Améliorer les mesures de sécurité sans surcoût de personnel

Pour renforcer considérablement sa cybersécurité, un grand comté du sud-ouest des États-Unis s'est tourné vers la solution Dell Managed Detection and Response.

Profil client

Comté des États-Unis

Administrations publiques et locales | États-Unis

« Nous savions que nous devions améliorer notre posture de sécurité. Dell Managed Detection and Response permet d'y arriver sans augmenter l'effectif. »

Directeur des systèmes d'information
Grand comté du sud-ouest des États-Unis

Besoins opérationnels

Face à l'essor rapide des attaques par rançongiciel et autres cybermenaces ciblées contre les administrations publiques et locales, un vaste comté en pleine croissance situé au sud-ouest des États-Unis souhaitait renforcer sa posture de sécurité et améliorer sa capacité à détecter les menaces et à y répondre, sans les coûts et les efforts nécessaires pour recruter et former des experts de la sécurité supplémentaires.

Résultats commerciaux

- Améliore la posture de sécurité du comté sans augmenter les effectifs.
- Complète les connaissances, les compétences et la capacité d'évolution de l'équipe informatique.
- Libère le personnel de la charge liée à la surveillance et à la gestion des menaces 24x7.
- Rationalise la détection des violations de serveur et l'application rapide de mesures correctives.
- Offre le confort de disposer de spécialistes expérimentés sur lesquels le comté peut s'appuyer.

Aperçu des solutions

- Managed Detection and Response

Grand comté en pleine croissance situé au sud-ouest des États-Unis comptant plusieurs centaines de milliers de résidents et connu pour la diversité des entreprises qui y sont implantées, allant d'entreprises médicales, de biotechnologies et de fabrication dynamiques à des exploitations agricoles et d'élevage vitales.

Ces dernières années, les menaces de cybersécurité contre les administrations publiques et locales ont considérablement augmenté. Aux États-Unis, en 2020, 79 attaques par rançongiciel ont été lancées contre des entités gouvernementales à tous les niveaux du pays, entraînant près de 19 milliards de dollars de coûts de temps d'arrêt et de récupération.[1]

Après une expérience frustrante avec l'offre d'un autre fournisseur, le comté du sud-ouest des États-Unis a choisi la solution Dell Managed Detection and Response, optimisée par le logiciel d'analytique de sécurité Secureworks® Taegis™ XDR. La solution est un service de bout en bout managé, 24x7, qui surveille, détecte, analyse et contre les menaces dans l'ensemble de l'environnement IT du comté.

« Nous savions que nous devions améliorer notre posture de sécurité », explique le directeur des systèmes d'information du comté. « Dell Managed Detection and Response permet d'y arriver sans augmenter l'effectif. »

Combinaison de deux fonctionnalités clés

La solution rassemble les deux composants les plus importants pour une posture de sécurité redoutable :

- L'expertise des analystes de sécurité Dell Technologies pour compléter l'équipe réduite du comté composée uniquement d'un analyste de sécurité, d'un administrateur système et d'un ingénieur
- Les fonctionnalités étendues de Secureworks Taegis XDR, une plateforme d'analytique de sécurité Cloud native conçue pour détecter les menaces les plus avancées, permettant aux analystes MDR de rationaliser et de collaborer avec le comté sur les procédures d'enquête, et de les aider à prendre les mesures appropriées pour limiter les impacts

« Lorsque nous avons eu besoin de l'aide des spécialistes Dell Technologies, ils se sont implantés de manière virtuelle dans notre système pendant une semaine ou dix jours. Nous savions que nous étions entre de bonnes mains. »

Directeur des systèmes d'information
Grand comté du sud-ouest des États-Unis

[1] Bischoff, Paul, « Ransomware attacks on US government organizations cost $18,9bn in 2020 », Comparitech, 17 mars 2021. https://www.comparitech.com/blog/information-security/government-ransomware-attacks/

« Ils nous ont aidés à installer des agents logiciels sur chaque serveur et station de travail, avec des déclencheurs sélectionnés pour arrêter les services ou une machine, ou encore, fermer un compte et nous avertir lorsqu'une menace a été détectée », affirme le directeur des systèmes d'information. « Les spécialistes Dell Technologies nous ont fourni de précieux conseils et ont hiérarchisé les étapes à suivre au cours des 90 jours de mise en œuvre. »

Maîtrise rapide d'une tentative de violation

La solution inclut également jusqu'à 40 heures par trimestre de conseils détaillés pour répondre aux menaces et y remédier, même dans les situations les plus complexes, et 40 heures supplémentaires par an pour enquêter sur les activités et lancer la récupération en cas d'incidents de sécurité graves, si nécessaire.

Le directeur des systèmes d'information du comté se souvient : « Ce qui nous a vraiment convaincus de l'intérêt de la solution, c'est la vraie tentative de violation que nous avons subie. Un groupe de hackers a découvert une faille dans le serveur de messagerie Microsoft Exchange. Après en avoir été informés par Microsoft et l'agence de cybersécurité de notre État, nous avons constaté que l'un de nos trois serveurs avait été compromis. L'équipe Dell Technologies a fait preuve d'une grande minutie pour enquêter sur la violation et nous aider à restaurer notre serveur. »

Il poursuit : « Je recommande à n'importe quel CIO de comté d'opter pour une solution de sécurité de niveau entreprise telle que Dell Managed Detection and Response, plutôt que pour une offre d'un fournisseur de logiciels de protection antivirus. Lorsque nous avons eu besoin de l'aide des spécialistes Dell Technologies, ils se sont implantés de manière virtuelle dans notre système pendant une semaine ou dix jours. Nous savions que nous étions entre de bonnes mains. Ensemble, nous avons travaillé plus intelligemment, et il y avait beaucoup de synergie entre nos équipes. »

En savoir plus sur Dell Managed Detection and Response

Contactez un expert en solutions Dell Technologies

DELL Technologies

Suivez-nous sur les réseaux sociaux

Copyright © 2022 Dell Inc. ou ses filiales. Tous droits réservés. Dell Technologies, Dell et les autres marques commerciales sont des marques commerciales de Dell Inc. ou de ses filiales. Les autres marques éventuellement citées sont la propriété de leurs détenteurs respectifs. Cette étude de cas est fournie à titre d'information uniquement. Dell considère les informations contenues dans le présent document comme exactes au moment de sa publication (septembre 2022). Ces informations peuvent être modifiées sans préavis. Dell n'offre aucune garantie, expresse ou implicite, concernant cette étude de cas.