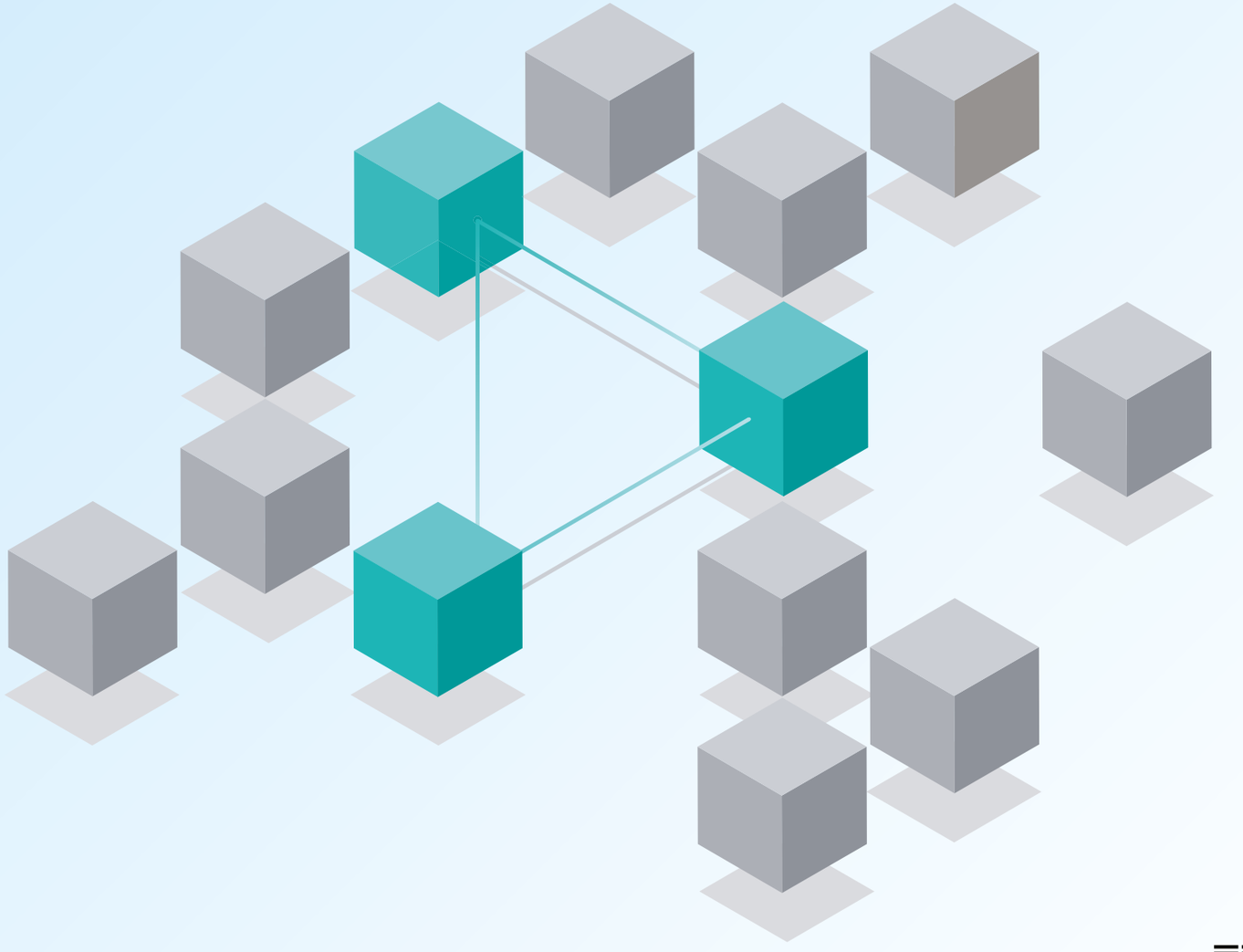
Leitfaden für den EDR-Kauf

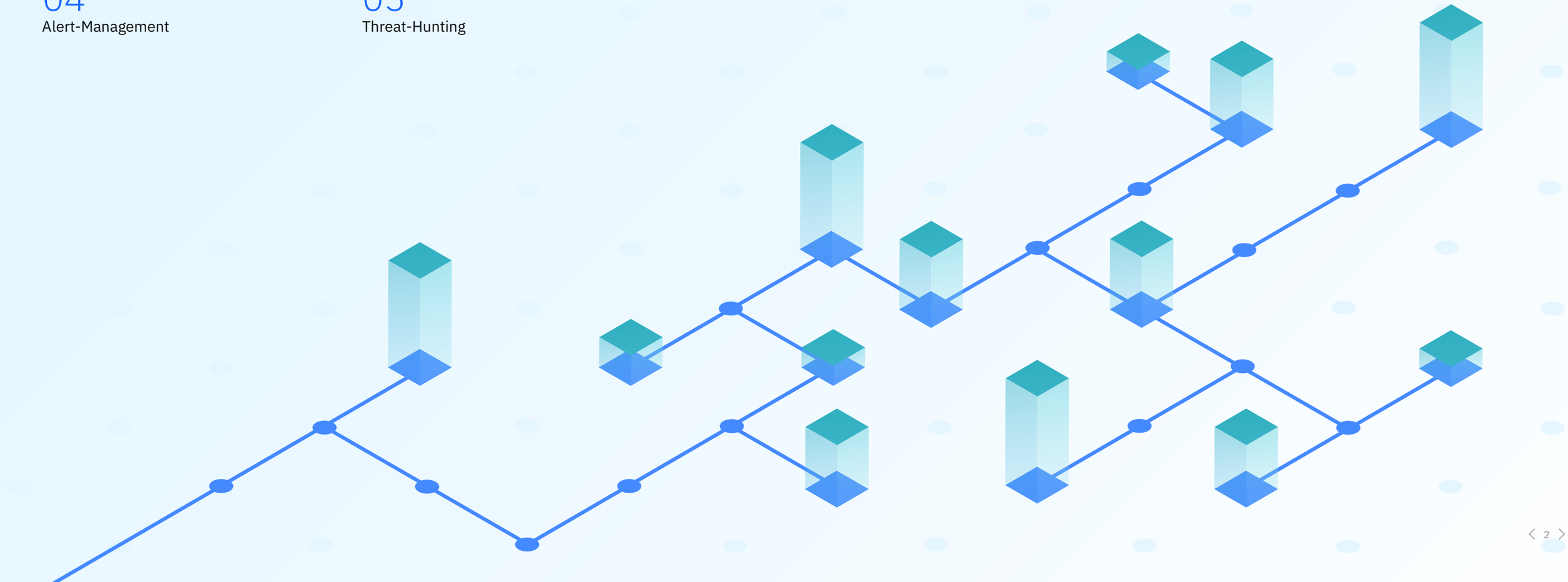
Wählen Sie die beste Endpoint-Detection- und Response-Lösung für Ihr Unternehmen



REAQTA
an IBM Company

IBM

Inhalt



01
Einführung

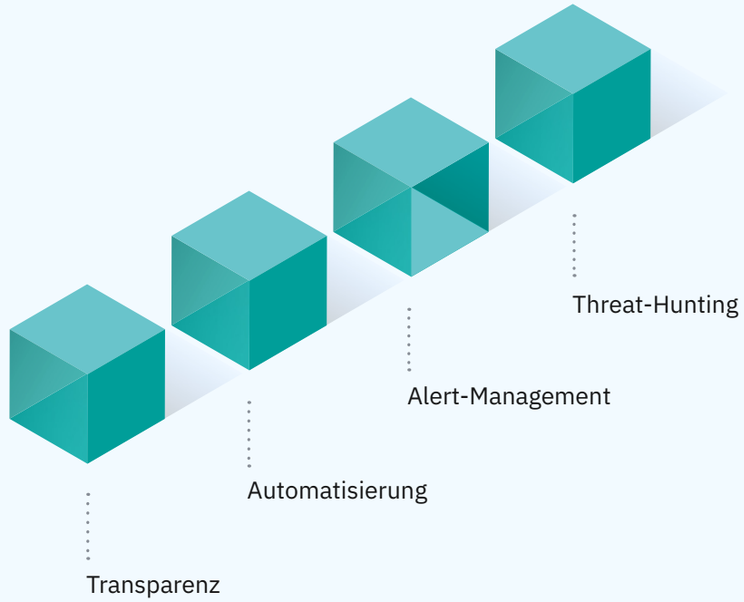
Was ist EDR und warum brauche ich das?
In den letzten Jahren haben wir eine steigende Verbreitung und Vernetzung von Endgeräten und Daten erlebt, zudem haben bösartige Aktivitäten von Schadakteuren zugenommen. Diese Faktoren haben für große wie kleine Unternehmen zu einer wesentlichen Bedrohung der Geschäftskontinuität beigetragen. Immer mehr Unternehmen fallen Angriffen von Cyberkriminellen und nationalstaatlichen Akteuren zum Opfer.

Herkömmliche Schutzmethoden bekämpfen zwar bekannte Bedrohungen, sind aber anfällig für ausgefeilte und unbekannte Angriffstechniken. Sie bieten keinen Einblick in die Systeme, was eines der Haupthindernisse für deren Absicherung ist. Fachkompetenz beim Endpunkt-Schutz ist meist nur den größten oder finanzstärksten Organisationen vorbehalten. Dies und die Tatsache, dass viele Angriffe jetzt mit maschineller Geschwindigkeit und vielen veränderlichen Komponenten erfolgen, haben dazu geführt, dass menschliche Teams, die mit herkömmlichen Endpunktschutzlösungen arbeiten, nicht mehr Schritt halten können.

Eine EDR-Lösung blockiert und isoliert Malware proaktiv und automatisch, und rüstet die Sicherheitsexperten mit den richtigen Tools zum souveränen Umgang mit diesen Herausforderungen aus. Eine moderne EDR kann die Geschäftskontinuität gewährleisten, indem sie ohne Mehraufwand für die Analysten und ohne hoch qualifizierte Sicherheitsspezialisten rasant zunehmende, automatische und moderne Bedrohungen, wie etwa Ransomware oder dateilose Angriffe, gering hält.

Kommen Ihnen diese Herausforderungen bekannt vor?
- Versagen vorhandener Lösungen
- Begrenzte Transparenz
- Mangel an qualifizierten Beschäftigten
- Ermüdung der Alarmbereitschaft
- Ruhende Bedrohungen

Eine moderne und effektive EDR umfasst vier Kernelemente, die wir uns in den folgenden Kapiteln genauer ansehen werden:



02 Komplette Transparenz Ihres Endpunktbestands

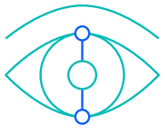
Eines der größten Hindernisse beim Schutz von Endpunkten ist die mangelnde Transparenz. Daher sollte eine moderne EDR-Lösung einen kompletten und tiefen Einblick in die laufenden Anwendungen und Prozesse bieten.

Beim Auftreten einer Bedrohung muss ein Echtzeit-Alert das Verhalten in Form eines graphischen Ablaufs aufzeigen, der automatisch während des laufenden Angriffs erstellt wird und Analysten mit MITRE ATT&CK Mapping komplette Transparenz und ein vollumfängliches Verständnis des Angriffsvorgangs bietet.

Die allermeisten Softwarelösungen für die Endpunktsicherheit arbeiten innerhalb des Betriebssystems, was eine Einschränkung für den Endpunkt-Agenten bedeutet. Die Möglichkeiten und die Transparenz des Agenten werden begrenzt bei gleichzeitig gesteigertem Rechnerressourcen-Verbrauch. Ein Agent, der auf der Hypervisor-Ebene agiert und unerkennbar bleibt, minimiert nicht nur den Ressourceneinsatz, sondern bietet auch außergewöhnliche Transparenz bei der Überwachung aller Prozessverhaltensweisen, während er für Angreifer unsichtbar bleibt.

Wichtige Eigenschaften:

- Komplette Endpunkt-Transparenz
- Echtzeit-Alert
- Ablaufdiagramm
- Reibungsloser Agent
- Vereinheitlichter Workflow



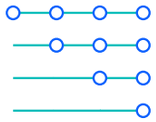
Fragen, die Sie sich stellen sollten:

→ Bietet Ihre Lösung umfassende, gründliche Transparenz der laufenden Anwendungen und Prozesse?

→ Liefert Ihre Lösung bei einem Angriff aussagekräftige Echtzeit-Informationen, die das Verständnis der Bedrohung verbessern?

→ Bietet Ihr MSSP neben einer Erkennungs- und Alert-Funktion auch End-to-End-Response und -Maßnahmen?

03
Automatisierung und Anwendungsfreundlichkeit



Angesichts der Prognose, dass hoch entwickelte Bedrohungen ebenso wie der Umfang der Angriffsflächen 2022 und darüber hinaus weiter zunehmen werden, stehen viele Organisationen unter großem Druck, Cyberkriminellen einen Schritt voraus zu bleiben. Eine moderne EDR sollte das wachsende Arbeitspensum durch intelligente Automatisierung reduzieren und durch Anwendungsfreundlichkeit den Bedarf an hoch qualifizierten Sicherheitsspezialisten verringern.

Der Schlüssel zur schnellen Wertschöpfung mit EDR sind Automatisierung und Vereinfachung. Durch KI-Automatisierung fällt der Großteil der Arbeit den Algorithmen zu, die Notwendigkeit für menschliches Eingreifen wird reduziert. Solche KI-Algorithmen ermöglichen eine einfachere Bedienung der Software und lange Einarbeitungszeiten entfallen.

Bei einem Angriff ist die Reaktionsgeschwindigkeit entscheidend: Die Ermittlungsdauer sollte weit unter einer Minute liegen, um komplexe Bedrohungen zu entfernen, bevor sie Ihrer Infrastruktur Schaden zufügen können.

Eine EDR-Lösung sollte autonom laufen sowie automatische Erkennung und Reaktion bieten. Analysten erhalten so einen klaren Echtzeit-Blick auf den Angriffsvorgang und können gezielte Maßnahmen ergreifen, um den Normalbetrieb rasch wiederherzustellen.

Wichtige Eigenschaften:
- Autonome Erkennung
- Gezielte Maßnahmen
- Agent-Analysen
- Schnelle Reaktionszeit
- Anwendungsfreundlichkeit

Fragen, die Sie sich stellen sollten:

→ Erfordert der Betrieb der EDR-Lösung fortgeschrittene Kenntnisse?

→ Kann die EDR-Lösung zur Reduzierung des Arbeitsaufwands der Analysten autonom laufen?

→ Werden – im Hinblick auf die Reaktionszeiten – Bedrohungen in der Cloud analysiert oder durch den Agenten?

→ Falls Bedrohungen in der Cloud analysiert werden: Was geschieht bei einer Unterbrechung der Internetverbindung?

04
Alert-Management

Im Unterschied zu einer EDR-Lösung erkennen Antiviren-Programme Bedrohungen anhand von verfügbaren Signaturen. Damit sie eine Bedrohung blockieren können, muss sie ihnen „bekannt“ sein. Eine EDR-Lösung verwendet hingegen einen verhaltensbasierten Ansatz und erkennt Malware und andere potenzielle Bedrohungen daran, was sie an einem Endpunkt tun. Im Gegensatz zu herkömmlichen AV-Programmen ist eine EDR-Lösung zudem von Natur aus schlank und erfordert keine häufigen Updates.

Die bei moderner EDR verwendete KI muss daher zu schneller, präziser und zuverlässiger Erkennung in der Lage sein, um die Alert-Menge – und den Arbeitsaufwand für Analysten – möglichst gering zu halten. Informieren Sie sich über die verwendeten Techniken für maschinelles Lernen und KI. Im Vergleich zu KI-Engines, die zur Erkennung vortrainierte Modelle und Analysen einsetzen, ermöglichen EDR-Lösungen, die ein anfängliches Lernmodell zur Erkennung des Normalverhaltens jedes Endpunkts verwenden, eine höhere Präzision bei der Erkennung und warnen bei Abweichungen vom Normalverhalten.

Um die Reaktionszeiten zu verringern und die Ermüdung der Alarmbereitschaft bei Analysten zu vermindern, sollte eine moderne EDR-Lösung über ein robustes, KI-gestütztes Alert-Managementsystem verfügen, das vom Analysten lernen kann und dann dessen Entscheidungsprozesse beim alltäglichen Umgang mit Alerts autonom anwendet. Der Einsatz eines vollautomatischen und KI-gestützten Alert-Managementsystems ist der Schlüssel im Kampf gegen die Ermüdung der Alarmbereitschaft, senkt die Mitarbeiterfluktuation und gibt Ihnen die Kontrolle zurück.

Wichtige Eigenschaften:
- Zuverlässige Alerts
- Verwendung von KI-Modellen
- Vorbeugung vor Ermüdung der Alarmbereitschaft
- Automatisches Alert-Management

Fragen, die Sie sich stellen sollten:

→ Kann Ihre Lösung Alerts automatisch verarbeiten und quittieren?

→ Kann Ihre Lösung Arbeitszeit für Analysten sparen?

→ Reduziert Ihre Lösung Fehlalarme?

→ Wenn Mitarbeitende das Unternehmen verlassen, wie lassen sich ihre Kenntnisse unserer Unternehmensstruktur dann erhalten?

05
Threat-Hunting

Threat-Hunting ist ein wichtiger Bestandteil einer modernen EDR-Lösung und in einer bedrohungsfreien Umgebung unerlässlich. Durch Threat-Hunting lässt sich schnell feststellen, ob neue Bedrohungen eingedrungen sind und wo sich welche Schwachstellen befinden. Data-Mining ermöglicht Ihnen das Aufspüren und Entfernen andernfalls unerkannter latenter Bedrohungen, die Monate oder Jahre schlummern können, bis sie von einem Angreifer benutzt werden.

Naturgemäß sind dateilose und speicherresidente Bedrohungen schwer aufspürbar und noch schwerer verfolgbar, wenn in einer großen Infrastruktur verschiedene Varianten eingesetzt werden. Eine moderne EDR-Lösung sollte die Suche automatisieren und es den Sicherheitsexperten ermöglichen, per Data-Mining automatisch nach Bedrohungen zu suchen, die auf Verhaltens- und Funktionsebene Ähnlichkeiten mit anderen Vorfällen aufweisen, sodass innerhalb von Sekunden Ergebnisse vorliegen.

Beim Threat-Hunting ist Flexibilität äußerst wichtig. Streben Sie eine EDR-Lösung an, die neben einer umfangreichen Bibliothek an vordefinierten Erkennungsstrategien zum sofortigen Einsatz auch individuelle Strategien bietet, die sich einfach und ohne Programmierkenntnisse erstellen lassen und auf unternehmensspezifische Sicherheitsszenarien eingehen.

Threat-Hunting wird oft mit der sprichwörtlichen Suche nach der Nadel im Heuhaufen verglichen. Eine EDR-Suche muss umfassende und detaillierte Ergebnisse in Echtzeit bieten, indem sie spezifische Hunting-Parameter gezielt ansetzt, die sich inklusiv oder exklusiv kombinieren lassen. Als weitere Hilfestellung und Entlastung für Analysten sollten die Ergebnisse leicht verständlich grafisch dargestellt werden, sodass zu jeder Zeit und von jedem Endpunkt aus unkompliziert und intuitiv nach allen Vorfällen gesucht werden kann.

Wichtige Eigenschaften:
- Suche nach latenten Bedrohungen
- Automatisches Hunting
- Erstellung individueller Strategien
- Kein Programmieren erforderlich
- Data-Mining
- Echtzeit-Funktionalitäten
- Grafische Übersicht

Fragen, die Sie sich stellen sollten:

→ Können Anwender eigene Erkennungsstrategien erstellen?

→ Lassen sich Threat-Hunting-Szenarien automatisieren?

→ Bieten Sie eine grafische Übersicht des Threat-Huntings zur schnellen Vorsortierung?

→ Erfordert die Erstellung von Strategien Programmierkenntnisse?

Nächste Schritte

Erfahren Sie mehr über IBM Security ReaQta und fordern Sie eine Demo an.

IBM Deutschland GmbH
IBM-Allee 1
71139 Ehningen
ibm.com/de

IBM Österreich
Obere Donaustraße 95
1020 Wien
ibm.com/at

IBM Schweiz
Vulkanstrasse 106
8010 Zürich
ibm.com/ch

Hergestellt in den Vereinigten Staaten von Amerika
April 2022