DATENBLATT

THREATDOWN™
Powered by Malwarebytes

ThreatDown Identity Threat Detection & Response

Stoppen Sie Sicherheitsverletzungen mit einer einheitlichen Endpoint-zu-Identitäts-Abwehr

Überblick

Da identitätsbasierte Angriffe rasant zunehmen und der Missbrauch von Zugangsdaten zur häufigsten Ursache von Sicherheitsverletzungen geworden ist, stehen Unternehmen unter wachsendem Druck, ihr Geschäft zu schützen – ohne ihre Sicherheitsteams zu vergrößern. Hybride Umgebungen mit Active Directory, Entra ID und Okta schaffen blinde Flecken, die klassische IAM-, MFA- und Endpoint-Tools nicht erkennen können – und hinterlassen eine Post-Authentifizierungs-Lücke, die Angreifer gezielt ausnutzen.

Nr. 1 **Identitätsbasierte Angriffe sind der häufigste Angriffsvektor***

ThreatDown ITDR begegnet diesen Herausforderungen, indem es Identitätsverhalten kontinuierlich überwacht, mit Endpoint-Aktivitäten korreliert und automatisierte Reaktionen nutzt, um Angriffe früher und mit weniger Aufwand zu stoppen. Unternehmen verbessern so ihre Sicherheitslage, erfüllen regulatorische Anforderungen und sichern die Geschäftskontinuität – ohne zusätzlichen Overhead oder Personalaufbau.

Vorteile von ThreatDown ITDR

- **Die vollständige Angriffskette erkennen – vom Endpoint-Verhalten bis zur Identitätskompromittierung**: ThreatDown korreliert nativ Benutzer-Telemetriedaten aus Ihrem EDR mit Identitätsaktivitäten über lokale Active-Directory-Umgebungen, Entra ID und Okta hinweg. Wenn sich ein Angreifer von einem kompromittierten Endpoint über gestohlene Anmeldeinformationen bis hin zur Privilegieneskalation bewegt, sehen Sie die gesamte Kette an einem Ort. Kein Kontextwechsel. Keine blinden Flecken zwischen Endpoint- und Identitätsebene.

* IBM X-Force 2025; IBM Cost of a Data Breach 2025

Herausforderungen

- Identitätsbasierte Bedrohungen nehmen stark zu Identität ist inzwischen die Nr. 1 unter den Cyberangriffsflächen, wobei die Mehrheit der Datenschutzverletzungen gestohlene Zugangsdaten beinhalten
- Software- und Anbieterwildwuchs in der IT-Security 70 % der Unternehmen arbeiten aktiv an der Konsolidierung ihrer Sicherheitstools, doch viele ITDR-Lösungen schaffen lediglich ein weiteres Silo
- Langsame Reaktion verstärkt den Schaden Unternehmen benötigen durchschnittlich 241 Tage, um eine Sicherheitsverletzung zu erkennen und einzudämmen

Mehrwert

- Proaktive Identitätsabwehr Hochriskante Schwachstellen werden kontinuierlich identifiziert und beseitigt – mit priorisierten Erkenntnissen, die das organisatorische Risiko reduzieren
- Schnellere Erkennung und Reaktion Reduzierte operative Komplexität durch Verwaltung von ITDR über dieselbe einheitliche, cloudbasierte Konsole wie der gesamte ThreatDown-Security-Stack. Optimierte Workflows steigern die Effizienz und senken die Betriebskosten der IT-Security
- Beschleunigte Untersuchungen und Behebung Die native Endpoint-zu-Identitäts-Korrelation reduziert Rauschen und die mittlere Reaktionszeit erheblich. Mit 24x7-MDR stehen jederzeit erfahrene Analysten bereit, um Bedrohungen schneller und präziser einzudämmen

- **Proaktive Härtung von Angriffspfaden**: ThreatDown ITDR korreliert nativ Endpoint-Telemetrie mit Identitätsereignissen aus Active Directory, Entra ID und Okta, um Sicherheitsteams die vollständige Angriffsgeschichte gebündelt an einem Ort bereitzustellen. In Kombination mit MDR überwachen erfahrene Security-Analysten die Nutzung von Anmeldeinformationen, Privilegienaktivitäten und Sitzungsverhalten rund um die Uhr (24x7).

- **Vereinfacht Abläufe für schlanke Teams**: Mit einer Bereitstellung in nur wenigen Klicks und der zentralen Verwaltung über dieselbe Konsole wie ThreatDown EDR und E-Mail-Sicherheit reduziert ITDR Tool-Wilduchs, sowie operativen Aufwand. So erhalten Teams mehr Schutz – ohne zusätzliche Komplexität.

- **Dark-Web-Bedrohungen sichtbar gemacht**: Die kontinuierliche Überwachung von Dark-Web-Quellen deckt geleakte, mit Ihrer Organisation verknüpfte Anmeldeinformationen auf. Werden kompromittierte Konten erkannt, macht ThreatDown diese direkt in Ihrer Konsole sichtbar und ermöglicht schnelles Handeln – von erzwungenen Passwort-Zurücksetzungen bis zur Priorisierung von Maßnahmen für Ihre risikoreichsten Benutzer.

- **Compliance-fähige Identitäts-Einblicke**: Einheitliche Transparenz über Identitäten und aussagekräftige, umsetzbare Reports unterstützen Unternehmen bei der Einhaltung von DSGVO, HIPAA und Audit-Anforderungen – mit klarer, belastbarer Dokumentation für Aufsichtsbehörden, Stakeholder und Security-Verantwortliche.

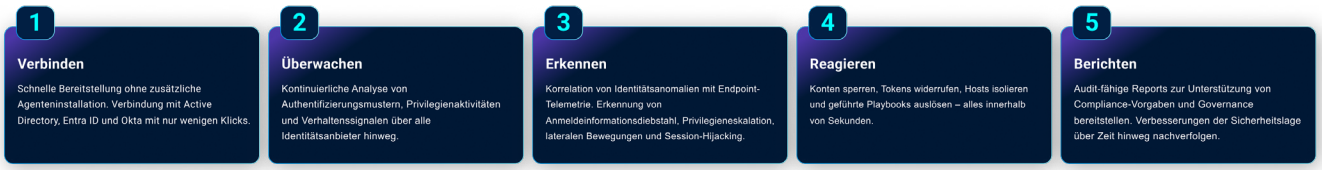
- **Schnelle Eindämmung**: Integrierte, geführte Playbooks für zentrale Maßnahmen wie Host-Isolierung, Kontosperrung und die Behebung von Angriffspfaden, um Alarmrauschen zu reduzieren und schlanken Teams zu ermöglichen, in Sekunden statt in Stunden zu reagieren.

- **Managed Services stoppen anmeldeinformationsbasierte Angriffe früher**: In Kombination mit MDR überwachen erfahrene Security-Analysten rund um die Uhr (24x7) die Nutzung von Anmeldeinformationen, Privilegienaktivitäten und Sitzungsverhalten. Sie helfen dabei, Bedrohungen wie Credential Theft, Privilegieneskalation, Token-Missbrauch und laterale Bewegungen zu erkennen und zu blockieren, bevor sie zu Sicherheitsvorfällen werden. Das ist das Identity-Security-Team, das Sie nicht einstellen mussten.

SO FUNKTIONIERT ES

Von der Erkennung bis zur Eindämmung in Sekunden – nicht in Tagen

ThreatDown ITDR überwacht kontinuierlich das Benutzerverhalten in Ihrer gesamten Umgebung. Wird eine Bedrohung erkannt, sorgen automatisierte Reaktionsmaßnahmen dafür, dass sie eingedämmt wird, bevor sich der Schaden ausbreitet.



Erfahren Sie mehr darüber, wie ThreatDown ITDR das Cyberrisiko Ihres Unternehmens reduzieren kann: threatdown.com/itdr