Managed Detection and Response für einen starken Sicherheitsstatus

Erkennen, Untersuchen und Reagieren auf Advanced Threats in der IT-Umgebung

Dell Managed Detection and Response

Dell Technologies kombiniert sein Sicherheitsfachwissen und fundiertes Know-how bezüglich IT-Umgebungen mit einer großen Auswahl an branchenführenden XDR-Sicherheitsanalyseplattformen.

Wie sicher ist Ihr Unternehmen?

Die IT-Teams haben oft Schwierigkeiten, mit der wachsenden Zahl der sich ständig weiterentwickelnden Sicherheitsbedrohungen Schritt zu halten. Im Jahr 2022 gab es weltweit 5,5 Milliarden Malwareangriffe – das sind 100 Millionen mehr als 2021.[1]

Wenn Sie Ihr Unternehmen umfassend schützen möchten, müssen Sie neue Bedrohungen in der gesamten Umgebung schnell erkennen und effektiv darauf reagieren können. Dies ist eine große Herausforderung, da Einzelprodukte und -tools den Überblick erschweren. Zudem ist es alles andere als einfach, qualifizierte SicherheitsexpertInnen zu finden und zu halten. Nicht zuletzt sind die IT-Teams bereits mit kritischen Anforderungen und dem Tagesgeschäft voll und ganz ausgelastet.

Managed Threat Detection and Response

Dell Managed Detection and Response ist ein vollständig verwalteter 24/7-End-to-End-Service zur Überwachung, Erkennung, Untersuchung und Reaktion auf Bedrohungen in der gesamten IT-Umgebung. So können Unternehmen mit 50 oder mehr Endpunkten ihren Sicherheitsstatus schnell und nachhaltig verbessern und zugleich die IT entlasten.

Der Service umfasst zwei wichtige Komponenten:

- Fachwissen, das die Dell Technologies SicherheitsanalystInnen durch jahrelange Erfahrung beim Schutz von Unternehmen auf der ganzen Welt gewonnen haben
- Branchenführende XDR-Sicherheitsanalyseplattformen (Extended Detection and Response), die KI-gestützte Analysen von Telemetriedaten und Ereignissen aus mehreren Angriffsvektoren umfassen

Hauptvorteile:

- Einheitliche Erkennung und Reaktion in der ganzen Umgebung
- Kontinuierliche Aktualisierung der Bedrohungsdatenbank für stets aktuellen Schutz
- Zuverlässige Erkennung der raffiniertesten Methoden von BedrohungsakteurInnen
- Umfassender Überblick über die End-to-End-Aktivitäten von AngreiferInnen
- Ein Team von Dell Technologies Sicherheitsprofis mit Fachwissen im Bereich Sicherheit, erweiterte Infrastruktur, Cloud und mehr
- Kompetente Unterstützung bei der Implementierung der cloudnativen SaaS-XDR-Lösung
- Schnelle Reaktion auf Cyber-Incidents, die eine Sicherheitsverletzung verursachen
- Kontinuierliche Ausrichtung auf ein Höchstmaß an Sicherheitscompliance der Serviceanbieter

Full-Service-Lösung

Die SicherheitsanalystInnen von Dell Technologies unterstützen Sie bei der Ersteinrichtung, beim Monitoring sowie bei der Erkennung, Korrektur und Reaktion – all dies zu einem planbaren Preis. Sie arbeiten eng mit Ihrem IT-Team zusammen, um die Umgebung zu verstehen, Empfehlungen zu Verbesserungen des Sicherheitsstatus zu geben und die Bereitstellung des XDR-Software-Agent auf Endpunkten zu unterstützen.

Warnmeldungen werden 24/7 überwacht und überprüft. Wenn aufgrund einer Warnmeldung weitere Ermittlungen erforderlich sind, bestimmen AnalystInnen die geeignete Reaktion und führen sie durch. Wenn eine Bedrohung bösartig oder eine Aktion von Ihrer Seite erforderlich ist, werden Sie entsprechend informiert und erhalten bei Bedarf Schritt-für-Schritt-Anweisungen.

Bei einem Sicherheits-Incident hilft Ihnen Dell Technologies, den Prozess zur Wiederaufnahme des Geschäftsbetriebs zu initiieren.

Wählen Sie Ihre XDR-Plattform

Ihre Sicherheits- und Technologieanforderungen und -präferenzen sind einzigartig. Wir bieten Ihnen die Flexibilität, aus drei branchenführenden Optionen zu wählen: Secureworks® Taegis™ XDR, CrowdStrike Falcon® XDR oder Microsoft Defender XDR – so erhalten Sie eine XDR-Plattform, die Ihren Anforderungen entspricht.[2]

Hauptmerkmale

Zuverlässiger Support

- Wir arbeiten eng mit Ihnen zusammen, um Ihre Umgebung zu verstehen, Untersuchungen durchzuführen und Sie bei der Verbesserung Ihres Sicherheitsstatus zu beraten.
- Sie profitieren von 24/7-Monitoring mit den XDR-Plattformen Ihrer Wahl, die KI-gestützte Analysen von Telemetriedaten und Ereignissen aus mehreren Angriffsvektoren umfassen.
- Wir bieten kompetente Beratung bei der Bereitstellung und Konfiguration der XDR-Plattform.

Bedrohungsabwehr und Sicherheitskonfiguration

- Mithilfe von XDR-Funktionen automatisiert das Dell SOC-Team die Korrekturmaßnahmen bzw. arbeitet eng mit Ihnen zusammen, um die beim Monitoring erkannten Bedrohungen zu beseitigen.
- Es stehen leicht verständliche, detaillierte Anweisungen zur Verfügung, die Ihnen dabei helfen, Bedrohungen auch in komplexen Situationen einzudämmen.
- Bis zu 40 Stunden servicebezogene Sicherheitskonfiguration sind pro Quartal inklusive.

24/7-Erkennung und -Untersuchung

- Auf die Sicherheitsumgebung Ihres Unternehmens zugeschnittene und automatisierte Prozesse und Warnmeldungen für effiziente tägliche Abläufe
- Proaktive Bedrohungssuche, die speziell auf die Umgebung jedes Kunden abgestimmt ist, um neue Bedrohungen oder Varianten bekannter Bedrohungen zu erkennen, die den Sicherheitssystemen entgehen
- Tägliche Zusammenfassung weniger kritischer Warnmeldungen, sodass sich das Dell SOC-Team auf die kritischen Warnmeldungen konzentrieren kann
- Vierteljährliche Berichte zu Untersuchungen, Analysen von Warntrends und Hinweisen zum Sicherheitsstatus

Einleiten von Maßnahmen gegen Cyber-Incidents

- Mit 40 Stunden Incident-Response-Remotesupport pro Jahr lassen sich Untersuchungen schnell einleiten.
- Sie erhalten Hilfestellung durch unsere zertifizierten SicherheitsexpertInnen, die schon Unternehmen jeder Größe dabei geholfen haben, schwerwiegende Sicherheitsvorfälle zu beheben.

Sichern Sie Ihre Umgebung noch heute mit Dell

Die durchschnittlichen Gesamtkosten einer Sicherheitsverletzung durch Ransomware liegen bei 5,13 Millionen US-Dollar – dies sind 13 % mehr als im Jahr 2022. Daher ist es jetzt an der Zeit, mehr darüber zu erfahren, ob Dell Managed Detection and Response das Richtige für Sie ist.[3]

Wenden Sie sich noch heute an Ihre/n VertriebsmitarbeiterIn.

1. Statista, Annual number of malware attacks worldwide from 2015 to 2022.
2. Für den Einsatz von Microsoft Defender XDR sind mindestens 500 Endpunkte erforderlich.
3. IBM, Cost of a Data Breach Report 2023.

Februar 2024-NS.