DATENBLATT

THREATDOWN™

ThreatDown Managed Detection & Response

Ergänzen Sie Ihr Team mit unseren Experten für 24x7x365 Bedrohungsüberwachung, -untersuchung und -beseitigung

Überblick

Sicherheitsteams benötigen die Bereitstellung hochwertiger Sicherheitsdienstleistungen für den Schutz der IT-Umgebungen vor Bedrohungen. Ideal ist ein qualifiziertes Team, das rund um die Uhr Überwachung bietet. Dennoch haben viele Organisationen knappe Personalressourcen und es fehlen tiefgreifende Cybersicherheitskenntnisse. Zusätzlich sind die vorhanden Mitarbeiter ständig mit Aufgaben zur Alarm-Triage überlastet. Hinzu kommen die explodierenden Kosten und die Komplexität der Verwaltung mehrerer Lösungen zur Aufdeckung versteckter Bedrohungen. Das führt zu Ineffizienz und langen Reaktionszeiten bei Vorfällen.

92 % **berichten von Kompetenzlücken und Engpässen in ihren Organisationen[2]**

ThreatDown, basierend auf Malwarebytes, löst diese Herausforderungen mit einem speziell entwickelten Managed Detection and Response (MDR)-Angebot. Ihr Unternehmen stärkt die Cyber-Resilienz mit Expertendiensten, die die Bedrohungserkennung und -reaktion präzise erkennen und Schwachstellen sofort bekämpfen. ThreatDown MDR bietet flexible Threat Response Optionen, die sowohl den Bedürfnissen Ihres Unternehmens als auch Ihrer Sicherheitsumgebung entsprechen. Damit gewährleisten Sie volle Transparenz und Kontrolle über Ihre Endpunkte.

Vorteile von ThreatDown MDR

- **24x7x365 Überwachung**: Wir überwachen Endpunkte und führen Tag und Nacht, Werktage, am Wochenenden und an Feiertage Expertenuntersuchungen durch. Wir überwachen und agieren immer!

[1] State of Cybersecurity 2024, ISACA.
[2] 2023 Cybersecurity Workforce Study, ISC2.
[3] Cost of a Data Breach Report 2024, Ponemon Institute.

Herausforderungen

- Begrenzte Ressourcen und Personal zur Abdeckung des Sicherheitsbedarfs – 57 % berichteten von Personalmangel an Cybersicherheitspersonal[1]
- Organisationen fehlen benötigte Sicherheitskenntnisse – 92 % berichten von Kompetenzlücken in ihren Organisationen[2]
- Langsame Reaktion bieten Angreifern mehr Zeit auf Ihren Endpunkten zu verweilen – Durchschnittlich 292 Tage, bis eine Datenpanne erkannt und behoben wird[3]

Vorteile

Schützen Sie die Arbeitsplätze und Server Ihrer Organisation mit ThreatDown MDR

- Kontinuierliche Erkennung, Reaktion und aktive Bekämpfung – Erweitern Sie die Sicherheit durch 24/7-fachkundige Überwachung und liefern priorisierte Erkenntnisse ohne Handbücher oder manuelles Fallmanagement
- Schnellere Expertenanalyse – Expertenteams beschleunigen die Analyse und Triage, was die Kosten für die Beseitigung deutlich senkt im Vergleich zu Organisationen, die intern Warnungen bearbeiten
- Expertenbeseitigung und -anleitung – Ermöglicht eine schnellere Bedrohungseindämmung und Einsatzreaktion bei gleichzeitiger Minimierung menschlicher Fehler und Angriffsauswirkungen

- **Erfahrene MDR-Analysten**: Unser Team von Sicherheitsexperten sind erfahrene Analysten mit umfassender Erfahrung in Incident Response und jahrzehntelanger Erfahrung in Triaging und Behebung komplexer Malware-Bedrohungen.
- **Preisgekröntes EDR**: Unsere ThreatDown Endpoint Detection and Response (EDR)-Plattform leitet alles an und reichert durch die wichtigsten Bedrohungsinformationsquellen, darunter MITRE und andere, auch weiter an.
- **Flexible Behebung der Sicherheitslücken**: Unser MDR-Team kann Bedrohungen aktiv beheben, sobald sie entdeckt werden. Alternativ leiten wir Ihre IT-Teams aktive bei der Umsetzung und Behebung, der Sicherheitslücken an.
- **Aktive Bedrohungssuche**: Unser MDR-Team betreiben proaktive Bedrohungsssuche unbekannte Bedrohungen anhand von Kompromittierungsindikatoren (IOCs) und verdächtiger Aktivitäten an Endpunkten.
- **Schnelle Bereitstellung**: ThreatDown EDR ist bekannt für seine einfache Einrichtung und ermöglicht es Ihrem Sicherheitsteam, neue Endpunkte innerhalb weniger Minuten schnell in unseren 24/7-MDR-Service einzubinden.

Wie funktioniert das?

Sobald die unseren Endpunktagenten eingesetzt sind, wird der MDR-Dienst innerhalb von Minuten aktiviert und ThreatDown-Analysten können die Umgebung des Kunden überwachen. Detektionsdaten werden in die MDR Security Information and Event Management (SIEM) und Security Orchestration, Automation, and Response (SOAR) Plattform eingespeist, wo sie mit internen und externen Bedrohungsinformationen angereichert werden. Dieser Prozess beschleunigt die Identifizierung, Analyse und Triage (Reaktionspriorisierung und Untersuchung) von Sicherheitsereignissen. Zu diesem Zeitpunkt überprüft die MDR SIEM/SOAR-Plattform verdächtige Aktivitätswarnungen auf tatsächliche Bedrohungen oder harmlose Erkennungen. Damit wird der Schweregrad bestimmter und die EDR-Erkennungen basierend auf Bedrohungsinformationen erhöht. Fälle, die eine Abhilfe fordern, werden entweder vom Analysten durchgeführt und abgeschlossen. Alternativ wird dem Kunden oder MSP eine Anleitung gegeben, falls diese sich entschieden haben, eigene Abhilfemaßnahmen durchzuführen.

ThreatDowns Branchenauszeichnungen

ThreatDown erhält konstant die Spitzenplatzierung der Level-1-Zertifizierung bei den vierteljährlichen 360-Grad-Tests von MRG Effitas. Darüber hinaus validieren G2-Auszeichnungen ThreatDown als Nr. 1 Endpoint Security Suite und MDR Grid Leader für die effektive und einfach zu bedienende Lösung von ThreatDown.

Erfahren Sie mehr

Um mehr darüber zu erfahren, wie ThreatDown MDR dazu beitragen kann, das Cyber-Risiko Ihrer Organisation zu reduzieren, besuchen Sie bitte threatdown.com/mdr