Hands on ICT
Your Security - Managed XDR

Een anticiperende incident & respons oplossing voor je IT Security

www.handsonict.nl

Managed XDR

Een proactieve cybersecurity

Met YourSecurity bieden wij diverse Managed Security diensten aan waarbij we beheer en beveiliging van je organisatie overnemen. Managed XDR (Extended Detection and Response) is hierin cruciaal.

Managed XDR biedt een geïntegreerde oplossing voor de detectie en respons op cyberdreigingen. We werken hiervoor samen met cybersecurity expert Eye. Met hun always-on Security Operating Center (SOC) en zeer ervaren team van cybersecurityspecialisten die 24/7 zorgen voor monitoring, onderzoek en herstel, zorgen we voor een continue bescherming van jouw IT-omgeving.

Het belang van Managed Security

Bescherming tegen bedreigingen van buitenaf is cruciaal omdat deze voortdurend evolueren en steeds geavanceerder worden. Cyberaanvallen kunnen leiden tot dataverlies, financiële schade, en reputatieschade. Ze kunnen bedrijfsactiviteiten verstoren en gevoelige informatie compromitteren, wat juridische en compliance-problemen kan veroorzaken. Een robuuste cybersecuritystrategie helpt deze risico's te minimaliseren door tijdige detectie en respons op dreigingen. Zonder adequate bescherming lopen bedrijven een aanzienlijk risico op kostbare en destructieve aanvallen.

Het verschil tussen een SOC en Managed XDR

Een Security Operations Center (SOC) richt zich vooral op het monitoren en detecteren van dreigingen. Managed XDR gaat verder. Dit door niet alleen te detecteren en dit in een portal weer te geven, maar ze reageren ook daadwerkelijk direct op incidenten. Dit betekent dat je niet alleen op de hoogte wordt gebracht van een dreiging, maar dat deze ook meteen wordt aangepakt.

"Wist je dat 5% van de bedrijven die starten met Managed XDR al een bestaande hack vindt, zonder dat organisaties zich hiervan bewust zijn?"

De uitdagingen van organisaties

Organisaties staan voor diverse uitdagingen als het gaat om cybersecurity.

Beperkte middelen

Veel IT-afdelingen hebben te maken met beperkte budgetten en middelen. Ze missen vaak de specifieke expertise en technologie die nodig zijn om een robuust cybersecurityprogramma op te zetten en te onderhouden. Dit resulteert in kwetsbaarheden die door cybercriminelen kunnen worden uitgebuit.

Snel veranderend dreigingslandschap

Het cyberdreigingslandschap verandert snel, met nieuwe en geavanceerde aanvallen die voortdurend opduiken. Het bijhouden van deze veranderingen en het aanpassen van beveiligingsmaatregelen vergt aanzienlijke inspanningen en middelen. Organisaties die dit tempo niet kunnen bijhouden, lopen een verhoogd risico op succesvolle aanvallen. Potentiële bedreigingen blijven vaak onopgemerkt, waardoor aanvallen zich ongehinderd kunnen voltrekken. Zonder volledige zichtbaarheid kunnen IT-teams geen effectieve verdediging opzetten tegen dreigingen die ze niet kunnen zien.

Complexiteit

Moderne cybersecurityoplossingen zijn vaak complex om te implementeren en te beheren. De integratie van verschillende beveiligingstools en -systemen vereist gespecialiseerde kennis en voortdurende aandacht, wat een uitdaging kan zijn voor organisaties zonder voldoende interne expertise.

Gebrek aan zichtbaarheid

Potentiële bedreigingen blijven vaak onopgemerkt, waardoor aanvallen zich ongehinderd kunnen voltrekken. Zonder volledige zichtbaarheid kunnen IT-teams geen effectieve verdediging opzetten tegen dreigingen die ze niet kunnen zien.

Managed XDR met Eye Security

Hands on ICT werkt samen met Eye Security, een toonaangevende partner in cybersecurity. Eye Security, opgericht in 2020, heeft kantoren in Nederland, België, en Duitsland, en richt zich op het bieden van geavanceerde beveiligingstechnologieën en expertise. De oprichters van Eye Security hebben een security achtergrond bij de AIVD en MIVD waarbij ze de expertise hebben omgezet naar een oplossing voor de business. Met een groeiend team van beveiligingsspecialisten levert Eye een allesomvattende Managed XDR-oplossing voor detectie en respons. Eye Security is officieel erkend door het Nationaal Cyber Security Centrum (NSCS). Met deze samenwerking van diepgaande expertise kunnen we jouw IT-omgeving continue beschermen tegen cyberdreigingen.

Hoe Managed XDR werkt

Managed XDR van Eye Security biedt een uitgebreide aanpak voor cybersecurity. Het proces begint met een intake en beoordeling van de huidige beveiligingsstatus en coördinatie van het incident response plan. Binnen 24 uur wordt de Managed XDR-dienst geïmplementeerd. Eye Security integreert met top leveranciers van endpoint-security zoals Microsoft Defender en gebruikt Microsoft Sentinel SIEM indien nodig.

Hands on ICT en Eye Security werken nauw samen om een correcte implementatie te garanderen. We bewaken alle systemen, waaronder Windows, Linux, Mac en cloudomgevingen zoals Microsoft Office. Het forensische team van Eye Security reageert direct op actieve dreigingen en biedt volledige ondersteuning totdat het incident is opgelost. Daarnaast levert Eye Security ondersteuning bij acute situaties en dringende vragen over cyberveiligheid. Jaarlijks geven ze deskundig advies om de cyberweerbaarheid verder te verbeteren door zowel interne als externe data te analyseren. Maandelijkse rapportages geven aanbevelingen voor netwerkbeveiliging. Deze rapportages kun je terugvinden op de Eye-portal.

Wat zit er in Managed XDR

Extended Detection and Response (XDR)

Een team van specialisten helpt jouw organisatie dag en nacht bij het detecteren, onderzoeken en oplossen van beveiligingsdreigingen op endpoints zoals computers, laptops, servers en cloudomgevingen zoals Microsoft 365. Real-time monitoring identificeert ongebruikelijke of verdachte activiteiten effectief.

Security Operating System (SOC)

Het Security Operating System (SOC) biedt continu toezicht door een team van ervaren beveiligingsexperts die dag en nacht jouw IT-omgeving monitoren. Dit zorgt voor een snelle detectie en reactie op dreigingen, waardoor jouw systemen altijd beschermd zijn.

Attack Surface Management (ASM)

ASM houdt jouw IT-infrastructuur voortdurend in de gaten en identificeert kwetsbaarheden voordat cybercriminelen deze kunnen uitbuiten. Deze proactieve benadering zorgt ervoor dat potentiële zwakke plekken snel worden aangepakt en gedicht.

Active Managed Response

Het interne forensische team staat klaar om onmiddellijk te reageren op actieve dreigingen. Ze bieden volledige ondersteuning tijdens een incident en zorgen ervoor dat alle problemen snel en effectief worden opgelost.

Vulnerability Hunting

De threat intelligence-analisten controleren jouw systemen voortdurend op kritieke kwetsbaarheden. Ze bieden volledige ondersteuning om deze kwetsbaarheden te mitigeren voordat aanvallers hiervan kunnen profiteren.

Incident Response

Bij escalatie biedt de Managed XDR-oplossing vier uur directe ondersteuning door het Incident Response-team. Het forensische team is 24/7 beschikbaar via telefoon, e-mail en op locatie.

Het Incident Response Team

Wanneer jouw organisatie getroffen wordt door een cyberincident, kunnen de gevolgen ernstig zijn, zoals gelekte bestanden, stilstaande operaties of grote financiële verliezen. In zo'n situatie komt er veel op je af, vaak met zaken waar je geen ervaring mee hebt. Bij escalatie biedt deze Managed XDR-oplossing 4 uur directe incident-ondersteuning door het Incident Response-team. Dit team is 24/7 beschikbaar via telefoon, e-mail en op locatie voor forensische hulp. Hier hoeft niet apart voor betaald te worden. De gemiddelde reactiesnelheid op een incident is 4 minuten.

De cyberspecialisten hebben jarenlange ervaring opgedaan bij onder andere de AIVD en MIVD, en behoren tot de top van de cybersecuritywereld. Ze zijn gewend aan complexe digitale aanvallen en weten precies hoe ze moeten handelen om de situatie snel onder controle te krijgen. Hun prioriteit is dan ook om jouw systemen zo snel mogelijk weer veilig online te krijgen, met minimale verstoring van de bedrijfsvoering.

De Managed XDR-portal

In principe hoor je niets over de security incidenten aangezien deze in de meeste gevallen op de achtergrond voor je worden opgelost door Eye. Ben je toch geïnteresseerd in wat er in je IT-omgeving gebeurt aan incidenten? Dan kun je in de Portal altijd terugvinden welke incidenten zijn gedetecteerd en opgelost door het team van Eye. Daarnaast krijg je in de portal inzichtelijke rapportages zoals endpoint- en MFA-dekking en aanbevelingen om jouw beveiliging continue te verbeteren.

CISO-as-a-service

Additioneel vindt er jaarlijks een overleg met Eye security, Hands on ICT en jouw IT-security team. Dit overleg staat in het teken van een cyberrisicobeoordeling van jouw organisatie. Hierin krijg je als klant inzicht in welke maatregelen er genomen moeten worden om de cyberweerbaarheid te verhogen.Daarnaast is er een helpdesk voor alle beveiligingsgerelateerde vragen en advies. De specialisten zijn als extra dienst beschikbaar om je te helpen met uitdagingen op het gebied van governance en compliance.

Managed XDR in 4 stappen

Van onboarding tot in gebruikname, hieronder vind je de stappen die we gaan ondernemen om Managed XDR voor je aan te zetten.

Stap 1 - Expert intake

De eerste stap die gezet moet worden is de intake om Managed XDR in te regelen én het incident respons plan vorm te geven. Vragen die door ons gesteld gaan worden zijn o.a.:

- Hoe ziet jullie huidige (security) situatie eruit?
- Zitten er op dit moment cruciale gaten in jullie beveiliging en hoe spelen we hierop in?
- Met wie wordt op welk moment contact opgenomen als een incident plaatsvindt?

In de regel willen al onze klanten dat elk incident direct wordt opgepakt, ongeacht of het incident in de nacht of op een feestdag zoals Kerstavond plaats vindt. Een aantal uur vertraging in responstijd kan namelijk al zorgen voor grote schade. In het incident response plan worden deze zaken allemaal doorgenomen.

Stap 2 - Threat session

Na de intake sessie zal er een Threat session uitgevoerd worden. Dit is een assessment op jullie IT-omgeving om te kijken of je wellicht al gehackt bent. In 5% van de gevallen blijken organisaties namelijk al gecomprimeerd te zijn zonder dat ze dit zelf doorhebben. Deze hacks zullen direct door de security experts van Eye worden opgepakt en verholpen.

Stap 3 - Start implementatie

Na de intake en de threat session zal het daadwerkelijk implementeren van het Managed XDR platform plaatsvinden.

Managed XDR plugt hierbij in op jullie EDR, Cloud en Microsoft omgeving (min. Defender for Endpoint P2 licentie voor nodig). Door deze combinatie heeft Eye zeer goed overzicht van alles wat er gebeurt in je omgeving en is daardoor in staat zeer snel incidenten te identificeren én op te lossen.

Voor de implementatie hoef je verder niets te doen. Heeft Hands on ICT je IT-omgeving al in beheer, dan kan bijna alles geïmplementeerd worden zonder dat je er iets van merkt. Zowel de intake als de threat session en het implementeren kan al binnen 24 uur worden afgerond.

Stap 4 – Ongoing 24/7 security

Alle sensoren zijn actief, de 24/7 security monitoring, detect en respons tooling draait.

Twee maanden na de implementatie zal er een cybersecurity-evaluatie plaatsvinden, waar ze aan de slag gaan met het verder verkleinen van jullie aanvalsoppervlak.

De voordelen van Managed XDR

Managed XDR biedt IT-managers 24/7 monitoring en bescherming, snelle detectie en respons op dreigingen, en ontlast het interne team. Het integreert geavanceerde technologieën met specialistische expertise voor een robuuste beveiliging, zorgt voor naleving van compliance-eisen en geeft continue verbeteringsadviezen, waardoor bedrijfscontinuïteit gewaarborgd wordt.

- 24/7 **toezicht en bescherming** en directe reactie op cyberdreigingen.
- Doorlopende en **proactieve scanning** en beheersing van jouw aanvalsoppervlak.
- Directe **incident response** bij incidenten met ondersteuning van experts.
- Duidelijke en begrijpelijke **rapportages** via het Managed XDR portal.
- Toegang tot **expertise en advies** op het gebied van cybersecurity en compliance.

Pricing

Voor de intake, de threat session en de implementatie van Managed XDR worden onboardingskosten gerekend. Deze kosten zijn afhankelijk van het aantal medewerkers binnen je organisatie en zijn eenmalig.

De maandprijs van Managed XDR wordt gebaseerd op het aantal endpoints. Dat wil zeggen; Windows, laptops, desktops en/of servers binnen je organisatie. Onze ICT-consultants kunnen vooraf een scan draaien om het exact aantal hiervan te inventariseren. Aan de hand daarvan kan de offerte voor je worden opgemaakt. Managed XDR kan voor minimaal een jaar worden afgenomen of voor 3 of 5 jaar. De facturatie zal per kwartaal plaatsvinden, op basis van de daadwerkelijk actief gekoppelde endpoints.

Systeemeisen & voorwaarden

Voor de inrichting van Managed XDR worden een aantal voorwaarden gesteld zodat ook daadwerkelijk een juist securityniveau gehaald kan worden:

- Je organisatie heeft minimaal Microsoft Defender for Endpoints Plan 2. Deze is los verkrijgbaar per user per maand, als E5 Security Add-on op Microsoft 365 E3 of de licentie maakt onderdeel uit van Microsoft 365 E5.
- Multi Factor Authentication (MFA) is volledig ingericht voor alle gebruikers in jullie organisatie; en regulier update van devices zijn ingeregeld.

Wil je graag advies over de aankoop van de licenties of inrichting van deze eisen, neem dan contact met ons op voor vrijblijvend advies.

Additioneel: de cybersecurityverzekering

Eye Security biedt daarnaast een cybersecurityverzekering aan waarbij de kosten voor incident response, schadeherstel en bedrijfsonderbreking worden gedekt. Dit biedt gemoedsrust en zorgt ervoor dat jouw bedrijf snel kan herstellen na een aanval, zonder onverwachte uitgaven. Met deze verzekering ben je verzekerd van zowel financiële als operationele ondersteuning bij cyberincidenten, wat cruciaal is voor de continuïteit en veiligheid van je organisatie.

Veel verzekeraars bieden geen cybersecurityverzekering óf tegen hoge kosten door een hoog risicoprofiel. Dit is vooral het geval voor branches die veel risico lopen zoals logistiek of productie. Door gebruik te maken van Managed XDR in combinatie met de verzekering van Eye kun je gebruik maken van gunstigere tarieven en minimaliseer je de financiële impact van een aanval. Deze verzekering kan via Hands on ICT aangevraagd worden.

yoursecurity

Managed XDR: Onderdeel van YourSecurity

Met YourSecurity bieden we een scala aan diensten en producten om ervoor te zorgen dat je altijd en overal veilig aan het werk bent en dat bedrijfsdata goed geborgd is. Een belangrijk onderdeel hiervan is Managed Security waarbij we beheer en beveiliging van IT-systemen en netwerken overnemen.
Dit omvat een breed scala aan beveiligingsdiensten en -oplossingen die continu worden beheerd en bewaakt om dreigingen te detecteren, te voorkomen en erop te reageren.

Meer informatie

Contactgegevens
Hands on ICT
info@handsonict.nl
www.handsonict.nl
+31(0)88 - 181 1300

Weesp
Nesland 5a
1382 MZ Weesp

Zwolle
Schrevenweg 5
8024 HB Zwolle

Venlo
Prinsessesingel 20-26
5911 HT Venlo

Wormerveer
Vrijheidweg 38
1521 RR Wormerveer