DATENBLATT

THREATDOWN | ELOVADE

INCIDENT RESPONSE

Der bewährte Standard für die automatische Endpunktsanierung

Bei einem Cyberangriff zählt schnelles Handeln zu den kritischsten Faktoren zur Beseitigung von Schadsoftware. Auf den Cyberspace spezialisierte Sicherheitsteams sollten Bedrohungen in weniger als einer Stunde aus der IT-Umgebung entfernen, um ausgefeilte Cyberangriffe wirksam zu bekämpfen und den Schaden zu vermeiden, den eine erfolgreiche Sicherheitsverletzung für den Ruf und den Gewinn eines Unternehmens bedeuten kann.

Doch die Unternehmen sehen sich mit einer zunehmenden Komplexität und einem hohem Ressourcenverbrauch im Security Operations Center (SOC) konfrontiert, da die manuelle Verwaltung von Abhilfemaßnahmen an verteilten Standorten und von verstreuten Mitarbeitern immer schwieriger wird. Dies führt zu langen Reaktionszeiten, die das Unternehmen einem erheblichen Risiko aussetzen.

Die Investition in eine Lösung, welche die Endpunktsanierung automatisiert, beschleunigt die Reaktionszeiten erheblich und bringt Ihre SOC-Sicherheitspraktiken voran.

PRODUKTÜBERSICHT

Incident Response (IR) ist der bewährte Standard für die automatisierte Endpunktsanierung. Die Lösung stärkt die Cyber-Resilienz von Unternehmen, indem sie ihre Reaktionszeiten durch eine schnelle und vollständige Beseitigung von Schadsoftware verkürzt. Mit unserem automatisierten Ansatz sorgt IR für eine höhere betriebliche Effizienz. Die Analysten sparen Zeit, die Anwender werden nicht in ihrer Arbeit unterbrochen und die Sicherheit Ihres Unternehmens wird verbessert.

Unsere flexiblen Implementierungsoptionen mit ständigem oder nicht-ständigem Agent ermöglichen Ihnen einen Einsatz entsprechend Ihrer Endpunktstrategie. Die API unserer IR-Lösung ermöglicht die Integration mit Ihrer bestehenden Sicherheitsinfrastruktur, um die Automatisierung und Orchestrierung Ihrer Sicherheitsprozesse weiter voranzutreiben.

Mit IR erhält Ihr Unternehmen eine wirksame und gründliche Endpunktsanierung, sobald Angriffe auftreten, und unsere geschützte Technologie zur Beseitigung von Schadsoftware entfernt dynamische und verwandte Artefakte auf gründlichste Weise.

ENTSCHEIDENDE VORTEILE

Verkürzung der Reaktionszeit

Holen Sie sich den bewährten Standard für die automatisierte Endpunktsanierung, mit dem Sie Angreifer in kürzester Zeit ausschalten und vollständig beseitigen können.

Steigerung der betrieblichen Effizienz

Verbessern Sie Ihre SOC-Praktiken mit einer Lösung, die die Sicherheitsabläufe beschleunigt, die Ressourcen der Sicherheitsanalysten schont und die Produktivität der Benutzer bewahrt.

Bedarfsgerecht einsetzbar

Mit der Wahl zwischen einem ständigen und einem nicht-ständigen Agent können Sie unsere flexiblen Optionen entsprechend Ihrer Endpunktstrategie einsetzen.

Orchestrierung automatisieren

Unsere API bietet Integrationsmöglichkeiten mit Ihrer bestehenden Infrastruktur, um die Automatisierung und Orchestrierung Ihrer Sicherheitsprozesse voranzutreiben.

> ThreatDown ist eine große Hilfe bei der Automatisierung unserer Angriffsreaktion. So generiert der Schutz vor Bedrohungen eine hohe Investitionsrendite. Die Anzahl der per Reimaging wiederherzustellenden Systeme wird reduziert und Sie erhalten wertvolle Informationen zur Verhinderung von Sicherheitsverletzungen. So generiert ThreatDown eine erhebliche höhere Investitionsrendite.
>
> Bob Chadwick, Senior SOC Manager
> Analoge Geräte

FUNKTIONEN

Automatisierte Endpunktreaktion, die Antwortzeiten verkürzt
Mit unserem automatisierter Ansatz können Sicherheitsanalysten den manuellen Aufwand zur Behebung von Angriffen eliminieren und so wertvolle Zeit sparen. Automatisierte Aufgaben werden in kürzerer Zeit und mit größerer Genauigkeit ausgeführt und verkürzen Ihre Reaktionszeit.

Automatisierte Abhilfemaßnahmen, die den Angreifer auslöschen
Die meisten Lösungen beseitigen nur aktive Schadsoftwarekomponenten – eine vollständige Beseitigung ist damit nicht möglich. Die Linking Engine verwendet einen geschützten Ansatz, der auch dynamische und verwandte Artefakte erkennt und entfernt. Unsere Engine wendet die sogenannte verbundene Sequenzierung an, um die Beseitigung von Schadsoftware-Persistenzmechanismen sicherzustellen.

Ständiger oder nicht-ständiger Agent – Sie bestimmen
ThreatDown bietet flexible Optionen für eine bedarfsgerechte Bereitstellung – Sie können einen ständigen oder aber einen nicht-ständigen Agent auf dem Endpunkt einsetzen. Beide Ansätze lassen sich problemlos in Ihr Bereitstellungstool integrieren und ermöglichen einen schnellen und für den Endbenutzer transparenten Einsatz.

Cloudverwaltetes System vereinfacht die Reaktion an verteilten Standorten
IR wird über die Cloud gesteuert und erleichtert die Verwaltung von Reaktionsmaßnahmen an verteilten Standorten und bei mobilen Mitarbeitern. Mithilfe der zentralisierten Dashboards erhalten Ihre Sicherheitsanalysten schnell einen Überblick über die Reaktion auf Angriffe und den Abhilfestatus.

Detaillierte Bedrohungsinformationen, die eine effektive Reaktion auf Endpunkte ermöglichen
Dank unserer Cyber-Intelligence-Expertise bei der Beseitigung von Sicherheitslücken verfügen wir über ein genaues, detailliertes Verständnis der Angriffe, die erfolgreich auf Unternehmensgeräten ausgeführt werden können. Damit steht Ihrem Unternehmen eine Lösung zur Verfügung, die sich auf die Erkennung und Beseitigung von Bedrohungen auf Millionen von ThreatDown-geschützten Endgeräten stützt – sowohl von Unternehmen als auch von Privatanwendern.

Skalierbar bis zum größten Unternehmen
Mit unserer Cloud-Lösung müssen Sie keine Geräte kaufen oder verwalten, und IR lässt sich so skalieren, dass es die Anforderungen Ihres Unternehmens an die Reaktion auf Vorfälle problemlos erfüllt.

ORCHESTRIERUNG DER AUTOMATISIERUNG ÜBER IHRE GESAMTE SICHERHEITSSTRUKTUR HINWEG

Die ThreatDown-API bietet Integrationsmöglichkeiten für Ihre gesamten Sicherheitsstruktur, z. B. SIEM, SOAR und ITSM, um die Automatisierung und Orchestrierung Ihrer Sicherheitsprozesse weiter voranzutreiben. Dadurch wird die Cyber-Resilienz des Unternehmens durch schnellere Maßnahmen zum Schutz und zur sofortigen Reaktion auf Angriffe erhöht.

Security Orchestration, Automation and Response (SOAR)

Automatisierung der Reaktion auf mögliche Bedrohungen durch Einleitung von automatischen Abhilfemaßnahmen

Security Incident and Event Management (SIEM)

Erweitern Sie Ihre Bedrohungsanalyse mit Schadsoftware-spezifischen Informationen, Asset-Informationen und Trendanalysen

Network Access Control (NAC)

Bewertung der Sicherheitslage von Geräten vor dem Netzzugang

Unified Endpoint Management (UEM)

Die Bereitstellung für Ihre Endgeräteflotte planen und verwalten

Information Technology Service Management (ITSM)

Arbeitsabläufe automatisieren und den Fortschritt vom Vorfall bis zur Behebung nachverfolgen

Incident Response

API-Integrationen

ELOVADE

Kontaktdaten für Deutschland & Österreich:

ELOVADE Deutschland GmbH
malwarebytes@elovade.com
DE: +49 6441 67118 842
AT: +43 820 0010 36
elovade.com/malwarebytes

Kontaktdaten für die Schweiz:

ELOVADE Swiss AG
sales@elovade.ch
CH: +41 55 552 27 92
elovade.ch/malwarebytes

Copyright © Malwarebytes. Alle Rechte vorbehalten. Malwarebytes, das Malwarebytes-Logo, ThreatDown und das ThreatDown-Logo sind Marken von Malwarebytes. Andere Marken können als Eigentum Dritter beansprucht werden. Alle hierin enthaltenen Beschreibungen und Spezifikationen können ohne vorherige Ankündigung geändert werden und werden ohne jegliche Gewährleistung bereitgestellt.