DATASHEET

Bitdefender

MDR

Bitdefender Managed Detection & Response Service

MODERNE MDR-DIENSTEN VOOR GROTE EN KLEINE BEDRIJVEN EN ONDERNEMINGEN

www.bitdefender.nl

Wij bieden permanent geavanceerde preventie en remediëring van aanvallen, zodat u dat niet hoeft te doen.

"Bitdefender MDR verzekert mij dat iemand ons volledige netwerk bewaakt in real time, ook wanneer mijn personeel en ik niet op kantoor zijn." - IT Director, Archdiocese

Het oplossen van beveiligingsuitdagingen voor de organisatie

Beveiliging wordt een steeds belangrijker onderwerp voor bedrijven wereldwijd. Aanvallen worden steeds meer complex en bouwen een sterkere weerbaarheid op tegen traditionele preventiemiddelen. Bedrijven moeten hun beveiligingsstrategieën en resources afstemmen zodat ze inbreuken snel en doeltreffend kunnen identificeren, en snel kunnen reageren.

33% van de inbreuken zijn het resultaat van aanvallen die gebruikmaken van social engineering, zoals phishing. Laptops en desktops stellen zo'n 25% van de gegevensinbreuken voor – 2019 DBIR Verizon

Een tekort aan beveiligingspersoneel: beveiligingsanalisten vormen een zeldzame en dure resource, en zijn moeilijk in dienst te nemen en te behouden. Volgens een recente Ponemon-enquête overweegt 60% van SOC-teamleden zijn baan op te geven als gevolg van te veel stress.

Detectie van geavanceerde aanvallen: geavanceerde aanvallen zijn moeilijk te detecteren omdat ze gebruikmaken van tactieken, technieken en procedures (TTP's) die elk afzonderlijk kunnen worden geaanzien als normale activiteiten. De gemiddelde kosten van cyberincidenten is voor bedrijven in de afgelopen 5 jaar met niet minder dan 72 procent gestegen, tot 13 miljoen dollar - 2019 Accenture “Cost of Cybercrime”

Tijdrovend onderzoek: beveiligingsanalisten hebben niet genoeg tijd om elke waarschuwing te beoordelen en om prioriteiten te stellen voor verder onderzoek. Gemiddelde responstijd (MTTR, Mean Time To Respond) wordt voor de meeste organisaties uitgedrukt in maanden, terwijl aanvallers gegevens compromitteren en exfiltreren in slechts enkele dagen.

Een overdaad aan tools: organisaties beschikken voor het beheer van hun beveiligingsarchitectuur over meerdere consoles met verschillende technologieën. Bijna 40% van de deelnemers aan de Ponemon-enquête zegt te veel tools te hebben. En 71% heeft behoefte aan meer automatisering om waarschuwingen te beheren en bewijsmateriaal te verzamelen.

Hoe kan de Managed Detection & Responsedienst (MDR) van Bitdefender hierbij helpen?

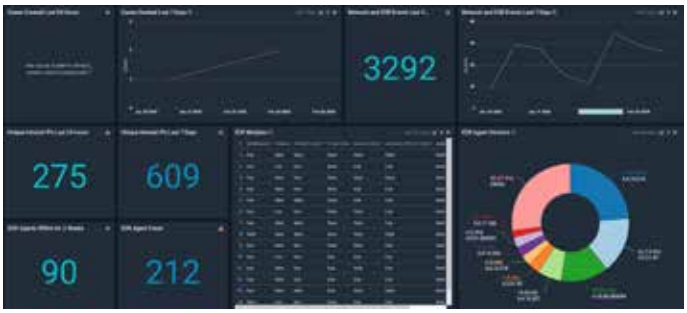
De Bitdefender MDR-dienst is een combinatie van toonaangevende cyberbeveiliging voor endpoints, plus netwerk- en beveiligingsanalyses, en expertise op het vlak van dreigingsdetectie. Het Bitdefender SOC (Security Operations Center) bestaat uit vooraanstaande beveiligingsanalisten uit de Amerikaanse luchtmacht en zeemacht, de NSA en de Britse inlichtingendiensten. Onze methodologie, die we hebben overgenomen uit de militaire wereld, laat ons IOA's (Indicators

of Attack) ontwikkelen voor nieuwe en geavanceerde aanvallen, en namens onze klanten tegenmaatregelen implementeren.

SOC-personeel op aanvraag: Bitdefender biedt onze klanten een volledig uitgerust Security Operations Center, dat schaalt met de klant mee en dat verzekert dat onze beveiligingsanalisten over de nodige technologie en opleiding beschikken voor de klantenomgevingen waar zij ondersteuning voor bieden.

Detectie van geavanceerde aanvallen: beveiligingsanalisten voeren voortdurend onderzoek aangaande dreigingsinformatie alsook detectiemissies uit, op basis van klantspecifieke dreigingsprofielen. Vervolgens combineren ze deze gegevens met host- en netwerktelemetriegegevens en beveiligingsanalyses om geavanceerde en doelgerichte aanvallen te detecteren.

Detectie en snelle responstijden verbeteren: realtime telemetrie en waarschuwingen zijn nauw met elkaar verbonden over verscheidene gegevensstromen heen, en responsacties worden afgestemd op elke afzonderlijke klant om de impact van beveiligingsincidenten te beperken.



Minder operationele belemmeringen: de Bitdefender MDR-dienst beheert namens u de beveiligingstechnologie, zodat u uw team kunt laten concentreren op meer strategische initiatieven. Dit heeft een rechtstreekse impact op de kosten, aangezien personeelskosten worden gedrukt en u minder licenties nodig heeft voor externe tools. Realtime dashboards, korte overzichten en actie-evaluaties bieden input voor strategische besluitvorming.

Opties voor Bitdefender MDR-diensten

Wij bieden drie MDR-oplossingen aan. Daarnaast zijn er uitbreidingen beschikbaar voor het gelicentieerde pakket MDR-diensten.

	MDR Core	MDR Advanced	MDR Enterprise
Next-gen AV (NGAV)	✓	✓	✓
Automatische remediëring	✓	✓	✓
Beheer van toepassingen en apparaten	✓	✓	✓
Op host gebaseerde firewall & webbeheer	✓	✓	✓
EDR - Detectie en respons op endpoint-niveau	✓	✓	✓
Accountmanager		✓	✓
Risicoanalyse gebruikers		✓	✓
Detectie van doelgerichte dreigingen		✓	✓
Aangepaste acties als respons op incidenten, op basis van Playbooks		✓	✓
Klantspecifiek dreigingsmodel		✓	✓
Monitoring van phishing van domeinregistratie			✓
Monitoring van niet-geoorloofde publicatie van code of klanteninformatie			✓
Monitoring van het Dark Web			✓
Integratie met aangepaste tools			✓
Monitoring van hoogwaardige doelen en risicovolle doelen			✓
Uitbreidingen			
Bescherming van agentloze IoT-apparaten		✓	✓

U ontdekt meer op https://www.bitdefender.com/MDR

WAAROM BITDEFENDER?

ONBETWISTE MARKTLEIDER OP HET GEBIED VAN INNOVATIE

38% van alle cybersecurity leveranciers (wereldwijd) heeft ten minste één Bitdefendertechnologie geïntegreerd. Aanwezig in 150 landen.

'S WERELDS EERSTE END-TO-END BREACH AVOIDANCE

Het eerste security platform dat hardening, preventie, detectie, reactie en services verenigt over endpoints, netwerken en de cloud.

Als beste geteste beveiliging. AWARDED ACROSS THE BOARD.

Bitdefender®

Opgericht in 2001, Roemenië
Aantal medewerkers 1800+

Hoofdkantoor
Enterprise HQ - Santa Clara, CA, Verenigde Staten
Technologie HQ - Boekarest, Roemenië

WERELDWIJDE KANTOREN
USA & Canada: Ft. Lauderdale, FL | Santa Clara, CA | San Antonio, TX | Toronto, CA
Europa: Kopenhagen, DENEMARKEN | Parijs, FRANKRIJK | München, DUITSLAND | Milaan, ITALIË | Boekarest, Iasi, Cluj, Timisoara, ROEMENIË | Barcelona, SPANJE | Dubai, Verenigde Arabische Emiraten | Londen, VK | Den Haag, NEDERLAND
Australië: Sydney, Melbourne

IN HET TEKEN VAN DE WOLF

Informatiebeveiliging is een industrie waar alleen het duidelijkste beeld, de scherpste geest en het diepste inzicht kunnen winnen - een spel zonder marge voor fouten. Het is onze taak om iedere strijd te winnen, duizend van de duizend keer en een miljoen van de miljoen keer.

En dat doen we. We zijn de industrie te slim af door niet alleen het helderste zicht, de scherpste geest en het diepste inzicht te hebben, maar ook door iedereen, of het nu gaat om black hats of collega-security experts, een stap voor te blijven. De schittering van onze collectieve geest is als een **lichtgevende Dragon-Wolf** aan uw zijde, aangedreven door een ontwikkelde intuïtie, gecreëerd om te beschermen tegen alle gevaren die verborgen zijn in de mysterieuze details van de digitale wereld.

Deze eigenschap is onze superkracht en we gebruiken het in de kern van al onze baanbrekende producten en oplossingen.

Bitdefender-MOH-Datasheet-creat4741-nl_NL-09/01/20September 1, 2020 11:41 pm09/01/20