kaspersky

EDR vs MDR vs XDR

EDR
Endpoint Detection and Response

Identifiziert neue, unbekannte und schwer zu erkennende Bedrohungen, die den Endpunktschutz umgehen, und automatisiert routinemäßige Sicherheitsaufgaben.

MDR
Managed Detection and Response

Bietet kontinuierlichen, verwalteten Schutz selbst vor den komplexesten und innovativsten Nicht-Malware-Bedrohungen.

XDR
Extended Detection and Response

Proaktive Erkennung komplexer Bedrohungen auf mehreren Infrastrukturebenen und automatische Reaktion auf diese Bedrohungen und deren Bekämpfung.

Funktionsweise

- Ermöglicht erweiterte Erkennung und Suche nach Bedrohungen, die Präventionsmechanismen umgehen.
- Verbessert die Sichtbarkeit und Visualisierung von Bedrohungen
- Vereinfacht die Ursachenanalyse
- Liefert zentralisierte, automatisierte Antworten

- Sammelt Telemetriedaten von Sicherheitsprodukten, analysiert proaktiv die Metadaten der Systemaktivität auf Anzeichen eines aktiven oder bevorstehenden Angriffs und bietet verwaltete oder geführte Reaktionen.

- Integriert mehrere Tools und Sicherheitsanwendungen
- Überwachung von Daten auf Endgeräten, Netzwerken, Clouds, Webservern, Mailservern usw. zur Erkennung und Beseitigung komplexer Bedrohungen.
- Vereinfacht die Verwaltung der Informationssicherheit durch Automatisierung der produktübergreifenden Interaktion.

Für wen ist diese Lösung geeignet?

- Unternehmen mit einem internen IT-Sicherheitsteam, das einen detaillierten Einblick in die Endpunkte und eine zentralisierte Reaktion benötigt, um manuelle Aufgaben zu reduzieren.

- Unternehmen, die ihre internen IT-Sicherheitskapazitäten durch Auslagerung wichtiger Erkennungs- und Reaktionsaufgaben erweitern wollen.
- Organisationen, die möglicherweise nicht über das Budget oder Fachpersonal verfügen, um ihr eigenes internes SOC aufzubauen.

Sicherheitserfahrene Unternehmen, die sich eine einzige Plattform wünschen:

- Ein schlüssiges Bild der Vorgänge in der gesamten Infrastruktur
- Integrierte Bedrohungsjagd und Threat Intelligence
- Hervorragende Priorisierung von Vorfällen und weniger falsch-positive Warnmeldungen

Geschäftswert

- Gibt dem Sicherheitspersonal die einheitliche Sichtbarkeit und Kontrolle, die es braucht, um aktiv nach Bedrohungen zu suchen, anstatt auf Warnmeldungen zu warten.
- Maximiert die Kapazitäten bestehender IT-Sicherheitsteams durch die Automatisierung einer Reihe von Analyse-, Untersuchungs- und Reaktionsprozessen.
- Steigert die Kosteneffizienz, indem es IT-Sicherheitsteams ermöglicht, effektiver zu arbeiten, ohne mit mehreren Tools und Konsolen jonglieren zu müssen.

- Löst den Fachkräftemangel im Bereich Cybersicherheit und bietet sofortigen Schutz vor komplexen Bedrohungen.
- Ermöglicht die Auslagerung von Vorfallmanagementprozessen, um begrenzte und teure interne Ressourcen besser auf die entscheidenden Ergebnisse zu konzentrieren.
- Senkung der Gesamtsicherheitskosten, ohne dass komplexe Sicherheitslösungen eingesetzt und eine Reihe von internen Sicherheitsspezialisten beschäftigt werden müssen.

- Bietet ganzheitlichen Schutz gegen die sich entwickelnde Bedrohungslandschaft.
- Ökosystem-Ansatz maximiert die Effizienz der beteiligten Cybersicherheits-Tools, spart Ressourcen und reduziert Risiken.
- Vereinfacht die Arbeit von IT-Sicherheitsspezialisten und gibt ihnen den zusätzlichen Kontext, den sie zur Untersuchung von Multi-Vektor-Angriffen benötigen.
- Minimiert MTTD und MTTR, welche entscheidend bei der Bekämpfung von komplexen Bedrohungen und gezielten Angriffen sind.
- Ermöglicht zentralisierte und automatisierte Reaktionen über die gesamte Sicherheitstechnologie hinweg.

Wenn Sie ein sicherheitsbewusstes Unternehmen sind, das von den XDR-Funktionen profitieren möchte, sollten Sie sich die Lösung ansehen.

Kaspersky Expert Security

Weitere Informationen