KURZBESCHREIBUNG

Autonome Rekonstruktion von Vorfällen Von Signalen zum Angriffspfad

Vereinheitlichen Sie Signale. Beschleunigen Sie die Reaktion. Der gesamte Verlauf des Angriffs.

Moderne Sicherheitsvorgänge erfordern Klarheit und Effizienz, zwei Dinge, die schwer zu erreichen sind, wenn Analysten Dutzende von unbearbeiteten Warnmeldungen für jede Bedrohung durchsuchen müssen. Der vorfallzentrierte Ansatz von WatchGuard Advanced EPDR und Orion konsolidiert mehrere Signale vom gleichen Endpoint zu einem einzigen, angereicherten Vorfall, der den gesamten Angriffsverlauf darstellt. Anstatt Warnmeldungen einzeln zu bearbeiten, untersuchen Analysten ein Gesamtbild, das die Zusammenhänge schnell aufzeigt.

> Ein Vorfall > Eine Ansicht > Eine Antwort

Warum das wichtig ist

Sicherheitsteams sehen sich oft einer überwältigenden Flut von Warnmeldungen ausgesetzt. Ein einzelner Angriff kann mehrere Benachrichtigungen für jeden Angriffsindikator (IoA), Befehlszeilenverhalten, Dateiablage oder Berechtigungseskalation auslösen. Das Ergebnis ist Überlastung:

- **Verlangsamt die Untersuchung**
- **Erhöht das Risiko von verpassten Signalen**
- **Verursacht Alarmermüdung**

Das Untersuchungsmodell von WatchGuard konzentriert sich auf Vorfälle und verwandelt diese fragmentierte Erfahrung in eine optimierte Erfahrung, reduziert Nebensächliches, priorisiert echte Positive und beschleunigt die Triage. Da Teams jetzt weniger, aber dafür umfangreichere, Vorfälle prüfen müssen, können sie mit weniger Aufwand mehr echte Bedrohungen erkennen.

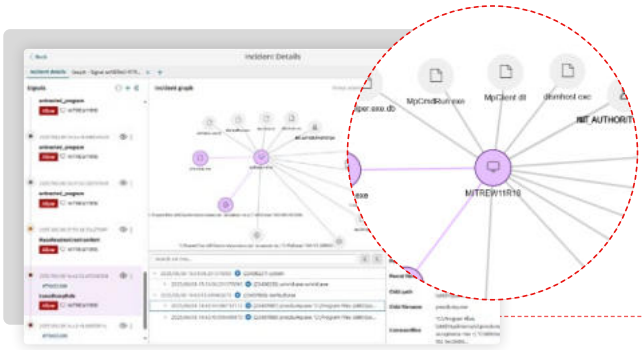
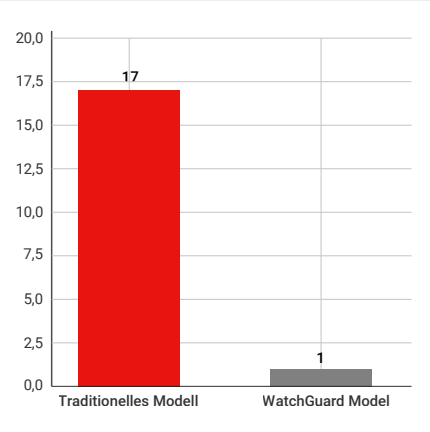


Abb. 1. Analysten können Signale hinzufügen oder ausblenden, den Vorfall mit einem umfassenderen Kontext durch den Prozessbaum hinweg untersuchen und Telemetrie zur Alarmzeit erfassen und das Aktivitätsdiagramm von Prozessen und Verhalten untersuchen. Verhaltensalarme werden MITRE ATT&CK-Techniken zugeordnet, um die Analyse zu erleichtern.

> Von Warnungen zu Vorfällen



> Eine einzelne, bösartige Aktivität kann in traditionellen Modellen Dutzende von Warnmeldungen auslösen – aber nur einen Vorfall in WatchGuard.

Weniger Lärm. Mehr Kontext. Höhere Effizienz der Analysten.

In realen Szenarien reduziert WatchGuard die Anzahl der Warnmeldungen um 70–80 % pro Vorfall auf Endpoint-Ebene und konsolidiert Ereignisse mit mehreren Warnungen in einer einzigen, kontextualisierten Ansicht, die Analysten hilft, sich auf das Wesentliche zu konzentrieren.

Strategische Vorteile

> Für Sicherheitsteams

- Verbessern Sie Ihren Effizienzindex: mehr Erkennungen, weniger Lärm
- Konzentrieren Sie sich auf das Wesentliche – korrelierte Vorfälle, keine fragmentierten Warnungen
- Reduzieren Sie Alarmermüdung und Untersuchungszeit

> Für MSPs

- Weiten Sie den Betrieb kundenübergreifend und mit weniger Zeitaufwand für Analysten aus
- Erhöhen Sie die Erkennungsgenauigkeit ohne SIEM- oder MDR-Abhängigkeiten
- Stellen Sie hochwertigere Erkenntnisse und Berichte für Endkunden bereit

> Für Führungskräfte

- Zeigen Sie Effizienzsteigerungen bei Erkennung und Reaktion auf
- Nutzen Sie Informationen auf Vorfallebene zur Unterstützung der Risiko- und Compliance-Berichterstattung
- Schaffen Sie die Grundlage für ergebnisorientierte Sicherheitsmetriken

> Was ist die Effizienz des Sicherheitsteams?

Die Effizienz des Sicherheitsteams ist die Fähigkeit, High-Fidelity-Bedrohungen mit minimalem operativem Aufwand zu erkennen und zu beheben. Die Effizienz schafft ein Gleichgewicht zwischen Erkennungserfolg, Arbeitsbelastung der Analysten und Signalqualität.

Wir drücken dies als Effizienzindex aus:

Effizienzindex = Erkennung / (False Positives + Anzahl an Alarmen)

Ein höherer Index bedeutet bessere Ergebnisse mit weniger Ablenkungen, weniger Alarmermüdung und schnelleren Entscheidungen. Der auf Vorfälle ausgerichtete Ansatz von WatchGuard wurde entwickelt, um diesen Index zu verbessern, indem korrelierte Signale zu verwertbaren Vorfällen kombiniert werden – wodurch redundante Warnmeldungen reduziert und gleichzeitig der Kontext erhalten wird.

Wichtigste Funktionen

Funktion	Beschreibung
Einheitliche Sicht auf Vorfälle	Aggregiert und korreliert Signale, die an einem einzigen Endpoint generiert werden, zu einem einzigen Vorfall. Kein Springen mehr zwischen isolierten Erkennungen.
KI-gestützte Korrelation und Aggregation	Verwendet Verhaltensanalysen, Sitzungskontext, Threat Intelligence und abgeleitete Muster, um den Angriffsverlauf zu rekonstruieren.
Anpassbarer Analyseumfang für Vorfälle	Analysten können Signale aus dem Vorfall manuell einbeziehen oder ausschließen, um den Vorfall zielgerichtet und fokussiert zu untersuchen.
Dynamische Anreicherung des Vorfalls	Vorfälle entwickeln sich weiter, wenn neue, verwandte Signale erkannt werden, sodass MITRE TTPs, Beziehungen zwischen Entitäten und chronologische Ereignisse hinzukommen.
Weniger Alarme	Mehrere Erkennungen werden zu einem einzigen Vorfall zusammengefasst. Analysten behandeln ein Objekt, nicht Dutzende von Warnmeldungen.
Ansicht des vollständigen Angriffsverlaufs	Die visuelle Zeitleiste zeigt den Fortschritt des Angreifers – wer, was, wann und wie – und unterstützt die Ursachenanalyse (Root Cause Analysis, RCA) und Abhilfemaßnahmen.

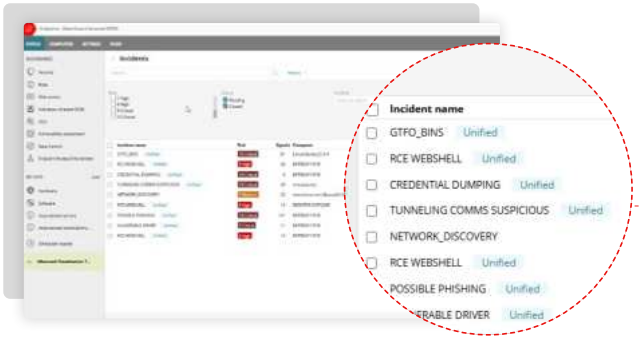


Abb. 2. Die Vorfall-Liste enthält ausstehende und gelöste Fälle, geordnet nach Wichtigkeit. Dank der automatischen Korrelation von Warnungen zu Vorfällen können sich Analysten auf das Wesentliche konzentrieren und effizienter arbeiten.

Die Zahlen hinter den verschiedenen Alarmen

1. Stoppen einer Kampagne zum Diebstahl von Zugangsdaten, bevor sie sich ausbreitet

Ein verwalteter Endpoint löst eine Warnung für eine ungewöhnliche Anmeldung aus. Kurz darauf erscheint ein PowerShell-Befehl und schreibt in einen sensiblen Registrierungsschlüssel. Herkömmliche Tools generieren separate Warnungen für jede Aktion, sodass Analysten die einzelnen Punkte manuell miteinander in Beziehung bringen müssen. Mit WatchGuard werden diese Signale automatisch zu einem einzigen Vorfall korreliert, der den gesamten Angriffsverlauf, einschließlich Abfolge und Kontext, anzeigt.

> **Ergebnis: Der Analyst erkennt schnell die Gefährdung, isoliert den Endpoint und leitet das Zurücksetzen der Anmeldedaten ein, bevor die Bedrohung eskaliert.**

2. Untersuchung eines dateilosen Angriffs, der durch eine Phishing-E-Mail ausgelöst wurde

Ein Anwender öffnet eine E-Mail-Anlage, die ein Skript ablegt, das dann einen WMI-Befehl ausführt, um für längere Zeit im System zu verbleiben. Die Vorfallansicht von WatchGuard verknüpft Signale aus der Dateiausführung, dem Skriptverhalten und dem WMI-Missbrauch zu einem Vorfall, der mit MITRE-Taktiken, -techniken und -verfahren (TTPs) und dem Verlauf angereichert wird.

> **Ergebnis: Der Analyst versteht den Ursprung und das Fortschreiten der Bedrohung an einem Ort – ohne zwischen mehreren Tools oder Protokollen wechseln zu müssen.**

3. Reduzierung von False Positives aus repetitiven Verhaltenserkennungen

Ein Endpoint beginnt, mehrere Warnungen für Verhaltensanomalien auszulösen – Dateiveränderungen, nicht signierte Binärdateien und Registrierungsänderungen. Anstatt separate Warnungen zu generieren, konsolidiert WatchGuard diese in einem priorisierten Vorfall, der mit Kontext und einer Bewertung des Schweregrads angereichert wird.

> **Ergebnis: Nebensächliches wird reduziert, echte Bedrohungen heben sich ab und Analysten können sich auf die wichtigsten Punkte konzentrieren.**

Abb. 3. Das Aktivitätsdiagramm stellt die Rekonstruktion der Prozesse und ihrer Aktivitäten im Laufe der Zeit für Analysten visuell dar. So können sie besser verstehen, wie sich der Angriff entwickelt hat, und können jeden Schritt in der Ausführungskette nachverfolgen.

Möchten Sie sehen, wie die vorfallsorientierte Untersuchung die Effizienz Ihres Teams steigert?

Fordern Sie noch heute eine Demo an und entdecken Sie, wie WatchGuard Ihnen hilft, mit weniger mehr zu erkennen, Alarmermüdung zu reduzieren und Untersuchungen zu beschleunigen.

Informationen zu WatchGuard

WatchGuard® Technologies, Inc. gehört zu den führenden Anbietern im Bereich Cybersicherheit. Unser Unified Security Platform®-Ansatz ist speziell auf Managed Service Provider ausgelegt, damit sie erstklassige Sicherheit bieten können, die die Skalierbarkeit und Schnelligkeit des 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 über 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 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 WEB: www.watchguard.de WatchGuard Technologies, Inc.

© 2025 WatchGuard Technologies, Inc. Alle Rechte vorbehalten. WatchGuard und das WatchGuard-Logo sind eingetragene Marken von WatchGuard Technologies, Inc. in den USA und/oder anderen Ländern. Alle weiteren Markennamen sind das Eigentum ihrer jeweiligen Inhaber. Teilenr. WGCE67865_090425