cybereason

2023

Ransomware und das moderne SOC

So prägt Ransomware die Anforderungen an eine SOC-Modernisierung

Inhalt

Einleitung

Security Operations Centers (SOCs) aller Größen und Entwicklungsstände befinden sich in einem ständigen Würgegriff, der durch Personalmangel, mangelnde Transparenz und Automatisierung, eine unübersichtliche Vielzahl an Tools und eine Überlastung durch Warnmeldungen verursacht wird. Der Status quo des ständigen Kampfes, den Gegnern einen Schritt voraus zu sein, die Rentabilität von Sicherheitsinvestitionen aufzuzeigen und zugleich sicherzustellen, dass das schwer zu findende Personal nicht bis zum Burnout überlastet wird, ist auf Dauer unhaltbar.

In einer neuen Umfrage von Cybereason wurden 1.203 Sicherheitsexperten aus acht Ländern und einem Dutzend Branchen gebeten, die Herausforderungen zu beschreiben, mit denen ihre SOCs derzeit konfrontiert sind, und wie sich diese auf ihre Modernisierungspläne auswirken.

Fast die Hälfte der Befragten (49 %) gab an, dass Ransomware-Angriffe die häufigste Art von Vorfällen darstellen, mit denen sie täglich zu tun haben, dicht gefolgt von Angriffen auf die Lieferkette (46 %). 37 Prozent der Befragten gaben an, dass tägliche Warnmeldungen den größten Teil ihrer Zeit in Anspruch nehmen, und 31 Prozent nannten gezielte Angriffe als eine ihrer täglichen Hauptbeschäftigungen.

1.203
SICHERHEITSEXPERTEN

8
LÄNDER

HÄUFIGSTE VORFÄLLE

- RANSOMWARE **49 %**
- ANGRIFFE AUF DIE LIEFERKETTE **46 %**
- ALLTÄGLICHE SICHERHEITSBELANGE **37 %**
- GEZIELTE ANGRIFFE **31 %**

Fazit

57 % der Befragten geben an, dass die Behebung eines Vorfalls nach der Entdeckung 3 bis 6 Stunden dauert.

59 % der Befragten gaben an, dass ihr Unternehmen zwei Stunden bis einen Tag braucht, um einen Ransomware-Vorfall zu beheben. **19 %** gaben an, dass die Behebung eines Ransomware-Vorfalls 3 bis 7 Tage dauert.

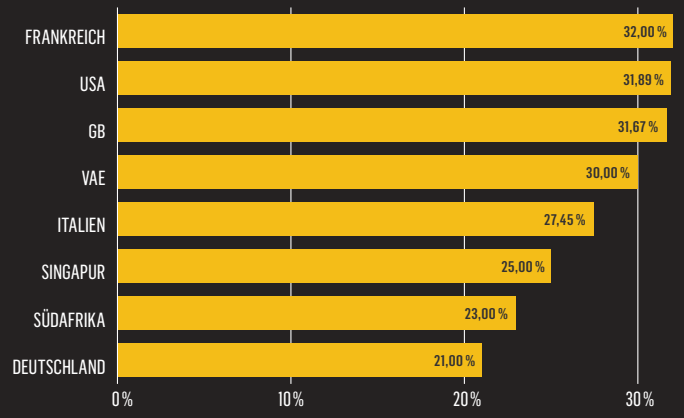
88 % der Befragten gaben an, dass sie wegen eines Ransomware-Angriffs schon einmal einen Feiertag oder ein Wochenende ausfallen lassen mussten.

Mehr als ein Drittel der Unternehmen berichtet, dass sie zwischen

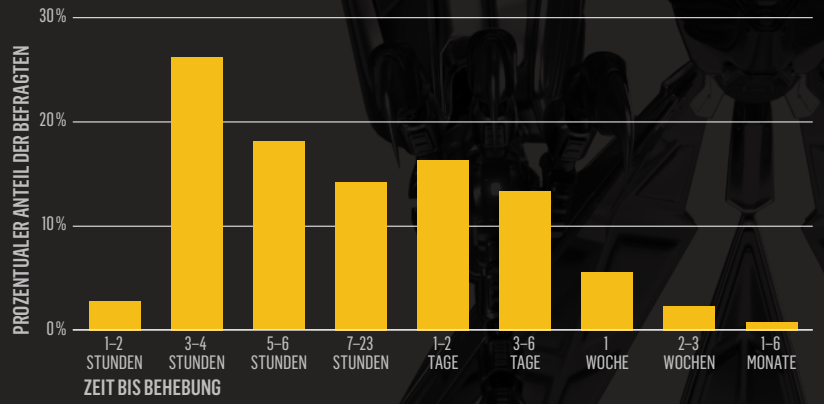
10.000 und 15.000

Sicherheitswarnungen pro Tag erhalten.

BEFRAGTE WELTWEIT, DIE ANGABEN, DASS RANSOMWARE DEN BEDARF AN AUTOMATISIERUNG UND KÜRZEREN REAKTIONSZEITEN ERHÖHT HAT



DURCHSCHNITTLICHE ZEIT, DIE ZUR BEHEBUNG EINES RANSOMWARE-ANGRIFFS BENÖTIGT WIRD



RANSOMWARE UND DAS FÄHIGKEITSBASIERTE SOC

Die bisher ermittelten Herausforderungen reichen aus, um die für die Modernisierung heutiger SOCs erforderlichen Investitionen zu rechtfertigen. Es ist jedoch wichtig zu wissen, dass es nicht mehr nur ein standardisiertes SOC-Modell gibt, das Unternehmen verwenden können. Beim Aufbau oder der Modernisierung eines SOC geht es heute nicht mehr um einen zentralen Standort mit spezifischen Sicherheitstools. Es geht um die Bereitstellung spezieller Funktionen, Fähigkeiten und Ergebnisse, die ein bestimmtes Unternehmen benötigt.

Mehr als 58 Prozent der Umfrageteilnehmer gaben an, dass ihr SOC die meiste Zeit damit verbringt, auf Ransomware und Angriffe auf die Lieferkette zu reagieren, die zu Ransomware-Vorfällen führen können. Auf die Frage, wie sich Ransomware auf ihre Pläne für die SOC-Modernisierung auswirkt, nannten die Umfrageteilnehmer insbesondere vier Anforderungen:

38 %
Neue Erkennungsmöglichkeiten, die eine bessere Erkennungseffizienz aufweisen

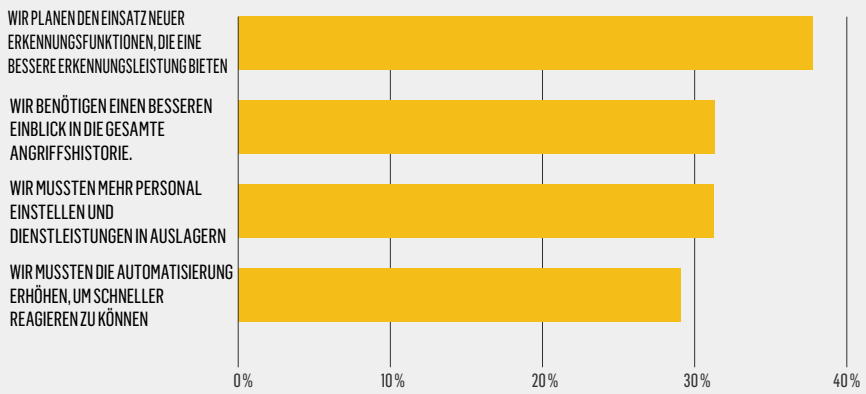
31 %
Besserer Einblick in die Angriffshistorie

31 %
Mehr Personal und Dienstleistungsverträge

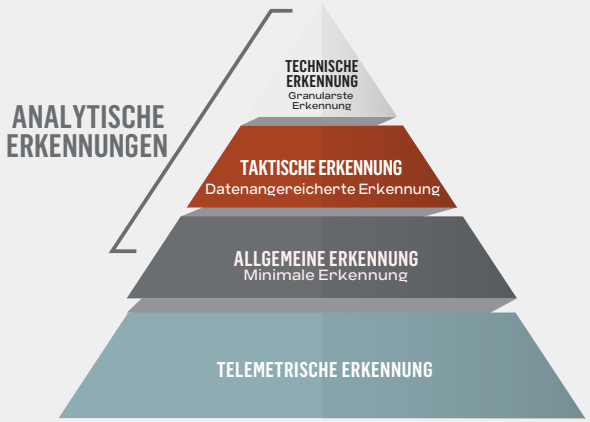
29 %
Verstärkte Automatisierung zur Verkürzung der Reaktionszeiten

Der Aufbau, die Modernisierung und der Betrieb eines SOC sind evolutionäre Prozesse, die sich mit dem Unternehmen, seinen Anforderungen und der Bedrohungslandschaft verändern. Die Richtung für das SOC der Post-COVID-Ära steht fest: Das moderne SOC wird eine dezentralisierte, fähigkeitsbasierte Einrichtung sein, die branchenführende Erkennungs-, Präventions-, Sichtbarmachungs- und Automatisierungstechnologien einsetzt, die häufig durch verwaltete Dienste ergänzt werden.

F1 WIE, WENN ÜBERHAUPT, HAT RANSOMWARE IHRE SOC-FÄHIGKEITEN VERÄNDERT?



BEDARF AN NEUEN ERKENNUNGS-VERFAHREN



Analytische Erkennungen beruhen auf einem umfangreicheren Datensatz und sind eine Kombination aus technischen und taktischen Erkennungen. SOC-Teams benötigen für datenangereicherte Erkennungen dringend diese differenzierte Sicht auf die Vorgänge.

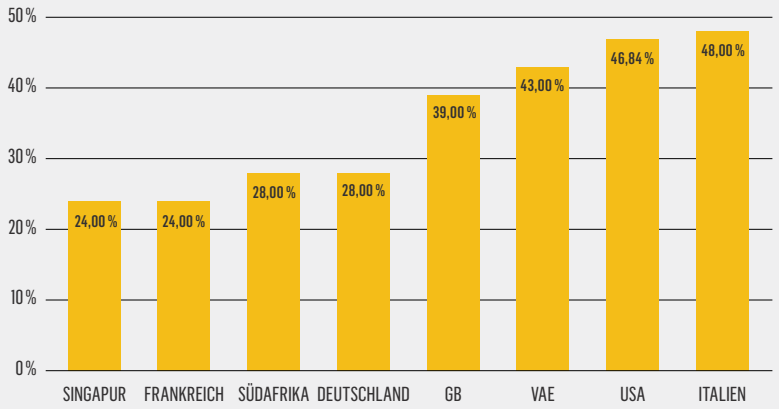
38 Prozent der Umfrageteilnehmer gaben an, dass sie planen, neue Funktionen zur Erkennung von Bedrohungen mit besserer Erkennungseffizienz einzusetzen.

Unabhängig von Größe und Komplexität kann ein modernes SOC gezielte Fähigkeiten zur Erkennung von und Reaktion auf Bedrohungen nutzen, die sich an den Risiken und Prioritäten des jeweiligen Unternehmens orientieren.

Herkömmliche Sicherheitslösungen für Endgeräte verlassen sich auf eingeschränkte Kompromittierungsindikatoren (Indicators of Compromise, IOCs) – die Artefakte von bereits bekannten Angriffen. Moderne Erkennungsfunktionen gehen über IOCs hinaus und nutzen Verhaltensindikatoren (Indicators of Behavior, IOBs), um bereits subtile Anzeichen eines Angriffs zu erkennen. Diese Verhaltensketten offenbaren einen Angriff in den frühesten Stadien, indem sie böswillige menschliche und maschinelle Aktivitäten erkennbar machen und so nie zuvor gesehene Angriffe einzeln aufdecken und aufhalten, bevor sie zu einem größeren Sicherheitsverstoß eskalieren.

Lösungen, die gegen heutige Bedrohungen – insbesondere ausgefeilte Bedrohungen wie Ransomware – hocheffizient sind, müssen in der Lage sein, bösartige Aktivitäten sofort zu erkennen, ohne zusätzliche Verarbeitungszeit oder das Eingreifen menschlicher Analysten abzuwarten.

F2 BEFRAGTE, DIE DEN EINSATZ NEUER ERKENNUNGSTECHNOLOGIEN AUFGRUND VON RANSOMWARE PLANEN



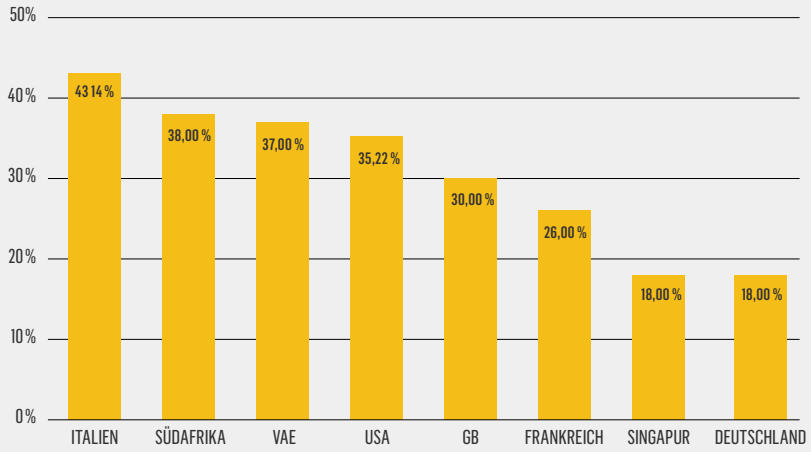
NOTWENDIGKEIT EINES BESSEREN EINBLICKS IN DIE GESAMTE ANGRIFFSHISTORIE

31 Prozent der Befragten gaben an, dass die Bedrohung durch Ransomware gezeigt hat, dass sie einen besseren Einblick in die gesamte Angriffshistorie benötigen.

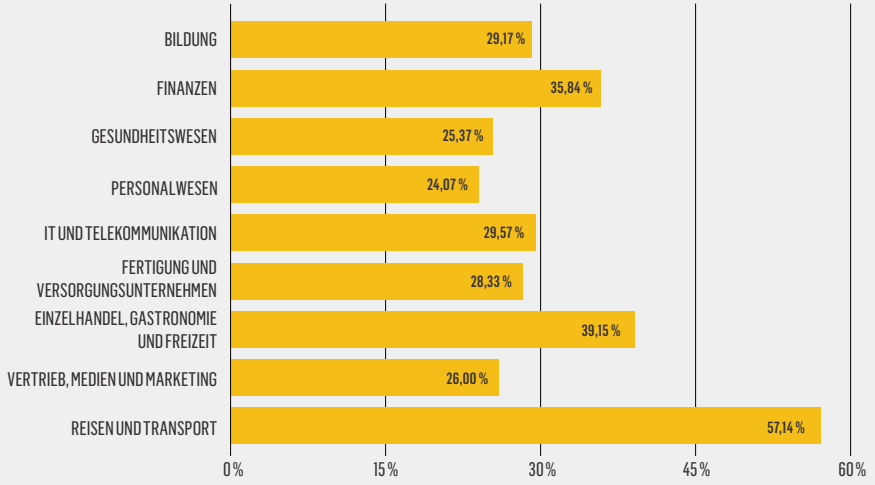
Die Bewertung der Fähigkeit von Lösungen, Transparenz zu bieten, quantifiziert ihre Effektivität bei der Bereitstellung des vollständigen Kontexts eines Angriffs, der Aufdeckung des Ursprungs, der betroffenen Objekte, des zeitlichen Ablaufs der Ereignisse und der detaillierten Details der Angriffskette.

Die Nutzung eines betriebszentrierten Ansatzes bedeutet, dass die gesamte Angriffshistorie von A–Z in einem einzigen Bildschirm dargestellt wird, einschließlich aller betroffenen Benutzer und Geräte. Dieses einzigartige Verständnis der Datenbeziehungen bedeutet, dass der vollständige Kontext eines Angriffs zu jeder Erkennung innerhalb eines **kriminellen Vorgangs** zur Verfügung steht und alle Benutzer, Geräte, Identitäten und Netzwerkverbindungen umfasst.

F3 BEFRAGTE PERSONEN NACH LÄNDERN, DIE SAGEN, DASS SIE EINEN BESSEREN EINBLICK IN DIE GESAMTE ANGRIFFSHISTORIE BENÖTIGEN



F4 BEFRAGTE NACH BRANCHEN, DIE ANGEBEN, DASS SIE EINEN BESSEREN EINBLICK IN DIE GESAMTE ANGRIFFSHISTORIE BENÖTIGEN



BEDARF AN MEHR PERSONAL UND DIENSTLEISTUNGEN

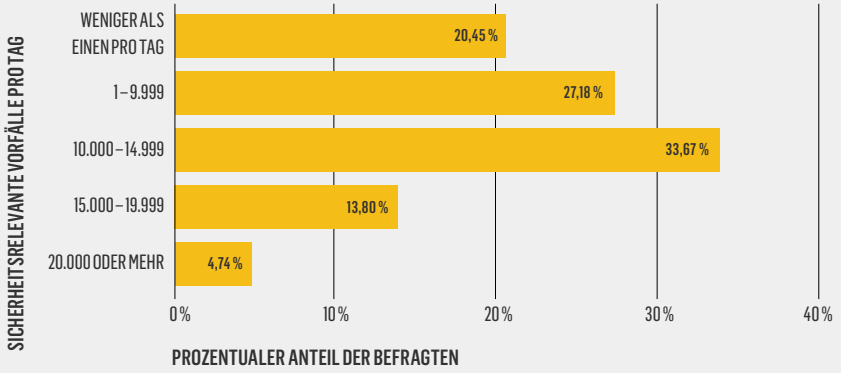
Mehr als ein Drittel der Befragten gab an, dass ihre SOCs zwischen 10.000 und 15.000 Sicherheitswarnungen pro Tag erhalten.

Die Informationsflut ist nach wie vor die Hauptursache für das Problem der Überlastung. Sicherheitsinformations- und Ereignisverwaltungsplattformen (SIEM) sind so konzipiert, dass sie eher zu viel Transparenz bieten, als dass sie eine Warnmeldung übersehen, die sich später als kritisch erweist und zu einem ernsthaften Sicherheitsereignis führt.

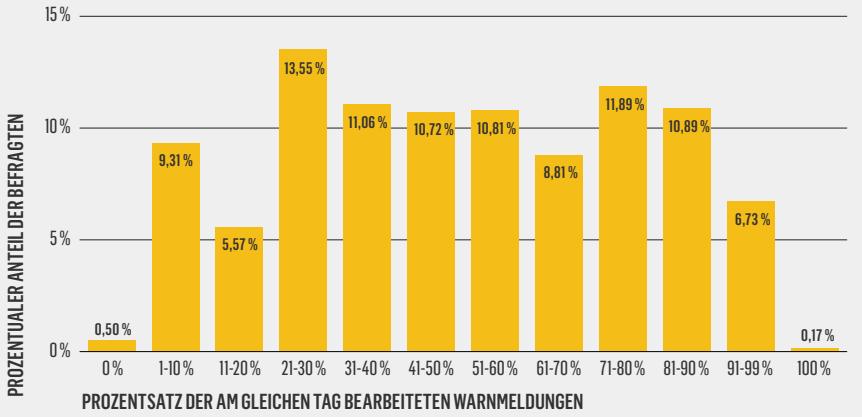
Die globale Cybersecurity-Talentkrise hat sich auf die SOC-Teams weltweit ausgewirkt und das Problem der Überlastung durch Warnmeldungen noch verschärft. Die Cyber-Branche hat mit einem massiven Mangel an qualifiziertem Personal zu kämpfen, der weltweit zu einer negativen Beschäftigungslage und etwa 3,5 Millionen unbesetzten Stellen im Cyber-Bereich geführt hat. Die qualifiziertesten Tier-III-Analysten sind extrem schwierig zu finden und noch schwieriger zu halten. Es überrascht nicht, dass die Informationsflut und der Druck, dem Analysten bei dem Versuch ausgesetzt sind, bösartige Aktivitäten aufzudecken, zu Burnout und einer hohen Personalfluktuation geführt haben.

Diese Herausforderungen haben ein verstärktes Interesse an Diensten rund um Managed Detection and Response (MDR) hervorgerufen. MDR befreit die Sicherheitsteams von der Last und dem mühsamen Prozess der Bewertung und Priorisierung von Warnmeldungen und spart Zeit, die ihnen dann zum Durchführen von Abhilfemaßnahmen und für die Konzentration auf andere Prioritäten zur Verfügung steht. Als eigenständige Sicherheitslösung oder als zusätzliche Sicherheitsebene zu einem bestehenden SOC verbessert MDR unmittelbar die Sicherheitslage eines jeden Unternehmens.

F5 WIE VIELE SICHERHEITSRELEVANTE VORFÄLLE MUSS IHR SOC AN EINEM DURCHSCHNITTLICHEN TAG BEARBEITEN (SOFERN ZUTREFFEND)?



F6 PROZENTSATZ DER WARNMELDUNGEN, DIE NOCH AM GLEICHEN TAG BEARBEITET WERDEN



NOTWENDIGKEIT EINER VERSTÄRKTEN AUTOMATISIERUNG ZUR VERKÜRZUNG VON REAKTIONSZEITEN

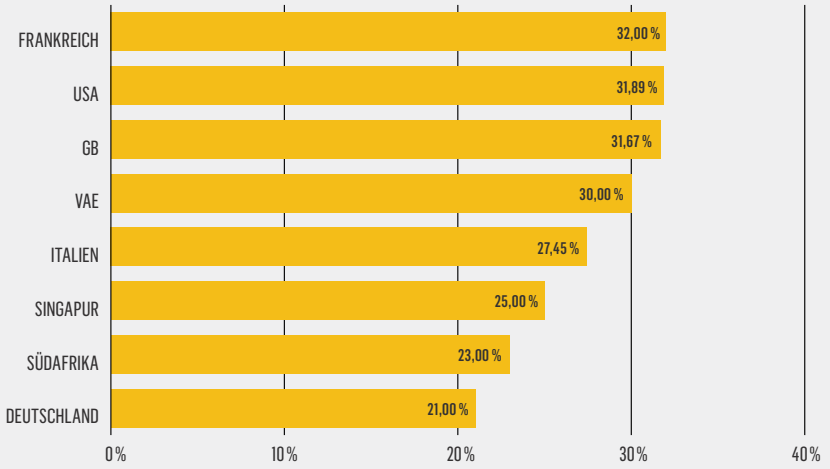
29 Prozent der Befragten weltweit gaben an, dass Ransomware ihren Bedarf an Automatisierung und kürzeren Reaktionszeiten erhöht hat.

Lösungen, die gegen heutige Bedrohungen – insbesondere ausgefeilte Bedrohungen wie Ransomware – hocheffizient sind, müssen in der Lage sein, bösartige Aktivitäten sofort zu erkennen, ohne zusätzliche Verarbeitungszeit oder das Eingreifen menschlicher Analysten abzuwarten.

Die Reaktion auf Vorfälle sollte orchestriert und automatisiert werden und alle betroffenen Endgeräte und Benutzer durch maßgeschneiderte Reaktionspläne erreichen, ohne dass eine externe SOAR-Lösung (Security Orchestration, Automation and Response) erforderlich ist.

Diese fortschrittliche und automatische Form der Analyse erhöht die Geschwindigkeit und Genauigkeit der Analysten, indem sie die „Dauerbeschallung" durch Warnmeldungen durch eine gezielte Dekonstruktion des Gesamtvorgangs reduziert. Durch die übersichtliche Darstellung aller Informationen, die Analysten benötigen, um eine böswillige Operation einzugrenzen und darauf zu reagieren, kann ihre MTTR (Mean Time to Respond) drastisch reduziert werden.

F6 PROZENTUALER ANTEIL DER BEFRAGTEN, DIE ANGABEN, DASS RANSOMWARE IHREN BEDARF AN AUTOMATISIERUNG ERHÖHT HAT



Anmerkung zur Methodik

Dieser Bericht basiert auf einer weltweiten Umfrage unter 1.203 Cybersicherheitsexperten, die in Unternehmen mit mehr als 700 Mitarbeitern arbeiten. Die Umfrage wurde zwischen dem 27. September 2022 und dem 4. Oktober 2022 durchgeführt.

Bei den beruflichen Rängen der Befragten ergab sich folgende Verteilung:

ÜBER CYBEREASON

Cybereason ist ein XDR-Unternehmen, das sich gemeinsam mit Defenders der Abwehr von Angriffen auf Endgeräteebene, in der Cloud und im gesamten Unternehmens-Ökosystem verschrieben hat. Nur die KI-gestützte XDR-Plattform von Cybereason bietet vorausschauende Prävention, Erkennung und Reaktion für bisher unerreichten Schutz gegen moderne Ransomware und fortschrittliche Angriffstechniken. Cybereason MalOp™ liefert sofort und mit unvergleichlicher Geschwindigkeit und Genauigkeit kontextreiche Angriffsinformationen über jedes betroffene Gerät, jeden Benutzer und jedes System. Cybereason verwandelt Bedrohungsdaten in umsetzbare Entscheidungen, die mit der Dynamik von Geschäftsprozessen Schritt halten können.

Cybereason hat mehrere unabhängige Branchenauszeichnungen erhalten, darunter die Bewertung als „Leader" im Gartner Magic Quadrant 2022 für Endgeräteschutz-Plattformen, und erzielte im Jahr 2022 die höchste Punktzahl in der Geschichte der MITRE ATT&CK-Unternehmensbewertungen.

Cybereason ist ein internationales Unternehmen in Privatbesitz mit Hauptsitz in Boston und Kunden in mehr als 40 Ländern.

Erfahren Sie mehr auf **www.cybereason.com**