Extended Detection and Response (XDR) – Beginner's Guide

SOPHOS
Cybersecurity evolved.

Was ist XDR?

Eine einheitliche Definition zu XDR gibt es nicht. Je nachdem, wen man fragt, erhält man unterschiedliche Antworten.

- Für die meisten Analystenhäuser und Cybersecurity-Anbieter steht XDR für **Extended Detection and Response**. „Extended" bezieht sich darauf, dass XDR über die Endpoint- und Server-Ebene hinausgeht und zusätzliche Datenquellen wie Firewalls, E-Mails, Cloud und Mobilgeräte berücksichtigt.
- Eine weitere Interpretation lautet, dass das „X" für **„Cross-Product"-Erkennung und -Reaktion** steht, weil Daten aus mehreren Produkten oder Schutzschichten kombiniert werden.
- Das „X" kann aber auch als eine Art mathematische Variable betrachtet werden, die für alle Datenquellen steht, die Sie zur Lösung der Aufgabe in die Gleichung aufnehmen können.

Alle drei Definitionen beziehen sich jedoch auf dieselben Kernfunktionen. Das heißt, XDR ermöglicht es, auf unterschiedliche Datenquellen zuzugreifen und diese abzufragen, um unternehmensweit für mehr Transparenz und Kontext zu sorgen.

Was kann XDR?

XDR bietet Unternehmen einen ganzheitlichen Überblick über ihren Cybersecurity-Status und ihre IT-Umgebung. Auch Detail-Informationen lassen sich schnell abrufen, um bei Bedarf tiefer gehende Analysen zu erstellen

Gartner über XDR:

„Zu den wichtigsten Leistungsversprechen einer XDR-Lösung zählen Produktivitätssteigerungen in IT-Security-Abteilungen sowie bessere „Detection and Response"-Funktionen, die durch die Integration unterschiedlicher Security-Komponenten, die eine Einheit bilden, erzielt werden. Eine integrierte Lösung muss mehrere Telemetriedatenströme umfassen und sowohl Optionen für unterschiedliche Erkennungsarten als auch unterschiedliche Reaktionsoptionen bieten."

Gartner, „Innovation Insight for Extended Detection and Response" (2020)

Eine häufig gestellte Frage lautet: „Wie unterscheidet sich XDR von EDR?" Tatsächlich sollten XDR-Lösungen die geschäftskritischen Funktionen umfassen, die EDR (Endpoint Detection and Response) zur Beantwortung spezifischer Fragen bietet. Das bedeutet, dass Live-Daten direkt von einem Endpoint oder Server abgerufen werden können und auf Cloud-Daten zugegriffen werden kann, wenn ein Gerät offline ist.

XDR baut auf dieser soliden Grundlage auf, fügt jedoch noch mehr Daten und Kontext hinzu. So wird die Transparenz erhöht und der Benutzer erhält bei Analysen detailliertere Informationen. Das Ergebnis: eine schnellere und zuverlässigere Incident Detection and Reponse. Diese zusätzlichen Datenquellen können Firewall-, E-Mail-, Cloud-Informationen und Daten von Mobilgeräten umfassen. So ermöglichen beispielsweise Firewall-Daten, schädlichen Datenverkehr mit einem kompromittierten Endpoint zu korrelieren. Oder Sie können sehen, welche Anwendung die Netzwerkverbindung des Büros verlangsamt.

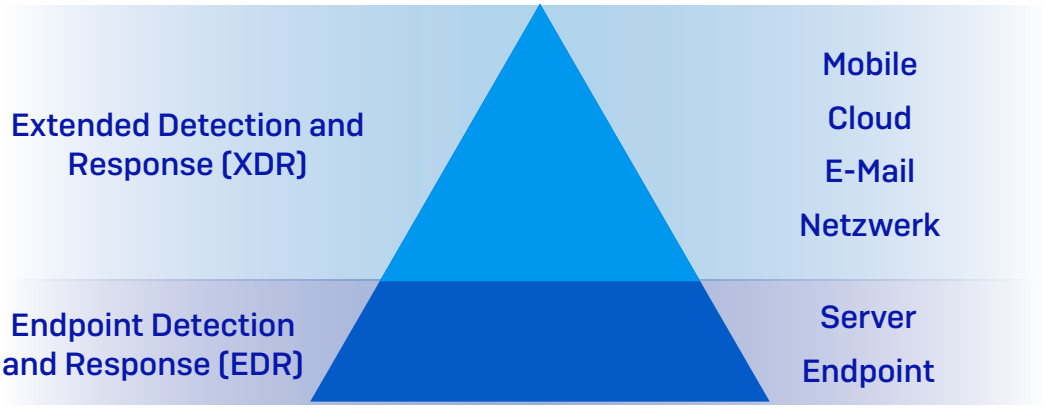
Als besonders effektiv erweist sich das „Makro"-Spotlight. Über diese XDR-Funktion erhalten Sie die passenden Tools, um Ihre gesamte Umgebung zu scannen und verdächtige Aktivitäten, anomales Verhalten sowie weitere IT-Probleme aufzudecken. Wird ein Problem erkannt, können Sie sich gezielt mit einem bestimmten Gerät befassen, Live-Daten abrufen oder remote auf das Gerät zugreifen, um noch detailliertere Informationen einzusehen und Maßnahmen zur Bereinigung zu ergreifen.

Mehr Datenquellen

So leistungsstark EDR-Tools auch sind: Sie beschränken sich auf die Erkennung und Reaktion auf Endpoint- und Server-Ebene. Das ist nicht grundsätzlich verkehrt: Wenn Sie sich zur Erkennung und Reaktion für einen Ort entscheiden müssten, wären Endpoints und Server eine gute Wahl.

Jedoch bleiben bestimmte Punkte außen vor, wenn Sie sich ausschließlich auf diese konzentrieren. Schließlich ist Ihre IT-Umgebung ein verbundenes System aus Netzwerken, Kommunikationstools, Mobilgeräten, Cloud-Anwendungen und vielem mehr. Um Ihre IT-Infrastruktur umfassender zu schützen, ist ein integriertes Erkennungs- und Reaktionssystem von entscheidender Bedeutung. Hier kommt XDR ins Spiel.

XDR entwickelt die Idee von EDR weiter. Statt sich nur auf Endpoints und Server zu konzentrieren, werden auch Daten von anderen Sicherheitstools wie Firewalls, E-Mail-Gateways, Public-Cloud-Tools und Mobile-Threat-Management-Lösungen integriert. XDR ist eine neue Technologie, die noch in den Kinderschuhen steckt. Die Datenquellen und Funktionen unterscheiden sich daher von Anbieter zu Anbieter. Die folgende Abbildung gibt jedoch einen allgemeinen Überblick darüber, welche zusätzlichen Funktionen XDR im Vergleich zu EDR bietet.



XDR-Anwendungsfälle

Die Vorteile von XDR in der Praxis lassen sich am besten anhand der Funktionen aufzeigen, die IT-Teams bei der Erledigung ihrer täglichen IT-Operations- und Threat-Hunting-Aufgaben unterstützen. Hierzu haben wir auch EDR-Beispiele angeführt, da Ihre XDR-Lösung auch diese Anwendungsfälle abdecken sollte.

	IT Operations	Threat Hunting
EDR	• Warum läuft ein System langsam? • Welche Geräte verfügen über bekannte Schwachstellen, unbekannte Dienste oder nicht autorisierte Browser-Erweiterungen? • Werden Programme ausgeführt, die entfernt werden sollten?	• Welche Prozesse versuchen, eine Netzwerkverbindung über Nicht-Standardports herzustellen? • Prozesse anzeigen, die kürzlich Dateien oder Registry-Schlüssel geändert haben • Erkannte Kompromittierungs-Indikatoren mit Zuordnungen zum MITRE ATT&CK Framework auflisten
XDR	• Nicht verwaltete, Gast- und IoT-Geräte erkennen • Warum ist die Netzwerkverbindung des Büros langsam? Welche Anwendung ist dafür verantwortlich? • Verlaufsdaten auf verloren gegangenen oder zerstörten Geräten auf ungewöhnliche Aktivitäten innerhalb der letzten 30 Tage prüfen	• Analyse auf 30 Tage ausweiten, ohne dass das betroffene Gerät wieder online gehen muss • Analyse verdächtiger Hosts mithilfe von ATP- und IPS-Erkennungen der Firewall • E-Mail-Header-Informationen, SHAs und andere IoCs vergleichen, um Datenverkehr zu einer schädlichen Domäne zu identifizieren

Wie Sophos helfen kann

Sophos XDR bietet Unternehmen einen ganzheitlichen Überblick über ihre gesamte Cybersecurity-Umgebung mit der Möglichkeit, bei Bedarf Detail-Informationen abzurufen. Das heißt, Sie erhalten sowohl eine übergreifende Ansicht aus Vogelperspektive, als auch spezifische Detail-Informationen, falls erforderlich.

XDR-fähige Lösungen senden Daten von Endpoints, Servern, Firewalls und E-Mail-Gateways sowie Informationen aus weiteren Datenquellen* an den Sophos Data Lake, ein Cloud-Repository für kritische XDR- und Offline-Gerätedaten. Alle wichtigen Daten befinden sich damit an einem zentralen Ort, sodass Sie schnell geschäftskritische Fragen beantworten, Ereignisse aus verschiedenen Datenquellen korrelieren und noch besser gezielte Maßnahmen ergreifen können.

Dank einer Library mit vorformulierten, individuell anpassbaren Abfragen können Sie gleich loslegen. Wählen Sie einfach eine Kategorie, fügen Sie Geräte hinzu und beantworten Sie alle Fragen rund um IT-Security und Threat Hunting.

Gartner Innovation Insight for Extended Detection and Response, Peter Firstbrook, Craig Lawson, 19. März 2020.

Gartner befürwortet in seinen Forschungsbeiträgen keine bestimmten Hersteller, Produkte oder Dienstleistungen und rät Technologie-Nutzern nicht ausschließlich zu Anbietern mit besten Bewertungen. Forschungsbeiträge von Gartner sind als Meinungsäußerungen des Gartner Forschungsinstituts einzustufen und in keinem Fall als Tatsachenfeststellung zu werten. Gartner übernimmt keinerlei Gewähr für die vorliegenden Forschungsergebnisse und schließt jegliche Mängelgewährleistung oder Zusicherung der erforderlichen Gebrauchstauglichkeit aus.

* Cloud Optix und Sophos Mobile in Kürze verfügbar

Weitere Infos unter
www.sophos.de/xdr

SOPHOS

21-04-06 WP (NP)