Managed Extended Detection en Response

Beperk de impact van cyberbedreigingen door toevoeging van 24/7 beveiliging

De uitdaging

De cyberdreiging neemt jaarlijks in omvang en complexiteit toe, en veel bedrijven vinden het lastig om zichzelf voldoende te beschermen tegen een onvermijdelijke aanval en de nasleep daarvan. Waarom is het zo moeilijk? Wij denken dat het neerkomt op vier factoren:

1. **Gebrek aan zichtbaarheid**
   Potentiële bedreigingen kunnen onopgemerkt blijven waardoor een aanval zich kan voltrekken.

2. **Beperkte middelen**
   Internet IT-afdelingen ontberen de middelen of specifieke expertise om hun eigen cybersecurity te beheren.

3. **Complexiteit**
   Cybersecurityoplossingen kunnen complex te implementeren en beheren zijn, waardoor gespecialiseerde kennis en middelen noodzakelijk zijn.

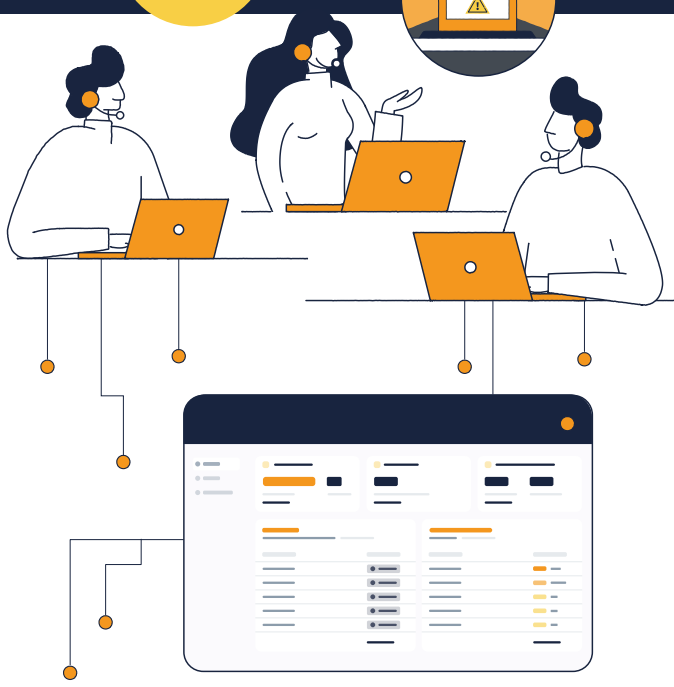
4. **Snel veranderende dreigingslandschap**
   Organisaties kunnen het snel veranderende dreigingslandschap niet bijhouden.

De oplossing

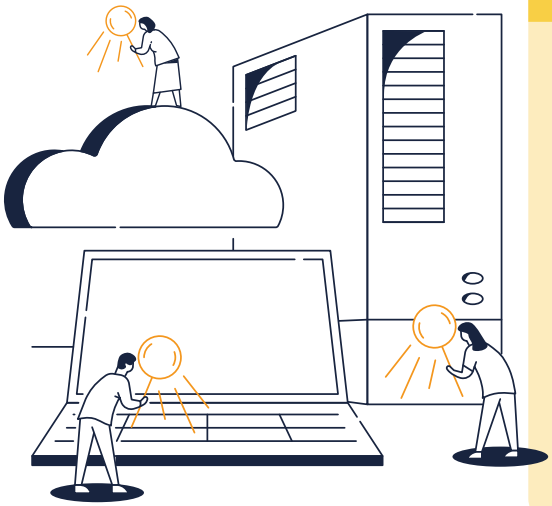
Wij beschermen jou van binnenuit en van buitenaf met een 24/7 Open XDR-oplossing en onze kennis en expertise om zo cyberdreigingen snel te kunnen identificeren en beheersen. Maar het bestaat uit veel meer:

Kenmerken

- Managed Extended Detection en Response (Managed XDR)
- 24/7 Security Operations Center (SOC)
- Attack Surface Management (ASM)
- Opsporen van bedreigingen
- Incident Response
- Management Reporting
- CISO-as-a-Service (inclusief jaarlijkse pentest en beveiligingsadvies)



Kenmerken



Managed XDR

Geavanceerd en ontworpen om endpoint- en cloudactviteiten in realtime te bewaken, helpt ons systeem bij het detecteren van, onderzoeken van en reageren op security-dreigingen op endpoint-apparaten zoals computers, laptops, servers en cloudomgevingen zoals Microsoft 365.

24/7 Security Operations Center (SOC)

Ons SOC is het zenuwcentrum waar ons 24/7 securityteam, bestaande uit doorgewinterde experts, beveiligings-dreigingen en -incidenten controleert, erop reageert en ze inperkt. Zie ons als een uitbreiding op jouw team.

Attack Surface Management (ASM)

Met menselijke expertise en een ultramoderne beveiligingsconfiguratie maken we jouw cybersecurity zo waterdicht mogelijk. We scannen voortdurend jouw aanvalsoppervlak en komen in actie wanneer we een kritieke kwetsbaarheid identificeren, zodat jij aanvallers te slim af kunt zijn.

Opsporen van bedreigingen

Onze threat intelligence-analisten controleren jouw systemen voortdurend op kritieke kwetsbaarheden en bieden vervolgens kennis, inzicht en aanbevelingen voordat hackers er misbruik van kunnen maken.

Incident response (IR)

Zelfs buiten kantooruren en wanneer u het meest kwetsbaar bent, kun je rekenen op onze allerbeste experts om je rugdekking te geven en jouw bedrijfscontinuïteit te garanderen. Managed XDR omvat bij incidenten 4 uur directe ondersteuning door het IR-team van Eye Security, dat 24/7 beschikbaar is per telefoon, e-mail en op locatie.

Eye Anti-Spoofing Tool (EAST)

EAST is onze geavanceerde cybersecurity-oplossing om spoofing van Microsoft-inlogpagina's tegen te gaan. De tool gebruikt bij het inloggen een aangepast CSS-bestand om onderscheid te maken tussen legitieme en malafide pagina's en voegt een visueel element om gebruikers te waarschuwen.

Het Eye-portal

Je wilt eenvoudige, begrijpelijke aanbevelingen – gelukkig hebben we het Eye-portal om u te sturen met een beschrijvende, intuïtieve interface zodat u snel kunt doen wat nodig is, op gebieden zoals endpoint en 2FA dekking en suggesties over hoe u cyberweerbaarheid te verbeteren.

CISO-as-a-service

We ondersteunen organisaties met jaarlijkse beoordelingen, uitgebreide cyberrisicoanalyses door middel van pentests en bieden daarnaast een helpdesk voor alle security gerelateerde vragen en advies over afwijkingen. Onze specialisten helpen je bovendien met uitdagingen op het gebied van governance en compliance.

Start met Managed XDR binnen 24 uur

1.

Intake en beoordeling – Starten is eenvoudig via een online platform. We kunnen vervolgens je beveiligingsstatus beoordelen en jouw incident en response-plan bespreken tijdens het intakegesprek met in- en externe stakeholders.

2.

Uitrol – Onze Managed XDR-dienst wordt uitgerold en binnen al enkele uren worden jouw systemen gemonitord. We gebruiken hiervoor een bewezen methode die geen verdere invloed heeft op uw systemen.

3.

Beschermd! – Onze software is actief. We kijken mee tijdens de eerste weken om te zien of zaken soepel verlopen. Na 2 maanden beoordelen we jouw cybersecurity en kijken we waar je mogelijk verbeteringen kunt doorvoeren.

Voordelen van Managed XDR

Agnostisch
Ons systeem integreert met de software van best-of-breed endpointsecurity-leveranciers:

Microsoft Defender · SentinelOne · CROWDSTRIKE

Afstemming met partners
Door afstemming met IT-dienstverleners (MSP's) zorgen we ervoor dat de implementatie op de juiste wijze wordt uitgevoerd.

Toezicht
We bewaken alle systemen, waaronder Windows, Linux en Mac, maar ook cloudomgevingen (Microsoft en Google).

Active Managed Reponse
Ons interne incidentresponse-team reageert op actieve dreigingen en biedt volledige ondersteuning totdat het incident opgelost is.

Ondersteuning
We bieden proactieve ondersteuning en zijn 24/7 beschikbaar om op aanvallen te reageren.

Deskundig advies
We bieden een jaarlijkse bijeenkomst, waarbij we interne en externe gegevensbronnen verder analyseren om jouw cyberweerbaarheid te verbeteren.

Waarom bedrijven voor Eye Security kiezen

1. Betaalbare, geavanceerde cybersecurity voor alle bedrijfsgroottes.
2. Doorgewinterde experts reageren snel op digitale dreigingen.
3. Door onze toegang tot systemen en data valt er een last van jouw IT-team
4. Volledig eigenaarschap van incidenten en transparante rapportage.
5. Eenvoudig te begrijpen inzichten voor verbeterde beveiliging.
6. Door verzekering gedekte bescherming zorgt voor uitgebreide aanvalsdekking.

Deze zes stappen helpen je cyberrisico's beter te beheren

Cyberrisico wordt gezien als een van de grootste bedreigingen voor bedrijven. Om de kans op een cyberaanval te minimaliseren, is het belangrijk om je bedrijf meer weerbaarder te maken. Hier zijn zes stappen om je op weg te helpen:

Multi-Factor Authenticatie (MFA)

Multi-factor authenticatie is een must voor iedereen die met een apparaat toegang heeft tot je netwerk.

Regelmatige updates en patches

Cruciale beveiligingspatches beschermen jouw bedrijf tegen aanvallen door bekende kwetsbaarheden in jouw software af te dichten.

Beveiligde back-ups en herstel

Back-upoplossingen zijn essentieel voor jouw bedrijf. Bij een aanval kan jouw bedrijf dan de back-up van het systeem gebruiken in plaats van een enorme som losgeld te betalen.

Getest Incident Responseplan

Hoewel het doel is om nooit slachtoffer van een cyberaanval te worden, is het belangrijk om je wel voor te bereiden op een mogelijk incident, zodat je de gevolgen kunt beperken.

Awareness-training voor werknemers

Regelmatige awareness-trainingen voor werknemers kunnen helpen teamleden leren om oplichting zoals zoals e-mailphishing te herkennen, en op de juiste manier te handelen.

Systeem- en cloudbeveiliging Configuratie hardening

Op je werkstations, servers en cloud moeten specifieke best practices voor beveiliging en configuratie zijn ingeschakeld.

Meer informatie?

Eye Security biedt een betaalbaar totaalpakket om uw cyberrisico direct beheersbaar te maken. Als je wilt onderzoeken hoe cyberweerbaar je eigenlijk bent, scan dan hier:

Eye Security is een cyberbeveiligingsbedrijf op abonnementsbasis dat haalbare cyberbeveiliging en verzekeringen levert voor Europese bedrijven. Met een groeiend team van beveiligings- en verzekerings-experts biedt Eye Security een hoogwaardige, betaalbare alles-in-één beveiligingsdienst door Managed Extended Detection and Reponse (MDR) en cyberverzekering te combineren. Eye Security is opgericht in 2020 en is actief in Europa met kantoren in Nederland, België, Duitsland en via zijn partners.

Bezoek eye.security