

Les statistiques et tendances des menaces présentées dans ce rapport sont basées sur des données de télémétrie globales d'ESET. Sauf mention contraire explicite, les données incluent les détections indépendamment de la plateforme ciblée. De plus, les données excluent les détections d'applications potentiellement indésirables, d'applications potentiellement dangereuses et de logiciels publicitaires, sauf indication contraire dans les sections spécifiques à une plateforme et dans la section sur les menaces liées aux cryptomonnaies. Ces données ont été traitées avec la sincère intention de limiter les biais et dans le but de maximiser la valeur des informations fournies. La plupart des graphiques dans ce rapport montrent des tendances de détection plutôt que de fournir des valeurs. Cela est dû au fait que les données peuvent être sujettes à de mauvaises interprétations, surtout lorsqu'elles sont comparées directement à d'autres données de télémétrie. Cependant, les valeurs absolues ou les ordres de grandeur sont fournis lorsque cela est jugé pertinent.

ZONE D'ATTERRISSAGE AZURE

La zone d'atterrissage applicative Azure, plus connue sous le nom de Landing Zone n'est pas un sujet simple. Sans être un casse-tête, bien comprendre et bien préparer cette étape est un gage de réussite.

Le sujet est à aborder dans son ensemble. Ce n'est pas tant une difficulté technique, mais plutôt une projection cohérente et rationnelle de ce qui est attendu en termes de résultats. C'est même souvent une démarche qui met (ou remet) l'entreprise devant une feuille blanche et qui lui demande de rebalayer ses environnements pour décider de la suite.

Bien se préparer...

Bien se préparer, c'est une cible pour une arrivée prochaine sur le Cloud, donc pour un nouveau client, mais c'est également une cible si l'on est déjà présent (même massivement), mais que les déploiements initiaux n'ont pas été faits dans les règles de l'art.

FORUM
IN CYBER
EUROPE

26–28 MARS 2024

LILLE GRAND PALAIS

Parés pour l'IA ?

organisé par

ceis | Forward

avec le soutien de

Région Hauts-de-France

europe.forum-incyber.com

Et encore, il faut préciser cette partie. Ce n'est pas que les ressources n'ont pas été déployées dans les règles de l'art, mais c'est plutôt parce que le Framework d'atterrissage (CAF, ou Cloud Adoption Framework) n'a pas été le choix de démarrage.

Alors oui, tout fonctionne correctement, mais on se rend tout de même compte que… il y a quelques manques ou quelques possibilités que l'on ne peut pas exploiter complètement et correctement. Il devient, au fur et à mesure des déploiements, beaucoup plus difficile de contrôler :

- Les autorisations RBAC (Role-Based Access Control) données aux équipes.
  - > Elles manquent de granularité
  - > Elles manquent d'homogénéité
  - > Il est difficile de savoir qui est vraiment responsable de quoi
- Les règles et contraintes d'entreprise par les Policy comme :
  - > Les contraintes réglementaires
  - > Le contrôle des coûts (Finops)
  - > Les bonnes pratiques d'entreprise

L'article qui va suivre s'adresse donc aux entreprises déjà sur le Cloud ou à celles qui vont y venir à court terme. La philosophie doit être la même, même si la mise en œuvre technique et l'énergie pour y arriver vont être différentes.

Partir de zéro aura forcément moins d'impact que de repenser et redéfinir l'existant.

Landing Zone

Landing Zone donc. Ou plutôt, « Architecture conceptuelle menant à la Landing Zone ». Mieux de le lire de cette manière. La zone d'atterrissage, c'est un peu la cerise sur le gâteau. L'aboutissement du concept qui va permettre à l'entreprise de déployer ses premières charges de travail. Et de le faire de manière contrôlée ou pour employer un terme plus adapté, de manière gouvernée.

La philosophie de départ est d'une grande simplicité. Découper son activité dans une arborescence, une portée, puis lui assigner des droits et des contraintes. Pour ensuite, déployer ses premières ressources (réseaux et sécurité des réseaux dans un premier temps).

Sur le papier, comme déjà dit, c'est d'une grande simplicité. Mais uniquement une fois que les étapes permettant d'arriver à la cible sont bien comprises. Quatre mots pour détailler la mise en œuvre :

- Management group
- Subscription
- Policy
- RBAC

Que je conserve en Anglais, puisqu'ils sont souvent utilisés de cette manière.

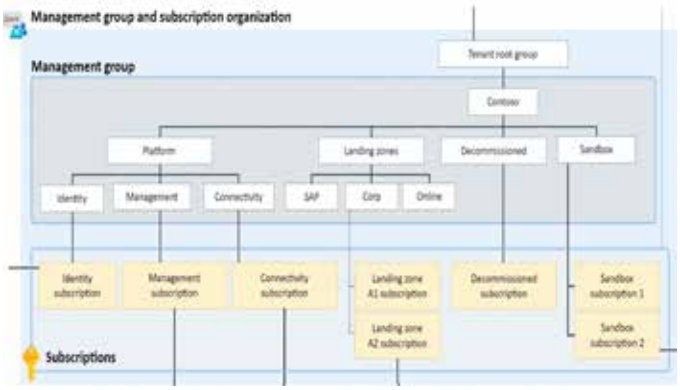
Le sujet qui suit, traite plutôt de la gouvernance de la Landing Zone, pas du positionnement des ressources qui est un sujet complémentaire et qui va également s'appuyer sur les règles du CAF.

L'arborescence

Le découpage, c'est la création d'une arborescence qui permettra de positionner les éléments de gouvernance. Il y a différents modèles pour cela, le plus courant et le plus utilisé est le modèle CAF. C'est un Framework éprouvé, il assure un démarrage dans les meilleures conditions. Et s'il parait très (trop ?) complet au départ, il n'en est rien.

Il est en revanche évolutif, n'est pas figé et va supporter les charges de travail existantes, mais également l'évolution de ces charges de travail.

Voici la partie visuelle la plus intéressante pour la préparation, image retravaillée et simplifiée de la documentation éditeur pour ne conserver que la vue sur l'arborescence.



Il y a ici deux sortes de conteneur. Les Management groups et les Subscriptions (ou abonnements). Un Management group ne peut contenir que des subscriptions ou d'autres management groups.

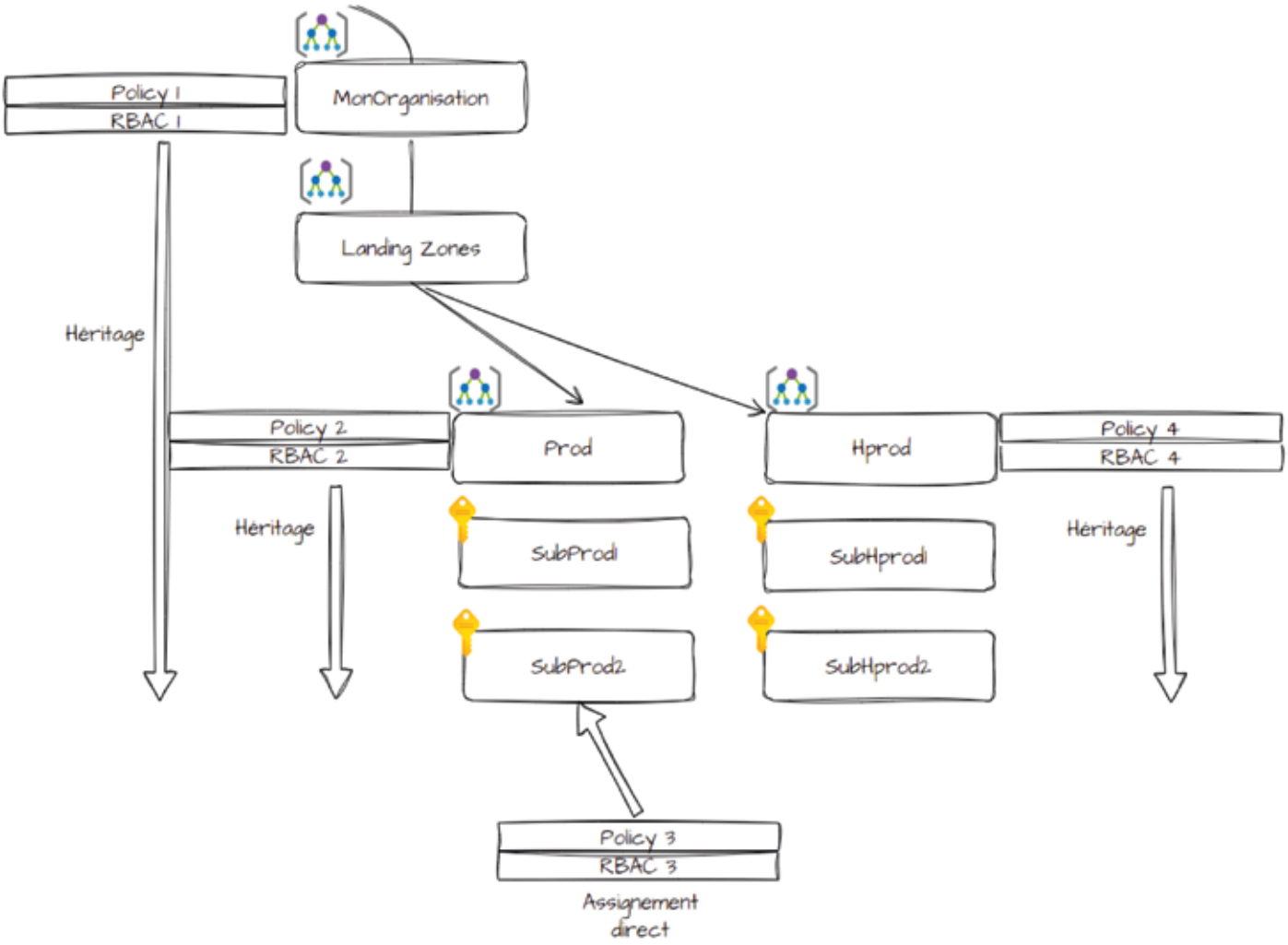
Une subscription ne peut contenir qu'un autre type de conteneur (le dernier) qui n'apparait pas ici, le groupe de ressources. Et les ressources Azure de tout type dans ce conteneur groupe de ressources.

Un Management group ne peut contenir que des subscriptions ou d'autres management groups.

Pourquoi c'est important ? Parce que tout ce qui va se trouver lié sur ces différents niveaux va avoir un impact. Tout, ce sont les RBAC et les Policy, liés sur les conteneurs et qui fonctionnent « de haut en bas » par héritage.

L'image suivante est un parfait exemple de cette notion d'héritage. C'est un zoom sur la partie Landing Zone de l'arborescence. Au sommet, le management group intermédiaire, qui porte normalement le nom de l'organisation, au-dessous, la Landing Zone, et à nouveau en dessous, deux nouveaux management groups. Un qui va contenir les environnements de production, un les environnements hors production.

Une remarque, ces conteneurs ne sont pas facturés.



Pour illustrer ce schéma par des exemples, on trouve liés à différents niveaux 4 rôles RBAC et 4 Policy. Ce qui donne de la valeur à ce modèle, c'est la liaison entre le niveau d'arborescence et le contenu.

Voilà l'explication :

Policy1 et RBAC1 vont porter des paramètres qui sont appliqués par héritage à tout ce qui trouve en dessous.

- RBAC1 : Un rôle Azure est positionné sur le management group *MonOrganisation* et est attaché sur ce rôle le groupe de sécurité de mes équipes d'administrateurs de haut niveau, qui vont exploiter tous les environnements.
- Policy1 : J'interdis le déploiement de ressources dans toutes les régions sauf France Centrale et France Sud. C'est une règle d'entreprise, elle est valable pour l'ensemble des ressources.

Tout ce qui est en dessous se voit imposer les mêmes paramètres par la règle de l'héritage. De manière automatique et cohérente.

Même logique pour Policy2 et RBAC2, positionnés sur Prod et qui vont porter des paramètres qui sont appliqués par héritage à tout ce qui trouve en dessous.

- RBAC2 : Un rôle Azure est positionné mais cette fois sur un groupe d'administrateurs qui ne gèrent que les ressources dans le management group Prod. C'est une équipe dédiée qui avec ses droits peut agir sur le management group Prod, sur les subscriptions qui sont sous cette arborescence, mais pas ailleurs.
- Policy2 : Je force les déploiements des ressources dans un mode de redondance de type GRS (redondance géographique) pour garantir ce paramètre sur la production.

Et toujours la même logique pour Policy4 et RBAC4, positionnés sur HProd et qui vont porter des paramètres qui sont appliqués par héritage à tout ce qui trouve en dessous.

- RBAC4 : Un rôle Azure est positionné mais sur un groupe d'administrateurs qui ne gère que les ressources dans le management group HProd.
- Policy4 : Je force les déploiements des ressources dans un mode de redondance de type LRS (redondance locale) pour garantir un coût moindre sur un environnement Hors Production qui n'a pas toujours besoin d'une redondance forte.

Et pour finir :

- RBAC3 : Un rôle Azure est positionné mais sur un groupe d'administrateurs qui ne gère que les ressources dans la subscription SubProd2 du schéma.
- Policy3 : J'interdis dans la subscription SubProd2 le déploiement de certains niveaux de services trop coûteux.

De cette manière, et sur toute l'étendue, il est possible de profiter de l'héritage pour homogénéiser son environnement. Sans le CAF, ces mêmes actions sont plus difficiles à mener. Imaginons 10 subscriptions de type Prod sans les managements groupes « chapeau ». Il faudra lier les RBAC et les Policy sur chaque subscription. Ce n'est pas la même charge de travail.

Il faut répéter les opérations unitairement, conteneur par conteneur. Garantir que le modèle de gouvernance est homogène lorsque l'on commence à travailler sans appliquer les règles au plus haut niveau, ce n'est pas chose facile.

Transformer son existant

Une fois le modèle bien assimilé, facile d'appliquer et de démarrer à l'état de l'art.

Pour un environnement existant, c'est un peu différent. Plusieurs points à prendre en compte avant de transformer et d'adapter son architecture conceptuelle. Particulièrement s'il existe déjà des management groups mais qu'ils ne respectent pas le CAF.

La transformation de l'existant dans un modèle CAF demande de la préparation et une mesure des impacts avant de se lancer.

La bascule doit être préparée avec soin. Déplacer une subscription n'est pas sans impact. Le point de départ ne porte pas forcément les mêmes RBAC et Policy que le point d'arrivée. Cela peut occasionner des blocages, ou à contrario, donner des droits trop importants. Il existe plusieurs solutions pour basculer en douceur, comme celle associant les Policy en mode Audit plutôt qu'en mode Deny ou Deploy. L'impact est mesurable par le taux de Compliance affiché dans la console Azure Policy.

Idem pour le contrôle des RBAC, il n'existe pas d'outils natifs, mais il est conseillé de créer un cahier de recettes et de mener les tests appropriés.

L'adoption du CAF est une belle aventure, qui assure à l'entreprise conformité, contrôle, cohérence et homogénéité.

L'impact est mesurable par le taux de Compliance affiché dans la console Azure Policy.

A retenir : un bon point de départ en 3 étapes

1 / Les conteneurs ne sont pas des ressources Azure facturées. Il faut donc profiter de la souplesse apportée par ce modèle pour créer une arborescence cohérente.

2 / RNAC et Policy sont les deux éléments essentiels à prendre en compte pour avoir une gouvernance fine de son infrastructure.

3 / La transformation de l'existant dans un modèle CAF demande de la préparation et une mesure des impacts avant de se lancer.

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

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.

Open Lake Technology
S'ENGAGE POUR LA CONFORMITÉ ET LA SUPERVISION DE VOTRE TÉLÉPHONIE UNIFIÉE

L'univers des technologies de l'information est complexe ! Open Lake Technology, éditeur de logiciels dédié à la résolution des risques, la conformité, l'adoption et la compréhension de la téléphonie unifiée, aide les DSI à relever les nombreux défis auxquels ils sont confrontés.

Qu'il s'agisse de conformité avec les réglementations ou d'adoption des nouvelles technologies sans oublier la compréhension de la complexité des outils IT, les DSI doivent à la fois éclairer, former et écouter les utilisateurs.

Comme le souligne **Anthony Derbès**, Président d'Open Lake Technology « les DSI sont désormais

Les DSI doivent à la fois éclairer, former et écouter les utilisateurs.

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

confrontés à un océan mouvementé de réglementations telles que le RGPD, MIFID 2, DORA, HIPAA, et bien d'autres normes sectorielles. Naviguer à travers ces eaux agitées exige une compréhension approfondie des exigences légales, mais aussi une capacité à mettre en œuvre des solutions technologiques conformes ». La responsabilité du DSI est donc cruciale pour l'aspect conformité mais aussi côté innovation et compétitivité. « L'adoption réussie des outils IT nécessite une stratégie claire, des programmes de formation efficaces et une communication transparente. Les DSI doivent créer un environnement propice à l'expérimentation et à l'apprentissage continu, encourageant ainsi une culture d'innovation au sein de leurs équipes. ».

Comment impulser une communication claire pour un avenir numérique sécurisé, performant et innovant ? **Anthony Derbes** revient sur ces sujets.

Avant tout, un mot de présentation sur Open Lake Technology ?

Open Lake Technology a été créé en 2018 afin d'aider les DSI à répondre à l'augmentation croissante des problématiques liées aux règlementations, aux nouveaux usages et à la supervision de leur téléphonie unifiée.

Les DSI sont des phares, éclairant le chemin à travers la complexité technologique pour l'ensemble de l'organisation.

Nous maitrisons développons et maintenons notre suite logicielle depuis la France, ce qui est une valeur ajoutée en termes de simplification d'échanges avec nos clients français.

De plus, notre solution est agnostique (elle se met en place sur n'importe quelle téléphonie de type TEAMS, CISCO Webex, IPC, BT TRADING, ZOOM...) ce qui nous permet de nous adapter à toutes les solutions du marché.

Enfin, nous sommes la seule solution française capable de répondre parfaitement aux obligations règlementaires de MIFID 2 en ce qui concerne la téléphonie régulée et son écosystème IT

La conformité est cruciale pour les DSI aujourd'hui. Quels sont les 3 points de vigilance à prendre en compte ?

Le premier point est la supervision des équipements régulés tels que les enregistreurs de communications où une solution dédiée s'impose.

ANTHONY DERBÈS

Le second est la validation d'un stockage WORM et la maitrise de durée de rétention bien spécifiques

Enfin, des process clairs sont indispensables entre l'équipe IT et Conformité non seulement pour un partage clair des responsabilités mais surtout pour une réactivité accrue et une diminution des risques de non-conformité.

Face à l'innovation, quelle stratégie doivent-ils mettre en place pour maintenir le cap ?

Les DSI sont des phares, éclairant le chemin à travers la complexité technologique pour l'ensemble de l'organisation. La technologie devrait être un catalyseur d'efficacité, mais pas un obstacle. Concrètement, les DSI peuvent maintenir le cap en mettant en place quelques démarches clés.

- Être toujours en état de la veille technologique
- Ne pas hésiter à remettre en cause une stratégie passée (cf. cloud public, vs hybride, vs privé)
- Faire des RFI (Request For Information) dès que le besoin se fait sentir ou qu'une nouvelle règlementation comme DORA par exemple est en préparation.

> Par Sabine Terrey

Priorités des investissements des entreprises en 2024

Parle-t-on d'optimisme des cadres ? Malgré la conjoncture macroéconomique, 83% prévoient d'augmenter les investissements dans les outils et technologies digitales (12 à 18 prochains mois) et 52 % en matière de durabilité !

Confiance dans la croissance

Retour sur les plans d'investissement de 2 000 cadres dirigeants (Monde). « *Notre rapport annuel sur le sentiment et les intentions d'investissement des entreprises du monde entier incite à l'optimisme en ce début d'année 2024* » selon Aiman Ezzat, Directeur général du groupe Capgemini. En effet, 56 % des cadres dirigeants restent confiants dans la croissance future de leur entreprise.

Expérience client, innovation, talents et connaissances, durabilité et chaînes d'approvisionnement sont autant de domaines stratégiques pour les entreprises. « *La technologie et l'IA sont en passe d'être les moteurs de la prochaine phase de la transition vers une économie mondiale plus digitale et plus durable.* »

Outils & Technologies digitales

Les outils et technologies digitales sont au cœur des priorités, notamment l'IA.

• ***L'IA, moteur d'innovation***
Prise de conscience du pouvoir de l'IA et de l'IA générative pour stimuler l'innovation et favoriser la croissance du chiffre d'affaires - 88 % se concentreront sur cette technologie.

• ***L'IA et les prises de décision stratégiques***
La prise de décision stratégique sera assistée par l'IA d'ici cinq ans. Dans le secteur des sciences de la vie, près de la moitié des prises de décisions stratégiques devraient s'appuyer sur l'IA d'ici cinq ans. Mais le jugement humain reste le plus important dans un monde régi par l'IA.

• ***La priorité de la cybersécurité***
61 % des dirigeants considèrent les menaces de cybersécurité comme l'un des principaux risques pour la croissance de l'entreprise.

Initiatives durables

• ***Le changement climatique, menace existentielle***
Le changement climatique sera le facteur N° 1 de désorganisation opérationnelle au cours de la prochaine décennie. L'absence de pratiques et de processus durables constituera un risque existentiel à long terme.

• ***Les politiques incitatives pour l'investissement***
57 % augmenteront les investissements dans les clean tech aux États-Unis au cours des deux ou trois prochaines années (loi sur la réduction de l'inflation - Inflation Reduction Act, IRA). 57% augmenteront aussi les investissements dans les clean tech soutenues par l'Union européenne en réaction au plan industriel du pacte vert - Green Deal Industrial Plan.

Montée en puissance du *nearshoring*[2] et du *friendshoring*[3]

L'impact de Covid-19 et des confinements économiques ont montré la vulnérabilité des chaînes d'approvisionnement du commerce mondial. Comment minimiser le risque de perturbation ? Les enseignements favorisent le développement de solutions de *nearshoring* et de *friendshoring* pour l'approvisionnement, réduisant la vulnérabilité aux tensions macro-économiques et logistiques.

Selon 45 %, une part importante des achats sera issue du friendshoring à l'avenir, et 49 % investissent dans des économies émergentes pour réduire leur dépendance à l'égard de la Chine.

Talents et lieu de travail

La pénurie de talents dotés des compétences requises figure parmi les principaux risques d'entreprise. Si on note des politiques de retour au bureau, un quart prévoit d'augmenter les investissements dans les espaces de bureaux.

Les entreprises pensent aussi que les modes de travail flexibles et hybrides sont appelés à perdurer.

2 Le nearshoring est le fait de délocaliser une activité économique, mais dans une autre région du même pays ou dans un pays proche, ou de la relocaliser dans une région plus proche.
3 Le friendshoring est une pratique commerciale où les réseaux de la chaîne d'approvisionnement se concentrent sur des pays considérés comme des alliés politiques et économiques afin de réduire davantage l'exposition au risque.

Source Capgemini Research Institute – Embracing a brighter future: Investment Priorities for 2024 - Vers un avenir meilleur : Priorités d'investissement pour 2024 - 2 000 cadres dirigeants d'entreprises - 10 secteurs d'activité et 15 pays (Allemagne, Australie, Brésil, Canada, Chine, Espagne, États-Unis, France, Inde, Italie, Japon, Pays-Bas, Royaume-Uni, Singapour et Suède) - novembre 2023.

Règlement DORA : DSI, COOPÉREZ AVEC LA DIRECTION DES RISQUES

L'Union Européenne renforce la sécurité informatique de ses institutions financières avec le règlement DORA (Digital Operational Resilience Act). Ce dernier doit minimiser la vulnérabilité systémique du secteur et lui permettre de rester résilient en cas de perturbation majeure des Systèmes d'Information. La DSI et la Direction des Risques devront renforcer leurs liens et mutualiser leurs ressources pour s'y conformer. Nicolas Chaine, Partner et Djibril Bamba, Managing Consultant chez Julhiet Sterwen nous éclairent.

Harmoniser en réponse à un contexte

La dépendance grandissante du secteur financier aux TIC (Technologies de l'Information et de la Communication) et l'interconnexion entre ses différents acteurs ont favorisé l'émergence de nouvelles menaces. Celles-ci font porter des risques sur la résilience opérationnelle numérique des acteurs du secteur financier européen.

La DSI et la Direction des Risques devront renforcer leurs liens et mutualiser leurs ressources pour s'y conformer.

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

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

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

iTPro.fr

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

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

iTPro.fr

9 chaînes informatiques

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

Des ressources exclusives

Enjeux DSI
Cloud Computing
Collaboration & mobilité
Exchange Server
IBM i

Un Club Abonnés

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

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

NICOLAS CHAINE

DJIBRIL BAMBA

Pour les contrer, le règlement DORA a été adopté en novembre 2022 par le Conseil de l'Union Européenne. Ce règlement européen d'application directe est entré en vigueur début 2023, et sa mise en application est prévue pour le 17 janvier 2025. Les régulateurs des 27 états de l'UE veilleront à la bonne application du texte. Pour la France, il s'agira de l'ACPR. Des sanctions définies par chaque Etat membre s'appliqueront en cas de non-conformité.

Ce règlement impose d'adapter les exigences de la réglementation aux problématiques de chaque institution.

Les exigences de DORA, qui imposent de manière inédite une obligation de résultat, s'articulent autour de cinq piliers. Les institutions financières et leurs prestataires de services TIC doivent s'organiser pour analyser ces nouvelles exigences et évaluer leurs impacts stratégiques et opérationnels sur leurs activités.

Répondre à une pression réglementaire accrue

Une bonne mise en œuvre de DORA permettra aux Directions des Systèmes d'Information (DSI) d'atteindre l'objectif d'amélioration et de valorisation des mécanismes de résilience opérationnelle numérique. Concrètement, ce règlement impose d'adapter les exigences de la réglementation aux problématiques de chaque institution. Pour cela, les DSI devront travailler conjointement et régulièrement avec les Directions des Risques et de la Conformité.

DORA impose aux DSI d'être maîtres de leur capacité à répondre à des incidents entraînant une dégradation, voire une interruption, des activités critiques. En cela, DORA se rapproche du texte NIS 2 qui exige de renforcer les mesures de protection et de notification à appliquer en cas d'incident.

DORA constitue cependant une règle spéciale qui prend le pas, en droit, sur la règle générale. Il impose aux institutions d'être en conformité avec ce règlement en priorité. En conséquence, la pression réglementaire, auparavant surtout ressentie par les Directions des Risques et de la Conformité, s'exerce maintenant sur les DSI.

DSI : s'affirmer comme membre essentiel d'une équipe coordonnée...

Pour que l'entreprise soit conforme à DORA, la DSI devra travailler étroitement avec, entre autres, la Direction des Risques pour répondre aux exigences du règlement sur **ses 5 piliers**.

Le premier pilier est **la gestion des risques liés aux TIC**. La DSI devra constituer et mettre à jour, annuellement, un inventaire des actifs informatiques. Ceux sur lesquels s'appuieront les activités critiques seront à identifier en priorité avec la Direction des Risques. Cette dernière coconstruira et maintiendra avec la DSI une procédure d'évaluation et de gestion des risques, l'analyse des menaces et les tolérances d'impact. Les synergies entre les deux directions permettront de capitaliser sur les tests pour élaborer ou actualiser la matrice des risques. La DSI devra enfin, là aussi annuellement, sensibiliser et former le comité exécutif aux risques TIC et plus particulièrement cyber. Pour cela, elle mettra à profit les échanges avec la Direction des Risques sur l'approche à adopter.

La classification et la notification des incidents liés aux TIC constituent le deuxième pilier. La DSI devra formaliser et optimiser les processus et procédures de gestion des incidents. Elle établira ensuite une classification des incidents conforme aux exigences réglementaires avec la Direction des Risques. Elles œuvreront aussi la DSI à établir des KPIs qui permettront un pilotage optimal des incidents en qualifiant leur sévérité. La Direction des Risques étant experte dans l'élaboration d'un plan de communication et de réaction, elle travaillera avec la DSI sur les incidents liés aux TIC.

Le troisième pilier concerne **la réalisation de tests périodiques de résilience opérationnelle numérique**. Ils permettront d'assurer la réalisation et la valorisation de tests de résilience en impliquant les métiers. Ils seront effectués par des collaborateurs indépendants internes ou externes, en priorité sur les actifs et applications critiques. Les entreprises devront privilégier les exercices les plus proches des conditions réelles. Pour éviter de perturber les opérations, la Direction des Risques assistera la DSI, notamment dans l'ajustement des niveaux de difficulté. Les résultats seront alors plus significatifs que ceux de « simples » tests.

Le quatrième pilier est consacré à **la gestion des risques liés aux prestataires tiers de services TIC**. Cette gestion passera par une collaboration entre les départements. Ainsi, en plus de la DSI et la Direction des Risques, les départements Juridique et Achats seront concernés. La DSI s'appuiera sur leurs expertises pour définir une politique d'utilisation des services TIC critiques. Elle contribuera également à structurer les tables du registre d'information fournisseurs. Le Juridique et les Achats poseront un œil averti sur les contrats de services. De son côté, la Direction des Risques évaluera le niveau de risque associé aux services mentionnés. Aussi, des stratégies de sortie seront à prévoir pour garantir la continuité des activités critiques supportées par des fournisseurs TIC.

Le cinquième et dernier pilier concerne **le partage d'informations liées aux cybermenaces**. La DSI et la Direction des Risques devront collaborer pour formaliser une procédure de reporting au régulateur. Cela sera possible via la future plateforme de l'UE dédiée aux incidents majeurs liés aux TIC.

… pour maîtriser les enjeux actuels et futurs du règlement DORA

Le succès des projets de mise en conformité avec le règlement DORA dépendra de la capacité de la DSI à être un membre actif d'une équipe soudée, formée avec les directions des Risques, de la Conformité, du Juridique, des Achats et des Opérations. La réussite des actions à mener repose sur le changement de pratiques qu'implique cette étroite collaboration.

La DSI devra ainsi adopter une approche par les risques, tandis que les autres directions renforceront leur maîtrise des enjeux liés aux TIC. Ensemble, elles pourront être à l'avant-garde de la résilience opérationnelle numérique pour anticiper et non subir les exigences du régulateur.

DORA constitue cependant une règle spéciale qui prend le pas, en droit, sur la règle générale.

1 La gestion des risques liés aux TIC, la gestion, la classification et la notification des incidents liés aux TIC, la réalisation de tests de résilience opérationnelle numérique, la gestion des risques liés aux prestataires tiers de services TIC et le partage d'informations liées aux cybermenaces.

AI Act : QUEL ENCADREMENT DES SYSTÈMES D'IA PAR L'UE ?

La proposition de règlement visant à réguler de manière harmonisée les systèmes d'intelligence artificielle a été présentée à la Commission Européenne en avril 2021. Eclairage par Maître Pauline Ducoin, avocate associée au sein du Cabinet Cornet Vincent Ségurel à Lyon.

Au terme d'un trilogue institutionnel, l'adoption du texte est intervenue le 8 décembre 2023 et les ajustements techniques de cohérence ont eu lieu au cours du mois de janvier 2024, pour aboutir à une version finalisée le 26 janvier 2024.

Cette règlementation, qui s'inscrit dans la stratégie numérique pour l'Europe, vise à encadrer une des technologies de rupture les plus impactantes de ces dernières années (voire décennies) et est notable à plusieurs égards.

Contrairement aux reproches habituellement formulés contre les textes visant à réguler *a posteriori* des technologies ou des usages déjà largement déployés en pratique, ce texte d'initiative européenne, sera le premier texte contraignant d'envergure sur l'intelligence artificielle à être adopté dans le monde.

Les Etats-Unis disposent par comparaison de principes directeurs superficiels (*Blueprint for an Artificial Intelligence Bill of Rights*) et d'*executive orders* non contraignants.

Cette proposition de règlement est construite sur une approche par les risques inhérents aux technologies et usages qu'elle vise à encadrer.

Définition et Champ d'application

Un système d'IA est défini comme « *un système basé sur une machine, conçu pour fonctionner avec différents niveaux d'autonomie, qui peut faire preuve d'adaptabilité après son déploiement et qui, pour des objectifs explicites ou implicites, déduit, à partir des données qu'il reçoit, comment générer des résultats tels que des prédictions, du contenu, des recommandations ou des décisions pouvant influencer des environnements physiques ou virtuels* » (art.3). Les systèmes logiciels basés uniquement sur des règles définies par des humains sont expressément exclus du champ d'application du règlement.

Aux termes de cette définition, l'une des principales caractéristiques des systèmes d'IA est leur capacité d'**inférence**.

Cette inférence fait référence au processus d'obtention des résultats, tels que les prédictions, le contenu, les recommandations ou les décisions, qui peuvent influencer les environnements physiques et virtuels, et à la capacité des systèmes d'IA à dériver des modèles et/ou des algorithmes à partir d'entrées/données. Les techniques qui permettent l'inférence lors de la construction d'un système d'IA comprennent les approches d'apprentissage automatique qui apprennent à partir des données comment atteindre certains objectifs, et les approches basées sur la logique et la connaissance qui infèrent à partir de la connaissance codée ou de la représentation symbolique de la tâche à résoudre. La capacité d'un système d'IA à déduire va au-delà du traitement de base des données, permet l'apprentissage, le raisonnement ou la modélisation (considérant 6).

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

IT AND CYBERSECURITY MEETINGS BY WEYOU GROUP

WWW.IT-AND-CYBERSECURITY-MEETINGS.COM

19, 20 & 21 MARS 2024

PALAIS DES FESTIVALS ET DES CONGRÈS DE CANNES

ILS SONT DÉJÀ INSCRITS

by weyou group

Professional Exhibitions and One to One Meetings Exhibitions

PAULINE DUCOIN

Les types de systèmes régulés ainsi définis, l'IA Act produit ses effets de manière extraterritoriale puisque les règles édictées s'appliquent à tout acteur qui fournit, distribue, déploie (voire utilise) des systèmes d'IA sur le territoire de l'Union Européenne.

Règles édictées et délais de mise en conformité

Dans son contenu, le règlement impose des **obligations** différentes selon les catégories auxquelles les systèmes d'IA appartiennent :

- Les systèmes d'IA à **risque inacceptable** sont purement **interdits** (scoring social à usage général) et encourent le plus haut niveau de sanctions : 35 millions d'€ ou 7% du chiffre d'affaires annuel mondial.
- Les systèmes d'IA à **haut risque** (traitement de données biométriques, santé, droits fondamentaux, infrastructures critiques, etc.) sont soumis à des **prérequis contraignants**, tels que **l'enregistrement** du système dans une base de données européenne et le marquage CE
- Les systèmes d'IA à **risques limités** (deep fake à vocation artistique, chatbot, etc.) sont soumis à des obligations **d'information transparente** quant à l'utilisation du système
- Les systèmes d'IA à **risques minimes** (jeux vidéo, filtres techniques, etc.) sont invités à se soumettre volontairement aux obligations prévues par le règlement.

Le délai de mise en conformité aux obligations découlant du règlement pour les acteurs concernés est par principe de **24 mois à compter de l'entrée en vigueur du règlement**.

Les Etats membres bénéficient également de ce délai de 24 mois pour permettre une pleine efficacité de ces dispositions sur leur territoire. En particulier, ils doivent procéder à la désignation de l'autorité nationale en charge du suivi de cette règlementation (la CNIL en France), la mise en place du **bac à sable règlementaire**, et la pleine effectivité des sanctions.

Par exception, certaines obligations ont des échéances dérogatoires :

- **6 mois** après l'entrée en vigueur, les interdictions relatives aux systèmes d'IA **inacceptables** produisent leurs effets,
- **9 mois** pour la finalisation des codes de pratiques pour les **modèles généraux** (GPAI)
- La création de **l'office européen de l'IA** doit intervenir dans les **12 mois**,
- Le délai de mise en conformité est porté à **36 mois** pour les systèmes d'IA à haut risque destinés à être utilisés comme composants de sécurité d'un produit
- Un délai de **4 ans** est laissé aux systèmes d'IA d'ores et déjà sur le marché au jour de l'entrée en application du règlement pour se conformer à ses obligations

Evolutions technologiques et règlementaires

De nombreuses évolutions d'usages et de technologies ont été prises en compte au cours des discussions sur l'AI Act, en particulier les systèmes d'IA génératives et les modèles de langages à usage général.

C'est ainsi que la dernière mouture du texte intègre de nouvelles dispositions concernant les modèles d'IA à usage général ou GPAI et crée des obligations horizontales spécifiques, incluant la documentation technique et des évaluations de risques.

Face au constat que les systèmes de fondation présentent un risque systémique, la dernière version du texte a prévu un **seuil quantitatif** de classification des GPAI.

Le délai de mise en conformité aux obligations découlant du règlement pour les acteurs concernés est par principe de 24 mois à compter de l'entrée en vigueur du règlement.

La capacité de calcul, de même que le développement des technologies, augmentent toutefois de manière exponentielle, de sorte que le règlement prévoit une évaluation continue des règles applicables et impose une mise à jour périodique du règlement 3 ans après son entrée en application, puis tous les 4 ans.

Enfin, des précisions devront être apportées par les autorités dédiées, au premier lieu desquelles l'Office européen sur l'IA, pour permettre une compréhension opérationnelle des exigences règlementaires.

La mise en conformité des acteurs va ainsi nécessiter une prise en compte des contraintes réglementaires de l'IA Act, ainsi que des nombreux autres impératifs nationaux et européens, dès le stade de la conception des systèmes d'IA pour permettre de ne pas freiner l'innovation tout en maîtrisant les usages.

Changements sociétaux : 5 tendances à surveiller par les entreprises

Voici 5 tendances qui permettront aux entreprises de tirer parti de la puissance des nouvelles technologies en 2024 !.

Changements technologiques, augmentation des consommateurs phygitaux à l'IoT et à l'IA, pratiques de travail durables, main-d'œuvre décentralisée ... autant de points à prendre en compte ! Selon Insight « *les changements sociétaux favorisent l'adoption des technologies émergentes et les implications se font sentir à tous les niveaux de l'entreprise* ».

S'adapter et faire preuve de souplesse sont les maitres mots en 5 points.

• L'expérience numérique humanisée

L'utilisation de la technologie pour transformer l'expérience des clients et des employés est une priorité pour les entreprises qui cherchent des moyens novateurs de relier les mondes numérique et physique.

• L'IA pour débloquer les données

L'IA générative pour maximiser l'intelligence organisationnelle : avec l'IA générative, les entreprises veulent obtenir des informations à partir des données, stimuler la productivité et améliorer la satisfaction de la clientèle. Cependant, la réflexion se porte sur les réglementations, la gouvernance, les données, la sécurité, avec la mise en place de normes, règles, politiques éthiques, mesures de sécurité.

• Les pratiques de travail durables

Dans le domaine des technologies, il faut prendre en compte l'utilisation de l'énergie, la durabilité de la supply chain et les cycles de vie des produits pour garantir et maintenir des pratiques commerciales durables.

• La connectivité intelligente

L'essor de l'IoT change le monde avec la prolifération des appareils et la convergence de l'IA et de l'IoT. L'Intelligent Edge est clé pour capturer et transformer les données en connaissances.

• L'espace de travail redéfini

Les employés exigent plus de travail décentralisé. Avec la mondialisation et la main-d'œuvre à distance notamment, l'informatique jouera un rôle pour la décentralisation, la flexibilité et la collaboration.

Phil Hawkshaw, EMEA CTO & Director of Technology d'Insight commente « *notre deuxième rapport annuel sur les tendances offre aux entreprises de toutes tailles une vue d'ensemble claire sur la manière de tirer parti des dernières technologies dans la poursuite de leurs objectifs stratégiques* ».

Source Rapport Insight 2024 Trends

Consol Connect : UNE SEULE PLATEFORME AUTOMATISÉE POUR GÉRER SA CONNECTIVITÉ AVEC SOUPLESSE ET RAPIDITÉ

Consol Connect qui dispose d'un bureau à Paris depuis plusieurs mois, offre à ses partenaires un service automatisé de providing de connexions privées (network as a service) via une plateforme dédiée. Pour en savoir plus, Lionel Rayon, Vice President, Technology Partnerships chez Console Connect a accepté de répondre à quelques questions.

Qui est Console Connect ? Qu'est-ce qui vous distingue ?

Console Connect est une solution SaaS permettant d'acheter des connexions privées MPLS de niveau 2 et 3 à la demande en fonction de ses besoins en bande passante. La plateforme utilise la technologie propriétaire SDCI (Software Defined Cloud Interconnect), adossée au réseau mondial de PCCW Global. Depuis le portail Console Connect, les entreprises peuvent provisionner très simplement et de manière automatisée des accès au cloud depuis 950 centres de données pour des durées allant de 1 jour à plusieurs mois.

+100
entreprises

+6000
participants

CYBER SHOW PARIS

29-30 mai 24

+5000
m2 d'animation

+100
interventions

TOUS CONCERNÉS, TOUS MOBILISÉS.

L'ESPACE CHAMPERRET
6 rue Jean Oestreicher
75017 Paris

TICKET

> S'INSCRIRE À L'EVENT
CYBERSHOWPARIS.FR

Contrairement aux solutions utilisant l'internet public, les connexions sont sécurisées et offrent des niveaux de performance et de disponibilité parmi les meilleurs au monde.

Depuis plusieurs mois les responsables IT sont confrontés à de véritables défis tant du point de vue de la souplesse de leur infrastructure réseau que des coûts associés. Les besoins évoluent à la hausse tout comme les tarifs. Le modèle économique ultra compétitif de réseau facturé à la demande offre la flexibilité, la sécurité et la réduction des dépenses réseau exigée par les entreprises.

Qu'est-ce que vous entendez par « réseau plateforme first » ?

Cela signifie que le client gère son réseau via la plateforme digitale Console Connect. Il n'est plus nécessaire de contracter avec plusieurs fournisseurs pour créer ses connexions réseau. Une seule plateforme entièrement automatisée par API permet désormais de créer et de gérer sa connectivité avec des bandes passantes garanties.

Nous offrons à nos clients l'un des plus grands réseaux mondiaux privés. Transférer ses données vers le cloud ou faire du multicloud est désormais un jeu d'enfant comparé aux méthodes traditionnelles d'achat réseau auprès d'opérateurs historiques.

Nous pouvons comparer le saut technologique opéré avec notre plateforme à celui effectué par les éditeurs de logiciels au milieu des années 2010. Ceux-ci ont abandonné la mise à disposition de leur technologie en mode on premise au profit du SaaS. Les bénéfices utilisateurs en termes de gestion des parcs informatiques ont été indéniables. Aujourd'hui nous vivons le même phénomène pour la gestion des infrastructures réseau. Tout est désormais plus simple, plus rapide et plus efficace.

À propos de l'Edge computing, il est possible de déployer des liens privés pour connecter des flottes de cartes SIM ou des architectures IoT. Pouvez-vous en dire plus ?

Nous avons rapidement pris conscience du besoin grandissant des entreprises à disposer d'une solution pour couvrir les enjeux liés à l'IoT. En effet, alors que la maturité de cette technologie n'est plus à démontrer, il est clair que celle-ci devrait connaître un boost considérable à court terme. Le besoin en collecte de données, notamment lié à l'accélération de l'utilisation de l'IA, est de plus en plus important. Il est dès lors essentiel de disposer de solutions dédiées pour ne pas être bridé pour de simples questions de coûts dans son développement technologique.

Console Connect a développé une offre permettant d'automatiser la fourniture de connectivité IoT vers le cloud tout en restant sur un réseau mobile (2G/3G/4G/5G) privé de bout en bout.

LIONEL RAYON

La solution Edge SIM permet de commander ses cartes SIM, de les activer et de leur attribuer des droits d'accès aux Clouds souhaités directement depuis la plateforme. Les données peuvent ensuite être acheminées en toute sécurité vers le cloud via notre service CloudRouter.

Quelles sont les technologies de virtualisation et d'hyperautomatisation nécessaires ? Quels sont les avantages pour les entreprises ?

L'hyperautomatisation et l'orchestration du service sont entièrement prises en charge par Console Connect et sont compatibles avec les technologies de virtualisation. Sur ce modèle SaaS, aucune dépense en équipement n'est nécessaire pour les entreprises. La connectivité est facile à mettre en place et est automatisée par API, facturée à la demande, offrant une flexibilité dans la gestion des flottes de cartes SIM. Cette solution évite les failles de sécurité liées à l'Internet public tout en offrant des performances réseau élevées pour connecter tout type d'objet aux applications hébergées par les fournisseurs de cloud.

Une seule plateforme entièrement automatisée par API permet de créer et de gérer sa connectivité avec des bandes passantes garanties.

Ce dernier point est notable. En 2010, on comptait environ 1 milliard d'objets connectés dans le monde, chiffre qui passera à 50 milliards en 2025 et à 100 milliards en 2030. Le besoin est énorme mais il engage un double dynamique : un accroissement des coûts potentiels pour assurer leur connectivité réseau et l'augmentation de failles potentielles de sécurité. Notre offre entend contribuer à améliorer les défis des responsables réseau en charge de ces sujets.

> Par Sabine Terrey

Paysage des cybermenaces mondiales

Basé sur les observations de plus d'un milliard de données au cours des 12 derniers mois, le rapport d'Elastic Security Labs met en avant la diversification et le développement rapide des ransomwares.

Quelles sont les grandes tendances identifiées ?

Malwares : BlackCat, Conti et Hive parmi les plus répandus !

La majorité des malwares observés appartiennent à un petit nombre de familles de ransomwares d'outils prêts à l'emploi - "Commercial Off-the-shelf" COTS.

- *BlackCat, Conti, Hive, Sodinokibi et Stop*

Ce sont les familles de ransomwares les plus répandues identifiées par le biais de signatures, soit 81 % de l'activité des ransomwares.

- *Les malwares "COTS" comme Metasploit et Cobalt Strike*

Ils constituent 5,7 % des signatures observées. Sur Windows, ces familles représentent environ 68 % des tentatives d'intrusion.

- *Les machines sous Linux les plus touchées*

Environ 91 % des signatures de malwares proviennent de machines sous Linux (représentant 6% sur Windows).

Endpoints : les techniques d'exécution de code et le contournement des défenses privilégiées

Les entreprises doivent évaluer l'inviolabilité des capteurs de sécurité sur les endpoints et identifier les pilotes des périphériques vulnérables utilisés pour désactiver les technologies de sécurité.

- *Exécution de code & Techniques de contournement*

Cela représente plus de 70 % de toutes les alertes recensées sur les endpoints.

- *Techniques discrètes*

Les techniques les plus discrètes visent les appareils sous Windows, ciblent des attaquants et enregistrent 94 % des alertes liées à des comportements suspects, suivis de macOS à hauteur de 3 %.

- *Collecte d'identifiants macOS*

La collecte d'identifiants macOS (Credential Dumping) constitue 79 % des techniques de compromission des accès des attaquants, soit +9 % depuis l'année dernière.

Sécurité du cloud

Les acteurs malveillants profitent des mauvaises configurations, des contrôles d'accès laxistes, des identifiants non sécurisés et de l'absence de systèmes fonctionnels basés sur le principe du moindre privilège.

- *Amazon Web Services*

Les tactiques utilisées sont le contournement des défenses (Defense Evasion) 38 %, la compromission des identifiants d'accès - 37 % et l'exécution de code - 21 %.

- *Microsoft Azure*

Parmi les événements recensant les compromissions d'accès, 53 % étaient liés à des comptes Microsoft Azure authentiques.

- *Microsoft 365*

Plus de 86 % des indicateurs de compromissions sont liés à l'utilisation d'identifiants d'accès.

- *Google Cloud*

85 % des indicateurs de détection de menaces dans Google Cloud étaient liés à la technique de contournement des défenses (Defense Evasion).

- *Kubernetes*

La découverte (Discovery) représentait 61 % des indicateurs relatifs à Kubernetes, liés à des demandes de compte de service inattendues ayant été rejetées.

Source Global Threat Report – Elastic Security Labs – 2eme édition

Inclusion et IA générative

AU CŒUR DES DÉCISIONS DES DIRIGEANTS ET DES TENDANCES RH

Si l'environnement professionnel connait déjà de nombreux changements, il en connaîtra bien d'autres en 2024. Les évolutions vont s'accélérer : diversité, équité et inclusion (DEI), gestion des données et intelligence artificielle générative, technologies RH, conformité et développement des talents... Les priorités influencent les prises de décision des dirigeants.

Rester à la pointe de ces bouleversements est fondamental. Alors quels sont les éléments à ne pas sous-estimer et à mettre en place ?

L'inclusion au premier plan

Diriger en tenant compte de la DEI est une priorité pour les décideurs. Certaines organisations se focalisent particulièrement sur l'inclusion par rapport à la diversité et l'équité.

LE DROIT À LA DÉCONNEXION : UN ENJEU RH

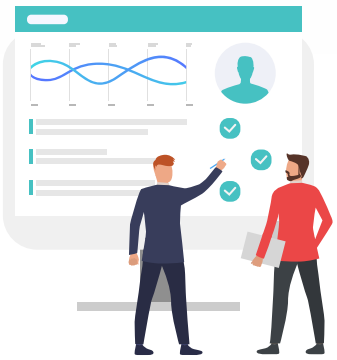
DANS UN MONDE RÉGI PAR L'IMMÉDIATETÉ,
LA DÉCONNEXION N'EST PLUS UNE OPTION, MAIS UN DROIT.

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

Les évolutions législatives (index de l'égalité professionnelle ou recul de l'âge de départ à la retraite) incitent les entreprises à revoir les programmes d'inclusion, de diversité, d'équité, les pratiques de recrutement, et les plans de développement de carrière. Pour placer l'inclusion au cœur de la stratégie RH, l'initiation et la sensibilisation des collaborateurs à ce sujet sont une étape clé.

Les précurseurs en matière de diversité, équité et inclusion

De plus en plus d'entreprises adoptent une approche proactive en matière de DEI, sans attendre la législation. Elles reconnaissent les avantages qui en découlent : productivité, innovation et performance. C'est le cas pour la transparence des rémunérations, dont une directive européenne a été adoptée en mai 2023 obligeant les employeurs à fournir aux collaborateurs, sur demande, des informations sur les niveaux de rémunération moyens des salariés effectuant un travail identique.

L'IA générative va optimiser les processus RH et de paie.

Selon l'étude d'ADP « Le potentiel de la paie en 2024 », près de la moitié des responsables de paie (Monde) signalent une augmentation du nombre de questions portant sur l'égalité salariale et la transparence de la paie depuis l'année dernière (46 % et 44 %, respectivement).

Sans attendre de se mettre en conformité d'ici la transposition de cette directive dans le droit français, le 7 juin 2026 au plus tard, des organisations jouent la carte de la transparence des salaires, un véritable levier pour améliorer l'équité salariale et l'égalité femmes-hommes.

Il est donc essentiel de développer une stratégie de rémunération. Disposer de données sur les salaires est primordial pour guider les approches et prévoir un plan pour se mettre en conformité.

Des technologies RH intelligentes grâce à l'IA générative

En 2024, les dirigeants peuvent s'attendre à des technologies RH plus intelligentes et faciles à utiliser. L'IA générative va optimiser les processus RH et de paie, faciliter la gestion des tâches complexes et permettre aux dirigeants de se concentrer sur leurs effectifs et rationaliser les opérations de croissance. Si les utilisations de l'automatisation et de la robotique permettent déjà de réduire les contraintes de temps et des processus chronophages, l'IA générative analysera plus rapidement les données de paie dont disposent les entreprises pour accompagner les dirigeants à établir leurs priorités.

Les solutions de RH et de paie intègrent déjà l'IA générative et des fonctionnalités avancées de l'IA pour faciliter la recherche et la sélection de candidats, l'onboarding et la formation, la gestion de la paie et des avantages sociaux, les plans de développement individuel, la gestion de la performance et de la succession, la gestion administrative du personnel, et l'engagement des collaborateurs.

L'éthique et la conformité au cœur de la gestion des données et de l'IA générative

Les stratégies en matière d'éthique et de conformité deviennent cruciales pour évaluer la manière dont les données seront utilisées avec l'IA générative, les personnes qui accèderont à cette technologie et les meilleures pratiques de conformité aux exigences légales et réglementaires notamment.

Les organisations examineront attentivement les aspects éthiques et de conformité, en se posant les deux questions suivantes :

- Comment la confidentialité et la sécurité des données sont-elles gérées, compte tenu des avancées de l'IA générative ?
- Quels sont les droits des salariés concernant l'utilisation de leurs données pour former des modèles d'IA générative ?

Les piliers du bien-être, des avantages sociaux et de la reconnaissance

Les principaux fournisseurs de solutions RH mettent au point des outils de gestion des avantages sociaux et de reconnaissance du personnel, composants de l'expérience collaborateur. Pour 20 % des organisations aux Etats-Unis, les outils de gestion des avantages sociaux et de reconnaissance figurent parmi les quatre principales catégories des dépenses en technologies RH pour 2024.

De même, les outils améliorant le bien-être au travail (santé physique, morale et financière) sont indispensables. Cet élément fait partie intégrante des politiques de recrutement et de rétention des talents. Le bien-être financier devient fondamental alors que le pouvoir d'achat des salariés est mis à mal.

De plus en plus d'entreprises adoptent une approche proactive en matière de DEI, sans attendre la législation.

La dimension mondiale du travail à distance

Les frontières internationales représentent de moins en moins un obstacle pour l'emploi, notamment pour les nomades numériques, pouvant travailler à distance, quel que soit le lieu. Ainsi, un tiers des salariés français (33 % - 48 % Monde) seraient prêts à déménager à l'étranger tout en continuant à travailler pour leur employeur actuel selon l'enquête de l'ADP Research Institute, « *People at Work 2023 : l'étude Workforce View* ». Plus d'un collaborateur sur 10 (12 %) déclare d'ailleurs avoir déjà sauté le pas.

La flexibilité (horaires, lieu de travail) s'inscrit dans la volonté des collaborateurs de bénéficier d'un meilleur équilibre vie professionnelle - vie privée. Mais, les employeurs doivent veiller à maintenir le lien social, la cohésion et le sens du collectif. Surtout, lorsque les salariés travaillent à distance depuis l'étranger. Des conditions logistiques ou de sécurité informatique sont également importantes : accès sécurisé aux réseaux de l'entreprise ou gestion du travail sur différents fuseaux horaires pour des équipes internationalisées.

Les compétences pour répondre à la pénurie de main-d'œuvre

L'inadéquation entre la formation des collaborateurs et les besoins des entreprises est réelle, notamment pour les compétences en matière de nouvelles technologies. C'est par exemple un cas frappant au sein des équipes de gestion de la paie, où les compétences spécialisées en lien avec la sécurité des données, les outils d'analyses ou la gestion de la conformité sont en augmentation.

Selon l'enquête ADP *People at Work 2023 : l'étude Workforce View*, les compétences en management et en relations humaines seront nécessaires et les soft skills seront très demandées pour créer des liens entre les collaborateurs et promouvoir l'empathie.

L'évolution du parcours professionnel traditionnel

Le parcours professionnel traditionnel, qui consistait à obtenir un diplôme, entrer sur le marché du travail puis gravir les échelons est devenu une trajectoire rare. Aujourd'hui, les carrières se déroulent différemment : les travailleurs naviguent à travers un éventail de possibilités professionnelles, ils peuvent choisir entre la mobilité et la stabilité.

Les soft skills seront très demandées pour créer des liens entre les collaborateurs et promouvoir l'empathie.

Certains travailleurs optent pour des domaines qui n'exigent pas de diplôme ou entrent sur le marché du travail tout en poursuivant leurs études. Aussi, les dirigeants doivent repenser la manière dont ils conçoivent la gestion des carrières pour aller à la rencontre les talents là où ils se trouvent.

Source Expertise ADP (Automatic Data Processing)

L'Open Source Intelligence :
UN OUTIL NÉCESSAIRE DE CYBERDÉFENSE

Si l'open source, ces données accessibles à tous sans restriction, existe depuis longtemps, l'Intelligence Artificielle (IA), notamment générative, a redistribué les cartes. La possibilité d'analyser un nombre toujours plus important de données a rendu l'Open Source Intelligence (OSINT) indispensable aux cybercriminels, toujours plus innovants, mais également aux professionnels de la sécurité. Ces derniers peuvent ainsi mettre en place une défense proactive et garder une longueur d'avance sur les hackers. Entretien avec Andy Thompson, spécialiste de la cybersécurité chez CyberArk qui nous livre son analyse.

Que sont les outils OSINT et quelle est leur place dans les activités de renseignement au sens large ?

L'Open Source Intelligence (OSINT) est une discipline qui remonte à l'aube de l'humanité. Elle consiste, en bref, à collecter des informations accessibles à tous pour les exploiter à des fins de renseignement. Pendant la Seconde Guerre mondiale, par exemple, les services américains étaient parvenus, en se basant sur les variations du prix des oranges, à évaluer l'état des voies ferroviaires après des campagnes de bombardement. Les avancées technologiques récentes, en particulier l'adoption d'outils d'IA générative, ont considérablement accru le potentiel des outils OSINT : les pirates comme les équipes de sécurité peuvent désormais rassembler de vastes quantités de données provenant de sources multiples afin d'en tirer les informations dont ils ont besoin. Ces outils offrent donc un moyen de renforcer la cybersécurité des entreprises, mais ils leur permettent aussi de garder un œil sur la réputation de leur marque, les préférences de leurs clients et leur présence sur les réseaux sociaux.

ANDY THOMPSON

Comment peut-on mettre ces outils au service de la sécurité des entreprises ?

Le volume des attaques en ligne ne cesse d'augmenter, signe que les outils de sécurité traditionnels ne sont ni assez rapides, ni assez complets pour couvrir toutes les vulnérabilités présentes dans les systèmes de défense. La collecte d'informations de Threat Intelligence à l'aide d'outils OSINT peut et doit faire partie intégrante des tâches quotidiennes des équipes de sécurité, notamment parce que cette approche est déjà mise en œuvre de manière offensive contre les entreprises. Or, certaines informations disponibles dans les plateformes open source, les forums du Dark Web et les réseaux sociaux peuvent donner une longueur d'avance aux équipes de cybersécurité. Si ces équipes avaient su trouver les informations disponibles sur la vulnérabilité Log4j dans le Dark Web, et ce, bien avant qu'elle n'ait fait l'objet d'articles dans la presse grand public, elles auraient pu intervenir à temps pour la neutraliser.

Les outils OSINT peuvent aussi être utilisés pour identifier des menaces internes aux entreprises, par exemple, en permettant une détection accélérée des employés insatisfaits qui critiquent systématiquement leurs responsables sur internet. Il est également possible de s'en servir pour valider les fournisseurs tiers, car ils donnent les moyens d'effectuer une évaluation approfondie des risques et de déterminer si un partenaire potentiel présente des vulnérabilités susceptibles de faciliter, par exemple, une attaque de sa supply chain.

Les entreprises peuvent enfin utiliser ces outils pour bloquer toute usurpation de leur nom de domaine et de leur URL, protégeant ainsi leurs salariés et leurs clients contre les attaques de phishing. Du point de vue de la réponse aux incidents, les pratiques de l'OSINT nous aident à mieux comprendre les outils, les tactiques et les motivations des hackers, ce qui permet de nous défendre de manière proactive contre leurs tentatives d'intrusion, mais aussi de reprendre plus rapidement une activité normale en cas d'incident.

Comment les outils OSINT renforcent-ils les pratiques traditionnelles de cybersécurité et pourquoi deviennent-ils actuellement un aspect essentiel des stratégies de cyberdéfense ?

Il reste un long chemin à parcourir avant que les outils OSINT ne soient reconnus comme un aspect essentiel de la cyberdéfense. Ils commencent à être adoptés par les grandes entreprises disposant de solutions de cybersécurité d'une maturité plus élevée, ainsi que d'une plus grande visibilité publique. Mais trop d'entreprises de moindre envergure ont encore une vision très limitée des paramètres à prendre en compte pour assurer leur sécurité. Elles tardent donc à comprendre ou à exploiter pleinement tout ce que l'OSINT peut leur apporter en tant qu'approche et qu'arsenal d'outils.

Quels sont les défis et les problèmes éthiques à résoudre lors de la collecte et de l'utilisation de renseignements OSINT ?

Tout outil utilisé pour collecter et analyser de grandes quantités d'informations implique des précautions éthiques, la plus importante restant probablement celle de la conformité. Avec le RGPD par exemple, les entreprises doivent être très attentives à la manière dont elles traitent et stockent les données qu'elles collectent. D'où viennent-elles ? Leur exploitation est-elle possible ? Qui doit être informé ?

Tout outil utilisé pour collecter et analyser de grandes quantités d'informations implique des précautions éthiques

Il est également nécessaire de veiller à l'exactitude et à l'intégrité des données ainsi collectées et traitées, en éliminant toute propagande et rumeurs infondées dans les informations recueillies, afin d'aboutir à des conclusions correctes et objectives. Enfin, il incombe aux entreprises de se doter des systèmes de contrôle nécessaires pour garantir que les données en leur possession ne tombent pas entre de mauvaises mains.

NOUVEAUTÉS
DANS LA GESTION DES IDENTITÉS EXTERNES

Microsoft, il y a peu, a complété l'environnement Azure, Office 365 pour faciliter la gestion des environnements multi Tenants. Certaines applications comme le nouveau client Teams, profitent, par ailleurs, de ces nouveautés. Petit tour d'horizon rapide pour bien comprendre.

Comme vous le savez sûrement, un Tenant est un ensemble relativement fermé, axé principalement autour d'un annuaire Azure AD unique et des fonctionnalités comme Microsoft Exchange Online, SharePoint Online etc. Un Azure AD gère et authentifie un ou plusieurs domaines d'authentification. Au sein de ce Tenant, les utilisateurs peuvent interagir avec la même expérience utilisateur.

Dès lors qu'une entreprise fusionne ou acquiert une autre entreprise, se pose la question soit de conserver les deux Tenants soit de fusionner ces derniers. De ce fait, plusieurs entreprises, à ce jour, doivent gérer volontairement ou involontairement plusieurs Tenants Microsoft, tout en permettant aux utilisateurs de pouvoir échanger, et communiquer avec une expérience similaire.

Par ailleurs, ces mêmes entreprises, doivent pouvoir partager en toute sécurité, des données avec des membres d'autres sociétés utilisant M365, voire parfois avec des utilisateurs n'ayant pas de licence M365 (gmail.com, Yahoo.com etc.)

Rappelons que sans paramétrage particulier entre deux Tenants et pour permettre aux utilisateurs de partager des documents il vous faudra créer des comptes invités de part et d'autre et maintenir manuellement la cohérence de ces deux annuaires.

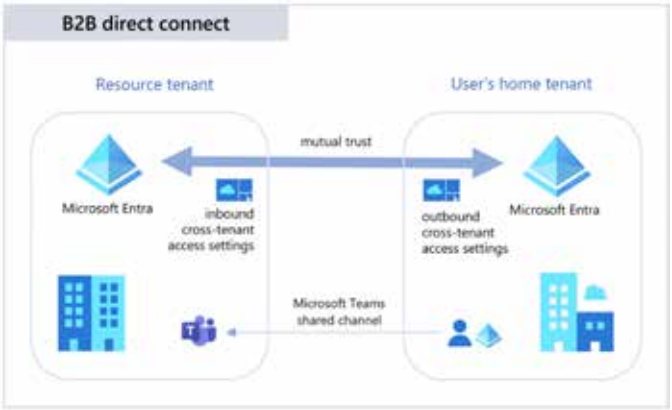
Rassurez-vous, il y a plus simple.

Pour cela, et pour répondre à ces besoins croissants, Microsoft offre à ce jour quatre modes d'organisation au regard des différents cas de figure qui peuvent se présenter.

- B2B direct connect
- B2B collaboration
- Cross-Tenant synchronization
- Multi Tenants Organization

B2B direct connect

Le mode de connexion B2B direct connect va permettre d'établir une relation de confiance limitée à deux Tenants comme le montre la figure issue de la documentation Microsoft.



Grace à ce paramétrage, il vous sera possible d'activer dans Microsoft Teams des canaux partagés. Les utilisateurs, de part et d'autre, pourront alors partager des données en utilisant leurs identifiants personnels. Chaque entreprise pourra, dans cette relation de confiance, choisir, si elle accorde ou pas, l'accès à certaines applications pour les personnes provenant de l'autre Tenant.

Les utilisateurs invités se connectent alors à vos applications et services avec leur identité professionnelle, scolaire ou sociale.

Autre avantage, il est possible d'inclure, soit la totalité de vos utilisateurs dans cette relation de confiance, soit de la limiter à une partie de votre population.

Une solution pratique mais limitée à deux Tenants.

B2B collaboration

La seconde solution permet d'inviter des utilisateurs externes en leur créant des comptes invités dans votre annuaire Entra ID. Les utilisateurs invités se connectent alors à vos applications et services avec leur identité professionnelle, scolaire ou sociale.

La personne invitée utilisera, par conséquent, ses propres identités et identifiants, qu'elle ait ou non un compte sur votre environnement Entra.

La figure suivante illustre ce mode de collaboration

C'est une solution très pratique qui devrait selon moi être encadrée, mais qui permet à des personnes externes voire des particuliers d'accéder à une partie de vos informations. Si vous mettez en place cette solution et si vous permettez à vos utilisateurs, d'inviter des personnes externes, je ne saurais trop vous conseiller d'activer la revue des accès.

Dans le cas contraire, vous risquez de vous retrouver au bout de quelques mois avec plusieurs centaines voire milliers de comptes externes qui resteront ad vitam aeternam au sein de votre annuaire.

Comme pour la solution **B2B direct connect**, vous pourrez limiter l'accès à certaines applications et certaines ressources.

Synchronisation entre Tenants

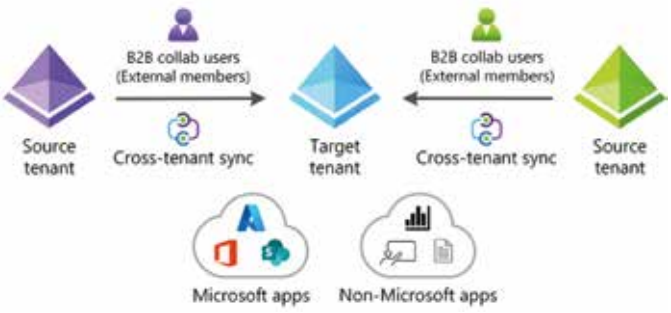
La synchronisation entre Tenants permet d'échanger tout ou partie de son annuaire vers un autre

Tenant. Le principal avantage de cette solution est qu'elle offre un service de synchronisation à sens unique qui automatise la création, la mise à jour et la suppression des utilisateurs entre les Tenants concernés. On notera que cette solution ne synchronise pas les groupes, les périphériques et les contacts.

Les utilisateurs concernés par cette solution verront leurs expériences légèrement améliorées, car ils n'auront pas la nécessité de recevoir de message d'invitation et d'accepter une demande de consentement.

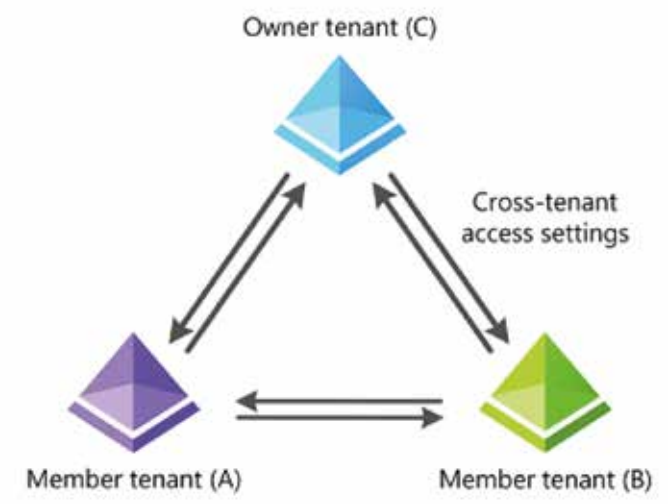
Malheureusement, cette solution, si elle simplifie la gestion des identités, n'améliore pas les expériences Teams ou Microsoft 365 actuelles.

La figure suivante illustre la mise en place de cette solution



L'organisation Multi Tenants

L'organisation Multi Tenants permet de mettre en place un meilleur niveau d'intégration avec un maximum de 5 Tenants et 100 000 utilisateurs. Cela va permettre de différencier les utilisateurs externes appartenant à l'organisation de ceux qui n'en font pas partie. La figure suivante illustre ce mode d'organisation.



Les utilisateurs d'un Tenant n'apparaissent plus en tant qu'invités mais en tant que membres du Tenant cible auquel ils peuvent accéder. De plus, le nouveau client Teams Desktop permet aux utilisateurs de plus facilement travailler avec plusieurs univers (Tenant).

Ainsi, ces derniers pourront fixer leur statut de présence dans chaque environnement et seront prévenus lorsqu'on cherche à les joindre depuis un Tenant « étranger ». Ils pourront, tout en étant connectés à leur Tenant, répondre à des conversations initiées depuis un autre Tenant sans pour cela basculer de compte.

Les entreprises qui souhaitent rationaliser la collaboration entre différentes entités, auront donc tout intérêt à retenir ce nouveau mode de collaboration.

Ces quatre modes ne sont pas complètement exclusifs ce qui permet de définir comment votre entreprise ou votre groupe souhaite collaborer avec des entités parfois externes ou au contraire, proches de votre écosystème.

Autrement dit, ce n'est pas parce que vous choisissez une organisation multi Tenants avec vos partenaires proches ou filiales que vous vous interdisez de faire un partage B2B direct Connect avec des utilisateurs isolés. L'un n'empêche pas l'autre bien au contraire. C'est l'intérêt de ces quatre modes de fonctionnement.

Ne pas adresser ce sujet serait une erreur car les utilisateurs trouveront toujours le moyen de collaborer.

Mettre en place ces solutions vous imposera vraisemblablement de définir des niveaux de proximité et de confiance vis-à-vis des entités avec lesquelles vos utilisateurs travaillent étroitement. En s'accordant sur le niveau de sécurité minimal que vous et vos partenaires devez respecter dans une organisation multi-Tenants, vous élaborerez ainsi votre premier cercle de proximité et faciliterez la collaboration de vos utilisateurs.

Ne pas adresser ce sujet serait une erreur car les utilisateurs trouveront toujours le moyen de collaborer.

Aussi, je pense sincèrement qu'il est préférable de collaborer sur des documents de façon sécurisée à travers les quatre modes présentés ci-dessus plutôt que de s'envoyer par messagerie des documents qui n'ont pas à transiter en clair sur internet.

Bonne configuration !

> Laurent Teruin | https://unifiedit.wordpress.com/MVP

Infortive PRÔNE UN DSI DE TRANSITION PRÊT À AFFRONTER TOUTES LES SITUATIONS CRITIQUES

Infortive Transition, cabinet expert du Management de Transition IT, propose aux organisations des managers de transition pour accélérer la transformation digitale mais aussi pour mener des projets de transformation ou encore gérer des crises. Pour cela, il s'appuie sur sa large communauté de DSI/CTO de transition.

Trois questions à Pierre Fauquenot, cofondateur et CEO d'Infortive Transition, pour en savoir sur ce pure player.

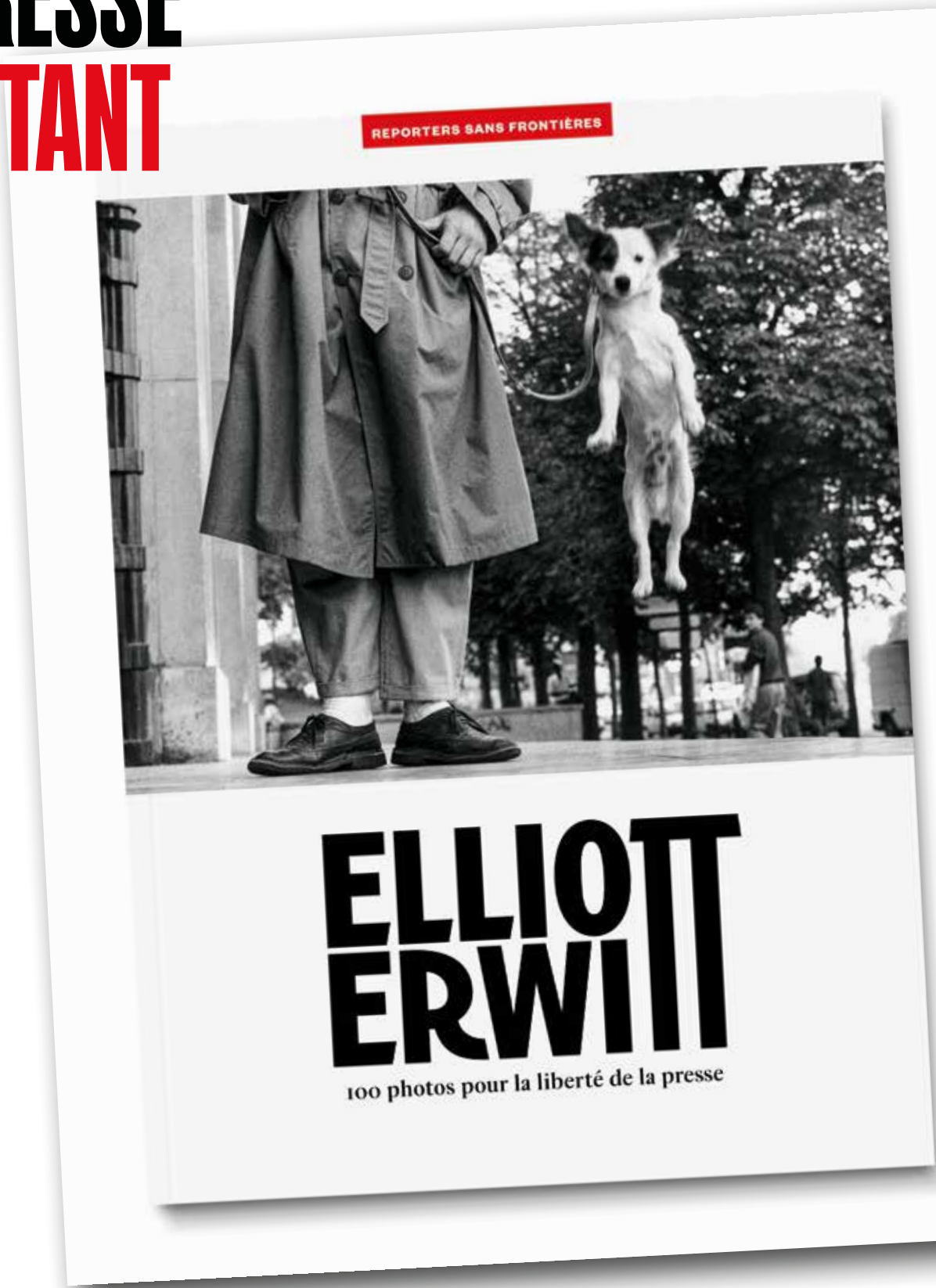
Pourquoi avoir créé Infortive ? Qu'est-ce qui vous différencie ?

J'ai toujours utilisé l'informatique pour améliorer la performance des organisations ou leur créer des avantages concurrentiels. Après avoir été DG, je me suis positionné en 2002 comme DSI de transition car j'étais un geek qui venait des Métiers, ce qui me permettait d'être différent de mes confrères !

J'ai fait partie des pionniers du management de transition en France et je suis resté 16 ans DSI de transition avec une vingtaine de missions de DSI dans des entreprises de toutes tailles, en France et à l'étranger. Je suis un homme de terrain qui a eu à réparer de nombreuses DSI.

Mon expérience de DSI et de manager de transition s'est construite en mission, mais également au

SOUTENEZ LA LIBERTÉ DE LA PRESSE EN ACHETANT NOTRE ALBUM 12,50 €



RSF
REPORTERS
SANS FRONTIÈRES

travers d'une association de management de transition où mes pairs me partageaient leurs bonnes pratiques en mission.

J'ai souvent constaté le décalage entre la DSI et des Métiers en perpétuelle évolution et aux besoins digitaux croissants.

En 2019, avec **Hervé Bébin**, nous avons créé Infortive qui est une communauté de DSI de transition et également une entreprise de management de transition spécialisée sur l'IT et le Digital.

Nous avons mesuré à quel point la prise de brief dans le domaine technologique est déterminante pour définir le profil adéquat et sélectionner le candidat idéal qui saura mener à bien la mission de transition proposée.

Ce qui nous différencie, c'est une compréhension du secteur de l'IT très élevée par rapport à nos confrères généralistes. Nous animons une communauté de DSI de transition, nous avons créé ensemble la formation "CIO Executive Certificate", une formation pour des DSI par des DSI, que nous avons lancée l'année dernière avec CentraleSupélec Exed et nous nous sommes lancés dans la chasse de tête. C'est tout cet écosystème autour de l'IT qui nous permet de rester au meilleur niveau.

Si on devait retenir quelques points clés de la méthodologie Infortive, quels seraient-ils ?

Notre méthodologie est celle du management de transition avec une spécificité IT. Le fil conducteur du management de transition **c'est arriver, transformer, partir**.

- Dans un premier temps, nous écoutons et creusons le besoin du client. La prise de brief est déterminante. Nous apportons notre expérience du terrain en miroir aux attentes exprimées pour définir les compétences et aptitudes des personnes qui pourront amener le client là où il le souhaite. Ces managers de transition sont des DSI surexperimentés, ils seront donc tout de suite opérationnels. Nous accompagnons le manager de transition tout au long de sa mission.

- À son arrivée, le DSI de transition procède à une analyse approfondie pour comprendre les défis et les opportunités uniques de l'organisation.

- Il met en œuvre des stratégies de transformation adaptées, visant à optimiser les processus, renforcer les équipes et stimuler l'innovation.

- Enfin, le départ est planifié pour assurer une transition durable, laissant l'entreprise dans une position de force et prête pour l'avenir.

PIERRE FAUQUENOT

Pour vous, quels sont les atouts d'un Manager de Transition ?

Pour assurer le succès d'une mission de management de transition en IT, le DSI doit posséder un large éventail de compétences techniques et managériales.

Il doit être capable de proposer une **stratégie claire, alignée sur les objectifs de l'entreprise**, en comprenant parfaitement ses besoins et en collaborant avec toutes les parties prenantes.

Il doit avoir une **capacité à aborder à 360 les aspects techniques** : la maîtrise des technologies de l'information, la gestion de projet, la cybersécurité, la gestion des données et bien d'autres compétences techniques sont indispensables.

Le DSI de transition apporte une expertise avérée, une indépendance et une rapidité d'action

Il est avant tout **un manager** ! En tant que leader, le DSI de transition doit motiver et guider les équipes, tout en gérant efficacement le changement. Il doit surmonter les résistances pour mener à bien les transformations nécessaires.

Le management de transition pour la DSI est une solution efficace pour faire face aux situations critiques ou de transformation de l'entreprise. Le DSI de transition apporte une expertise avérée, une indépendance et une rapidité d'action qui permettent la sécurisation de projets IT et renforcent sa crédibilité auprès des Métiers.

> Par Sabine Terrey

ENTREPRISE ET CYBERSÉCURITÉ

CYBER-SÉRÉNISEZ VOTRE ACTIVITÉ

À l'ère de la transformation numérique et à l'heure des questions de souveraineté numérique, **cyber-séréniser vos activités devient vital face aux impacts financiers des cyberattaques.**

Protection des réseaux, des données, des postes et serveurs ; choisir les solutions Stormshield, c'est faire appel à un acteur de cybersécurité de confiance.

STORMSHIELD

www.stormshield.com

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