Enterprise Strategy Group | Getting to the bigger truth.™

LIVRE BLANC ESG

Détection et réponse managées : pour une croissance rapide du programme de sécurité

Par Dave Gruber, Principal Analyst

Août 2022

Ce livre blanc ESG a été réalisé à la demande de Dell Technologies et est diffusé avec l'autorisation de TechTarget, Inc.

Sommaire

Résumé

Face à l'accélération de la transformation numérique, à l'adoption rapide du Cloud, au paysage des menaces plus complexe et à la pénurie continue de compétences en sécurité, les équipes de sécurité atteignent leurs limites. Les solutions de sécurité actuelles ne parviennent pas à suivre le rythme, ce qui oblige nombre d'entre elles à hiérarchiser les initiatives de modernisation du SOC pour repenser les technologies et les processus. Les mégatendances du secteur autour du Zero-Trust ainsi que de la détection et de la réponse étendues (XDR) offrent une nouvelle vision. Cependant, beaucoup ont du mal à implémenter ces stratégies ou à en exploiter des implémentations efficaces. Les services de détection et de réponse managées (MDR) soulagent les équipes, en apportant à de nombreuses organisations le personnel, les processus et les technologies nécessaires pour consolider leurs programmes de sécurité dans cet environnement agité.

Introduction

Forcées de consacrer une part de leurs pensées et de leur budget au risque de plus en plus élevé que constituent les cyberattaques, au lieu de les consacrer aux objectifs métier essentiels, les organisations doivent répondre en renforçant les programmes de cybersécurité. Certaines peuvent créer leur programme de sécurité entièrement avec des ressources internes, mais la plupart ont besoin de ressources tierces pour permettre une croissance et une évolutivité rapides du programme.

Les opérations de sécurité (SecOps), responsables de la surveillance et de la protection de tous les aspects de la surface d'attaque numérique, sont au cœur de tous les programmes de cybersécurité. Face aux quantités croissantes de données de télémétrie et d'alertes de sécurité liées aux SecOps, qui englobent le réseau, les points de terminaison, le Cloud, les identités, les applications et les données, les organisations atteignent leurs limites. Nombre d'entre elles se tournent donc vers des prestataires de services MDR.

Ceux-ci sont devenus un mécanisme essentiel pour ces organisations. Ils fournissent un large éventail d'offres de services de sécurité, comme la réponse aux incidents, la surveillance 24 h/24, la gestion des programmes et la gestion des risques. Selon l'étude d'Enterprise Strategy Group (ESG), les services MDR sont devenus un composant standard des stratégies de cybersécurité modernes pour les organisations de toutes tailles, quelle que soit leur maturité en matière de sécurité.

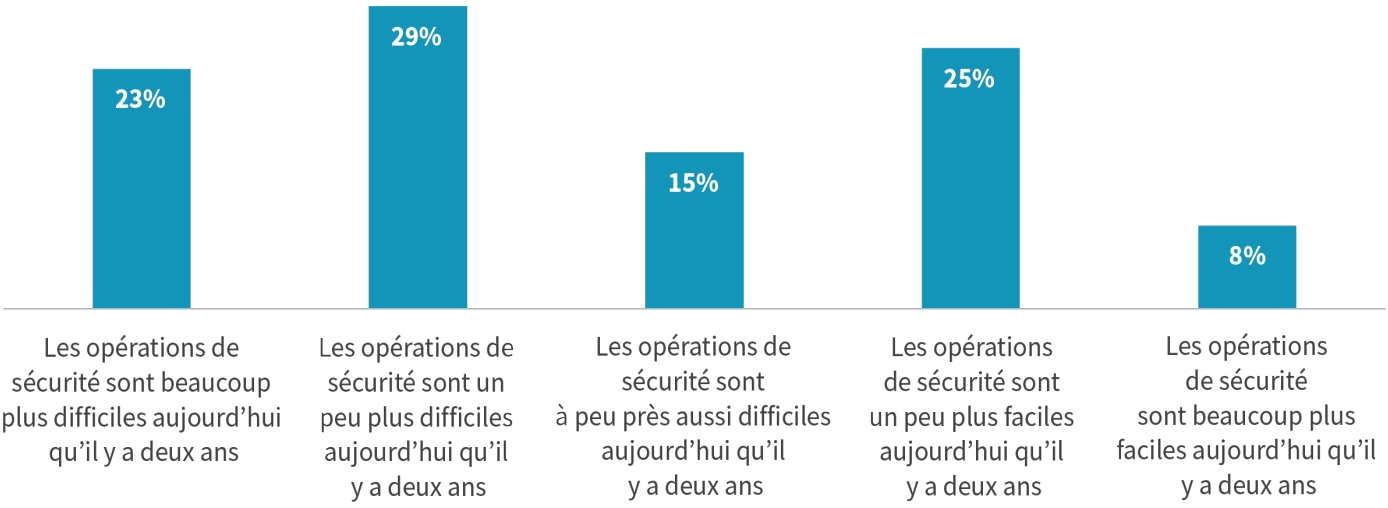
Défis croissants liés aux opérations de sécurité

Selon l'étude d'ESG (voir Figure 1), la plupart des organisations reconnaissent que l'ensemble du scénario SecOps est plus difficile aujourd'hui qu'il y a deux ans.[1]

[1] Source : ESG Complete Survey Results, *SOC Modernization and the Role of XDR*, août 2022. Sauf indication contraire, toutes les références et tous les graphiques ESG présentés dans ce livre blanc proviennent de cet ensemble de résultats d'enquête.

Figure 1. Plus de la moitié estiment que les SecOps sont plus difficiles

Parmi les réponses suivantes, laquelle reflète le mieux votre opinion sur les opérations de sécurité au sein de votre organisation ? (Pourcentage de personnes interrogées, N = 376)

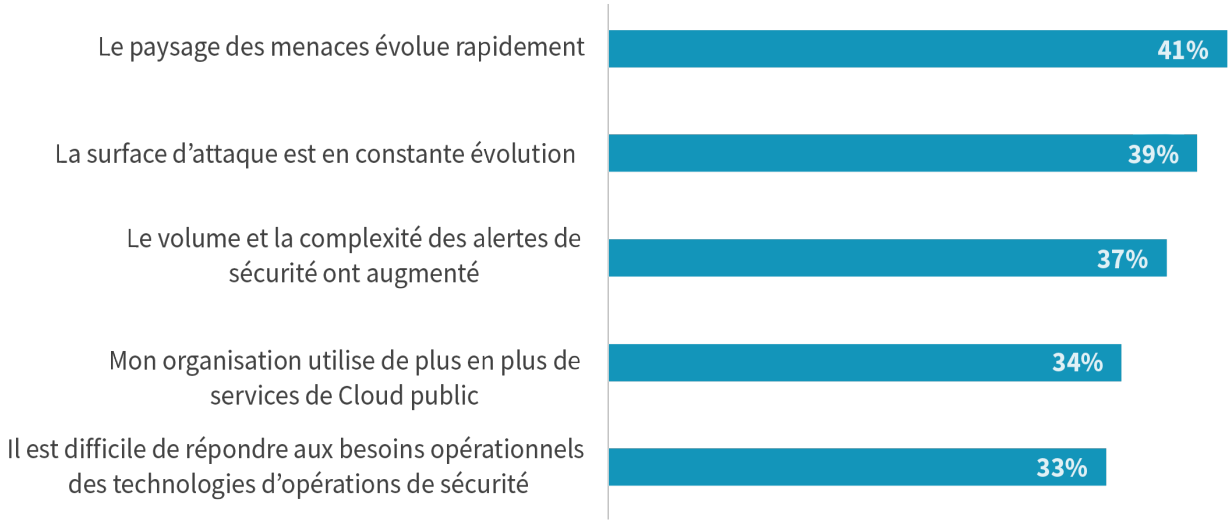


Source : ESG, une division de TechTarget, Inc.

Comme le montre la Figure 2, l'étude d'ESG met également en évidence d'autres défis qui rendent la détection et la réponse plus difficiles que jamais. Il s'agit notamment de l'extension de la surface d'attaque, de la croissance et la diversité du paysage des menaces, et de l'utilisation croissante des services Cloud pour un plus large éventail d'applications et de cas d'utilisation.

Figure 2. Cinq principales raisons pour lesquelles les SecOps sont plus difficiles

Vous avez indiqué que les opérations de sécurité étaient plus difficiles au sein de votre organisation qu'il y a deux ans.Quelles sont les principales raisons pour lesquelles vous pensez cela ? (Pourcentage de personnes interrogées, N = 194, plusieurs réponses possibles)



Source : ESG, une division de TechTarget, Inc.

Modernisation des programmes de détection et de réponse

La taille et la complexité des surfaces d'attaque et du paysage des menaces ont augmenté, tout comme l'utilisation de contrôles de sécurité, générant des milliers d'alertes et de grandes quantités de données de sécurité. Pour pouvoir trier les alertes et incidents et mener l'enquête, les équipes de sécurité doivent agréger, mettre en corrélation et analyser ces données, ce qui nécessite souvent un nombre incalculable de processus manuels. Mais la capture et l'analyse des alertes et des données de sécurité ne suffisent pas.

Les équipes de sécurité repensent les opérations globales du programme afin de mieux intégrer les données sur les ressources et les risques des équipes informatiques et de direction opérationnelle, le but étant de se concentrer sur les menaces qui représentent le plus de risques pour les objectifs organisationnels. Par exemple, le vol d'informations d'identification pour l'administration de domaine peut avoir de nombreux impacts négatifs potentiels sur les opérations, les finances et la réputation de l'organisation, à court et à long terme.

À mesure que les responsables de la sécurité reconsidèrent leurs stratégies, de plus en plus d'organisations délèguent les activités opérationnelles quotidiennes à des tiers, car cela leur permet de réorienter les ressources internes vers des activités de sécurité plus stratégiques. Les ressources de sécurité internes se concentrent ainsi sur la réorganisation des processus d'opérations de sécurité, tandis que les prestataires de services MDR gèrent la détection, le tri des incidents et la réponse apportée, en prenant rapidement des mesures pour prévenir les dommages et limiter les disruptions métier opérationnelles potentielles.

D'autres organisations se tournent vers les fournisseurs MDR pour obtenir des conseils sur le développement global du programme. L'intervention d'experts et les processus d'opérations de sécurité éprouvés permettent d'optimiser les résultats.

Tandis que le mouvement XDR crée une vision et une feuille de route des éléments nécessaires pour moderniser les programmes de détection et de réponse, d'autres font appel à des fournisseurs MDR pour aider à la mise en œuvre de solutions de qualité XDR.

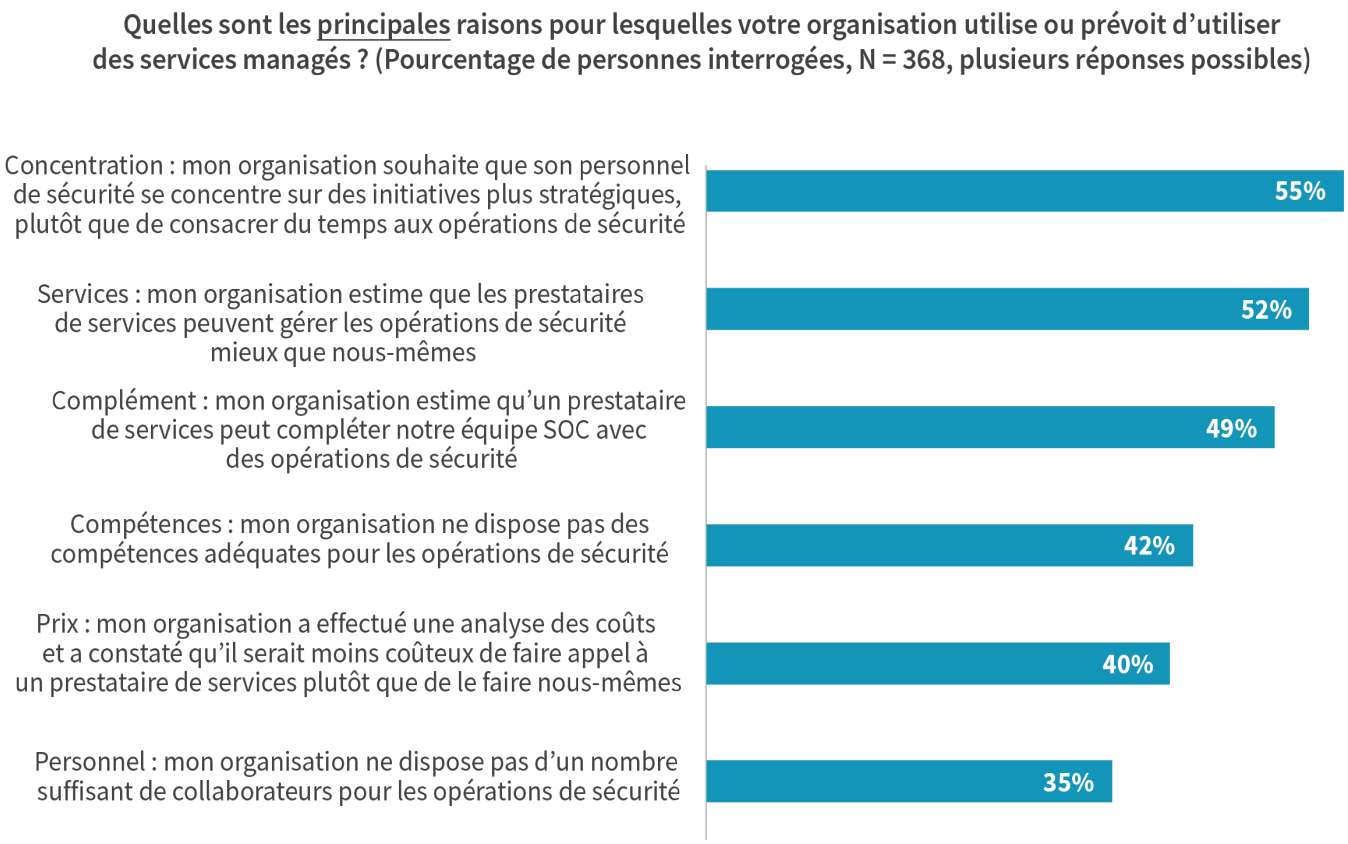
Cas d'utilisation MDR

De nombreux fournisseurs MDR proposent un large éventail de services de sécurité, mais les services de détection et de réponse de base, visant à surveiller, trier les alertes et mener l'enquête, sont souvent le point de départ des engagements précoces. Les modèles opérationnels varient selon les fournisseurs MDR. Les responsables de la sécurité doivent donc choisir un fournisseur MDR capable de répondre à leurs objectifs spécifiques, en fonction de leurs besoins organisationnels individuels. Par exemple, certains responsables de la sécurité choisissent de sous-traiter toutes leurs opérations de sécurité, en faisant appel à un fournisseur MDR qui propose une couverture complète de la surface d'attaque, la surveillance des menaces et des mesures correctives. Dans ce modèle, les fournisseurs MDR fournissent souvent le package technologique, les processus et les experts en sécurité nécessaires. Pour d'autres organisations, les services MDR sont une extension de leur fonction d'opérations de sécurité interne, et apportent une couverture en dehors des heures de bureau ou des experts en sécurité supplémentaires à l'équipe interne, principalement responsable du package technologique et du processus opérationnel. Ce ne sont que deux exemples des nombreux cas d'utilisation où les services MDR sont utilisés.

La solution MDR n'est donc pas universelle. Il s'agit souvent d'un ensemble personnalisable de fonctionnalités qui peuvent être répondre aux besoins d'une organisation individuelle.

Différentes organisations choisiront un partenaire MDR pour différents aspects de la détection et de la réponse, en fonction de leurs ressources et compétences internes. L'étude d'ESG explore les principales raisons dans la Figure 3.

Figure 3. Pourquoi les organisations choisissent des partenaires MDR



Source : ESG, une division de TechTarget, Inc.

Principaux moteurs de valeur pour l'engagement MDR

Le développement d'un programme de sécurité nécessite de prêter une attention particulière à l'efficacité. Les services MDR peuvent avoir un impact positif dans ce domaine.

- Amélioration et efficacité opérationnelles. La solution MDR peut aider les organisations à réduire le coût total des opérations de sécurité de plusieurs manières, comme l'infrastructure, le personnel et la gestion. Elle peut également résoudre le problème de « fatigue liée aux alertes » et augmenter les probabilités que les faux positifs soient considérablement réduits.

- Amélioration de l'efficacité de la cybersécurité et réduction des risques. La solution MDR peut aider les organisations à stopper les menaces déjà en cours, à améliorer la détection des menaces potentielles et des attaques avancées persistantes, à favoriser une chasse aux menaces proactive et à renforcer les contrôles, afin d'identifier et de prévenir les futures attaques.

Caractéristiques à rechercher chez un fournisseur de solutions MDR moderne

Gardez à l'esprit que les solutions MDR, en général, ne sont pas nouvelles. Elles sont même présentes depuis un certain temps et ont de bons antécédents en matière de réussite. Cependant, de nombreuses solutions MDR de « génération 1.0 » ont été conçues et implémentées à une autre époque : moins de données, moins de menaces, détection plus simple. La nouvelle génération de solutions MDR, ainsi que les tiers qui les déploient et les gèrent, doit prendre en compte un ensemble de défis plus vaste, profond et complexe, qui rend la détection et la réponse plus importantes et difficiles que jamais.

Lorsqu'elles étudient des solutions MDR, les organisations doivent rechercher les fonctionnalités suivantes :

- La surveillance 24x7 des événements et des journaux, pour apporter des informations rapides et à visibilité élevée sur les activités suspectes et les alertes par volume, emplacement et type.
- La surveillance continue et évolutive du réseau, et l'analyse des menaces.
- Des recommandations basées sur l'IA pour les options de réponse contextuelle.
- La création de rapport sur la conformité aux normes.
- Des conseillers en sécurité « humains » en contact direct avec les équipes internes.
- Une analyse détaillée et en temps réel basée sur la détection des menaces, le tri, les procédures d'enquête et les analyses approfondies.
- Des évaluations, la hiérarchisation et des conseils sur l'atténuation des failles de sécurité.

Face au grand nombre de prestataires de services potentiels qui peuvent fournir une partie, la plupart, voire la totalité des fonctionnalités MDR sous-traitées, les organisations doivent rechercher des partenaires capables de fournir les fonctions suivantes :

- Une intelligence sur les menaces contextuelle.
- Une télémétrie riche.
- Une expérience éprouvée dans la zone géographique, le marché vertical et le profil réglementaire de l'organisation.
- Des capacités démontrées en matière de chasse aux menaces.
- Un engagement à long terme en faveur d'une solution MDR basée sur le Cloud, avec des fonctionnalités étendues dans les environnements multi-Cloud et de Cloud hybride, le Zero-Trust et le modèle de responsabilité partagée de la sécurité du Cloud.
- Une capacité éprouvée à faire évoluer leur service au fil du temps, avec une technologie innovante, des processus éprouvés et une expertise démontrée par ses collaborateurs.

L'approche de Dell Technologies en matière de MDR

L'approche de Dell Technologies en matière de détection et de réponse managées associe des technologies flexibles, intelligentes et évolutives à des professionnels de la cybersécurité expérimentés. Son service basé sur abonnement est conçu pour offrir aux organisations à la fois une prévisibilité des coûts et une transition fluide vers un niveau de service supérieur, si nécessaire.

La plate-forme technologique du service de détection et de réponse managées de Dell est Taegis XDR, un service Cloud natif entièrement managé développé par Secureworks, une société Dell Technologies. Taegis XDR détecte, analyse et traite les menaces entièrement vérifiées sur une surface d'attaque distribuée et diversifiée. Cette solution aide ainsi à protéger les organisations, qu'il s'agisse de grandes sociétés mondiales ou de petites entreprises.

La puissance de Taegis XDR est optimisée par l'expertise et les compétences d'un grand groupe d'analystes et d'ingénieurs de sécurité Dell, dont les connaissances collectives couvrent des décennies d'expertise. La solution contribue ainsi à protéger les organisations contre les menaces connues ou encore inconnues. Cette combinaison offre un moyen efficace d'unifier la détection et la réponse dans l'ensemble de l'architecture informatique, en grande partie grâce à la base de données d'intelligence sur les menaces mise à jour en continu. Le service de détection et de réponse managées de Dell surveille, analyse et identifie également les comportements malveillants afin de réduire le temps moyen de détection et de réponse.

Configuré et déployé en tant que service managé basé sur un abonnement, Dell Managed Detection and Response réduit considérablement le besoin pour les organisations de rechercher et de recruter des professionnels de la sécurité pour gérer plus de menaces, d'attaques et d'alertes. Dell Managed Detection and Response complète et étend efficacement les capacités internes d'une organisation. Par conséquent, le personnel SecOps interne peut consacrer plus de temps et d'énergie à d'autres tâches liées à la sécurité.

Exemples de réussite : fonctionnement concret de la solution MDR

ESG a interrogé des responsables IT et de sécurité de clients Dell MDR afin d'obtenir des informations sur des cas d'utilisation, des modèles opérationnels et des résultats spécifiques.

Exemple 1 : administrations locales de taille moyenne

Les ressources informatiques et de cybersécurité des administrations locales sont rarement comparables à celles de leurs homologues du secteur privé, mais peuvent pourtant être confrontées aux mêmes types de problèmes. Dans cet exemple, un comté de taille moyenne dans un État du sud-ouest des États-Unis a eu des difficultés à faire face au nombre croissant de menaces de sécurité, tout en respectant un budget strict.

Lors de son embauche, le nouveau directeur informatique a immédiatement identifié le paysage croissant des menaces auxquelles sa petite équipe faisait face, et a perçu les failles de sécurité potentielles dans leurs capacités de détection et de réponse. « Notre posture de sécurité n'était pas à la hauteur, mais nous devions réussir à étendre nos capacités sans augmenter le budget, un sujet très sensible pour les décideurs, a-t-il déclaré. Mais je sais que je peux les rassurer concernant ces limites budgétaires tout en soulignant la nécessité de résoudre nos failles de sécurité. »

Il a d'abord voulu évaluer le fournisseur de sécurité des points de terminaison responsable du comté, qui vantait alors une « évaluation gratuite » de 90 jours des mises à niveau logicielles pour améliorer la détection et la réponse. Mais, en constatant que le logiciel ne répondait pas aux besoins du comté et que les communications du fournisseur n'étaient pas à la hauteur, le directeur informatique a décidé d'opter pour une solution MDR plus complète.

« Heureusement, nous avions mis en place un accord pour que Dell fournisse un CSO (directeur de la sécurité) virtuel. Les responsables du comté pouvaient ainsi percevoir les avantages liés à l'utilisation d'une approche de services managés de détection et de réponse. » Il a ajouté que l'équipe Dell avait complété la petite équipe interne de professionnels de la sécurité et de l'informatique du comté, au lieu de la remplacer. « C'était une extension de notre équipe, et ils ont collaboré avec nous de manière très fluide. »

L'avantage concret apporté par l'arrangement est devenu évident lorsqu'une campagne de piratage mondiale a ciblé la messagerie Web Microsoft Exchange, une plate-forme populaire utilisée par un large éventail d'organisations, y compris le comté. « Microsoft a développé et envoyé un correctif une fois l'attaque détectée, mais celle-ci avait probablement été lancée un mois plus tôt », a déclaré le directeur informatique du comté. « Nous avons été contactés par notre CSO virtuel Dell en dehors des heures de bureau, et l'équipe Dell MDR est intervenue. Elle nous a envoyé des scripts pour vérifier les serveurs et nous avons rapidement découvert que l'un d'entre eux était compromis. »

« Dell et ses partenaires Secureworks savaient vraiment ce qu'ils faisaient. Nous avons échangé deux ou trois appels par jour, tous les jours, tant que nous avons été confrontés à la tentative de violation. » Il a ajouté que l'équipe de réponse aux incidents avait passé en revue ses conclusions avec le personnel du comté, en lui montrant des extraits de code et d'autres indications sur la tentative de violation, ainsi que la preuve de la compromission.

Enfin, l'équipe a fourni un certain nombre de recommandations techniques et non techniques qui ont non seulement traité l'impact potentiel de la tentative de violation, mais ont également renforcé le profil de cybersécurité du comté, sur une portée et une durée supérieures.

« Notre expérience nous a montré que, pour bénéficier d'une détection et d'une réponse améliorées, la bonne solution consiste à trouver un expert MDR fiable, éprouvé et de confiance qui a déjà été confronté à ces situations, plutôt que d'essayer de trouver un moyen économique de mettre à niveau le logiciel EDR », a-t-il déclaré. « Pendant la tentative de violation, mais aussi lors des collaborations régulières avec l'équipe, je me souviens de cette sensation rassurante d'avoir à nos côtés les bonnes personnes pour nous aider à nous protéger. »

Exemple 2 : district scolaire de taille moyenne

Les districts scolaires ont toujours sous-investi dans l'informatique en général et dans la cybersécurité en particulier. Mais, face à la hausse des attaques de ransomware et autres cyberattaques visant les districts scolaires, les responsables locaux de l'enseignement public se sont efforcés de trouver des moyens plus efficaces, fiables et abordables de se protéger contre les failles de sécurité.

Par exemple, un district scolaire des États-Unis de taille moyenne a été attaqué par un ransomware et toutes ses opérations axées sur la technologie ont été mises à l'arrêt. Avec 8 500 étudiants et du personnel répartis sur 21 sites, le district avait mis en place un profil informatique aux dimensions raisonnables, avec 100 serveurs physiques et 63 serveurs virtuels supplémentaires, connectés à plus de 11 000 appareils utilisés par les étudiants et le personnel. De toute évidence, ce district présentait de nombreux points d'entrée potentiels pour les acteurs malveillants et avait besoin d'un partenaire capable d'agir rapidement.

Après avoir déterminé que l'attaque par ransomware était bien réelle et qu'elle devait être traitée immédiatement, l'équipe informatique du district scolaire a contacté Dell Managed Detection and Response. « Au deuxième jour de l'attaque, 10 collaborateurs de chez Dell étaient présents chez nous », se souvient le directeur informatique du district. « Nous avons développé une relation de confiance étroite avec l'équipe Dell, qui a pris les commandes immédiatement. »

Heureusement, le résultat net a été positif pour le district. « Sur plus de 6 millions de fichiers présents sur nos systèmes, nous n'en avons perdu que six », a indiqué le directeur informatique. « Et nous n'avons même pas dû verser la rançon à l'auteur de la menace. Nous sommes un exemple concret montrant qu'il est possible de survivre aux ransomware et de poursuivre notre travail en toute sécurité. »

« Notre collaboration avec Dell a été une expérience positive. Notre analyste de sécurité sur site est toujours satisfait après avoir discuté avec les collaborateurs de Dell et nous avons une position 95 % plus efficace depuis que nous travaillons avec Dell sur la détection et la réponse managées. »

Ce qu'il faut retenir

Forcées de consacrer une part de leurs pensées et de leur budget au risque de plus en plus élevé que constituent les cyberattaques, au lieu de les consacrer aux objectifs métier essentiels, les organisations doivent renforcer les programmes de cybersécurité. Les cas d'utilisation varient, mais la plupart font appel à des prestataires de services MDR pour faire évoluer leurs programmes.

Les prestataires de services MDR offrent un moyen de surmonter de nombreux défis reconnus dans la création d'un programme de sécurité efficace, avec notamment des experts en sécurité, des processus éprouvés et des technologies de sécurité évolutives et faciles à déployer.

Dell Technologies a mis en place un ensemble étroitement intégré de technologies, d'experts en sécurité expérimentés et de pratiques d'excellence pour aider les organisations à détecter les menaces et à y répondre en temps quasi réel. Comme nous l'avons vu dans les études de cas de ce livre blanc, Dell Technologies a aidé un large éventail d'organisations, issues de différents secteurs et possédant différents profils de ressources, à éviter l'impact des menaces émergentes dans toute l'entreprise.

Enterprise Strategy Group est une entreprise intégrée d'analyse, de recherche et de stratégie technologiques qui fournit des données relatives aux marchés, des renseignements exploitables et des services de commercialisation à la grande communauté informatique.

www.esg-global.com contact@esg-global.com 508.482.0188