kaspersky

EDR vs MDR vs XDR

EDR
Endpoint Detection and Response

Identificeert nieuwe, onbekende en ongrijpbare bedreigingen die endpointbeveiliging omzeilen en automatiseert routinebeveiligingstaken

MDR
Managed Detection and Response

Biedt continu beheerde bescherming tegen zelfs de meest complexe en innovatieve non-malware bedreigingen

XDR
Extended Detection and Response

Detecteert proactief complexe bedreigingen op meerdere infrastructuurniveaus, reageert automatisch op deze bedreigingen en gaat ze tegen

Hoe het werkt

- Maakt geavanceerde detectie en zoektocht naar bedreigingen die preventiemechanismen omzeilen mogelijk
- Verbetert de zichtbaarheid en visualisatie van bedreigingen
- Vereenvoudigt de analyse van hoofdoorzaak
- Geeft gecentraliseerde, geautomatiseerde respons

- Verzamelt telemetrie van beveiligingsproducten, analyseert proactief metagegevens voor systeemactiviteiten om te zoeken naar tekenen van een actieve of dreigende aanval en biedt een beheerde of begeleide respons

- Integreert meerdere tools en beveiligingsapplicaties
- Bewaakt gegevens op endpoints, netwerken, clouds, webservers, mailservers enz. om complexe bedreigingen te detecteren en elimineren
- Vereenvoudigt beveiligingsbeheer van informatie door cross-productinteractie te automatiseren

Voor wie is dit het beste?

- Bedrijven met een intern IT-beveiligingsteam die een gedetailleerd endpoint-overzicht en gecentraliseerde respons nodig hebben zodat er minder taken handmatig uitgevoerd hoeven te worden

- Bedrijven die hun interne IT-beveiligingsmogelijkheden willen uitbreiden door belangrijke detectie- en responstaken uit te besteden
- Organisaties die niet over het budget of het gespecialiseerde personeel beschikken om hun eigen interne SOC te bouwen

Ervaren beveiligingsorganisaties die één platform willen:

- Een samenhangend beeld van wat er in hun infrastructuur gebeurt
- Ingebouwde zoektocht naar bedreigingen en informatie over bedreigingen
- Uitstekende incidentprioritering en minder false positive-waarschuwingen

Zakelijke waarde

- Geeft beveiligingspersoneel de geïntegreerde zichtbaarheid en controle die het nodig heeft om actief te zoeken naar bedreigingen in plaats van te wachten op waarschuwingen
- Maximaliseert de mogelijkheden van bestaande IT-beveiligingsteams door een reeks analyse-, onderzoek en responsprocessen te automatiseren
- Verhoogt de kostenefficiëntie door IT-beveiligingsteams efficiënter te kunnen laten werken zonder te hoeven worstelen met meerdere tools en consoles

- Lost de cyberbeveiligingscrisis op en biedt onmiddellijke bescherming tegen complexe bedreigingen
- Maakt uitbesteding van incidentbeheerprocessen mogelijk om beperkte en dure interne middelen beter te richten op de kritische resultaten die worden geleverd
- Verlaagt de totale beveiligingskosten zonder complexe beveiligingsoplossingen te hoeven implementeren en een reeks interne beveiligingsspecialisten in dienst te hoeven nemen

- Biedt holistische bescherming tegen het ontwikkelende bedreigingslandschap
- Ecosysteemaanpak maximaliseert de efficiëntie van de gebruikte cyberbeveiligingstools, bespaart middelen en vermindert risico's
- Vereenvoudigt het werk van IT-beveiligingsspecialisten en geeft ze de aanvullende context die ze nodig hebben om multivector-aanvallen te onderzoeken
- Minimaliseert MTTD en MTTR - cruciaal in de strijd tegen complexe bedreigingen en gerichte aanvallen
- Maakt gecentraliseerde en geautomatiseerde respons mogelijk binnen de hele beveiligingstechnologie-stack

Als jouw organisatie ervaren is op het gebied van beveiliging en wil profiteren van XDR-mogelijkheden, kijk dan eens naar

Kaspersky Expert Security

Meer informatie