MASERO

CYBER SECURITY

Security Operations Center

Maximale zichtbaarheid, minimale risico's

Inhoud

Inleiding

Cyberdreigingen evolueren razendsnel. Bedrijven worden geconfronteerd met steeds geavanceerdere aanvallen, terwijl de impact van datalekken en verstoringen groter is dan ooit. Traditionele verdedigingsmethoden zijn vaak niet opgewassen tegen moderne dreigingen zoals ransomware, supply chain aanvallen en complexe phishing methodes. Daarbij zijn niet alleen grote bedrijven het doelwit: ook het MKB wordt steeds vaker slachtoffer. Uit recent onderzoek blijkt dat 1 op 5 bedrijven in Nederland in 2024 schade heeft geleden door cybercriminaliteit[1].

Tegelijkertijd neemt de snelheid waarmee incidenten zich ontwikkelen ook toe. Een succesvolle aanval kan zich al binnen enkele minuten verspreiden binnen het netwerk, met grote schade tot gevolg. Dat vraagt om een beveiligingsaanpak die niet alleen preventief werkt, maar juist ook proactief. Om de impact van een aanval zo minimaal mogelijk te houden, moeten verdachte activiteiten razendsnel worden gedetecteerd en aangepakt.

Daarnaast is de druk vanuit regelgeving sterker dan ooit. Met de invoering van de NIS2-richtlijn in de EU worden strengere eisen gesteld aan cybersecurity, risicobeheer en incidentmelding. Bedrijven moeten kunnen aantonen dat zij hun digitale weerbaarheid serieus nemen, en daar hoort een solide beveiligingsstrategie bij.

Kortom, het beveiligingslandschap is de afgelopen tijd fundamenteel veranderd en zal dat blijven doen. Alleen wie verder kijkt dan traditionele oplossingen is in staat zichzelf daadwerkelijk te wapenen tegen de dreigingen van vandaag en morgen.

[1]Bron: Cybertrends-rapport 2025, ABN AMRO

Van EDR naar XDR

Om in te kunnen spelen op de steeds complexere cyberdreigingen is het belangrijk om verder te kijken dan alleen endpoints. Traditionele endpoint security oplossingen bieden slechts een beperkt zicht op wat er écht gebeurt binnen de IT-omgeving. Daarom kiezen wij voor een krachtigere aanpak: XDR - Extended Detection and Response.

XDR maakt het mogelijk om beveiligingsdata vanuit verschillende bronnen samen te brengen. Denk daarbij aan endpoints, identiteiten, e-mail, servers, cloudomgevingen en netwerken. Door deze informatie te correleren, ontstaat er een compleet beeld van wat er speelt. Geen losse puzzelstukjes meer, maar één geïntegreerd beveiligingsbeeld.

Volledige zichtbaarheid

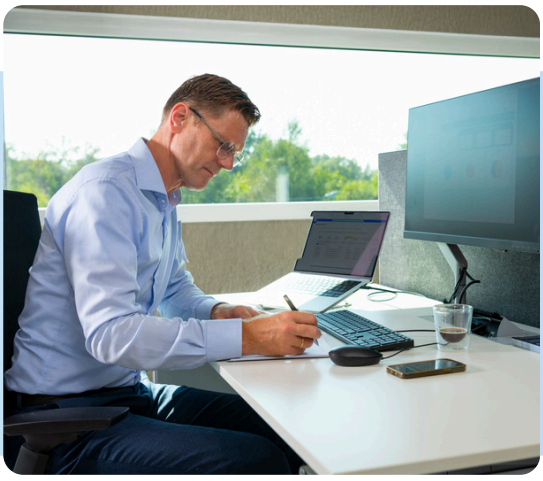
Het grootste voordeel van XDR is de volledige zichtbaarheid. Waar andere tools vaak incidenten in silo's analyseren, legt XDR verbanden tussen verschillende signalen. Een verdachte inlogpoging op een account, gecombineerd met een afwijkend netwerkpatroon of het openen van een schadelijk bestand, kan zo leiden tot een directe alert.

Sneller en effectiever

Bovendien stelt XDR onze analisten in staat om sneller en effectiever te reageren. Door de kracht van automatisering te combineren met menselijke expertise, kunnen we proactief dreigingen onderscheppen voordat ze schade aanrichten.

"Beveiliging begint bij het juiste inzicht. Met XDR als fundament creëren we een beveiligingsstrategie die meebeweegt en toekomstbestendig is."

Wilko Buijs, Operationeel directeur



Managed XDR

Beveiliging is geen individuele bezigheid. Het is een continu proces dat vraagt om expertise, technologie en samenwerking. Met onze Managed Extended Detection and Response (MXDR) dienst bieden we een krachtige combinatie van 24/7 monitoring, geavanceerde detectie en directe responsmogelijkheden - afgestemd op de behoeften van de klant én hun MSP.

Het Masero SOC

Onze MXDR-dienst is gebaseerd op de nieuwste Microsoft technologie en wordt bemand door een toegewijd team van securityspecialisten. Ons SOC bevindt zich in Veenendaal en is ISO 27001 gecertificeerd. We leveren:

- 24/7 monitoring van endpoints, identiteiten, cloud en netwerken
- Geautomatiseerde detectie en menselijke dreigingsanalyse
- Directe incidentrespons, afgestemd op jouw organisatie
- Heldere rapportages en doorlopende optimalisatie
- Samenwerking met interne IT-teams of IT-partner

Detectie & respons

Het SOC levert 24/7 detectie en respons vanuit een speciaal ingerichte SOC-ruimte. Afwijkende inlogpatronen worden gedetecteerd om zo misbruik van toegangsrechten en laterale bewegingen binnen netwerken te onderscheppen en ongeautoriseerde toegang vroegtijdig te stoppen. Alerts worden altijd onderzocht, tegenmaatregelen worden getroffen en escalaties worden indien nodig uitgevoerd. Incidenten worden direct door specialisten behandeld en alle activiteiten worden gedocumenteerd.

Managed XDR

Incidenten worden volgens een gestandaardiseerd proces opgevolgd. Wanneer een dreiging wordt gedetecteerd, voert het SOC een grondige analyse uit en wordt de ernst van de situatie bepaald. Indien nodig worden direct maatregelen genomen, zoals het isoleren van geïnfecteerde systemen of het blokkeren van verdachte activiteiten.

Het SOC gebruikt zowel geautomatiseerde playbooks als handmatige triage, categorisering en reactie bij incidenten. Analisten isoleren dreigingen door in te grijpen op netwerk-, endpoint- en identiteitsniveau. Nadat de dreiging is geïsoleerd, wordt de oorzaak onderzocht. Na validatie dat de dreigingen is weggenomen, worden systemen en identiteiten opnieuw in de omgeving geplaatst. Over deze processen worden duidelijke afspraken gemaakt.

Managed XDR

Integratie met Third-Party Security-oplossingen
De MXDR-dienst ondersteunt ook third-party security-oplossingen door koppelingen te maken met externe beveiligingslogs (zoals firewalls en netwerkapparaten) van verschillende leveranciers. Dit zorgt voor een flexibele en uitgebreide beveiligingsaanpak die aansluit op bestaande infrastructuren. Voordat externe logbronnen worden geïntegreerd, wordt vooraf gezamenlijk vastgesteld of er risico's zijn die deze integratie noodzakelijk maken.

Threat Intelligence en Threat Hunting
Om dreigingen sneller te detecteren en effectiever aan te pakken, maakt Masero gebruik van een open threat intelligence-platform (OpenCTI). Hiermee verzamelt, verrijkt en deelt Masero dreigingsinformatie uit diverse bronnen, waaronder publieke feeds, commerciële databronnen en en samenwerkingen met andere beveiligingsorganisaties. Dit biedt real-time inzicht in opkomende cyberdreigingen en stelt Masero in staat om direct te reageren op nieuwe aanvalstechnieken.

- **Onderzoek op basis van incidenten**
- **Automatische onderbreking van geavanceerde cyberaanvallen**
- **Zichtbaarheid van cyberaanvallenketen**
- **Automatisch herstel van getroffen assets**
- **AI en Machine Learning**

Onze keuze voor Microsoft

Onze SOC-dienstverlening is gebaseerd op Microsoft Sentinel en Microsoft Defender. De belangrijkste redenen voor onze keuze voor Microsoft lichten we hieronder verder toe.

Geïntegreerde beveiligingsoplossing

Sentinel en Defender vormen samen een krachtige en geïntegreerde suite van beveiligingsoplossingen. Sentinel fungeert als SIEM (Security Information and Event Management) en SOAR (Security Orchestration, Automation and Response) platform, terwijl Defender zich richt op het bieden van endpoint-, netwerk- en applicatiebeveiliging. Met de geïntegreerde Microsoft Security oplossing kunnen wij binnen de gehele IT-omgeving dreigingen detecteren, onderzoeken en erop reageren. Dit geldt voor zowel cloudomgevingen, on-premises systemen en hybride omgevingen. Masero maakt een koppeling met deze omgeving zodat de klantdata binnen de klantomgeving kan blijven, wat belangrijk is voor de GDPR.

Microsoft Solutions Partner
Security

Microsoft Solutions Partner Security

Masero is Microsoft Solutions Partner Security en daar zijn we trots op. Deze partnership vertegenwoordigt de hoogste erkenning voor beveiligingsspecialisten binnen het Microsoft ecosysteem. Deze certificering wordt toegekend aan organisaties die een hoog kennisniveau hebben van de Microsoft security oplossingen, de juiste certificering hebben en bewezen ervaring hebben met implementaties.

Gebruik van AI en machine learning

Sentinel maakt gebruik van AI en machine learning voor het analyseren van grote hoeveelheden data en het identificeren van verdachte activiteiten. Dit verhoogt de nauwkeurigheid van de detectie van dreigingen en helpt bij het verminderen van false positives.

Onze keuze voor Microsoft

Integratie met Microsoft 365 en andere Microsoft producten
Sentinel biedt naadloze integratie met Microsoft 365, Azure, Intune en andere Microsoft producten. Het kan gemakkelijk gegevens verzamelen, wat zorgt voor een efficiënte beveiligingsmonitoring.

Automation & Orchestration
Sentinel biedt uitgebreide mogelijkheden voor Automation & Orchestration van security operations. Dit maakt het mogelijk om veel voorkomende incidenten automatisch te detecteren en erop te reageren, waardoor de responstijd wordt verkort en onze SOC-specialisten zich kunnen focussen op complexere dreigingen.

Aansluiting op bestaande licenties
Om optimaal gebruik te maken van onze MXDR-dienst, is een passende Microsoft licentie noodzakelijk. Veel bedrijven hebben reeds Defender licenties in hun huidige licentie zitten (Business Premium of E3 en E5). Gebruik van andere (EDR) tools leidt tot dubbele kosten.

We adviseren je graag over de juiste licentiestructuur, zodat je optimaal profiteert van alle beschikbare functionaliteiten.

Identity-driven security

Moderne aanvalstechnieken zijn steeds vaker gericht op accounts en identiteiten. Daarom hebben wij gekozen voor een identity-driven aanpak binnen ons SOC.

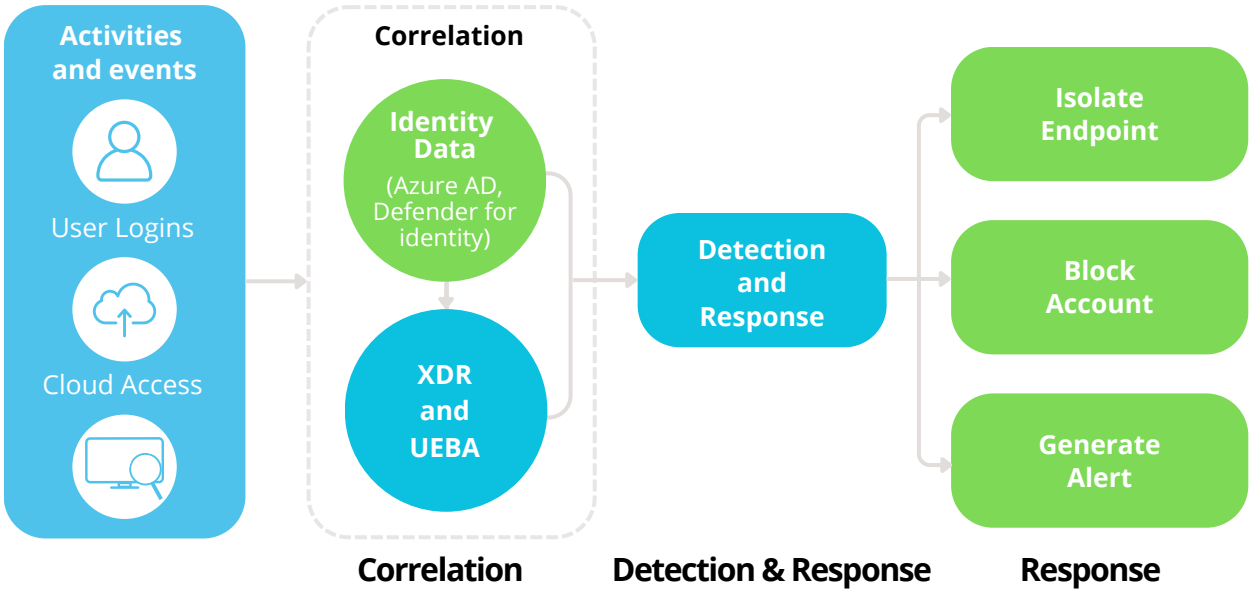
Identity is de nieuwe perimeter
Werknemers werken overal, op verschillende apparaten en netwerken. De enige constante factor is de Identity van de gebruiker.

80% van de aanvallen is gericht op de Identity
De meest succesvolle cyber-aanvallen zijn gericht op gebruikersaccounts, door middel van gestolen of gelekte inloggegevens.

Snellere detectie insider threats
Zowel opzettelijke insiders als gehachte accounts vertonen afwijkend gedrag. Een Identity-driven SOC is in staat dit vroeg te herkennen.

Inzicht in risico's en compliance
Een Identity approach helpt bij het maken van risicobeoordelingen en is voor compliance en auditing (ISO 27001, NIS2, GDPR) vaak een vereiste.

Identity-Driven Threat Correlation



Het proces

Een sterke beveiliging begint bij een gestructureerde samenwerking. We nemen onze klanten en partners stap voor stap mee in het proces, zodat de aansluiting op onze MXDR-dienst soepel en effectief verloopt. Onze aanpak is helder, voorspelbaar en afgestemd op de praktijk.

Onboarding - een stevige basis leggen

Een succesvolle samenwerking begint bij een zorgvuldige onboarding. In deze fase brengen we de IT-omgeving in kaart, richten we benodigde integraties in (zoals Microsoft Defender, Entra ID, Sentinel) en stemmen we ons af op de specifieke risico's en doelstellingen van jouw organisatie. We bepalen samen:

- welke bronnen worden gemonitord;
- welke risico's prioriteit hebben;
- de rollen en verantwoordelijkheden bij incidentresponse.

De onboarding is grotendeels geautomatiseerd, kan binnen een uur gerealiseerd worden en heeft geen verdere invloed op uw systemen. Direct na de onboarding starten we de daadwerklijke monitoring. Tijdens een inleerperiode wordt de omgeving en het verkeer dat daarin plaatsvindt in kaart gebracht en beoordelen we de cyberveiligheid. Ook bepalen we welke mogelijke verbeteringen kunnen worden doorgevoerd.

Detectie - 24/7 monitoring en analyse

Zodra de onboarding is afgerond, start de permanente monitoring van verdachte activiteiten. We combineren geautomatiseerde detectie met menselijke expertise. Onze SOC analisten onderzoeken meldingen, filteren false positives en houden voortdurend zicht op bedreigingen. Dankzij correlatie van signalen over systemen heen detecteren we complexe aanvallen sneller en preciezer. Je ontvangt alleen meldingen die ertoe doen, inclusief heldere duiding en aanbeveling.

Response - snel en effectief

Bij een incident telt elke seconde. Wij staan klaar om snel en doeltreffend te reageren: van containment maatregelen tot communicatie richting IT- of managementteams. We stemmen de response af op de mate van samenwerking met interne IT-teams of MSP's. Daarnaast ontvang je:

- duidelijke incidentrapportages
- aanbevelingen en ondersteuning bij vervolgstappen
- feedback voor structurele verbeteringen

Security Awareness

Als de techniek en de processen perfect zijn ingericht, is er nog altijd de menselijke factor. Deze is minstens zo belangrijk - en misschien wel het allerbelangrijkst voor een solide cybersecuritybeleid.

Cybercriminelen richten zich steeds vaker op het MKB en het is belangrijk dat je medewerkers zich bewustzijn van de risico's. De tijd dat een phishing mail makkelijk te herkennen was, is voorbij en de kans dat je op een verkeerde link klikt, is groter dan ooit. Daarom is het van cruciaal belang dat het beveiligingsbewustzijn binnen alle lagen van de organisatie versterkt wordt.

Waarom Awareness training cruciaal is

- 90% van de succesvolle aanvallen begint met phishing
- Medewerkers vormen de eerste verdedigingslinie
- Bewustwording vermindert de risico's op menselijke fouten

Security Awareness Training

Door middel van een op maat gemaakte Security Awareness training op locatie help je je medewerkers om cyberrisico's beter te leren herkennen. Ook leren ze in deze trainingen wat goede cyberhygiëne inhoudt en wat de huidige trends en ontwikkelingen zijn op het gebied van cybercriminaliteit.

Ook bieden we een doorlopende online trainingsmogelijkheid aan, waarbij regelmatig phishing simulaties worden rondgestuurd om te testen hoe scherp je medewerkers zijn. Aan de hand van interactieve trainingen wordt hun kennis aangescherpt en onderhouden, zodat ze de gevaren snel leren herkennen.

De voordelen voor je organisatie

- Verhoogde weerbaarheid: je medewerkers als eerste verdedigingslinie
- Voldoe aan normen en richtlijnen zoals ISO 27001, AVG en NIS2
- Verantwoordelijkheidsgevoel met betrekking tot digitale veiligheid
- Aanzienlijk kleinere kans op incidenten en datalekken

Waarom Masero

Masero is in 2020 opgericht met de missie om het MKB weerbaarder te maken tegen cyberaanvallen en meer grip te geven op cybersecurity. Dankzij onze jarenlange ervaring en opgedane kennis kunnen we enterprise level cybersecurity bieden tegen een betaalbaar kostenniveau.

Waarom bedrijven voor Masero kiezen:

- 24/7 bewaking door gepassioneerde securityspecialisten
- Gericht op nauwe samenwerking met IT-team en/of -partner
- Maximale zichtbaarheid als uitganspunt met Microsoft als basis
- Acteren als securitypartner: SOC, compliance en awareness
- Transparante en concurrerende prijsstelling
- Pragmatische no-nonsense aanpak

MASERO

CYBER SECURITY

www.masero.nl
info@masero.nl
(0318) 762 620

Citadel 28-1
3905 NK, Veenendaal
Nederland