SIEBEN IRRTÜMER
über XDR

Die Cybersicherheitsbranche hat zu lange mit isolierten, unverbundenen Sicherheitstools gearbeitet. Sicherheitsteams benötigen eine Lösung, die ein einheitliches Sicherheitskonzept bietet. XDR vereint verschiedene Sicherheitstools in einer einzigen Architektur und stellt so Transparenz, hochautomatisierte Erkennung und effektivere Korrelation, Priorisierung und Reaktionsmöglichkeiten bereit, um anhand eines neuen Ansatzes proaktive Sicherheitsverfahren zu vereinfachen und zu verbessern.

Und obwohl die Akzeptanz von XDR zunimmt, halten sich einige Irrtümer hartnäckig. Sieben dieser Mythen wollen wir nun aufdecken.

1 Einrichtung und Konfiguration von XDR sind kompliziert

Unternehmen jeder Größe sind dem Risiko ausgesetzt, gehackt zu werden, einschließlich KMUs, die oft als leichte Ziele angesehen werden. XDR ermöglicht ihnen, die Leistung ihrer begrenzten Anzahl von Mitarbeitern durch Automatisierung und einheitliche Visualisierung zu maximieren. Trotzdem müssen alle Aspekte bei der Bereitstellung von Sicherheit vereinfacht werden, um beispielsweise komplexe Einrichtungen und Konfigurationen zu vermeiden.

2 XDR kann bei vielen weniger leistungsfähigen Point-Sicherheitsprodukten effektiv sein

Viele XDR-Anbieter sind auf ein bestimmtes Fachgebiet spezialisiert, entweder auf Netzwerk oder Endpoint, oder bieten mit SIEM oder SOAR eine attraktivere Lösung an. XDR ist jedoch darauf ausgelegt, die Funktionalität der Sicherheitsstruktur zu optimieren, und nicht darauf, sie zu ersetzen. Die Anbieter müssen in allen Bereichen hervorragende Leistungen erbringen und gleichzeitig zusammenarbeiten, um zusätzliche Anwendungsfälle durch kontinuierliche Überwachung, Korrelation, Erkennung und Reaktion über diese Produkte hinweg abzudecken.

3 XDR kann ohne Berücksichtigung der Identität effektiv sein

Angreifern geht es vor allem um den Zugriff auf wichtige Daten, in der Regel als Anwender mit höheren Berechtigungen, und eine unbemerkte laterale Bewegung. EDR bietet kritische detaillierte Einblicke und präzise Reaktionsmaßnahmen für Endpoints. Sicherheitsteams benötigen jedoch konsolidierte und umfassende Einblicke in Echtzeit sowie umsetzbare Aktionen für die gesamte Sicherheitsstruktur, darunter auch für Identitäten wie Anwender.

4 XDR ersetzt SIEM und umgekehrt

XDR ersetzt SIEM nicht, da dies auf Anwendungsfälle abzielt, die nicht mit Sicherheit zusammenhängen, beispielsweise die Speicherung von Protokollen im Rahmen der Compliance und die Analyse von Geschäftsdaten. XDR deckt zwar Anwendungsfälle bei der Cybersicherheit ab und kann SIEM in dieser Hinsicht ersetzen – ein Unternehmen kann jedoch andere Anforderungen haben, die sich nur von SIEM erfüllen lassen. XDR ist außerdem nicht nur eine andere Art von SIEM. XDR gibt es nicht ohne integrierte Reaktion („Response“), wie der Name schon sagt. Erfahren Sie mehr.

5 XDR muss Daten aus allen Quellen aufnehmen

Es ist wichtig zu beachten, dass XDR nicht dazu gedacht ist, alle möglichen Daten aus dem Unternehmen zu erfassen. XDR-Inputs müssen einen Mehrwert für die Erkennungs-, Ermittlungs- und Reaktionsphase im Lebenszyklusmanagement der Bedrohung darstellen oder sollten nicht einbezogen werden. Andernfalls sehen sich die Sicherheitsteams mit Problemen bei der Aufbewahrung und Speicherung von Daten sowie mit der Uneinheitlichkeit der Daten konfrontiert, ähnlich wie bei SIEM.

6 XDR stützt sich auf die Vereinheitlichung von Tools verschiedener Hersteller durch APIs

Offenes XDR ermöglicht Sicherheitsteams, Tools mithilfe von APIs zu integrieren. Dieser Ansatz hat jedoch viele Nachteile, darunter eine mangelnde Integrationstiefe, eine gemeinsame Datenstruktur und Verzögerungen bei der Datenabfrage. Dies macht die Automatisierung bei der Erkennung und Reaktion sowie bei Sicherheits- und Skalierbarkeitsproblemen schwierig, die sich erheblich auf alle Aspekte auswirken können, angefangen bei den Kosten bis hin zur Effizienz. Hier erfahren Sie mehr über diese Herausforderungen.

7 XDR vereinheitlicht die einzelnen Produkte, indem es ihre Protokolle integriert

Zur Verbesserung der Transparenz muss XDR relevante Verhaltenstelemetrie von Systemen und Anwendungen im gesamten Sicherheitsökosystem erhalten. Das ultimative Ziel ist es jedoch, die Erkennung von und Reaktion auf Bedrohungen in der gesamten Sicherheitsstruktur zu automatisieren und zu beschleunigen. Bei Syslog geht es nur um die Aufnahme von Protokollen, nicht um die Ermöglichung von Korrelation und Erkennung und noch weniger um autonome Reaktionen.

Für WatchGuard ist XDR ein moderner Cybersecurity-Ansatz, der für jedes Unternehmen zugänglich sein sollte. Alles beginnt mit unserer **Unified Security Platform**-Architektur – der Grundlage für den Aufbau und die Weiterentwicklung Ihres Sicherheitsökosystems, unterstützt durch die einzigartige **WatchGuard Sicherheit**. Daher stellt WatchGuard **ThreatSync** als produktübergreifende XDR-Funktion ohne zusätzliche Kosten zur Verfügung.

Weitere Informationen finden Sie unter watchguard.com/de

Deutschland, Österreich, Schweiz: +49 700 92229333 INTERNATIONALER VERTRIEB: +1 206 613 0895 WEB: www.watchguard.com/de

WatchGuard Technologies, Inc.