

WHITEPAPER

Weerbaarheid in het AI-tijdperk

Van sneller veranderende cyberdreigingen naar concrete verdedigingsactie.

Digiweerbaar.nl

DE KERN VAN HET PROBLEEM

Cyberdreigingen veranderen door AI razendsnel

AI helpt aanvallers sneller kwetsbaarheden te vinden, aanvalstechnieken aan te passen en misbruik op te schalen. Daardoor blijft er minder tijd over om te bepalen: raakt dit ons en welke maatregel is nodig?

VAN MAANDEN NAAR UREN

Volgens de NCTV daalde de gemiddelde tijd tussen ontdekking en misbruik van een kwetsbaarheid van enkele maanden in 2024 naar enkele uren in 2026.

HET RISICOVENSTER WORDT KORTER



DIT IS HET RISICOVENSTER

De tijd tussen een relevante dreiging en een uitgevoerde maatregel.

HET PROBLEEM DAT DE RADAR OPLOST

Organisaties en MSP's moeten voortdurend weten welke dreigingen voor hen relevant zijn. De Cyber Dreigingsradar vergelijkt nieuwe dreigingen met het organisatieprofiel - zoals technologieën, leveranciers, sector en onderwerpen - en meldt wanneer er een match is.

Bron: NCTV, Cybersecuritybeeld Nederland 2026, 6 november 2026.

WAAROM AI DE DRUK VERHOOGT

AI maakt bestaande aanvalstechnieken sneller en schaalbaarder

AI automatiseert werk dat aanvallers voorheen grotendeels handmatig deden. Daardoor kunnen zij sneller doelwitten onderzoeken, zwakke plekken vinden en aanvalstechnieken aanpassen of herhalen.

WAT VERANDERT ER?

Sneller vinden

AI helpt aanvallers sneller kwetsbaarheden en doelwitten te vinden.

→

Sneller aanpassen

Aanvalscode en werkwijzen kunnen sneller worden aangepast.

→

Groter bereik

Aanvallen kunnen efficiënter en op grotere schaal worden uitgevoerd.

HET GEVOLG VOOR UW ORGANISATIE

De beschikbare reactietijd krimpt. Een proces dat dagen of weken nodig heeft, sluit niet meer aan op kwetsbaarheden die in uren kunnen worden misbruikt.

TECHNOLOGIE VERSNELT, MENSEN BESLISSEN

Mensen moeten nog steeds bepalen: zijn wij geraakt, wat heeft prioriteit en welke maatregel voeren we uit? Een kortere informatieketen helpt kostbare zoektijd te beperken.

Bronnen: NCTV, Cybersecuritybeeld Nederland 2026; NCSC, AI in de Cyber Kill Chain.

HET RISICOVENSTER

De tijd tussen dreiging en verdedigingsactie

Het risicovenster begint wanneer een dreiging relevant wordt en eindigt wanneer een passende maatregel is uitgevoerd. Niet iedere stap kan of moet worden geautomatiseerd. Wel kan onnodige zoektijd en overdracht worden beperkt.



RISICOVENSTER - doel: onnodige vertraging verkleinen

ONDERSTEUND DOOR DE RADAR

Melden op basis van het organisatieprofiel, mogelijke relaties zichtbaar maken en duiding en context toevoegen.

ORGANISATIE / MSP

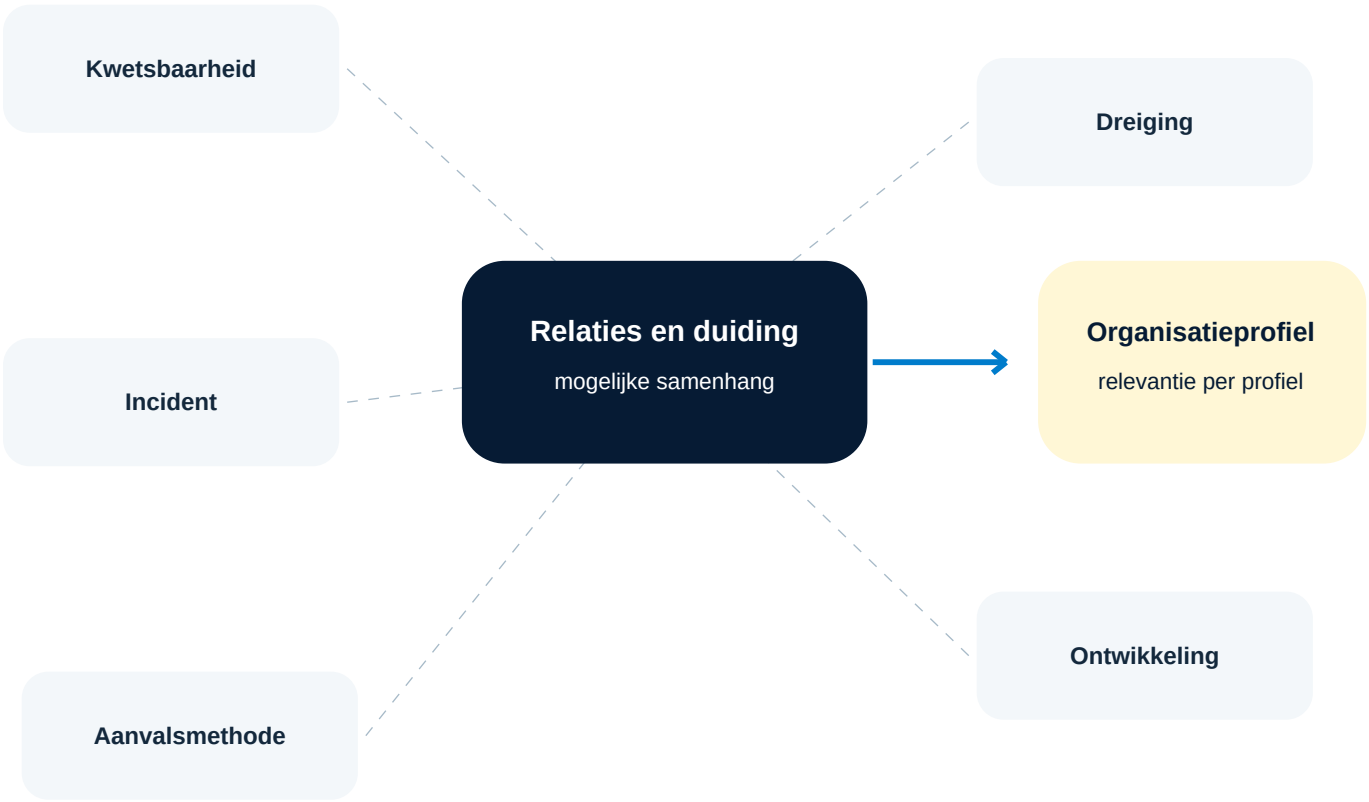
Prioriteren, besluiten, uitvoeren en controleren.

Deze figuur is conceptueel. Er worden geen gemeten doorlooptijden of gegarandeerde tijdsbesparingen geclaimd.

VAN LOSSE SIGNALEN NAAR SAMENHANG

Een afzonderlijk signaal vertelt niet altijd het hele verhaal

Een los bericht wordt pas waardevol wanneer het past bij uw omgeving. In het organisatieprofiel legt u technologieën, leveranciers, sector en onderwerpen vast. De Cyber Dreigingsradar koppelt nieuwe dreigingen aan dat profiel en meldt wat relevant kan zijn.



VAN INFORMATIE NAAR BEOORDELING

- Meldingen op basis van het organisatieprofiel.
- Meer houvast bij het beoordelen van relevantie.
- Een betere basis voor prioriteit en vervolgstappen.

Gestippelde lijnen tonen mogelijke relaties, geen bewezen causaliteit.

DE CYBER DREIGINGSRADAR

Van dreigingsinformatie naar handelingsperspectief

In het organisatieprofiel legt u technologieën, leveranciers, sector en onderwerpen vast. De Cyber Dreigingsradar vergelijkt nieuwe dreigingen met dit profiel en meldt wanneer er een match is. Vervolgens krijgt u duiding, samenhang en mogelijke acties.

WAARDEKETEN



WAT DE RADAR ONDERSTEUNT

- Meldingen op basis van het organisatieprofiel.
- Dagelijkse duiding.
- Relaties en acties.
- Dagelijkse en wekelijkse briefings.
- Strategische dreigingsanalyse.

WAT UW TEAM VERVOLGENS DOET

- Controleert of de organisatie werkelijk geraakt is.
- Beoordeelt impact en urgentie.
- Prioriteert de passende maatregel.
- Voert uit en controleert de opvolging.

Niet alles zelf volgen, maar op basis van uw profiel sneller zien welke dreiging aandacht vraagt en welke vervolgstap nodig is.

DE MENS BLIJFT IN CONTROLE

Inzicht uit de radar, verantwoordelijkheid bij de mens

De Cyber Dreigingsradar vervangt de ICT- of securityverantwoordelijke niet. De toegevoegde waarde ontstaat door dreigingsinformatie te combineren met menselijke beoordeling, organisatiekennis en uitvoeringskracht.

1	**Signaleren** Meldingen ontvangen op basis van het organisatieprofiel	RADAR
2	**Verbinden** Mogelijke relaties en samenhang zichtbaar maken	RADAR
3	**Duiden** Betekenis en context toevoegen	RADAR
4	**Prioriteren** Urgentie en impact beoordelen	MENS / MSP
5	**Handelen** Patchen, configureren en andere maatregelen uitvoeren	MENS / MSP

De radar ondersteunt het inzicht. De mens blijft eigenaar van het besluit en de uitvoering.

PRAKTIJKVERTALING VOOR MSP'S

Weten welke dreiging voor welke klant relevant kan zijn

Een MSP beheert klanten met verschillende technologieën, leveranciers en risicoprofielen. Met de juiste organisatieprofielen kan de radar signaleren welke dreigingen per klant relevant kunnen zijn. De MSP bepaalt vervolgens de werkelijke impact en actie.

ILLUSTRATIEF SCENARIO

Verschillende klanten gebruiken technologie van dezelfde leverancier. Er ontstaat een kwetsbaarheid. De radar meldt bij welke organisatieprofielen deze dreiging past. De MSP controleert daarna de exacte softwareversies en omgeving, bepaalt de prioriteit en plant passende maatregelen.

Illustratief scenario; geen claim van automatische klant- of versiedetectie.

ROLVERDELING

DE RADAR ONDERSTEUNT

- Meldingen per organisatieprofiel.
- Mogelijke relaties en context.
- Duiding en mogelijke acties.

DE MSP BEPAALT EN VOERT UIT

- Relevantie per klant.
- Urgentie en prioriteit.
- Patching of configuratiewijzigingen.
- Controle en communicatie.

De radar signaleert relevantie. De MSP vertaalt dit naar concrete klantactie.

ZAKELIJKE WAARDE EN ENTERPRISE

Een herhaalbaar proces voor organisaties en MSP's

De waarde ligt niet alleen in meer informatie, maar in een consistenter proces om informatie te beoordelen, te prioriteren en op te volgen.

Snelheid

Minder losse zoekstappen tussen informatie en beoordeling.

Samenhang

Dreigingen in een bredere context kunnen beoordelen.

Consistentie

Een vaste werkwijze voor signaleren, duiden en opvolgen.

Profielmatch

Gerichter zien welke dreiging bij een organisatie of klant past.

ENTERPRISE VOOR ONDER MEER MSP'S

Alles uit Elite, aangevuld met:

- Onderzoeken
- een onbeperkt intelligenceprofiel
- afspraken op maat
- prijs op aanvraag

Snelheid, schaalbaarheid en aantoonbaarheid zijn mogelijke voordelen. Zonder praktijkmetingen worden geen concrete besparingen of incidentreducties geclaimd.

CONCLUSIE

Verklein de afstand tussen weten en handelen

De Cyber Dreigingsradar vergelijkt actuele dreigingen met het organisatieprofiel en meldt wat relevant kan zijn. Relaties, duiding en context geven vervolgens een betere basis voor een passende verdedigingsactie, zonder de menselijke verantwoordelijkheid over te nemen.

VIJF VRAGEN VOOR UW HUIDIGE PROCES

- Hoe snel wordt een relevante dreiging herkend?
- Hoe worden mogelijke verbanden tussen signalen beoordeeld?
- Hoe wordt relevantie voor de organisatie of klant bepaald?
- Wie bepaalt de prioriteit en voert maatregelen uit?
- Hoe wordt opvolging aantoonbaar gemaakt?

Hoe groot is uw risicovenster?

Bespreek hoe de Cyber Dreigingsradar binnen uw organisatie of securitydienstverlening kan passen.

radar.digiweerbaar.nl

PUBLIEKE BRONBASIS

NCTV: Cybersecuritybeeld Nederland 2026, 6 november 2026.
NCSC: Artificial Intelligence in de Cyber Kill Chain, 6 oktober 2026.
Openbare abonnementeninformatie Cyber Dreigingsradar, meting 1 oktober 2026.

De observaties over AI zijn kwalitatieve constateringen van Digiweerbaar. Deze whitepaper bevat geen gekwantificeerde causaliteit of resultaatgarantie.