DATENBLATT

THREATDOWN™
Powered by Malwarebytes

ThreatDown Managed Detection & Response

Erweitern Sie Ihr Team mit expertengeführter 24x7x365-Bedrohungsüberwachung, Untersuchung und Behebung

Überblick

Für Sicherheitsteams ist es eine große Herausforderung, hochwertige Sicherheitsservices bereitzustellen und Unternehmensumgebungen frei von Bedrohungen zu halten. Dafür ist ein qualifiziertes Team erforderlich, das eine 24x7-Abdeckung gewährleisten kann. Viele Organisationen stehen jedoch vor begrenzten Personalressourcen und verfügen nicht über tiefgehende Cybersicherheits-Expertise. Zusätzlich sind sie ständig mit der Triage von Warnmeldungen überlastet. Hinzu kommen die stark steigenden Kosten und die Komplexität bei der Verwaltung mehrerer Lösungen zur Aufdeckung verborgener Bedrohungen, was zu Ineffizienz und langen Reaktionszeiten bei Vorfällen führt.

92 % **berichten über Kompetenzlücken in ihren Organisationen[2]**

ThreatDown, unterstützt von Malwarebytes, begegnet diesen Herausforderungen mit einem speziell entwickelten Managed Detection and Response (MDR)-Angebot. Ihr Unternehmen gewinnt an Cyber-Resilienz durch Expertendienstleistungen, die die Bedrohungserkennung und -reaktion präzise beschleunigen. ThreatDown MDR und MDR Plus bieten flexible Reaktionsoptionen, die sowohl den Anforderungen Ihres Unternehmens als auch Ihrer Sicherheitsumgebung entsprechen und sicherstellen, dass Sie jederzeit volle Transparenz und Kontrolle über Ihre Endpunkte und Identitäten behalten.

Vorteile von ThreatDown MDR

- **24x7x365-Überwachung**: Wir überwachen Endpunkte und Identitäten rund um die Uhr und führen fachkundige Untersuchungen durch – Tag und Nacht. Wir sind immer wachsam.
- **Erfahrene MDR-Analysten**: Unser Team aus Sicherheitsexperten besteht aus versierten Threat Huntern mit umfassender Erfahrung in Incident Response und jahrzehntelanger Praxis bei der Analyse und Eindämmung komplexer Malware-Bedrohungen.

Herausforderungen

- Begrenzte Ressourcen zur Bewältigung von Sicherheitsanforderungen – 57 % berichten über Personalmangel im Bereich Cybersicherheit[1]
- Fehlende Sicherheitskompetenz – 92 % berichten über Qualifikationslücken[2]
- Langsame Reaktion verschafft Angreifern mehr Zeit auf Ihren Endpunkten – durchschnittlich 292 Tage bis zur Identifizierung und Eindämmung eines Sicherheitsvorfalls[3]

Vorteile

Schutz Ihrer Workstations und Server mit ThreatDown MDR

- Kontinuierliche Erkennung und Reaktion – Erweiterung der Sicherheit durch 24/7-Überwachung durch Experten mit priorisierten Erkenntnissen ohne Playbooks oder manuelles Fallmanagement
- Schnellere Expertenanalyse – Beschleunigte Analyse und Triage durch Expertenteams, wodurch die Behebungskosten im Vergleich zur internen Bearbeitung deutlich reduziert werden
- Fachkundige Behebung und Anleitung – Schnellere Eindämmung von Bedrohungen und Reaktion auf Vorfälle bei gleichzeitiger Minimierung menschlicher Fehler und der Auswirkungen von Angriffen

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

- **Service Level Objectives**: Schnelle Reaktionszeiten basierend auf definierten Leistungszielen zur Beschleunigung der Erkennung und Minimierung der Auswirkungen:
  - **Kundenbenachrichtigung: <10 Minuten** nach bestätigter Bedrohungserkennung
  - **Analysteneinsatz: <30 Minuten** für Untersuchungs- und Reaktionsbeginn
- **Ausgezeichnete EDR-Technologie**: Basierend auf unserer ThreatDown Endpoint Detection and Response (EDR)-Plattform und angereichert mit mehreren Threat-Intelligence-Quellen, einschließlich MITRE und anderen.
- **Identity Threat Detection & Response (ITDR)**: Wir stoppen identitätsbasierte Angriffe durch kontinuierliche Überwachung von Verhalten im Zusammenhang mit Anmeldeinformationen, Berechtigungen und Zugriffen über Active Directory, Entra ID und Okta*
- **Flexible Behebungsoptionen**: Unser MDR-Team kann Bedrohungen aktiv beheben oder IT-Teams klare, umsetzbare Anleitungen für eigene Maßnahmen bereitstellen.
- **Aktives Threat Hunting**: Unser MDR-Team sucht proaktiv nach bislang unentdeckten Bedrohungen anhand früherer Kompromittierungsindikatoren (IOCs) und verdächtiger Aktivitäten auf Endpunkten.
- **Schnelle Bereitstellung**: ThreatDown EDR und ITDR sind für ihre einfache Einrichtung bekannt, sodass neue Endpunkte und Identitäten innerhalb weniger Minuten integriert werden können.

Vorteile von ThreatDown MDR Plus

- **Malware-Entfernungsservice**: Praktische Unterstützung durch Analysten zur vollständigen Entfernung komplexer, persistenter Bedrohungen.
- **Ursachenanalyse**: Nachbearbeitung von Vorfällen zur Klärung, wie ein Angreifer eingedrungen ist, was passiert ist und welche Änderungen erforderlich sind.
- **Threat-Intelligence-Feeds**: Erweiterte Erkennung durch Informationen zu kompromittierten Anmeldeinformationen – für frühzeitige Warnungen, bevor Angreifer diese nutzen können.
- **Vertragliche SLAs**: Garantierte Reaktions- und Eindämmungszeiten.

Wie funktioniert das?

Nach der Bereitstellung der Endpoint-Agenten wird der MDR-Service innerhalb weniger Minuten aktiviert, und ThreatDown-Analysten beginnen mit der Überwachung der Kundenumgebung. Erkennungsdaten werden in die MDR-SIEM- und SOAR-Plattform eingespeist und mit internen sowie externen Threat-Intelligence-Quellen angereichert. Dieser Prozess beschleunigt die Identifikation, Analyse und Triage (Priorisierung und Untersuchung) von Sicherheitsereignissen. Anschließend überprüft die Plattform verdächtige Aktivitäten und klassifiziert sie als tatsächliche Bedrohungen oder harmlose Ereignisse. Bei Bedarf wird die Kritikalität bestimmter EDR-Erkennungen erhöht. Fälle, die eine Behebung erfordern, werden entweder vom Analysten abgeschlossen oder es werden dem Kunden bzw. MSP konkrete Handlungsempfehlungen bereitgestellt.

Auszeichnungen der Branche

ThreatDown erzielt regelmäßig die höchste Einstufung (Level-1-Zertifizierung) in den vierteljährlichen 360-Grad-Tests von MRG Effitas. Zudem bestätigen G2-Auszeichnungen wie „#1 Endpoint Security Suite“ und „MDR Grid Leader“ die Effektivität und Benutzerfreundlichkeit der Lösung.

Weitere Informationen dazu, wie ThreatDown MDR das Cyberrisiko Ihres Unternehmens reduzieren kann, finden Sie unter: threatdown.com/mdr

THREATDOWN™ Powered by Malwarebytes | threatdown.com/mdr | sales@threatdown.com