G DATA CyberDefense

Extended Detection and Response (XDR): ja, nein, vielleicht?

Whitepaper

Extended Detection and Response (XDR): ja, nein, vielleicht?

Whitepaper

Was ist eigentlich eine XDR-Lösung? Welche Vorteile bringt sie? Das fragen sich viele Unternehmen – und treffen auf einen Begriffsdschungel, von EDR bis MXDR. Das macht die Beurteilung nicht gerade leichter.

Dieses Paper definiert klar, was ein XDR-System ausmacht. Erfahren Sie, wie XDR funktioniert, was es von Antiviren-Software und EDR unterscheidet und für wen XDR als Managed Service sinnvoll ist.

Inhaltsverzeichnis

Was ist Extended Detection and Response (XDR)?

Extended Detection and Response (XDR) bezeichnet eine Software-Lösung, die Unternehmen dabei hilft:

- **Cyberbedrohungen zu erkennen**, die präventive Abwehrmaßnahmen überwinden konnten **(Detect – das „D“ in XDR)**
- und mit **Gegenmaßnahmen** darauf zu reagieren **(Respond – das „R“ in XDR).**

Dazu überwacht und analysiert XDR kontinuierlich die Aktivitäten in den IT-Systemen. Sobald die XDR Software eine verdächtige Aktivität erkennt, reagiert sie automatisch und/oder alarmiert das IT-Team. Hier sollten professionelle Analyst*innen arbeiten, da die Auswertung der Meldungen und Prüfung des Kontextes IT-Security-Fachkenntnisse erfordert. Stellt sich die Aktivität als bösartig heraus, greift das Team sofort ein, um den Angriff zu stoppen.

XDR ist die Weiterentwicklung von Endpoint Detection and Response (EDR). EDR sendet zwar auch Daten an eine Plattform, aber analysiert diese nur isoliert pro einzelnen Endpoint. XDR hingegen setzt diese Daten miteinander in Beziehung. Diese Korrelation erlaubt wertvolle Rückschlüsse darauf, was im Netzwerk passiert.

Welche Aktivitäten überwacht XDR?

Um verdächtiges Verhalten zu erkennen, überwacht XDR Aktivitäten und Ereignisse wie:

- Starten oder Beenden von Prozessen
- Erstellen oder Löschen von Dateien
- Zugriffe auf die Windows-Registry
- Event Logs des Betriebssystems
- Ereignisverfolgung für Windows (ETW)
- Software-Installation oder -Deinstallation
- Benutzeranmeldung, -abmeldung oder -erstellung

Wie funktioniert XDR?

1 Überwachung der Aktivitäten:

Um XDR zu nutzen, wird auf Endgeräten wie PCs und Servern jeweils ein Software-Agent installiert. Dieser erfasst in Echtzeit die Aktivitäten und Ereignisse auf den Geräten.

2 Übertragung an XDR-Plattform:

Die Software-Agenten schicken die erfassten Daten zur Analyse an eine Cloud-basierte oder lokale XDR-Plattform, die der Hersteller zur Verfügung stellt.

3 Korrelation und Analyse der Daten:

Die XDR-Plattform korreliert und analysiert die Daten, um verdächtiges Verhalten festzustellen. Durch Machine Learning lernt das System stetig dazu, wie der normale Betrieb aussieht und was verdächtig ist.

4 Reaktion auf verdächtige Aktivitäten:

Sobald die XDR-Plattform etwas als verdächtig einstuft, löst sie einen Alarm bei den Analyst*innen aus. Diese nehmen eine genaue Analyse vor und greifen bei Bedarf sofort ein, um den Vorfall zu beheben. Je nach Fall kann die XDR-Plattform auch direkt automatisiert reagieren, um zum Beispiel einen PC vom Netzwerk zu isolieren.

5 Speicherung für künftige Erkennung:

Nach jeder manuellen Analyse werden die gewonnenen Erkenntnisse gespeichert. So können künftige Bedrohungen noch effizienter erkannt und gestoppt werden.

Warum XDR statt Antiviren-Software?

Die klassische Antiviren-Software versucht, Cyberangriffe durch präventive Schutztechnologien direkt abzuwehren. Das Ziel von XDR ist es hingegen, die Angriffe zu entdecken, die von den präventiven Schutztechnologien nicht abgewehrt werden konnten. Dazu setzt XDR zusätzliche Sensoren ein, um eine umfassende Analyse zu erlauben (Detect). XDR bietet außerdem die Möglichkeit, mit Gegenmaßnahmen zu reagieren (Respond).

XDR als Bank: Diebe erkennen und stoppen

Um den Mehrwert von XDR zu verdeutlichen, stellen wir uns einmal eine Bank vor:

Prevent:

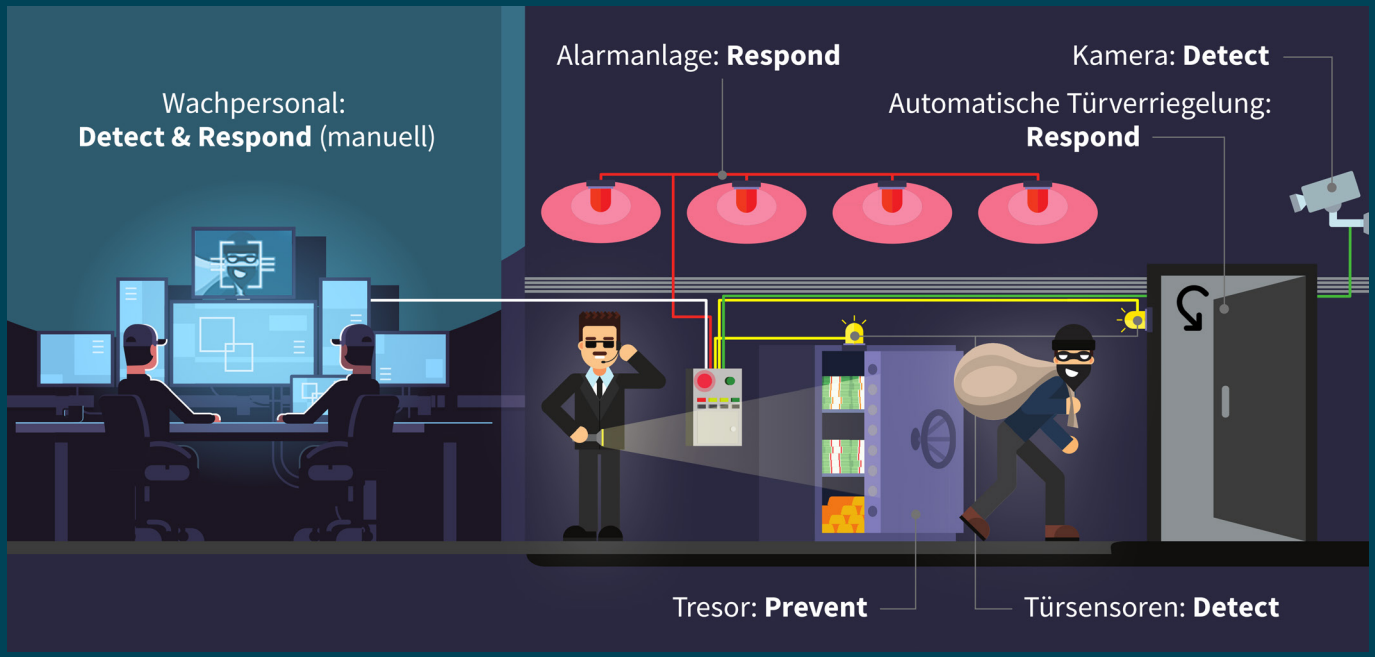
Als präventive Schutzmaßnahme liegt das Geld in einem Tresor. Lässt man jedoch einen gut ausgestatteten Dieb lange genug mit dem Tresor allein, ohne dass er Angst haben muss, entdeckt zu werden, wird er ihn irgendwann öffnen. Genauso verhält es sich mit aktiven Angreifenden, die AV-Software umgehen möchten.

Detect:

Um den Dieb immerhin zu entdecken, nachdem er den Tresor öffnen konnte, installieren wir Kameras. Außerdem bringen wir Türsensoren an, die bemerken, wenn jemand um 1 Uhr nachts die Eingangstür oder Tresortür öffnet. Solche Sensoren enthalten auch XDR-Lösungen – zusätzlich zu den präventiven Schutztechnologien.

Respond:

Wir setzen zudem eine Alarmanlage, eine automatische Türverriegelung sowie Wachpersonal ein. Die Wache reagiert auf Meldungen der Kameras und Sensoren. Sie prüft, ob bei einem Alarm tatsächlich ein Dieb durch den Raum gelaufen ist – und kann ihn sofort stellen. Analog dazu sind es bei XDR die Analyst*innen, die Vorfälle prüfen und darauf reagieren.



XDR vs. Endpoint Protection

Im Vergleich zur klassischen Antiviren-Software enthalten moderne Sicherheitslösungen wie Endpoint Protection oder Next-Gen-AV gelegentlich bereits Funktionen, um Gefahren anhand des Verhaltens zu erkennen. Das heißt, sie haben gewisse XDR-Anteile im Bereich der Erkennung (Detect).

Was jedoch der große Unterschied ist: XDR setzt eine deutlich erweiterte Sensorik zur Erkennung ein, die einem Analysten-Team vorgelegt wird.

Endpoint Protection und Next-Gen-AV hingegen erlauben keinen interaktiven Zugriff auf das System, um den Vorfall umfassend zu analysieren und auf der Basis manuell zu reagieren (Respond).

Genau das ist der entscheidende Vorteil von XDR.

Beispiel: Wie XDR auf Cyberangriffe reagiert

Nehmen wir als Beispiel an: Die XDR-Sensoren entdecken einen Prozess, der die Passwörter ausliest und einen unbekannten Server kontaktiert. Der Prozess schreibt sich selbst in den Autostart, sodass er bei jedem Neustart direkt wieder geladen wird. Das sieht verdächtig aus.

Das passiert in diesem Fall:

- Der betroffene PC wird automatisch vom Netz isoliert, um eine Ausbreitung zu verhindern.
- Die Analyst*innen untersuchen, ob eine echte Gefahr vorliegt, da auch IT-Admins legitim Passwörter auslesen könnten. Ihr Ergebnis: Es greift jemand an.
- Die Analyst*innen entfernen daher die Autostart-Einträge.
- Sie benachrichtigen die IT-Admins, dass neue Passwörter vergeben werden müssen.

Warum XDR als Managed Service?

Der sinnvolle Einsatz eines XDR erfordert „Wachpersonal“, das verdächtige Prozesse näher untersucht und bei Bedarf einschreitet. Im Idealfall sind diese Fachkräfte im Unternehmen direkt angestellt, denn internes Personal kennt das Netzwerk am besten. Doch das ist nicht immer möglich.

Notwendiger Schichtbetrieb:

Für einen echten Sicherheitsgewinn sollte das „Wachpersonal“ 24/7 im Schichtbetrieb arbeiten. Denn Cyberkriminelle schlagen auch um 1 Uhr nachts, am Wochenende oder an Feiertagen zu. Wenn dann niemand den Alarm untersuchen und darauf reagieren kann, bleibt der Mehrwert von XDR vollständig aus. Angesichts begrenzter Mittel ist ein Schichtbetrieb für viele Unternehmen jedoch nur schwer umsetzbar.

Fehlende Zeit und Fachkräfte:

Es erfordert außerdem sehr hohe Fachkenntnisse und genug Zeit, um die XDR-Meldungen zu analysieren und richtig darauf zu reagieren. Das können viele IT-Teams aufgrund von Fachkräftemangel und hohem Workload nicht leisten. Meist reicht die Zeit schon nicht, um regelmäßig die Meldungen der Endpoint Protection auszuwerten – wenn gleichzeitig ein Kollege Hilfe bei einem Software-Problem braucht und schon das nächste Ticket wartet. Für die noch größere Anzahl an komplexen XDR-Meldungen sind daher professionelle Security-Analyst*innen nötig, die sich nur darauf konzentrieren.

Alarmmüdigkeit:

Der Zeitmangel begünstigt auch die sogenannte „Alert fatigue“ – ein oft unterschätztes Sicherheitsrisiko. Die Warnungen, mit denen IT-Teams täglich konfrontiert werden, stellen sich oftmals als Fehlalarme heraus. Das kann dazu führen, dass ohnehin schon überlastete Teams Hinweise auf echte Angriffe übersehen oder ignorieren. Dadurch kann keine zeitnahe Reaktion erfolgen, was die IT-Sicherheit des Unternehmens gefährdet.

Deshalb kann es eine gute Lösung sein, die Aufgabe des „Wachpersonals“ in die Hände eines spezialisierten Dienstleistungsunternehmens zu geben. In dem Fall spricht man von Managed XDR oder MXDR. Alternativ werden die Begriffe Managed Detection and Response (MDR) oder Managed Threat Response (MTR) verwendet.

Tipp: Achten Sie bei der Recherche genau darauf, was Sie miteinander vergleichen. XDR umfasst nur die Software-Komponenten. Das heißt, Ihr IT-Team muss selbst 24/7 die Meldungen analysieren und darauf reagieren. Bei Managed XDR übernimmt dies komplett ein spezialisiertes Dienstleistungsunternehmen für Sie.

Mit Managed XDR die NIS-2-Richtlinie umsetzen

Managed XDR hilft Unternehmen außerdem, die neue NIS-2-Richtlinie der EU umzusetzen. Mit NIS-2 gelten ab Oktober 2024 für viele Unternehmen und Organisationen in 18 Sektoren verpflichtende IT-Sicherheitsmaßnahmen.

Dazu zählt, dass sie Maßnahmen zur Erkennung, Analyse und Reaktion auf Sicherheitsvorfälle umsetzen müssen. Bei Verstößen drohen hohe Geldstrafen.

Mythos: “XDR kann auch voll automatisiert ohne Analyst*innen funktionieren.”

Es ist ein großer Irrtum anzunehmen, dass XDR dank maschinellem Lernen auf alle Sicherheitsvorfälle automatisiert richtig reagieren kann. Es gibt zwar eindeutige Fälle, in denen eine automatisierte Response ausreicht. Aber in vielen Fällen ist eine tiefergehende, manuelle Analyse durch Fachleute nötig.

Sie können mit ihrer Expertise entscheiden, ob verdächtiges Verhalten tatsächlich eine Gefahr ist – und wie diese nachhaltig beseitigt wird.

Vorteile von Managed XDR im Vergleich zum selbst betreuten XDR

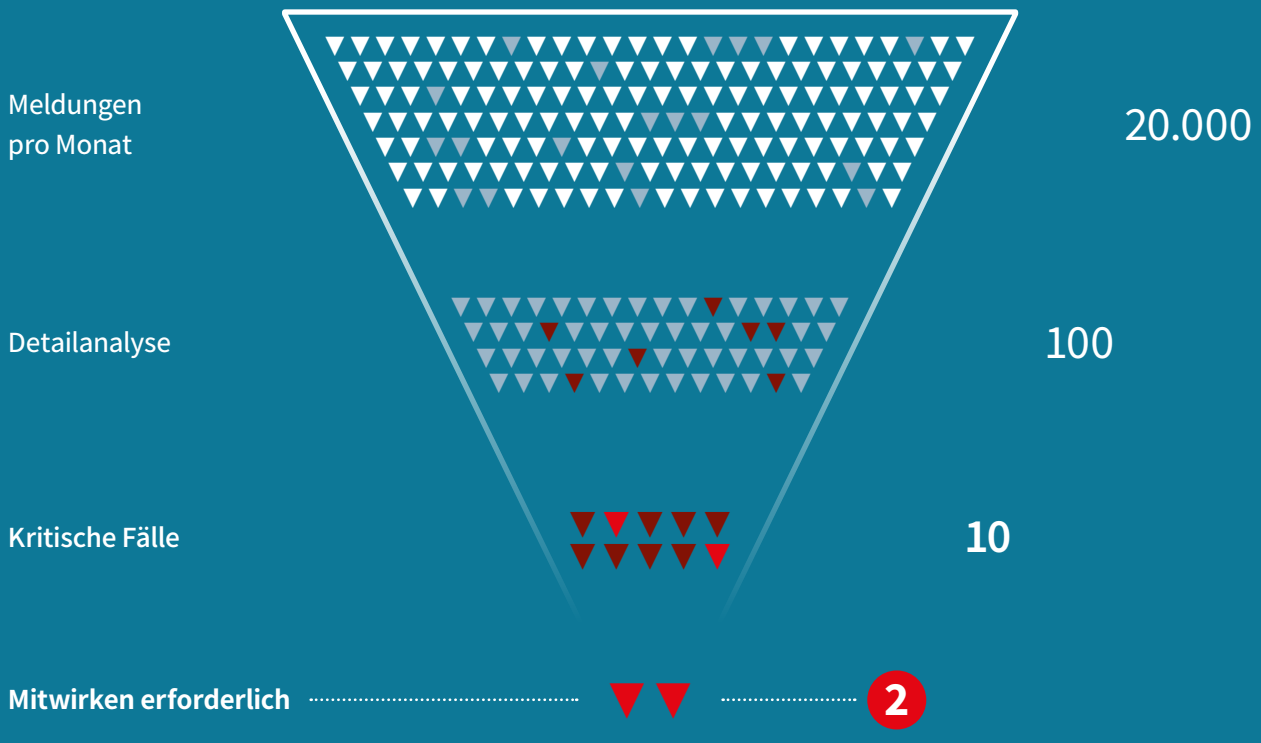
24/7-Expertenschutz

Die Sicherheitsanalyst*innen eines Managed-XDR-Anbieters sind rund um die Uhr im Einsatz. Für Sie ist es, als hätte Ihr Unternehmen ein Security-Team, das immer verfügbar ist und weder durch Urlaub noch Krankheit ausfällt. Sie haben somit die beruhigende Gewissheit, dass Fachleute Ihre IT Security immer im Blick haben.

Freie Ressourcen im IT-Team

Die Analyst*innen nehmen Ihnen die gesamte Arbeit der Angriffserkennung und -abwehr ab: Sie analysieren verdächtige Vorgänge im Detail und sperren Angreifende in kritischen Fällen wieder aus. Dadurch ist nur noch in sehr wenigen Fällen Ihr Mitwirken erforderlich. Ihr IT-Team kann sich somit auf andere wichtige Projekte konzentrieren.

Starke Entlastung Ihres Teams



Mehr Sicherheit dank externer Expertise

Sie holen sich IT-Security-Expertise als Service ins Unternehmen. Im Gegensatz zum eigenen IT-Team kümmern sich die Analyst*innen ständig um verschiedenste Angriffe bei einer Vielzahl von Kunden. Diese Erfahrung können sich interne IT-Teams kaum aneignen. Die Analyst*innen verfügen zudem über nicht-öffentliches Fachwissen, mit dem sie auch neueste Angriffsarten erkennen – und das für eigene IT-Teams nur schwer zugänglich ist.

Dazu zählt zum Beispiel Wissen aus:

- Austausch mit weltweiter Cybercrime-Research-Community
- Erfahrungen aus IT-Notfall-Einsätzen
- regelmäßiger Zusammenarbeit mit Strafverfolgungsbehörden

Kostenersparnis

Sie erhöhen Ihre IT-Sicherheit, ohne zusätzliches Fachpersonal zu suchen und anzustellen. Für einen eigenen Schichtbetrieb sind mindestens acht Analyst*innen nötig, um Wochenenden, Feiertage, Urlaub und Krankheit abzudecken. Hinzu kommen 1-2 Führungskräfte sowie die XDR Software und Threat Intelligence Databases.

Managed XDR ist dagegen eine günstigere und zeitsparende Option.

G DATA: Managed XDR aus Deutschland

Als erfahrener IT-Sicherheitsspezialist aus Deutschland stehen wir Ihnen mit G DATA 365 | MXDR zur Seite: Unsere Analyst*innen überwachen Ihre IT-Systeme – rund um die Uhr, an 365 Tagen im Jahr. Wir erkennen, analysieren und reagieren für Sie auf Angriffe, bevor sie Schaden anrichten. Bei akuten Vorfällen rufen wir Sie direkt an.

G DATA Managed XDR ist eine gute Wahl für alle, die besonderen Wert auf Datenschutz und persönliche Betreuung legen.

Über G DATA:

- IT-Sicherheitsspezialist mit Hauptsitz in Bochum, Deutschland
- Fast 40 Jahre Erfahrung in der Erforschung und Abwehr von Cybergefahren
- Umfassende Cyber Defense für Privatanwender und Unternehmen
- Services von Managed XDR über Penetrationtests bis Incident Response
- G DATA Advanced Analytics GmbH ist BSI-qualifizierter APT-Response-Dienstleister

SecurITy made in Germany

Ihre Vorteile mit Managed XDR „Made in Germany“:

Höchster Datenschutz

Als deutsches Unternehmen sind wir den strengen deutschen Datenschutzgesetzen verpflichtet. Unsere Analyst*innen sehen Daten nur in Verdachtsfällen ein und nur, soweit Sie es uns beim Onboarding gestatten.

Datenhaltung in Deutschland

Die Datenhaltung erfolgt ausschließlich auf Servern in Deutschland: an unserem Hauptsitz in Bochum sowie auf den Servern unseres Partners, des deutschen Cloud-Anbieters IONOS, in Frankfurt und Berlin.

Prämierter 24/7-Support aus Deutschland

Bei jeglichen Fragen ist unser deutschsprachiger Support am Hauptsitz telefonisch für Sie da. Rund um die Uhr. Komplett kostenfrei. Wir nehmen uns immer Zeit für Sie – und zwar die Zeit, die es braucht.

Kontrolle behalten

Legen Sie mit uns gemeinsam fest, welche Geräte, Prozesse oder Dateien wir zwar prüfen, auf denen wir aber keine Reaktion vornehmen sollen. Oder welche wir gar nicht einsehen müssen.

Alles im Blick

In Ihrer Webkonsole sehen Sie in Echtzeit, welche Vorfälle es gab, was wir für Sie getan haben und ob Handlungsempfehlungen für Sie vorliegen. Diese sind klar verständlich und leicht umzusetzen.

Eigene XDR-Technologie aus Deutschland

Wir entwickeln die XDR Software komplett selbst – ebenfalls in Deutschland. So wissen wir genau, wie Alarme zu verstehen sind und können richtig reagieren. Als Träger des Siegels „IT Security Made in Germany“ haben wir uns verpflichtet, Lösungen ohne Hintertüren zu entwickeln.

Das sagen unsere Kunden

„Der Standort von G DATA hier in Deutschland ist für uns von zentraler Bedeutung. Der Hersteller sitzt in Reichweite und ich habe einen guten Draht dorthin und kann mir im Fall von Problemen und Fragen direkte Unterstützung holen.“

Thomas Rüby

IT-Leiter | Landratsamt Dachau

„Für uns war wichtig, dass der Anbieter in Deutschland sitzt und auch Support in deutscher Sprache anbietet. Einmal wegen des Datenschutzes, aber auch, weil bei einem so wichtigen Thema keine sprachlichen Barrieren bestehen sollten.“

Heiko Streichert

IT-Administrator | etna GmbH

Testsieger 2023 im Umgang mit Kundendaten

Wie vertrauenswürdig sind IT-Sicherheitsunternehmen? Welche Informationen gewinnen sie mit ihrer Software, wie und wo werden die Daten gespeichert und welche Drittanbieter haben Zugang? Das haben Connect und AV-Comparatives genau untersucht.

Ergebnis: G DATA ist das vertrauenswürdigste Unternehmen und wird daher als Testsieger ausgezeichnet.

Mehr Informationen unter gdata.de/mxdr