N-ABLE | XDR vs. MDR:

# Wählen Sie die beste Lösung für Ihr Unternehmen

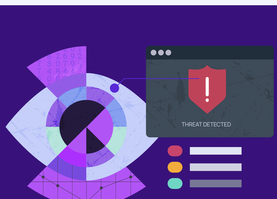
Unternehmen sehen sich zunehmenden Cyberbedrohungen und regulatorischen Verpflichtungen gegenüber – und das bei erschöpften Ressourcen und begrenzten Budgets. Deshalb ist es so wichtig, bestehende Sicherheitsinvestitionen zu nutzen, um die Rentabilität von Endpunkten, Cloud-Zugang, VPNs, Perimetersicherheit und Protokollierungssystemen zu maximieren.

Diese Tabelle enthält drei Optionen für Dienstleistungen im Bereich Sicherheitsmanagement: Managed Detection and Response (MDR), Extended Detection and Response (XDR) und N-able MDR. Vergleichen Sie die Einblicke in die einzelnen Dienstleistungen, um zu entscheiden, wo Sie Ihr begrenztes Budget investieren und Ihren Cyberschutz maximieren sollten.


| | MDR | XDR | N-able MDR |
|---|---|---|---|
| **Wer verwaltet was?** | Managed Service | Managed Service oder vom Kunden verwaltet | Managed Service oder vom Kunden verwaltet |
| **Datenquellen** | ◢ Endpunkt<br>◢ Netzwerk-Traffic<br>◢ Cloud-Dienste | ◢ Endpunkt<br>◢ Netzwerk-Traffic<br>◢ Perimeter<br>◢ Cloud-Dienste<br>◢ Active Directory<br>◢ E-Mail | ◢ Endpunkt<br>◢ Netzwerk-Traffic<br>◢ Perimeter<br>◢ Cloud-Dienste<br>◢ Active Directory<br>◢ E-Mail |
| **Erkennungen** | ◢ Malware/IoCs<br>◢ Dateilose Angriffe | ◢ Malware/IoCs<br>◢ Dateilose Angriffe<br>◢ Verhaltensanomalien<br>◢ Maschinelles Lernen | ◢ Malware/IoCs<br>◢ Dateilose Angriffe<br>◢ Verhaltensanomalien<br>◢ Maschinelles Lernen |
| **Untersuchung** | In SOC-Dienstleistung inbegriffen (variiert) | ◢ Erfordert Managed SOC-Dienstleistung<br>◢ SOC führt Untersuchungen durch | ◢ In SOC-Dienstleistung inbegriffen<br>◢ In SOC-Dienstleistung inbegriffen |
| **Reaktion** | MDR SOC-Dienstleistung: Selbstverwaltet | Erfordert Managed SOC-Dienstleistung | SOC-Dienstleistung: Erweitertes Sicherheitsteam |
| **Korrektur** | ◢ Endpunkt-Isolierung und -Blockierung<br>◢ Traffic-Blockierung (Quell-IP/DNS)<br>◢ Cloud-Zugang zurücksetzen oder deaktivieren | ◢ Endpunkt-Isolierung und -Blockierung<br>◢ Traffic-Blockierung (Quell-IP/DNS)<br>◢ Konto/Gruppe zurücksetzen oder deaktivieren<br>◢ Zugang zur Cloud zurücksetzen oder deaktivieren | ◢ Endpunkt-Isolierung und -Blockierung<br>◢ Traffic-Blockierung (Quell-IP/DNS)<br>◢ Konto/Gruppe zurücksetzen oder deaktivieren<br>◢ Zugang zur Cloud zurücksetzen oder deaktivieren |
| **Berichterstellung** | Abhängig von der SOC-Kapazität | ◢ Erfordert Managed SOC-Dienstleistung<br>◢ Mitverwaltete Berichterstellung | ◢ Erkennungen<br>◢ Untersuchungen<br>◢ Benutzerdefinierte Berichte<br>◢ Compliance-Einsichten<br>◢ Compliance-Prüferberichte<br>◢ Zusammenfassungen für Führungskräfte |
| **Gefahrenerkennung und -analyse** | Primitiv | Primitiv | ◢ Eigenes Team für Bedrohungsanalysen und Untersuchungen<br>◢ Feed für Bedrohungsanalysen<br>◢ Überwachung des Darknets<br>◢ Verwaltete Täuschungstechnologie |
| **Zeit bis zur Bereitstellung** | ◢ Erfordert zunächst Lizenzen für Dienstleistungen<br>◢ Wochenlange Konfigurations- und Abstimmungsarbeit | ◢ Erfordert zunächst Lizenzen für Dienstleistungen<br>◢ Wochenlange Konfigurations- und Abstimmungsarbeit | ◢ Bereitstellung in wenigen Tagen<br>◢ Agent wird über Gruppenrichtlinienobjekt (GPO) bereitgestellt |
| **Sichtbarkeit** | SOC-Anfragen nach Berichten oder Informationen über Untersuchungen | Co-Management variiert | ◢ 100 % Sichtbarkeit für den Kunden: Der Kunde hat Zugriff auf dasselbe Portal wie das SOC<br>◢ Echtzeit-Kundenberichte |
| **Kontext** | ◢ SOC-Anfragen für Berichte oder Informationen zu Untersuchungen<br>◢ Begrenzte Compliance-Berichterstellung | Co-Management variiert | ◢ Eine vereinfachte Ansicht: Der Kunde hat Zugriff auf dasselbe Portal wie das SOC<br>◢ Bedrohungen und Erkennungen<br>◢ Risikoprogramme<br>◢ Verletzungen der Network Health Policy<br>◢ Compliance-Einsichten |

## Bringen Sie Bedrohungen ans Licht und schalten Sie Risiken aus

Erfahren Sie mehr darüber, wie die Managed Detection and Response-Dienstleistungen und die Security Operations Platform von N-able Ihr Team in die Lage versetzen, Bedrohungen zu erkennen, Cyber-Risiken zu reduzieren und die Kontrolle zu übernehmen.




N-ABLE

N-able bietet MSPs und IT-Serviceanbietern leistungsstarke Software zur Überwachung, Verwaltung und Absicherung von IT-Infrastrukturen und Netzwerken. Unser Angebot umfasst eine skalierbare Plattform, eine sichere Infrastruktur, Tools für die einfachere Verwaltung komplexer IT-Umgebungen und Ressourcen für die digitale Transformation. Wir unterstützen unsere Partner in jeder Wachstumsphase beim Schutz ihrer Kunden sowie beim Ausbau ihres Angebots – durch das ständig wachsende flexible Portfolio an Integrationen führender Anbieter. n-able.com/de