
## Die wichtigsten Vorteile

### Verhindern

- Identifizieren von Sicherheitslücken in der gesamten Umgebung, um Patching-Vorgänge zu priorisieren
- Erkennen falsch konfigurierter oder problematischer Sicherheitskontrollen, die ausgenutzt werden könnten
- Genaues Untersuchen hochgradig riskanter Pfade zu wertvollen Ressourcen oder Daten mithilfe von jährlichen Pentests
- Verbessern der Mitarbeiterwachsamkeit durch Sicherheitsschu-lungen in Form von regelmäßigen, kompakten Modulen

### Reagieren

- Bedrohungserkennung und -reaktion rund um die Uhr in der gesamten Umgebung
- Durchgängiges Erfassen von Angriffsaktivitäten
- Nutzung von Telemetrie und Korrelation von Ereignissen aus vielen gängigen Sicherheitstools

# Dell Managed Detection and Response Pro Plus

## Vollständig verwaltete, umfassende SecOps-Lösung für Endpunkte, Netzwerke und Clouds

### Bewältigen kritischer Herausforderungen im Sicherheitsbetrieb

Viele IT-Abteilungen haben Bedrohungsmonitoring und -erkennung eingeführt, um mit der stetig wachsenden Anzahl vielfältiger Bedrohungen Schritt zu halten.

Bedrohungsmonitoring und -erkennung decken zwar wichtige Bereiche ab, jedoch ist es am besten, potenzielle Sicherheitslücken im Voraus zu schließen, bevor Cyberkriminelle sie ausnutzen. IT-Teams können bösartige Aktivitäten verhindern, indem sie Sicherheitslücken in Software, falsch konfigurierte Sicherheitskontrollen und fahrlässiges Mitarbeiterverhalten proaktiv in Angriff nehmen.

Erfahrene SicherheitsexpertInnen sind mit dem Patchen von Sicherheitslücken vertraut, allerdings ist es für die meisten IT-Abteilungen unmöglich, alle Schwachstellen zu beheben. Im Jahr 2021 wurden monatlich mehr als 1.500 neue Sicherheitslücken gemeldet.[1] Damit die Patching-Last kontrollierbar bleibt, müssen Kunden die Sicherheitslücken mit dem größten Risiko priorisieren.

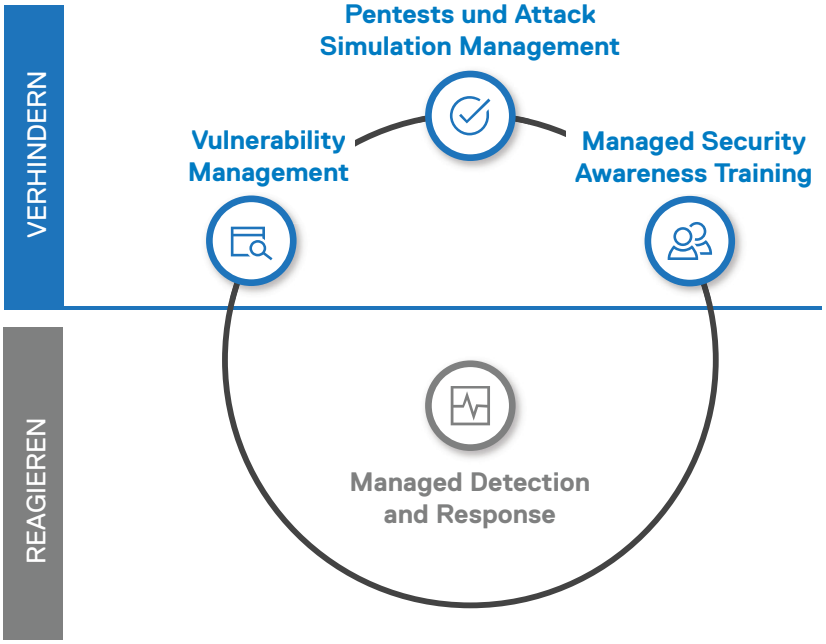
Die Überprüfung all Ihrer Sicherheitskontrollen (z. B. E-Mail-Gateways oder Webanwendungsfirewalls) ist eine ebenso gewaltige Aufgabe. Angesichts Hunderter Kontrollen und komplexer Konfigurationen ist es für IT-Sicherheitsteams schwierig, zu gewährleisten, dass Sicherheitskontrollen unzulässige Aktivitäten blockieren.

Darüber hinaus müssen MitarbeiterInnen Cyberkriminelle erkennen, die versuchen, an Anmeldedaten oder vertrauliche Informationen zu gelangen. Laut einer Studie wurden 83 % der befragten Unternehmen im Jahr 2021 Opfer eines erfolgreichen E-Mail-basierten Phishingangriffs.[2]

# Managed Detection and Response Pro Plus

Die SicherheitsexpertInnen von Dell Technologies haben diese wesentlichen SecOps-Anliegen sorgfältig geprüft und einen neuen, umfassenden Service für den Sicherheitsbetrieb entwickelt: Managed Detection and Response Pro Plus.

MDR Pro Plus ist eine vollständig verwaltete SecOps-Lösung, bei der führende Sicher-heitsexpertInnen innovative Tools einsetzen, um Bedrohungen zu verhindern, Angriffsversuche schnell zu erkennen und einzudämmen und Recovery-Vorgänge im Fall von Sicherheitsverletzungen einzuleiten. MDR Pro Plus unterstützt Sie dabei, den Sicherheitsstatus Ihres Unternehmens kontinuierlich zu verbessern.




## Schließen von Lücken in Software und Sicherheitskontrollen

**Vulnerability Management** umfasst eine monatliche Schwachstellenprüfung in Ihrer Umgebung sowie maschinelles Lernen, um die Sicherheitslücken zu priorisieren, die am wahrscheinlichsten ausgenutzt werden und erhebliche Auswirkungen zur Folge haben. Dank einer priorisierten Liste kann sich Ihr IT-Team auf die wichtigsten Sicherheitslücken konzentrieren.

Cyberkriminelle suchen nicht nur nach ungepatchten Sicherheitslücken, sondern auch nach falsch konfigurierten oder veralteten Sicherheitskontrollen. Deshalb müssen IT-Abteilungen sie zuerst finden und korrigieren. **Pentests und Attack Simulation Management** bietet monatlich automatisierte Simulationen von Sicherheitsverletzungen und Angriffen (Breach and Attack Simulations, BAS) sowie jährliche Penetrationstests.

BAS identifiziert fehlerhafte Sicherheits-kontrollen auf Geräten und Software in Ihrer IT-Umgebung. Pentests ergänzen BAS durch den Versuch, ein bestimmtes Ziel zu erreichen, z. B. hochwertige Systeme. Erfahrene PentesterInnen ahmen Angriffsmethoden nach, einschließlich Pivoting- und Anpassungstechniken, um das Ziel zu erreichen.

Dell führt Schwachstellenanalysen und BAS-Simulationen mit kontinuierlich aktualisierten Datenbanken durch, um sicherzustellen, dass Patching und Sicherheitskontrollen auf dem neuesten Stand bleiben.

## Fördern von Mitarbeiterwachsamkeit

Ein gängiges Modell für Schulungen zum Sicher-heitsbewusstsein sind jährliche, mehrstündige Schulungssitzungen. MitarbeiterInnen bewahren diese im Rahmen von „Ankreuzaufgaben“ vermittelten Informationen oftmals nicht. Falls sie dann einem Social-Engineering-Angriff oder einer E-Mail mit bösartigem Link ausgesetzt sind, reagieren sie möglicherweise nicht mit ausreichender Vorsicht.

**Managed Security Awareness Training** beinhaltet kompakte Sicherheitsschulungen über das ganze Jahr hinweg. Sie beziehen MitarbeiterInnen mithilfe von individuellen Lernpfaden aktiv ein und rücken den Sicherheitsaspekt in den Mittelpunkt. Lernpfade werden auf Basis von Mitarbeiterrollen, Bedrohungsrisiken und Fortschritten erstellt.

## Schnelles Erkennen und Eindämmen von Angriffsversuchen

Dell MDR Pro Plus umfasst **Managed Detection and Response** rund um die Uhr. Qualifizierte AnalystInnen überwachen Ihre Umgebung und untersuchen Bedrohungen mithilfe einer fortschrittlichen XDR-Plattform für Sicherheitsanalysen. ML- und DL-gestützte Telemetrie- und Ereignisanalysen bieten AnalystInnen wertvolle Informationen, um Angriffspfade und -aktivitäten zurückzuverfolgen. Das Dell Team stellt Ihnen dann Anweisungen zum Eindämmen und Beseitigen von Bedrohungen bereit. Bei einem Sicherheits-Incident unterstützt Sie Dell Technologies dabei, den Prozess zur Wiederaufnahme des Geschäftsbetriebs einzuleiten.

## Verbesserter Sicherheitsbetrieb mit Dell

Die MDR Pro Plus-Lösung verhindert bösartige Aktivitäten, indem sie Sie regelmäßig über Sicherheitslücken, falsch konfigurierte Sicherheitskontrollen und hochgradig riskante Pfade zu wertvollen Ressourcen informiert. Darüber hinaus erhalten Sie das ganze Jahr über kompakte, einprägsame Sicherheitsschulungen für Ihre MitarbeiterInnen. Threat Detection and Response beinhaltet eine durchgängige Überwachung und Erfassung verdächtiger Aktivitäten.

MDR Pro Plus bietet Ihnen eine intelligente, umfassende Lösung für den IT-Sicherheitsbetrieb – mit Services, die auf fortschrittlicher Technologie basieren und von ExpertInnen bereitgestellt werden. Verwaltet wird all das von Dell Technologies, auf dessen innovative IT-Geräte, -Infrastrukturen und -Services Unternehmen aller Größen weltweit vertrauen.

Weitere Informationen zu Dell Managed Detection and Response Pro Plus

Kontakt zu Dell Technologies ExpertInnen

[1] Quelle: „With 18,378 vulnerabilities reported in 2021, NIST records fifth straight year of record numbers“, ZDNet, 8. Dezember 2021. https://www.zdnet.com/article/with-18376-vulnerabilities-found-in-2021-nist-reports-fifth-straight-year-of-record-numbers/

[2] Quelle: „2020 Phishing Attack Landscape Report [Greathorn]“, Cybersecurity Insiders, (2020). Stand vom 15. November 2022 von https://www.cybersecurity-insiders.com/portfolio/2020-phishing-attack-landscape-report-greathorn/


März 2023 – LC | Dell Managed Detection and Response Pro Plus – Übersicht