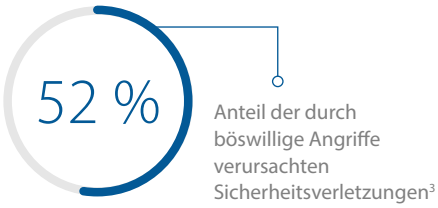
# Threat Hunting Service

## Anzahl von Cyberbedrohungen und verdeckten Angreifern immer höher

Die Cyberkriminalität stellt für Unternehmen und Behörden eine andauernde Gefahr dar. Die Daten zeigen eine rapide Zunahme der Anzahl (jährliche Steigerung von 11 %[1]) und Ausgereiftheit der Angriffe sowie der Kosten, die diese für Unternehmen verursachen. (Die durchschnittlichen Gesamtkosten einer Sicherheitsverletzung für Unternehmen mit mehr als 25.000 Mitarbeitern betragen 5,52 Mio. USD und für Unternehmen mit weniger als 500 Mitarbeitern 2.64 Mio. USD.[2])

Obwohl die zunehmenden Investitionen in die Cybersicherheit (+ 10 %, 60,2 Mrd. USD[3]) zu einem verbesserten Schutz beigetragen haben, gibt es keine absolute Sicherheit. Unternehmen können es sich nicht leisten, einen Angriff abzuwarten und erst dann Maßnahmen zu ergreifen, denn so gewinnen Angreifer nur Zeit, um auf das Unternehmensnetzwerk zuzugreifen.




Anteil der durch böswillige Angriffe verursachten Sicherheitsverletzungen[3]

Land mit den höchsten Kosten aufgrund von Sicherheitsverletzungen[3]

Sobald sie einmal eingedrungen sind, verstecken sich böswillige Angreifer in der charakteristischen Struktur und der Komplexität der Umgebung ihres Opfers. Dabei nutzen sie häufig legitime Mechanismen und verbergen ihre Aktivitäten im normalen Datenverkehr des Netzwerks, um ihre Ziele zu verfolgen. Je nachdem, wie ausgereift die Sicherheitsvorkehrungen im Zielnetzwerk sind, hat ein Angreifer so häufig sehr viel Zeit, sein böses Werk zu vollbringen.

## Was Sie über Cyberangriffe wissen sollten

Beim Threat Hunting wird aktiv nach Cyberbedrohungen gesucht, die sich unerkannt im Unternehmensnetzwerk verstecken. Ihre Umgebung wird eingehend untersucht, um böswillige Angreifer aufzudecken, die herkömmliche Sicherheitsmaßnahmen umgehen konnten.

Ist ein Angreifer erst einmal drin, kann er sich manchmal monatelang unerkannt in einem Netzwerk aufhalten. Er wartet dann auf die perfekte Gelegenheit, um Daten zu stehlen, vertrauliche oder personenbezogene Informationen aufzudecken, wichtige Mitarbeiter im Unternehmen zu erkennen und deren Anmeldedaten abzugreifen, mit denen er sich dann ungehindert in der gesamten Umgebung bewegen kann.

Nachdem ein Angreifer unerkannt ins Netzwerk eindringen konnte und mit seinem Angriff beginnt, fehlt es vielen Unternehmen am notwendigen Budget, an der Technologie, den Prozessen und vor allem an einem Team von Experten, um solch einen Angriff zu verhindern und zu erkennen. Für diese Unternehmen ist es unmöglich, entsprechende Abwehrmaßnahmen mit der gleichen Geschwindigkeit zu verbessern, mit der sich die Cyberkriminalität ausbreitet.

-3,58 MILLIONEN $

Kosteneinsparungen bei vollständig bereitgestellter Automatisierung in Vergleich zu keiner Automatisierung[3]

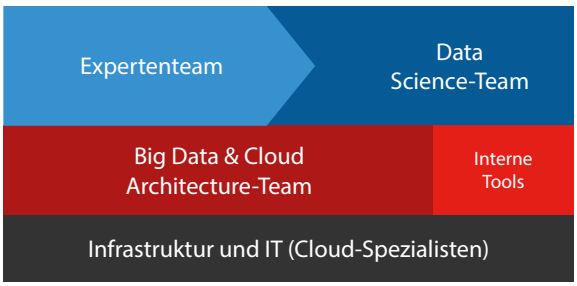
315 TAGE

Durchschnittliche Zeit zum Erkennen und Eindämmen einer Sicherheitsverletzung durch einen böswilligen Angriff[3]

Während die Anzahl erfolgreicher Cyberangriffe rapide ansteigt, ist es besonders wichtig, proaktiv vorzugehen, um sie zu erkennen. Sie dürfen nicht passiv bleiben und sich auf eine automatische Warnung verlassen, die Sie auf einen Angriff aufmerksam macht. Sie müssen aktiv nach potenziell böswilligem Verhalten in Ihrem Netzwerk suchen und Indikatoren für Angriffe (IoA) ausmachen, damit Sie einen Vorfall so schnell wie möglich erkennen und darauf reagieren können.

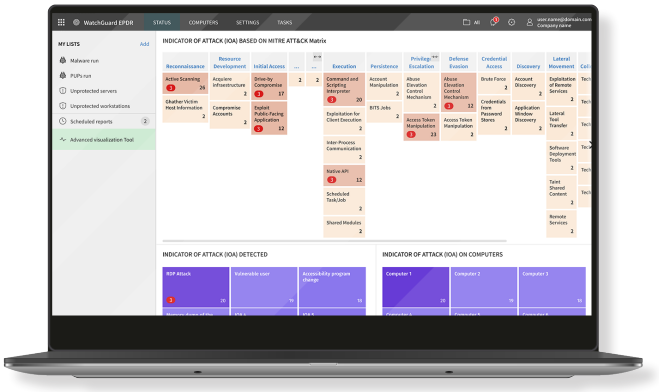
# Jagd nach dem Unbekannten

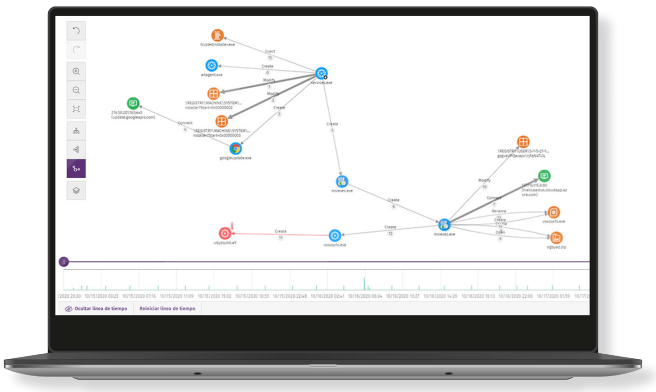
Die laufende Überwachung der Endpoint-Aktivität durch WatchGuard ermöglicht dem Agent, als Sensor zu fungieren und die Cloud-Plattform nicht nur über die ausgeführten Dateien zu informieren, sondern auch über deren Ausführungskontext (was ist direkt vor der Ausführung passiert, welche Benutzer versuchen, welche Befehle oder Anwendungen auszuführen, welcher Netzwerkdatenverkehr wird generiert, auf welche Datendateien wird zugegriffen, Parameter usw.).



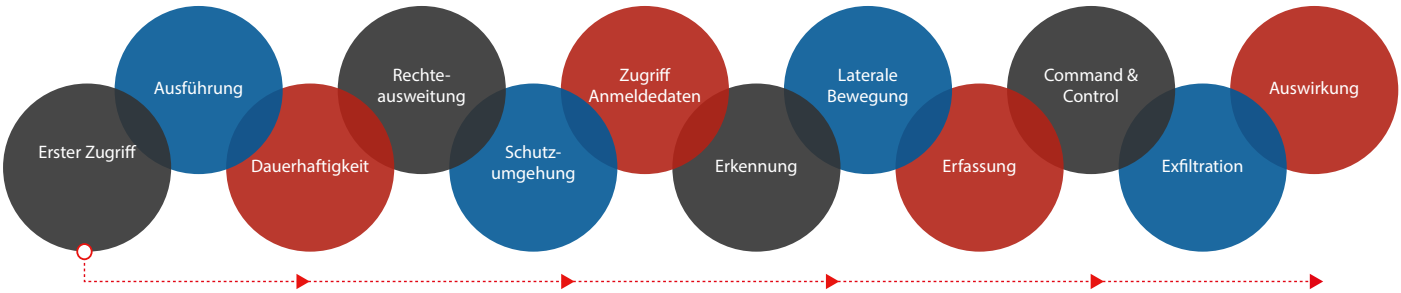

So kann unser Threat Hunting Service ungewöhnliche Verhaltensweisen und verdächtige Aktivitäten erkennen und diese mit hoher Sicherheit und ohne falsch positive Ergebnisse als Angriffsindikatoren kategorisieren.

Wir bei WatchGuard haben das MITRE ATT&CK™ Framework (eine global zugreifbare Wissensdatenbank mit Angriffstaktiken und -techniken basierend auf realen Beobachtungen) über mehrere WatchGuard Endpoint Security-Prozesse und Produktfunktionen implementiert, um die Produktivität von Analysten zu verbessern und Sicherheitsverletzungen zu verhindern. Durch die Umsetzung dieses Frameworks haben wir die folgenden spezifischen Phasen von Angriffsindikatoren in die WatchGuard EPDR- und WatchGuard EDR-Lösungen aufgenommen.





Angriffsindikatoren sind häufig mit bestimmten Phasen der Cyber Kill Chain oder den Taktiken im MITRE ATT&CK Framework verknüpft, das von den erweiterten WatchGuard Endpoint Security-Lösungen übernommen wurde.




Das Erkennen von Angriffsindikatoren, bevor Daten abgezogen (oder im Falle von Ransomware-Angriffen verschlüsselt) werden, ist ein sehr effektiver Verteidigungsmechnismus, insbesondere gegen LotL-Angriffe (Living-off-the-Land) und selbst dann, wenn Endpoints bereits manipuliert wurden.

WatchGuard EDR und WatchGuard EPDR integrieren innerhalb des gleichen Schutz-Agents einen umfassenden Technologie-Stack, um Angriffsindikatoren in verschiedenen Angriffsphasen zu erkennen. Sie sind keine statische Technologie, sondern werden ständig mit neuen Angriffsmustern und -techniken aktualisiert, die vom Threat Hunting Service erkannt werden.

Hacker führen **extrem ausgereifte Cyberangriffe** durch. Es gibt keine Sicherheitsmaßnahmen, die einen 100%igen Schutz gewährleisten. Insbesondere dateilose Angriffe stellen eine zunehmende Bedrohung dar, da sie immer schwieriger zu erkennen sind. **Hacker hinterlassen aber immer Spuren**, anhand derer wir unbekannte Angriffe erkennen können, die Living-off-the-Land-Techniken nutzen.

**Der automatisierte Threat Hunting Service von WatchGuard überwacht ständig alles**, was an den Endpoints passiert, und zwar in Echtzeit und in Form vom **Ereignistelemetrie**. Im Falle eines **bestätigten Angriffs** durch eine LotL-Technik wird der Angriffsindikator in der Webkonsole angezeigt und aufgezeichnet.

RDP-Brute-Force-Angriffe, Rechteausweitung, dateilose Angriffe und laterale Bewegungen sind Beispiele für Angriffsindikatoren, die der Threat Hunting Service erkennt, der als kostenlose Ergänzung in unseren EDR-Lösungen enthalten ist.

## Der automatisierte Threat Hunting Service – das nicht Erkennbare erkennen

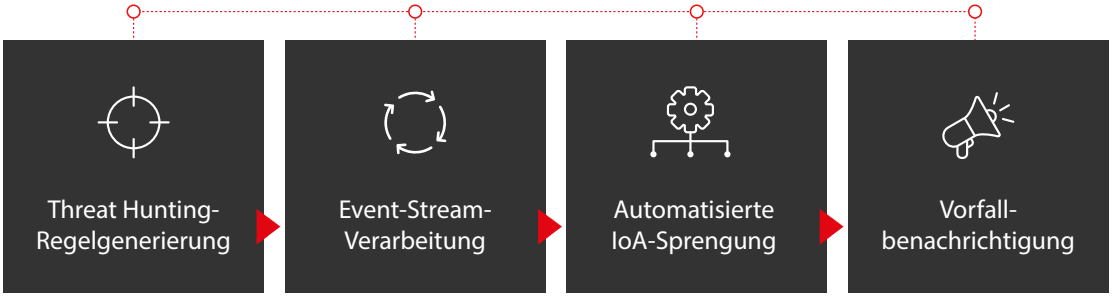
Unser Threat Hunting Service, enthalten in WatchGuard EDR und WatchGuard EPDR, basiert auf einer Reihe von Threat-Hunting-Regeln, die von Bedrohungsspezialisten entwickelt wurden und die automatisch auf alle durch die Telemetrie erfassten Daten angewendet werden. Hierdurch werden höchst zuverlässige Angriffsindikatoren ausgelöst und die Anzahl der falsch positiven Meldungen verringert, um den MTTD- und MTTR-Aufwand zu minimieren („Mean Time To Detect“ und „Mean Time To Respond“).

Diese Angriffsindikatoren sind ein Ergebnis des fortlaufenden Prozesses zur Erkennung von Angreifern anhand einer fortschrittlichen Datenanalyse, unserer eigenen Bedrohungsanalyse und des Fachwissens unserer Analysten.

Dieser Service nutzt die umfassende Cyberintelligence, die wir in all den Jahren unserer Erforschung von Cyberbedrohungen perfektioniert haben, sowie die Einblicke in einen Katalog von Anwendungsverhalten, der seit mehr als 30 Jahren über mehr als 10 Mrd. Ereignisse pro Tag, Benutzer und Computer erhält. Wir pflegen strategische Partnerschaften mit internationalen Organisationen wie der Cyber Threat Alliance, mit denen wir Angriffsindikatoren (IoAs), Gefährdungsindikatoren (IoCs) und die entsprechenden Reaktionen austauschen.

Fall sie eine ungewöhnliche Situation beobachten, wird der Kunde über die Webkonsole informiert, in der Details und Diagramme zu der Anomalie, eine forensische Analyse der betroffenen Systeme, der Ursprung des Angriffs und die verwendeten Techniken angezeigt werden. Sie stellen außerdem Empfehlungen bereit, welche Maßnahmen gegen den Angriff unternommen und wie die Angriffsoberfläche verringert werden kann, damit Sie in Zukunft nicht mehr ein Opfer solcher Angriffe werden.

### Funktionsweise des Threat Hunting Service




*1. Help Net Security: 2020: The year of increased attack sophistication*
*2. Canalys: Cybersecurity investments will increase up to 10% in 2021*
*3. Ponemon Institute and IBM Security: Cost of a Data Breach Report 2020*

## Über WatchGuard

WatchGuard® Technologies, Inc. gehört zu den führenden Anbietern im Bereich Netzwerksicherheit, Endpoint-Sicherheit, sicheres WLAN, Multifaktor-Authentifizierung und Network Intelligence. Über 18.000 Vertriebspartner und Dienstleister im Bereich Sicherheit verlassen sich auf die prämierten Produkte und Services des Unternehmens und sorgen somit für den Schutz von mehr als 250.000 Kunden. Die Philosophie von WatchGuard ist es, Sicherheit auf Enterprise-Niveau für Unternehmen jeder Größenordnung und Art zu realisieren. Das macht WatchGuard insbesondere für mittelständische und dezentral aufgestellte Unternehmen zum idealen Anbieter. 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.com/de.

Deutschland, Österreich, Schweiz +49 700 92229333 INTERNATIONALER VERTRIEB +1.206.613.0895 watchguard.com/de