Managed Detection and Response für einen starken Sicherheitsstatus

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

Dell Technologies Managed Detection and Response

Dell Technologies kombiniert sein Sicherheitsfachwissen und sein fundiertes Know-how über IT-Umgebungen mit der führenden Secureworks® Taegis™ XDR-Security-Analytics-Software

Wie sicher ist Ihr Unternehmen?

IT-Abteilungen stehen vor der Herausforderung, mit der wachsenden Zahl immer neuer Sicherheitsbedrohungen Schritt zu halten. Mehr als 60 % der Unternehmen haben bereits eine Datenpanne aufgrund einer ausgenutzten Sicherheitslücke erlebt.[1]

Damit Ihr Unternehmen umfassend geschützt ist, müssen Sie neue Bedrohungen in der gesamten Umgebung schnell erkennen und angemessen reagieren. Problematisch wird dies durch isolierte Produkte und Tools, die die Sichtbarkeit einschränken, die schwierige Suche und Bindung qualifizierter Sicherheitsfachkräfte und schließlich IT-Teams, die durch kritische Anforderungen und den täglichen Betrieb ohnehin voll ausgelastet sind.

Verwaltete Erkennung und Reaktion auf Bedrohungen

Dell Technologies Managed Detection and Response mit Unterstützung von Secureworks Taegis XDR ist ein vollständig verwalteter 24x7-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 gleichzeitig die IT entlasten.

Der Service umfasst zwei wesentliche Funktionsbereiche:

- Das Fachwissen, das das Dell Technologies Sicherheitsanalystenteam durch jahrelange Erfahrung beim Schutz von Unternehmen auf der ganzen Welt gewonnen hat.
- Die Leistung der offenen Secureworks Taegis XDR-Security-Analytics-Software, die auf mehr als 20 Jahren Know-how in operativer Informationssicherheit, der Analyse und Erforschung realer Bedrohungen und unserer Erfahrung in der Erkennung und Reaktion auf Advanced Threats basiert.

Wichtige Vorteile:

- Einheitliche Erkennung und Reaktion in der ganzen Umgebung
- Kontinuierliche Aktualisierung der Bedrohungsdatenbank für stets aktuellen Schutz
- Zuverlässige Erkennung der raffiniertesten Taktiken von Bedrohungsakteuren
- Umfassender Überblick über die End-to-End-Aktivitäten von Angreifern
- Ein Team von Dell Technologies Sicherheitsfachkräften mit Fachwissen im Bereich Sicherheit, erweiterte Infrastruktur, Cloud und mehr
- Kompetente Unterstützung bei der Implementierung der Cloud-nativen SaaS-XDR-Lösung
- Schnelle Reaktion auf Cyber-Incidents, die eine Sicherheitsverletzung verursachen

Full-Service-Lösung

Das Dell Technologies Sicherheitsanalystenteam bietet Unterstützung für Ersteinrichtung, Monitoring, Erkennung, Korrektur und Reaktion – alles zu einem kalkulierbaren Preis. Das Team analysiert die Umgebung in enger Zusammenarbeit mit dem IT-Team, erteilt Empfehlungen zur Verbesserung des Sicherheitsstatus und unterstützt Sie bei der Bereitstellung von XDR-Software-Agents an Endpunkten.

Warnmeldungen werden im 24x7-Betrieb überwacht und überprüft. Wenn eine Warnmeldung eine Untersuchung erfordert, wird die angemessene Reaktion vom Analystenteam ermittelt und durchgeführt. Sie werden informiert, wenn eine Bedrohung bösartig ist oder Ihr Handeln erfordert, und erhalten bei Bedarf Schritt-für-Schritt-Anweisungen.

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

Hauptmerkmale	
Unterstützte Agentverteilung • Wir analysieren gemeinsam mit Ihnen die Umgebung und unterstützen Sie bei der Bereitstellung des Software-Agents auf den entsprechenden Endpunkten – ohne zusätzliche Kosten. • Umsetzung durch sehr erfahrene BereitstellungsexpertInnen	**Erkennung und Untersuchung von Bedrohungen** • Nutzung von Secureworks-Angriffsdaten aus mehr als 1.400 Incident-Response-Projekten im letzten Jahr • Vierteljährliche Überprüfungen mit Anleitungen zur Verbesserung des Sicherheitsstatus im Kundenunternehmen
Reaktion und aktive Korrektur • Bereitstellen von Schritt-für-Schritt-Anweisungen, um Bedrohungen auch in komplexen Situationen einzudämmen • Bis zu 40 Stunden Remotekorrektur unter Anleitung pro Quartal	**Einleiten von Maßnahmen gegen Cyber-Incidents** • Mit 40 Stunden Incident-Response-Remoteunterstützung pro Jahr lassen sich Untersuchungen schnell einleiten. • Anleitung durch unsere zertifizierten SicherheitsexpertInnen, die schon Unternehmen jeder Größe geholfen haben, schwerwiegende Sicherheitsvorfälle zu beheben.

Sichern Sie Ihre Umgebung noch heute mit Dell

Datenschutzverletzungen verursachen im Durchschnitt Kosten von 13 Mio. US-Dollar. Deshalb sollten Sie jetzt herausfinden, wie Sie von Dell Technologies Managed Detection and Response profitieren können.[2]

Wenden Sie sich an unser Vertriebsteam.

[1]Von Dell in Auftrag gegebenes Forrester Consulting Thought Leadership Paper: BIOS Security – The Next Frontier for Endpoint Protection, Juni 2019.
[2]Accenture, Ninth Annual Cost of Cybercrime Study, März 2019

DELL Technologies