kaspersky

EDR vs MDR vs XDR

EDR
Endpoint Detection and Response

Identifica le minacce nuove, sconosciute ed elusive che aggirano la protezione degli endpoint e automatizza le attività di sicurezza di routine

MDR
Managed Detection and Response

Fornisce una protezione gestita continua contro le minacce malwareless più complesse e innovative

XDR
Extended Detection and Response

Rileva in modo proattivo le minacce complesse su più livelli di infrastruttura e risponde automaticamente a tali minacce per contrastarle

Come funziona

- Consente il rilevamento avanzato e la ricerca delle minacce che tentano di aggirare i meccanismi di prevenzione
- Migliora la visibilità e la visualizzazione delle minacce
- Semplifica la root-cause analysis
- Fornisce una risposta centralizzata e automatizzata

- Raccoglie dati di telemetria dai prodotti di sicurezza, analizza in modo proattivo i metadati dell'attività del sistema per rilevare eventuali segnali di un attacco attivo o imminente e fornisce una risposta gestita o guidata

- Integra più strumenti e applicazioni di sicurezza
- Monitora i dati su endpoint, reti, cloud, server Web, server di posta e così via per rilevare ed eliminare le minacce complesse
- Semplifica la gestione della sicurezza informatica automatizzando l'interazione tra i prodotti

Per chi è più indicato?

- Aziende con un team di sicurezza IT interno che necessitano di visibilità granulare degli endpoint e risposta centralizzata per ridurre le attività di gestione manuale

- Aziende che intendono espandere la capacità della sicurezza IT interna, alleggerendo il carico dei task di rilevamento e risposta
- Organizzazioni che potrebbero non disporre del budget o del personale specializzato per creare un proprio SOC interno

Organizzazioni di livello avanzato in materia di sicurezza che desiderano un'unica piattaforma in grado di offrire:

- Un quadro coerente di ciò che sta accadendo nell'infrastruttura
- Ricerca delle minacce e threat intelligence integrate
- Migliore definizione delle priorità degli incidenti e meno avvisi di falsi positivi

Valore aziendale

- Fornisce al team responsabile della sicurezza la visibilità e il controllo unificati di cui ha bisogno per ricercare attivamente le minacce invece di attendere gli avvisi
- Ottimizza le capacità dei team di sicurezza IT esistenti automatizzando una serie di processi di analisi, indagine e risposta
- Favorisce l'efficienza dei costi consentendo ai team responsabili della sicurezza di lavorare in modo più efficiente, senza spostarsi tra più strumenti e diverse console

- Risolve il problema della mancanza di talenti nel campo della cybersecurity garantendo una protezione immediata contro le minacce complesse
- Consente l'outsourcing dei processi di gestione degli incidenti per concentrare meglio le risorse interne, limitate e costose, sui risultati critici
- Riduce i costi complessivi della sicurezza, senza bisogno di implementare complesse soluzioni di sicurezza e assumere esperti di cybersecurity

- Fornisce una protezione olistica contro il panorama delle minacce in evoluzione
- L'approccio basato sull'ecosistema ottimizza l'efficienza degli strumenti di cybersecurity coinvolti, consente di risparmiare risorse e riduce i rischi
- Semplifica il lavoro degli specialisti della sicurezza IT e fornisce loro il contesto aggiuntivo necessario per indagare sugli attacchi multi-vettore
- Riduce al minimo MTTD e MTTR, fondamentali per contrastare minacce complesse e attacchi mirati
- Consente una risposta centralizzata e automatizzata nell'intero stack tecnologico di sicurezza

Se la vostra è un'organizzazione di livello avanzato in termini di sicurezza che desidera trarre vantaggio dalle funzionalità XDR, date un'occhiata a

Kaspersky Expert Security

Per saperne di più