SONICWALL®

SonicWall Managed Detection and Response (MDR)

Ihre Endpoint-Security. Unsere Expertise.

Bei Managed Detection and Response (MDR) handelt es sich um einen umfassenden Service mit 24/7-Threat-Monitoring, -Threat-Hunting und -Threat-Detection/-Response. Der MDR-Service von SonicWall auf Basis von Solutions Granted nutzt erweiterte Analysen, Bedrohungsdaten und menschliche Expertise für eine durchdachte, gründliche Untersuchung von Vorfällen einschließlich angemessener Maßnahmen. Der Service umfasst ebenfalls die Validierung von Vorfällen sowie Remote-Response-Services wie die Eindämmung von Bedrohungen. Sie können sich entspannt in dem Wissen zurücklehnen, dass Sie in besten Händen sind – egal, was passiert.

- Identifizieren Sie ausgeklügelte Endpoint-Bedrohungen, die Ihre bestehenden Verteidigungsmechanismen umgehen
- Stellen Sie Ihren Kunden proaktive Sicherheitsservices über ein von Experten geführtes 24/7-SOC bereit, das die neuesten Bedrohungsdaten nutzt
- Verhindern Sie die Ausbreitung von Ransomware mit einer automatischen Isolierung des Netzwerks und der Unterbrechung von Ransomware-Prozessen
- Vermeiden Sie Alert-Fatigue und reduzieren Sie falsch positive Meldungen
- Kombinieren Sie die Lösung mit SonicWall Capture Client für eine benutzerfreundliche einheitliche Verwaltungsplattform oder nutzen Sie sie gemeinsam mit Ihrer bestehenden Windows-Defender- oder SentinelOne-Implementierung

„Das SOC von Solutions Granted hat um 2 Uhr nachts merkwürdige Aktivitäten auf einem Kundenserver beobachtet. So konnten wir die Sicherheitslücke frühzeitig eindämmen. Ich schlafe nachts besser, wenn ich weiß, dass Solutions Granted meine Netzwerke schützt.“

DAN BROWNE, CEO, DMB NETWORKS

Entdecken Sie die Vorteile einer soliden Partnerschaft mit einem Sicherheitsprovider: Erhalten Sie bessere Einblicke in Ihr gesamtes Ökosystem und profitieren Sie von der schnellen Reaktion unseres vollständig besetzten 24/7/365-SOC.

Kontaktieren Sie uns noch heute, um mehr über die vielen Vorteile für SonicWall-SecureFirst-Partner zu erfahren!

partnerdevelopment@sonicwall.com

BEWÄHRTE TECHNOLOGIEN. ÜBERRAGENDER SCHUTZ.

So verbessert SonicWall MDR die Sicherheit bei gleichzeitiger Optimierung des Ressourceneinsatzes:

AGENTBASIERTE IMPLEMENTIERUNG

Auf Endgeräten installierte Lightweight-Agents bieten einen dauerhaften und kontinuierlichen Zugriff und ermöglichen gleichzeitig eine Überwachung und Datenerfassung in Echtzeit.

ANOMALIEBASIERTE ERKENNUNG

Mithilfe heuristischer Methoden, statistischer Analysen und maschinellen Lernens markiert der Agent untypische Ereignisse oder Features eines Artefakts oder einer Datei und hilft so, ausgeklügelte Angriffe oder Zero-Day-Bedrohungen zu erkennen.

Die anomaliebasierte Erkennung umfasst:

- Echtzeitüberwachung von Prozessen und Skripts
- Kontinuierliche Echtzeitanalyse des Arbeitsspeichers
- Erkennung von PowerShell-Methoden und anderen cyberkriminellen Techniken wie LOTL (Living off the Land)
- Verhinderung der missbräuchlichen Verwendung von Benutzerkonten und legitimen administrativen Tools
- Funktionen, um zu verhindern, dass sich Bedrohungen seitlich ausbreiten

VERHALTENSBASIERTE ERKENNUNG

Die Behavioral-Analytics-Engine prüft legitime Prozesse und Ereignisse auf verdächtige Verhaltensweisen. Diese Anomalien werden dann mit bekannten Taktiken, Techniken und Abläufen (Tactics, Techniques and Procedures, TTPs) abgeglichen, wie sie im MITRE-ATT&CK-Framework beschrieben sind. SonicWall MDR konzentriert sich auf 20 der am häufigsten beobachteten ATT&CK-Techniken und ist daher äußerst effektiv darin, Angreifer auf frischer Tat zu ertappen.

FORENSISCHE ZUSTANDSANALYSE

Der Agent kann forensische Livedaten von Endgeräten erfassen und analysieren, einschließlich Daten im flüchtigen und nichtflüchtigen Speicher. Weil Tausende von Hosts proaktiv auf aktuelle und historische Kompromittierungen untersucht werden, können Sie die Ursache der erkannten Angriffe besser identifizieren. Die Analyse erfolgt wahlweise ohne Agent oder über den ARR-Agent.

Die forensische Zustandsanalyse umfasst:

- Aktive Prozesse und Skripts
- Priorisierung der Echtzeitanalyse des flüchtigen Speichers
- Registry und Autoruns (Run-Keys, Startordner, lnk-Dateien, schtasks/cron etc.)
- Ausführungsartefakte (shimcache, amcache, prefetch)
- Betriebssystem-Subversion (API-Hooks, deaktivierte Kontrollen)
- Priorisierung lokaler Ereignisprotokolle
- Privilegierte Konten
- Installierte Anwendungen und Schwachstellen
- Aktive Host-Verbindungen und Listener

KONTINUIERLICHE ENDPUNKTÜBERWACHUNG, REAKTION UND FORENSISCHE ANALYSEN

Erweitertes Threat-Hunting und -Monitoring sorgt für eine zusätzliche Sicherheitsschicht. Der Fokus liegt hierbei darauf, wesentliche Verhaltensweisen zu identifizieren, die während eines Angriffs oder danach beobachtet werden. Dank der automatisierten forensischen Analyse können unsere Experten die Integrität von Endgeräten proaktiv überprüfen und im Falle eines sicherheitsrelevanten Ereignisses in kurzer Zeit die Ursache ermitteln. MDR ermöglicht eine einfachere und schnellere Identifizierung und Untersuchung komplexer Cyberangriffe einschließlich angemessener Reaktionen.

Über SonicWall

SonicWall ermöglicht eine stabile, skalierbare und nahtlose Cybersicherheit für eine extrem dezentrale Arbeitswelt, in der jeder remote, mobil und potenziell gefährdet ist. Durch die Identifizierung unbekannter Bedrohungen, moderne Echtzeit-Überwachungsfunktionen und eine herausragende Wirtschaftlichkeit hilft SonicWall großen Unternehmen, Behörden und KMUs weltweit, die Cybersicherheitslücke zu schließen. Weitere Informationen erhalten Sie unter www.sonicwall.de.

SonicWall, Inc.
1033 McCarthy Boulevard | Milpitas, Kalifornien 95035, USA
Weitere Informationen erhalten Sie auf unserer Website.
www.sonicwall.com