Vorfalluntersuchung und -reaktion mit WatchGuard Advanced EPDR

Die Bedrohungsbekämpfung war noch nie so einfach

Einleitung

In einer Welt, in der sich Cyberbedrohungen ständig weiterentwickeln, benötigen Unternehmen fortschrittliche Lösungen, die Bedrohungen nicht nur erkennen, sondern auch eine effektive Untersuchung und Reaktion ermöglichen. WatchGuard Advanced EPDR erfüllt diese Anforderungen, da es eine robuste und umfassende Lösung bietet, die alle Funktionen von WatchGuard EPDR sowie erweiterte Funktionen für die Untersuchung von Vorfällen und die Reaktion darauf über eine einzige cloudbasierte Konsole umfasst.

Die Herausforderung von 100%igen LotL-Angriffen

LotL-Angriffe (Living-Off-the-Land-Angriffe) gehören zu den ausgeklügeltsten und am schwierigsten zu erkennenden Bedrohungstechniken. Im Gegensatz zu herkömmlichen Angriffen, die auf Malware oder schädlichen Anwendungen basieren, greifen LotL-Angriffe auf legitime Systemtools und -funktionen zurück, um bösartige Aktivitäten durchzuführen, die von vielen herkömmlichen Sicherheitslösungen nicht erkannt werden.

Mit dem Zero-Trust Application Service von WatchGuard werden alle Angriffe, die auf schädlichen Anwendungen basieren, automatisch blockiert. 100%ige LotL-Angriffe, bei denen keine neuen Dateien in das System eingeführt werden, können jedoch eine dauerhafte Bedrohung bleiben. Bei diesen Angriffen werden oft Tools wie PowerShell, die Windows-Verwaltungsinstrumentation (WMI) oder Office-Makros genutzt, deren Erkennung ohne kontinuierliche Überwachung, Telemetrieanalyse und Threat Intelligence schwierig ist.

Beispiele für LotL-Techniken:

- **PowerShell:** Wird bei LotL-Angriffen häufig verwendet, um schadhafte Skripte herunterzuladen und auszuführen, ohne offensichtliche Spuren zu hinterlassen. Angreifer können damit Remote-Verbindungen aufbauen oder Systemkonfigurationen ändern.
- **Windows-Verwaltungsinstrumentation (WMI):** WMI ist ein natives Windows-Tool für die Systemverwaltung und -überwachung. Angreifer können WMI ausnutzen, um Befehle aus der Ferne auszuführen oder über einen längeren Zeitraum im System zu verbleiben.
- **Remoteverwaltungstools:** Tools wie PsExec, die für die legitime Remote-Systemverwaltung entwickelt wurden, können von Angreifern für die Ausführung bösartiger Befehle auf Remote-Systemen zweckentfremdet werden.
- **Office-Makros:** Makros in Microsoft Office-Dokumenten sind Skripte, die Aufgaben automatisieren. Sie werden von Angreifern oft verwendet, um beim Öffnen des Dokuments schadhaften Code auszuführen. Dabei wird das Vertrauen der Anwender in scheinbar legitime Dateien ausgenutzt.

Um diese Herausforderungen anzugehen, bietet WatchGuard Advanced EPDR eine umfangreiche Lösung, die eine kontinuierliche Überwachung, Zugriff auf angereicherte Telemetrie sowie erweiterte Untersuchungs- und Reaktionsfähigkeiten umfasst. Angereicherte Telemetrie beinhaltet Befehlszeilendetails, die Zuordnung verdächtiger Aktivitäten zu MITRE ATT&CK-Taktiken und -Techniken sowie Einblicke in schädliche Anwendungen, z. B. potenzielle Verhaltensweisen, die MITRE ATT&CK zugeordnet sind, sowie Aufrufe externer Bibliotheken. So erhalten Sicherheitsanalysten die Tools an die Hand, die sie benötigen, um solche Angriffe zu erkennen und einzudämmen, bevor sie großen Schaden anrichten.

Funktionen und Vorteile von WatchGuard Advanced EPDR

1. Alle WatchGuard EPDR-Funktionen inklusive

WatchGuard Advanced EPDR umfasst alle Funktionen von WatchGuard EPDR, was bedeutet, dass es Präventiv- und Bedrohungserkennungstechnologien wie Anti-Exploit- und kontextbezogene Erkennung mit fortschrittlichen Sicherheitsdiensten wie dem Zero-Trust Application Service und Threat Hunting Service kombiniert. Diese Technologien und Dienste schützen vor ausgeklügelten Malware-basierten Angriffen und zahlreichen dateilosen Angriffen, die LotL-Techniken nutzen, ohne dass Eingriffe vonseiten der Sicherheitsanalysten erforderlich sind. Einige LotL-basierte Angriffe müssen jedoch von Sicherheitsexperten untersucht und validiert werden, um die Unannehmlichkeiten falsch positiver Erkennungen zu vermeiden. Hier bietet Advanced EPDR einen erheblichen Nutzen.

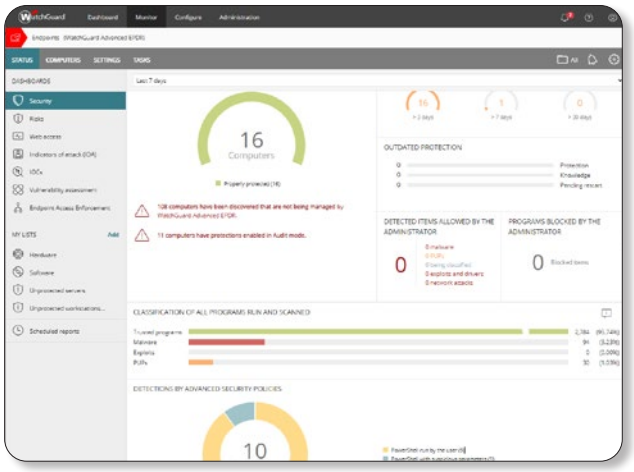

Abbildung 1: WatchGuard Advanced EPDR – Security Dashboard

2. Erweiterte Untersuchung von Vorfällen durch Zugriff auf angereicherte Telemetrie

- **Zugriff auf angereicherte Telemetrie:** Mit Advanced EPDR können Sicherheitsanalysten auf detaillierte Telemetrie zugreifen, die von Endpoints gesammelt wurde, einschließlich Prozessvorgänge, Netzwerkverbindungen und anderer verdächtiger Aktivitäten. Diese Telemetrie spielt bei der Untersuchung ungewöhnlicher Verhaltensweisen, die auf einen LotL-Angriff hinweisen könnten, eine entscheidende Rolle. Eine der automatisierten Anreicherungen ist die Zuordnung verdächtiger Aktivitäten zu den Taktiken und Techniken des MITRE ATT&CK-Frameworks. Diese Zuordnung bietet wichtige Einblicke, um die Identifizierung von Angriffsmustern und eine schnelle Reaktion zu beschleunigen.

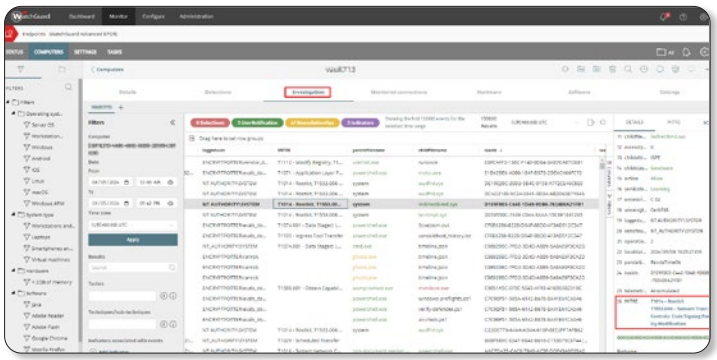

Abbildung 2: WatchGuard Advanced EPDR – Zugriff auf die angereicherte und detaillierte Telemetrie von Endpoints aus. Die MITRE ATT&CK-Zuordnung ist hervorgehoben.

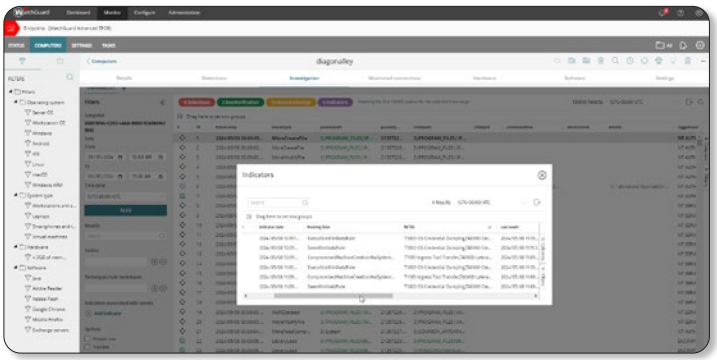

Abbildung 3: IoAs ausgelöst am Endpoint im untersuchten Zeitfenster

- **Intuitive Visualisierung und Navigation:** Über eine intuitive Benutzeroberfläche können Analysten Angriffsgraphen visualisieren und Telemetrieabfragen durchführen, die eine zügige Identifizierung von Angriffsmustern und eine effektive Reaktion auf Vorfälle ermöglichen. Die detaillierte und angereicherte Telemetrie ist von der zentralen cloudbasierten Konsole von Advanced EPDR aus zugänglich, sodass Sie nicht zu anderen Anwendungen wechseln oder sich mit manuellen Abfragen oder Anreicherungen befassen müssen.

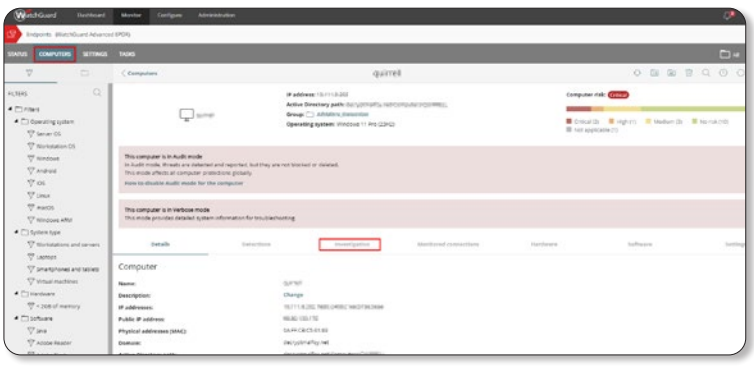

Abbildung 4: Zugriff auf das Untersuchungstool mit vollständigem Zugang zur angereicherten Telemetrie

3. Tiefgreifende Dateianalyse mit dem CAPA-Tool

- **Tiefgreifende Dateianalyse:** Die Integration des CAPA-Tools in WatchGuard Advanced EPDR ermöglicht eine tiefgreifende Analyse von Anwendungen, einschließlich derjenigen, die vom Zero-Trust Application Service blockiert wurden. CAPA identifiziert Angriffstechniken, die dem MITRE ATT&CK-Framework zugeordnet sind, die Fähigkeiten bösartiger Aktivitäten und die vom Programm verwendeten externen Funktionen, die wichtige Informationen für die Untersuchung von Vorfällen und die Reaktion darauf liefern.

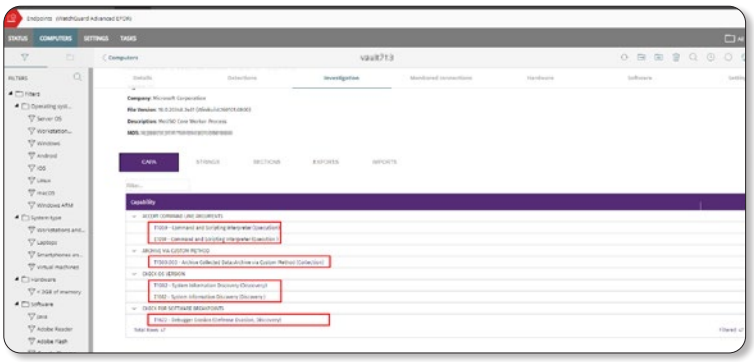

Abbildung 5: Einblicke über das CAPA-Tool in eine schadhafte Anwendung, zugänglich im Untersuchungsbereich

4. Ausführlicher Modus für die Angriffssimulation

- **Ausführlicher Modus/Angriffssimulation:** Dieser erweiterte Modus ermöglicht die Erfassung detaillierter Telemetrie während Angriffssimulationen und identifiziert dabei jede Taktik und Technik, die von simulierten Bedrohungsakteuren verwendet werden. Dies ist unverzichtbar, damit MSPs ihre Services um Red-Team-Übungen und Penetrationstests erweitern können, um die Sicherheitslage ihrer Kunden zu verbessern.

5. Endpoint Access Enforcement

- **Blockieren des Zugriffs von Hochrisiko-Endpoints:** Mit der Möglichkeit, Zugriffsanforderungen von Endpoints zu verweigern, die nicht den Sicherheitsrichtlinien entsprechen, sorgt WatchGuard Advanced EPDR dafür, dass nur sichere Geräte eine Verbindung zu geschützten Endpoints herstellen können, wodurch die Angriffsfläche reduziert und eine laterale Bewegung von Bedrohungen verhindert wird.

Abbildung 6: Überwachung der Erzwingung des Endpoint-Zugriffs mit zugelassenen und verweigerten Verbindungen

6. Remote Shell unter Windows, Linux und macOS

- **Remote-Endpoint-Zugriff:** Diese Funktionalität ermöglicht es Sicherheitsanalysten, Untersuchungen durchzuführen, Daten abzurufen und Sicherheitsverletzungen zu beheben, indem sie aus der Ferne auf Endpoints unter Windows, Linux und macOS zugreifen. Dies ist für die Ausweitung der MSP-Serviceabdeckung enorm wichtig und gewährleistet eine schnelle, effektive Reaktion auf Vorfälle in heterogenen Umgebungen.

7. Funktionen im Rahmen der Reaktion

- **Isolierung von Geräten:** Die Fähigkeit, kompromittierte Geräte schnell zu isolieren, ist von entscheidender Bedeutung, um die Ausbreitung von Bedrohungen innerhalb des Netzwerks einzudämmen.
- **Neustarten von Geräten:** Durch den Neustart kompromittierter Geräte direkt von der Konsole aus können Systeme schnell in einen sicheren Zustand versetzt werden.
- **Remote-Zugriff auf Endpoints:** Indem Sie eine Remote-Verbindung zu betroffenen Endpoints herstellen, können Sie direkt mit Dateien und Prozessen arbeiten und so eine agile und präzise Vorfallreaktion ermöglichen.

Fazit

WatchGuard Advanced EPDR ist eine umfassende und fortschrittliche Lösung, die alle Funktionen von WatchGuard EPDR mit erheblichen Verbesserungen bei der Vorfalluntersuchung und -reaktion kombiniert. Die Fähigkeit, 100%ige LotL-Angriffe durch kontinuierliche Überwachung, Zugriff auf angereicherte Telemetrie, leistungsstarke Analysen, die verdächtige Aktivitäten automatisch MITRE ATT&CK-Taktiken und -Techniken zuordnen, sowie Reaktionstools abzuwehren, hilft den Unternehmen, komplexe Bedrohungen so schnell wie möglich zu erkennen und einzudämmen sowie schwere Schäden abzuwenden. Durch die Einführung von WatchGuard Advanced EPDR und mit dem Know-how von Sicherheitsanalysten können Unternehmen ihre Sicherheitslage verbessern und eine widerstandsfähigere Umgebung gegen aufkommende Cyberbedrohungen gewährleisten.

Um mehr über WatchGuard Advanced EPDR zu erfahren, wenden Sie sich an Ihren WatchGuard-Ansprechpartner.

Über WatchGuard

WatchGuard® Technologies, Inc. gehört zu den führenden Anbietern im Bereich Cybersicherheit. WatchGuards Unified Security Platform®-Ansatz ist speziell auf Managed Service Provider ausgelegt, damit sie erstklassige Sicherheit bieten können, die die Skalierbarkeit und Schnelligkeit ihres Unternehmens erhöht und gleichzeitig die betriebliche Effizienz verbessert. Über 17.000 Vertriebspartner und Dienstleister im Bereich Sicherheit verlassen sich auf die prämierten Produkte und Services des Unternehmens, die die Bereiche Network Security and Intelligence fortschrittlicher Endpoint-Schutz, Multifaktor-Authentifizierung sowie sicheres WLAN umfassen, und sorgen somit für den Schutz von mehr als 250.000 Kunden. Gemeinsam bieten diese Bereiche die fünf entscheidenden Elemente einer Sicherheitsplattform: umfassende Sicherheit, kollektive Intelligenz, Transparenz und Kontrolle, operative Ausrichtung und Automatisierung. Neben der Zentrale in Seattle im US-Bundesstaat Washington unterhält das Unternehmen Niederlassungen in ganz Nordamerika, Lateinamerika und Europa sowie im asiatisch-pazifischen Raum. Weitere Informationen finden Sie unter watchguard.de.

Deutschland, Österreich, Schweiz +49 700 92229333 INTERNATIONALER VERTRIEB +1 206 613 0895 www.watchguard.de