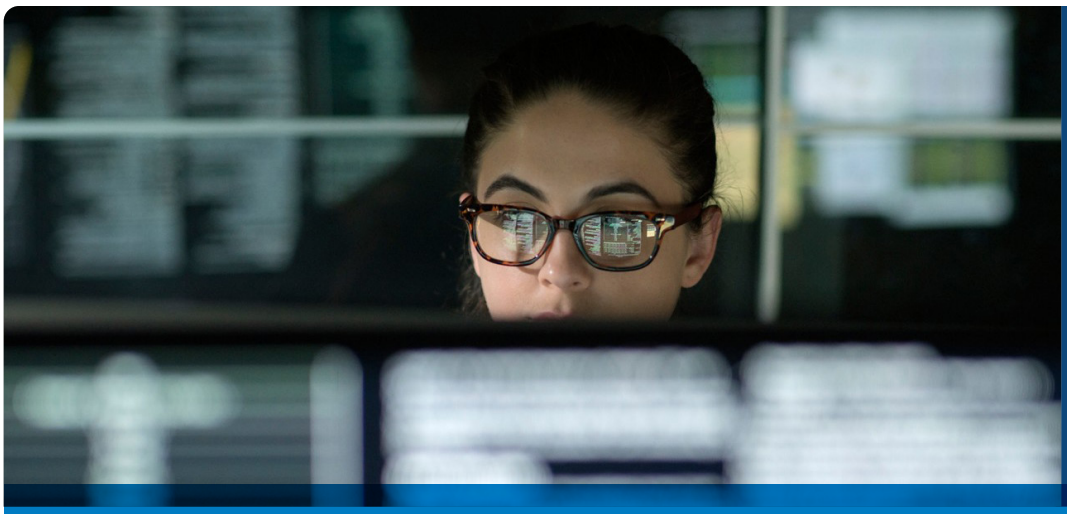
Verhindern von und Reagieren auf Bedrohungen in Ihrer IT-Umgebung



Erkennen von Sicherheitslücken und Priorisieren für sofortige Maßnahmen

Managed Detection and Response Pro

Kombination von Vulnerability Management und Managed Detection and Response in einer einzigen Lösung zum Schutz Ihrer IT-Umgebung

Im Jahr 2022 beliefen sich die durchschnittlichen Kosten einer Datenschutzverletzung auf 4,35 Mio. USD.[1] Fakt ist, dass im Jahr 2021 fast 22.000 neue Sicherheitslücken veröffentlicht wurden – und diese Zahl nimmt weiter zu.[2] Unternehmen müssen einen Weg finden, um ihre Umgebung vor dieser steigenden Anzahl an Sicherheitsbedrohungen und den Folgen einer eventuellen Sicherheitsverletzung zu schützen.

Für den effizienten Schutz Ihrer IT-Umgebung müssen Sicherheitslücken behoben, Bedrohungen untersucht und effektive Reaktionsmaßnahmen ergriffen werden. Zudem stehen die Unternehmen vor der Herausforderung, qualifizierte SicherheitsexpertInnen zu finden und zu binden, außerdem sind die IT-Abteilungen mit kritischen Anforderungen und dem täglichen Geschäftsbetrieb ausgelastet.

Deshalb haben wir Managed Detection and Response Pro entwickelt. MDR Pro ist eine vollständig verwaltete Lösung zur Erkennung und Priorisierung von Sicherheitslücken sowie für die 24/7-Bedrohungserkennung und -reaktion. Unsere ExpertInnen arbeiten mit Ihrem internen Sicherheitsteam zusammen, damit Ihre IT-Umgebung geschützt ist, Ihr Sicherheitsstatus stetig verbessert wird und Sie immer auf alles vorbereitet sind.

Identifizieren und Priorisieren von Sicherheitslücken über die gesamte Angriffsfläche

Die Dell ExpertInnen setzen führende Technologie ein, um Ihre IT-Umgebung in regelmäßigen Abständen zu scannen und so einen vollständigen Überblick über die Sicherheitslücken Ihrer Endpunkte, Netzwerkinfrastruktur und Cloud-Ressourcen zu erhalten. Mithilfe von maschinellem Lernen ermitteln die Dell ExpertInnen Sicherheitslücken, die quasi „in freier Wildbahn“ aktiv ausgenutzt werden können und daher mit höherer Wahrscheinlichkeit in naher Zukunft ins Visier geraten werden. Auf diese Weise können Sie Korrekturmaßnahmen für Sicherheitslücken mit dem höchsten Sicherheitsrisiko sowie für Ihre kritischen Ressourcen priorisieren.

Hauptvorteile:

- Abwehr immer auf dem neuesten Stand durch wiederholte Sicherheitslückenscans und das -management
- Vollständiger Überblick über die Sicherheitslücken Ihrer Endpunkte, Netzwerkinfrastruktur und Cloud
- Priorisierung der zu schließenden kritischen Sicherheitslücken vor ihrer Ausnutzung
- Einheitliche Erkennung und Reaktion in der ganzen Umgebung
- Erkennung neuer Angriffstypen dank einer kontinuierlich aktualisierten Bedrohungsdatenbank
- Korrelation von Ereignissen und Nachverfolgung der End-to-End-Aktivität von AngreiferInnen
- Nutzung des Know-hows und Fachwissens des Dell Sicherheitsteams

Erkennen von und Reagieren auf Angriffe, bevor Schaden entsteht

Managed Detection and Response ist ein vollständig verwalteter und umfassender 24x7-Service, der Bedrohungen in der gesamten IT-Umgebung überwacht, erkennt, untersucht und abwehrt. Unternehmen mit 50 oder mehr Endpunkten können ihren Sicherheitsstatus schnell und deutlich verbessern und gleichzeitig die IT entlasten.

Der Service umfasst zwei wesentliche Funktionsbereiche:

- Fachwissen, das die Dell Technologies SicherheitsanalystInnen durch jahrelange Erfahrung beim Schutz von Unternehmen auf der ganzen Welt gewonnen haben
- Moderne XDR-Software für Sicherheitsanalysen, die auf mehr als 20 Jahren SecOps-Fachwissen, der Analyse und Erforschung realer Bedrohungen und unserer Erfahrung in der Erkennung von und Reaktion auf Advanced Threats basiert

Hauptmerkmale

Bedrohungserkennung und -ermittlung

- Dell analysiert gemeinsam mit Ihnen die Umgebung und unterstützt Sie bei der Bereitstellung des Software-Agents auf den entsprechenden Endpunkten – ohne zusätzliche Kosten.
- Wir nutzen die Angriffsdaten aus über 1.400 Incident-Response-Projekten im letzten Jahr.
- Mit Schritt-für-Schritt-Anleitungen dämmen Sie die Bedrohung auch in komplexen Situationen ein.
- Sie können für Korrekturen bis zu 40 Stunden Remoteanleitung pro Quartal nutzen.
- Mit bis zu 40 Stunden Incident-Response-Remoteunterstützung pro Jahr lassen sich Untersuchungen schnell initiieren.

Erkennung und Priorisierung von Sicherheitslücken

- Die Sicherheitslückenscans erfolgen monatlich, zusätzliche Scans können je nach Vereinbarung zwischen dem Dell Team und dem Kunden stattfinden.
- Der Ressourcenbestand wird anhand von aktuellen Datenbanken mit bekannten Sicherheitslücken auf Schwachstellen und erforderliche Updates geprüft.
- Der Kunde erhält Feedback zur Priorisierung der Sicherheitslücken mit dem höchsten Risiko sowie Unterstützung bei deren Behebung.
- Die Scans werden mithilfe einer fortschrittlichen ML-basierten Plattform durchgeführt.
- Der Kunde wird durch vierteljährliche Überprüfungen über Sicherheitslückentrends in seiner Umgebung und in der Branche informiert.

Schützen Sie Ihre Umgebung noch heute – mit Dell

Sicherheitsverletzungen treten immer häufiger auf, mit stetig steigenden Kosten. Mithilfe von Managed Detection and Response Pro können Sie Ihre IT-Umgebung sowie die wichtigsten Ressourcen vor bösartigen BedrohungsakteurInnen schützen und gleichzeitig den Sicherheitsstatus Ihres Unternehmens verbessern.

Wenden Sie sich gleich an Ihre/n VertriebsmitarbeiterIn.

[1] IBM. (2022). „Cost of a Data Breach Report 2022". Abgerufen am 20. September 2022 von https://www.ibm.com/downloads/cas/3R8N1DZJ.

[2] Tenable (2021)m „Tenable's 2021 Threat Landscape Retrospective". Abgerufen im August 2022 von https://www.tenable.com/cyber-exposure/2021-threat-landscape-retrospective.