

# KPN Managed Detection and Response

Beveiliging die nooit slaapt



# Wat is KPN Managed Detection and Response?

**KPN Managed Detection and Response (MDR) is het 24/7 digitale alarmsysteem dat geavanceerde AI combineert met menselijke expertise vanuit het Nederlandse KPN SOC. Dreigingen worden direct gedetecteerd, gevalideerd en waar mogelijk opgelost. Jouw Business Partner houdt altijd de regie richting jou.**

## **Wat is het Nederlandse KPN SOC?**

Het KPN Security Operations Center (SOC) is het centrale team van security-experts dat 24/7 digitale omgevingen van klanten en netwerken bewaakt, verdachte activiteiten detecteert en analyseert, en bij dreigingen direct adviseert of ingrijpt om schade te voorkomen. Hierbij combineert het SOC geavanceerde detectietechnologie met menselijke validatie en neemt het bij kritieke incidenten de regie over door alerts te beoordelen, jouw partner te informeren en ondersteuning te bieden bij de juiste vervolgstappen, zodat organisaties continu beschermd en digitaal weerbaar blijven.

## **De voordelen van KPN MDR voor jou**

- Detectie binnen minuten in plaats van dagen
- Continuïteit van bedrijfsvoering, ook buiten kantooruren en in het weekend
- Rust en zekerheid: de organisatie hoeft zich niet bezig te houden met cyberdreigingen
- Aantoonbare verlaging van het risico op ransomware en datalekken door continue monitoring en snelle respons
- Snel live zonder gedoe: na je bestelling is je security-omgeving binnen 15 minuten volledig ingericht en actief, inclusief Microsoft Sentinel (SIEM)



# Hoe werkt KPN MDR?

**KPN Managed Detection and Response biedt continu beveiliging van de digitale werkomgeving. Met 24/7 monitoring worden werkplekken, Office 365-omgevingen en identiteiten actief bewaakt op verdachte activiteiten en dreigingen.**

KPN MDR werkt met meerdere security risiconiveaus. Bij de lage risiconiveaus is jouw Business Partner in control. Hoge risico's worden opgevolgd door KPN SOC.

Bij ernstige dreigingen neemt het KPN Security Operations Center de incidentbeoordeling en advisering over. SOC analyseert, valideert en ondersteunt jou direct bij de juiste vervolgstappen.

- KPN MDR onderneemt automatisch actie met AI waar mogelijk
- Eventueel worden aanvullende acties door jouw Business Partner uitgevoerd
- Jouw Business Partner bepaalt de opvolging richting jou

## Managed Detection

- 24/7 bewaking van de digitale omgeving
- Slimme detectie van verdachte activiteiten
- Menselijke validatie door security experts (SOC)

## Alerts & Response

- Directe response door AI
- Waarschuwing partner bij serieuze dreiging
- Optioneel: afnemen KPN Incident Response\*

## Insights

- Dashboard met inzicht in risico's, beveiligingsniveau en afgehandelde incidenten

\*KPN Incident Response is een los product, die je als optie bij KPN MDR kunt afnemen. Met KPN Incident Response MKB ben je verzekerd van specialisten die bij een cyberincident direct ingrijpen. De dienst biedt professionele analyse, containment en herstelbegeleiding, ondersteund door een vooraf opgesteld responseplan en gegarandeerde beschikbaarheid via de retainer. Vraag jouw Business Partner naar alle informatie en prijzen.

# In de praktijk

## 1 Onmogelijke reis

**Een medewerker logt 's ochtends in vanuit Frankrijk. Een uur later probeert “dezelfde medewerker” in te loggen vanuit Amerika.**

### Hoe KPN MDR dit ziet:

KPN MDR vergelijkt locatie, snelheid en device-gebruik en herkent dit als een identity-aanval.

### Welke actie volgt:

- KPN MDR blokkeert het account automatisch en zet een MFA-reset klaar.

### Effect voor de klant:

De aanvaller komt er niet in. De medewerker kan veilig opnieuw inloggen. Continuïteit blijft volledig behouden.

## 2 "MFA-fatigue" medewerkers krijgt tientallen MFA-pushes

**Een medewerker krijgt 's avonds ineens veel MFA- aanvragen, “wil je dit inloggen goedkeuren?”, terwijl hij nergens probeert in te loggen. Aanvallers hopen dat iemand in paniek of onoplettendheid op “ja” drukt.**

### Hoe KPN MDR dit ziet:

Het systeem herkent dit patroon als een MFA Fatigue Attack (MFA-bombardement).

### Welke actie volgt:

- MFA wordt opnieuw ingesteld
- Het account kan (tijdelijk) worden geblokkeerd
- Tokens worden ongeldig gemaakt

### Effect voor de klant:

De aanvaller kan niet via “per ongeluk goedkeuren” alsnog toegang krijgen.

## 3 Een laptop begint zich vreemd te gedragen

**Een medewerker merkt dat zijn laptop traag wordt. Zijn laptop begint ineens massaal bestanden te wijzigen en script-processen te starten, en vertoont ransomware achtig gedrag.**

### Hoe KPN MDR dit ziet:

Via signalen vanuit Microsoft Defender herkent KPN MDR ransomwaregedrag en koppelt deze aan eerdere afwijkingen.

### Welke actie volgt:

- Endpoint wordt automatisch geïsoleerd
- Kwaadaardige processen worden beëindigd
- Verdachte bestanden worden in quarantaine geplaatst

### Effect voor de klant:

Verspreiding wordt direct gestopt. De werkplek is veilig.

