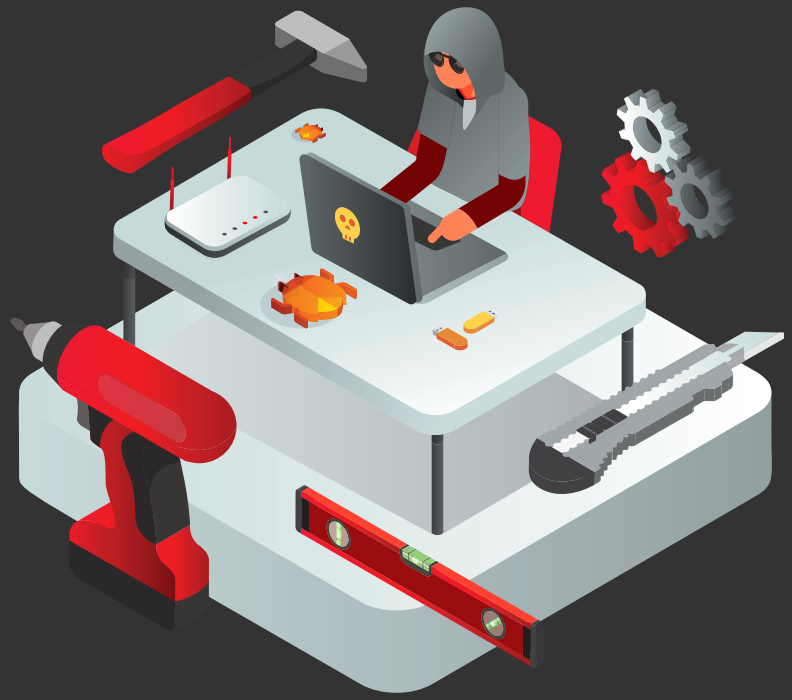
Fortschrittliche Endpoint-Sicherheit für SOCs

PROAKTIVER UMGANG MIT IHRER CYBERSICHERHEIT

Ihr Threat Hunting vereinfacht mit WatchGuard

Index



WatchGuard

Ihr Threat Hunting vereinfacht mit WatchGuard für SOCs

Ausbreitung

Wenn es um Sicherheit geht, ist nichts hundertprozentig sicher.

Es ist klar, dass keine Organisation immun ist, unabhängig von ihrem Standort, ihrer Größe oder der Branche, in der sie tätig ist.

- Da die Gegner ihre Methoden immer weiter verfeinern, war es noch nie so wichtig wie heute, technologiebasierte Kontrollen durch menschliches Fachwissen zu ergänzen.
- Das Tempo der gegnerischen Aktivitäten nimmt ebenfalls rapide zu. Zudem werden die Gegner immer geschickter darin, mit weniger mehr zu erreichen.
- Bei vielen Angriffen wird heute dateilose Malware eingesetzt, die in einigen Phasen des Angriffs die sich ständig weiterentwickelnden „Living off the Land"-Techniken nutzt.

Was bedeutet dies für die Wirksamkeit des Sicherheitsprogramms der Organisation?

Die Bedrohungsakteure von heute sind gut organisiert, hoch qualifiziert, motiviert und auf ihre Ziele fokussiert. Diese Angreifer könnten in Ihrem Netzwerk lauern oder damit drohen, in Ihr Netzwerk einzudringen, und immer stärker ausgefeilte Methoden anwenden, um ihr Ziel zu erreichen. Einfach ausgedrückt besteht für Angreifer oft keine Notwendigkeit, in den frühen Phasen eines Angriffs Malware zu installieren. Sie besitzen in der Regel alle notwendigen Werkzeuge, um in das Netzwerk einzudringen, sich dort ungehindert zu bewegen und die legitimen Anwendungen an den Endpoints zu instrumentalisieren.

Darüber hinaus können die Angriffe von vielen verschiedenen Bedrohungsoberflächen ausgehen. So sollen die vielen Schwachstellen ausgenutzt werden, die im Netzwerk, an den Endpoints und bei den Mitarbeitern eines Unternehmens vorhanden sein können. Das Schlimmste dabei ist, dass Unternehmen nicht wissen, von wem, wann, wo oder wie ein gut geplanter Angriff erfolgen wird. Selbst fortschrittliche Erkennungsmechanismen können heute nur schwer vorhersehen, wie sich die Angriffsvektoren zukünftig entwickeln werden.

Dieser Trend stellt die Sicherheitsprogramme von Unternehmen vor immense Herausforderungen. Er macht deutlich, wie wichtig eine Kombination aus technologiebasierter Kontrolle und einem von Menschen geleiteten, proaktiven Threat-Hunting-Service ist, um sicherzustellen, dass Unternehmen schneller reagieren, als Bedrohungen auftreten, und gut geschützt und widerstandsfähig bleiben.

Angreifer, die **LotL** verwenden, suchen auf den Zielsystemen nach Werkzeugen, wie z. B. Betriebssystemkomponenten, Fehlkonfigurationen oder installierte Software, die sie zur Erreichung ihrer Ziele nutzen können. LotL-Angriffe werden als dateilose Malware eingestuft, da sie keine Artefakte hinterlassen.

Als „Living-off-the-land"-(LotL)-Angriff bezeichnet man einen Cyberangriff, bei dem Hacker legitime Software und Funktionen des Systems für böswillige Machenschaften nutzen.

WatchGuard

1. Die Threat-Hunting-Funktion

Threat Hunting ist eine häufig falsch verstandene Nischenfunktion. Daher sollten wir zunächst klären, was wir mit dem Begriff Threat Hunting meinen.

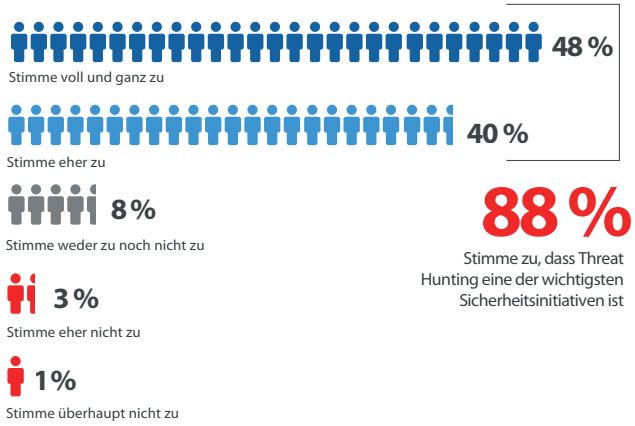
Es kann als analystenzentrierter Prozess definiert werden, mit dem Unternehmen verborgene, komplexe Bedrohungen ans Licht bringen können, die von automatisierten vorbeugenden und aufdeckenden Kontrollmechanismen übersehen werden. Einfach ausgedrückt: Threat Hunting soll unbekannte Bedrohungen enttarnen, die in der Lage sind, technologiebasierte Kontrollen zu umgehen.

Beim Threat Hunting geht es um das letzte 1 % der unbekannten Verhaltensweisen. Es geht nicht darum, Malware zu finden und abnormale Aktivitäten zu identifizieren. Technologie stellt die notwendige Ausgangsbasis dar, um Bedrohungen in der Cyber-Kill-Chain proaktiv zu erkennen und zu stoppen, bevor der Schaden entsteht. Obwohl es beim Threat Hunting nicht darum geht, Malware zu finden, kommt das in den WatchGuard Advanced Endpoint Security-Lösungen enthaltene Threat Hunting dem Zero-Trust Application Service zugute. Es sorgt für das Blockieren aller Angriffe beim Versuch einer bösartigen Anwendung, ausgeführt zu werden, selbst wenn das anormale Verhalten nicht gestoppt wird.

Threat Hunting ist eine der wichtigsten Sicherheitsinitiativen

Obwohl Threat Hunting noch eine junge Disziplin ist, besteht laut der letzten Umfrage von Cybersecurity Insiders über den Reifegrad der Sicherheitspraxis Threat Hunting daran ein großes Interesse.

Laut Pulse **geben 32 Prozent der IT-Führungskräfte an, dass ihre Unternehmen planen, die Sicherheit ihrer Endpoints zu verbessern, indem sie ein Threat Hunting-Programm in ihre allgemeine Sicherheitsstrategie aufnehmen.**



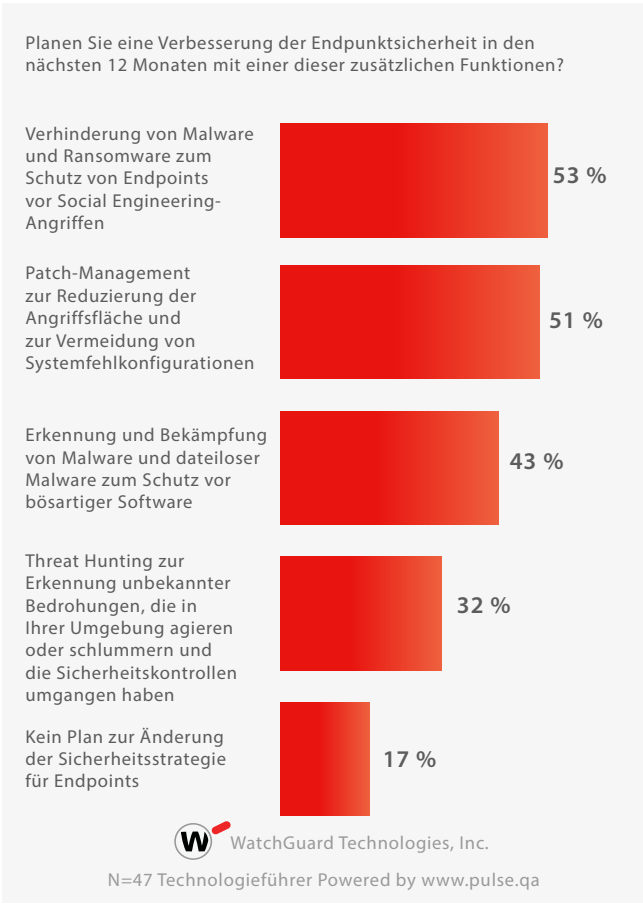


Abbildung 1. WatchGuard Advanced EDR und Advanced EPDR bieten Ihnen in Kombination mit dem Threat Hunting Service und WatchGuard Patch Management eine einzige Lösung, um damit alle in den nächsten 12 Monaten geplanten zusätzlichen Funktionen abzudecken.

Mit nur einem einzigen, schlanken Agenten, der über eine einzige cloudbasierte Konsole verwaltet wird, stellen sie eine natürliche Erweiterung Ihres aktuellen Serviceangebots dar.

Threat Hunting ist eine Disziplin, die Unternehmen nicht mehr als ein optionales Extra, sondern als unverzichtbar betrachten sollten. Es sollte sich um eine kontinuierliche Funktion handeln, wie sie für jedes robuste Cybersicherheitsprogramm unerlässlich ist, und nicht um eine punktuell aktivierte Funktion.

WatchGuard

So fügt sich die Threat-Hunting-Funktion in Ihr Sicherheitsprogramm ein

Unternehmen haben sich bisher auf Prävention und richtlinienbasierte Sicherheitskontrollen verlassen. Heute werden Unternehmen massiv mit fortschrittlichen und gezielten Angriffen konfrontiert. Für komplexe Bedrohungen gehört nicht viel dazu, diese Sicherheitsvorkehrungen zu überwinden. Unternehmen sind somit ungeschützt und haben nur einen begrenzten oder gar keinen Einblick in die Bedrohungsaktivitäten.

Neben der Reduzierung der Angriffsfläche und der Verstärkung ihrer Präventionskapazitäten müssen die Sicherheitsteams einen proaktiven Sicherheitsansatz verfolgen.

Sie müssen einen robusten und vollständigen Lebenszyklus des Bedrohungsschutzes implementieren, Bedrohungen im Netzwerk und an den Endpoints effektiv aufspüren und entsprechend reagieren. Ihr Ziel muss es sein, Sicherheitsverletzungen zuvorzukommen und die Normalität so schnell wie möglich wiederherzustellen.

Dies bedeutet ein **Umdenken mit Blick auf die Sicherheit. Es muss zu einem Wechsel von Prävention und Reaktion auf Vorfälle hin zu proaktiver und kontinuierlicher Reaktion kommen,** basierend auf der Annahme, dass die Organisationen gefährdet ist und ständige Überwachung und Abhilfe notwendig sind.

Jede Minute produzieren Benutzer und Endgeräte, die von diesen Organisationen verwendet werden, wertvolle Telemetriedaten über das, was im gesamten Unternehmen geschieht. Die überwiegende Mehrheit dieser Telemetriedaten bezieht sich auf legitime alltägliche Aktivitäten.

Nach der Analyse **durch fortschrittliche Sicherheitstechnologien wie maschinelles Lernen und Verhaltensanalyse werden jedoch abnormale Verhaltensweisen erkannt, die Sicherheitssignale auslösen.**

Die Ausführung dieses Standardprozesses, der auf der automatisierten Analyse abnormaler Verhaltensweisen basiert, erfordert spezifische Technologien, Prozesse und Analysen.

Threat Hunting ist eine Funktion, die parallel zu diesem Arbeitsablauf arbeitet. Ihre wesentliche Funktion besteht in der Verwendung von Abfragen an den Data Lake und spezifischen Tools, um Erkenntnisse aus der Telemetrie zu gewinnen und neue deterministische Analysen zu automatisieren. Außerdem gehören zum Threat Hunting auch die kombinierte Anwendung dieser neuen Analysen auf die Telemetrie und die Kontextualisierung schwacher Signale, um die Identifizierung tatsächlicher Angriffe zu optimieren.

Wird die Threat-Hunting-Funktion in Echtzeit ausgeführt, verkürzt sich die Zeit, um auf Bedrohungen zu reagieren, erheblich.

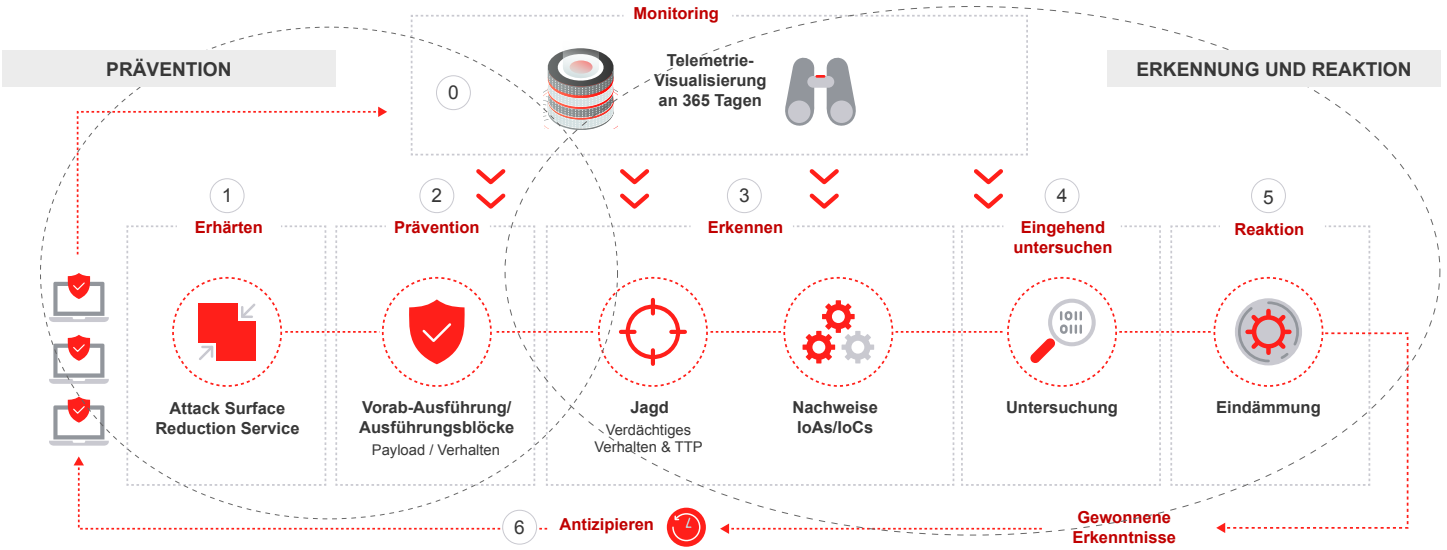


Abbildung 2. Der Lebenszyklus des Bedrohungsschutzes, den ein robustes Sicherheitsprogramm abdecken muss

2. Die Threat-Hunting-Vorgänge

Die Aktivitäten rund um Threat Hunting-Vorgänge lassen sich grob in drei Hauptgruppen einteilen:

- Der analytisch orientierte Ansatz. Beim Threat Hunting werden statistische Methoden angewendet, um Ausreißer zu untersuchen und häufige Analysen durchzuführen. So werden nie zuvor gesehene Aktivitäten oder Unregelmäßigkeiten erkannt, die nach den Basisdaten für die Umgebung bösartig sein könnten.
- Beim hypothesenbasierten Ansatz haben erstklassige Bedrohungsjäger die Möglichkeit, kreativ zu werden und wie der Gegner zu denken. Es geht darum, Theorien darüber zu entwickeln und zu testen, wo und wie ein entschlossener Angreifer versuchen könnte, zu operieren, sich im Netzwerk zu bewegen und unbemerkt zu verweilen, bis er entscheidet, dass der beste Zeitpunkt für einen Angriff gekommen ist.
- Der intelligente Ansatz schließlich ist die gängigste Vorgehensweise und beinhaltet die Verwendung aktueller Bedrohungsdaten, um historische Daten nach Signalen für Eindringversuche zu durchsuchen. Heutzutage neigen viele Unternehmen dazu, diesen Ansatz selbst zu integrieren. Sie verwenden dazu eine Sammlung bekannter IoCs, wie IP-Adressen oder Hashes.

Beim Threat Hunting sollten sich Bedrohungsanalysen nicht mit der Verwendung von IoCs zufrieden geben. Wichtiger für Bedrohungsjäger sind Bedrohungsanalysen, die als Tools, Techniken und Prozeduren (TTP) bezeichnet werden. TTP können definiert werden als „Muster von Aktivitäten oder Methoden, die mit einer bestimmten Bedrohung oder einer Gruppe von Bedrohungen verbunden sind".

TTP sind für einen Angreifer im Vergleich zu IoCs viel schwieriger zu modifizieren. Angreifer verwenden ihre TTP bei allen Angriffen wieder, ändern aber die Binärdateien oder die „Command and Control"-(C&C)-Infrastruktur. Das Ändern einer C&C-IP-Adresse ist zum Beispiel banal. Das Ändern des verwendeten Kommunikationsprotokolls ist dagegen wesentlich schwieriger, da dafür ein hoher Programmieraufwand erforderlich ist. Das MITRE ATT&CK-Framework versucht, diese TTP in etwas Brauchbares zu verwandeln.

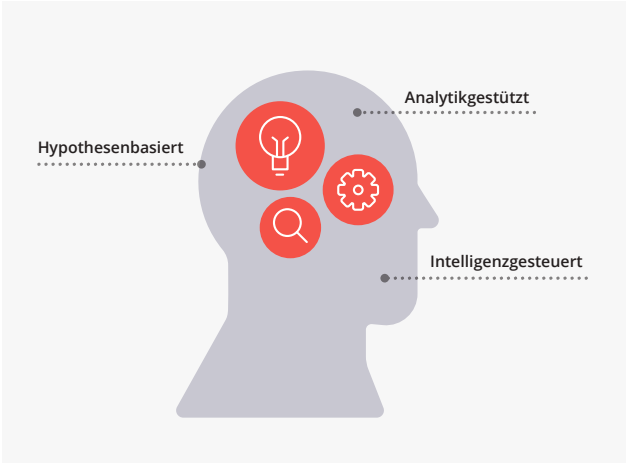
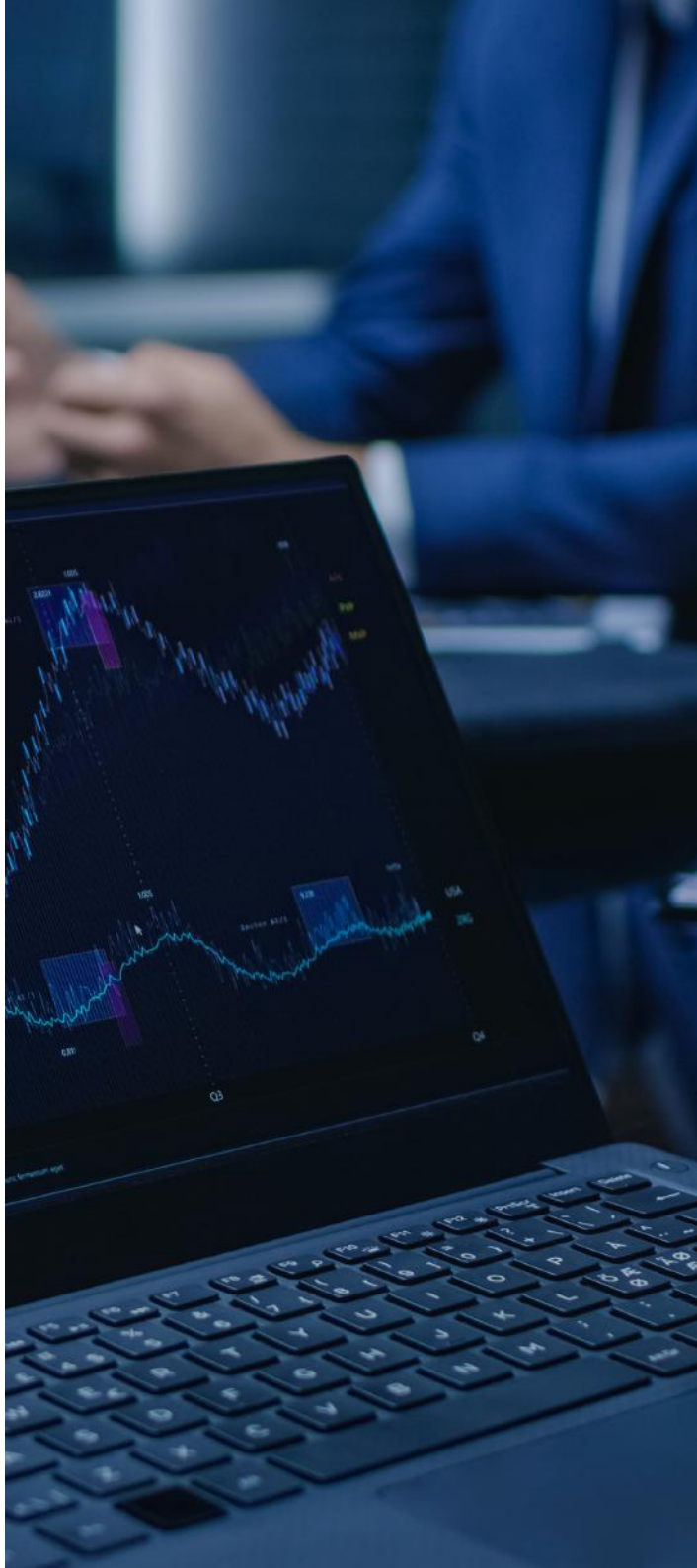


Abbildung 3. Bedrohungsjäger und Analysten von WatchGuard überwachen kontinuierlich alles, was in Echtzeit und rückwirkend (365 Tage) in der Telemetrie aller unserer Kunden geschieht bzw. geschehen ist. Kontinuierliche Echtzeit-Überwachung, Technologien und von Menschen geleitete proaktive Hunting-Services ermöglichen durch die Nutzung von LotL-Techniken die Enttarnung von Hackern und böswilligen Mitarbeitern.



3. Der Wert des Threat Hunting

Threat Hunting bietet Unternehmen unter anderem die folgenden Vorteile:

Frühzeitige Entdeckung und Unterbrechung interner und externer Bedrohungen, die technologiebasierte Kontrollen umgangen haben, bevor es zu einer Sicherheitsverletzung kommt.

Ergänzung der bestehenden technologiebasierten Kontrollen durch menschliches Fachwissen.

Erweiterung der Sicherheitstechnologien durch menschliches Fachwissen, um die Verweildauer zu verkürzen.

Threat Hunting nutzt die menschliche Erfahrung, um hochentwickelte Angriffe zu erkennen und zu stoppen, die andernfalls Tage, Wochen oder sogar Monate lang unentdeckt bleiben würden. Es verkürzt die Verweildauer und ist der Schlüssel zur zuverlässigen Verhinderung von Sicherheitsverletzungen.

Es liefert Sicherheitsteams Erkenntnisse, mit denen sie ausreichend gerüstet sind, um Angreifer in großem Umfang zu stören

Auch wenn die Jagdaktivitäten in der ersten Phase stattfinden, ist die Schlacht erst halb gewonnen, wenn diese unbekannten Bedrohungen aufgedeckt werden. Ein gut strukturiertes und wirksam umgesetztes Threat-Hunting-Programm gibt den Sicherheitsteams die Erkenntnisse an die Hand, die sie benötigen, um die Bedrohungen zu stoppen.

Es trägt dazu bei, die Angriffsfläche zu verringern und die automatischen Erkennungsfunktionen zu verbessern.

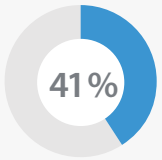
Neue Muster müssen zur Optimierung der Erkennungsfunktionen genutzt werden, so dass Bedrohungen keine Verstecke mehr finden.

Was sind die Hauptziele des Threat-Hunting-Programms Ihrer Organisation?[1]

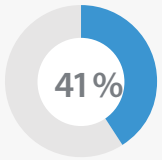
51 %
Verringerung der Gefährdung durch interne Bedrohungen

45 %
Verringerung der Anzahl von Sicherheitsverletzungen und Infektionen

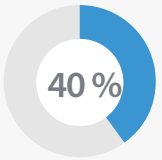
43 %
Reduzierung der Angriffsfläche



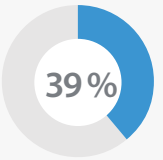
Verkürzung der Zeit bis zur Eindämmung (Ausbreitung verhindern)



Verringerung der Gefährdung durch externe Bedrohungen



Schnellere und genauere Reaktion auf Bedrohungen



Verkürzung der Verweilzeit von der Infektion bis zur Entdeckung

WatchGuard

4. Hindernisse für ein erfolgreiches Threat-Hunting-Programm

Die Einrichtung eines internen Threat-Hunting-Programms ist mit einigen Herausforderungen verbunden. Die wichtigste Aufgabe besteht darin, qualifizierte Mitarbeiter zu finden und die vorhandenen Mitarbeiter zu schulen.

Mit qualifizierten und sachkundigen Mitarbeitern kann ein Unternehmen die Werkzeuge und Technologien besser auswählen und die für die Durchführung eines Threat-Hunting-Programms erforderlichen Prozesse besser definieren. Die wichtigsten Herausforderungen bei der Umsetzung von Aktivitäten für die Bedrohungsjagd sind im Folgenden zusammengefasst:

1. Fehlen von Fachleuten für das Threat Hunting

Entscheidungen darüber, was und wie Analysen zur proaktiven Erkennung und Steuerung von Eingangsdaten und Fragen automatisiert werden sollen, können nur erfahrene Schwachstellenforscher treffen. Diese Fragen bleiben angesichts der sich ständig verändernden Bedrohungen nicht statisch. Erfahrene Spezialisten müssen diese daher ständig anpassen. Dies bedeutet, dass Sie die kontinuierliche Bedrohungsjagd in Ihre täglichen Sicherheitsabläufe einbinden müssen.

Viele Unternehmen versuchen, das Threat Hunting als zusätzliche Aufgabe an Sicherheitsanalysten zu delegieren, die bereits mit einer Unzahl täglicher Aufgaben jonglieren. Threat-Hunting-Aktivitäten werden daher dann durchgeführt, wenn es die Zeit erlaubt, und oft fehlt die erforderliche Struktur, um die Erkenntnisse und Beobachtungen zu definieren, auszuführen und anzuwenden.

Die Threat Hunting Services von WatchGuard liefern Top-Expertise für das Threat Hunting und erweitern die bereits vorhandenen Fähigkeiten des Sicherheitsteams.

2. Mangel an strukturierten Arbeitsabläufen zur Beschleunigung der Verarbeitung

Strukturierte Arbeitsabläufe und Beständigkeit sind heute der Schlüssel zum Erfolg bei der Bedrohungsjagd in Unternehmen.

Ein ad-hoc- oder unstrukturierter Ansatz bei der Bedrohungsjagd verringert die Erfolgschancen gegenüber Bedrohungen, die gut organisiert und mit guten Ressourcen ausgerüstet sind.

Der Threat Hunting-Prozess von WatchGuard basiert auf einer gut strukturierten Jagdmethode, die die wertvollen und langfristigen Telemetriedaten (365 Tage) optimal nutzt. Er umfasst die Werkzeuge und Arbeitsabläufe, die notwendig sind, um die Telemetrie zu optimieren und nach unentdeckten Bedrohungen zu suchen. Gleichzeitig integriert er die Technologien und Prozesse, die sicherstellen, dass die beim Threat Hunting gemachten Entdeckungen genutzt werden, um die automatischen Erkennungsfähigkeiten zu verbessern und unmittelbare Erkenntnisse zu liefern, um Bedrohungen zu entschärfen und die Angriffsfläche zu reduzieren.

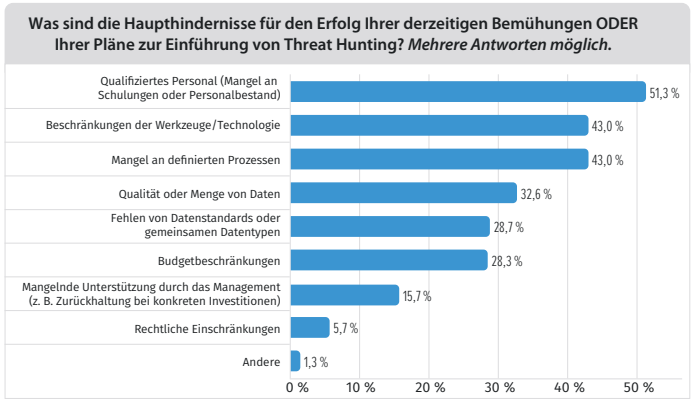
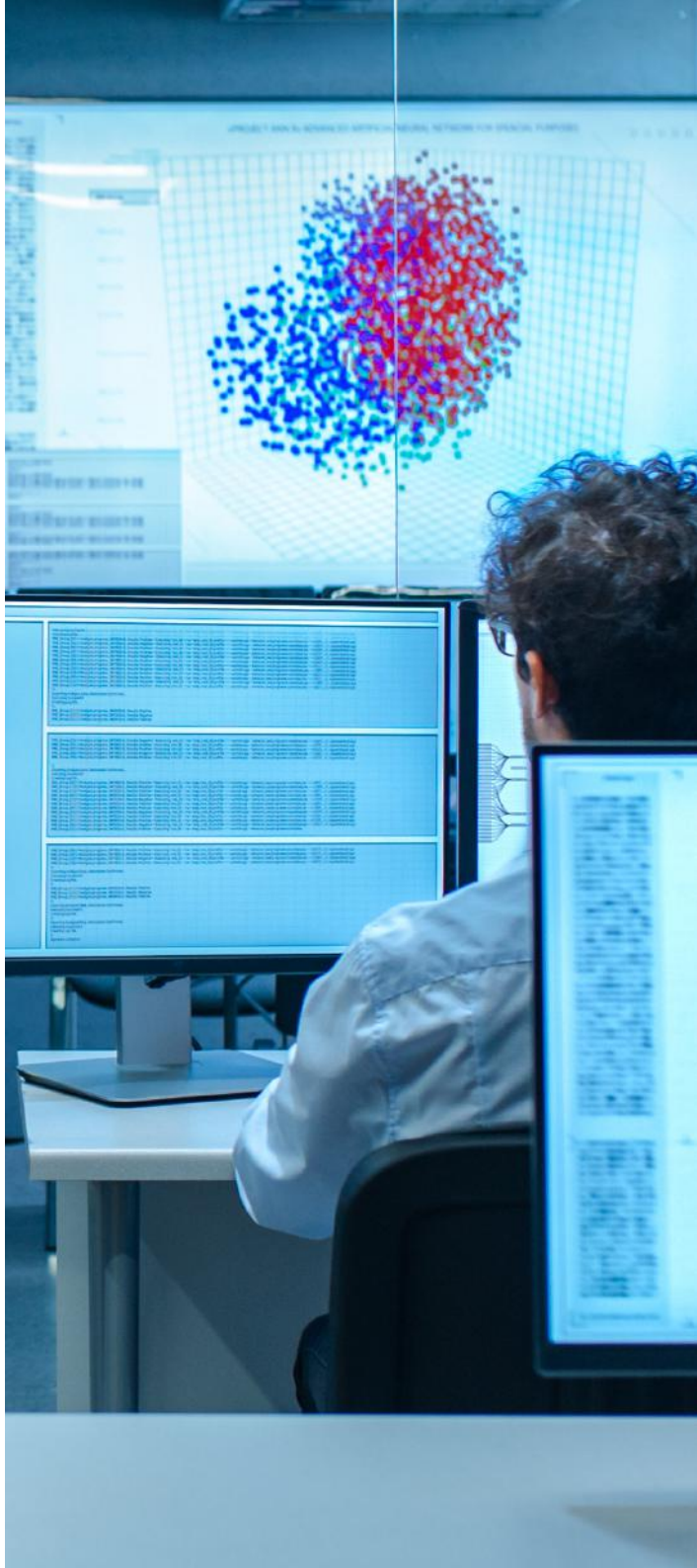


Abbildung 4. Laut der Umfrage zum Threat Hunting von Cybersecurity Insight, 2021, sind fehlendes Fachwissen, fehlende Technologien, Werkzeuge und Informationen, fehlende strukturierte Arbeitsabläufe und fehlende Transparenz/Daten die Haupthindernisse für die Implementierung eines Threat-Hunting-Programms.



3. Fehlende Transparenz

Was Sie nicht sehen können, können Sie auch nicht aufhalten. Beim Thema Endpointerkennung und -reaktion ist eine alle Endpoints umfassende Telemetrie entscheidend. Schlanke Endpoint-Agenten müssen robuste Telemetriedaten sammeln und hohe Transparenz gewährleisten, um eine schnellere und genauere Jagd sowie die Untersuchung und Reaktion auf Vorfälle während des Lebenszyklus des Bedrohungsschutzes zu unterstützen.

Die Telemetriedaten müssen automatisch normalisiert, in großem Umfang gespeichert und für eine sofortige und konsistente Analyse zugänglich sein. Ob für die Suche, Untersuchung oder Forensik, der langfristige Zugriff auf die Telemetrie ist unerlässlich.

Nach Angaben des Ponemon Institute dauert es im Jahr 2021 durchschnittlich 212 Tage, bis eine Sicherheitsverletzung erkannt wird, und weitere 75 Tage, um sie einzudämmen – insgesamt beträgt die Lebensdauer einer Sicherheitsverletzung also 287 Tage. Schwachstellenforscher und Sicherheitsanalysten müssen mindestens 300 Tage lang rückwirkende Untersuchungen durchführen, da sonst ihre Nachforschungen und Ermittlungen wirkungslos verpuffen könnten.

WatchGuard hält eine 365-tägige Speicherung für unerlässlich. Unsere Schwachstellenforscher nutzen die reichhaltigen Telemetriedaten in Echtzeit, so dass sie jederzeit für absolute Transparenz sorgen.

4. Mangel an Technologien, Werkzeugen und minutenaktuellen Bedrohungsanalysen

Eine effektive EDR-Lösung erfordert, dass die riesigen Mengen an Telemetriedaten, die von den Endpoints gesammelt werden, automatisch mit Kontext angereichert und korreliert werden, damit sie mit verschiedenen Analysetechniken auf Anzeichen von Angriffen untersucht werden können. Ein Schlüsselattribut ist die „File Reputation".

Such- und Visualisierungswerkzeuge, die eine schnelle und einfache Suche in der Telemetrie für beliebige Anwendungsfälle ermöglichen, sind für Spezialisten elementar. Sie ermöglichen es, Einrichtungen, Ereignisse und Parameter schnell und einfach auszuwerten, um Angriffsmuster zu identifizieren und Geschehen an Endpoints zu untersuchen. Bedrohungen werden so schneller erkannt.

Schließlich muss jedes erfolgreiche Threat-Hunting-Programm auf Informationen beruhen. Die überwiegende Mehrheit der Unternehmen, die heute eine interne Bedrohungsjagd durchführen, arbeiten auf einer niedrigen Stufe des Jäger-Reifegradmodells, da ihre Jagdaktivitäten häufig auf bekannten IoCs basieren. Im Gegensatz dazu ist echtes Threat Hunting eine proaktive Übung, nicht reaktiv. Es geht um die Suche nach unbekanntem Verhalten mit dem Ziel, Bedrohungen aufzudecken und zu unterbrechen, bevor Schaden entsteht. Für eine erfolgreiche, kontinuierliche Bedrohungsjagd müssen die Spezialisten qualitativ hochwertige, kontextbezogene Informationen in Echtzeit erhalten.

WatchGuard Unified Security Platform™ bereichert die Telemetrie mit unserem einzigartigen Zero-Trust Application Service und einer riesigen Menge an minutenaktuellen, qualitativ hochwertigen und kontextualisierten Bedrohungsanalysen.

5. Und schließlich, kostenintensiv und komplex

Heutzutage erkennen Unternehmen zunehmend die Notwendigkeit, nach sich ständig weiterentwickelnden Bedrohungen zu suchen. Diejenigen, die versucht haben, intern ein ausgereiftes Threat-Hunting-Programm einzurichten, haben jedoch schnell die Komplexität, die Kosten und den Aufwand erkannt, die mit dem Aufbau eines solchen Programms verbunden sind, und zwar aufgrund der erforderlichen Infrastruktur, Werkzeuge, Kenntnisse, Bedrohungsanalysen und Arbeitsabläufe. Darüber hinaus ist die konsequente Aufrechterhaltung der Praxis über einen langen Zeitraum ohne externe Unterstützung selbst für die erfahrensten Sicherheitsteams praktisch unmöglich.

Für ein Unternehmen, das versucht, dies intern zu tun, ist es äußerst schwierig, die Investitionsrentabilität auf täglicher Basis zu quantifizieren. Zudem ist es außerordentlich komplex, da die Jagdvorgänge in hohem Maße strukturiert sein müssen. Die Entwicklung von Arbeitsabläufen und Prozessen, die das Ergebnis garantieren, erfordert folglich eine interne hochkarätige Kompetenz in puncto Threat-Hunting.

5. Ein effizientes Sicherheitsprogramm mit WatchGuard Advanced Endpoint Security

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.

Wie bereits erwähnt, beträgt der durchschnittliche Lebenszyklus einer Sicherheitsverletzung 287 Tage. Es dauert mindestens 300 Tage, um eine erfolgreiche nachträgliche Untersuchung durchzuführen.

Keine Daten, keine Jagd! Punkt!

WatchGuard hält eine 365-tägige Speicherung für unerlässlich. Unsere Schwachstellenforscher nutzen die reichhaltigen Telemetriedaten in Echtzeit, so dass sie jederzeit für absolute Transparenz sorgen.

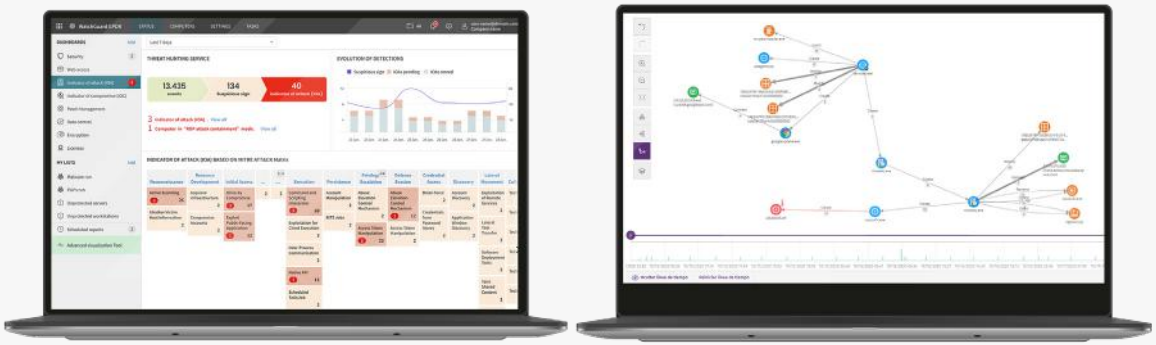
Die Threat Hunting Services von WatchGuard, unterstützt durch die 365-Tage-Telemetrie, die verhaltensorientierte KI-Engine, Threat Radar und unsere Threat Intelligence – Open-Source-Intelligence (OSINT) wie MITRE ATT&CK, Cyber Threat Alliance und proprietäre Intelligenz – identifiziert abnormale Verhaltensweisen und kategorisiert sie als Hinweise auf Angriffe (IoAs).

Die Spezialisten von WatchGuard durchforsten diese Hinweise auf der Suche nach weniger verdächtigen und solchen mit starkem Verdachtspotential, die dann auf der Administratorkonsole als IoAs (Indicators of Attack) angezeigt werden.

Die IoAs liefern wertvolle Informationen zur Entschärfung des Angriffs. Danach können Maßnahmen ergriffen werden, um beim nächsten Mal kein Ziel für Bedrohungen mehr zu sein, z. B. Anpassung der Systemkonfigurationen, Patchen von Endpoints oder Entzug von Anwender-Zugangsrechten. RDP Brute-Force-Angriffe, Privilegienerweiterung, dateilose Angriffe und laterale Bewegungen sind Beispiele für IoAs, die vom Threat Hunting Service erkannt werden, der ohne zusätzliche Kosten in unseren WatchGuard Advanced Endpoint Security-Lösungen enthalten ist.

MITRE ATT&CK™ Framework

Wir bei WatchGuard implementieren das MITRE ATT&CK™ Framework (eine global zugreifbare Wissensdatenbank mit Angriffstaktiken und -techniken basierend auf realen Beobachtungen) über die verschiedenen WatchGuard Security-Prozesse und Produktfunktionen, um die Produktivität von Analysten zu verbessern und Sicherheitsverletzungen zu verhindern.



Mit der Einführung dieses systematischen Jagdprozesses haben wir die folgenden spezifischen Services in unser Advanced Endpoint Security-Portfolio aufgenommen:

Der **Threat Hunting Service** macht die Jagd nach MITRE ATT&CK TTP schnell und mühelos. Der Service, der standardmäßig in allen WatchGuard Advanced Endpoint Security-Lösungen enthalten ist, verwandelt schwache Signale in solide Indikatoren für dateilose Malware-Angriffe in den Netzwerken (IoAs). Die kontextualisierten IoAs werden in der Konsole mit interaktiven Diagrammen über den Verlauf der Aktion angezeigt.

Der Essential Threat Hunting Service wird kostenlos für alle Advanced Endpoint Security-Lösungen von WatchGuard angeboten.

Der Premium Threat Hunting Service[2] bietet eine zusätzliche Ebene der Proaktivität. Alle schwachen Anzeichen von abnormalem Verhalten werden von unserem Cybersicherheitsteam geprüft, untersucht und mit Informationen und Analysen korreliert, um mögliche Angriffe explizit auszuschließen. Darüber hinaus arbeiten unsere Threat Hunter aktiv mit den Telemetriedaten unserer Premium Threat Hunting-Kunden und suchen nach neuen Angriffsmustern, die aus den aktuellen Bedrohungsdaten und Angriffshypothesen stammen.

Diese neuen Muster bieten eine wertvolle Gelegenheit zur Verbesserung und Verstärkung automatischer Erkennungstechniken an den Endpoints.

Sobald eine Hunting-Hypothese erfolgreich in ein neues Muster für die Erkennung von dateiloser Malware umgewandelt wurde, werden neue Sensoren nahtlos auf den Endpoints unserer Kunden eingesetzt, die neue Daten in den Data Lake einspeisen, um Bedrohungen in großem Umfang zu erkennen und zu blockieren. Diese Kombination aus Prozessen, Technologie und Fachwissen ermöglicht es unseren Kunden, ihre Sicherheitsreife zu erhöhen und ihre Sicherheitslage deutlich zu verbessern.

In den letzten Jahren haben die Threat Hunter von WatchGuard zahlreiche neue verhaltens- und kontextbasierte Erkennungen und IoAs-Muster entwickelt, die in die Lösungen von WatchGuard Advanced Endpoint Security für SOCs als Ergebnis unserer kontinuierlichen Hunting-Aktivitäten integriert wurden.

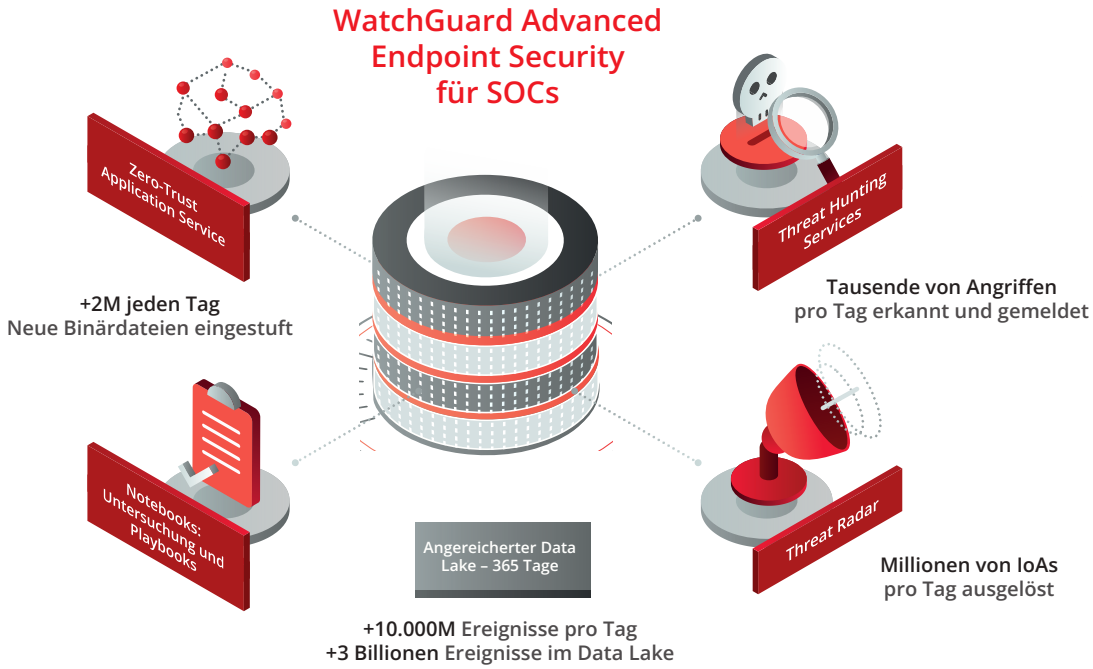


Abbildung 5. Die cloudnative Plattform bietet Echtzeitüberwachung über 365 Tage der Endpoint-Aktivität, verweigert die Ausführung von Malware, Ransomware oder anderen bösartigen Anwendungen und identifiziert abnormales Verhalten in Echtzeit. Die Threat Hunting Services erkennen und benachrichtigen proaktiv über Angriffe, die auf dateiloser Malware basieren und die in das Netzwerk eindringen und die Endpoints erreichen konnten.

Die Schleifen der WatchGuard Threat Hunting-Vorgänge

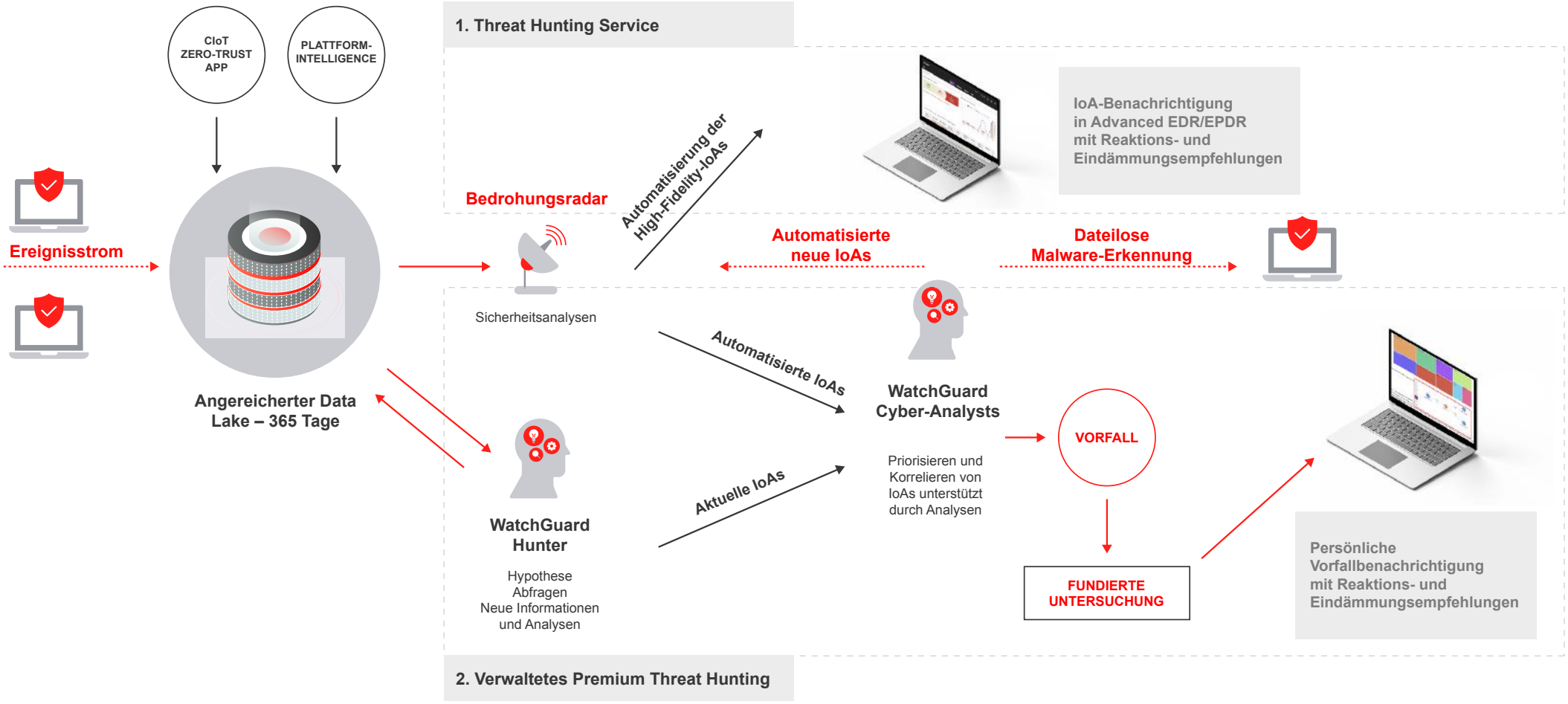


Abbildung 6. Jede erfolgreiche Hunting-Aktivität sollte mit der Einleitung einer Sicherheitsmaßnahme enden. Unser Hunter-Team kommuniziert mit dem Sicherheitsteam unserer Partner entweder über die Konsole oder durch direkte Kommunikation.

6. Der Threat Hunting Service als Erweiterung Ihres Teams

Ein kooperativer und koordinierter Ansatz ist der Schlüssel, um die Sicherheitsverletzungen von heute zu stoppen und Ihren Kunden nahtlos ein Höchstmaß an verwalteter Sicherheit zu bieten.

Sie oder Ihre Partner können ihre Dienste schnell erweitern, indem sie die Ergebnisse der Threat Hunting Services durch die Validierung der IoAs nutzen und auf den Angriff reagieren.

WatchGuard Advanced EDR und WatchGuard Advanced EPDR können Sie sofort benachrichtigen, wenn ein neuer IoA auftaucht. Jeder IoA wird mit einer Liste empfohlener Maßnahmen zur Blockierung, Behebung und Vermeidung künftiger Angriffe mit denselben TTP als Ausgangspunkt für Sie oder Ihren Partner geliefert.

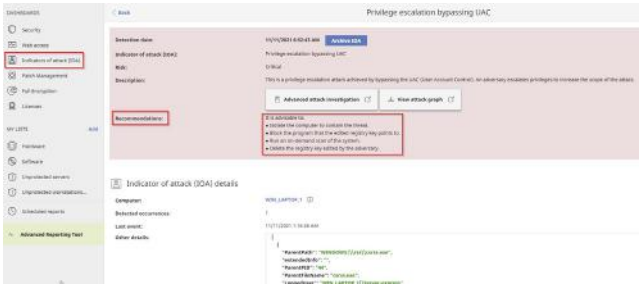


Abbildung 7. Der Threat Hunting Service zeigt alle Details zur Eindämmung von und Reaktion auf Bedrohungen, wenn IoAs entdeckt werden.

Der **Premium*** Threat Hunting Service bietet die innovativen Funktionen, um – von Algorithmen oder Menschen geleitet – Daten zu filtern, potenzielle gezielte Angriffe zu untersuchen und Sie oder unsere Partner über relevante Ereignisse auf den Endpoints ihrer Kunden zu informieren.

Unser Cybersicherheitsteam leitet einen Untersuchungsprozess für jede verdächtige Aktivität ein, die im Zusammenhang mit einem tatsächlichen Vorfall steht. Der Untersuchungsprozess nutzt ML-Algorithmen, die über einen Zeitraum von 365 Tagen gesammelten Telemetriedaten sowie Cyber Intelligence, um andere TTPs zu identifizieren, die Angriffsstufe zu bestimmen und die betroffenen Anlagen zu identifizieren.

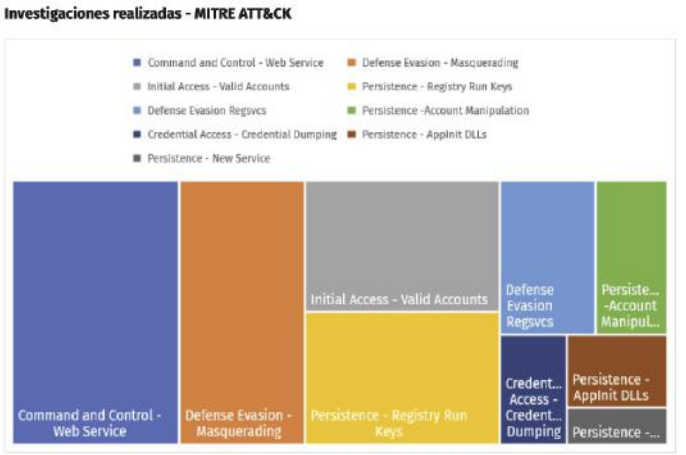
Das Ergebnis der Untersuchung ist eine klar definierte Vorgehensweise, die Ihnen oder Ihrem Partner per E-Mail oder Telefonanruf mitgeteilt wird. Dazu gehören auch alle Details und Empfehlungen, um die Bedrohung schnell zu stoppen, zu entschärfen und darauf zu reagieren. Sie oder Ihre Partner können dann den Vorfall mit den Kunden regeln.

Darüber hinaus erhalten unsere Partner oder Kunden einen individuellen monatlichen Bericht über die bei jedem Kunden durchgeführten Threat Hunting-Aktivitäten und Untersuchungen. Anhand dieses monatlichen Berichts können Partner den Wert des Dienstes automatisch nachweisen.

Das Gesamtergebnis der WatchGuard Hunter und Ihrem Partner oder Ihrem Team ist ein effizienter, proaktiver Erkennungs- und Reaktionsdienst für hochentwickelte, dauerhafte Bedrohungen.

Der zweite große Vorteil dieses Modells besteht darin, dass Sie oder Ihr Partner Kenntnisse über die Prozesse des Threat Hunting und über die Techniken der Bedrohungen erhalten.

**Dieses Produkt kann nicht ohne vorherige Genehmigung erworben werden. Wenden Sie sich an Ihren WatchGuard-Vertriebsmitarbeiter, um weitere Informationen zu erhalten.*



Táctica - Técnica MITRE ATT&CK	Ocurrencia
Command and Control - Web Service	12
Defense Evasion - Masquerading	9
Initial Access - Valid Accounts	7
Persistence - Registry Run Keys	7
Defense Evasion Regsvcs	4
Persistence -Account Manipulation	3
Credential Access - Credential Dumping	2
Persistence - AppInit DLLs	2

Abbildung 8. Der Premium Threat Hunting Service führt eine Triage und Untersuchung aller verdächtiger Aktivitäten durch, die durch Analysen, Hypothesen und Cyber Intelligence entdeckt werden. Der monatliche Bericht ist ein wertvolles Instrument zur Zusammenfassung der durchgeführten Threat Hunting-Aktivitäten.

7. Fazit

Lassen Sie uns einige wichtige Erkenntnisse für die Partner zusammenfassen, die derzeit einen Threat Hunting Service durchführen oder die Einrichtung eines solchen Dienstes in Erwägung ziehen:

1. **Bedrohungen bewegen sich schneller als je zuvor.** Denken Sie an die Geschwindigkeit, mit der Bedrohungen agieren und sich weiterentwickeln.

2. **Keine Organisation ist immun, unabhängig von Größe, Branche oder Standort.** Jede Organisation ist ein Ziel, unabhängig von ihrem Standort und der Branche, in der sie tätig ist.

3. **Threat Hunting ist heute ein Muss für jedes Unternehmen.** In Anbetracht der Geschwindigkeit, mit der sich Bedrohungen entwickeln, ist Threat Hunting kein optionales Extra mehr, sondern gehört in jedes Unternehmen.

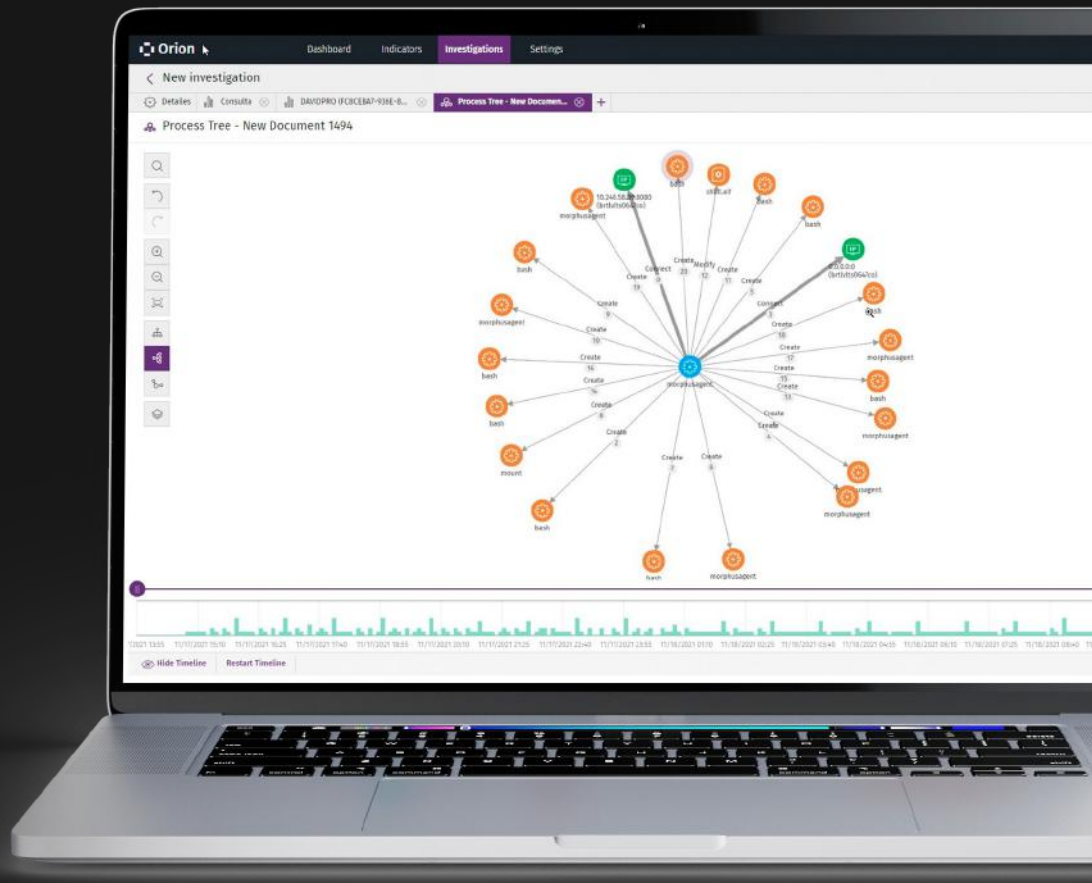
4. **Geschwindigkeit, Umfang und Beständigkeit sind entscheidend.** Threat Hunting muss schnell und in großem Umfang durchgeführt werden können. Dies erfordert strukturierte, wiederholbare Prozesse, ausgereifte Technologien, langfristige Transparenz und Bedrohungsjäger, die über fundiertes Fachwissen, Kenntnisse und Bedrohungsdaten verfügen.

5. **Strukturieren Sie Ihre Jagden mithilfe des MITRE ATT&CK-Frameworks.** Die Advanced Endpoint-Lösungen von Cytomic sind mit vielen identifizierten ATT&CK-Techniken ausgestattet und ermöglichen es dem Sicherheitsteam, sich auf die Bekämpfung von Sicherheitsbedrohungen zu konzentrieren. Dazu nutzen sie klar definierte Informationen, die das Framework bereitstellt und von unserem Cybersecurity-Team erweitert werden.

6. **Wenn Sie dies nicht intern erledigen können, sollten Sie mit einem Anbieter zusammenarbeiten, der dies kann.**

WatchGuard

Sie möchten mehr über WatchGuard Endpoint für SOCs wissen



1. Cybersecurity Insiders hat das vierte jährliche Threat Hunting-Forschungsprojekt durchgeführt, um tiefere Einblicke in den Reifegrad und die Entwicklung der Sicherheitspraxis zu gewinnen. Dieser Threat Hunting-Bericht basiert auf den Ergebnissen einer umfassenden Online-Umfrage unter Cybersecurity-Experten, die im Februar 2021 durchgeführt wurde, um tiefe Einblicke in die neuesten Trends, die wichtigsten Herausforderungen und Lösungen für das Threat Hunting-Management zu gewinnen. Die Befragten reichen von technischen Führungskräften bis hin zu Managern und IT-Sicherheitspraktikern und repräsentieren einen ausgewogenen Querschnitt von Unternehmen unterschiedlicher Größe und verschiedener Branchen.

2. Der Premium Threat Hunting Service steht Partnern und Kunden von WatchGuard zur Verfügung

DAS WATCHGUARD-PORTFOLIO

Network Security

Netzwerksicherheitslösungen von WatchGuard sind von Grund auf so konzipiert, dass sie einfach zu implementieren, verwenden und verwalten sind – und darüber hinaus ein Höchstmaß an Sicherheit bieten. Unsere einzigartige Herangehensweise an die Netzwerksicherheit bedeutet, jedem Unternehmen, unabhängig von seiner Größe oder seinem technischen Fachwissen, die bestmögliche Sicherheit auf Enterprise-Niveau zur Verfügung zu stellen.

Multifaktor-Authentifizierung

Mit WatchGuard AuthPoint® können Sie die passwortbasierende Sicherheitslücke mithilfe von Multifaktor-Authentifizierung auf einer benutzerfreundlichen Cloud-Plattform ganz einfach schließen. Beim einzigartigen Ansatz von WatchGuard wird die „DNA des Smartphones" als Identifizierungsfaktor genutzt. Auf diese Weise erhält nur die richtige Person Zugriff auf vertrauliche Netzwerke und Cloudanwendungen.

Sicheres, cloudverwaltetes WLAN

Die Secure Wi-Fi Solution von WatchGuard ist eine richtungsweisende Neuerung für den Markt von heute: Sie schafft eine sichere, geschützte WLAN-Umgebung, eliminiert den Verwaltungsaufwand und ermöglicht beträchtliche Kostensenkungen. Die Kombination aus leistungsstarken Verwaltungs- und Analysemöglichkeiten und einer tiefgehenden Visualisierung sichert Unternehmen die entscheidenden Wettbewerbsvorteile für den geschäftlichen Erfolg.

Endpoint-Sicherheit

WatchGuard Endpoint-Sicherheit ist ein cloudnatives, fortschrittliches Endpoint-Sicherheitsportfolio, das Unternehmen jeder Art vor gegenwärtigen und zukünftigen Cyberangriffen schützt. Seine auf künstlicher Intelligenz basierende Flagship-Lösung WatchGuard EDPR verbessert unmittelbar die Sicherheitslage von Unternehmen. Sie kombiniert die Funktionen Endpoint-Schutz (EPP) und Detection and Response (EDR) mit Zero Trust Application und Threat Hunting Services.

Informationen zu 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.

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

Teilenr. WGCE67539_042022