Renforcement de votre posture de sécurité avec Managed Detection and Response

Détecter, rechercher et contrer les menaces avancées dans l'ensemble de votre environnement IT

Dell Managed Detection and Response

Associez l'expertise en matière de sécurité et les connaissances approfondies des environnements IT de Dell Technologies aux plateformes d'analyse de la sécurité XDR leaders sur le marché de votre choix.

Quel est le niveau de sécurité de votre entreprise ?

Les équipes informatiques ont du mal à faire face au volume croissant de menaces de sécurité en constante évolution. En 2022, il y a eu 5,5 milliards d'attaques par logiciels malveillants dans le monde, soit 100 millions de plus qu'en 2021[1].

Pour assurer pleinement la protection de votre organisation, il est nécessaire de mettre en place une détection rapide des nouvelles menaces afin d'y répondre efficacement dans l'ensemble de l'environnement. L'utilisation de produits et d'outils ad hoc fragmentant la visibilité et les difficultés à recruter et fidéliser des professionnels de sécurité qualifiés rendent la tâche d'autant plus malaisée, alors même que les équipes informatiques sont déjà entièrement occupées par les demandes stratégiques et les opérations quotidiennes.

Managed Threat Detection and Response

La solution Dell Managed Detection and Response est un service entièrement géré, de bout en bout, 24 heures sur 24 et 7 jours sur 7 qui surveille, détecte, recherche les menaces et les contre sur l'ensemble de l'environnement IT. Cela permet aux organisations disposant d'au moins 50 points de terminaison d'améliorer rapidement et considérablement leur posture de sécurité, tout en réduisant la charge sur le service IT.

Le service repose sur deux atouts principaux :

- L'expertise de Dell Technologies en matière d'analyse de la sécurité, acquise au fil d'années d'expérience passées à aider les organisations du monde entier à mieux protéger leurs activités
- Des plateformes d'analyse de la sécurité, de détection et de réponse étendues (XDR) leaders sur le marché qui intègrent des analyses par IA de la télémétrie et d'événements provenant de plusieurs vecteurs d'attaque.

Principaux avantages :

- Une détection et une réponse unifiées dans l'ensemble de l'écosystème
- La base de données de menaces actualisée en permanence maintient à jour la protection
- Même les tactiques les plus furtives des cybercriminels peuvent être détectées
- Une vue complète de l'activité de bout en bout d'un cybercriminel
- Une équipe de professionnels de la sécurité Dell Technologies experts en sécurité, infrastructure avancée, Cloud, et bien plus
- Une aide d'experts lors de la mise en œuvre du système XDR SaaS Cloud natif
- Une initiation rapide de la réponse aux cyberincidents en cas de faille
- Un alignement en permanence sur le plus haut niveau de conformité de la sécurité pour les prestataire de services

Une solution complète

Les analystes de la sécurité Dell Technologies vous accompagnent dans la configuration initiale, la surveillance, la détection, les mesures correctives et la réponse, le tout à un prix prévisible. Ils travaillent en étroite collaboration avec votre équipe IT pour comprendre votre environnement, vous conseillent sur les améliorations à apporter à la posture de sécurité et vous aident à déployer l'agent logiciel XDR sur les points de terminaison.

Les alertes sont surveillées et examinées 24 heures sur 24, 7 jours sur 7. Si une alerte nécessite une procédure d'enquête, les analystes déterminent et exécutent la réponse appropriée. Si une menace est malveillante ou nécessite votre action, vous êtes informé et, si nécessaire, des instructions étape par étape vous sont fournies.

En cas d'incident de sécurité, Dell Technologies vous aide à lancer le processus de remise en route de votre entreprise.

Choisissez votre plateforme XDR

Vos besoins et préférences en matière de sécurité et de technologie sont uniques. Nous vous donnons la possibilité de choisir parmi trois options leaders sur le marché : Secureworks® Taegis™ XDR, CrowdStrike Falcon® XDR ou Microsoft Defender XDR. Vous pouvez ainsi bénéficier d'une plateforme XDR qui correspond à vos besoins[2].

Principales fonctionnalités

Soutien de confiance

- Une étroite collaboration pour comprendre votre environnement, résoudre les procédure d'enquête et vous conseiller en vue d'améliorer votre posture de sécurité
- Une surveillance 24 heures sur 24 et 7 jours sur 7 grâce aux plateformes XDR de votre choix qui intègrent des analyses par IA de la télémétrie et d'événements provenant de plusieurs vecteurs d'attaque
- Des conseils d'experts pour déployer et configurer la plateforme XDR

Configuration de la réponse aux menaces et de la sécurité

- À l'aide des fonctionnalités XDR, l'équipe Dell SOC automatisera les mesures correctives ou collaborera avec vous afin de traiter les menaces découvertes pendant la surveillance
- Fourniture d'instructions à la fois détaillées et faciles à comprendre pour contenir la menace, même dans des situations complexes
- Jusqu'à 40 heures de configuration de la sécurité liée aux services incluses par trimestre

Détection et procédure d'enquête 24 heures sur 24, 7 jours sur 7

- Des processus et des alertes adaptés à l'environnement de sécurité de votre organisation et automatisés pour assurer l'efficacité de vos opérations quotidiennes
- Une recherche proactive des menaces spécifique à l'environnement de chaque client afin de découvrir de nouvelles menaces ou des variantes de menaces connues qui échappent aux systèmes de sécurité
- Le récapitulatif quotidien des alertes de bas niveau permet à l'équipe Dell SOC de se concentrer sur les alertes stratégiques
- Des rapports trimestriels sur les procédures d'enquête, les analyses sur les tendances d'alertes et les conseils sur la posture de sécurité

Initiation à la réponse aux cyberincidents

- 40 heures d'assistance annuelle de réponse aux incidents à distance qui permettent de débuter rapidement des procédures d'enquête
- Des conseils de nos experts en sécurité certifiés, qui ont aidé des organisations de toutes tailles à effectuer des restaurations à partir d'événements de sécurité graves

Commencez dès aujourd'hui à sécuriser votre environnement avec Dell

Le coût total moyen d'une attaque par ransomware s'élève à 5,13 millions de dollars, soit 13 % de plus qu'en 2022. Il est temps de découvrir si la solution Dell Managed Detection and Response est adaptée à vos besoins[3].

Contactez votre agent commercial Dell dès aujourd'hui.

1. Statista, Annual number of malware attacks worldwide from 2015 to 2022
2. L'utilisation de Microsoft Defender XDR nécessite un minimum de 500 points de terminaison
3. IBM, Cost of a Data Breach Report 2023

Février 2024-NS