Managed Detection en Response (MDR)

Doorlopende beveiligingsdienst: 24/7 bewaking, detectie en respons

DOCUMENT
Managed Detection en Response (MDR)

DATUM
Juni 2026

CLASSIFICATIE
Openbaar

VERSIE
V1.1 - Definitief

WAT IS MDR?

Managed Detection en Response (MDR) is een doorlopende beveiligingsdienst waarbij een extern Security Operations Center (SOC, een team van securityspecialisten) 24 uur per dag, 7 dagen per week jouw werkplekken, accounts en Microsoft 365-omgeving bewaakt op beveiligingssignalen, deze beoordeelt en bij een bevestigde dreiging ingrijpt.

De dienst is ingericht en uitgevoerd via een gespecialiseerde partner. Dynamic richt de koppeling in, is je vaste aanspreekpunt en wordt geïnformeerd bij incidenten.

MDR vult de geautomatiseerde beveiliging in je werkplek-pakket aan met menselijke bewaking. Het SOC neemt de beoordeling en respons uit handen, ook 's nachts, in het weekend en op feestdagen.

Wat zit erin

Bewaking

Het SOC bewaakt de beveiligingssignalen uit:

- De computers en servers van je medewerkers (endpoint-detectie)
- Je Microsoft 365-omgeving: aanmeldingen, accounts, mail en bestanden
- Je firewall, de overgang tussen je netwerk en het internet
- De virusbescherming op je apparaten

De bewaking gebruikt de signalen die je bestaande Microsoft-beveiliging (Defender) en je netwerkapparatuur afgeven. Er hoeft geen aparte apparatuur geplaatst te worden.

Detectie en beoordeling

- Het SOC verzamelt de meldingen, filtert de ruis en houdt over wat relevant is.
- Verdachte signalen worden door specialisten onderzocht en gecorreleerd, zodat losse gebeurtenissen die samen een aanval vormen herkend worden.
- Alleen bevestigde, hoog-prioritaire incidenten leiden tot actie of een melding aan jou.

Respons

- Bij een bevestigde aanval wordt een besmet apparaat geïsoleerd van het netwerk, zodat de dreiging zich niet verspreidt.
- Schadelijke processen worden gestopt, bijvoorbeeld bij ransomware die bestanden begint te versleutelen.
- Een geïsoleerd apparaat heeft tijdelijk geen netwerk- en internettoegang totdat de dreiging is opgeruimd.

Melding en rapportage

- Elk serieus incident komt als melding bij Dynamic binnen; wij pakken de opvolging met jou op.

- Periodiek ontvang je een rapportage met de signalen die zijn gezien, gefilterd en aangepakt.
- Beveiligingsgebeurtenissen worden bewaard voor onderzoek achteraf en als bewijslast bij een audit. De logging bevat technische gebeurtenissen, geen inhoud van berichten of bestanden.

Scope: wat het team niet inziet

Het SOC werkt op beveiligingssignalen, niet op de inhoud van je werk. De inhoud van mails, documenten en chats wordt niet gelezen en bestanden worden niet geopend. De verzamelde informatie wordt uitsluitend gebruikt voor het bewaken en afhandelen van beveiligingsincidenten.

Hoe het werkt in de praktijk

- **Health-check**. Controle of je Microsoft 365-omgeving en apparaten de benodigde signalen leveren.
- **Koppeling en uitrol**. De bewaking wordt op afstand geactiveerd op je werkplekken en je Microsoft 365-omgeving, via het beheer dat al in je pakket zit (Intune).
- **Overdracht aan het SOC**. Het SOC neemt de monitoring over en stemt de eerste periode af op jouw omgeving, zodat valse meldingen worden teruggebracht.
- **Doorlopende bewaking**. Vanaf dat moment bewaakt het SOC 24/7 en grijpt het in bij een bevestigde dreiging.

Voor wie

MDR past bij organisaties die:

- Onder NIS2 (de Europese cyberbeveiligingswet) vallen of als ketenpartner moeten kunnen aantonen dat detectie en respons 24/7 belegd zijn.
- Van een grote klant of toezichthouder de eis krijgen dat beveiliging continu bewaakt wordt.
- Werken met gevoelige gegevens of een verhoogd risico lopen en niet afhankelijk willen zijn van bewaking binnen alleen kantooruren.

Wat wij niet doen

- **Geen vervanging van een back-up**. MDR beperkt de schade door snel in te grijpen. Herstel na schade gebeurt vanuit de back-up, die standaard in je werkplek-pakket zit.
- **Geen volledige garantie**. MDR verkleint de kans en de schade van een aanval door snelle detectie en respons. Een sluitende garantie tegen elke aanval bestaat in security niet.
- **Geen vervanging van de beveiligingsbasis**. MDR bouwt voort op de beveiliging in je werkplek-pakket (Defender, conditionele toegang, updates) en komt daar bovenop.

Wat wij afspreken

Voor een goede samenwerking spreken we een paar dingen met je af.

- Een vast aanspreekpunt binnen jouw organisatie voor afstemming over meldingen en opvolging.
- Een vooraf afgesproken contactroute voor een ernstig incident buiten kantooruren.
- Toestemming om bij een bevestigde aanval direct in te grijpen, ook als een apparaat daarvoor tijdelijk wordt geisoleerd.

Verhouding tot de pakketten

- **Werkplek Compliant**: MDR is een standaard onderdeel van het pakket. De 24/7-bewaking onderbouwt de bewijslast die Compliant levert richting auditor of ketenpartner.
- **Werkplek Veilig**: MDR is een losse optie bovenop het pakket, voor organisaties die 24/7-bewaking willen zonder de volledige compliance-laag van Compliant.
- **Werkplek Modern**: MDR is niet beschikbaar.

Wat het kost

Binnen Werkplek Compliant is MDR onderdeel van de pakketprijs. Bij Werkplek Veilig wordt MDR als meerwerk afgenomen; de prijs staat in de offerte, per werkplek per maand bovenop het pakket.

CONTRACTUELE BASIS

Op deze dienst zijn de **Hoofdovereenkomst, Algemene Voorwaarden en Service Level Agreement (SLA)** van Dynamic ICT van toepassing. Voor deze dienst geldt **SLA A**. Als losse optie bij Werkplek Veilig geldt **SLA B.**

Standaard looptijd is **12 maanden.** Daarna loopt de overeenkomst door voor onbepaalde tijd, met **1 maand opzegtermijn.** Opzeggen doe je schriftelijk via INFO@DYNAMICICT.NL.