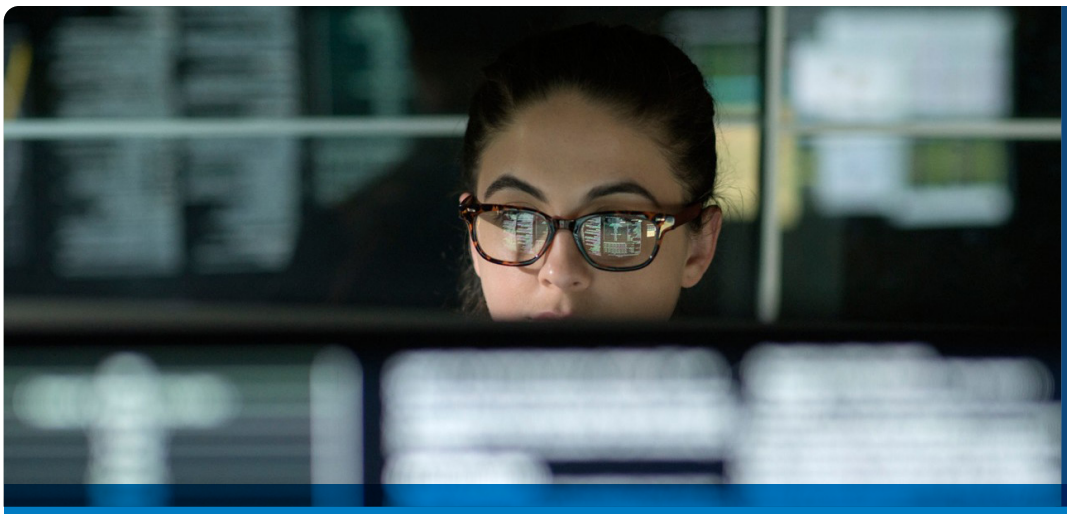
Prévenir et contrer les menaces dans votre environnement IT



Identifier et hiérarchiser les failles de sécurité en vue d'une attention immédiate

Managed Detection and Response Pro

Vulnerability Management et Managed Detection and Response s'allient dans une solution unique pour vous aider à sécuriser votre environnement IT

En 2022, le coût moyen d'une violation de données s'est élevé à 4,35 millions de dollars[1]. En fait, près de 22 000 nouvelles failles de sécurité ont été publiées en 2021, et ce nombre ne cesse d'augmenter[2]. Les organisations doivent trouver un moyen de protéger leur environnement contre le volume croissant de menaces de sécurité et les implications associées à une violation.

La sécurisation de votre environnement IT implique de résoudre les failles de sécurité, d'enquêter sur les menaces et d'y répondre efficacement. Les organisations sont également confrontées au défi de trouver et de garder des professionnels de la sécurité qualifiés, alors que les départements IT se consacrent aux demandes stratégiques et aux opérations métier quotidiennes.

C'est pour ces raisons que nous avons conçu Managed Detection and Response Pro. MDR Pro est une solution entièrement managée qui permet d'identifier et de hiérarchiser les failles de sécurité, mais aussi de détecter et de contrer les menaces 24x7. Nos experts collaborent avec votre équipe de sécurité interne pour sécuriser votre environnement IT, améliorer continuellement votre posture de sécurité et vous préparer à toute éventualité.

Identifier et hiérarchiser les failles de sécurité sur l'ensemble de la surface d'attaque

Les experts de Dell utilisent des technologies de pointe pour analyser votre environnement IT à intervalles réguliers : vous obtenez une vue complète des failles de sécurité sur vos points de terminaison, votre infrastructure réseau et vos ressources Cloud. Les experts de Dell utilisent l'apprentissage automatique pour localiser les failles de sécurité exploitées de manière active chez les utilisateurs et susceptibles d'être ciblées dans un avenir proche. Cela vous aide à hiérarchiser les efforts d'application de correctifs à vos failles de sécurité les plus risquées et à vos ressources stratégiques.

Principaux avantages :

- Maintien de vos défenses à jour avec une gestion et des analyses récurrentes des failles de sécurité
- Vue d'ensemble complète de vos failles de sécurité sur les points de terminaison, l'infrastructure réseau et le Cloud
- Hiérarchisation des failles de sécurité stratégiques à corriger avant qu'elles ne soient exploitées
- Détection et réponse unifiées sur l'ensemble de l'écosystème
- Détection de nouveaux types d'attaques avec une base de données des menaces continuellement mise à jour
- Corrélation d'événements et suivi de l'activité de l'attaquant de bout en bout
- Utilisation des connaissances et de l'expertise de l'équipe de sécurité de Dell

Détecter et contrer les attaques avant qu'un dommage ne se produise

Managed Detection and Response est un service de bout en bout entièrement managé, 24x7, qui surveille, détecte, analyse et contre les menaces dans l'ensemble de l'environnement IT. Les organisations dotées de 50 points de terminaison ou plus peuvent améliorer leur posture de sécurité de manière rapide et significative, touten réduisant la charge de travail du département IT.

Le service repose sur deux principaux atouts :

- 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
- La puissance du logiciel d'analytique avancée de la sécurité XDR (Extended Detection and Response), reposant sur 20 ans de savoir-faire SecOps, l'intelligence et la recherche sur les menaces dans le monde réel, et enfin, l'expérience en matière de détection et de réponse face aux menaces avancées

Principales fonctionnalités

Détection des menaces et investigation

- Accompagnement de partenaires Dell pour comprendre votre environnement et vous aider à déployer l'agent logiciel sur les points de terminaison applicables, sans frais supplémentaires
- Utilisation des données sur les cybercriminels acquises au cours de plus de 1 400 interventions de réponse aux incidents l'année dernière
- Instructions étape par étape pour contenir la menace, même dans des situations complexes
- Jusqu'à 40 heures de conseil incluses par trimestre pour les mesures correctives à distance
- Jusqu'à 40 heures d'assistance annuelle en cas d'incident, à distance, qui permettent d'effectuer rapidement des activités d'investigation

Identification et hiérarchisation des failles de sécurité

- Analyses mensuelles des failles de sécurité, avec des analyses supplémentaires en fonction des conclusions des discussions entre l'équipe Dell et le client
- Création d'un inventaire des ressources vérifié par rapport aux bases de données des failles de sécurité connues afin de rechercher d'éventuels points faibles et des mises à jour nécessaires
- Communication au client d'informations sur la hiérarchisation des failles de sécurité présentant le niveau de risque le plus élevé, à traiter en priorité, et conseils pour l'application de correctifs
- Analyses effectuées à l'aide d'une plateforme avancée basée sur l'apprentissage automatique (ML)
- Revues trimestrielles pour informer le client sur les tendances en matière de failles de sécurité dans son environnement et son secteur d'activité

Dès aujourd'hui, sécurisez votre environnement avec Dell

À mesure que la fréquence et le coût des violations continuent d'augmenter, Managed Detection and Response Pro vous aidera à sécuriser votre environnement IT et à protéger vos ressources les plus critiques contre les auteurs de menaces malveillantes, tout en améliorant la posture de sécurité de votre organisation.

Contactez votre agent commercial Dell dès aujourd'hui.

[1] IBM (2022). Rapport intitulé « Cost of a Data Breach Report 2022 », téléchargé le 20 septembre 2022 à l'adresse https://www.ibm.com/downloads/cas/3R8N1DZJ

[2] Tenable (2021). Rapport intitulé « Tenable's 2021 Threat Landscape Retrospective », téléchargé en août 2022, à l'adresse https://www.tenable.com/cyber-exposure/2021-threat-landscape-retrospective

DELL Technologies