WatchGuard-Bericht für Unternehmen

Hochmodernes Threat Hunting

Einblicke unterstützt durch PULSE

EINFÜHRUNG

Bedrohungen können nicht vermieden werden. 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, die legitimen Anwendungen an den Endpoints zu instrumentalisieren und einen LotL-Angriff (Living off the Land) zu starten.

Dieser Trend stellt die Sicherheitsprogramme von Unternehmen vor immense Herausforderungen. Er macht deutlich, wie wichtig eine Kombination aus technologiebasierter Kontrolle und von Menschen geleitetem, proaktivem Threat Hunting ist, um sicherzustellen, dass Unternehmen schneller reagieren, als Bedrohungen auftreten, Angreifer früh stoppen können und gut geschützt und widerstandsfähig bleiben.

Die Threat-Hunting-Funktion

Threat Hunting ist eine häufig falsch verstandene Nischenfunktion. 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, indem es untypische Verhaltensweisen erkennt.

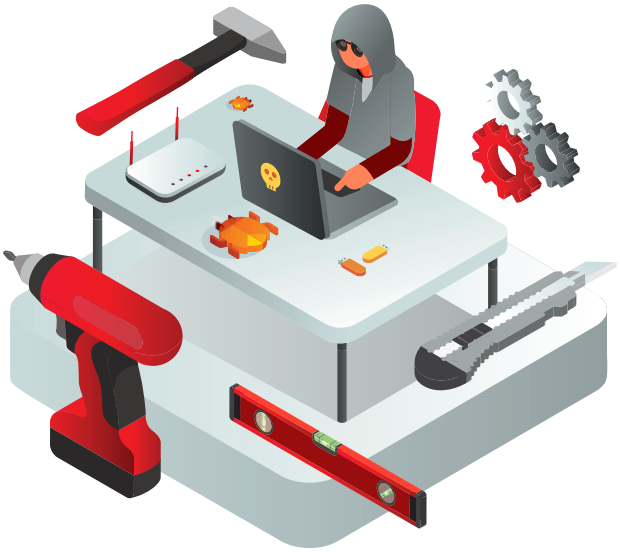
Threat Hunting ist eine Disziplin, die Unternehmen nicht mehr als ein optionales Extra, sondern als unverzichtbar betrachten sollten. Es sollte sich um eine kontinuierliche Funktion handeln, wie sie für jedes robuste Cybersicherheitsprogramm unerlässlich ist, und nicht um eine punktuell aktivierte Funktion.

Die Umsetzung eines Abwehrkonzepts ist mit vielen Herausforderungen verbunden. Wie gehen IT-Führungskräfte mit diesem Problem um?

Herausragende Einblicke:

- Auch wenn Threat Hunting noch eine junge Disziplin ist, besteht ein großes Interesse daran. Nahezu alle Befragten stimmen überein, dass eine konstante Überwachung (96 %) und Threat Hunting (87 %) zu den wichtigsten Initiativen in Bezug auf Sicherheit zählen sollten.
- Dennoch bezeichnen nur 3 % der Befragten das Level ihres Threat Huntings als ausgereift. Mehr als die Hälfte der IT-Führungskräfte setzt noch kein Threat Hunting ein.
- Allerdings planen 53 % der Befragten, Threat Hunting innerhalb der nächsten 12 Monate als Sicherheitsinitiative einzuführen.

Wir danken **PULSE** für die Unterstützung bei dieser einzigartigen Forschungsarbeit. Viel Spaß mit dem Bericht.



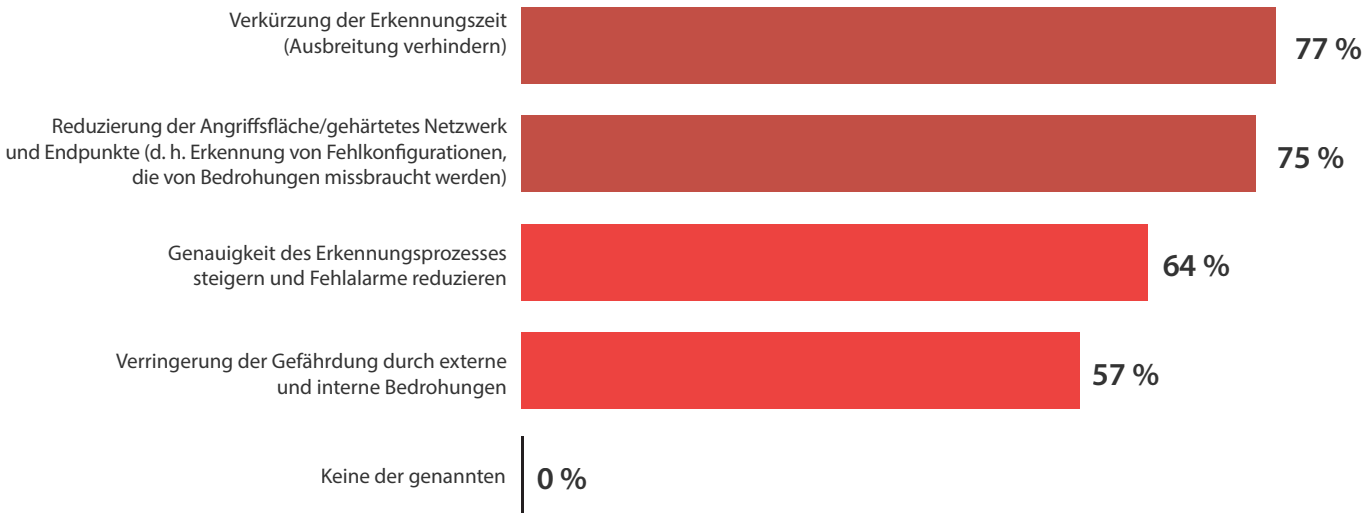
Datenerhebung: 11. November bis 8. Dezember 2021 Befragte: 100 Entscheidungsträger im Bereich IT,

VORTEILE DES THREAT HUNTINGS

Threat Hunting reduziert die Zeit für die Erkennung von Bedrohungen und ist als effektive Sicherheitslösung auf dem Vormarsch.

Alle Befragten sehen Vorteile in der Bedrohungserkennung und der Bedrohungsjagd. Die Mehrheit sieht die größten Vorteile der Bedrohungserkennung in der reduzierten Erkennungszeit (77 %) und der geringeren Angriffsfläche (75 %).

Welche der Nachfolgenden sind die größten Vorteile der Bedrohungserkennung und Bedrohungsjagd?



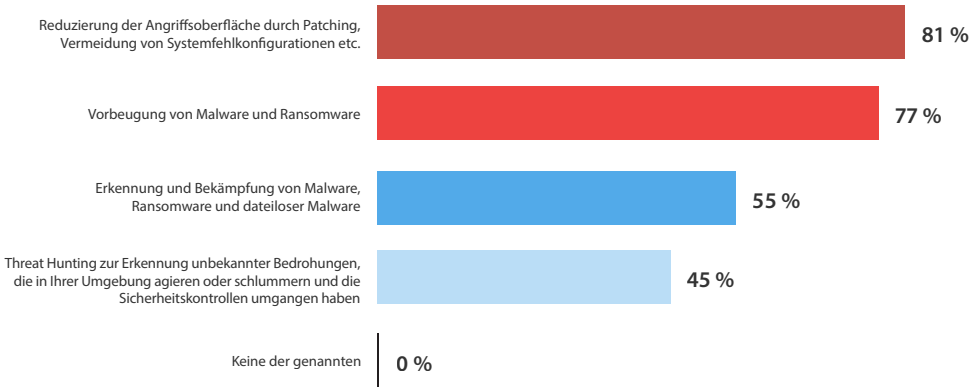
> **„Durch die Erkennung wird eine Bedrohung entdeckt, während sie auftritt, und möglicherweise gestört. Die Jagd hingegen beinhaltet die Suche nach schlummernden Bedrohungen oder durch Malware geöffnete Hintertüren."**
>
> Finanzen, Bankwesen und Versicherungen, ab 10.001 Mitarbeitern. EMEA

WatchGuard

PRIORITÄT DES THREAT HUNTINGS

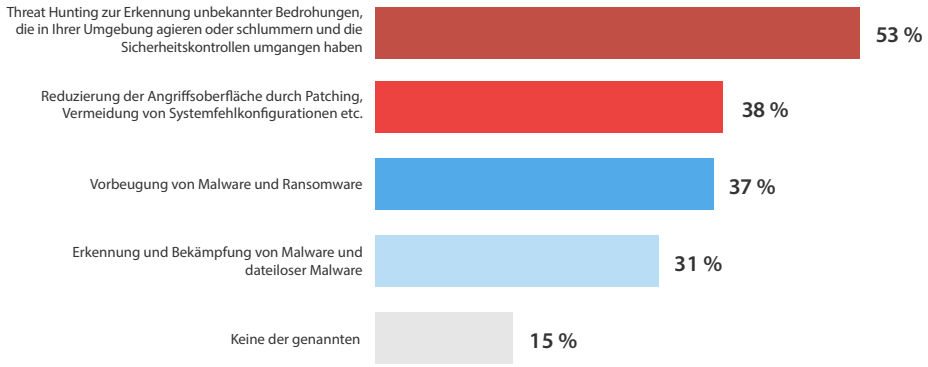
Lediglich 45 % der Befragten haben bereits Threat-Hunting-Prozesse zur Erkennung unbekannter Bedrohungen, die die Sicherheitskontrollen umgangen haben und in Ihrer Umgebung agieren oder schlummern, implementiert.

Welche der folgenden Sicherheitsmaßnahmen hat Ihr Unternehmen bereits implementiert, um Sicherheitsverletzungen zu verhindern?



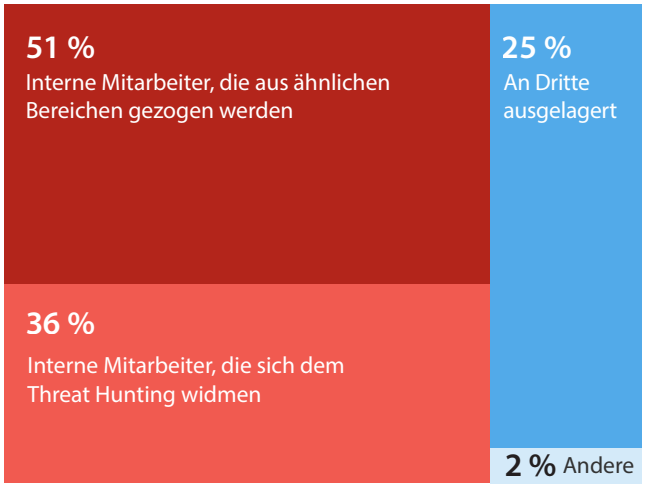
Jedoch planen 53 % der Befragten, Threat Hunting innerhalb der nächsten 12 Monate als Sicherheitsinitiative einzuführen.

Welche der folgenden Sicherheitsmaßnahmen plant Ihr Unternehmen innerhalb der nächsten 12 Monate einzuführen?



Die meisten Befragten (51 %) ziehen für ihre Threat-Hunting-Aktivitäten Personal aus anderen verwandten Bereichen in ihrem Unternehmen ab.

Wie stellen Sie derzeit das Personal für Ihre Threat Hunting-Aktivitäten bereit?



WatchGuard

THREAT HUNTING vs. BEDROHUNGSERKENNUNG

Threat Hunting ist ein proaktiver Ansatz, der im Gegensatz zu einem reaktiven Ansatz steht.

Auch wenn die Definitionen von Threat Hunting und Bedrohungserkennung variieren, stimmen 39 % der Befragten zu, dass die Jagd ein proaktiver Ansatz ist, während die Erkennung reaktiv ist.

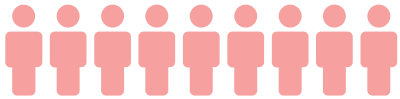
Was ist der Unterschied zwischen Bedrohungserkennung und Bedrohungsjagd, falls es einen gibt?

39 %

sind der Meinung, dass die Erkennung reaktiv und die Jagd proaktiv ist

20 %

Ich weiß nicht



13 %

sehen keinen Unterschied zwischen der Erkennung und der Jagd

12 %

nehmen an, dass Bedrohungen im Rahmen einer Erkennung automatisch über KI/ML entdeckt werden und bei der Jagd menschlicher Einsatz erforderlich ist

10 %

verbinden die Erkennung mit einer akuten Gefährdung und sehen die Jagd als eine Möglichkeit der Erkennung, bevor eine akute Gefährdung entsteht

6 %

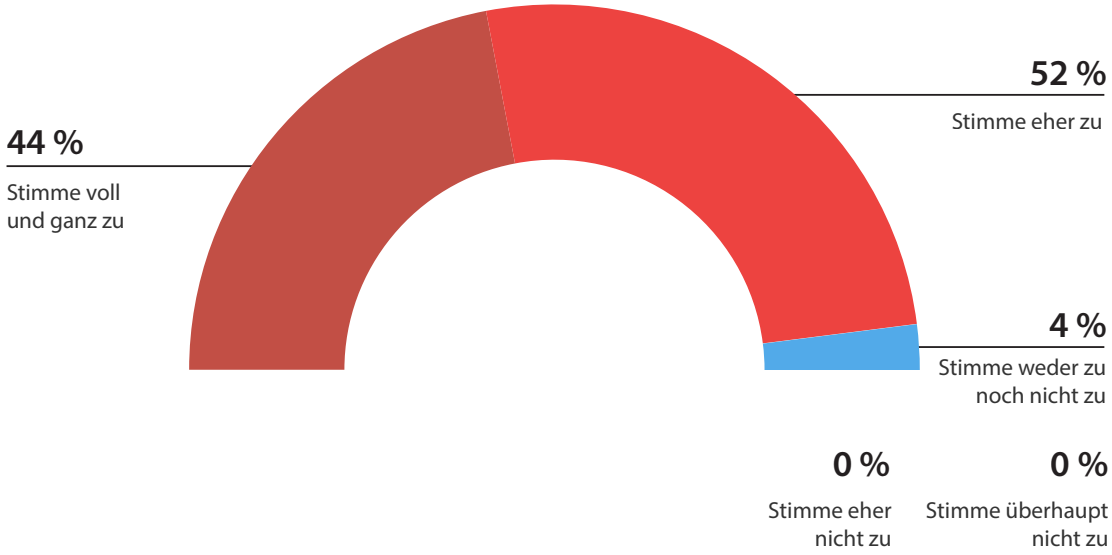
verbinden die Erkennung mit bekannten Bedrohungen und die Jagd mit unbekannten Bedrohungen

WatchGuard

Sowohl die kontinuierliche Bedrohungserkennung UND Threat Hunting zählen zu den wichtigsten Sicherheitsinitiativen.

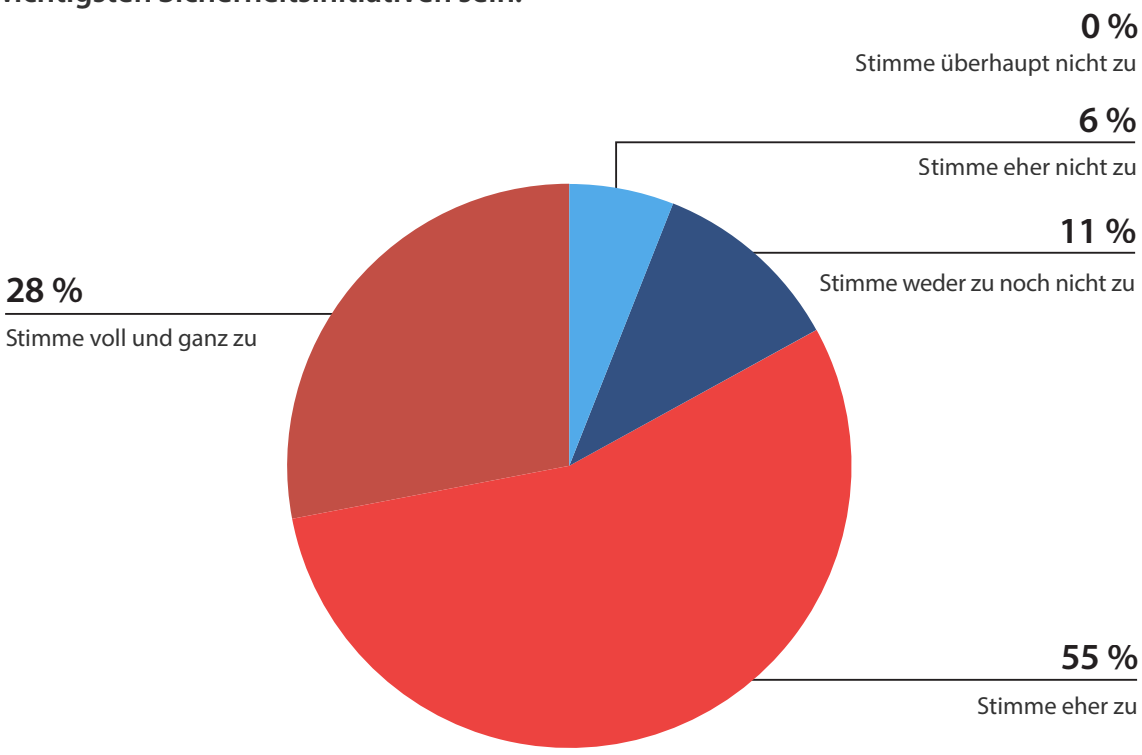
96 % der Befragten stimmen zu, dass eine fortlaufende Überwachung und eine verhaltensbasierte Erkennung zu den wichtigsten Sicherheitsinitiativen zählen sollten.

Inwieweit stimmen Sie der folgenden Aussage zu oder widersprechen ihr: Fortlaufende Überwachung und verhaltensbasierte Erkennung sollten zu den wichtigsten Sicherheitsinitiativen zählen.



83 % der Befragten stimmen zu, dass Threat Hunting eine der wichtigsten Sicherheitsinitiativen sein sollte.

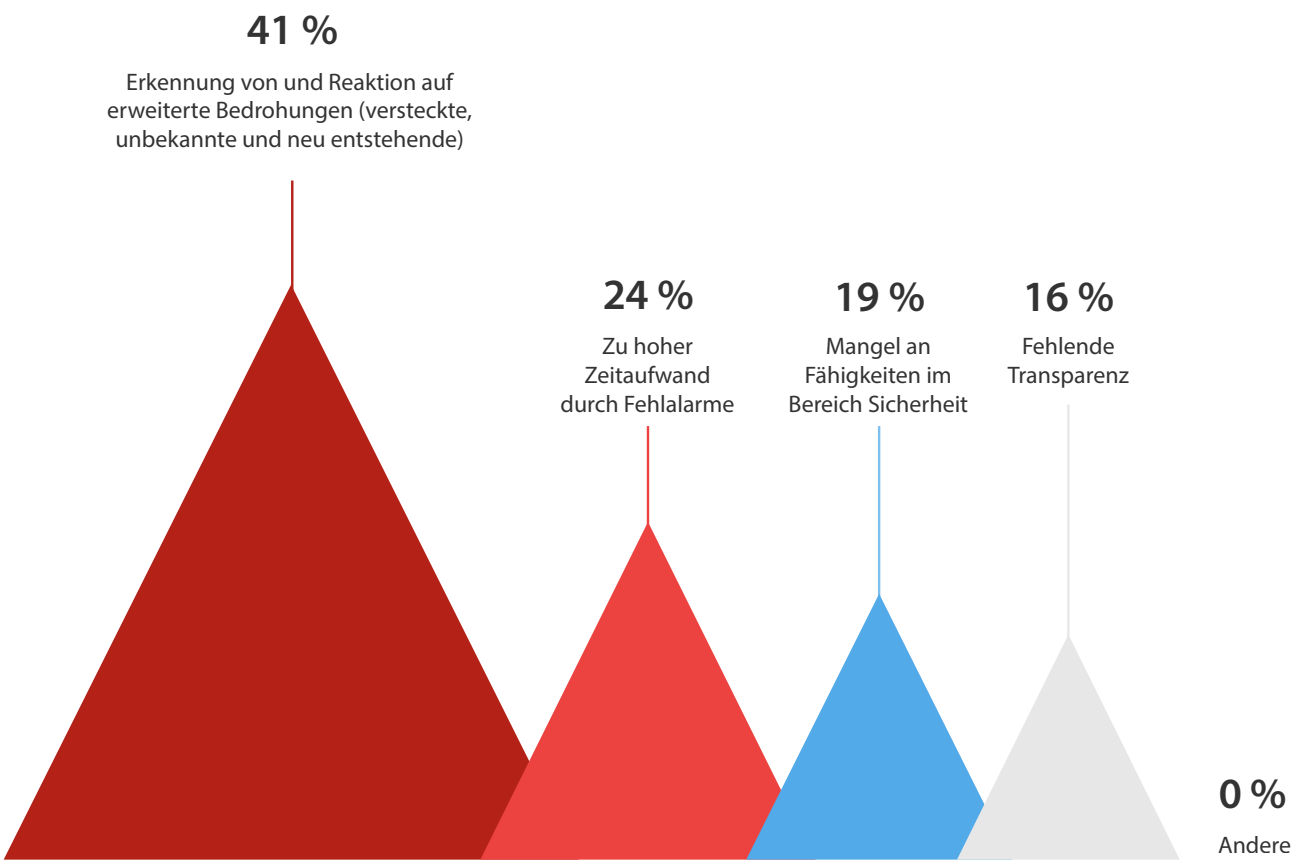
Inwieweit stimmen Sie der folgenden Aussage zu oder widersprechen ihr: Threat Hunting sollte eine der wichtigsten Sicherheitsinitiativen sein.



DIE GRÖSSTEN SICHERHEITSHERAUSFORDERUNGEN

Laut den Umfrageergebnissen nennen Experten auf dem Gebiet der Cybersicherheit die rechtzeitige Erkennung erweiterter Bedrohungen (41 %), einen zu hohen Zeitaufwand für falsche Alarme – **eine sogenannte Alarmmüdigkeit** – (24 %), einen Mangel an fachkundigem Sicherheitspersonal für die Erkennung und Minimierung von Bedrohungen (19 %) und eine fehlende Transparenz (16 %) als die größten Herausforderungen ihrer Sicherheitsteams.

Welche der folgenden Optionen ist Ihrer Meinung nach die größte Herausforderung für Ihr Sicherheits- oder IT-Team?

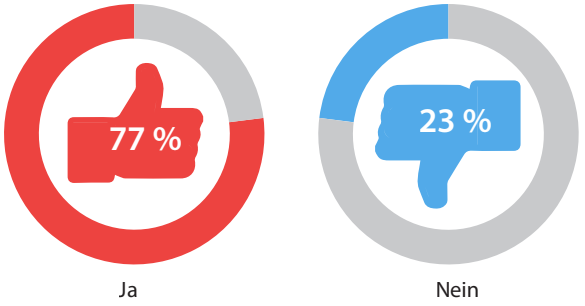


> **„Die Bedrohungserkennung ist ein Prozess, der in den meisten Fällen automatisiert ist und darauf abzielt, bekannte Bedrohungen zu erkennen. Im Gegensatz dazu ist die Bedrohungsjagd ein kreativer Prozess mit flexiblen Methoden, der sich auf die Jagd nach versteckten oder nicht erkannten Hackerangriffen konzentriert."**
>
> Director Einzelhandelsunternehmen mit 1.001–5.000 Mitarbeitern. Nordamerika

GRENZEN FÜR EIN BESSERES THREAT HUNTING

Erfolgreiche Threat-Hunting-Programme können sicherstellen, dass Sicherheits- und IT-Teams in der Lage sind, Bedrohungen zu erkennen und auf diese zu reagieren. Um den Erfolg zu garantieren, muss Threat Hunting jedoch schnell und in großem Umfang durchgeführt werden. Dies erfordert strukturierte, wiederholbare Prozesse, ausgereifte Technologien, langfristige Transparenz und Threat Hunter, die über fundiertes Fachwissen, Kenntnisse und Bedrohungsdaten verfügen.

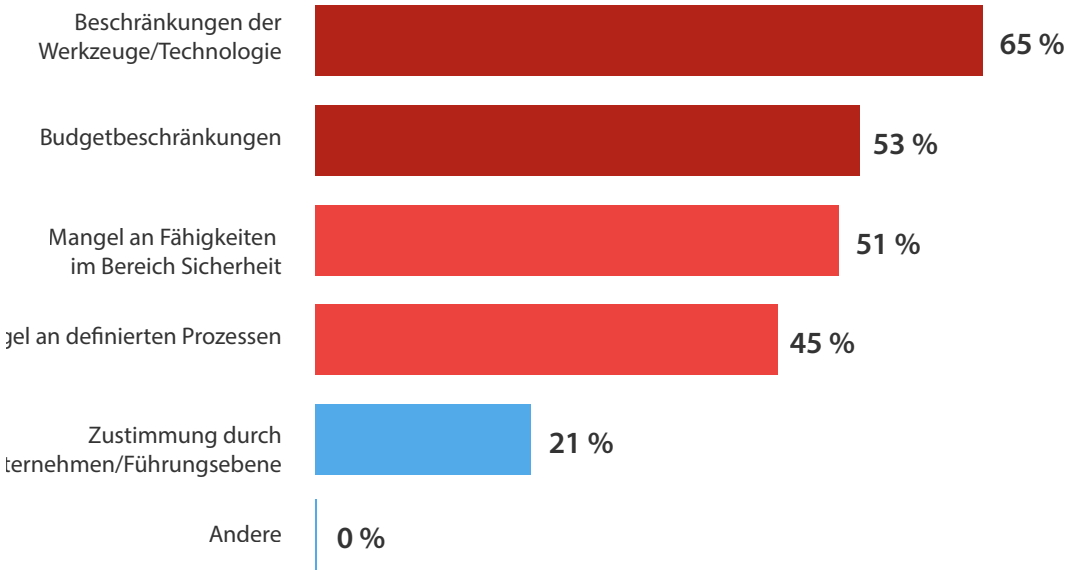
Unterscheiden sich die für das Threat Hunting erforderlichen Technologien, Prozesse und Fähigkeiten von den für die Bedrohungserkennung erforderlichen?



77 % der Befragten sagen, die für das Threat Hunting erforderlichen Technologien, Prozesse und Fähigkeiten unterscheiden sich von den für die Bedrohungserkennung erforderlichen.

In Bezug auf das Threat Hunting verfügen Sicherheitsteams oft nicht über die erforderlichen Tools und Technologien sowie Fähigkeiten und Prozesse und sind durch ein mangelndes Budget eingeschränkt. Die meisten Befragten (65 %) gaben an, dass die Grenzen ihrer Tools und Technologien eine Hürde für die erfolgreiche Implementierung von Threat Hunting darstellen. Für mehr als die Hälfte (51 %) stellen oder stellten Budgetbeschränkungen und mangelnde Fähigkeiten im Bereich Sicherheit eine Barriere dar.

Was sind die Haupthindernisse für den Erfolg Ihrer derzeitigen/künftigen Bemühungen zur Einführung von Threat Hunting?

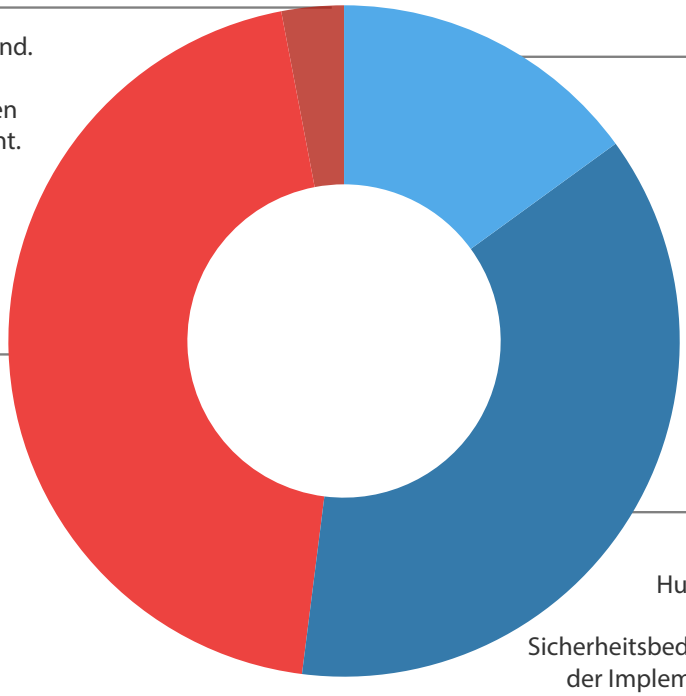


WatchGuard

REIFEGRAD DES THREAT HUNTINGS

Unternehmen werden fortlaufend mit sich schnell entwickelnden Bedrohungen konfrontiert, vor denen Sie Ihre Umgebungen schützen müssen. In Bezug auf den Reifegrad geben lediglich 3 % der Befragten an, dass ihr Thread Hunting auf dem neuesten Stand ist. Mehr als die Hälfte (52 %) geben an, dass sie entweder kein aktives Thread Hunting betreiben oder in Bezug auf Bedrohungen hauptsächlich reaktiv handeln.

Wie bewerten Sie den Reifegrad Ihres Threat Huntings?



3 %

Wir sind auf dem neuesten Stand. Wir identifizieren und stoppen Bedrohungen in ihren frühesten Phasen. Nichts bleibt unerkannt.

15 %

Wir führen kein aktives Threat Hunting durch. Unsere Strategie beruht fast ausschließlich auf herkömmlichen, reaktiven Sicherheitstechnologien.

45 %

Unser Ansatz ist ziemlich ausgereift. Wir erkennen nicht jede Bedrohung, aber unser Sicherheitskonzept ist größtenteils proaktiv statt reaktiv.

37 %

Wir stehen in Bezug auf Threat Hunting noch ganz am Anfang. Wir reagieren überwiegend auf Sicherheitsbedrohungen, beginnen jedoch mit der Implementierung der grundlegendsten Threat-Hunting-Funktionen.

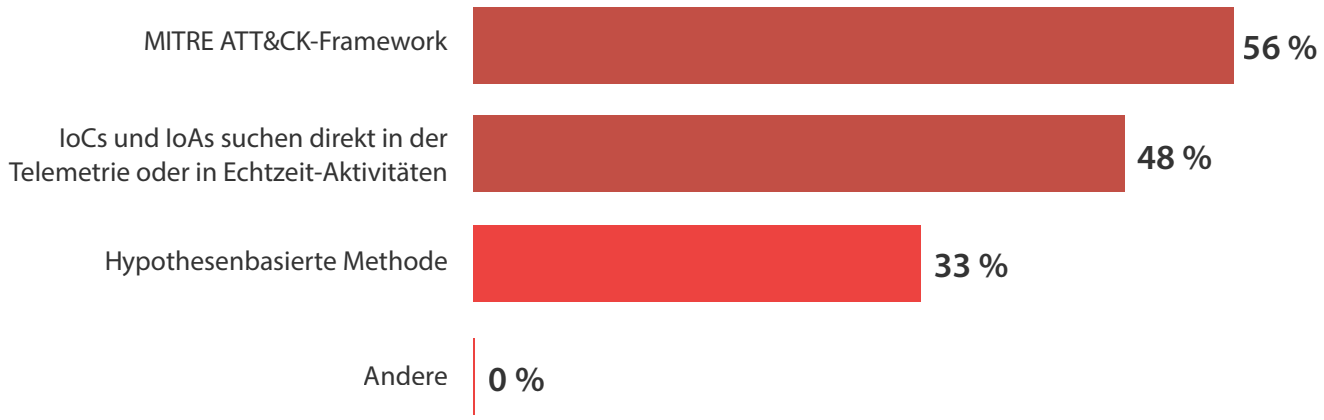
Ziehen Sie bei der Beurteilung des Hunting-Fähigkeit Ihres Unternehmens diese drei Faktoren in Betracht:

- Qualität der für das Hunting erhobenen Daten
- Werkzeuge für das Bewerten und Analysieren von Daten
- Fähigkeiten der Analysten, die diese Daten und Tools verwenden, um Sicherheitsvorfälle zu erkennen

METHODEN VON THREAT HUNTERN

Nur 33 % der Befragten setzen einen hypothesenbasierten Ansatz für das Threat Hunting ein. Die meisten Befragten verlassen sich weiterhin auf das MITRE ATT&CK-Framework (56 %) und/oder dir direkte Suche durch IoCs und IoAs (48 %).

Welche Methoden verwenden Sie für das Hunting? (n=85)



FAZIT

Unternehmen, die derzeit überlegen, eine interne Threat-Hunting-Funktion einzuführen, sollten sich über Folgendes im Klaren sein:

- **Bedrohungen bewegen sich schneller als je zuvor.** Denken Sie an die Geschwindigkeit, mit der Bedrohungen agieren und sich weiterentwickeln.
- **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.
- **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.
- **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.
- **Strukturieren Sie Ihre Jagden mithilfe des MITRE ATT&CK-Frameworks.** Fortschrittliche Endpoint-Sicherheitslösungen von WatchGuard sind mit vielen identifizierten ATT&CK-Techniken ausgestattet.
- **Wenn Sie dies nicht intern erledigen können, sollten Sie mit einem Dienstanbieter zusammenarbeiten, der dies kann.**

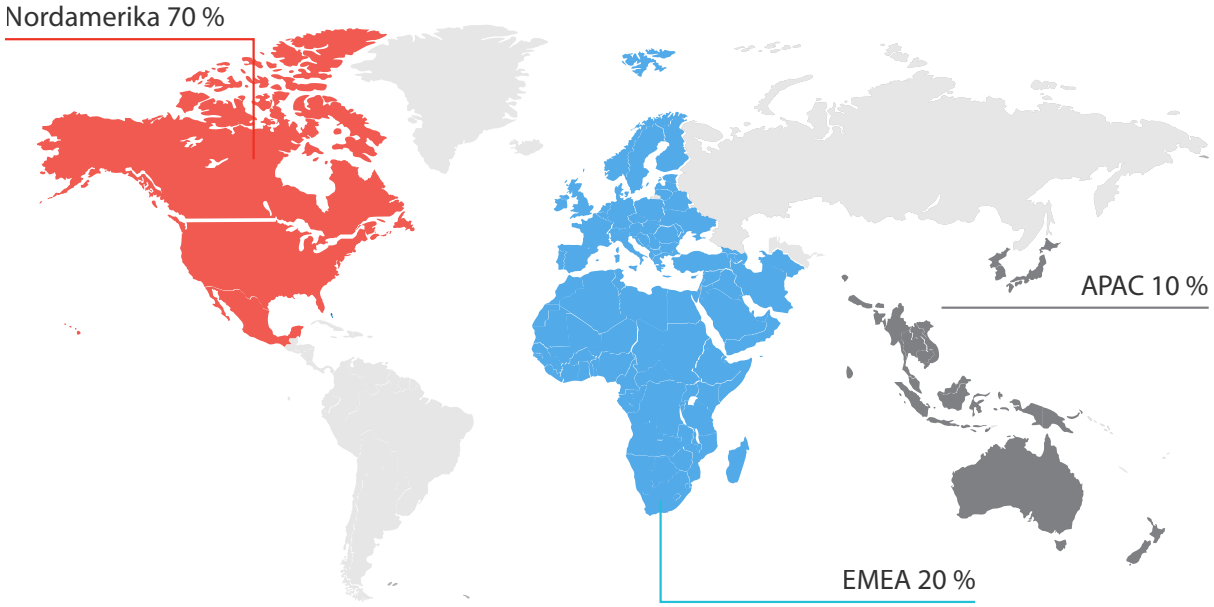
WatchGuard EPDR ist eine innovative Cybersicherheitslösung für Desktop-PCs, Laptops und Server, die über die Cloud bereitgestellt wird. Sie kombiniert eine sehr breite Palette an Schutztechnologien (EPP) mit EDR-Funktionen und bietet zwei, in die Lösung eingebundene Services, die von WatchGuard-Experten verwaltet werden: Zero-Trust Application Service und Threat Hunting Service. Mit nur einem einzigen, schlanken Agenten, der über eine einzige cloudbasierte Konsole verwaltet wird, stellt WatchGuard EPDR eine natürliche Erweiterung zum Sicherheitsprogramm eines jeden Unternehmens dar.

Erfahren Sie von unseren führenden Schwachstellenforschern alles Wissenswerte über das Threat Hunting in unserem neuesten eBook **Threat Hunting: Nehmen Sie eine proaktive Position** mit Ihrer Cybersicherheit ein und beginnen Sie Ihre Bedrohungsjagd mit **WatchGuard Advanced Endpoint Security.**

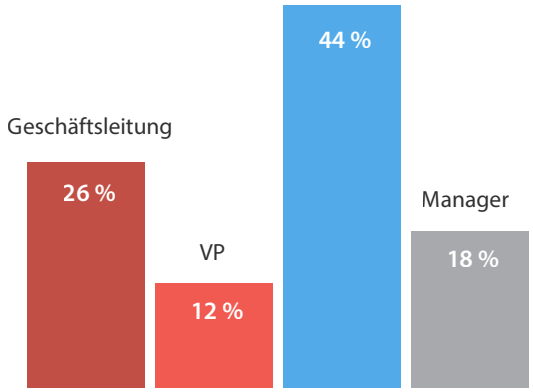
WatchGuard

Aufschlüsselung der Befragten

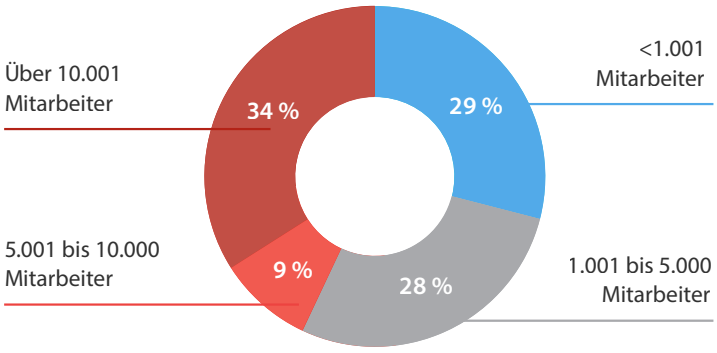
REGION



POSITION



UNTERNEHMENSGRÖßE



Das Sprichwort „Zeit ist Geld“ trifft wahrhaft auf Cyberangriffe zu und wenn ein Angriff stattfindet, tickt die Uhr. Handeln Sie also proaktiv statt reaktiv.

Weitere Informationen finden Sie auf unsere Website

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