Struktur eines Bedrohungsberichts

Einleitung

Wie tief sind die Einblicke, die Sie in Ihr Netzwerk haben? Welche Geräte kommunizieren miteinander und welche Arten von Daten werden zu und von Ihrem Netzwerk übertragen? Das Verständnis der Aktivitäten Ihres Netzwerks und die Identifizierung von Risiken und Bedrohungen sind entscheidend für den Schutz Ihres gesamten Unternehmens und Ihrer Lieferanten, Partner und Kunden.

Durch die proaktive Bewertung des Sicherheitsstatus Ihres Netzwerks mit automatisierten Risiko- und Bedrohungsberichten können Sie Schwachstellen oder Cyberangriffe identifizieren, die Ihren Perimeterschutz möglicherweise umgangen haben. Dieser proaktive Ansatz ermöglicht es Ihnen, diese Probleme rechtzeitig anzugehen, Ihre Cybersicherheitsstrategie zu stärken und Ihr Unternehmen zu schützen.

Grundlegende Netzwerk- und Ransomware-Berichterstattung

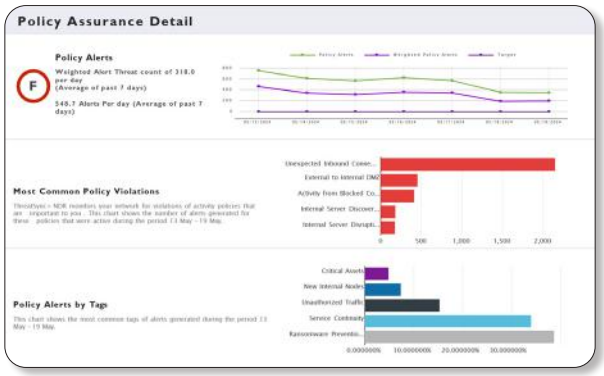
ThreatSync+ NDR umfasst einen Netzwerkbedrohungsbericht und einen Bericht zum Schutz vor Ransomware. Beide Berichte beginnen mit einer Zusammenfassung, der den allgemeinen Risikowert und -trend des gesamten Netzwerks anzeigt. Sie liefern detaillierte Informationen zu verschiedenen Richtlinien und Kontrollen, die vom NDR-System aktiv überwacht werden. Jeder Unterabschnitt zeigt zu jeder überwachten Richtlinie oder Kontrolle den jeweiligen Bedrohungswert und die Trendlinie. Wenn Lücken oder Ausfälle festgestellt werden, wird eine Anleitung zur Behebung zur Verfügung gestellt. Diese Berichte können leicht an die konkreten Anforderungen von Organisationen oder Cyber-Abwehrprogrammen angepasst werden. Sie dienen dazu, bestehende Probleme hervorzuheben und Führungskräften die Möglichkeit zu geben, Ziele für den Netzwerkschutz festzulegen und entsprechende Fortschritte und Verbesserungen zu verfolgen.

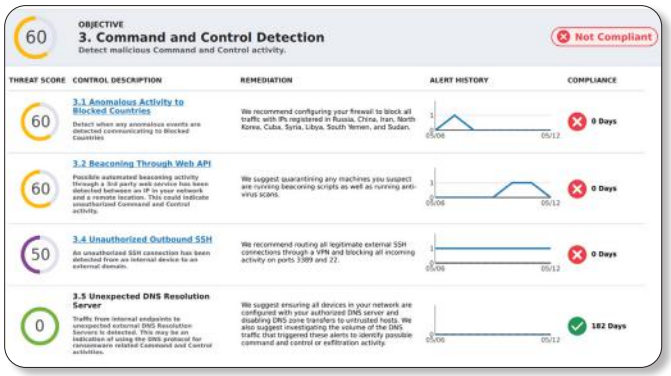
Berichte zum Schutz vor Netzwerkbedrohungen und Ransomware liefern eine äußerst detaillierte Bewertung der Vorgänge in Ihrem Netzwerk. Sie sind für Ihr Cyber-Abwehrprogramm unerlässlich, da sie die erforderlichen Informationen liefern, um Ihre Sicherheitslage zu verstehen, und Anleitungen zu Verbesserungsschritten enthalten. Welche Informationen genau enthalten sind, hängt von den Bewertungsergebnissen ab. Normalerweise handelt es sich dabei aber um folgende:

- Eine Liste aller identifizierten Sicherheitsrisiken
- Der Gefährdungsgrad eines jeden Risikos – i. d. R. als kritisch, hoch oder mittel eingestuft
- Eine Beschreibung jedes Risikos, einschließlich der Art, des Schweregrads und der potenziellen Auswirkungen
- Zu den Empfehlungen zur Beseitigung der einzelnen Risiken gehören das Installieren von Sicherheitsupdates, das Entfernen von Malware, das Isolieren von Geräten, das Ändern von Anmeldeinformationen oder das Konfigurieren von Sicherheitseinstellungen.

Beispiele für konkrete Sicherheitsrisiken, die bei der Bewertung ermittelt werden können:

- Aktivitäten an ungesicherten Ports
- Befehls- und Steuerungserkennung
- Unbefugter Fernzugriff
- Fehlgeschlagene Backups
- Unnötige und ungewöhnliche Port-Aktivitäten
- Aktiv ausgenutzte Sicherheitsschwachstellen
- Offene Warnmeldungen
- Nicht identifizierte und risikoreiche Geräte
- Verstöße gegen Richtlinien
- Bösartige Netzwerkaktivitäten
- Datenlecks bei KMU
- Ungewöhnliche VPN-Aktivitäten





Für weitere Informationen zum Netzwerkbedrohungsbericht und Bericht zum Schutz vor Ransomware von WatchGuard wenden Sie sich bitte an Ihren WatchGuard-Vertreter.

Über WatchGuard

WatchGuard® Technologies, Inc. gehört zu den führenden Anbietern im Bereich Cyber-Sicherheit. 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.

WatchGuard

DEUTSCHLAND, ÖSTERREICH, SCHWEIZ +49 700 92229333 INTERNATIONALER VERTRIEB +1 206 613 0895 www.watchguard.de