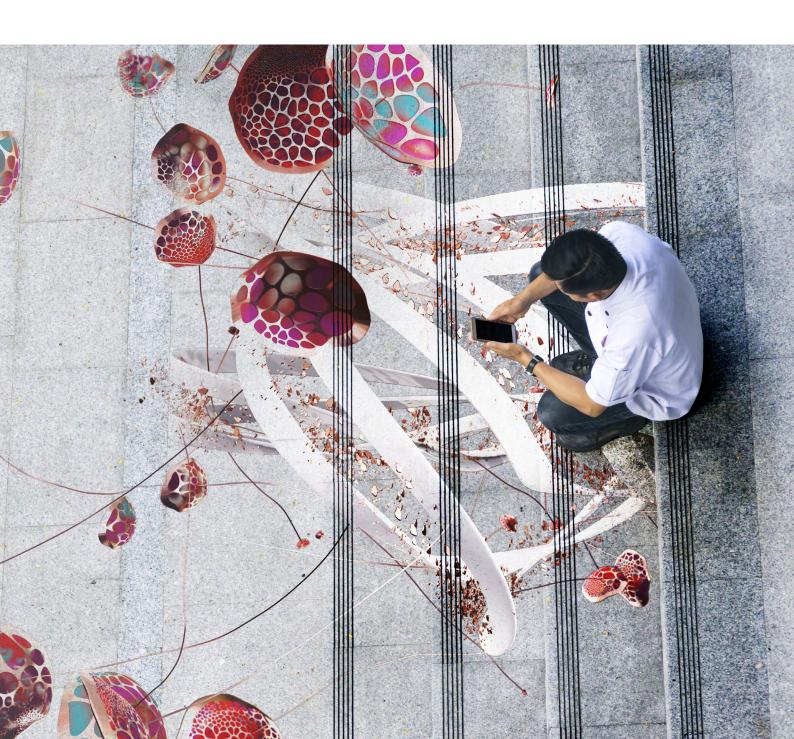


# Schneller wissen, wo's brennt

Extended Detection and Response (XDR)



#### BESTIMMT KENNEN SIE DAS

Eigentlich sind Sie in der IT-Security gut aufgestellt. Schließlich sind Unternehmen im Finanzsektor seit jeher ein bevorzugtes Ziel für Cyberkriminelle. Denn hier gibt es nicht nur Geld, sondern auch jede Menge wertvolle Kundendaten zu erbeuten. Da Cybervorfälle heute als größtes operationelles Risiko der Branche gelten, genießt die Security in Ihrem Unternehmen hohe Priorität.

Doch Ihre IT-Umgebung ist mittlerweile so komplex und Cyberkriminelle agieren so raffiniert, dass es immer schwieriger wird, für angemessenen Schutz zu sorgen. Was, wenn doch einmal ein Angreifer durchkommt? Dann zählt jede Minute, die Sie die Gefahr früher entdecken und eindämmen. Als KRITIS-Organisation müssen Sie zudem in der Lage sein, einen Sicherheitsvorfall zeitnah an das BSI zu melden.

### WIE GUT IST IHRE DETECTION & RESPONSE?

Klar, dass Sie bereits eine Vielzahl an leistungsfähigen Security-Systemen einsetzen. Bestimmt haben Sie ein SIEM und vielleicht auch ein SOC. Aber trotzdem bleibt da immer noch ein ungutes Gefühl:



Ihre Mitarbeiter werden täglich mit unzähligen Security Alerts überflutet. Wer kann in dieser Masse noch schnell genug erkennen, was wirklich wichtig ist?



Ein einheitlicher Blick auf einen Sicherheitsvorfall fehlt. Um einen Angriff nachzuvollziehen, müssen die Analysten viele verschiedene Security-Systeme betrachten und Indizien in mühevoller Kleinarbeit zusammentragen. Das dauert zu lange, und es kann schnell einmal ein Fehler passieren.



Da das SIEM nach Events pro Sekunde lizensiert wird, fallen durch die vielen angeschlossenen Security-Systeme hohe Kosten an.



Auch Use Cases für SIEM- und SOC-Projekte zu erstellen und die entsprechende Logik aufzubauen, ist aufwändig und teuer.

# SO KÖNNEN SIE MEHR ERKENNEN UND SCHNELLER REAGIEREN

Sie brauchen eine zuverlässige technische Lösung für Extended Detection and Response (XDR), die alle Vektoren in der IT-Umgebung abdeckt: von den Endpunkten über E-Mails, Server bis hin zu Cloud-basierten Workloads und Netzwerken. Sie sammelt Meldungen aller angeschlossenen Security-Systeme in einem Data Lake, filtert die relevanten Alerts heraus und korreliert sie zu verwertbaren Warnungen.



Machine Learning, KI und die Einbeziehung globaler Threat Intelligence sorgen für schnelle, treffsichere Analysen. Security-Mitarbeiter gewinnen mithilfe einer einzigen, zentralen Konsole Transparenz über das Bedrohungsgeschehen in der gesamten IT-Umgebung. Darüber hinaus kann die XDR-Lösung auch Logquellen für das SIEM konsolidieren und mit ihren automatisierten Analysen die Arbeit im SOC optimieren.

Laut Gartner zählt XDR zu den <u>Top Security and Risk Management Trends</u>. Unser Tipp: Wählen Sie einen XDR-Anbieter, dessen Security-Systeme möglichst oft weltweit installiert sind. Denn die KI der XDR-Lösung lässt sich umso besser trainieren, je größer ihre Datenbasis ist. Außerdem sollten Sie darauf achten, dass der Lösungsanbieter Expertise im Bereich von Zero-Day-Schwachstellen mitbringt. Nur so können Sie sicherstellen, dass Sie auch vor bisher unbekannten Bedrohungen geschützt sind.

## WENIGER WARNUNGEN = MEHR SICHERHEIT

Eine <u>Studie von ESG Research</u> zeigt: Unternehmen, die automatisiert Daten ihrer Security-Systeme aggregieren, korrelieren und analysieren, sind sicherer. 72 Prozent der Organisationen mit einer hohen Ausrichtung auf XDR ignorieren weniger als 25 Prozent der Security Alerts. Im Vergleich: 65 Prozent der Organisationen mit geringer Ausrichtung auf XDR ignorieren mehr als 25 Prozent der Alarme.

### DARUM LOHNT SICH XDR



- Sie können die Zahl der Security-Events um bis zu 90 Prozent reduzieren und sich auf die Warnungen konzentrieren, die wirklich wichtig sind.
- Dank der Automatismen und Künstlicher Intelligenz erhöhen Sie Ihre Analysegeschwindigkeit.
- Das Security-Team erkennt gefährliche Aktivitäten sofort, kann Angriffe schnell nachvollziehen und erhält Empfehlungen für Gegenmaßnahmen.
- Sie sparen Personalkosten. Auf die Frage, wie viele Personen in Vollzeit benötigt würden, um ihre automatisierten Systeme zu ersetzen, gaben Unternehmen laut dem <u>ESG Research Insights</u> <u>Report</u> durchschnittlich acht Vollzeit Security-Mitarbeiter an.
- Sie sparen SIEM-Kosten, da die XDR-Lösung als zentrale Logquelle dienen kann und so die Zahl der Events pro Sekunde reduziert, die Sie lizensieren müssen.
- Sie reduzieren Aufwände für die Planung von SIEM und SOC-Projekten, da die XDR-Lösung bereits gängige Use Cases liefert.

### DER PARTNER AN IHRER SEITE



Mit XDR von Trend Micro erhalten Sie Best of Breed-Lösungen vereint aus einer Hand von einem Marktführer. Zudem unterhält Trend Micro mit der Zero Day Initiative (ZDI) das branchenweit führende herstellerunabhängige Programm zur Schwachstellenforschung. Über die ZDI werden über die Hälfte aller veröffentlichten Zero-Day-Schwachstellen gemeldet. Trend Micro wurde im Forrester Wave™: Enterprise Detection and Response als Leader genannt (1. Quartal 2020) und ist laut MITRE ATT&CK Evaluations – APT29 führend bei der Ersterkennung.

Trend Micro (börsennotiert in Tokyo) hat über 30 Jahre Erfahrung als Spezialist für Sicherheitslösungen. Das Unternehmen wird seit 15 Jahren erfolgreich von seiner Mitgründerin Eva Chen geleitet, die als Leading Woman in IT international anerkannt ist. Als Mehrheitseignerin achtet sie mit ihrem Managementteam darauf, dass das Unternehmen gesund wächst und reinvestiert auch in Krisenzeiten umfangreich in Forschung und Entwicklung.

Ihr Credo: "Unsere einzige Konkurrenz sind Cyberkriminelle, denen man Einhalt gebieten muss."



Copyright © 2021 Trend Micro Incorporated. Alle Rechte vorbehalten. Trend Micro, das Trend Micro Logo und das T-Ball-Logo sind Marken oder eingetragene Marken von Trend Micro Incorporated. Alle anderen Firmen- bzw. Produktnamen sind Unternehmenskennzeichen oder eingetragene Marken ihrer jeweiligen Eigentümer. Die in diesem Dokument enthaltenen Informationen können sich ohne vorherige Ankündigung ändern. Trend Micro, das Trend Micro Logo und das T-Ball-Logo tragen das Registered-Trade-Mark-Symbol der USA. Einzelheiten dar über, welche personen bezogen Daten wir erfassen und warum, finden Siein unserer Datenschutzerklärung auf unserer Website unter: <a href="https://www.trendmicro.com/de-de/about/legal/privacy.html">https://www.trendmicro.com/de-de/about/legal/privacy.html</a>.