GIDS

De complete gids voor Managed Detection & Response

Kosten, selectiecriteria, MDR vs EDR vs SOC, NIS2-compliance, ROI en implementatie. Met actuele Nederlandse marktdata en bronvermelding.

Maart 2026

IBGIDS NL

INHOUDSOPGAVE

Kerncijfers op een rij

MDR groeit wereldwijd met meer dan 20% per jaar. Voor MKB-bedrijven zonder eigen SOC is het de meest toegankelijke route naar 24/7 cyberbeveiliging.

EUR 850K+
Kosten per jaar voor een eigen SOC (8--10 FTE, tooling, faciliteiten)
Diverse bronnen [1]

201%
ROI van MDR over 3 jaar, terugverdientijd minder dan 6 maanden
Forrester [2]

22%
Jaarlijkse groei van de globale MDR-markt (CAGR tot 2030)
Mordor Intelligence [3]

277 dagen
Gemiddelde breach lifecycle zonder MDR -- met MDR: minder dan 1 dag
IBM [4]

EUR 270K
Gemiddelde schade per cyberincident voor Nederlands MKB
ESET/Hallo [5]

EUR 10--25
Kosten per endpoint per maand voor MKB MDR-diensten
Diverse bronnen [6]

24 uur
NIS2-meldplicht: vroegtijdige waarschuwing binnen 24 uur na ontdekking
NCSC [7]

USD 5,1 mrd
Globale MDR-marktwaarde 2026, verwacht USD 11,3 mrd in 2030
Mordor Intelligence [3]

1. Wat is MDR?

Managed Detection & Response (MDR) is een uitbestede cybersecurity-dienst waarbij een externe partij 24/7 je IT-omgeving monitort, dreigingen opspoort en bij incidenten direct ingrijpt.

MDR combineert technologie (EDR/XDR/SIEM) met menselijke expertise (SOC-analisten en threat hunters). Het is de snelst groeiende categorie in cybersecurity -- en voor MKB-bedrijven de meest realistische manier om 24/7 beveiliging te realiseren zonder een eigen SOC op te bouwen [1].

WAT MAAKT MDR UNIEK?

- **Detectie** -- Continue monitoring van endpoints, netwerk, cloud en identiteit op verdacht gedrag
- **Analyse** -- Menselijke analisten beoordelen alerts, filteren false positives en verrijken met context
- **Response** -- Actief ingrijpen bij dreigingen: isoleren van systemen, blokkeren van accounts, containment
- **Threat hunting** -- Proactief zoeken naar onbekende dreigingen die detectieregels omzeilen

Kernverschil met MSSP: Een MSSP (Managed Security Service Provider) stuurt alerts door en laat de respons aan jou over. MDR grijpt actief in. Dat is het verschil tussen "je hebt een probleem" en "we hebben het probleem opgelost" [8].

2. Waarom is het belangrijk?

MKB-bedrijven zijn het meest kwetsbaar voor cyberaanvallen, maar hebben het minste budget en personeel om zich te beschermen. MDR lost dat op.

HET MKB-PROBLEEM

Een eigen SOC kost meer dan EUR 850.000 per jaar: 8--10 FTE analisten (24/7 dekking), SIEM/XDR-tooling, training en faciliteiten [1]. Dat is voor vrijwel elk MKB-bedrijf onbetaalbaar. Tegelijkertijd is 24/7 monitoring noodzakelijk: 77% van het Nederlandse MKB heeft in de afgelopen twee jaar te maken gehad met cybercriminaliteit [9] en de gemiddelde schade per incident bedraagt EUR 270.000 [5].

DETECTIETIJD: VAN MAANDEN NAAR MINUTEN

Zonder MDR bedraagt de gemiddelde breach lifecycle 277 dagen -- 207 dagen om een breach te detecteren plus 70 dagen om te containen [4]. Met MDR daalt de detectietijd naar minuten tot uren en de responstijd naar minuten. In EMEA is de mediaan dwell time 22 dagen -- de langste van alle regio's [10]. MDR reduceert dit naar real-time detectie.

DE CIJFERS

EUR 2,55 mrd

Nederlandse cybersecurity-markt 2026

Mordor Intelligence [3]

8,4%

Jaarlijkse groei cybersecurity-diensten in Nederland (2026--2031)

Mordor Intelligence [3]

De globale MDR-markt groeit van USD 5,09 miljard in 2026 naar USD 11,30 miljard in 2030. De Nederlandse cybersecurity-markt als geheel groeit van USD 2,55 miljard naar USD 3,79 miljard in dezelfde periode [3]. Groeidrivers: AI-gedreven detectie, tekort aan cybersecurity-experts, NIS2-regeldruk en toenemende complexiteit van cyberaanvallen.

> **Cybersecurity-talent is schaars**
>
> Een SOC-analist kost EUR 70.000--120.000 per jaar in Nederland, en het verloop is hoog door burnout. Met MDR is personeelsschaarste het probleem van de provider, niet van jou [1].

3. Hoe werkt het?

Van onboarding tot dagelijkse monitoring: zo ziet een MDR-traject eruit in de praktijk.

HET ONBOARDING-PROCES

1 Kick-off & discovery

DAG 1--2

Inventarisatie IT-omgeving, assets, huidige security-maatregelen en risicoprofiel.

2 Agent deployment

DAG 3--7

EDR/XDR agents uitrollen op endpoints: laptops, servers, mobiele apparaten.

3 Telemetrie configuratie

DAG 5--10

Log-feeds, SIEM-integratie, cloud-connectoren en netwerkmonitoring aansluiten.

4 Playbook setup

DAG 7--14

Respons-scenario's, escalatiepaden en communicatieprotocol vastleggen.

5 Tuning & baselining

WEEK 2--4

False positives reduceren, environment-specifieke detectieregels instellen [11].

6 Operationeel

DOORLOPEND

24/7 monitoring actief. Dagelijkse detectie, analyse, respons en rapportage.

DOORLOOPTIJD PER SEGMENT

ORGANISATIEGROOTTE	DOORLOOPTIJD	TOELICHTING
Klein MKB (< 50 endpoints)	3--10 dagen	Standaard omgeving, weinig integraties
Middelgroot MKB (50--500)	1--3 weken	Meerdere systemen, custom playbooks

ORGANISATIEGROOTTE	DOORLOOPTIJD	TOELICHTING
Enterprise (500+)	6--12 weken	Complexe integraties, governance, compliance

Ter vergelijking: een eigen SOC opbouwen kost 6--12 maanden. MDR is operationeel in dagen tot weken [11].

RESPONSMODELLEN

MODEL	BESCHRIJVING	GESCHIKT VOOR
Fully Managed	MDR-team beheert volledige threat response namens jou	MKB zonder eigen security-team
Co-Managed	MDR-team werkt samen met je interne IT/security-team	MKB met basis IT-team
Advisory	MDR-team alerteert en geeft advies, jij voert uit	Organisaties met eigen SOC die versterking willen [12]

TIP

Kies "Fully Managed" als je geen intern security-team hebt. Je wilt dat de MDR-provider daadwerkelijk ingrijpt bij een dreiging -- niet alleen een alert sturen die om 3:00 's nachts op een mailbox belandt die niemand checkt.

4. Wat kost het?

MDR is aanzienlijk goedkoper dan een eigen SOC, maar de prijzen varieren sterk. Dit zijn de modellen en indicaties voor de Nederlandse markt.

PRIJSMODELLEN

PRIJSMODEL	INDICATIE	TOELICHTING
Per endpoint/maand (basis)	EUR 10--25	Standaard monitoring, detectie en basis respons [6]
Per endpoint/maand (premium)	EUR 25--50+	Met dedicated advisors, threat hunting, vulnerability management
Jaarcontract 100 endpoints	EUR 12.000--30.000	Endpoint-only MDR
Jaarcontract 500 endpoints	EUR 44.000--193.000	Afhankelijk van scope en serviceniveau

MKB-SPECIFIEKE PRIJZEN NEDERLAND

SEGMENT	PRIJSINDICATIE	TOELICHTING
Klein MKB (< 50 medewerkers)	Vanaf EUR 20/maand (bedrijf)	Geautomatiseerde M365-monitoring, laagdrempelig
Middelgroot MKB (50--250)	EUR 40.000--100.000/jaar	Volledige MDR met 24/7 SOC
Groot MKB / enterprise	EUR 100.000--200.000+/ jaar	Full-stack MDR, meerdere domeinen [6]

MDR VS EIGEN SOC: KOSTENVERGELIJKING

COMPONENT	EIGEN SOC	MDR-DIENST
Personeel (8--10 FTE, 24/7)	> EUR 700.000/jaar	Inbegrepen
SIEM/XDR-tooling	EUR 50.000--200.000/jaar	Inbegrepen

COMPONENT	EIGEN SOC	MDR-DIENST
Training & certificering	EUR 20.000--50.000/jaar	Inbegrepen
Management overhead	EUR 50.000--100.000/jaar	Minimaal (aanspreekpunt)
Faciliteiten	EUR 30.000--80.000/jaar	N.v.t.
Totaal	**EUR 850.000--1.130.000+/jaar**	**EUR 12.000--200.000/jaar** [1]

ROI van MDR

MDR levert een ROI van 201% over 3 jaar met een terugverdientijd van minder dan 6 maanden [2]. De besparing komt niet alleen door lagere directe kosten, maar ook door snellere detectie (50--80% lagere schade), lagere cyberverzekeringspremies en geen wervingskosten voor schaars security-talent.

5. Waar moet je op letten?

De MDR-markt is onoverzichtelijk. Deze selectiecriteria en vragen helpen je de juiste keuze te maken.

SELECTIECRITERIA

CRITERIUM	WAAROM HET ERTOE DOET
Actieve respons, niet alleen alertering	Veel aanbieders noemen zich MDR maar grijpen niet actief in. Alleen alerts doorsturen is MSSP, geen MDR [13]
24/7/365 dekking	Niet alleen kantooruren + on-call. Cyberaanvallen vinden vaker buiten kantooruren plaats
SLA met harde responstijden	Detectie < 15 min, acknowledge < 30 min, containment < 1 uur als standaard [14]
Transparantie over werkwijze	Geen black-box AI. Je moet kunnen begrijpen waarom een alert afgaat en hoe de respons werkt
Integratie met bestaande tools	MDR moet naadloos aansluiten op je huidige IT-omgeving, niet alles vervangen
Schaalbaarheid	Groei van je organisatie of infra mag niet leiden tot contractheronderhandeling of serviceonderbrekingen
Rapportage en compliance-ondersteuning	Maandelijkse rapportages over detecties, respons en SLA-performance. NIS2-ondersteuning
Exit-strategie	Geen vendor lock-in bij proprietary tooling. Data-export moet mogelijk zijn bij contracteinde

10 VRAGEN AAN EEN MDR-PROVIDER

1. Wat doet jullie team concreet als er een dreiging wordt gedetecteerd?
2. Wat is de gegarandeerde tijd van detectie tot containment?
3. Hoeveel analisten zitten er in het SOC en hoe is de 24/7 dekking geregeld?
4. Welke domeinen worden gemonitord: alleen endpoints of ook cloud, netwerk en identiteit?
5. Hoe ziet de onboarding eruit en hoe lang duurt het tot de dienst operationeel is?
6. Welke rapportages krijg ik en hoe ondersteunen jullie bij NIS2-compliance?
7. Hoe gaan jullie om met false positives en alert fatigue?

8. Wat zijn de verborgen kosten (extra endpoints, playbooks, data-ingestie)?
9. Wat gebeurt er bij contracteinde -- kan ik mijn data exporteren?
10. Bieden jullie incident response als onderdeel van de MDR-dienst of is dat apart?

> **LET OP: VERBORGEN KOSTEN**
>
> Vraag altijd naar extra kosten voor endpoint-uitbreiding, custom playbooks, API-integratie en data-ingestie boven het afgesproken volume. Sommige providers hanteren een laag instaptarief maar rekenen fors bij voor uitbreidingen.

6. Veelgemaakte fouten

Deze valkuilen ondermijnen de waarde van je MDR-investering.

1. Verantwoordelijkheid volledig overdragen

MDR is geen "set and forget". Je blijft zelf verantwoordelijk voor je cybersecurity. De MDR-provider monitort en reageert, maar jij moet de aanbevelingen opvolgen, patches installeren en je team trainen. Zonder interne commitment wordt MDR een duur alertingsysteem [13].

2. Kiezen op prijs alleen

Goedkope providers missen vaak geavanceerde detectie of ervaren analisten. Een MDR-dienst die EUR 5/endpoint/maand kost maar alleen alerts doorstuurt is geen MDR. Kijk naar de waarde: wat krijg je concreet voor je geld?

3. Vage SLA's accepteren

Een SLA die zegt "zo snel mogelijk reageren" is waardeloos. Eis harde responstijden: detectie < 15 minuten, acknowledge < 30 minuten, containment < 1 uur. Vraag naar boeteclausules als de SLA niet gehaald wordt [14].

4. Geen eigen IR-plan naast MDR

MDR detecteert en reageert op dreigingen, maar bij een groot incident (ransomware, datalek) heb je meer nodig: crisismanagement, juridische ondersteuning, communicatie. Zorg dat je een IR-plan hebt dat aansluit op je MDR-dienst.

5. Black-box AI vertrouwen

Als de provider niet kan uitleggen waarom een alert afgaat, heb je geen detectie maar geavanceerde alert fatigue. Vraag om transparantie over de detectielogica en de menselijke beoordeling [13].

6. Integratie negeren

MDR die niet naadloos integreert met je bestaande tools (Microsoft 365, Google Workspace, cloudplatformen) creert operationele bottlenecks en blinde vlekken. Controleer vooraf welke integraties beschikbaar zijn.

TIP

Vraag de provider naar referenties in jouw sector en omvang. Een MDR-dienst die goed werkt voor een enterprise met 5.000 endpoints is niet per definitie geschikt voor een MKB-bedrijf met 50 werkplekken.

7. NIS2 en MDR

De Cyberbeveiligingswet (NIS2-implementatie) treedt naar verwachting in Q2 2026 in werking. MDR helpt je op meerdere punten aan de eisen te voldoen.

HOE MDR HELPT BIJ NIS2-COMPLIANCE

NIS2-EIS	HOE MDR DIT INVULT
24/7 monitoring	Continue monitoring is een kernfunctie van MDR
Incidentdetectie	SIEM/XDR-integratie detecteert incidenten in minuten in plaats van dagen [15]
24-uurs meldplicht	MDR-SOC kan een incident binnen minuten kwalificeren en escaleren
Incidentafhandeling	Actieve respons (containment, isolatie) is standaard onderdeel van MDR
Risicobeheersmaatregelen	MDR-rapportages tonen aangetoonde zorgplicht richting toezichthouders
Forensisch onderzoek	Veel MDR-providers bieden forensische capaciteit voor het NIS2-eindverslag

MELDPLICHT IN 3 STAPPEN

STAP	TERMIJN	VEREISTE
Vroegtijdige waarschuwing	Binnen 24 uur	Eerste melding na bewustwording van significant incident
Vervolgmelding	Binnen 72 uur	Gedetailleerde informatie over incident en impact
Eindverslag	Binnen 1 maand	Volledige analyse, oorzaak, genomen maatregelen [7]

WIE VALT ONDER NIS2?

Organisaties in een gedekte sector (energie, zorg, finance, digitale diensten, productie, etc.) met 50+ medewerkers of EUR 10M+ omzet/balans. Geschatte impact: duizenden Nederlandse organisaties [16].

MDR als NIS2-bewijs

Een MDR-contract met rapportages over detecties, responstijden en genomen maatregelen is concreet bewijs van zorgplicht bij een toezichthouder. Het toont aan dat je 24/7 monitort, incidenten snel detecteert en actief reageert -- precies wat NIS2 vraagt.

8. MDR vs EDR vs SOC vs SIEM vs XDR

De afkortingen stapelen zich op. Dit overzicht maakt het verschil helder.

TERM	TYPE	SCOPE	WAT KRIJG JE
EDR	Technologie (tool)	Endpoints	Software die verdacht gedrag op apparaten detecteert. Je moet zelf reageren
XDR	Platform	Endpoints + netwerk + cloud + email + identiteit	Geintegreerde detectie over meerdere domeinen. Meer context, minder silos
SIEM	Technologie (tool)	Log-aggregatie over hele infra	Gecentraliseerd logbeheer en analyse. Vereist eigen analisten
SOC	Team/functie	Organisatiebreed	Beveiligingsteam dat monitort en reageert. Intern of extern
MDR	Managed service	End-to-end	SOC + detectie + actieve respons als uitbestede dienst [8]
MSSP	Managed service	Breed	Meer gericht op alerts doorgeven, minder op actieve respons

HOE VERHOUDEN ZE ZICH?

- **EDR** is tactisch -- een tool op je endpoints
- **XDR** is architectureel -- een platform dat meerdere domeinen integreert
- **SIEM** is een datalaag -- logs verzamelen en correleren
- **SOC** is een team -- mensen die de tools bedienen
- **MDR** is operationeel -- detectie + actieve respons + menselijke expertise als dienst
- **MSSP** is passief -- alerts doorgeven zonder actief in te grijpen

RESPONS-NIVEAUS

NIVEAU	WAT DE PROVIDER DOET	CLASSIFICATIE
Alert & Notify	Melding sturen	MSSP, geen echte MDR

NIVEAU	WAT DE PROVIDER DOET	CLASSIFICATIE
Alert & Advise	Melding + aanbevolen acties	Lichtste vorm MDR
Alert & Contain	Melding + automatische isolatie	Standaard MDR
Full Response	Complete incidentafhandeling incl. forensics en recovery	Premium MDR [12]

TIP

Kies minimaal "Alert & Contain" als je geen intern security-team hebt. "Alert & Notify" is geen MDR -- het is een duur alertingsysteem.

9. Trends 2025--2026

Drie ontwikkelingen die de MDR-markt de komende jaren vormgeven.

1. AI-driven detectie en autonomous response

AI versnelt de detectie van onbekende dreigingen en automatiseert containment-acties. Maar AI versnelt ook de aanval: AI-gestuurde malware past zich aan en AI-gegenereerde phishing is nauwelijks van echt te onderscheiden [17]. Het resultaat: MDR-providers investeren zwaar in AI-augmented SOC-analisten die sneller kunnen reageren dan ooit.

2. Platform consolidatie

De markt consolideert: MKB-bedrijven willen niet vijf losse security-tools maar een integrale dienst. MDR evolueert naar "managed XDR" -- een dienst die endpoints, cloud, netwerk, email en identiteit in een platform combineert. Daarnaast bieden steeds meer providers MDR + incident response als gecombineerd pakket.

3. MDR voor MKB wordt betaalbaar

Nieuwe toetreders richten zich specifiek op klein MKB met geautomatiseerde, AI-gedreven monitoring vanaf EUR 20/maand per bedrijf. De drempel om te starten met professionele 24/7 monitoring is lager dan ooit. De combinatie van AI-automatisering en schaalvoordelen maakt MDR toegankelijk voor bedrijven die het zich voorheen niet konden veroorloven [6].

WAT BETEKENT DIT VOOR JOU?

De MDR-markt groeit met meer dan 20% per jaar, de kwaliteit stijgt en de prijzen dalen voor MKB. Tegelijkertijd maakt NIS2 24/7 monitoring en incidentdetectie voor duizenden organisaties een wettelijke verplichting. 2026 is het jaar om MDR serieus te overwegen -- of je huidige oplossing te evalueren.

10. Aan de slag

MDR is de meest impactvolle cybersecurity-investering die je als MKB-bedrijf kunt doen. Drie stappen om te starten.

1. Bepaal je scope

Welke domeinen wil je monitoren? Alleen endpoints of ook cloud, netwerk en identiteit? Hoeveel endpoints heb je? Gebruik je Microsoft 365 of Google Workspace? De antwoorden bepalen welk type MDR bij je past en wat het gaat kosten.

2. Vergelijk op kwaliteit, niet alleen prijs

Gebruik de 10 vragen uit hoofdstuk 5 om aanbieders te vergelijken. Kijk naar de SLA, het responsniveau (Alert & Contain vs Full Response), de onboarding-doorlooptijd en de rapportage-mogelijkheden. Een MDR-dienst die EUR 10/endpoint/maand kost maar alleen alerts stuurt is duurder dan een dienst van EUR 25 die daadwerkelijk ingrijpt.

3. Start met een pilot

De meeste MDR-providers bieden een pilotperiode aan (30--90 dagen). Gebruik deze periode om te evalueren: hoe snel detecteren ze, hoe communiceren ze, hoe gedetailleerd zijn de rapportages? Een pilot geeft meer inzicht dan elke offerte.

Bronnenlijst

[1] **Meriplex / Forenova** -- Eigen SOC kost EUR 850K--1,13M/jaar: personeel, tooling, faciliteiten. meriplex.com/what-is-mdr/

[2] **Forrester / MSP2Day** -- ROI van MDR: 201% over 3 jaar, terugverdientijd < 6 maanden. msp2day.com/technology-and-innovation/de-waardepropositie-van-mdr-het-meten-van-de-echte-roi-op-security-investeringen/

[3] **Mordor Intelligence** -- MDR Market Size: USD 5,09 mrd (2026), CAGR 21,95%. NL cybersecurity-markt: USD 2,55 mrd (2026). mordorintelligence.com/industry-reports/managed-detection-and-response-market

[4] **IBM** -- Cost of a Data Breach 2025: gemiddelde breach lifecycle 277 dagen, kosten USD 4,45M. ibm.com/reports/data-breach

[5] **ESET / Hallo** -- Cybercriminaliteit kost MKB EUR 270.000 per incident. hallo.eu/kennis/blogs/cybercriminaliteit-kost-mkb-euro-270-000-per-incident/

[6] **MDRProviders.io / Attic Security / UnderDefense** -- MDR pricing: EUR 10--25/endpoint/mnd MKB, EUR 20/mnd klein MKB. mdrproviders.io/pricing

[7] **NCSC** -- Meldplicht Cyberbeveiligingswet: 24u/72u/1mnd. ncsc.nl/cyberbeveiligingswet-nis2/bereid-je-voor/meldplicht

[8] **Orange Cyberdefense** -- SOC, SIEM, MDR, EDR: what are the differences? orangecyberdefense.com/global/blog/managed-detection-response/soc-siem-mdr-edr-what-are-the-differences

[9] **Vodafone Business** -- 77% MKB cybercrime in afgelopen 2 jaar. vodafone.nl/zakelijk/inspiratie/mkb-doelwit-cybercrime-onderzoeken

[10] **Mandiant / Google Cloud** -- M-Trends 2025: dwell time 22 dagen EMEA. cloud.google.com/blog/topics/threat-intelligence/m-trends-2025

[11] **eSentire / LevelBlue / SECUINFRA** -- MDR onboarding: 3--10 dagen MKB, 6--12 weken enterprise. esentire.com/what-we-do/esentire-managed-detection-and-response

[12] **Sophos / Palo Alto Networks / Microsoft** -- MDR responsmodellen: Fully Managed, Co-Managed, Advisory. sophos.com/en-us/cybersecurity-explained/what-is-mdr

[13] **Red Canary / CyberMaxx** -- 5 common MDR mistakes: alert-only, black-box AI, integratie negeren. redcanary.com/blog/product-updates/5-common-mdr-mistakes/

[14] **SecurityScorecard / BlueVoyant** -- SLA-standaarden: detectie < 15 min, acknowledge < 30 min, respond < 1 uur. securityscorecard.com/blog/how-to-use-incident-response-metrics/

[15] **Networking4all** -- Impact meldplicht NIS2 op 24/7 monitoring en IR. networking4all.com/nl/nieuws/blog/post/impact-meldplicht-nis2-op-cybersecurity-de-noodzaak-van-24-7-monitoring-incident-response

[16] **Digitale Overheid** -- Cyberbeveiligingswet, verwacht Q2 2026, duizenden bedrijven. digitaleoverheid.nl/overzicht-van-alle-onderwerpen/cyberbeveiligingswet/

[17] **Banken.nl** -- 2026 wordt het jaar van geindustrialiseerde cybercriminaliteit en AI-agents. banken.nl/nieuws/26681/2026-wordt-het-jaar-van-geindustrialiseerde-cybercriminaliteit-en-ai-agents/

Deze gids is samengesteld door IBgids.nl op basis van openbare bronnen en marktonderzoek. Alle genoemde prijzen zijn indicatief (peildatum: maart 2026). IBgids.nl is een onafhankelijk platform en geen dienstverlener of adviseur.