Les 7 étapes d'une stratégie cyber-résiliente.

Et affirmer que 1234 n'est pas un vrai mot de passe n'en fait pas partie >

Bitdefender®

BUILT FOR RESILIENCE

Intro

Aucun doute : on se souviendra de l'année 2021 en termes de cybersécurité. Depuis janvier 2021, le nombre d'attaques a augmenté de 36 %. Leur progression est sans précédent et s'accompagne de techniques toujours plus sophistiquées : ransomwares, phishing, cybermercenariat, attaques de type Zero-Day sur les smartphones et IoT… Vous aussi, vous avez encore à l'esprit les attaques qu'ont connues Pegasus et SolarWind ? Ce qui frappe aussi, c'est l'étendue des cibles : le temps où seules les grandes entreprises étaient impactées est révolu et les PME, TPE, collectivités locales et surtout les hôpitaux sont devenus des cibles de choix pour les hackers.

Chez Bitdefender, nous sommes convaincus que 2022 sera une année charnière pour la cybersécurité. Les lignes bougent du côté de la législation nationale et européenne, renforçant les lois et privilégiant une souveraineté numérique plus fiable en matière de protection des données.

Et puis il y a le concept de résilience, à la base de la philosophie et des solutions Bitdefender.

Car oui, on vous a déjà conseillé de ne pas utiliser « 1234 » comme mot de passe, d'opter pour la double authentification ou de toujours avoir une copie externalisée de vos données. Mais cela ne suffit plus !

Il est essentiel d'avoir un coup d'avance et pour ça, les organisations doivent devenir cyber-résilientes. Quésaco ? La résilience, c'est l'art de contrer l'imprévisible et les attaques permanentes en maintenant les données et les systèmes intègres, confidentiels et toujours disponibles. Les cyberattaques évoluent ? Et bien la **résilience offre une sécurité qui sait évoluer et s'adapter H24 elle aussi !**

On vous détaille en 7 étapes comment mener une stratégie cyber-résiliente.

1

Faire (enfin) la distinction entre cyber-résilience et cybersécurité.

Beaucoup plus démocratisé que son nouvel acolyte, le terme de cybersécurité renvoie aux personnes et surtout aux technologies qui agissent comme un rempart fiable aux cyberattaques. La cybersécurité peut créer, auprès des salarié.e.s non-experts, une croyance dangereusement erronée dans laquelle l'entreprise va être capable d'éviter les cyberattaques. Mais une protection efficace à 100 % et l'absolue certitude qu'aucune violation du système informatique n'est possible relève de la pure fiction. Et les années qui viennent de s'écouler ne peuvent qu'entériner l'idée qu'aucune entreprise, petite ou grande, n'est à l'abri d'une cyberattaque. Chaque nouvelle cybermenace détonne par sa sophistication et l'ingéniosité des hackers ne connaît plus vraiment de limite.

Amy Blackshaw, VP of Product Marketing explique, *"nous sommes à une ère d'ultra-connectivité et là je pense au services Cloud qui se développe à grande vitesse et aux objets connectés. De fait, chaque entreprise, chaque particulier présente un niveau de risque encore jamais atteint. Et à moins de vivre sans Internet, il semble désormais utopique de vivre dans un monde dans lequel il serait possible de diminuer le risque d'être touché par une cyberattaque".*

Et c'est là que la notion de résilience entre en scène et déploie toute sa force de frappe. La résilience induit que lorsque (et non pas "si") vous êtes en pleine mesure d'identifier rapidement un type d'incident, vous êtes capable d'y répondre afin de minimiser le plus possible l'impact sur l'entreprise. Et pour y parvenir il faut être conscient du risque, y être préparé et être prêt à rebondir. C'est une nuance qui passe presque inaperçue mais qui est cruciale parce qu'elle repose sur la capacité d'une entreprise et des professionnels de l'IT à savoir anticiper une menace et de reconnaître qu'un risque bien réel plane sur son organisation. Sans non plus entrer dans une méfiance excessive, c'est admettre que tout peut arriver et n'importe quand.

Face à l'imprévisibilité ambiante de ces dernières années, entre pandémie, géopolitique électrique et hackers qui s'en donnent à cœur joie, il n'est donc plus suffisant de se contenter d'une stratégie de détection et de réponse. Pourquoi ? Parce que si l'on se contente d'attendre la prochaine attaque majeure sans cette capacité d'anticipation, il est déjà trop tard. Une structure qui se découvre victime d'une attaque ne sera alors qu'en mesure de revenir sur ses pas et d'agir seulement après coup et les dégâts seront alors difficiles à minimiser. Cette notion de résilience est encore assez embryonnaire dans le monde de la sécurité et beaucoup de professionnels et de revendeurs portent des messages uniquement centrés autour de la détection et de la réponse avancée. Il n'est pas question dans ces propos de remettre cette stratégie en cause parce qu'après tout, elle porte ses fruits mais pour avoir "un coup d'avance" sur les cyber-criminels et ne pas faire la douloureuse expérience de constater des dégâts plus importants que prévus, il est impératif de s'approprier la notion de cyber-résilience.*"Il faut aussi penser à la prévention. Nous ne pouvons plus ignorer la prévention et je crois que le triptyque prévention, détection, réponse offre une voie vers la résilience dont nous avons tous vraiment besoin."* conclut avec justesse notre experte **Amy Blackshaw**.

2

Ne pas négliger la protection des objets connectés.

Nos confrères d'outre-Atlantique s'interrogent : *Internet of Things or Internet of Threats ?* Si l'on se concentre uniquement sur la France, il y aurait 244 millions d'objets connectés. Et pour environ 68 millions d'habitants en janvier 2022, cela représenterait en moyenne 3,5 IoT par habitant. Et dans les années à venir ces chiffres n'auront de cesse de croître. Vous l'aurez compris, les IoT font partie intégrante de notre quotidien aussi bien dans la sphère privée que professionnelle. Une telle montée en puissance de ces objets connectés augmente de manière exponentielle et quasiment inévitable les vecteurs d'attaques. Beaucoup de ces objets maintiennent des systèmes de mots de passe générique et ne sont pas configurés et sécurisés avec la même diligence que les ordinateurs par leur propriétaire. Les non-initiés aux règles élémentaires de l'IT n'évaluent pas encore pleinement le risque que représente les IoT et le télétravail généralisé de ces dernières années a plus que jamais flouté les frontières entre la maison et l'entreprise si bien que beaucoup de salarié.e.s se sont mis à utiliser leurs appareils personnels à des fins professionnelles et inversement. Or, si un appareil n'est pas suffisamment protégé, trouver une brèche sera un jeu d'enfant pour les hackers et il ne faut pas croire que c'est seulement son propriétaire qui sera impacté, c'est l'entreprise où celui-ci travaille qui fera les frais de cette négligence. Et si l'on en revient au nombre d'IoT existant uniquement en France, vous comprendrez pourquoi les professionnels de l'IT tirent la sonnette d'alarme depuis un certain temps déjà.

Quant aux IoT propres aux entreprises, notre experte **Amy Blackshaw** poursuit, *"Tout ce que vous connaissez en entreprise a de grandes chances de posséder une adresse IP, tout est connecté et ce dont nous voulons que les gens se souviennent, c'est qu'ils doivent surveiller ces terminaux et que le moindre petit objet connecté, même la bouilloire à thé de la salle de pause est un terminal qui, mal configuré, mal surveillé, représente une faille de taille dans la sécurité de l'entreprise. Nous comprenons tout à fait qu'il est impossible de dédier un agent à la surveillance d'un IoT. En revanche, notre travail consiste à ce que les entreprises comprennent l'impact de cette situation du point de vue du réseau".* Les entreprises doivent donc mettre en place une stratégie pour obtenir des informations sur ces appareils connectés, avoir un véritable plan d'action qui dit combien d'appareils se sont mis en ligne. En réalité, c'est un réseau à part entière qui doit se mettre en place et avoir une visibilité sur cette flotte afin de détecter rapidement la moindre faille, au même titre que la flotte de laptops.

3

S’appuyer sur les nouvelles technologies.

Dans une stratégie cyber-résiliente où la prévention demeure le véritable mot d’ordre, les entreprises doivent faire face à un certain nombre de contraintes. Entre le nombre d’informations à explorer, à analyser et les enjeux de rapidité, pour contrer au plus vite les menaces, les limites de chaque être humain sont rapidement atteintes et c’est bien naturel, à moins d’être un cyborg venu du futur. Mais comme tout le monde n’a pas cette chance, des technologies avancées comme l’apprentissage automatique (ou Machine Learning) prennent le relais des cerveaux humains. Elles constituent une aide technologique précieuse pour les acteurs de l’IT car elles sont en mesure de traiter un nombre gigantesque d’informations en très peu de temps.

Concrètement, le Machine Learning s’appuie sur la science complexe des algorithmes et des mathématiques pour identifier et apprendre par lui-même, en un temps record. Ce modèle va d’abord ingérer une énorme quantité de données, faire le tri parmi cette masse de data pour ensuite être capable d’identifier des anomalies allant de la simple brèche à la reconnaissance d’un modèle de malware et autre cyber-menaces, parmi les plus récentes et les plus sophistiquées.

Luana Pascu, chercheuse en cybersécurité apporte quelques précisions : *“Dans le domaine de la cybersécurité, les algorithmes de Machine Learning peuvent apprendre seuls à faire des prédictions basées sur l’expérience et sur l’analyse quotidienne de millions de programmes malveillants. En pratique, un modèle d’algorithme automatique est entraîné à identifier une menace nouvelle ou inconnue sur la base de similitudes avec des menaces connues”.*

Il existe deux types de modèles de Machine Learning, il y a un modèle dit supervisé et un second, non-supervisé. *“Mais les deux modèles ont leur importance”*, insiste **Amy Blackshaw**.“ *Non supervisé signifie que le modèle va apprendre en se basant uniquement sur les données et aussi sur ses propres découvertes, et donc il s’accorde lui-même en fonction de ce qu’il voit dans sa source de données. La structure des données est en quelque sorte autosuffisante pour apprendre et corriger. Le machine Learning supervisé signifie que vous avez besoin d’un humain pour vous aider à aiguiller correctement votre modèle. Un analyste doit donc compléter les informations de ce modèle et lui apprendre que telle anomalie n’en était pas une et ainsi lui permettre de faire la distinction lorsqu’un cas de figure similaire se présentera à nouveau”.*

Ces nouvelles technologies jouent un rôle capital car elles permettent de tirer parti des machines pour faire le travail que les humains ne peuvent pas effectuer et cela sert parfaitement l’objectif préventif d’une stratégie cyber-résiliente. Le Machine Learning permet d’identifier rapidement une menace avant qu’elle ne cause des dommages aux entreprises.

4

Sensibiliser davantage les collaborateurs aux cyber-menaces.

Il existe dans chaque entreprise autant de profils et de comportements face à la sécurité informatique que de salarié·e·s. Du bon élève à l'irresponsable, en passant par l'étourdi qui laisse son mot de passe écrit sur un post-it, bien en évidence sur son bureau, il est clairement difficile de maîtriser le facteur humain en matière de cybersécurité en entreprise.

"Vous avez beau construire un environnement fiable, le Cloud privé le plus sûr du marché ou encore des applications et des IoT avec un système de double authentification, tant qu'il y aura des humains et des utilisateur·rice·s imparfait·e·s, le risque existera toujours et lesmesures que vous aurez prises pour assurer la sécurité seront… vaines", constate **Amy Blackshaw.**

L'élément humain en termes de cybersécurité est pourtant essentiel mais est curieusement mis au second plan. Dans le cadre d'une stratégie de cyber-résilience, les entreprises auraient pourtant tout intérêt à faire de la sensibilisation une véritable mission et que les principes fondamentaux propres à la cybersécurité fassent partie intégrante de la culture d'entreprise. *"Je ne pense pas que se contenter d'une formation annuelle soit suffisant"*, commente **Amy Blackshaw**. Selon notre experte, il devrait y avoir une communication constante sur le sujet et autour des actualités récentes de la cybersécurité et pourquoi pas le partage régulier de circulaires autour des bonnes pratiques à adopter. Ensuite, la pratique a une fonction essentielle puisqu'elle permet d'illustrer au plus près la réalité des cyber-menaces. Les DSI, et c'est un exercice déjà bien connu en France, peuvent mettre en place des envois de faux phishing pour mesurer le taux de réactivité des salarié·e·s. Il ne s'agit pas là d'afficher sur un wall of shame les mauvais élèves mais plutôt d'alerter avec bienveillance et pédagogie sur les pratiques toujours plus insidieuses des hackers. Ces derniers n'hésitent pas à susciter craintes ou autres émotions pour parvenir à leurs fins et c'est quelque chose dont doivent prendre conscience les utilisateur·rice·s.

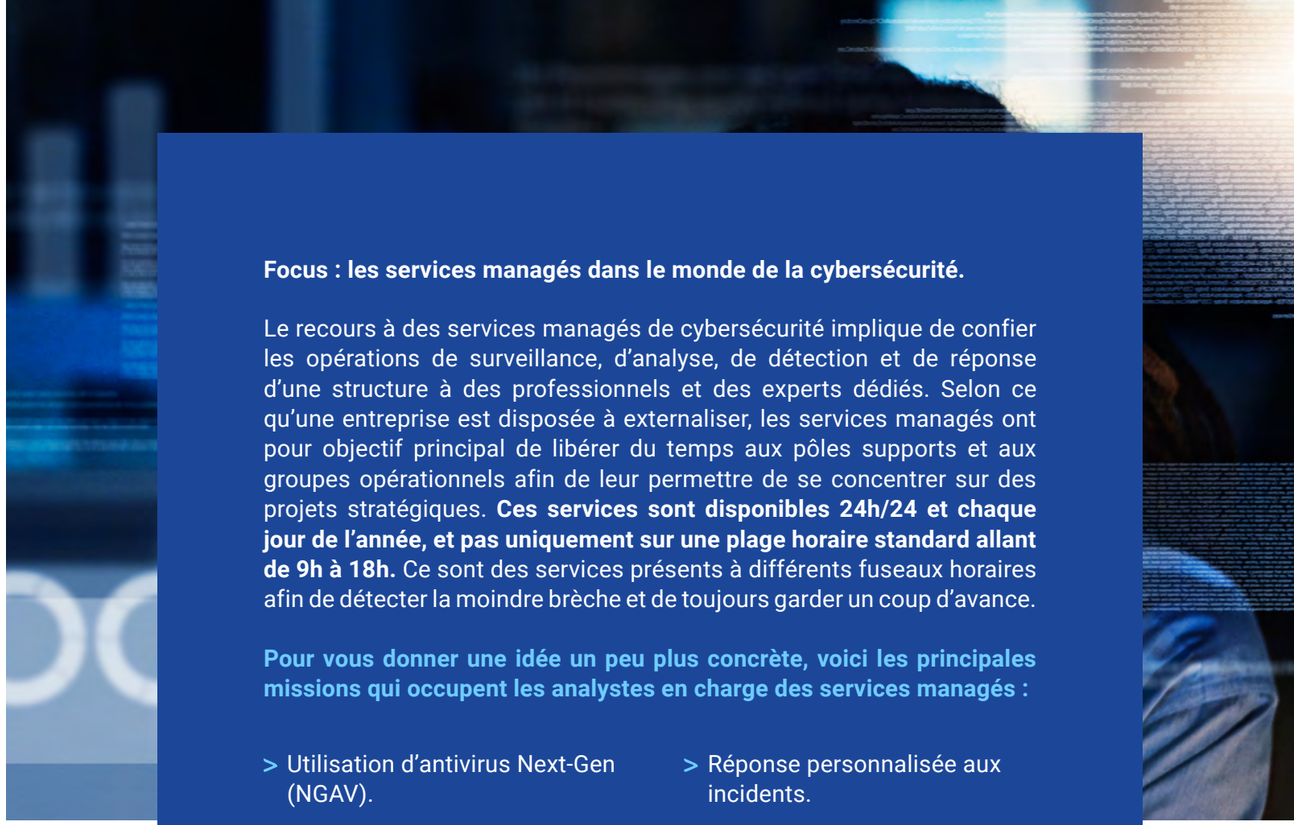
Il est du devoir des professionnels de la cybersécurité, chez Bitdefender ou ailleurs, de fournir cette prise de conscience au-delà des murs des entreprises. Il existe aux Etats-Unis le mois de la sensibilisation à la cybersécurité. Chaque mois d'octobre, des sessions de formations et des évènements dédiés sont mis en place. **Amy Blackshaw** poursuit : *"Je crois sincèrement que cette sensibilisation doit commencer dès les bancs de l'école, surtout à une époque où les enfants naissent et grandissent avec Internet et les écrans. Je vais donc dans les écoles et j'enseigne aux élèves quelques principes autour de la confidentialité des données, ce qu'il faut partager, ce qu'il ne faut pas partager, comment être prudent sur Internet . Et je le répète, il ne faut pas se contenter de parler de la dernière attaque, mais parler de ce que nous pouvons faire pour l'empêcher de se reproduire."*

5

Rééquilibrer les investissements cyber et se lancer dans les services managés.

Beaucoup d'entreprises font l'erreur assez commune de penser leur budget cybersécurité uniquement autour des notions de détection et de de réponse avancées. Nous l'avons écrit à maintes reprises, ce sont certes des éléments indispensables mais dans un cadre de cyber-résilience, un rééquilibrage des sommes investies, notamment au profit des contrôles préventifs s'avère plus que nécessaire. Investir dans la prévention permettra non seulement d'arrêter et bloquer certaines menaces bien en amont d'une phase de détection standard mais contribuera largement à libérer certaines ressources pour éviter au maximum cette phase de détection qui, comme nous l'avons vu dans un point précédent, arrive souvent trop tard. Passé ce constat, **Amy Blackshaw** poursuit et précise,

"Je pense que selon le type d'organisation dans laquelle vous évoluez, sa taille, le type de budget informatique et cybersécurité dont vous disposez, il serait peut-être judicieux d'envisager d'investir dans des services managés. Parce que vouloir à tout prix gérer son propre SOC (centre d'opérations de sécurité), embaucher ses analystes, donner encore plus de responsabilités à ses DSI coûtent trop cher et monopolisent un trop grand nombre de ressources. S'associer à un partenaire dédié pour des services gérés, en particulier la détection et la réponse, pouvoir compter sur cet allié de confiance qui fait ce travail en votre nom vous aidera véritablement à franchir le cap de la résilience. Je suis convaincue qu'il est plus important aujourd'hui de se poser la question quant au retour sur investissement de la mise en place de capacités internes et (ou) au recours aux services d'un partenaire."



Focus : les services managés dans le monde de la cybersécurité.

Le recours à des services managés de cybersécurité implique de confier les opérations de surveillance, d'analyse, de détection et de réponse d'une structure à des professionnels et des experts dédiés. Selon ce qu'une entreprise est disposée à externaliser, les services managés ont pour objectif principal de libérer du temps aux pôles supports et aux groupes opérationnels afin de leur permettre de se concentrer sur des projets stratégiques. **Ces services sont disponibles 24h/24 et chaque jour de l'année, et pas uniquement sur une plage horaire standard allant de 9h à 18h.** Ce sont des services présents à différents fuseaux horaires afin de détecter la moindre brèche et de toujours garder un coup d'avance.

Pour vous donner une idée un peu plus concrète, voici les principales missions qui occupent les analystes en charge des services managés :

- Utilisation d'antivirus Next-Gen (NGAV).
- Remédiation automatique.
- Contrôle des applications et des appareils.
- Pare-feu au niveau de l'hôte et contrôle Web.
- Solution de détection et de réponse étendues (XDR) couvrant les endpoints, le cloud, les identités, le réseau et les applications métiers (par exemple O365).
- Gestionnaire de compte dédié.
- Analyse des risques liés aux utilisateurs.
- Chasse aux menaces ciblée.
- Réponse personnalisée aux incidents.
- Modélisation des menaces spécifiques à chaque client.
- Surveillance de l'enregistrement de domaines de phishing.
- Lutte contre la publication non autorisée de code ou surveillance des informations du client.
- Surveillance du Dark Web.
- Intégration avec les outils personnalisés.
- Surveillance de cibles à grande valeur et à haut risque.

6

Élargir le champs dans la recherche de nouveaux profils cyber.

Une fois n'est pas coutume, parlons humains mais cette fois-ci non pas du côté utilisateur·rice·s mais plutôt du côté expertise. **Amy** nous raconte, *"J'ai commencé dans la cybersécurité il y a maintenant 12 ou 13 ans, c'était déjà une grande industrie mais au cours de la dernière décennie, nous avons vu une augmentation assez incroyable du besoin en personnel qualifié. Et depuis près de deux ans, les choses tendent à se préciser puisque nous assistons à une diversification des profils et des compétences. Nous avons rapidement compris qu'être ingénieur en cybersécurité ne suffisait pas. Nous avons besoin de personnes véritablement curieuses, qui savent poser les bonnes questions et qui ont une façon de penser qui sort un peu des sentiers battus même si cela implique qu'ils soient assez junior sur la partie technique."* Finalement, il n'y a pas de meilleure école que celle de la pratique donc, tout ce qui relève de la technique peut s'apprendre sur le tas. C'est bien en forgeant que l'on devient forgeron comme le veut ce vieil adage. En revanche, les soft skills que nomment **Amy** sont des choses qui ne s'apprennent pas. Ainsi, des programmes à l'image du Certified Information Systems Security Professional (CISSP) sont d'excellents moyens de détecter ce genre de profils et les intégrer au sein des entreprises. *"Pourquoi focaliser cette recherche sur un seul milieu, une seule filière ?"* s'interroge **Amy**. *"Il est nécessaire d'élargir les possibilités de carrière dans la cybersécurité et recruter dans de plus vastes domaines afin de continuer de construire et de sécuriser les innombrables transformations numériques que nous allons vivre durant les trente prochaines années."* Et que penser de la montée en puissance des Chief Data Officer à une époque où la data est une denrée aussi précieuse que le pétrole ? Ces profils ont une position tout à fait stratégique surtout depuis que les cas de violations de données se multiplient, que la législation sur la question épineuse des données personnelles se durcit et que les données circulent et sont stockées dans le Cloud. En outre, les consommateur·rice·s sont en droit d'attendre que les transactions bancaires qu'ils effectuent avec des sociétés ou les informations personnelles qu'ils partagent soient prises en charge avec un dispositif des plus sécurisés. Il faut que toutes ces entreprises se dotent de ces profils et que ces derniers agissent en tant qu'agent de la transformation numérique et réfléchissent en profondeur à ce que cela implique en termes de sécurité et de confidentialité de passer d'un Legacy On Premise à un système applicatif qui naît et vit dans le Cloud.

7

Opter pour des solutions Cloud plus souveraines.

La crise sanitaire a définitivement entériné l'usage du Cloud afin de maintenir la continuité des activités et offrir plus de réactivité dans un contexte de mutation des modes de travail. Ainsi, les entreprises et les services publics ont pu facilement basculer en télétravail grâce à l'incontestable flexibilité des services numériques qui découlent du Cloud. Nos communications, nos fichiers, nos outils de travail ont désormais vocation à transiter quotidiennement au sein des plateformes des géants du Cloud, à savoir les 5 plus gros détenteurs de serveurs externalisés connus sous l'acronyme GAFAM (pour Google, Apple, Facebook, Amazon et Microsoft). Un tel engouement s'explique par la très grande accessibilité des données, depuis n'importe quel endroit et depuis n'importe quel terminal et par la fiabilité du Cloud qui évite, même en cas de défaillance du matériel, de perdre de précieuses data. C'est un bien joli tableau, la solution miracle dirait-on, mais la protection de la confidentialité des données est-elle vraiment garantie ? L'actualité nous indiquerait plutôt que… non. La hausse des cyberattaques et des violations de données ces deux dernières années sur ces plateformes publiques ont prouvé que le Cloud n'est pas à l'abri des cyber-attaquants. Les attaques sur le Cloud visent en priorité les plateformes comme les drives : la durée de vie des données qui y sont stockées est illimitée et trop souvent les politiques d'effacement y sont ignorées. Et ce n'est pas la seule faiblesse à relever du côté des GAFAM. Car se pose la question épineuse de la souveraineté des données hébergées dans le Cloud. Où sont-elles vraiment hébergées et donc sous quelle législation ? L'opérateur de Cloud est-il indépendant sur l'ensemble de la chaîne de production ? Ou des sous-traitants régis par une législation hors Europe interviennent ? Les entreprises achètent des services Cloud auprès des fournisseurs mais qu'advient-il ensuite… N'est-il pas temps de prôner un Cloud plus souverain ?

Amy nous donne son avis sur le sujet : *"L'Europe a toujours eu une plus grande sensibilité quant au traitement et à la protection juridique de ses données, notamment avec l'avènement de la loi RGPD. L'idée du Cloud souverain qu'elle défend aujourd'hui prend tout son sens selon moi. Cela permettra aux organisations de tirer parti de tous les avantages de l'utilisation de plateformes publiques, sans l'inquiétude de la différence de traitement des données en fonction de différentes politiques ou du manque de transparence de certains sous-traitants. Nous devons encourager cette innovation d'indépendance numérique pour mieux maîtriser la vie et la disponibilité des données. C'est un exemple qu'il va être essentiel de poursuivre dans d'autres régions du monde et aux Etats-Unis."*

https://www.usine-digitale.fr/article/le-cloud-souverain-n-est-il-qu-un-fantasme.N1151837

https://solutions.lesechos.fr/tech/c/cloud-souverain-quels-sont-les-enjeux-pour-la-protection-des-donnees-et-lecologie-31841/

Conclusion

On estime le coût mondial de la cybercriminalité en 2021 à 6 trillions de dollars. Si elle était une économie, elle se classerait au troisième rang après les États-Unis et la Chine. C'est pour œuvrer à diminuer ce genre de chiffres que Bitdefender développe depuis plus de 20 ans des solutions innovantes en termes de cybersécurité.

Une expertise inégalée pour conseiller les organisations, autour de piliers :

> Une vision et des solutions conçues autour de la résilience, l'art de contrer l'imprévisibilité des cyberattaques et pouvoir toujours avoir un coup d'avance. Quand on apprend l'existence d'une attaque il est déjà trop tard, la philosophie Bitdefender c'est de pouvoir l'anticiper !

> Des technologies de pointe, notamment autour du Machine Learning et de l'intelligence artificielle.

> Un Security Operation Center (SOC) composé exclusivement d'analystes recrutés auprès d'agences de renseignement du monde entier qui assurent 24h/24, 7j/7, les opérations de cybersécurité des clients en matière de prévention, détection, réponse et reporting.

> Un Lab Bitdefender, à la recherche de menaces émergentes et qui œuvre au développement de nouvelles technologies de défense contre les malwares, pour assurer la sécurité des entreprises quelles qu'elles soient, où qu'elles soient et quel que soit l'attaquant. En étroite collaboration avec les forces de l'ordre et des chercheurs en cryptographie et informatique quantique, ses équipes d'experts incorporent sans cesse leurs dernières découvertes à leurs technologies de prévention.

Contactez-nous dès maintenant pour parler de votre cyber-résilience !

Bitdefender®

BUILT FOR RESILIENCE