DELL Technologies

LIVRE BLANC

DELL MANAGED DETECTION AND RESPONSE

La solution de sécurité gérée complète pour les PME.

SYNTHÈSE

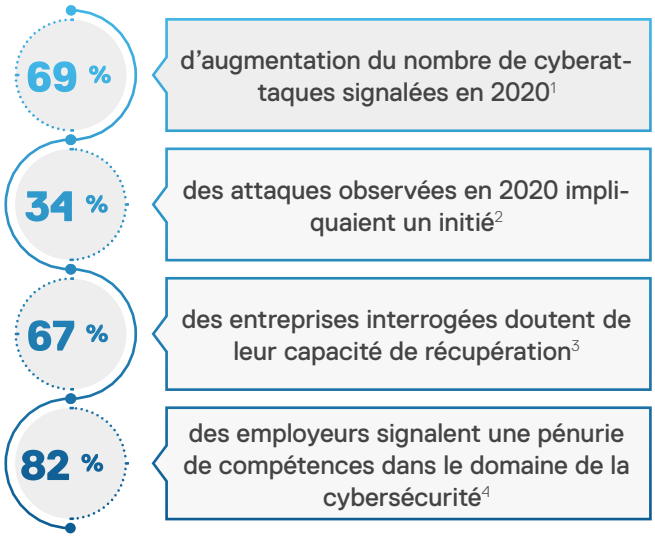
Le nombre de cyberattaques subies par les entreprises est en hausse. En 2021, l'Internet Crime Complaint Center du FBI a constaté une augmentation de 69 % par rapport à l'année précédente, avec un total de 4,2 milliards de dollars américains de pertes[1]. Les attaques ciblant les grandes entreprises font les gros titres, mais en réalité, les entreprises de toutes tailles sont vulnérables. Les petites entreprises, qui ne disposent pas des ressources étendues des grandes entreprises, sont particulièrement vulnérables.

La cybersécurité est essentielle à la protection des ressources de données, des opérations et de la continuité d'activité. Les grandes entreprises disposent souvent d'équipes de sécurité dédiées, dotées des technologies, méthodes et renseignements les plus récents. Toutefois, certaines PME ne disposent que d'un ou deux experts de la sécurité, qui doivent gérer et exploiter des baies de plus en plus complexes d'appliances de sécurité et d'outils logiciels.

Un défi informatique croissant

La prolifération des attaques envers les points de terminaison, les serveurs, les applications, les réseaux et le Cloud génère d'immenses volumes d'alertes, qui surchargent rapidement les équipes informatiques et de sécurité. En parallèle, les auteurs de menaces continuent à faire évoluer leurs techniques et à contourner agilement les défenses autrefois efficaces. Dans les années 2020, une bonne sécurisation des environnements informatiques nécessite une surveillance et une réponse 24x7x365 par des experts dédiés.

Les cyberattaques représentent une menace plus importante que jamais



Si les responsables informatiques des PME allouent suffisamment de personnel et de budget à la cybersécurité, des domaines importants tels que le développement d'applications et le DevOps en pâtiront. Le fait est que la protection contre les auteurs de menaces de maintenant nécessite un investissement dans des talents, des outils et des opérations que de nombreuses organisations ne peuvent tout simplement pas se permettre.

Managed Detection and Response apporte des réponses

Par conséquent, de plus en plus de sociétés envisagent de recourir à des solutions de Managed Detection and Response (MDR) proposées par des prestataires de services externes. Comment les décideurs informatiques peuvent-ils identifier un partenaire MDR exceptionnel ?

Un fournisseur de solutions MDR viable doit implémenter une technologie qui détecte les types de menaces connus, minimise les faux positifs, met en corrélation les événements, suit la séquence d'activité d'un intrus et automatise les actions de maîtrise et de prévention. Le fournisseur a besoin d'une équipe de professionnels de la sécurité hautement qualifiés et expérimentés, capables d'analyser les alertes et de corriger les menaces 24x7x365, ainsi que de rechercher de nouveaux types de menaces.

Principales raisons pour lesquelles les entreprises utilisent des solutions de Managed Detection and Response (MDR)

- **Accès à des spécialistes de la cybersécurité difficiles à trouver**
- **Couverture complète de la surveillance, de la détection et de la réponse**
- **Réduction de la charge de travail du personnel informatique, qui peut ainsi se concentrer sur le DevOps**

La fourniture de services MDR nécessite l'élaboration d'opérations de sécurité et l'établissement et l'affinage des processus. En outre, les analystes ont besoin d'outils de partage des connaissances et de formations régulières pour rester informés sur les dernières menaces et techniques.

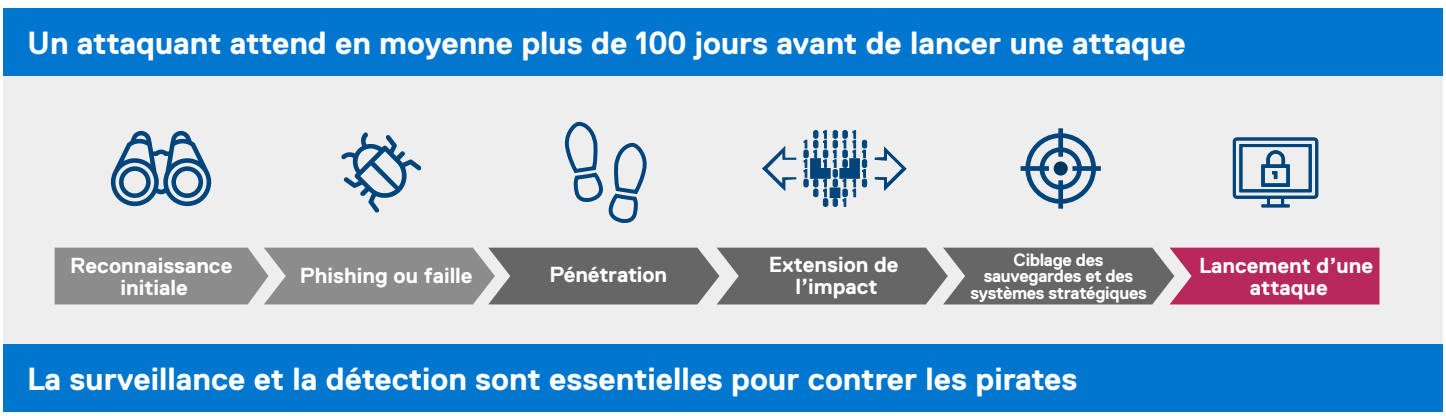
Bien que de nombreux prestataires de services assurent proposer des services de détection et de réponse gérés, seuls quelques-uns disposent de la capacité et des fonctionnalités nécessaires pour atteindre l'excellence.

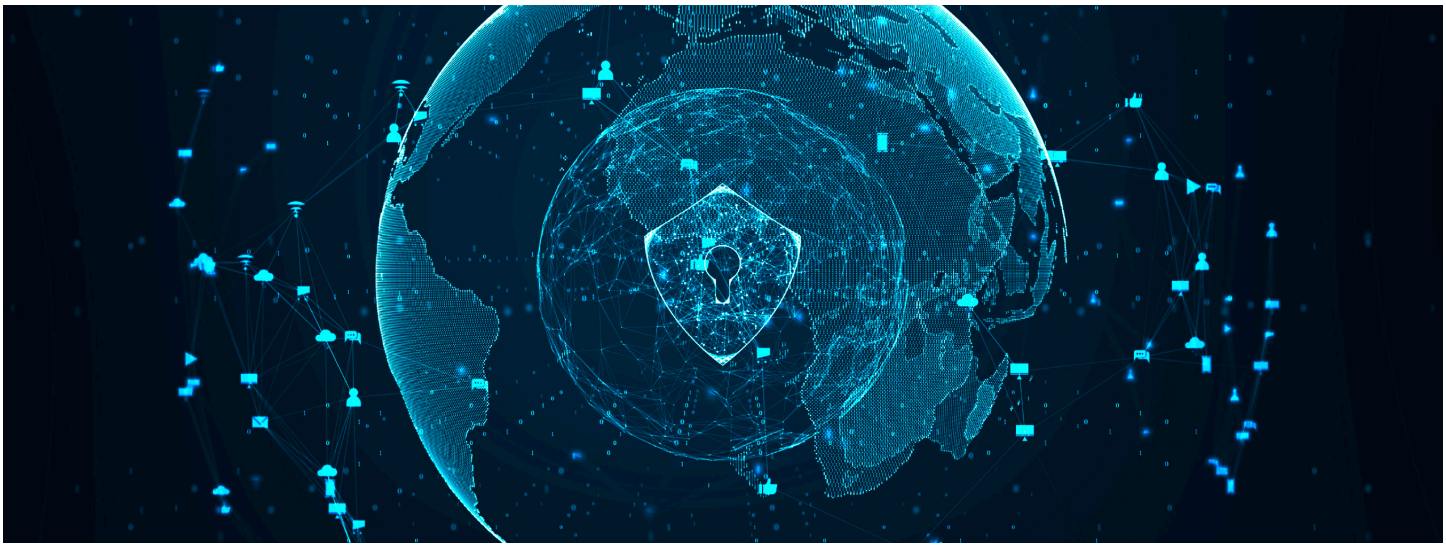
Dell Managed Detection and Response est une solution de bout en bout entièrement gérée, 24x7, qui surveille, détecte, analyse les menaces et y répond dans l'ensemble de l'environnement informatique d'une organisation. Qu'une entreprise compte 50 points de terminaison ou des milliers, la solution Dell MDR améliore rapidement et considérablement sa posture de sécurité, tout en réduisant la charge de travail du personnel informatique. Dell MDR tire parti de la capacité de Dell à investir dans les personnes, les processus et les outils pour fournir aux PME une surveillance et une réponse en matière de cybersécurité à l'échelle de l'entreprise.

ENVIRONNEMENT ACTUEL DES MENACES

Les auteurs de menaces modernes sont méthodiques et passent des semaines ou des mois à étudier la façon dont ils obtiendront l'accès à des applications et des données précieuses. Une fois qu'ils ont identifié une opportunité, ils peuvent exploiter une ouverture ou envoyer des e-mails de phishing pour inciter les utilisateurs à ouvrir une pièce jointe malveillante. La détection et la réponse sont des éléments essentiels d'un programme complet de cybersécurité, de même que la formation des collaborateurs, les évaluations de la cybersécurité, les tests de failles de sécurité et de pénétration, la planification de la résilience et de la récupération, etc.

Figure 1. Stratégie de l'auteur de la menace





Si l'acteur malveillant parvient à accéder au système, il souhaite d'abord établir une base à partir de laquelle élargir le périmètre de l'attaque. Là encore, il prend le temps de consolider ses positions au sein de l'infrastructure de la société. Par exemple, en plus d'attaquer des systèmes de l'entreprise, les attaques par ransomware visent souvent à mettre les systèmes de sauvegarde d'une société hors ligne et à bloquer l'accès aux sauvegardes. Cela peut éliminer la capacité de récupération d'une société, le paiement de la rançon devenant la seule option pour rétablir le bon fonctionnement des opérations.

Des fonctionnalités de détection et de réponse sophistiquées et constamment mises à jour sont essentielles pour reconnaître les attaques et d'autres indices. Un avertissement anticipé permet à l'organisation de réduire les dommages causés par l'attaque avant qu'elle ne se propage davantage.

Les organisations ont déployé un large éventail d'outils de cybersécurité, tels que ceux pour l'audit des mots de passe, les tests réseau, l'analyse des failles de sécurité, le chiffrement, la surveillance et la détection des menaces. Tous ces outils envoient des alertes au département informatique : le volume d'alertes est difficile à gérer, plus encore lorsqu'on sait combien il est complexe de mettre en corrélation les événements entre les outils. En outre, maîtriser en permanence toutes ces technologies représente un investissement considérable en temps de travail pour le personnel de sécurité informatique.

Pourquoi choisir le service Dell Managed Detection and Response

Personnes

- **Experts expérimentés en cybersécurité**
- **Analystes certifiés Taegis XDR**
- **Les certifications incluent également les suivantes : CEH, GIAC SANS, CISSP et CompTIA**

Technologie

- **Plate-forme d'analytique de sécurité Secureworks Taegis XDR leader sur le marché**
- **Surveillance continue des menaces de bout en bout à l'aide de la télémétrie issue d'un large éventail de points de terminaison, du réseau et du Cloud**

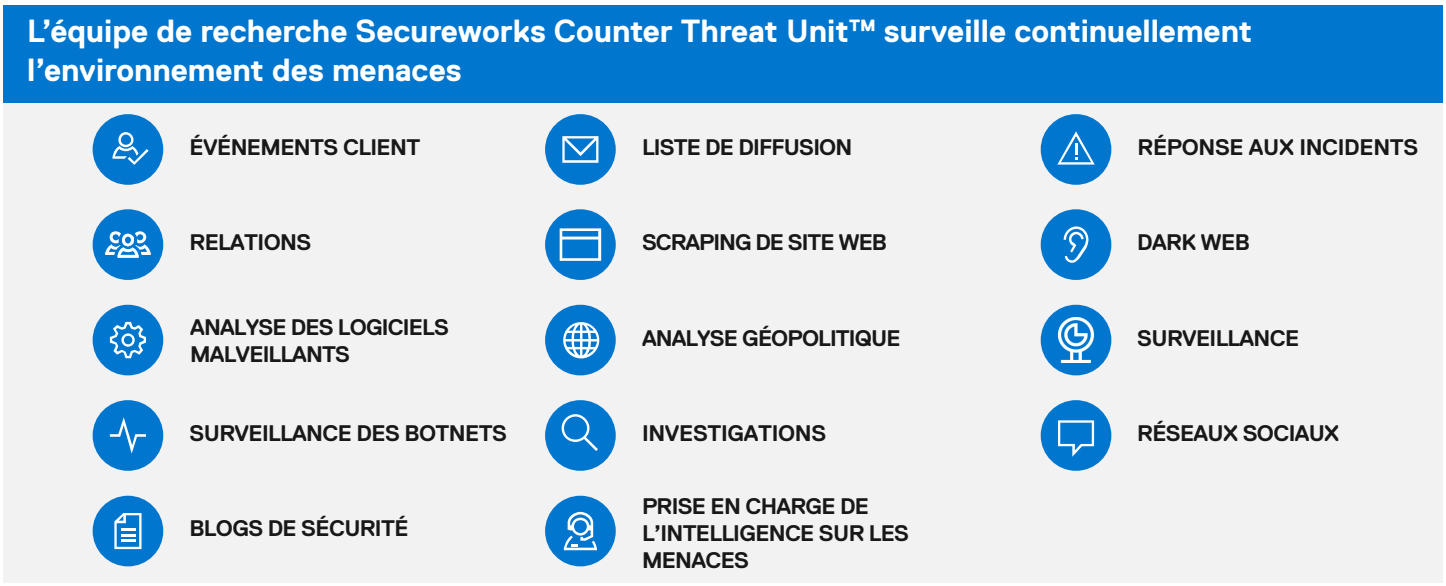
Processus

- **Délai de résolution rapide**
- **Couverture 24x7x365**
- **Assistance au déploiement de l'agent incluse**
- **40 heures par trimestre de conseils sur les mesures correctives à distance**
- **40 heures par an d'interventions pour la réponse aux incidents**

Partenaire de confiance

- **Considéré comme fiable dans le monde entier pour le support des appareils et de l'infrastructure**
- **Plus de 20 ans d'innovation dans la résilience métier**
- **Investissement continu dans le personnel, les processus et les outils**

Figure 2. Intelligence sur les menaces



Le côté humain de l'équation MDR nécessite un groupe de professionnels possédant des années d'expérience et de compétences en matière de cybersécurité, par exemple en administration des systèmes, en cyber-investigation, en enquêtes sur les menaces et en tests de pénétration. Ces professionnels sont difficiles à trouver, coûtent cher à l'embauche et sont constamment recrutés par des organisations plus importantes, capables de dépenser des sommes supérieures. L'enquête State of the CIO 2021 a identifié les postes de cybersécurité comme étant les plus difficiles à pourvoir parmi tous les rôles informatiques[5]. Fidéliser les analystes de sécurité et pourvoir les postes de ceux qui quittent l'entreprise est une bataille sans fin pour les responsables informatiques.

Même après avoir acquis les outils et talents essentiels, les sociétés doivent créer des installations et des opérations de sécurité 24x7.

Les services Dell Managed Detection and Response mettent à votre portée des fonctionnalités de premier niveau

Il n'est pas étonnant que les PME peinent souvent à se défendre correctement. L'environnement de la cybersécurité s'est transformé en un ensemble de menaces en constante évolution. L'avalanche d'activités a augmenté les besoins en personnel et la complexité des attaques a fait monter le niveau des talents requis.

Dell Managed Detection and Response étend les capacités de votre équipe de sécurité avec des experts en cybersécurité, des outils et des fonctionnalités opérationnelles comparables à ceux des très grandes entreprises mondiales. La solution Dell MDR réduit la charge de travail qui pèse sur votre équipe informatique, limite les risques et améliore considérablement la posture de sécurité de votre société, afin que vous puissiez vous concentrer sur les priorités de l'entreprise.

Dell Managed Detection and Response est une combinaison entièrement intégrée de technologies, d'expertise et d'opérations. Ce service s'appuie sur les connaissances des analystes de sécurité Dell Technologies, qui ont passé des années à aider les entreprises du monde entier à mieux protéger leurs opérations. Dell MDR exploite la puissance de Secureworks® Taegis™ XDR, une plate-forme logicielle d'analytique de sécurité avancée qui est le produit de plus de 20 ans de connaissances éprouvées, d'intelligence et de recherches concrètes sur les menaces, et d'une expertise en matière de détection et de réponse aux menaces sophistiquées.

Secureworks Taegis XDR

Secureworks Taegis XDR est une plate-forme de cybersécurité spécialisée qui apporte une solution aux problèmes de sécurité à l'échelle du Big Data. Plate-forme Cloud native, Taegis XDR inclut des évaluations continues, basées sur l'apprentissage automatique et sur le Deep Learning, sur la télémétrie et les événements issus de différents vecteurs d'attaque. Le tout est renforcé par des informations complètes sur les menaces.

Le seul moyen d'identifier les attaques sophistiquées et d'y répondre consiste d'abord à comprendre le fonctionnement et les motivations des acteurs malveillants. Chaque année, l'équipe Secureworks derrière XDR effectue environ 1 000 missions de réponse aux incidents. Elle bénéficie ainsi d'un avantage distinct pour percevoir l'évolution régulière des stratégies, techniques et processus des acteurs malveillants qui parviennent efficacement à entrer dans les entreprises clientes.

Taegis XDR analyse les données pertinentes en matière de sécurité, collectées à partir des points de terminaison, des réseaux, des systèmes Cloud et des systèmes métiers sur site pour détecter les menaces. XDR est une plate-forme entièrement ouverte qui complète l'infrastructure de sécurité existante, en garantissant une couverture complète et en protégeant les investissements précédents.

XDR fournit une réponse, des mesures correctives et des informations automatisées pour améliorer l'efficacité des opérations de sécurité, et offrir aux équipes de réponse la visibilité nécessaire pour prendre des mesures lorsqu'elles sont confrontées à une menace. Les clients Dell MDR bénéficient de l'intelligence sur les menaces issue de centaines de milliers de points de données, compilés entre des clients et des services d'intelligence partagés dans le monde entier.

Intégrez des experts en sécurité à votre équipe

Une équipe mondiale d'analystes de sécurité hautement qualifiés guette en permanence les incidents au sein de vos systèmes. Les experts en cybersécurité qualifiés de Dell sont expérimentés dans toutes les phases de la détection et de l'atténuation des menaces, y compris les enquêtes sur les menaces, la recherche des menaces, la sécurité des points de terminaison, ainsi que la réponse aux incidents et la récupération. Les analystes Dell sont certifiés XDR et disposent de nombreuses autres certifications gouvernementales et reconnues par le secteur, notamment CEH, GIAC OLD SANS, CISSP et CompTIA. Le centre d'opérations de sécurité distribué de Dell MDR fonctionne 24x7x365, en suivant les fuseaux horaires.

L'équipe Dell MDR connaît les opérations et l'infrastructure informatique d'une société. Elle utilise l'apprentissage automatique et des informations sur les menaces soigneusement sélectionnées, issues de milliers d'environnements informatiques et fournies via XDR, pour surveiller votre environnement. L'équipe Dell MDR passe instantanément à l'action en cas d'avertissement : elle mène l'enquête sur les données d'alerte pour découvrir les connexions et les schémas que seuls des analystes de sécurité formés et expérimentés peuvent reconnaître. Elle conseille ensuite les membres de l'équipe de réponse d'une organisation sur la meilleure marche à suivre.

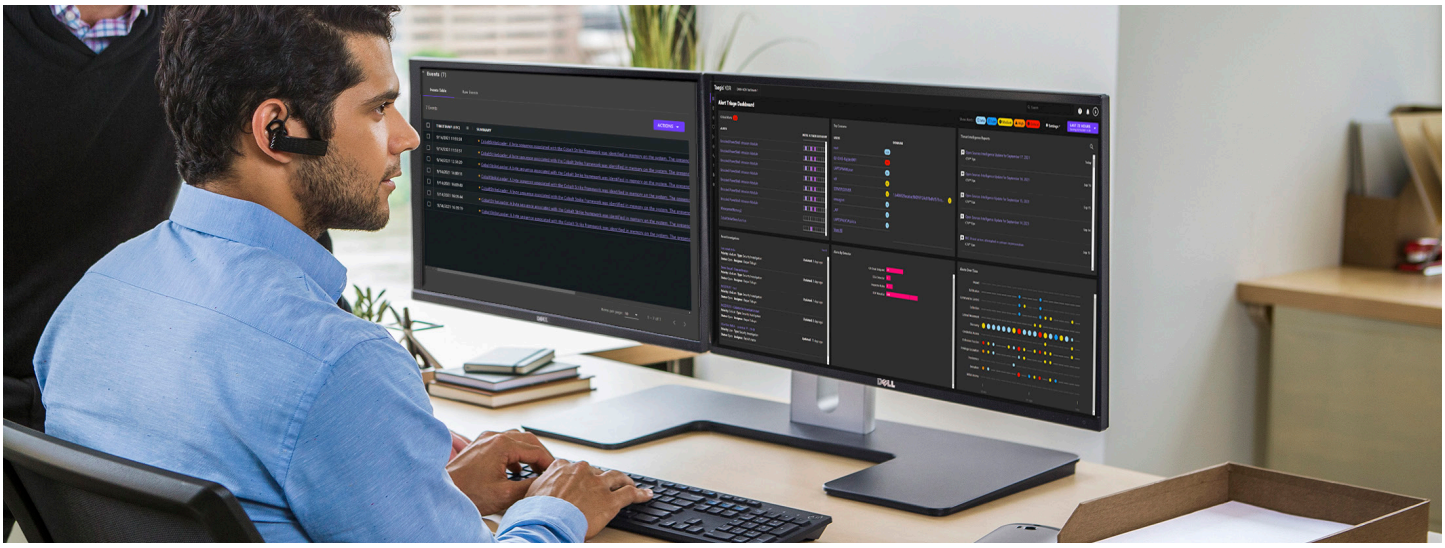
Dell MDR est issue des efforts de Dell sur plusieurs décennies, visant à développer une organisation de services informatiques de classe mondiale. En plus de fournir des conseils exceptionnels pour corriger les menaces, les experts en cybersécurité Dell MDR disposent donc également des compétences et du savoir-faire nécessaires pour les gérer, dans toutes les organisations.

Recherche des menaces : identification des menaces qui peuvent échapper aux systèmes automatisés

Les auteurs de menaces connaissent les systèmes de détection automatisés. Ils développent donc de nouveaux types d'attaque ou de nouvelles variantes de types d'attaque existants, afin de contourner ces systèmes. Avec un système tel que Taegis XDR, l'opération n'est pas aidée, mais reste possible.

Les analystes de sécurité utilisent la recherche des menaces pour identifier ces menaces « furtives ». Cette recherche étudie les indicateurs de compromission, qui peuvent être une série d'échecs de connexion à un compte suivis d'une connexion réussie ; ou des tentatives de connexion anormales, par exemple en dehors des heures de bureau classiques ; ou encore, des modifications répétées apportées à un fichier sur un court laps de temps.

La recherche efficace des menaces résulte de l'association de la technologie et des personnes. La plate-forme Taegis XDR offre une quantité considérable de détails sur l'activité d'un intrus. Les analystes Dell MDR explorent ces détails pour détecter les activités bien cachées.



DÉCOUVREZ DELL MDR

Les médias ont relayé les difficultés des administrations et des entreprises mondiales à contenir les menaces de cybersécurité. Les PME ne sont plus seules face à ce défi. Avec Dell MDR, votre organisation peut bénéficier d'experts en sécurité hautement qualifiés dédiés à votre protection, ainsi que d'une plate-forme de sécurité leader sur le marché, Secureworks Taegis XDR. Votre organisation utilise la capacité de Dell à investir dans des personnes, des processus et des outils pour créer un service de sécurité managé, adapté aux besoins de votre organisation. Le service Dell Managed Detection and Response est une cybersécurité de classe mondiale, accessible à tous.

En savoir plus sur Dell MDR

Contactez l'un de nos experts MDR

1. 69 % d'augmentation du nombre d'attaques enregistrées par le FBI : https://blog.isc2.org/isc2_blog/2021/03/fbi-cybercrime-shot-up-in-2020-amidst-pandemic.html
2. 34 % des attaques impliquaient un initié : https://www.verizon.com/business/resources/reports/dbir/
3. 67 % des entreprises interrogées doutent de leur capacité de récupération après une cyberattaque destructrice : www.delltechnologies.com/gdpi
4. 82 % des employeurs signalent une pénurie de compétences dans le domaine de la cybersécurité : https://www.csis.org/analysis/cybersecurity-workforce-gap
5. 13 most difficult-to-fill IT jobs. https://www.cio.com/article/221772/10-most-difficult-it-jobs-for-employers-to-fill.html

DELL Technologies