EDR

MOEITELOZE EN KRACHTIGE ENDPOINT DETECTIE EN RESPONS

Met onze Endpoint Detection and Response (EDR) kun je geavanceerde dreigingen detecteren en erop reageren. Onze EDR-oplossing is een gebruiksvriendelijke, cloud-gebaseerde EDR-oplossing die speciaal is ontworpen voor jouw bedrijf. EDR is ontworpen om voortdurend data te monitoren, te verzamelen en te analyseren, waardoor bedreigingen vroegtijdig worden gedetecteerd en geneutraliseerd.

BELANGRIJKSTE FUNCTIES VAN ONZE EDR-OPLOSSING

- **Click-to-respond**

Neem direct actie tegen geavanceerde bedreigingen vanuit je alertdashboard. Isoleer hosts, beëindig processen, verwijder bestanden en meer zonder kostbare seconden te verspillen.

- **Detecteer fileless aanvallen met gedragsanalyse**

Onze EDR-oplossing omvat gepatenteerde diepgaande geheugenanalyse om je op de hoogte te houden van zelfs de meest ongrijpbare bedreigingen.

- **MITRE ATT&CK mapping**

Onze alerts worden gekoppeld aan het MITRE ATT&CK-framework om context en helderheid te bieden, waardoor de benodigde beveiligingsexpertise wordt verminderd.

- **Slimme aanbevelingen**

Onze ervaren SOC-analisten hebben hun expertise vertaald in geautomatiseerde mitigatie-aanbevelingen voor de geavanceerde dreigingen van vandaag.

- **Schaalbare remote response acties**

Zodra een dreiging wordt gedetecteerd, is het essentieel om snel te reageren. Onze click-to-respond functie ondersteunt je team in het snel nemen van maatregelen tegen cyberaanvallen om potentiële schade te beperken.

- **Geïntegreerde EDR en RMM**

Onze EDR-oplossing integreert met onze RMM voor efficiënte en naadloze endpointbeheer.

WAAROM ANTIVIRUS EN EDR?

Een antivirusprogramma werkt meestal met een systeem voor dreigingsdetectie op basis van handtekeningen, waarbij een bestand dat als bedreiging is geïdentificeerd, wordt vergeleken met een database van kwaadaardige bestanden. Dit werkt goed voor het identificeren en stoppen van bekende malware en virussen zoals trojans en worms, maar minder goed voor nieuwere, niet-gecatalogiseerde bedreigingen, waar EDR in uitblinkt.

Dreigingsmitigatie mag je bedrijfsprocessen nooit verstoren. Met een EDR-systeem worden verdachte bestanden onmiddellijk in quarantaine geplaatst of geïsoleerd binnen sandboxes, zodat ze andere bestanden niet kunnen infecteren of je data kunnen compromitteren. EDR's kunnen ook bepaalde bedreigingsactiviteiten automatisch verhelpen, wat je tijd en moeite bespaart.

Ten slotte voeren antivirusoplossingen controles uit op geplande intervallen, terwijl een EDR 24/7 monitoring uitvoert om volledige veiligheid te garanderen.

HET BELANG VAN EEN EDR-OPLOSSING

Endpointbeveiliging is de eerste verdedigingslinie voor elke organisatie. Om dit te realiseren, moet je eerst zicht krijgen op al je endpoints, omdat je niet kunt beschermen wat je niet kunt zien.

Volgens een beveiligingsrapport is 58% van de organisaties zich bewust van minder dan 75% van de assets op hun netwerk. Een EDR-oplossing lost dit op door alle endpoints in je IT-omgeving te ontdekken en volledige perimeterbeveiliging te bieden.

EDR

DE BASISFUNCTIES VAN EDR

n deze sectie worden de essentiële functies van EDR besproken die het een onmisbare beveiligingstool voor endpoints maken:

• **Gegevensverzameling en analyse**
EDR-oplossingen verzamelen een verscheidenheid aan endpointgegevens, zoals procescreatie, het laden van drivers, registerwijzigingen, schijftoegangen en netwerkverbindingen voor analyse. Vervolgens wordt ingebouwde dreigingsinformatie toegepast om Indicators of Compromise (IoC) en Indicators of Attack (IoA) in de verzamelde gegevens te identificeren die wijzen op een cyberaanval.

• **Gedragsanalyse**
EDR maakt gebruik van gedragsanalyse om actief kwaadaardige aanvallen te detecteren en te neutraliseren. Het creëert een gedragsbaseline voor elk endpoint, zodat elke activiteit of patroon dat buiten de vastgestelde norm valt en een dreiging kan aangeven, onmiddellijk kan worden aangepakt.

• **Dreigingsdetectie**
EDR stelt beveiligingsteams in staat om complexe dreigingen, zoals fileless malware en ransomware, in real-time te detecteren en erop te reageren. In plaats van te wachten tot een dreiging opduikt, speurt EDR er actief naar, waardoor bedrijven twee stappen voor blijven op cybercriminelen.

• **Zichtbaarheid**
EDR-agents verzamelen en analyseren gegevens op elk endpoint om ervoor te zorgen dat geen enkele kan dienen als toegangspunt voor cybercriminelen.

• **Geautomatiseerde respons**
EDR-tools kunnen verschillende stappen ondernemen om een aanval te verhelpen of in te dammen, zoals:

- Verwijderen van bestanden en blokkeren van verdachte bestanden.
- Beëindigen van processen.
- Isoleren van het endpoint op het netwerk om laterale beweging van de aanval te voorkomen.
- Automatische of handmatige uitvoering van verdachte payloads in een sandbox.
- Uitvoeren van scripts op afstand op het endpoint.

• **Rapportage en waarschuwingen**
Geavanceerde EDR's hebben geavanceerde rapportagemogelijkheden die technici helpen om in enkele minuten aanpasbare en eenvoudig te begrijpen rapporten te maken. Deze functie stelt bedrijven in staat om naleving van beveiligingsvoorschriften aan te tonen en klantvertrouwen op te bouwen. Het verstrekken van real-time waarschuwingen met contextuele informatie over het ernstniveau en aanbevolen actie is een andere cruciale functie van een EDR-oplossing. Beveiligingsteams kunnen incidenten effectiever beheren wanneer ze op basis van prioriteit op waarschuwingen kunnen reageren.

NEEM DIRECT CONTACT MET ONS OP OM MEER TE WETEN TE KOMEN

info@heiper.nl