Business Tech, Réseaux, Cybersécurité et Tendances en matière de réduction des coûts Royaume-Uni 2023

Recherché et compilé par

David Montero – Global Head of Channel

Javier Pérez – Responsable de la recherche et des connaissances

Plus de 64 sources indépendantes se sont réunies pour créer le

L'externalisation, aux niveaux stratosphériques

www.sdwan-solutions.global

L'externalisation pour la gestion, le support et la formation technologiques devrait exploser en 2023

Les pénuries de compétences et la réduction des coûts sont à l'origine de la mégatendance les entreprises utilisatrices, qui cherchent à externaliser une grande partie de leur fourniture de technologie via des MSP. Cela réduit leur besoin des équipes internes et les coûts qui y sont associés, ainsi que d'annuler le besoin d'expertise spécifique. Faire des MSP une « partie étendue de l'équipe interne informatique » devrait apporter une formation « gratuite » pour une amélioration continue des compétences. Jours heureux!

Partenariats stratégiques MSP pour les compétences, le soutien et la réduction des coûts

Au sein du secteur des services informatiques, les activités de distribution et les revendeurs arrivent à la même réalisation que les clients finaux. Alors que la croissance exponentielle de l'innovation technologique entraîne encore plus de changements, les acteurs du secteur sous-traitent aux MSP pour les mêmes raisons. Ce conseil est en fait maintenant stipulé par des gouvernements et les agences de sécurité nationale et les conseillers en cybersécurité.

Le GCHQ conseille aux entreprises de se protéger de la cybercriminalité via les MSP

Le Centre national de cybersécurité a publié le « Joint Cyber Security Advisory (Alert AA22-131A) », dans lequel il conseille fortement aux entreprises de toutes sortes, dans de nombreux secteurs industriels, d'utiliser un MSP.

Toute entreprise dont les opérations se déroulent en ligne doit utiliser l'expertise des MSP pour le cloud, la cybersécurité et la connectivité sûre. Les clients professionnels des MSP devraient « demander des comptes à ces MSP », car il s'agit de leur domaine d'expertise. Nous sommes tout à fait d'accord!

www.sdwan-solutions.global

La méga-tendance de l'externalisation
FACT FILE

- 1,3 billion de dollars dépensé en 2023
- Augmentation de 519 milliards de dollars des dépenses d'externalisation en 2023
- Augmentation de 22 % en glissement annuel jusqu'en 2025
- 88 % des entreprises utilisent les MSP pour réduire leurs coûts
- 78 % utilisent les MSP pour standardiser l'ensemble de leur entreprise
- 63 % utilisent les MSP pour ajouter de la valeur à leur entreprise
- Cyberprotection, Cloud et Multi-Cloud et solutions de connectivité nouvelle génération principales externalisation informatique

Nous vous conseillons de vérifier:

www.ncsc.gov.uk/blog-post/using-msps-to-administer-your-cloud-services
www.ncsc.gov.uk/collection/cloud/the-cloud-security-principles

www.sdwan-solutions.global

“Nous prévoyons que les projets de conseil en cybersécurité et en technologie vaudront 1,5 billion de dollars au cours des 3 prochaines années jusqu'en 2027.”

Tech Project Partnerships 2023, McKinsey

“Certaines organisations font appel à un MSP ou à un revendeur pour effectuer des tâches spécifiques, telles que la fourniture de licences, la sécurité d'exploitation ou de centres de données, ou le provisionnement de nouvelles instances cloud. D'autres y vont « à fond » et externalisent la fourniture, la conception et l'exploitation de leurs applications métier (que ce soit en tant que SaaS partagé, tout déploiement individuel hébergé sur une structure cloud d'une manière ou d'une autre). Il y a des avantages évidents à faire cela, surtout si vous n'avez pas le personnel adéquat. Ce faisant, vous bénéficiez de l'expertise, de l'efficacité et de l'expérience de ces autres entreprises.”

Centre national de cybersécurité

www.sdwan-solutions.global

Réduction des coûts et de la complexité

www.sdwan-solutions.global

CONSOLIDATION - Faire plus avec moins

Loin de la récession actuelle entraînant de simples initiatives de réduction des coûts, les chefs d'entreprise demandent aux chefs de service de voir où des réductions intelligentes, à la fois en complexité et en coût, peuvent être initiées. La consolidation des technologies, des réseaux et de la sécurité jouera un rôle essentiel dans la réduction des coûts et de la complexité. Les entreprises prennent des vues approfondies sur la façon dont elles peuvent faire plus avec moins, ce qu'elles peuvent abandonner et ce qu'elles doivent garder, réduisant simultanément les coûts et la complexité. Cela peut sembler un croisement entre une évidence et un rêve utopique, mais il s'agit en fait d'une méga-tendance 2023, et elle commence d'abord dans un service informatique près de chez vous.!

Oubliez la gestion de crise... Évitement de crise le nouveau terme à la mode

La complexité de la vie moderne implique d'être prêt à tout et de veiller à ce que votre activité se poursuive normalement. Le besoin de solutions pour le travail a domicile n'a pas complètement disparu – la façon de résoudre le problème est devenue plus intelligente. Au lieu d'avoir une solution par problème, une solution métier critique globale doit résoudre tous les problèmes.

Bienvenue à Crisis Avoidance – rester calme et connecté est le mantra ici. Les entreprises cherchent à fournir des solutions de connectivité et de sécurité expertes qui tiennent à distance toutes les mauvaises nouvelles (alimentant davantage les tendances en matière d'externalisation et de MSP). Un réseau sécurisé n'importe où, une solution toujours active que les équipes soient en déplacement ou au bureau, qu'il y ait une pandémie, une grève, une crise énergétique, perturbation de la chaîne d'approvisionnement ou un Phénomène météorologique à l'horizon – Restez calme et connecté !

www.sdwan-solutions.global

La méga-tendance de l'externalisation
FACT FILE

- 52% des chefs d'entreprise s'attendent à ce que les budgets technologiques augmentent en 2023
- SEULEMENT 1 sur 7 pense que son budget informatique sera réduit
- Pour 3e année consécutive la technologie est considérée comme « le grand facilitateur »
- 80 % des entreprises pensent que l'innovation informatique les rendra plus productives
- 86% pensent que des investissements informatiques en 2023 aideront à réduire coûts au cours des 2 prochaines années
- Les dépenses de cyberprotection dépasseront tous les autres domaines

www.sdwan-solutions.global

« La récession émergente affectera moins l'investissement qu'une récession traditionnelle. Cela s'explique en partie par les retards, et en partie aussi par le fait que nous vivons dans un environnement où les grandes entreprises cherchent des technologies permettant d'économiser de la main-d'œuvre parce que les pénuries de main-d'œuvre auxquelles nous sommes confrontés ne sont pas cycliques »

Diane Swonk - Économiste en chef KPMG

au CNBC CFO Council Summit novembre 2022

« Les mauvaises nouvelles économiques s'accumulent et les indicateurs deviennent négatifs, mais malgré ou même à cause de cela, les entreprises savent que l'investissement dans la technologie reste crucial. À la fois pour maximiser l'efficacité de ce qu'ils ont déjà et pour devenir plus agiles et réactifs dans des conditions hautement imprévisibles, la technologie est le catalyseur clé »

Bev White, CEO of Nash Squared

Ne faites confiance à personne!
ZTNA : le réseau de choix

www.sdwan-solutions.global

Les menaces sont-elles à l'intérieur ?

60% des violations de données sont causées par des menaces internes, dont 67% sont causées par le phishing.

Actuellement, de telles attaques coûtent 11,5 millions de dollars par an a une grande entreprise (jusqu'à fin 2022). Bien qu'il soit reconnu que les attaques internes sont très rarement des actes malveillants, il s'agit plus probablement d'un manque de connaissances et de formation.

ZTNA plus rentable et fiable que la formation

Avec plus de 300 000 nouveaux logiciels malveillants lancés quotidiennement et des cyberattaques passant d'UN toutes les 11 secondes en 2022 à UN attaque toutes les 7 SECONDES d'ici la fin de 2023, les entreprises ont reconnu qu'il était pratiquement impossible de former le personnel à toutes les attaques possibles. Au lieu de cela, ZTNA est de plus en plus utilisé pour automatiser les protocoles, processus et procédures de sécurité.

Zero Trust Network Access
FACT FILE

- 90% d'économies sur le coût d'un cyberattaque, créés par ZTNA
- Le marché ZTNA vaut actuellement 819 millions de dollars
- Sera de 27,1 milliards de dollars d'ici la fin de 2023
- Et de 60,7 milliards de dollars d'ici la fin de 2027
- Croissance du TCAC de 36,6 % tout au long de 2023
- TCAC de 27,7 % en glissement annuel jusqu'en 2027
- 19 % des organisations ont investi dans la formation du personnel après la violation la plus perturbatrice
- Seulement 9 % des organisations ont installé, modifié ou mis à jour un logiciel antivirus ou anti-malware en 2023

“Pour les entreprises avant-gardistes ayant des besoins de sécurité complexes, la mise en œuvre de ZTNA est un outil essentiel non négociable pour la confidentialité des données et le contrôle global du réseau.”

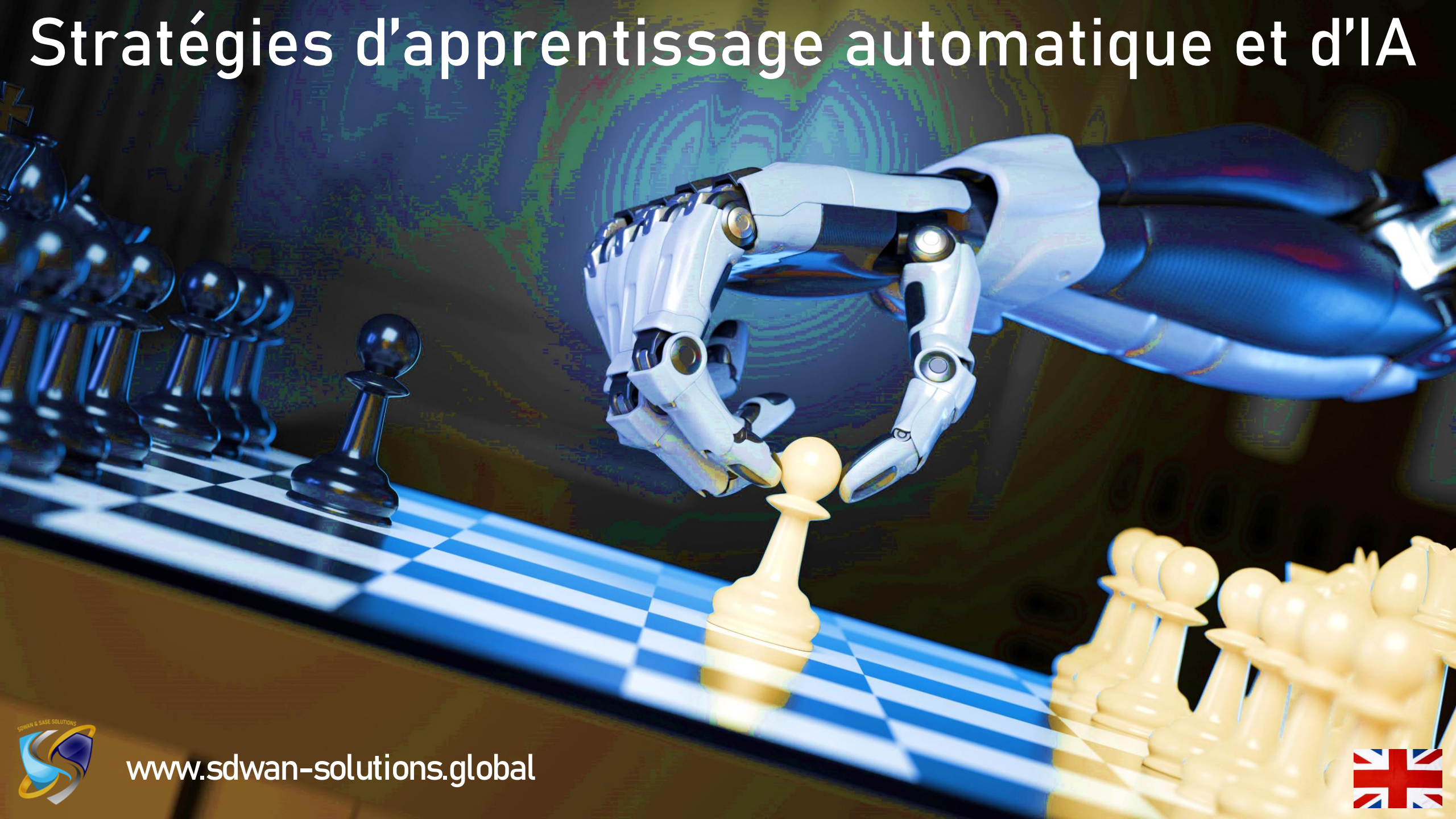
CONSEIL DE LA TECHNOLOGIE FORBES

“ D’ici 2025, 70% des nouveaux déploiements d’accès à distance seront principalement desservis par ZTNA, par opposition aux VPN. Il s’agit d’une augmentation énorme, contre moins de 10% à la fin de 2021 »

GARTNER

www.sdwan-solutions.global

Stratégies d'apprentissage automatique et d'IA



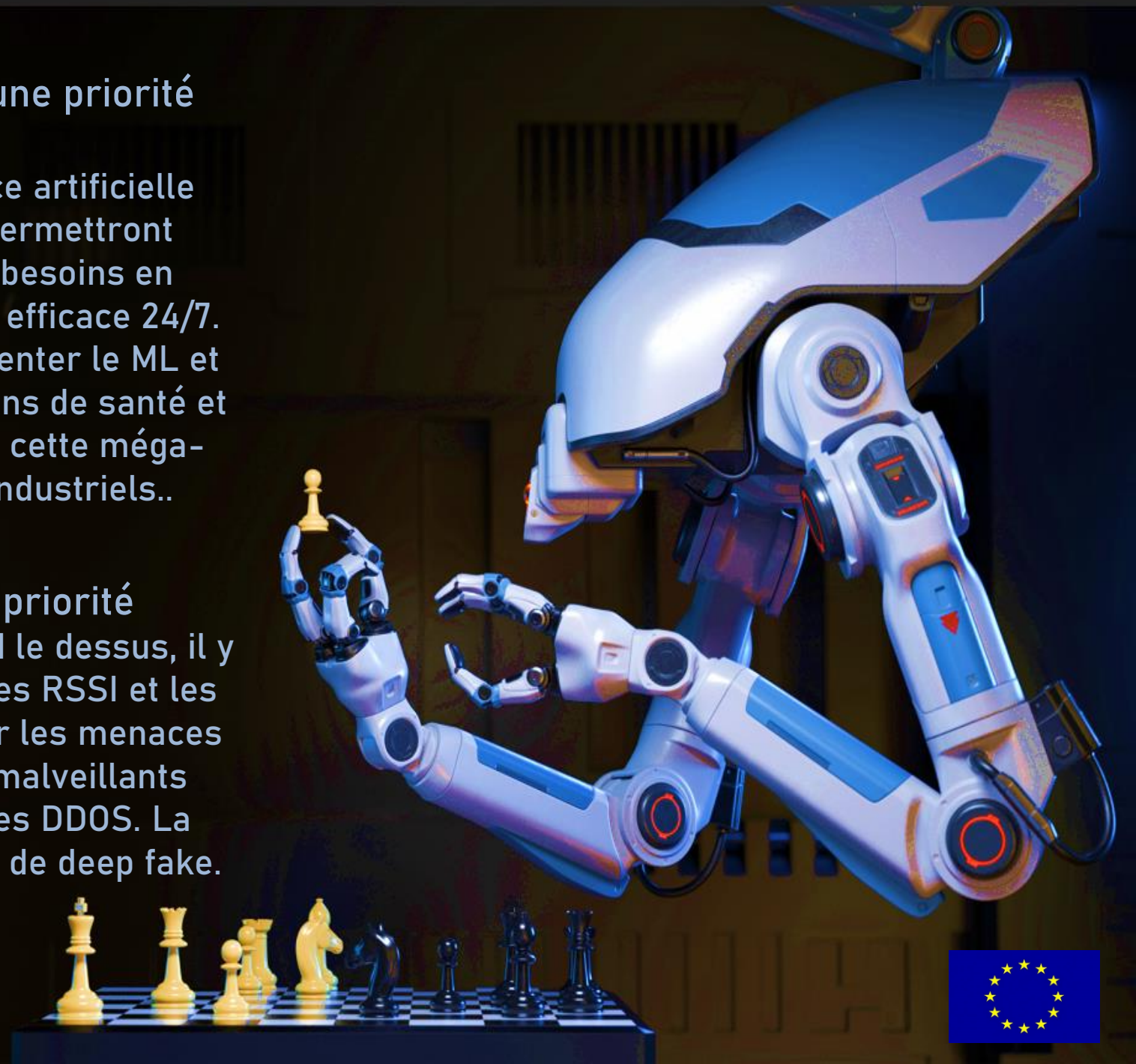
www.sdwan-solutions.global

4 entreprises sur 5 disent que l'IA est une priorité absolue

L'apprentissage automatique et l'intelligence artificielle combleront le déficit de compétences et permettront d'économiser de l'argent en réduisant les besoins en personnel, avec un fonctionnement vraiment efficace 24/7. Les domaines en 2023 qui cherchent à augmenter le ML et l'IA sont la fabrication, la comptabilité, les soins de santé et la logistique, mais il est prudent de dire que cette méga-tendance couvre la plupart des secteurs industriels..

Sécuriser le ML et l'IA la prochaine priorité

Au fur et à mesure que l'automatisation prend le dessus, il y a, bien sûr, un paysage de menaces accru. Les RSSI et les services informatiques chercheront à contrer les menaces persistantes avancées (APT), les logiciels malveillants alimentés par l'IA, le phishing et les attaques DDOS. La nouveauté pour 2023 sera aussi les attaques de deep fake.



www.sdwan-solutions.global

Le Machine Learning et l'iA
FACT FILE

- 51,2 milliards de dollars dépensés en 2022
- 70,9 milliards de dollars dépensés en 2023
- 94,4 milliards de dollars dépensés en 2024
- 126,1 milliards de dollars dépensés en 2025
- Croissance du marché de 38% prévue pour 2023
- 83% des entreprises déployeront le ML & Ai en 2023
- Augmentation de 40 % de la productivité grâce au ML et à l'IA

“Seulement 11 % des PME ont entièrement mis en œuvre une solution de sécurité IoT, et 52 % n’ont déployé aucune sécurité IoT.”

CheckPoint Software Technologies Ltd.

“La nouvelle loi de l’Union européenne sur la cyber-résilience vise à garantir que les fabricants d’appareils IoT intègrent des systèmes de sécurité avancés tout au long du cycle de vie des appareils IoT et empêchent ainsi ces dispositifs d’être la passerelle pour les cybercriminels. On estime que les dépenses consacrées à la cybercriminalité s’élèveront à 5,5 billons d’euros en 2031.”

Commission Européenne

www.sdwan-solutions.global

L'IoT conquiert le monde

www.sdwan-solutions.global

L'IoT domine véritablement le monde

L'IoT se généralisera en 2023 dans les domaines de soins (s'atteindra 267 milliards de dollars en 2027). Ce ne sont pas seulement les dispositifs portables et de surveillance qui sont à l'origine de ces tendances, mais aussi le besoin de « salles virtuelles » pendant le rétablissement et les consultations initiales en ligne. Le numérique et le métavers pour l'entreprise stimuleront également l'adoption de l'IoT en 2023.

Mais il est impératif de considérer que les appareils IoT sont piratables dans les secondes qui suivent leur mise en ligne..

Les chiffres de l'IoT ne font que croître et croître

Les statistiques varient considérablement en ce qui concerne l'IoT. Ce qu'ils ont tous en commun, c'est que 98% d'entre eux ne sont actuellement pas sécurisés. Certains appareils associés à l'entreprise utilisent encore des cartes SIM grand public. Ce qui est déprimant pour nous, c'est que ces faits et chiffres restent les mêmes que dans le rapport de l'année dernière. Nous avons compilé un énorme fichier d'information ici, alors lisez la suite pour plus d'informations

L'IoT conquiert le monde
FACT FILE

- 43 MILLIARDS d'appareils connectés à Internet 2023
- 14,4 MILLIARDS d'appareils IoT pour les entreprises 2023
- Croissance de 18 % des appareils IoT en 2023
- 75 MILLIARDS d'appareils dans le monde d'ici 2025
- 594 milliards de dollars valeur de marché en 2022
- 1.1 billion valeur de marché en 2023
- 6 milliards de dollars pour sécuriser l'IoT 2023 aux États-Unis

www.sdwan-solutions.global

« Comme les entreprises qui ont ignoré l'Internet au tournant du siècle, celles qui rejettent l'IoT risquent d'être laissées pour compte. »

Jared Newman Journaliste technique

Cité par Forbes Technology Council

« Les entreprises commencent à voir le potentiel des appareils IoT. Selon Gigabit, les entreprises pourraient investir jusqu'à 15 billions de dollars dans l'IoT d'ici 2025 et ajouter de la valeur à leurs activités. Les statistiques sur l'IoT montrent que plusieurs prestataires de soins de santé, fabricants et municipalités ont déjà choisi d'investir dans la technologie IoT.

PwC

SD-WAN et SASE 2023

Comment SD-WAN et SASE de SDWAN Solutions posibilitent les tendances 2023

www.sdwan-solutions.global

SASE est généralisé
Forbes Technology Council

Les principaux commentateurs informatiques du Forbes Technology Council affirment que « 2023 sera l'année où SASE décollera vraiment ». Nous sommes d'accord. Les prévisions sont que le marché mondial SASE vaudra 15 milliards de dollars en 2025, ce qui représente un TCAC de 116% par an. D'ici la fin de 2023, 40% de TOUTES les entreprises auront mis en place une stratégie d'adoption de la SASE.

La démocratisation de SASE via des solutions abordables pour les PME

2022 a été l'année où SASE s'est généralisé pour de nombreuses entreprises, mais 2023 sera l'année où les fournisseurs et les fournisseurs de SASE (MSP) créeront des solutions SASE abordables pour les petites et moyennes entreprises. Au sein de cette taille d'organisation, de nombreuses organisations du secteur privé peuvent être trouvées, telles que des organisations caritatives, des organismes sans but lucratif et même des prestataires d'éducation et de santé – Nous pouvons tous convenir que ces organisations ont besoin de SASE pour protéger nos données, nos enfants et notre bien-être collectif.

L'adoption de SASE stimule l'adoption du SD-WAN – MAIS rappelez-vous, il n'y a pas de SASE sans SD-WAN

De nombreuses entreprises ont déjà reconnu et capitalisé sur les avantages de productivité d'un réseau intelligent toujours actif comme le SD-WAN, mais il est important de dire que l'hypothèse selon laquelle SASE remplace en quelque sorte le SD-WAN n'est pas du tout correcte, en fait, il n'y a pas de SASE sans SD-WAN. En 2023, les consultants en informatique travailleront avec les MSP pour faire passer ce message, mettre en œuvre le SD-WAN en douceur afin que SASE puisse suivre en douceur.

SD-WAN
FACT FILE

- Taille du marché SD-WAN de 4 milliards USD en 2022
- TCAC de croissance estimé de 65 % pour 2023-2032
- Valeur de 66,5 milliards USD du marché SD-WAN d'ici 2032
- 50 % des achats SD-WAN feront partie de l'offre SASE d'un seul fournisseur
- Augmentation de 10% sur le SD-WAN et le point SASE au-dessus d'ici 2025
- 63 % des entreprises déploient déjà le SD-WAN
- 87 % des PME cherchent à trouver des MSP pour la fourniture de SD-WAN et SASE
- 86 % de toutes les tailles cherchent à réduire la complexité de la fourniture SD-WAN et SASE

MAIS souhaitent conserver différents fournisseurs pour ces technologies

www.sdwan-solutions.global

SASE

FACT FILE

- 94% des répondants déclarent que leur adoption des solutions SASE s'est accélérée cette année
- 52 % grâce à la sécurité du Cloud, y compris la visibilité et le contrôle dans les environnements Cloud
- 44 % sont motivés par l'innovation, y compris la migration d'applications cloud et l'intelligence artificielle
- 41 % motivés par la stratégie de sécurité, y compris la mise en œuvre du Zero Trust (ZTNA)
- 13 MILLIARDS USD – la taille du marché SASE dépassera ce chiffre d'ici 2026
- Augmentation de 100% d'une année sur l'autre de la mise en œuvre de SASE jusqu'en 2025
- 98 % pensent que la convergence du réseau et de la sécurité est essentielle ou très importante

Il existe plus de 70 fournisseurs de SD-WAN et chacun de leurs produits diffère en termes de fonctionnalités. Personne ne s'attend à ce qu'un responsable ou un directeur informatique soit un expert dans toutes les technologies SD-WAN, c'est à cela que servent les fournisseurs de services professionels spécialisés comme SDWAN et SASE Solutions, pour conseiller sur les technologies et les solutions qui conviennent le mieux, pour s'assurer que chaque entreprise obtient la bonne solution pour ses besoins.

Anthony Senter PDG de SDWAN et SASE Solutions

Tout comme il existe de nombreuses technologies SD-WAN, il existe également de nombreux revendeurs SD-WAN : les services informatiques doivent vérifier méticuleusement les accréditations et les références SD-WAN et SASE du revendeur, car trop sont des pseudo-experts sans fondement réel, ce qui conduit à des projets ratés, à de faibles profits et à des dépenses imprévues.

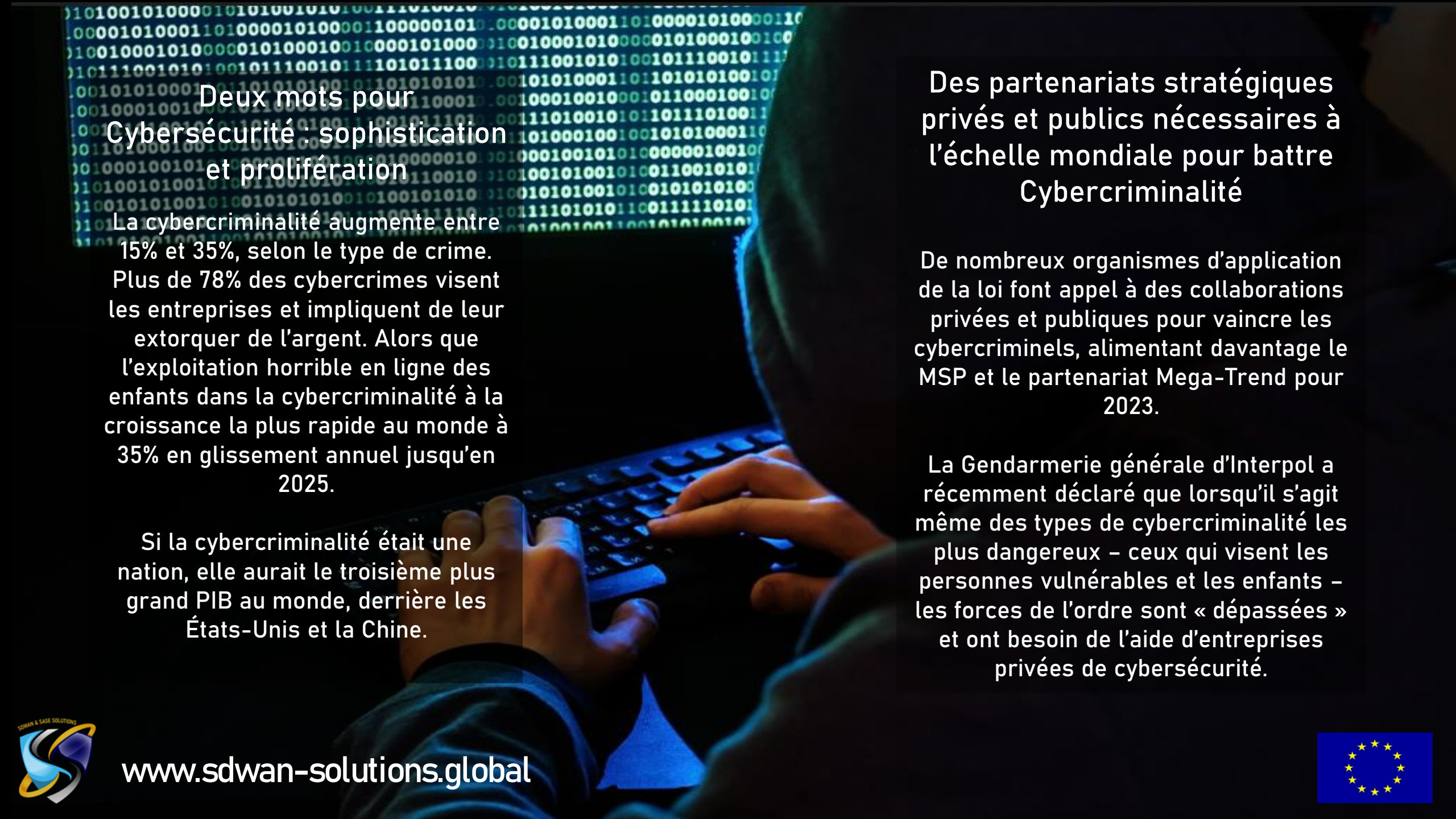
Toby Sturridge CTO de SDWAN y SASE Solutions

www.sdwan-solutions.global

SDWAN et SASE Solutions

Cyber-Crime Fact File 2023

www.sdwan-solutions.global



Deux mots pour Cybersécurité : sophistication et prolifération

La cybercriminalité augmente entre 15% et 35%, selon le type de crime. Plus de 78% des cybercrimes visent les entreprises et impliquent de leur extorquer de l'argent. Alors que l'exploitation horrible en ligne des enfants dans la cybercriminalité à la croissance la plus rapide au monde à 35% en glissement annuel jusqu'en 2025.

Si la cybercriminalité était une nation, elle aurait le troisième plus grand PIB au monde, derrière les États-Unis et la Chine.

Des partenariats stratégiques privés et publics nécessaires à l'échelle mondiale pour battre Cybercriminalité

De nombreux organismes d'application de la loi font appel à des collaborations privées et publiques pour vaincre les cybercriminels, alimentant davantage le MSP et le partenariat Mega-Trend pour 2023.

La Gendarmerie générale d'Interpol a récemment déclaré que lorsqu'il s'agit même des types de cybercriminalité les plus dangereux – ceux qui visent les personnes vulnérables et les enfants – les forces de l'ordre sont « dépassées » et ont besoin de l'aide d'entreprises privées de cybersécurité.

www.sdwan-solutions.global

Croissance de la cybercriminalité - Fact File

Dommages et coûts à l'échelle mondiale

10,5 BILLIONS DE DOLLARS DE CYBERCRIMINALITÉ MONDIALE (INTERPOL)
6,1 billions de dollars de dommages causés par les cybercriminels 2023
SEULEMENT 500 $ par petite entreprise sont dépensés pour la cybersécurité
60% des petites entreprises ne survivent pas au-delà de 6 mois après l'attaque

Violations de données et grandes marques

13 millions de dollars de dommages causés par des violations de données
3 MILLIARDS de comptes d'utilisateurs Yahoo piratés
600 MILLIONS de comptes Facebook se sont fait voler leurs données après une violation de données

Croissance mondiale

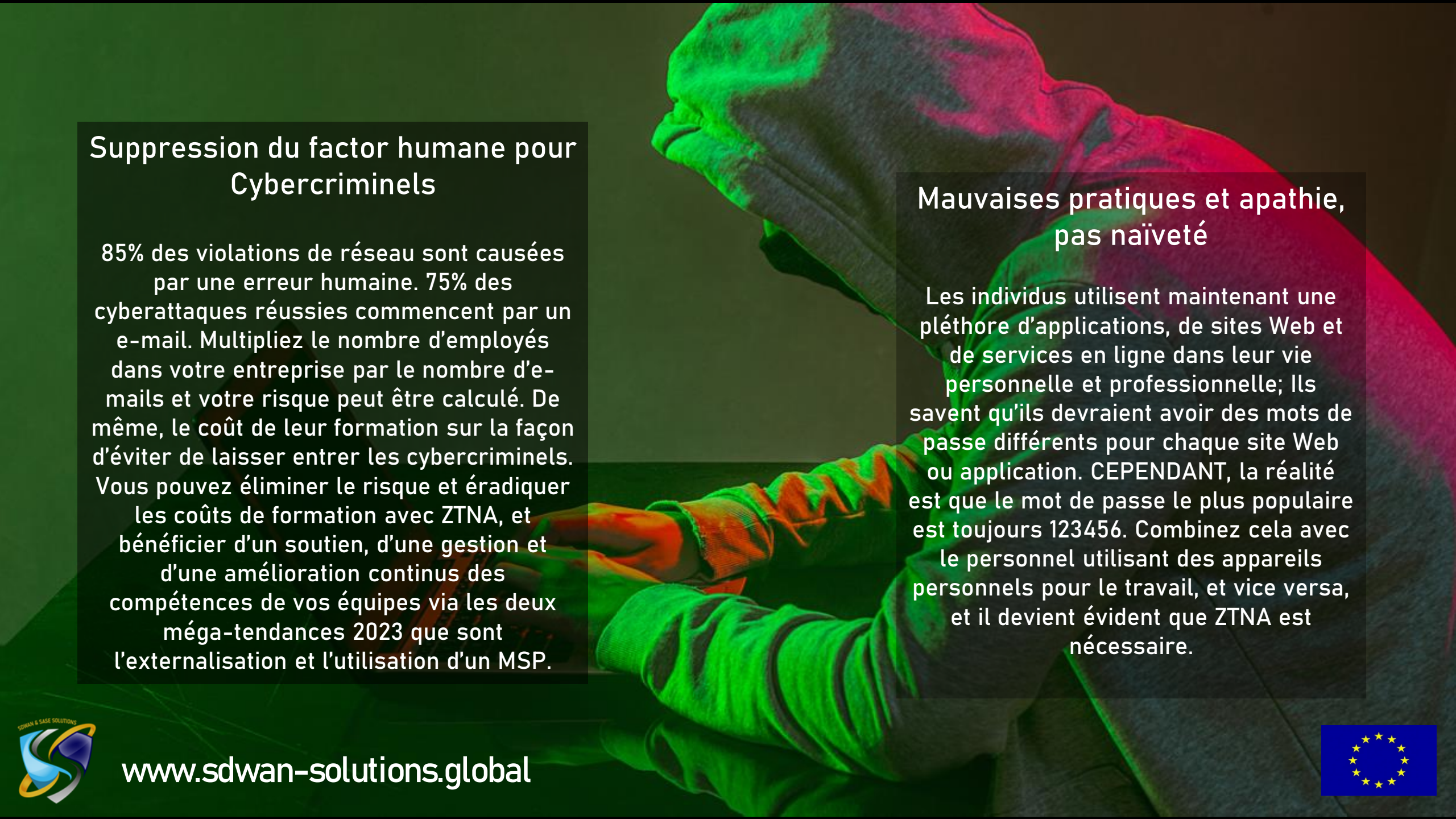
Toutes les 7 secondes une attaque a lieu 2023,
Toutes les 14 secondes, un ransomware se produit
Augmentation de 102 % des ransomwares au cours des 18 derniers mois

Les États-Unis ouvrent la voie!

50 % de tous les cybercrimes visant les États-Unis
Les États-Unis considérés comme une cible facile
Augmentation de 300% de la cybercriminalité au cours des 2 dernières années, selon le FBI
Croissance du TCAC de 12,3% de Cyber-Crime 2023
205,4 milliards de dollars de coût de la cybercriminalité aux États-Unis 2020

Il convient de noter que les États-Unis ont traditionne
18 mois d'avance sur l'Europe.

www.sdwan-solutions.global



Suppression du factor humane pour Cybercriminels

85% des violations de réseau sont causées par une erreur humaine. 75% des cyberattaques réussies commencent par un e-mail. Multipliez le nombre d'employés dans votre entreprise par le nombre d'e-mails et votre risque peut être calculé. De même, le coût de leur formation sur la façon d'éviter de laisser entrer les cybercriminels. Vous pouvez éliminer le risque et éradiquer les coûts de formation avec ZTNA, et bénéficier d'un soutien, d'une gestion et d'une amélioration continus des compétences de vos équipes via les deux méga-tendances 2023 que sont l'externalisation et l'utilisation d'un MSP.

Mauvaises pratiques et apathie, pas naïveté

Les individus utilisent maintenant une pléthore d'applications, de sites Web et de services en ligne dans leur vie personnelle et professionnelle; Ils savent qu'ils devraient avoir des mots de passe différents pour chaque site Web ou application. CEPENDANT, la réalité est que le mot de passe le plus populaire est toujours 123456. Combinez cela avec le personnel utilisant des appareils personnels pour le travail, et vice versa, et il devient évident que ZTNA est nécessaire.

www.sdwan-solutions.global

L'erreur humaine - Fact File

3,2 MILLIARDS de mots de passe et d'informations d'identification compromis ou volés chaque année

SEULEMENT 20% des gens changent leurs mots de passe, même après avoir été piratés!

53 % des personnes interrogées pensent que le télétravail aide les cybercriminels

60 % des comptes d'entreprise contiennent des connexions utilisateur obsolètes

95 identifiants d'utilisateur volés chaque seconde de chaque jour à travers la planète

58% des entreprises ont des fichiers, des dossiers ou des documents non protégés

60% des entreprises ont besoin d'une meilleure protection que leur pare-feu en ligne de défense

40% transportent plus de 1000 fichiers non protégés sur leurs serveurs

La cible cybercriminelle PRINCIPALE est les données personnelles du personnel, par exemple: dossiers médicaux, date de naissance, numéros de sécurité sociale

Saviez-vous que... Guide des cyberattaques

1 DOLLAR est tout ce qu'il en coûte à un pirate informatique pour obtenir ses outils

1 MILLION d'e-mails ou de mots de passe compromis ne coûte que 25 DOLLARS à un pirate informatique

200-300 DOLLARS le coût d'une trousse d'outils de piratage relativement sophistiquée

98% de toutes les rançons payées en Bitcoins

5 millions de dollars ont été versés par la société américaine Colonial Pipeline à des pirates informatiques utilisant des Bitcoins

300 millions de dollars de dommages à FedEx après une attaque

79% ont été effacés de la valeur des actions FedEx lors de la même attaque

3000 travailleurs sont employés dans le département de cybersécurité de JP Morgans

JP Morgan dépense 60 MILLIONS DE DOLLARS PAR AN EN SERVICES DE CYBERSÉCURITÉ

100 MILLIONS DE DOLLARS le montant JP Morgan a augmenté son budget 2023

Un budget de cybersécurité de 1 milliard de dollars sur Microsoft chaque année

Bitcoin joue des deux côtés de la cybercriminalité, les entreprises devant employer des experts bitcoin pour payer des cyber-rançons

Assurance cybersécurité - Fact File

7,6 milliards de dollars Marché mondial de l'assurance cybersécurité 2021

20,5 milliards de dollars en 2027

27 % des violations de données ont reçu des paiements d'assurance

24% des polices ont des exclusions qui empêchent le paiement complet

19% des organisations avaient une assurance cybersécurité en 2022 au-delà de 600 000 $

55 % déclarent avoir une assurance cybersécurité

68% des entreprises n'ont toujours pas d'assurance cybersécurité

25% des entreprises envisagent de souscrire une assurance cybersécurité

Les PME les grands réclamants

99 % de toutes les réclamations d'assurance proviennent de PME

13% du marché des technologies de cybersécurité sont des PME

Les PME font plus de confiance sur l'assurance que sur les outils technologiques de protection

60% des PME ne survivent pas à une attaque au-delà de 6 mois

10% des PME sont attaquées au moins une fois par an

97% des PME ont déjà couvert les COÛTS d'une attaque....

40 % ont fermé entièrement après l'attaque

Cyber-attaquants considèrent les PME comme des cibles faciles

Les cyberattaquants eux-mêmes se transforment en PME, créant des attaques plus spécialisées pour d'autres PME

Les PME sont la cible qui connaît la croissance la plus rapide parmi les cybercriminels

www.sdwan-solutions.global

« Nous devons remettre en question les hypothèses, les méthodes et les mentalités du passé si nous voulons que les praticiens de la cybersécurité soient efficaces. Un nouveau paradigme de partenariat est nécessaire. L'application des méthodes et technologies traditionnelles n'est plus efficace, et l'appel est donc lancé à l'industrie pour atteindre les objectifs de sécurité, de vigilance et de résilience dans la conception de ses programmes de cybersécurité. En appliquant une approche unifiée d'intégration, de partage et d'automatisation, il est possible pour la communauté mondiale de gérer efficacement le risque de cybermenace et de garder une longueur d'avance sur les cybercriminels.

DELOITTE 2023

Sur les collaborations privées et publiques en matière de cybersécurité

« Au cours de la réunion [d'Interpol], les données opérationnelles sur la cybercriminalité relatives aux cas réels ont été partagées entre les pays. Ces informations aideront à développer de nouveaux renseignements exploitables afin de réduire l'impact mondial de la cybercriminalité et de protéger les communautés pour un monde plus sûr.

Craig Jones, Directeur de la Direction de la cybercriminalité, INTERPOL

Autres tendances clés 2023 : 1-10

1. ZTNA - Sécurité d'accès réseau Zero Trust telle que SASE
2. Machine Learning et technologie de prise de décision basée sur l'IA
3. Des solutions WFA [Working From Anywhere] sécurisées et opérationnelles à tout moment
4. SD-WAN everywhere - des réseaux intelligents qui prennent en charge toute la transformation digitale et SASE
5. Consolidation et réduction de la complexité : Les équipes IT considérés un catalyseur de réduction des coûts....
6. Les budgets informatiques et technologiques augmenteront à mesure que d'autres seront réduits
7. Il en va de même pour la dotation en personnel technique, car davantage de personnel technique est nécessaire pour accélérer les économies de coûts et la transformation numérique
8. Tech MSPs utilisés pour améliorer les compétences, combler les besoins du personnel et réduire les coûts de formation du personnel.
9. Combler le déficit de compétences grâce à un MSP expert
10. Jumeau numérique par tout, des soins de santé aux infrastructures, de la construction aux initiatives vertes

Autres tendances clés 2023 : 11-20

11. La 5G prend le relais de la 4G à travers la planète
12. L'IoT continue dans les dizaines de milliards d'appareils et...
13. Des usines, des installations et des usines entières passent à l'IoT CEPENDANT....
14. La sécurisation de l'IoT largement non sécurisé (98%) est une priorité absolue
15. Automatisation de la fabrication, Ai et IoT : des installations entières sont automatisées
16. AIaaS – Active-learning-a-a-service – apprentissage en direct et formation n'importe quand, n'importe où
17. Plus de metaverse – au-delà du plaisir et sur le lieu de travail
18. Web3 – Internet de nouvelle génération permettant plus de metaverse et de transformation numérique
19. Efficacité et économies de coûts pour tous, partout, dans chaque département et équipe
20. La technologie des soins de santé devient courante et virtuelle, les salles et même les hôpitaux

Préparé par SDWAN Solutions

SDWAN SOLUTIONS

keeping you connected
keeping you protected

with complete SD-WAN and SASE solutions tailored to your exact needs