Cyberbedrohungen schneller erkennen und bekämpfen

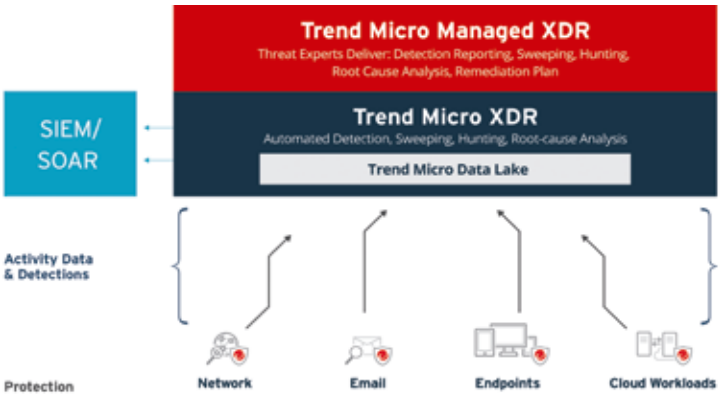
Mit Trend Micro XDR erhalten Unternehmen einen umfassenden Überblick über ihren Sicherheitsstatus. Gleichzeitig können sie Vorfälle aus verschiedenen Sicherheits-Silos miteinander in Verbindung bringen, um auch komplexe Angriffe zu erkennen.

Unternehmen haben mit einem stetigen Zuwachs von immer ausgefeilteren Cyberbedrohungen zu kämpfen. Dabei kann es gravierende Folgen haben, wenn ein solcher Angriff nicht frühzeitig erkannt und eingedämmt wird. Der massive Fachkräftemangel in der IT-Security verschärft diese Entwicklung zusätzlich.

Zu viele Lösungen, zu wenig Sicherheit

Viele Unternehmen reagieren darauf, indem sie eine Vielzahl unterschiedlicher Sicherheitslösungen einsetzen. So ergab eine Umfrage von ESG, dass 55 Prozent der befragten Unternehmen mehr als 25 verschiedene Cybersecurity-Technologien nutzen. Dennoch gelingt es Cyberangreifern regelmässig, die bestehenden Sicherheitsmechanismen zu umgehen. Die Vielzahl an Vorfällen erzeugt eine hohe Belastung für die wenigen Sicherheitsexperten und macht ihre Arbeit zunehmend ineffizient. So beträgt laut dem Verizon 2018 Data Breach Investigations Report die durchschnittlich benötigte Zeit bis zur Identifikation eines Datenabflusses 197 Tage. Bis der Abfluss gestoppt werden kann, dauert es weitere 69 Tage. Das bedeutet, dass Cyberkriminelle im Schnitt fast neun Monate Zeit haben, um Schaden in einem Unternehmen anzurichten.

«Die Bedrohungslandschaft stellt ebenso wie der Fachkräftemangel eine riesige Herausforderung dar. Darauf haben wir mit XDR reagiert», erklärt Michael Unterschweiger, Regional Director Schweiz und Österreich bei Trend Micro. «Unternehmen können sich bei der Security nicht alleine auf den Schutz verlassen. Vielmehr müssen sie davon ausgehen, dass es Angreifern gelingen kann, bestehende Sicherheitsbarrieren zu überwinden. Im Unterschied zu reinen EDR-Lösungen (Endpoint Detection and Response) können wir dabei mit unserer Lösung zusätzliche Angriffsvektoren analysieren. Wir skalieren Detection and Response damit auf weitere Quellen, um eine möglichst frühe und umfassende Erkennung zu gewährleisten.»



Verknüpfung von E-Mail, Netzwerk, Endpunkten und Cloud

Trend Micro XDR verbindet die Sicherheitslösungen für E-Mail, Netzwerk, Endpunkte und Cloud miteinander. So wird die Notwendigkeit manueller Tätigkeiten minimiert. Zudem korreliert die Lösung mittels künstlicher Intelligenz die Informationen über Ereignisse aus verschiedenen Silos und stellt diese in einer zentralen Konsole bereit. Damit können auch Daten analysiert werden, die Menschen angesichts der täglichen Flut von Sicherheitswarnungen nicht mehr verarbeiten können.

In einem grösseren Kontext werden aus Ereignissen, die allein betrachtet harmlos erscheinen, plötzlich wichtige Indikatoren für eine Gefährdung. Dadurch erleichtert XDR die Erkennung von sicherheitsrelevanten Vorfällen. Somit können Unternehmen die Auswirkungen von Angriffen schnell eindämmen und die Ausbreitung der Bedrohungen auf ein Minimum reduzieren.

Entlastung für Sicherheits-Teams

Die Ereignisinformationen werden zusätzlich um weitere Daten aus Trend Micros globalem Netzwerk für Bedrohungsinformationen ergänzt und die Erkennung durch spezifische Regeln verfeinert, mit denen Experten die wichtigsten Bedrohungen priorisiert bekämpfen können.

XDR ist zudem auch als Managed Service verfügbar, bei dem unternehmenseigene Teams durch Bedrohungsexperten von Trend Micro ergänzt und unterstützt werden. Trend Micro Managed XDR bietet Bedrohungsanalyse, Threat Hunting, Pläne zur Reaktion auf Angriffe und Empfehlungen zur Wiederherstellung betroffener Systeme rund um die Uhr an sieben Tagen pro Woche. ■

Trend Micro Schweiz GmbH, CH-8304 Wallisellen
✆ +41 (0)44 828 60 80, 🖷 +41 (0)44 828 60 81
marketing_alps@trendmicro.com
www.trendmicro.com