Enterprise Strategy Group | Getting to the bigger truth.™

LIVRE BLANC D'ESG

Détection et réponse managées (MDR) : une voie vers une croissance rapide de programmes de sécurité

Par Dave Gruber, analyste principal

Août 2022

Ce livre blanc d'ESG a été commandé par Dell Technologies et est distribué avec l'autorisation de TechTarget, inc.

Table des matières

Résumé

L'accélération de la transformation numérique, l'adoption rapide de l'infonuagique, un environnement de menaces plus complexe et un manque continu de compétences en matière de sécurité repoussent les limites des équipes de sécurité. Les solutions de sécurité actuelles ne sont pas en mesure de suivre le rythme, ce qui oblige plusieurs équipes à établir des priorités pour les initiatives de modernisation des centres des opérations de sécurité (COS) pour restructurer les technologies et les processus. Les tendances globales de l'industrie autour du modèle Zero Trust et de la détection et de l'intervention étendues (XDR) offrent une nouvelle approche. Toutefois, beaucoup d'organisations ont du mal à mettre en œuvre des stratégies efficaces. Les services de détection et de réponse managées (MDR) offrent des solutions sous forme de personnel, de procédés et de technologie nécessaires à la mise en place des programmes de sécurité des organisations dans cet environnement tourmenté.

Introduction

Alors que le risque croissant de cyberattaques dommageables détourne l'attention et le budget des objectifs commerciaux principaux, les organisations doivent agir en renforçant leurs programmes de cybersécurité. Pour certaines, la mise en place d'un programme de sécurité à partir de ressources internes est possible, mais pour la plupart, des ressources tierces sont nécessaires pour accélérer la croissance et l'évolution du programme.

Les opérations de sécurité sont au cœur de tous les programmes de cybersécurité et sont responsables de la surveillance et de la protection de tous les aspects de la surface d'attaque numérique. Le réseau, les extrémités, le nuage, l'identité, les applications, les données, la télémétrie de sécurité et les alertes de plus en plus fréquentes associées aux opérations de sécurité poussent les équipes au-delà de leurs limites, ce qui a forcé de nombreuses organisations à se tourner vers des fournisseurs de services de MDR pour obtenir de l'aide.

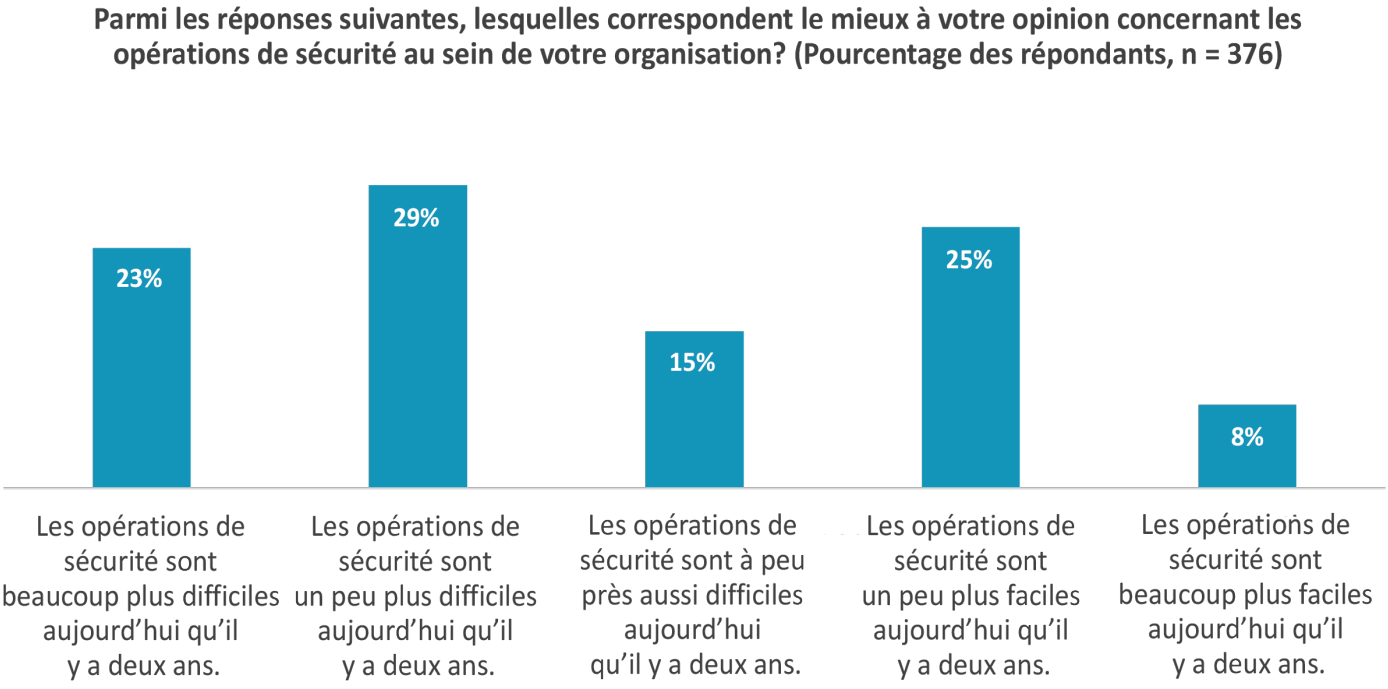
Les fournisseurs de services de MDR sont devenus essentiels pour ces organisations grâce à une offre de services de sécurité, comme la réponse aux incidents, la surveillance en tout temps, la gestion du programme et la gestion des risques. Une étude d'Enterprise Strategy Group (ESG) indique que les services de MDR sont devenus une composante grand public des stratégies de cybersécurité modernes pour les organisations de toutes tailles et tout niveau de maturité en matière de sécurité.

Défis croissants en matière d'opérations de sécurité

Selon une étude d'ESG (voir la figure 1), la plupart des organisations reconnaissent que la situation des opérations de sécurité est plus difficile à l'heure actuelle qu'il y a deux ans.[1]

[1] Source : Résultats du sondage complet d'ESG, *SOC Modernization and the Role of XDR*, août 2022. Toutes les références et tous les graphiques d'ESG contenus dans ce livre blanc ont été tirés de cet ensemble de résultats du sondage, sauf indication contraire.

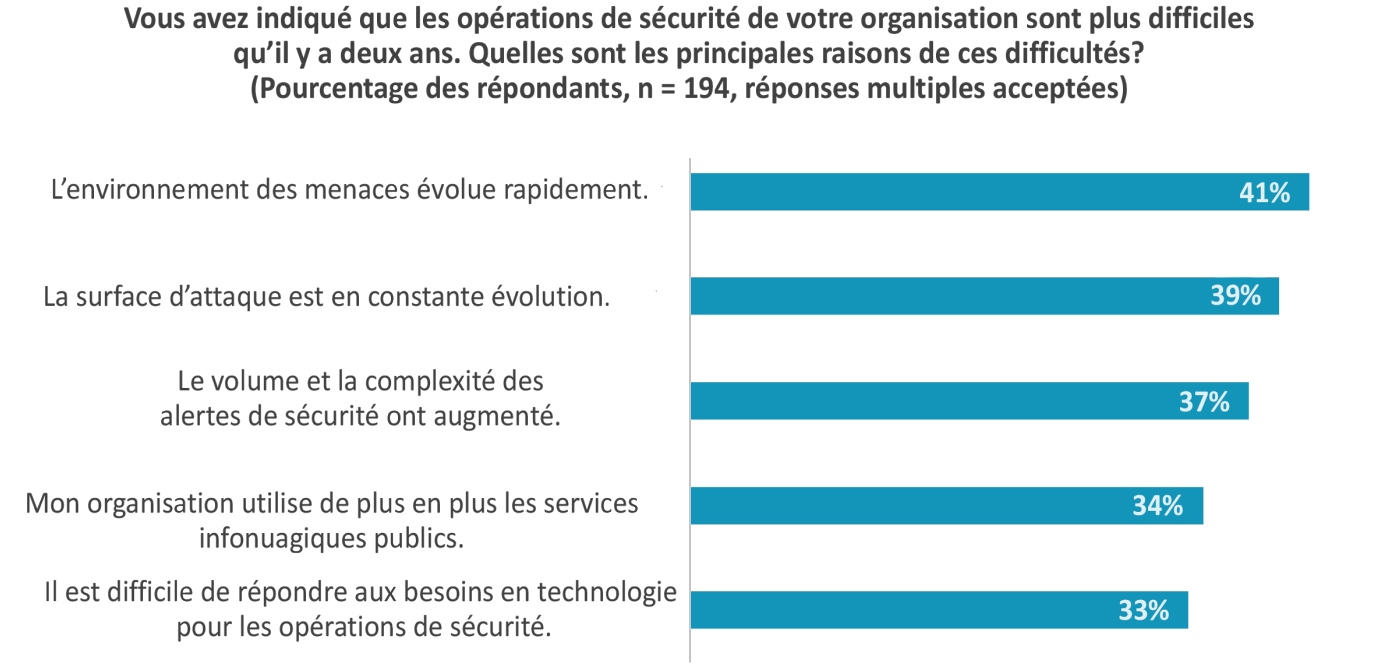
Figure 1. Plus de la moitié des personnes pensent que les opérations de sécurité sont plus difficiles



Source : ESG, une division de TechTarget, inc.

Comme l'indique la figure 2, l'étude d'ESG souligne également d'autres défis qui rendent la détection et la réponse plus difficiles que jamais, comme la surface d'attaque en pleine expansion, la croissance et la diversité de l'environnement des menaces et l'utilisation fulgurante de services infonuagiques pour un plus large éventail d'applications et de cas d'utilisation.

Figure 2. Les cinq principales raisons pour lesquelles les opérations de sécurité sont plus complexes



Source : ESG, une division de TechTarget, inc.

Modernisation des programmes de détection et de réponse

Les surfaces d'attaque et l'environnement des menaces sont devenus plus vastes et plus complexes, tout comme l'utilisation d'un plus grand nombre de contrôles de sécurité, qui génère des milliers d'alertes et des quantités considérables de données de sécurité. Afin de procéder au triage et à l'enquête des alertes et des incidents, les équipes de sécurité doivent regrouper ces données, établir une corrélation entre celles-ci et les analyser, ce qui exige souvent un traitement manuel immense. Toutefois, d'autres mesures s'imposent en plus de la collecte et de l'analyse des alertes et des données de sécurité.

Les équipes de sécurité revisitent l'ensemble des opérations du programme afin d'y inclure davantage de données sur les actifs et les risques provenant des TI et du secteur, afin de se concentrer sur les menaces qui posent le risque le plus important pour les objectifs organisationnels. Par exemple, le vol d'identifiants d'administration de domaine peut causer de nombreux effets néfastes sur les opérations, les finances et la réputation de la marque de l'organisation à court et à long terme.

Comme les gestionnaires de sécurité revoient leurs stratégies, de plus en plus d'organisations déchargent leurs activités opérationnelles quotidiennes vers de tierces parties pour réorienter leurs ressources internes vers des activités de sécurité plus stratégiques. Alors que les ressources de sécurité internes se concentrent à la réorganisation des processus d'opérations de sécurité, les fournisseurs de services de MDR gèrent la détection, le triage et l'intervention des incidents, en prenant des mesures rapides pour prévenir les dommages et limiter les perturbations opérationnelles potentielles.

D'autres s'intéressent aux fournisseurs de MDR pour obtenir des conseils sur l'élaboration générale du programme, la recherche d'experts et sur des processus d'opérations de sécurité éprouvés afin d'optimiser les résultats.

Et alors que le mouvement de XDR offre une vision et une feuille de route pour ce qu'il faut pour moderniser les programmes de détection et de réponse, d'autres organisations cherchent à tirer parti des fournisseurs de MDR pour aider à la mise en œuvre de solutions de calibre XDR.

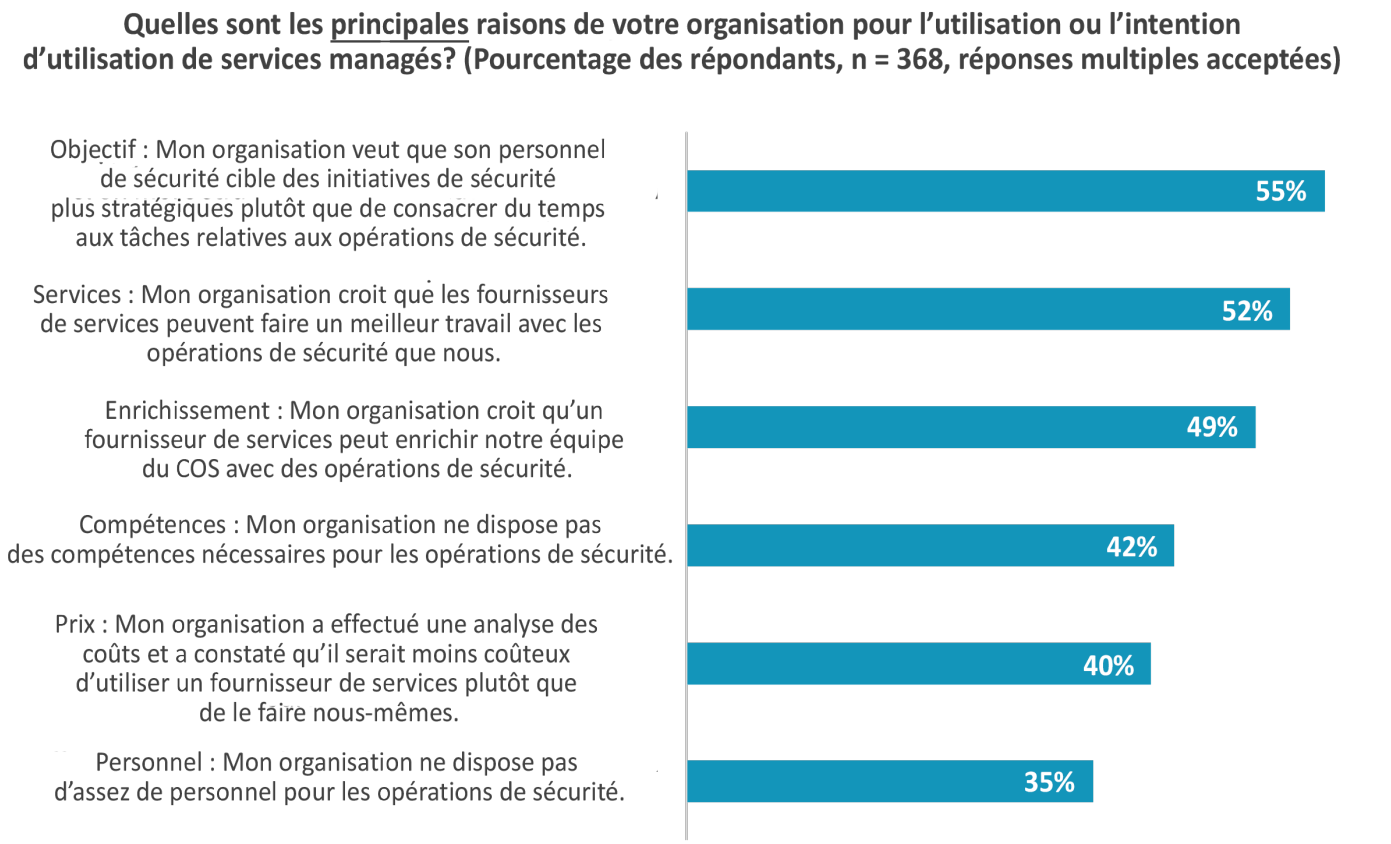
Cas d'utilisation de MDR

Bien que de nombreux fournisseurs de MDR offrent un large éventail de services de sécurité, les services de détection et de réponse de base qui surveillent et trient les alertes et enquêtent sont souvent à la base du processus. Les modèles opérationnels varient entre les fournisseurs de MDR; ainsi, les gestionnaires de sécurité doivent harmoniser soigneusement leurs exigences organisationnelles individuelles avec celles d'un fournisseur de MDR qui peut atteindre leurs objectifs propres. Par exemple, certains gestionnaires de sécurité confient toutes leurs opérations de sécurité à des personnes externes, en s'engageant avec un fournisseur de MDR pour offrir une couverture complète de la surface d'attaque, la surveillance des menaces et la remise en état. Dans ce modèle, les fournisseurs de MDR offrent souvent la gamme de technologie, les procédés et les experts en sécurité nécessaires à la prestation du service. Pour d'autres, les services de MDR sont un prolongement d'une fonction interne d'opérations de sécurité, avec l'ajout d'une couverture en dehors des heures de bureau ou des experts en sécurité supplémentaires à une équipe interne principalement responsable de la gamme de technologie et du processus d'exploitation. Il ne s'agit que de deux exemples des nombreux cas d'utilisation des services de MDR.

Les MDR n'est donc pas une solution unique. Il s'agit plutôt d'un ensemble de capacités à personnaliser qui peuvent être appliquées aux besoins individuels d'une organisation.

Différentes organisations choisiront un partenaire de MDR pour différents aspects de détection et de réponse, selon leurs ressources et leurs compétences internes. L'étude d'ESG explore les principales raisons derrière ce choix à la figure 3.

Figure 3. Pourquoi les organisations choisissent-elles des partenaires de MDR?



Source : ESG, une division de TechTarget, inc.

Principales motivations pour l'engagement envers les MDR

L'élaboration du programme de sécurité doit se consacrer à la fois sur l'efficacité et le rendement, et les services de MDR peuvent fournir une incidence positive sur ces deux aspects.

- Amélioration et efficacité opérationnelles. Les MDR peuvent aider les organisations à réduire le coût total des opérations de sécurité de plusieurs façons, comme l'infrastructure, le personnel et la gestion. Elle peut également résoudre le problème de « désensibilisation aux alarmes » et favoriser la réduction significative de fausses alertes.

- Amélioration de l'efficacité de la cybersécurité et réduction des risques. Les MDR peuvent aider les organisations à arrêter les menaces déjà en cours, à améliorer la détection des menaces et des attaques persistantes avancées, à lancer la chasse proactive aux menaces et à renforcer les contrôles pour déceler et prévenir les attaques futures.

Que rechercher auprès d'un fournisseur de solutions de MDR modernes?

Gardez à l'esprit que les solutions de MDR, en général, ne sont pas nouvelles. En fait, elles existent depuis un certain temps et ont démontré un bon bilan de réussite. Toutefois, de nombreuses solutions de MDR de « génération 1.0 » ont été conçues et mises en œuvre à une autre époque : moins de données, moins de menaces, avec une détection plus simple. La prochaine génération de solutions de MDR et les tierces parties qui les déploient et les gèrent doivent tenir compte d'un ensemble de défis plus vastes, plus graves et plus complexes qui rendent la détection et la réponse plus importantes et plus difficiles que jamais.

Lorsqu'elles réfléchissent à des solutions de MDR, les organisations doivent rechercher les fonctionnalités suivantes :

- Surveillance 24 heures sur 24, 7 jours sur 7 des événements et des fiches journalières, avec des renseignements rapides et à haute visibilité sur les activités suspectes et les alertes par volume, emplacement et type.
- Surveillance du réseau continue et évolutive et analyse des menaces.
- Recommandations basées sur l'IA pour les options de réponse aux menaces.
- Rapports de conformité légale.
- Conseillers en sécurité « humains » en communication directe avec les équipes en interne.
- Analyse détaillée et en temps réel basée sur la détection, le triage, l'enquête et l'aspect légal des menaces.
- Des évaluations de vulnérabilité, une hiérarchisation et des conseils de réduction.

Lorsque les organisations tiennent compte du grand nombre de fournisseurs de services potentiels qui peuvent offrir certaines, la plupart ou même toutes les fonctionnalités de MDR sous-traitées, elles doivent être à la recherche de partenaires pouvant fournir les services suivants :

- Renseignements sur la surveillance des menaces.
- Télémétrie riche.
- Antécédents éprouvés en matière de zone de couverture géographique, de marché vertical et de profil réglementaire de l'organisation.
- Capacités démontrées de chasse aux menaces.
- Engagement à long terme envers les MDR infonuagiques, avec des capacités étendues dans les environnements multinuages et de nuage hybride, le modèle Zero Trust et le modèle de responsabilité partagée de la sécurité infonuagique.
- Capacité éprouvée à faire évoluer leur service au fil du temps, grâce à une technologie novatrice, des processus éprouvés et une expertise démontrée par ses employés.

L'approche de Dell Technologies quant aux MDR

L'approche de Dell Technologies en matière de détection et de réponse managées combine des technologies flexibles, intelligentes et évolutives, ainsi que des professionnels expérimentés en cybersécurité. Son service par abonnement est conçu pour offrir aux organisations une prévisibilité des coûts et un changement harmonieux vers un niveau supérieur de service, si nécessaire.

La plateforme technologique pour la détection et la réponse managées de Dell est Taegis XDR, un service infonuagique entièrement géré et développé par Secureworks, une entreprise commerciale de Dell Technologies. Taegis XDR détecte et analyse des menaces entièrement contrôlées, en plus d'agir contre celle-ci sur une surface d'attaque distribuée et

diversifiée pour aider à protéger toutes les organisations, des grandes entreprises mondiales aux entreprises relativement petites.

La force de Taegis XDR est renforcée par l'expertise et les compétences du vaste groupe d'analystes et d'ingénieurs en sécurité de Dell dont les connaissances collectives représentent des décennies d'expertise, qui aident à protéger les organisations contre les menaces connues, mais également celles 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 sa base de données de surveillance des menaces continuellement mise à jour. La détection et la réponse managées de Dell surveillent, analysent et décèlent les comportements d'attaque, ce qui réduit le temps de détection et de réponse.

Configuré et déployé en tant que service managé par abonnement, le service de détection et de réponse managées de Dell réduit considérablement le besoin des organisations de rechercher et de recruter des professionnels de la sécurité pour gérer davantage de menaces, d'attaques et d'alertes. Le service de détection et réponse managées Dell complète et étend les capacités internes d'une organisation de manière efficace. Par conséquent, le personnel interne des SecOps peut consacrer plus de temps et d'énergies à d'autres tâches liées à la sécurité.

Témoignages de réussite : Fonctionnement des MDR dans le monde réel

ESG a discuté avec des gestionnaires des TI et de sécurité des clients du service de MDR de Dell pour obtenir des renseignements sur des cas d'utilisation spécifiques, des modèles opérationnels et des résultats.

Exemple n° 1 : Administration municipale de taille moyenne

Les ressources des administrations municipales en matière de TI et de cybersécurité correspondent rarement à celles de leurs homologues du secteur privé, mais cela ne signifie pas qu'elles ne sont pas confrontées aux mêmes problèmes. Dans cet exemple, un comté de taille moyenne dans un État du sud-ouest des États-Unis éprouvait des difficultés à faire face au nombre croissant de menaces en matière de sécurité, mais aussi à maintenir ses dépenses dans des limites strictes.

Lorsqu'un nouveau directeur des TI a été embauché, il a immédiatement identifié l'environnement des menaces grandissant auquel sa petite équipe faisait face et il a décelé des vulnérabilités potentielles dans leurs capacités de détection et d'intervention. « Notre position en matière de sécurité n'était tout simplement pas à la hauteur, mais nous devions étendre nos capacités sans augmenter la masse salariale, un sujet très délicat pour les décideurs, a-t-il affirmé. Mais je sais que je pourrais faire valoir leurs préoccupations en matière de frugalité budgétaire tout en soulignant la nécessité de remédier à nos vulnérabilités. »

Il a d'abord tenté d'évaluer le fournisseur de sécurité des extrémités actuel du comté, qui offrait un « essai gratuit » de 90 jours sur les mises à niveau logicielles afin d'améliorer la détection et la réponse. Mais, en constatant que les logiciels manquaient certaines fonctionnalités adaptées à leurs besoins et que les communications du fournisseur ne répondaient pas aux attentes, il a choisi une solution de MDR plus complète.

« Heureusement, nous avions une entente pour que Dell fournisse un agent de sécurité en chef virtuel, de sorte que les gestionnaires du comté étaient au courant des avantages d'une approche axée sur les services managés, soit la détection et la réponse dans ce cas-ci. » Il a ajouté que l'équipe Dell complétait la petite équipe interne de professionnels de la sécurité et des TI en place dans le comté, plutôt que de la remplacer. « Elle représentait plutôt une extension de notre équipe et a travaillé de façon transparente à nos côtés. »

Les avantages réels de l'entente sont rapidement devenus évidents lorsqu'une campagne mondiale de piratage a ciblé le courriel Microsoft Exchange, une plateforme populaire utilisée par de nombreuses organisations, y compris le comté. « Microsoft a développé et envoyé un correctif dès qu'il a découvert l'attaque, mais elle avait probablement été lancée

un mois avant, a indiqué le directeur des TI du comté. Notre agent de sécurité en chef virtuel de Dell nous a contactés en dehors des heures d'ouverture et l'équipe Dell MDR s'est regroupée. Elle nous a envoyé des scripts pour vérifier le serveur et nous avons rapidement découvert qu'un des serveurs avait été compromis.

Dell et ses partenaires Secureworks savaient vraiment ce qu'ils faisaient. Nous avons reçu deux ou trois appels par jour, sur une base quotidienne, tout au long de la période de traitement de la tentative d'accès non autorisé. » Il a ajouté que l'équipe d'intervention en cas d'incident a fait le point sur ses conclusions avec le personnel du comté, en lui montrant des extraits de code et d'autres indications de la tentative d'accès non autorisé et la preuve du compromis.

Enfin, elle a fourni un certain nombre de recommandations techniques et non techniques qui ont non seulement abordé l'incidence potentielle de la tentative d'accès non autorisé, mais ont également renforcé le profil de cybersécurité du comté avec une perspective et dans un délai élargis.

« Notre expérience nous a montré que trouver un spécialiste de MDR fiable et expérimenté qui a déjà abordé ce genre de problème est la voie à suivre, plutôt que d'essayer de trouver une façon bon marché de mettre à niveau le logiciel EDR, a-t-il affirmé. Je retiens simplement le doux sentiment de confiance que nous ressentons de savoir que nous avons une bonne équipe qui travaille pour assurer notre sécurité, non seulement durant la tentative d'accès non autorisé, mais également en travaillant avec eux sur une base régulière. »

Exemple n° 2 : District scolaire de taille moyenne

En général, les districts scolaires ont toujours sous-investi dans les TI et particulièrement dans la cybersécurité. Mais avec la hausse des attaques par logiciel de rançon et d'autres cyberattaques contre les districts scolaires, les responsables locaux de l'éducation publique ont mis au point des moyens de protection de meilleure qualité, plus fiables et abordables contre les vulnérabilités.

Par exemple, un district scolaire de taille moyenne aux États-Unis a été attaqué par un logiciel de rançon, et toutes ses opérations technologiques ont été interrompues. Avec 8 500 étudiants et employés dans 21 établissements, le district disposait d'un profil informatique raisonnablement dimensionné comprenant 100 serveurs physiques et 63 serveurs virtuels, connectés à plus de 11 000 appareils pour les étudiants et le personnel. De toute évidence, ce district possédait de nombreux points d'entrée potentiels pour les contrevenants et avait besoin d'un partenaire capable d'agir rapidement.

Après avoir déterminé que l'attaque par rançongiciel était réelle et qu'elle devait être résolue immédiatement, l'équipe informatique du district scolaire a communiqué avec le service de détection et réponse managées de Dell. « Le deuxième jour de l'attaque, 10 employés de Dell étaient sur place, se souvient le directeur des TI du district. Nous avons entretenu une relation de confiance avec l'équipe Dell, qui a assumé ses responsabilités immédiatement. »

Heureusement, le résultat net a été positif pour le district. « Sur plus de 6 millions de fichiers dans nos systèmes, nous n'en avons perdu que six, a indiqué le directeur des TI. Nous n'avons même jamais payé l'agent des menaces. Nous sommes un exemple concret de survivants de rançongiciel qui a pu poursuivre ses activités en toute sécurité.

Travailler avec Dell a été une expérience positive. Notre analyste de la sécurité sur place est toujours satisfait après avoir parlé avec les employés de Dell, et nous obtenons aujourd'hui une amélioration de 95 % depuis que nous travaillons avec la détection et la réponse managées de Dell. »

La grande vérité

Alors que les risques croissants de cyberattaques dommageables détournent l'attention et le budget des objectifs commerciaux principaux, les organisations doivent renforcer leurs programmes de cybersécurité. Bien que les cas d'utilisation varient, la plupart des fournisseurs de services de MDR s'appuient sur ceux-ci pour développer et renforcer leurs programmes.

Les fournisseurs de services de MDR offrent une façon de surmonter plusieurs des défis reconnus en matière de création d'un programme de sécurité réussi, y compris des experts en sécurité, des procédés éprouvés et des technologies de sécurité évolutives et faciles à déployer.

Dell Technologies a rassemblé une gamme étroitement intégrée de technologies, d'experts en sécurité expérimentés et de pratiques exemplaires pour aider les organisations à détecter et à répondre aux menaces en temps quasi réel. Comme l'indiquent les études de cas dans ce livre blanc, Dell Technologies a aidé un large éventail d'organisations dans différents secteurs et de différents profils de ressources à atténuer l'incidence des menaces émergentes dans l'ensemble de l'entreprise.

Enterprise Strategy Group est une entreprise intégrée d'analyse technologique, de recherche et de stratégie qui fournit des renseignements commerciaux, des renseignements exploitables et des services de contenu de commercialisation à la communauté informatique mondiale.

www.esg-global.com contact@esg-global.com 508 482-0188