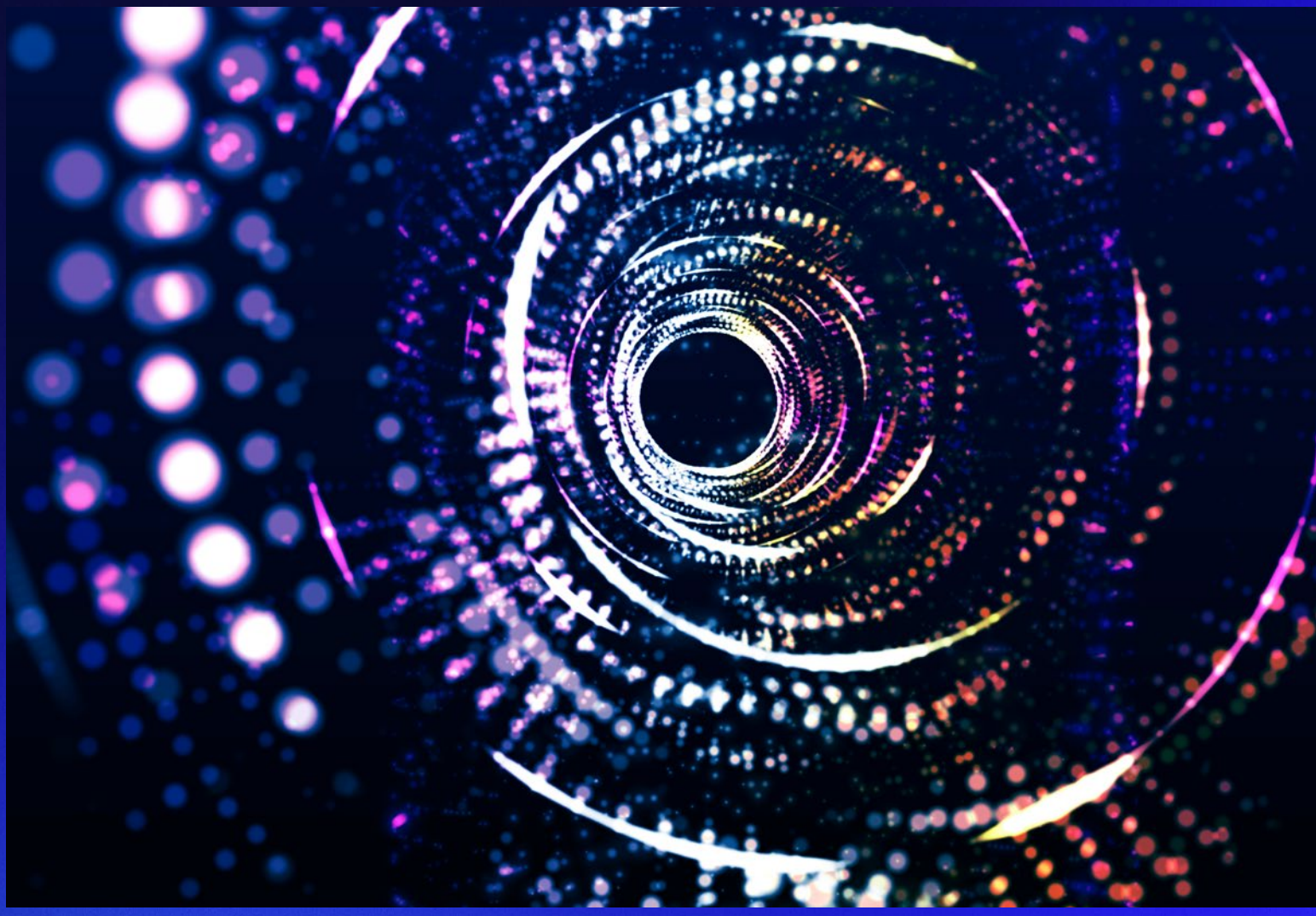
Secureworks®

LIVRE BLANC

AU-DELÀ DU POINT DE TERMINAISON

Résolvez vos principaux problèmes de cybersécurité dès aujourd'hui



L'ancien modèle de cybersécurité préconisait de « sécuriser le point de terminaison ». Or, une approche de la sécurité axée sur le point de terminaison ne permet plus de protéger vos précieuses données aussi efficacement que par le passé. En effet, aujourd'hui, les incidents de cybersécurité émanent de presque n'importe où sur la pile informatique. Chez nos quelque 4 500 clients, plus de 60 %[1] des principales données d'événement et de détection de menaces ne proviennent plus des points de terminaison. Autrement dit, les menaces peuvent contourner complètement votre détection sur les points de terminaison.

C'est pourquoi de nombreuses organisations ont le regard tourné vers l'avenir et réfléchissent à la manière dont elles peuvent optimiser à la fois la sécurité et l'efficacité. Cette réalité pousse un grand nombre d'organisations de sécurité à repenser leur approche de la sécurité, pour développer une vision à la fois stratégique et pérenne. Les entreprises cherchent également à s'associer au meilleur partenaire pour les accompagner dans cette démarche.

LA SITUATION ACTUELLE A ÉVOLUÉ :

Il fut un temps où la sécurité des points de terminaison était la panacée de la cybersécurité. En fin de compte, le plus grand défi pour les organisations aujourd'hui, c'est peut-être de reconnaître que les choses ont changé. Leur visibilité limitée sur les menaces au-delà du point de terminaison constitue un risque sérieux. Les données d'événements manquantes qui leur permettraient de détecter et d'atténuer les risques plus efficacement et plus rapidement se perdent dans tout un tas de systèmes Cloud, d'applications, de messagerie, de gestion des identités, etc.

Cette disparité des systèmes pourrait expliquer pourquoi 68 %[2] des organisations ont rapporté que la fréquence des attaques avait augmenté l'année dernière. De plus, dans la mesure où près des deux tiers1 des données d'événements proviennent désormais de données de télémétrie EDR externes, les entreprises risquent de laisser passer un trop grand nombre de menaces non détectées et inconnues, jusqu'à ce qu'il soit trop tard.

Tout a changé. Pour une cybersécurité efficace, il faut désormais découvrir les menaces connues et inconnues à mesure qu'elles se présentent et les traiter de manière rapide et précise afin de réduire le plus possible les éventuels problèmes de sécurité.

Quelle est la prochaine étape pour les organisations qui cherchent à rendre leurs opérations de sécurité plus efficaces tout en exploitant la valeur de leur couche EDR essentielle ?

Commençons par ce que l'on sait :

Les cyberattaques continuent de contourner les solutions EDR

La croissance effrénée du volume et de la sophistication des attaques a été (paradoxalement) la conséquence inévitable d'une meilleure protection des points de terminaison contre les logiciels malveillants et d'une meilleure sécurité EDR. Autres facteurs : l'essor du télétravail et l'appât du gain pour les cybercriminels. Une attaque réussie peut leur rapporter gros.

[1] Source : Données d'événements et de télémétrie du client issues de la solution Secureworks® Taegis™ XDR

[2] Source : Ponemon Institute, janvier 2020

Les disponibilités varient selon les zones géographiques. © 2023 Secureworks, Inc. Tous droits réservés.

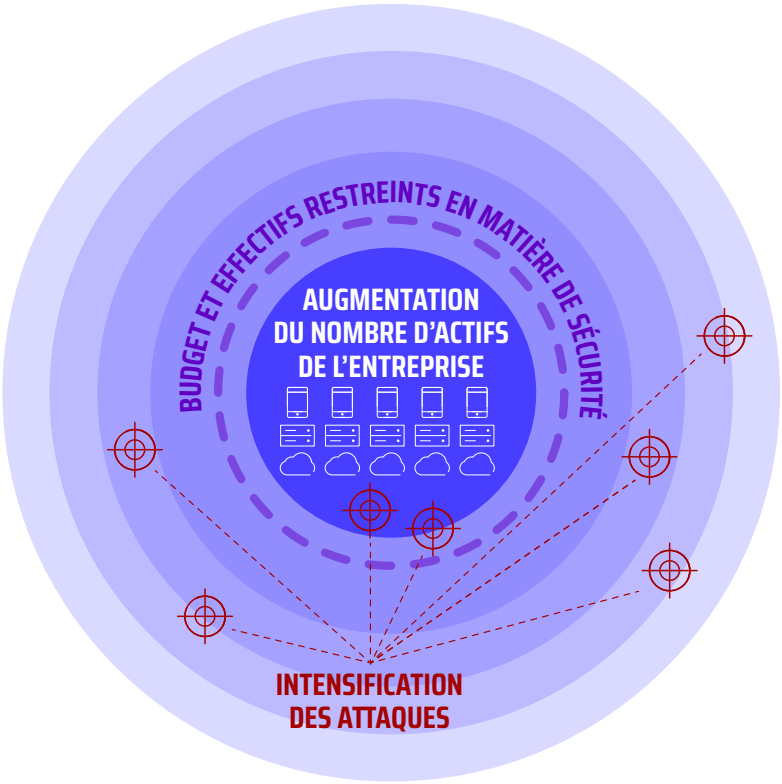
À cela s'ajoute la liste toujours plus longue des ressources nécessaires pour assurer la protection des organisations tout au long de leur transformation numérique : collecte et stockage d'encore plus de données et de liens numériques qui en résultent, avec une cohorte croissante de clients, de fournisseurs, de partenaires et de sous-traitants. Cette dynamique augmente de façon exponentielle les surfaces d'attaque d'une organisation.

Les cybercriminels le savent et font preuve de créativité en attaquant ces zones en dehors du point de terminaison, ou simplement en contournant ou en neutralisant les défenses du point de terminaison.

L'ÉVOLUTIVITÉ EST ESSENTIELLE, MAIS LE MANQUE DE MOYENS EST CRIANT

Les budgets sont limités[3] et il en va de même pour le nombre de spécialistes de la sécurité compétents et abordables[4]. Les organisations doivent également prendre en compte le nombre d'outils et de services de sécurité séparés qu'une équipe de sécurité peut intégrer et exploiter efficacement sans être saturée.

Ces conditions difficiles mettent les organisations au défi d'adapter leurs opérations de gestion de la sécurité de manière efficace et rentable, en particulier lorsqu'elles doivent faire face à des besoins essentiels pour résoudre les graves problèmes de cybersécurité auxquels elles sont confrontées.



Compte tenu de l'intensification des attaques, de l'expansion continue de l'environnement d'entreprise et des ressources limitées, les équipes SecOps doivent à présent atténuer les cybermenaces de manière beaucoup plus efficace.

[3] Source: Les dépenses des entreprises en cybersécurité ont augmenté d'environ 11% en 2022, passant de $155B à $172B (Gartner)

[4] Source: La pénurie de cybercompétences est causée par l'épuisement professionnel des analystes

Les disponibilités varient selon les zones géographiques. © 2023 Secureworks, Inc. Tous droits réservés.

Plus précisément, les organisations sont confrontées à ce qui s'apparente à un « double coup de massue » causé par des conditions difficiles. Elles doivent non seulement rendre leurs opérations de sécurité plus efficaces en couvrant l'infrastructure informatique complète, mais également les rendre beaucoup plus performantes, car le processus de recrutement et de fidélisation du personnel de sécurité qualifié et compétent est plus coûteux et plus difficile que jamais.

Or, si les organisations ne commencent pas à réaliser rapidement les gains d'efficacité nécessaires en matière de sécurité pour neutraliser les attaques efficacement et à grande échelle, elles continueront à être exposées aux niveaux de risque de cybersécurité inacceptables d'aujourd'hui, et devront assumer les coûts astronomiques qui vont de pair.

LA FINALITÉ EST D'ATTEINDRE UNE EFFICACITÉ D'ATTÉNUATION OPTIMALE :

Nous avons créé un terme pour aider les organisations à évaluer et à comprendre leur capacité globale à relever les défis de cybersécurité à grande échelle : l'« efficacité de l'atténuation ». Une évaluation rigoureuse de **l'efficacité de l'atténuation** peut aider les organisations à garantir une sécurité optimale grâce à leurs solutions, malgré des ressources et des budgets limités.

L'efficacité de l'atténuation correspond au rapport entre deux indicateurs :

i) Total des risques atténués
ii) Total des dépenses de cybersécurité

Total des risques atténués :

Cet indicateur est basé sur l'impact quantifié du coût qu'une violation réussie pourrait avoir sur votre organisation. L'impact du coût varie d'une organisation à l'autre et ne se résume pas au nombre de différentes menaces actives identifiées ou au nombre de CVE que vous corrigez. Le total des risques atténués tient plutôt compte des coûts potentiels d'une violation concrète comme un coût global pour l'organisation.

Il prend également en compte l'incidence de vos capacités d'atténuation actuelles sur ce coût. Par exemple, être capable d'identifier et de neutraliser un rançongiciel actif dans les quelques heures suivant l'intrusion initiale réduira de manière significative les coûts d'atténuation totale des risques et permettra de réaliser des économies plus importantes que si l'atténuation avait lieu après le chiffrement et l'exécution du processus de récupération.

Total des dépenses de cybersécurité :

Cet indicateur englobe l'ensemble des heures, outils, services et autres ressources nécessaires à votre organisation pour se protéger contre les attaques et les contrer.

Il s'agit principalement de postes budgétaires explicitement consacrés à la cybersécurité/aux opérations de sécurité. Il prend également en compte les heures du personnel informatique consacrées aux activités liées à la sécurité, les heures du personnel non technique consacrées à la formation à la cyberhygiène et les primes/tarifs différenciés auxquels ont droit les fournisseurs pour garantir la conformité aux normes de sécurité les plus strictes.

Les disponibilités varient selon les zones géographiques. © 2023 Secureworks, Inc. Tous droits réservés.

Créer de la valeur grâce à l'efficacité de l'atténuation :

L'application concrète du principe d'efficacité de l'atténuation ne vise pas à calculer un score pour votre organisation. Ce n'est pas une simple formule à appliquer. Il se peut que votre environnement soit trop étendu ou trop complexe pour que vous puissiez estimer avec précision le nombre de risques métier que vous atténuez tous les jours. Vous pouvez être affecté par des facteurs sectoriels particuliers qui augmentent intrinsèquement votre niveau de risque. Chaque organisation est différente. Il convient plutôt de regarder la logique concrète qui permet d'améliorer l'efficacité.

Une application concrète consiste à vous aider à reconnaître les facteurs qui peuvent avoir un impact profond sur l'efficacité de l'atténuation. En comprenant ces facteurs, vous serez en mesure de justifier davantage le fait de les prendre en compte immédiatement.

En fin de compte, les organisations doivent améliorer leur efficacité pour relever avec succès les défis de cybersécurité à grande échelle.

DÉFIS D'EFFICACITÉ COURANTS

Les facteurs les plus courants qui sapent la capacité des organisations à améliorer leur taux d'efficacité de l'atténuation sont les suivants :

Donner trop d'importance à l'EDR

Les menaces d'aujourd'hui s'éloignent de la vision EDR de la protection adéquate axée sur le point de terminaison, car nous avons désormais des infrastructures informatiques sans périmètre qui ont besoin que tous les actifs bénéficient d'une seule et même couverture de détection. Cela inclut les points de terminaison distants, les réseaux distribués, les systèmes Cloud, les systèmes d'entreprise (messageries, systèmes de gestion des informations d'identification), les applications Cloud, les systèmes IoT et bien plus encore.

Sécurité tactique et sécurité stratégique

La nature impitoyable des attaques d'aujourd'hui est telle que les équipes de sécurité se retrouvent souvent à lutter contre les attaques nuit et jour, jour après jour. Cette action tactique à court terme empêche d'avoir une vue d'ensemble et d'évaluer comment le temps et les ressources peuvent être alloués de manière plus stratégique et plus efficace.

Sécurité cloisonnée en silos

Les kits d'outils pour les opérations de sécurité se sont étoffés au fil du temps, ce qui a fait exploser les coûts de renouvellement et d'exploitation. En 2022, une entreprise utilisait en moyenne 76[5] outils ! Entre les licences, la formation, l'apprentissage, le temps de gestion et les pertes d'efficacité dues au fait d'avoir à jongler entre une multitude d'outils, la croissance des coûts atteint des niveaux inédits. De plus, de nombreuses couches de sécurité fonctionnent en silos, ce qui rend plus complexes et plus difficiles la détection des menaces et une réaction rapide.

[5] Panaseer Security Leaders Peer Report 2022

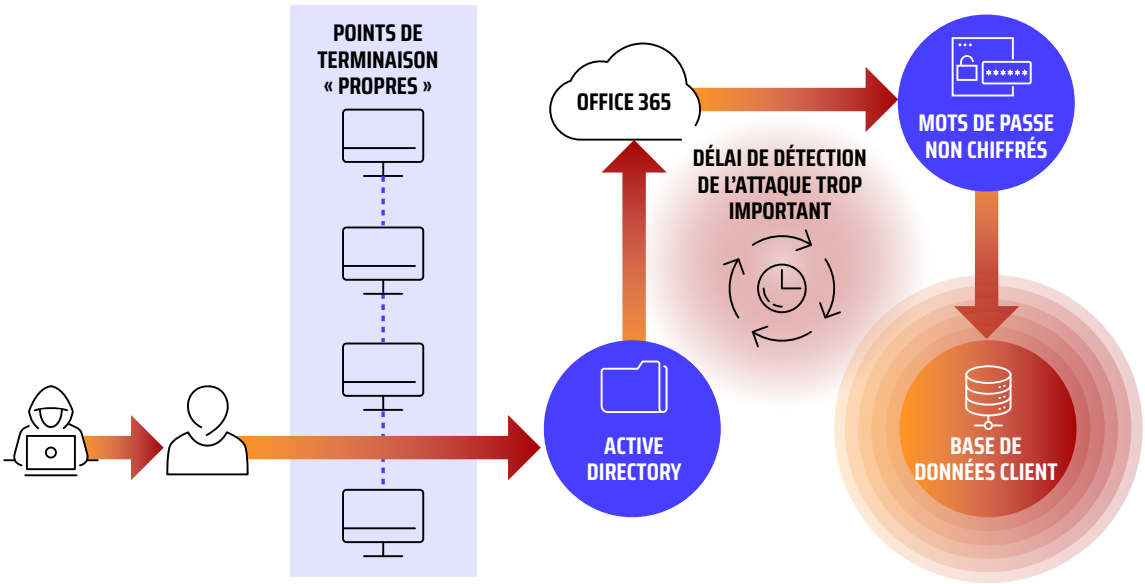
Les disponibilités varient selon les zones géographiques. © 2023 Secureworks, Inc. Tous droits réservés.

Manque de partenaires de sécurité transparents

Très peu de fournisseurs proposent des solutions et des services de sécurité qui optimisent la valeur commerciale et gèrent à la fois les aspects rentabilité et efficacité. Les équipes de sécurité doivent se contenter de « faire en sorte que ça fonctionne » malgré des kits d'outils fragmentés, des charges applicatives élevées et un manque de visibilité sur les événements. Les organisations ont besoin de s'appuyer sur un partenaire fournisseur de confiance, capable de mettre en place une stratégie de cybersécurité efficace adaptée, dans une relation de partenariat étroite et transparente.

Manque important de personnel informatique

Un trop grand nombre d'organisations ne disposent pas d'une équipe SecOps dédiée ou spécialisée, disponible 24x7. Or, les menaces, elles, ne s'arrêtent jamais. À cause des contraintes liées aux ressources, les organisations ne comptent souvent qu'un petit nombre d'analystes en sécurité. Pire encore, une petite équipe informatique peut être amenée à traiter avec des prestataires de services managés de points de terminaison/réseaux peu performants, ce qui brouille la visibilité sur le paysage des risques de l'organisation !



Une approche de sécurité obsolète basée sur le périmètre/le point de terminaison laisse les entreprises excessivement exposées à des attaques sophistiquées capables de déjouer la surveillance traditionnelle des points de terminaison.

Les disponibilités varient selon les zones géographiques. © 2023 Secureworks, Inc. Tous droits réservés.

ALLER AU-DELÀ DU POINT DE TERMINAISON : QUATRE FAÇONS DE GAGNER EN EFFICACITÉ

Quelles mesures pouvez-vous mettre en place dès maintenant pour accroître votre efficacité et assurer la défense à grande échelle nécessaire pour relever les défis auxquels vous êtes confronté en matière de cybersécurité ?

Voici quatre étapes essentielles qui vous permettront de devenir un maître en matière d'efficacité de l'atténuation :

1. Faire de l'efficacité de l'atténuation une priorité.

Il est d'une importance cruciale d'être en mesure de faire évoluer votre activité future et votre processus d'atténuation des cybermenaces. Pour ce faire, vous devez vous engager pleinement en faveur de l'efficacité en fournissant une solution d'opérations de sécurité stratégique qui évite à votre équipe d'être contrainte à répéter constamment un schéma tactique dans l'urgence.

De nombreuses organisations évoluent, mais restent à la traîne en matière d'efficacité, en optant pour une simple solution de détection et réponse managées. Or, pour obtenir une visibilité plus complète et une évolutivité concrète, il convient de faire appel à une aide extérieure en optant pour une plateforme de détection et de réponse étendues managées (ManagedXDR). Cette approche de plateforme partagée favorise la collaboration et fournit des informations plus pertinentes, et n'entraîne souvent que peu ou pas de différence de coûts d'exploitation par rapport à une solution MDR.

2. Exploiter une solution EDR en allant au-delà du point de terminaison.

Les organisations qui cherchent à obtenir plus de valeur et à gagner en efficacité peuvent bénéficier d'avantages considérables en s'éloignant résolument d'un modèle de défense du périmètre, axé sur les points de terminaison. Cette approche limite la visibilité en matière de sécurité et empêche les équipes de contrer les risques réels.

Utilisée seule, une solution EDR passe à côté de trop de menaces et les laisse subsister trop longtemps, ce qui nuit à l'efficacité de la détection et à la productivité de l'équipe de sécurité, et ne contribue pas non plus à stimuler les efforts stratégiques d'efficacité de l'atténuation. C'est la raison pour laquelle la visibilité fournie par une solution XDR est si importante.

Le fait d'accroître la visibilité globale des organisations sur les événements permet de passer à une approche Zero-Trust globale de la cybersécurité. En combinant toutes les données de télémétrie au sein d'une plateforme unique, les organisations peuvent faciliter l'analyse et la détection rapides des menaces actives en temps quasi réel.

Les disponibilités varient selon les zones géographiques. © 2023 Secureworks, Inc. Tous droits réservés.

3. Éliminer les frictions, maximiser la valeur.

Les équipes de sécurité sont moins efficaces si elles doivent attendre la réponse ou l'assistance d'un fournisseur. Le regroupement de données de télémétrie provenant de différentes sources leur fait également perdre un temps précieux. Lorsque ces équipes n'ont pas accès à un emplacement unifié pour enquêter et rechercher l'« aiguille dans la botte de foin », ces facteurs peuvent se cumuler et tous les efforts devenir désordonnés, coûteux et, vous l'aurez deviné, inefficaces.

Ce n'est que par l'intégration, l'unification des données et l'analyse automatisée à grande échelle que les équipes peuvent optimiser leur processus de chasse aux menaces, de recherche de menaces et d'atténuation. Quand elle est soutenue par des avancées techniques telles que l'automatisation, la moindre décision peut améliorer l'efficacité technique et humaine et, au final, générer de véritables gains de valeur stratégique.

4. Identifier la bonne combinaison de fonctions de sécurité.

Compte tenu de la pénurie de personnel de sécurité et du manque d'homogénéité entre les nombreuses solutions de sécurité existantes, il est essentiel que les organisations puissent identifier la bonne combinaison de solutions et de services de sécurité pour atteindre leurs objectifs en matière d'efficacité de l'atténuation. Dans les faits, la plupart des organisations ont du mal à retenir les compétences et l'expertise suffisantes en matière de sécurité pour pouvoir utiliser efficacement la technologie EDR, sans parler d'une plateforme MDR.

Avec une solution MDR sur une plateforme ManagedXDR ouverte, les organisations peuvent moduler avec précision la combinaison d'expertise interne et de complément de ressources, en tirant parti de l'expertise et des services de sécurité à la demande pour combler les lacunes au fur et à mesure. Grâce à ce modèle à la demande, vous pouvez étendre directement votre équipe de sécurité en faisant appel à des ressources externes si besoin. Par exemple, si vous souhaitez assurer une petite permanence interne chargée d'intervenir sur les petits incidents, vous voudrez peut-être avoir accès à une équipe de support plus importante en cas d'incidents majeurs.

Une solution MDR sur une plateforme XDR ouverte offre également à votre équipe la possibilité d'exploiter les investissements existants en matière de sécurité en intégrant la cybersécurité dans une seule couverture de défense, tout en optimisant la valeur de ces mêmes investissements. Dans l'idéal, les informations doivent être partagées de manière transparente avec votre équipe, il est donc important pour Secureworks® de donner la priorité à ce type de communications transparentes. Pour finir, une solution MDR assure une surveillance étroite de votre infrastructure informatique 24/7/365, surtout pendant les périodes où la couverture interne peut être réduite.

Les disponibilités varient selon les zones géographiques. © 2023 Secureworks, Inc. Tous droits réservés.

AU-DELÀ DU POINT DE TERMINAISON : UN CHOIX STRATÉGIQUE

Compte tenu du caractère primordial de l'efficacité de l'atténuation, le déploiement d'une solution de détection et réponse étendues revêt une importance stratégique.

Une solution MDR sur une plateforme XDR ouverte est suffisamment souple pour que vous puissiez laisser votre propre équipe gérer les opérations de sécurité, ou bien travailler (si vous faites appel à Secureworks) avec un prestataire de services XDR. Secureworks Taegis™ ManagedXDR fournit une plateforme XDR transparente, partagée et ouverte, parce que c'est ce qu'exige un véritable partenariat de sécurité. Le fait de fournir une solution MDR sur une plateforme XDR est un puissant atout, car :

Une solution MDR sur une plateforme XDR optimise vos investissements EDR actuels

L'approche XDR intègre vos défenses de télémétrie des points de terminaison EDR essentielles dans un modèle de cybersécurité moderne et global spécialement conçu pour gérer et répondre à la nature changeante des vecteurs d'attaque dans votre environnement informatique.

Même si les données de protection des points de terminaison et de télémétrie des points de terminaison sont essentielles, une solution XDR vous permet d'éliminer toute dépendance excessive à l'égard de certains mécanismes de défense spécifiques aux points de terminaison. La nouvelle visibilité et l'approche globale offertes par une solution XDR sont idéales pour aider les organisations à passer à une surveillance étroite et à favoriser un modèle Zero-Trust.

Une solution MDR sur une plateforme XDR intègre et unifie les opérations pour une amélioration immédiate de la sécurité

L'approche XDR associe la télémétrie étendue à l'analyse des menaces d'une manière que les solutions EDR, SOAR, SIEM[6] et MDR ne pourront jamais imiter. Avec une plateforme XDR, il n'est plus nécessaire de passer d'un écran à l'autre comme le font les analystes en sécurité qui utilisent plusieurs outils. Elle offre également une source de diagnostic unique permettant aux équipes de sécurité de collaborer pleinement pour détecter, identifier et contrer les menaces. Ce rythme de collaboration est la clé pour réduire rapidement les impacts négatifs et améliorer le taux d'efficacité de l'atténuation d'une organisation.

Une solution MDR sur une plateforme XDR est le moyen le plus puissant d'améliorer les services et le support

L'approche XDR est le moyen idéal de s'associer à des prestataires de services de sécurité. Cela permet aux organisations d'améliorer leurs résultats en matière de sécurité et de réaliser des économies, tout en utilisant des services complets pour soutenir leurs opérations de cybersécurité.

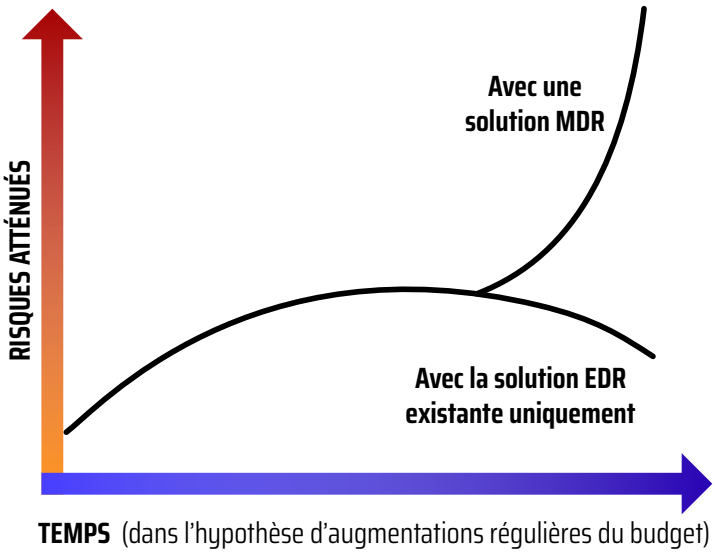
Que l'externalisation soit partielle ou totale, la solidité du partenariat de sécurité est ce qui permet réellement d'améliorer l'efficacité de l'atténuation. Un fournisseur de solutions XDR qui offre une expertise et un support supplémentaires en matière de sécurité dans les domaines de la réponse aux incidents, de la chasse aux menaces, des tests comparatifs, de la gestion des failles de sécurité et d'autres services de cybersécurité importants ne peut que faciliter l'obtention de meilleurs résultats en matière de sécurité.

[6] Source: XDR vs SIEM Choosing the Right Platform

Les disponibilités varient selon les zones géographiques. © 2023 Secureworks, Inc. Tous droits réservés.

Une solution MDR sur une plateforme XDR est déjà disponible !

Depuis toujours, l'un des principaux obstacles à l'amélioration de l'efficacité a été le manque de solutions d'opérations de sécurité, et il existe actuellement peu de solutions MDR éprouvées et établies sous forme de plateforme XDR ouverte. Ce n'est plus le cas. Avec Secureworks Taegis ManagedXDR, une plateforme de sécurité développée sur la base de plus de 20 ans d'expérience en matière de gestion SOC, les organisations peuvent être opérationnelles en moins de 30 jours.



Une solution MDR sur une plateforme XDR permet aux équipes de sécurité d'améliorer en permanence les mesures d'atténuation des cybermenaces les plus graves, tout en respectant la plupart des contraintes budgétaires et humaines existantes.

UNE SOLUTION MDR SOUS FORME DE SOLUTION XDR : L'AVENIR EN MATIÈRE D'EFFICACITÉ

L'amélioration de l'efficacité de l'atténuation de votre organisation est désormais à portée de main. Les responsables qui adoptent une solution MDR sur une plateforme XDR pour leur cybersécurité peuvent bénéficier des avantages suivants :

1. Détection des cybermenaces et défense contre les cybermenaces plus efficaces à grande échelle, allant au-delà du point de terminaison
2. Workflows de réponse aux incidents/événements plus rapides que ceux des processus existants
3. Réduction de la dépendance vis-à-vis des rares experts en matière de cybersécurité
4. Amélioration de l'accès à une expertise et à des services de qualité dans le domaine de la cybersécurité

Les disponibilités varient selon les zones géographiques. © 2023 Secureworks, Inc. Tous droits réservés.

5. Meilleur soutien à la croissance et à l'agilité de l'organisation
6. Modalités plus favorables des assurances contre les cyber-risques
7. Amélioration de la productivité du personnel de sécurité existant
8. Plus grande visibilité de la sécurité dans l'ensemble de l'infrastructure informatique
9. Consolidation des outils de sécurité par une meilleure compréhension des besoins et de la valeur
10. Très peu de lacunes en matière de sécurité grâce à l'unification et à l'intégration des outils et des technologies

La seule constante en matière de cybersécurité est l'évolution : l'évolution des menaces, des technologies et de votre approche pour être en mesure de combattre efficacement les adversaires auxquels vous êtes confronté chaque jour. Lorsque la présence numérique de votre organisation s'étend aux quatre coins du monde et que les menaces peuvent venir de n'importe où, vous devez résoudre le problème de l'efficacité à grande échelle. Pour cela, vous devez vous préparer à faire face aux réalités d'aujourd'hui et aux défis de demain en matière de cybersécurité.

Pour résoudre ces problèmes d'efficacité à grande échelle, vous aurez besoin d'une solution MDR sous forme de plateforme XDR comme élément central de votre stratégie, avec des services de gestion avancés en option si nécessaire. Un prestataire de services XDR fiable peut vous apporter une valeur ajoutée supérieure à celle que vous avez connue avec les solutions précédentes, grâce à la plateforme XDR testée et éprouvée qui constitue l'épine dorsale de ses solutions de détection et réponse managées.

Contactez Secureworks si vous souhaitez vous entretenir avec un expert qui pourra vous présenter la valeur réelle et le taux d'efficacité de l'atténuation que vous pouvez obtenir avec une solution MDR sous forme de plateforme XDR.

Les disponibilités varient selon les zones géographiques. © 2023 Secureworks, Inc. Tous droits réservés.

Secureworks®

Secureworks® (NASDAQ : SCWX) est un leader mondial de la cybersécurité qui protège l'évolution de ses clients au moyen de Secureworks® Taegis™, une plateforme d'analytique de la sécurité Cloud native reposant sur plus de 20 ans d'expérience dans le domaine de la recherche et de veille sur les menaces. Les clients peuvent ainsi mieux détecter les menaces avancées, rationaliser les investigations, collaborer plus efficacement et automatiser la mise en œuvre des mesures appropriées.

SIÈGE SOCIAL

États-Unis
1 Concourse Pkwy NE #500
Atlanta, GA 30328
+1 877 838 7947
www.secureworks.com

EUROPE ET MOYEN-ORIENT

France
8 avenue du Stade de France
93218 Saint Denis Cedex
+33 1 80 60 20 00

Allemagne
Main Airport Center,
Unterschweinstiege 10 60549
Frankfurt am Main Germany
069/9792-0

Royaume-Uni
One Creechurch Place,
1 Creechurch Ln
London EC3A 5AY
United Kingdom
+44(0)207 892 1000

1 Tanfield
Edinburgh EH3 5DA
United Kingdom
+44(0)131 260 3040

Émirats arabes unis
Building 15, Dubai Internet City
Dubai, UAE PO Box 500111 00971 4
420 7000

ASIE-PACIFIQUE

Australie
Building 3, 14 Aquatic Drive
Frenchs Forest, Sydney NSW
Australia 2086
1800 737 817

Japon
Otemachi One Tower 17F
2-1 Otemachi 1-chome, Chiyoda-ku
Tokyo 100-8159, Japan
81-3-4400-9373
www.secureworks.jp

Les disponibilités varient selon les zones géographiques. © 2023 Secureworks, Inc. Tous droits réservés.