Kaspersky Next XDR Expert

Für ein Plus an Sicherheit

kaspersky

XDR – ein Gamechanger?

XDR: Extended Detection and Response

XDR ist in aller Munde, aber wie bei allen relativ jungen Technologien weiß keiner so genau, was das ist oder was es für das eigene Unternehmen leisten kann. Eines ist sicher: XDR bedeutet einen Strategiewechsel vom reaktiven zum proaktiven Handeln – denn Abwarten ist in Sachen Cybersicherheit keine Option. Es lohnt sich durchaus, in XDR eine Strategie und nicht nur ein Produkt zu sehen.

Hat XDR also das Potential zum Gamechanger? Die Herausforderungen sind groß: Angefangen beim weltweiten Fachkräftemangel, der Überlastung von IT-Sicherheitsmitarbeitern und einer Bedrohungslandschaft, die niemals stillsteht, bis hin zur Alarmermüdung, unzusammenhängenden Tools, unzureichenden Bedrohungsdaten und immer größer werdenden Angriffsflächen. Laut IDC wird sich XDR zu „einer disruptiven Kraft entwickeln, die sich nicht nur auf den Vertrieb von SIEM-, EDR-, SOAR-, Netzwerkdaten- und Bedrohungsanalyse-Plattformen, sondern auch auf externe Threat Intelligence-Anbieter auswirken wird“[1]. Und bei Forrester geht man davon aus, dass differenzierte XDR-Technologien „demnächst EDR an Endpoints (Detection and Response) ablösen und langfristig SIEM verdrängen werden“[2].

Für welche Unternehmen ist XDR geeignet?

XDR wurde für Unternehmen mit einem ausgereiften Sicherheitskonzept entwickelt, die eine zentrale Plattform benötigen, um einen vollständigen Überblick über alle Vorgänge in ihrer Infrastruktur zu erhalten.

XDR wird sich zu einer disruptiven Kraft entwickeln – IDC

Mehr Geräte, mehr Anwendungen, mehr Netzwerkverkehr, mehr Daten, mehr Bedrohungen …

Für wen ist XDR geeignet – und welche Herausforderungen lassen sich damit angehen?

XDR wurde für Unternehmen mit einem ausgereiften Sicherheitskonzept entwickelt, die eine zentrale Plattform benötigen, um einen vollständigen Überblick über alle Vorgänge in ihrer Infrastruktur zu erhalten.

Die Herausforderungen für die Cybersicherheit, mit denen diese Unternehmen konfrontiert sind, sind überall dieselben und hinreichend bekannt. ESG Research befragte IT- und Cybersicherheitsexperten[3] in Unternehmen aus unterschiedlichen Branchen mit 100 Mitarbeitern oder mehr, davon über 80 % Großunternehmen. Hier die wichtigsten Erkenntnisse:

1 Quelle: IDC Global Security Products Analysis: From Power Point to Power Product, Where Is XDR Right Now? 2022

2 Quelle: Forrester, Extended Detection and Response (XDR) – A Battle Between Precedent and Innovation, Allie Mellen, Senior Analyst, 2021

3 Quelle: ESG Research Report, SOC Modernisierung und die Rolle von XDR, 2022

Schwierigkeiten mit den betrieblichen Anforderungen von SOC-Technologien Schritt zu halten

Die Verwaltung von Sicherheitssystemen ist heute komplexer als noch vor zwei Jahren. Dies ist unter anderem auf die hohen Anforderungen an den Betrieb der SOC-Technologien zurückzuführen – Skalierbarkeit der Datenpipeline, Verarbeitungsmodule für den Lastausgleich, erweiterte Speicherkapazitäten, usw. – und auf die Tatsache, dass das Management von Sicherheitssystemen heute komplexer ist als noch vor zwei Jahren.

Immer größer werdende und sich ständig wandelnde Angriffsfläche sowie die Bedrohungslandschaft als Ganzes

Mehr Geräte, mehr Anwendungen, mehr Netzwerkverkehr, mehr Daten, mehr Bedrohungen. Die Bedrohungslandschaft befindet sich im stetigen Wandel, und Cyberbedrohungen werden infolge der schnellen Ausbreitung neuer Tools immer umfangreicher und komplexer. Gleichzeitig sind die Einstiegshürden für Hacker so niedrig wie nie zuvor. Das Spektrum reicht von wenig qualifizierten Käufern billiger Bedrohungspakete im Darknet bis hin zu hochqualifizierten Hackern, die mit äußerster Geduld komplexe Angriffe entwickeln. Und nicht zu vergessen die Bedrohungen durch Insider und Schwachstellen in der Lieferkette.

Und noch immer basieren Sicherheitssysteme vielerorts auf manuellen Prozessen.

Immer mehr Sicherheitsdaten müssen erfasst und verarbeitet werden, und die manuelle Verarbeitung ist ineffizient und ineffektiv. Diese Faktoren wirken sich nicht nur negativ auf die Skalierbarkeit aus, sondern führen auch zu einer übermäßigen Abhängigkeit von menschlichen Eingriffen und beeinträchtigen die Effizienz der Bedrohungsbekämpfung im Allgemeinen.

Erkennungsregeln können nicht erstellt werden

Der Mangel an Zeit, Ressourcen und Qualifikationen führt dazu, dass Erkennungsregeln nicht erstellt werden, Sicherheitssysteme nicht verfeinert werden und eine schnelle und effiziente Erkennung und Abwehr von Bedrohungen nicht möglich ist. Die Unternehmen verfügen nicht über das notwendige Fachwissen oder Personal, um mit der Sicherheitsanalyse und den Sicherheitsprozessen Schritt zu halten. Was uns direkt zum nächsten Problem bringt …

Der globale Fachkräftemangel

Obwohl die Zahl der Beschäftigten im Bereich Cybersicherheit weltweit mit 4,7 Millionen Fachkräften ihren bisherigen Höchststand erreicht hat, besteht immer noch eine Lücke von 3,4 Millionen, die gefüllt werden müsste – aber nicht gefüllt wird. Diese Lücke wächst doppelt so schnell wie die Mitarbeiterzahlen, nämlich um 26,2 % im Vergleich zum Vorjahr.[4]

[4] Quelle: (ISC)², Studie zu Mitarbeitern in der Cybersicherheit, 2022

Die vorhandenen Tools reichen häufig nicht aus,

um hochentwickelte Bedrohungen zu erkennen und zu untersuchen. Denn um sie wirksam einzusetzen und zu verwalten, sind Spezialkompetenzen erforderlich.

Unzureichende Tools

Wenn die Tools selbst zum Teil des Problems werden, ist es an der Zeit zu handeln. Die vorhandenen Tools reichen häufig nicht aus, um hochentwickelte Bedrohungen zu erkennen und zu untersuchen. Denn um sie wirksam einzusetzen und zu verwalten, sind immer noch Spezialkompetenzen erforderlich. Wie Untersuchungen[5] zeigen, sind die derzeitig eingesetzten Tools häufig nicht dafür konzipiert, Warnmeldungen miteinander in Zusammenhang zu bringen. Gleichzeitig muss sich das IT-Sicherheitspersonal mit mehreren unzusammenhängenden Tools und nicht kompatiblen Daten auseinandersetzen. Eine solche Arbeitsweise ist ineffizient, umständlich, chaotisch und teuer. Eine weitere Herausforderung besteht darin, dass die derzeitigen Tools nicht skalierbar sind, um mit der wachsenden Angriffsfläche mitzuhalten, und dass es große Lücken bei den Erkennungs- und Reaktionsfunktionen in der Cloud gibt.[6]

Wen wundert es da noch, dass Ihr CISO gestresst aussieht?

Die gute Nachricht ist, dass Unternehmen der Verbesserung von SecOps nun Priorität einräumen und dafür auch Geld in die Hand nehmen. 88 % der Unternehmen planen, ihre Investitionen in diesem Jahr zu erhöhen, 66 % nennen die Konsolidierung ihrer Tools als vorrangige Aufgabe, und auch die Entwicklung und Bereitstellung moderner Programme hat an Dynamik gewonnen, was neue Qualifikationen erfordert.[7]

88%

der Unternehmen planen in diesem Jahr in die SecOps-Optimierung zu investieren

66%

geben an, sich vorrangig um die Konsolidierung ihrer Tools bemühen zu wollen

Die Vorteile von XDR

So begegnet XDR diesen Herausforderungen:

XDR erkennt hochentwickelte Bedrohungen besser

Die XDR-Funktionen zur Erkennung von Bedrohungen erfassen Endpoints, Netzwerke und Cloud-Umgebungen. Die Lösung nutzt lernfähige Algorithmen und Verhaltensanalysen, um raffinierte Bedrohungen wie Malware, Ransomware und hochentwickelte APTs (Advanced Persistent Threats) zu identifizieren.

Automatisierte Reaktion und Abhilfemaßnahmen

XDR automatisiert Reaktions- und Abhilfemaßnahmen und ermöglicht es Unternehmen, Bedrohungen schnell einzudämmen und mögliche Schäden gering zu halten. Gefährdete Endpoints werden in Quarantäne gesetzt oder isoliert, schädliche Aktivitäten blockiert und Schwachstellen behoben, wodurch der manuelle Aufwand und die Reaktionszeit reduziert werden.

[5] Quelle: ESG Research Report, SOC Modernisierung und die Rolle von XDR, Mai 2022

[6] Quelle: ESG Research Report, SOC Modernisierung und die Rolle von XDR, 2022

[7] Quelle: ESG Research Report, SOC Modernisierung und die Rolle von XDR, Mai 2022

Wie sich XDR in das Ökosystem von EDR, MDR, SOAR und SIEM einfügt

Die Antwort liegt im X – Extended, was so viel heißt wie „erweitert". XDR erweitert EDR um die Möglichkeiten der proaktiven Erkennung komplexer Bedrohungen auf mehreren Infrastrukturebenen und kann dadurch automatisch auf diese Bedrohungen reagieren und sie abwehren.

Der Schlüssel liegt in der Integration

Durch die Integration verschiedener Tools und Sicherheitsanwendungen sowie die Überwachung von Daten auf Endpoints, Netzwerken, Clouds, Webservern, Mailservern und mehr trägt XDR dazu bei, Bedrohungen zu erkennen und zu beseitigen. Gleichzeitig wird die Verwaltung der Informationssicherheit durch die automatisierte und produktübergreifende Interaktion vereinfacht.

Forrester ist der Ansicht, dass XDR die Sicherheitsanalyse-Plattformen in den meisten Fällen nicht vollständig ersetzen wird, und weist darauf hin, dass „XDR erst am Anfang steht, und [wir] erwarten, dass es in den nächsten fünf Jahren zu einer Konfrontation zwischen Sicherheitsanalyse-Plattformen und XDR kommen wird".

Für SIEM bestehen Einsatzmöglichkeiten jenseits der Bedrohungserkennung, und die Anpassungsfähigkeit von SOAR hat ihren eigenen Nutzen, aber wenn es um die Bedrohungserkennung und -reaktion geht, sind die erweiterten Analysefunktionen und der verbesserte Schutz von XDR unübertroffen.

Integration mit Tools zum Schutz von Endpoints

Die Integration mit EPP ist ein zentrales Thema, und XDR nutzt umfangreiche Endpoint-Telemetrie und Verhaltensanalysen, um tiefe Einblicke in die Aktivitäten an Endpoints zu ermöglichen. Zum Einsatz kommen fortschrittliche lernfähige Algorithmen, die verdächtiges Verhalten und Angriffsindikatoren (IOAs) erkennen, damit raffinierte Bedrohungen frühzeitig erkannt werden.

Bietet Transparenz in Echtzeit

XDR liefert einen Echtzeit-Überblick über die Sicherheitsstellung Ihres Unternehmens. Die Lösung erfasst und analysiert Daten aus verschiedenen Quellen, wie z. B. Endpoints, Servern, Firewalls und Cloud-Plattformen, und bietet über eine zentrale Konsole Einblick in laufende Bedrohungen und verdächtige Aktivitäten. So wird sie im wahrsten Sinne des Wortes vorausschauend aktiv – mit proaktivem Threat Hunting und schnellerer Vorfallsreaktion. Die detaillierte Übersicht sorgt dafür, dass Sicherheitsteams verdächtige Aktivitäten und potenzielle Sicherheitsvorfälle effizienter erkennen.

Stellt einen Kontext zwischen Daten und Bedrohungsinformationen her

Mithilfe hochwertiger Bedrohungsdaten und einer umfassenden Bedrohungsdatenbank liefert XDR äußerst nützliche kontextbezogene Informationen über Bedrohungen und Angreifer. Diese angereicherten Bedrohungsdaten vereinfachen Warnmeldungen aus Untersuchungsergebnissen sowie die Vorfallsbearbeitung und helfen Sicherheitsteams, die Taktiken, Techniken und die Stoßrichtung der Bedrohungsakteure zu verstehen, was eine effektivere Vorfallsreaktion und das proaktive Einleiten von Abwehrmaßnahmen ermöglicht.

Ermöglicht eine Optimierung des Sicherheitssystems

Bei korrekter Integration fügen sich die besten Lösungen problemlos in Ihre aktuelle Infrastruktur ein. Sie ziehen dabei den optimalen Nutzen aus der Automatisierung, erhalten volle Transparenz und umfassenden Einblick, ohne die bereits vorhandenen Sicherheitslösungen von Drittanbietern ersetzen zu müssen. Und wenn Sicherheitsvorfälle und Nutzerverhalten umfassend dargestellt werden können, sorgt die Integration auch für eine verbesserte Compliance.

XDR hält offensichtlich, was es verspricht: Kontrolle, Stabilität und diese alles entscheidenden Vorteile. Aber nicht alle XDR-Angebote sind gleich … Wie wählt man das passende aus?

5 Entscheidungskriterien beim Vergleich von XDR-Anbietern und -Lösungen

So begegnet XDR diesen Herausforderungen:

1

Zwischen der Qualität einer XDR-Lösung und der Synergie zwischen dem EPP- und EDR-Produkt eines Anbieters besteht ein direkter Zusammenhang

Ein zentrales Element von XDR ist die fortschrittliche Erkennung und Reaktion auf hochentwickelte Cyberbedrohungen auf Endpoint-Ebene. Gleichzeitig benötigt EDR eine robuste Endpoint Protection Platform (EPP), um eine große Anzahl von Massenbedrohungen automatisch herauszufiltern. Dabei sollte das Hauptaugenmerk auf den Endpoint-Schutzfunktionen liegen, um zu prüfen, ob alle Arten von Endgeräten – PCs, Laptops, virtuelle Maschinen, mobile Geräte und die unterschiedlichen Betriebssysteme – unterstützt werden.

2

Aktuelle Bedrohungsdaten und ein vollständiger Überblick über die Taktiken und Techniken von Cyberkriminellen sind unverzichtbar, um Cyberbedrohungen wirksam zu bekämpfen

Das Rad muss nicht neu erfunden werden. Jede gute XDR-Lösung bietet diese beiden Funktionen sowie zusätzlichen Kontext, um die Untersuchung und Reaktion auf Vorfälle zu verbessern und zu beschleunigen.

3

Integration mit Drittanbieter-Lösungen ist nachhaltiger und kostengünstiger

Wie gut sich eine XDR-Lösung mit Drittanbietern integrieren lässt, ist ein weiterer entscheidender Punkt, denn Interoperabilität macht eine Investition auch nachhaltiger. Eine XDR-Lösung, die zahlreiche funktionierende Integrationsoptionen bietet, kann mehr Datenquellen berücksichtigen und die Vorgänge in Ihrer Infrastruktur umfassender darstellen.

4

Unabhängige Bewertungen, weltweite Anerkennung und unabhängige Testergebnisse sind dafür ein guter Indikator

Wenn Sie für Ihr Unternehmen in etwas so Wichtiges wie Cybersicherheit investieren, sollten Sie einen Blick auf unabhängige Bewertungen werfen. Fragen Sie nach den Ergebnissen unabhängiger Tests. Informieren Sie sich über internationale Auszeichnungen von Forrester, IDC und anderen. Werden die Lösungen weltweit implementiert? Fragen Sie nach Fallstudien.

5

Ist Ihre Investition zukunftssicher?

Technologien entwickeln sich ständig weiter, das gilt um so mehr für ein relativ junges Produkt wie XDR. Daher sollten Sie sich genau anschauen, wie ein Anbieter seine Produkte langfristig weiterentwickeln will.

Warum Kaspersky?

Häufig getestet. Vielfach ausgezeichnet. Schutz von Kaspersky

Kaspersky ist ein etabliertes, weltweit tätiges Cybersicherheitsunternehmen mit langjähriger Expertise. Wir schützen seit über 25 Jahren Organisationen auf der ganzen Welt und haben für unsere Produkte und Dienstleistungen zahlreiche Auszeichnungen erhalten. Lösungen von Kaspersky haben zwischen 2013 und 2022

587

587 erste Plätze erreicht

685

685 Top-Drei-Platzierungen erreicht

827

an 827 unabhängigen Tests teilgenommen

Im Jahr 2023 wurde Kaspersky von dem weltweit führenden Technologieforschungs- und Beratungsunternehmen ISG zum Marktführer im Bereich XDR-Lösungen ernannt. ISG definiert „Leader“ als Unternehmen mit einem umfassenden Produkt- und Dienstleistungsangebot, das für Innovationskraft und Wettbewerbsstabilität steht.

Mehr erfahren

Kaspersky Extended Detection and Response

Mehr erfahren

www.kaspersky.de

#kaspersky
#bringonthefuture