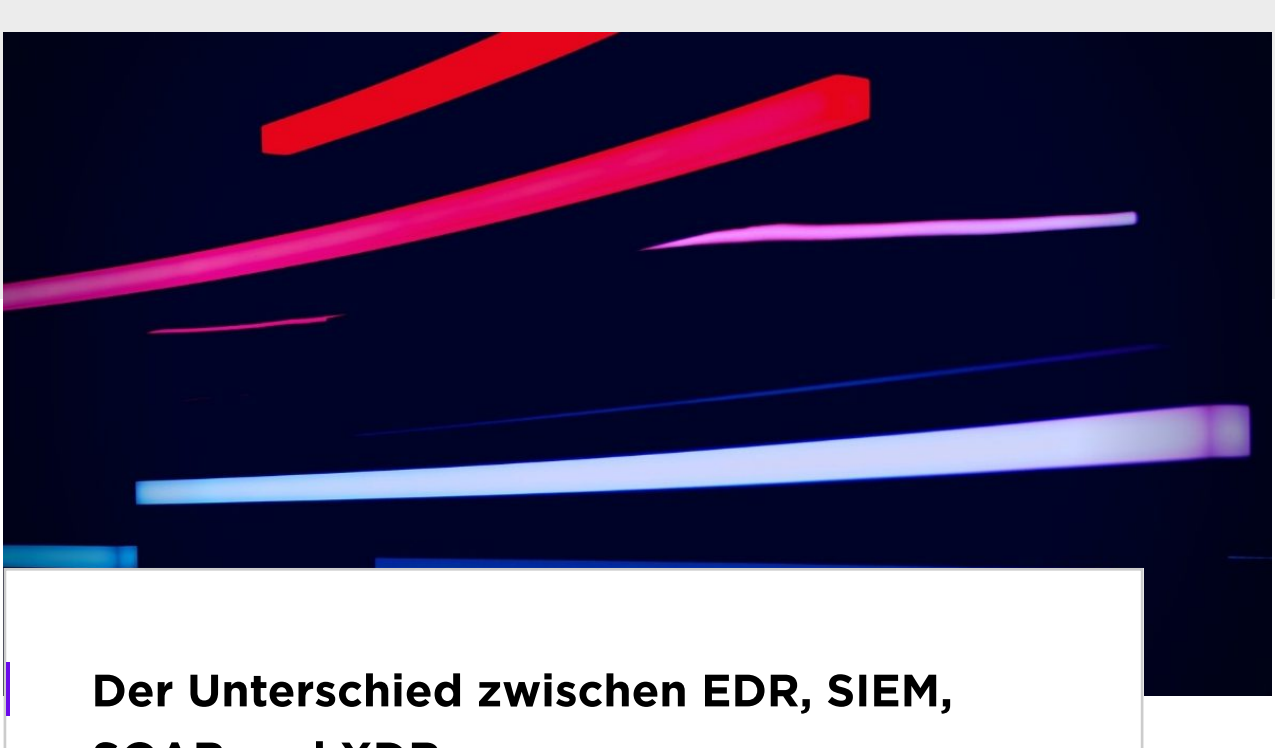

Der Unterschied zwischen EDR, SIEM, SOAR und XDR

Oktober 6, 2021
by Resha Chheda and Michael Leland

In der Cybersicherheitsbranche gibt es eine Fülle von Jargon, Abkürzungen und Akronymen. Da immer mehr ausgeklügelte Angriffsvektoren zur Verfügung stehen, von Endpunkten über Netzwerke bis hin zur Cloud, wenden sich viele Unternehmen einem neuen Ansatz zu, um fortschrittlichen Bedrohungen zu begegnen: Extended Detection and Response (Erweitertes Erkennen und Reagieren), was zu einem weiteren Akronym führt: XDR. Und obwohl XDR in diesem Jahr von Branchenführern und Analysten viel Aufmerksamkeit erhalten hat, handelt es sich dabei immer noch um ein sich entwickelndes Konzept, und als solches herrscht Verwirrung rund um das Thema.

- Was ist XDR?
- Wie unterscheidet sich XDR von EDR?
- Ist es dasselbe wie SIEM & SOAR?

Als führendes Unternehmen auf dem EDR-Markt und Pionier derder aufkommenden XDR-Technologie , werden wir oft gefragt, was diese Technologie bedeutet und wie sie letztendlich zu besseren Kundenergebnissen beitragen kann. Dieser Post soll einige häufig auftretenden Fragen rund um XDR und die Unterschiede zu EDR, SIEM und SOAR klären.

Was ist EDR?

EDR bietet einem Unternehmen die Möglichkeit, Endpunkte auf verdächtiges Verhalten zu überwachen und jede einzelne Aktivität und jedes Ereignis aufzuzeichnen. Dann setzt es Informationen in Beziehung, um wichtigen Kontext für die Erkennung von hochentwickelten Bedrohungen zu liefern. Schließlich führt es automatisierte Reaktionsmaßnahmen durch, wie die Isolierung eines infizierten Endpunkts vom Netzwerk in nahezu Echtzeit.

Was ist XDR?

XDR ist die Weiterwentwicklung von EDR, Endpoint Detection and Response. Anders als EDR, das Aktivitäten über mehrere Endpunkte hinweg sammelt und korreliert, erweitert XDR den Erkennungsbereich über die Endpunkte hinaus und bietet Erkennung, Analyse und Reaktion über Endpunkte, Netzwerke, Server, Cloud-Workloads, SIEM und vieles mehr.

Dies ermöglicht eine einheitliche Sicht über mehrere Tools und Angriffsvektoren hinweg. Diese verbesserte Sichtbarkeit bietet eine Kontextualisierung dieser Bedrohungen, um die Triage, Untersuchung und schnelle Abhilfemaßnahmen zu unterstützen.

XDR sammelt und verknüpft automatisch Daten über mehrere Sicherheitsvektoren hinweg und ermöglicht so eine schnellere Erkennung von Bedrohungen. Somit können Sicherheitsanalysten schnell reagieren, bevor sich die Bedrohung ausweitet. Sofort einsatzbereite Integrationen und vordefinierte Erkennungsmechanismen für verschiedene Produkte und Plattformen verbessern die Produktivität, Bedrohungserkennung und Forensik.

> Kurz gesagt, XDR *erweitert* über den Endpunkt hinaus, um Entscheidungen auf der Grundlage von Daten aus mehreren Produkten zu treffen, und kann Maßnahmen in ihrem gesamten Stack ergreifen, indem es auf E-Mail, Netzwerk, Identität und darüber hinaus reagiert.

Wie unterscheidet sich XDR von SIEM?

Wenn wir von XDR sprechen, denken manche Anwender, dass wir ein SIEM-Tool (Security Information & Event Management) auf eine andere Art und Weise beschreiben. Aber XDR und SIEM sind zwei verschiedene Dinge.

SIEM sammelt, aggregiert, analysiert und speichert große Mengen von Protokolldaten aus dem gesamten Unternehmen. SIEM begann seine Entwicklung mit einem sehr breit gefächerten Ansatz: dem Sammeln von verfügbaren Protokoll- und Ereignisdaten aus nahezu jeder Quelle im Unternehmen, um sie für verschiedene Anwendungsfälle zu speichern. Dazu gehören Governance und Compliance, regelbasierter Musterabgleich, heuristische/verhaltensbasierte Bedrohungserkennung wie UEBA und die Suche nach IOCs oder atomaren Indikatoren in Telemetriequellen.

SIEM-Tools erfordern jedoch viel Feinabstimmung und Aufwand bei der Implementierung. Sicherheitsteams können auch von der schieren Anzahl der Warnmeldungen, die von einem SIEM kommen, überfordert werden, was dazu führt, dass das SOC kritische Warnmeldungen ignoriert. Darüber hinaus ist ein SIEM, auch wenn es Daten aus Dutzenden von Quellen und Sensoren erfasst, immer noch ein passives Analysetool, das Warnmeldungen ausgibt.

Die XDR-Plattform zielt darauf ab, die Herausforderungen des SIEM-Tools für eine effektive Erkennung und Reaktion auf gezielte Angriffe zu lösen und umfasst Verhaltensanalyse, Bedrohungsdaten, Verhaltensanalysen und Analysen.

Wie unterscheidet sich XDR von SOAR?

SOAR-Plattformen (Security Orchestration & Automated Response) werden von ausgereiften Sicherheitsteams verwendet, um mehrstufige Playbooks zu erstellen und auszuführen, die Aktionen über ein API-verbundenes Ökosystem von Sicherheitslösungen automatisieren. Im Gegensatz dazu wird XDR die Integration von Ökosystemen überMarketplace ermöglichen und Mechanismen zur Automatisierung einfacher Aktionen gegen Sicherheitskontrollen von Drittanbietern bereitstellen.

SOAR ist komplex, kostspielig und erfordert ein sehr ausgereiftes SOC zur Implementierung und Pflege von Partnerintegrationen und Playbooks. XDR ist als „SOAR-lite“ gedacht: eine einfache, intuitive Zero-Code-Lösung, die von der XDR-Plattform aus mit angeschlossenen Sicherheitstools agieren kann.

Was ist MXDR?

Managed Extended Detection and Response (MXDR) erweitert die MDR-Dienste auf das gesamte Unternehmen, um eine vollständig verwaltete Lösung zu erhalten, die Sicherheitsanalysen und -abläufe, fortschrittliche Bedrohungssuche, Erkennung und schnelle Reaktion in Endpunkt-, Netzwerk- und Cloud-Umgebungen umfasst.

Ein MXDR-Dienst erweitert die XDR-Funktionen des Kunden um MDR-Dienste für zusätzliche Überwachungs-, Untersuchungs-, Bedrohungsjagd- und Reaktionsmöglichkeiten.

Warum gewinnt XDR an Attraktivität und sorgt für Aufsehen?

XDR ersetzt isolierte Sicherheitslösungen und hilft Unternehmen, die Herausforderungen der Cybersicherheit von einem einheitlichen Standpunkt aus anzugehen. Mit einem einzigen Pool von Rohdaten, der Informationen aus dem gesamten Ökosystem umfasst, ermöglicht XDR eine schnellere, tiefgreifendere und effektivere Erkennung von und Reaktion auf Bedrohungen als EDR, da Daten aus einer größeren Anzahl von Quellen gesammelt und zusammengestellt werden.

XDR sorgt für mehr Transparenz und Kontext bei Bedrohungen. Vorfälle, die sonst nicht erkannt worden wären, tauchen auf einer höheren Bewusstseinsebene auf, so dass Sicherheitsteams Abhilfemaßnahmen ergreifen und weitere Auswirkungen reduzieren sowie das Ausmaß des Angriffs minimieren können.

Ein typischer Ransomware-Angriff durchquert das Netzwerk, landet in einem E-Mail-Posteingang und greift dann den Endpunkt an. Wenn man die einzelnen Sicherheitsaspekte unabhängig voneinander betrachtet, sind die Unternehmen im Nachteil. XDR integriert unterschiedliche Sicherheitskontrollen, um automatisierte oder Ein-Klick-Reaktionsmaßnahmen im gesamten Sicherheitsbereich des Unternehmens zu ermöglichen, wie z. B. die Sperrung des Benutzerzugriffs, die Erzwingung der Multi-Faktor-Authentifizierung bei vermuteter Kontokompromittierung, die Sperrung eingehender Domänen und Datei-Hashes und vieles mehr – alles übervom Benutzer geschriebene Regeln oder über die in die Prescriptive Response Engine integrierte Logik.

Mit einem einzigen Pool von Rohdaten, der Informationen aus dem gesamten Ökosystem umfasst, ermöglicht XDR eine schnellere, tiefgreifendere und effektivere Erkennung von und Reaktion auf Bedrohungen als EDR, da Daten aus einer größeren Anzahl von Quellen gesammelt und zusammengestellt werden.

Diese umfassende Sichtbarkeit bringt mehrere Vorteile mit sich, darunter:

- Verkürzung der Mean Time to Detect (MTTD) durch Korrelation zwischen verschiedenen Datenquellen.
- Verkürzung der mittleren Untersuchungszeit (MTTI) durch Beschleunigung der Triage und Verkürzung der Zeit für die Untersuchung und den Umfang.
- Verkürzung der mittleren Reaktionszeit (MTTR) durch einfache, schnelle und relevante Automatisierung.
- Verbesserung der Transparenz im gesamten Sicherheitsbereich.

Darüber hinaus trägt XDR dank KI und Automatisierung dazu bei, den manuellen Arbeitsaufwand von Sicherheitsanalysten zu verringern. Eine XDR-Lösung kann proaktiv und schnell hochentwickelte Bedrohungen aufspüren, die Produktivität des Sicherheits- oder SOC-Teams erhöhen und dem Unternehmen einen massiven ROI-Schub verschaffen.

Abschließende Gedanken

Für viele Unternehmen ist es eine Herausforderung, sich in der Anbieterlandschaft zurechtzufinden, insbesondere wenn es um Erkennungs- und Reaktionslösungen geht. Oft besteht die größte Hürde darin zu verstehen, was die einzelnen Lösungen bieten, vor allem, wenn die Terminologie von Anbieter zu Anbieter unterschiedlich ist und verschiedene Dinge bedeuten kann.

Wie bei jeder neuen Technologie, die auf den Markt kommt, gibt es eine Menge Hype, und Käufer müssen vorsichtig sein. Tatsache ist, dass nicht alle XDR-Lösungen gleich sind. SentinelOne Singularity XDR vereinheitlicht und erweitert die Erkennungs- und Reaktionsfähigkeit über mehrere Sicherheitsebenen hinweg und bietet Sicherheitsteams eine zentralisierte End-to-End-Unternehmenstransparenz, leistungsstarke Analysen und automatisierte Reaktionen über den gesamten Technologiebereich hinweg.

Wenn Sie mehr über die SentinelOne Singularity Platform erfahren möchten, kontaktieren Sie uns oder fordern Sie eine kostenlose Demoan.

Like this article? Follow us on LinkedIn, Twitter, YouTube or Facebook to see the content we post.

Read more about Cyber Security