Trellix MDR Managed Detection and Response

Die Aufrechterhaltung einer kontinuierlichen Verteidigung rund um die Uhr ist anspruchsvoll und kostspielig. Ohne die richtigen Fähigkeiten oder ausreichendes Personal zur Erkennung, Reaktion und Verwaltung Ihrer Sicherheit bleiben Sie verwundbar.

Trellix Managed Detection and Response (MDR) - ***delivered by eyeT*** - bietet eine umfassenden 24/7 Schutz durch kontinuierliche Überwachung und Erkennung von Bedrohungen sowie schnelle Reaktion. In Zusammenarbeit mit eyeT Secure erfolgt die Implementierung des Clients für Forensik, EDR & Protection, während das Trellix MDR-Team im Anschluss administrativen Zugriff erhält. Trellix übernimmt daraufhin die vollständige Betreuung der Sicherheitsplattform, einschließlich Policy-Management, Benutzeradministration, Incident Response und Reporting.

Professionelle Bereitstellung und Management

Egal, ob Sie bereits über eine bestehende Trellix-Umgebung verfügen, gerade erst starten oder Ihre Implementierung abschließen müssen – unser Service kann innerhalb weniger Tage einsatzbereit sein. Trellix MDR-Analysten verfügen über umfassendes Fachwissen zu Ihren Trellix Endpoint Security (ENS), Trellix Endpoint Detection and Response (EDR), Trellix Insights und Trellix ePolicy Orchestrator (ePO) Lösungen, um Ihre Umgebung schnell zu implementieren, zu konfigurieren, zu optimieren und zu überwachen.

Wird eine potenzielle Bedrohung entdeckt, erfolgt umgehend eine Eskalation an die erfahrenen SOC-Analysten von Trellix MDR, die eine detaillierte Untersuchung durchführen. Sie bestimmen die Art der Bedrohung, reagieren darauf und passen bei Bedarf Ihre Konfigurationen, Regeln, Alarme oder Richtlinien an, um Ihre Verteidigung gegen vergleichbare Bedrohungen künftig noch robuster zu gestalten.

Welche Qualifikation hat das Trellix MDR-Team?

Das Team besteht aus hochqualifizierten Analysten mit Erfahrungen aus renommierten SOCs, darunter US Army Cyber Operations, McAfee, Intel und Cylance.*

Welche Qualifikation hat das eyeT Secure Team?

Als Trellix Platinum Partner verfügt eyeT Secure über höchste Trellix-Expertise, insbesondere in den Bereichen Endpoint Security und Endpoint Detection & Response (EDR) – ein Status, der nur wenigen anerkannten IT-Sicherheitsspezialisten zusteht. Seit 25 Jahren liefern wir McAfee/Trellix-Kompetenz auf höchstem Niveau – von der strategischen Beratung bis zur Umsetzung und fortlaufenden Betreuung.

Rund-um-die Uhr Monitoring und Schutz

Trellix MDR bietet 24/7 Überwachung, Analyse, Erkennung und Reaktion auf Bedrohungen, unterstützt durch die GenAI-gestützte Trellix Security Platform.

Schnelle Erkennung und Reaktion

Service Levels für kritische Incidents von weniger als 60 Minuten sowie vom Kunden definiertes Antwortprotokoll, vollständig integriert in SOC-Workflows und –Plattform

Durch Trellix Wise (GenAI) wird die Erkennungszeit um 50 % verkürzt, da es Bedrohungen automatisch analysiert, korreliert und Handlungsempfehlungen gibt.

Expertenunterstützung

Ein Team von Trellix-Sicherheitsexperten sorgt für schnelle Implementierung, Optimierung und Verwaltung von Trellix Endpoint Security, EDR, Insights und ePolicy Orchestrator (ePO). Bei Bedrohungserkennung erfolgt sofortige Eskalation und detaillierte Untersuchung.

Unübertroffene Bedrohungsintelligenz

Milliarden von Datensätzen in der globalen Datenbank für Bedrohungsinformationen.

Anbieter mit Forschungszentren für Cyber-Bedrohungen rund um den Globus.

Trellix Research: Jahrzehntelange Führungskompetenz im Bereich Bedrohungsinformationen und ein Team, das bei der Suche nach Bedrohungen und Schwachstellen produktiv ist

Strategische Beratung

Ein dedizierter Ansprechpartner steht Ihnen zur Seite. Direkter Zugriff auf Sicherheitsexperten rund um die Uhr maximiert die Sicherheit und verbesserte langfristige IT-Sicherheitsstrategie

Incident-Response- und Forensic Team

Im Falle eines Sicherheitsvorfalls sind die Experten des Incident-Response-Teams sofort einsatzbereit. Die Reaktion auf einen Vorfall erfolgt in enger Zusammenarbeit mit Ihrem Team und gemäß Ihren vordefinierten Anweisungen, die wir in unseren SOC-Workflow integrieren.

Trellix MDR Managed Detection and Response

Proaktive Bedrohungsabwehr

Trellix Insights liefert Kontext zu neuen Bedrohungen, priorisiert nach Relevanz für Branche oder Region, und ermöglicht präventive Maßnahmen zur Verbesserung der Sicherheitslage.

Schnelle Bereitstellung und OnBoarding für sofortigen Schutz und Betriebskontinuität.

Trellix MDR lässt sich nahtlos in Ihre bereits vorhandene Trellix Endpoint Security-Umgebung integrieren – ganz ohne zusätzliche Installation. Durch diesen effizienten Ansatz erzielen Sie sofortige Sicherheit und gewährleisten die betriebliche Kontinuität. So können sich die MDR-Experten von Trellix gezielt auf die entscheidende Bedrohungserkennung und -abwehr konzentrieren, ohne Ihren Betrieb zu beeinträchtigen.

Wie sind die Reaktionszeiten und Eskalationsprozesse definiert?

Reaktionszeiten basieren auf Schweregrad:

- Kritisch: 1 Stunde
- Hoch: 2 Stunden
- Mittel: 24 Stunden

Eskalationen erfolgen per Telefon und/oder E-Mail je nach Dringlichkeit.

Finanzielle Absicherung durch Trellix Breach Warranty

Eine **finanzielle Absicherung bis zu 1 Mio. $** bei Sicherheitsvorfällen, kombiniert mit schneller Expertenreaktion und reduzierten Cyberversicherungsraten.

Wie handhabt Trellix den Datenschutz?

Trellix MDR erfasst keine sensiblen Daten (Finanz-, Gesundheits- oder persönliche Identifikationsdaten). Alle Datenübertragungen erfolgen verschlüsselt, und Daten werden standardmäßig nach 30 Tagen gelöscht.

Bild 1: Trellix MDR kombiniert die Leistungsfähigkeit von Trellix Endpoint Security, Trellix EDR, Trellix Insights und Trellix ePolicy Orchestrator (ePO) mit herausragender Fachexpertise, GenAI-gestützter Bedrohungserkennung und durchgehender Verwaltung rund um die Uhr.

Warum Trellix MDR für Ihr Unternehmen wählen?

Trellix Managed Detection and Response (MDR) ist ein fortschrittlicher Cybersicherheitsservice, der kontinuierlich (24/7) Bedrohungen überwacht, erkennt, analysiert und gezielt darauf reagiert – unterstützt durch die GenAI-basierte Trellix Security Platform sowie spezialisierte Sicherheitsexperten. Ziel von Trellix MDR ist es, Unternehmen optimal vor Cyberangriffen zu schützen und gleichzeitig deren IT-Ressourcen effektiv zu entlasten, indem Sicherheitsrichtlinien und -konfigurationen kontinuierlich optimiert und Bedrohungen proaktiv abgewehrt werden.

Mit einer **breiten Abdeckung** unterstütz Trellix Endpoint Security mehr Betriebssysteme als andere Lösungen, was eine umfassende Sichtbarkeit der Endpunkte ermöglicht.

Welche Verantwortlichkeiten liegen beim Kunden und welche bei Trellix?

Kunden installieren mit Unterstützung von eyeT Secure die Trellix-Agenten für Forensik, EDR und Protection und gewähren dem Trellix MDR Team administrativen Zugang. Trellix übernimmt daraufhin Plattformadministration, Richtlinienerstellung, Benutzerverwaltung, Incident Management und Reporting.

Trellix MDR Managed Detection and Response | delivered by eyeT

Wie ist die Architektur der Trellix MDR-Lösung aufgebaut?

Managed Endpoints beinhalten:

- Trellix-Agent
- ENS Endpoint Security mit Threat Prevention und Firewall
- DER Endpoint Detection and Response
- Data Exchange Layer (DXL)
- Threat Intelligence Exchange (TIE)
- Die Kommunikation erfolgt über Port 443 und wird durch ePO sowie Identity Management gesteuert.

Welche Kernfähigkeiten bietet der MDR-Service?

- Plattformverwaltung und -optimierung
- Kontinuierliche Bedrohungserkennung
- Automatische Priorisierung und Ticketing
- Proaktive Eindämmung und Behebung mithilfe vorgefertigter Playbooks

Starker Fokus auf die Verbindung von Schutz und Erkennung

Im Gegensatz zu anderen Anbietern messen wir uns an den tatsächlich verhinderten Angriffen. So stellen wir sicher, stets einen Schritt voraus zu sein und Ihre Abwehrmechanismen kontinuierlich zu stärken. Wir nutzen Trellix Insights, globale Bedrohungsinformationen sowie IOC-Anreicherungen, kombiniert mit Praxiserfahrungen aus weltweiten Trellix-Implementierungen, um Ihre Richtlinien proaktiv zu aktualisieren und Schwachstellen zu schließen, bevor Angriffe überhaupt sattfinden.

Was umfasst das Konfigurationsmanagement im MDR-Service?

MDR startet mit bewährten Endpoint-Richtlinien. Individuelle Anpassungen erfolgen nach Kundengruppen und deren Risikotoleranz.

Trellix stellt die volle Nutzung bestehender Trellix-Lösungen (Endpoint Security (ENS), EDR, ePO, Insights) sicher, wodurch keine neue Implementierung erforderlich ist.

Trellix MDR optimiert kontinuierlich Sicherheitsrichtlinien und -konfigurationen, um Bedrohungen proaktiv zu begegnen.

Welche Reaktionsstufen gibt es bei Bedrohungen?

- Max Response: Volle Eindämmungsmaßnahmen
- Moderate Response: Entfernung von Schadsoftware ohne Neustart
- Cautious Response: Konservative Maßnahmen für kritische Server
- Notify Response: Benachrichtigung des Kunden bei sehr sensiblen Systemen

Wie schnell erfolgt typischerweise die Bedrohungsreaktion?

Innerhalb von etwa 70 Minuten von der Erkennung bis zur Eindämmung und Kundenbenachrichtigung.

Welche Standard-Reaktionsmaßnahmen sind vorgesehen?

- Gerätisolation
- Anwendungseindämmung
- Entfernung bösartiger Dateien
- Rollback von unerwünschten Änderungen
- Kundenbenachrichtigung

Welche Trellix-Lösungen umfasst der MDR-Service?

- Trellix ePolicy Orchestrator (ePO, SaaS/On-Premises)
- Endpoint Security (ENS)
- Endpoint Detection & Response (EDR)
- Threat Intelligence Exchange (TIE)
- Trellix Forensics
- Trellix Insights und Trellix Wise

Werden Drittanbieter im MDR-Service eingesetzt?

Ja, Trellix arbeitet ggf. mit zertifizierten Drittanbietern zusammen, die sich strikt an die Sicherheitsstandards von Trellix halten.

Welche professionellen Dienstleistungen bietet Trellix zusätzlich an?

Implementierung, Migration zu ePO SaaS und Optimierungen auf neueste Standards.

Welche Lösungen verwaltet Trellix MDR nicht?

Trellix MDR verwaltet derzeit keine Integrationen von Drittanbietern (gemäß offizieller Auskunft von Trellix Stand Juli 2025)