Microsoft Defender XDR managed by Inetum

Cybersecurity-inzicht omgezet in actie

inetum

In de security-wereld vliegen de acroniemen ons weleens om de oren. Zo gingen we van AV naar EPP naar EDR en nu XDR. Deze veranderende technologieën zijn dan ook een noodzaak om threats continu een stap voor te blijven. Niet altijd evident om bij te blijven en ook tijdig de gepaste acties te nemen om een incident te voorkomen. Met onze nieuwe managed Microsoft Defender XDR bieden we niet alleen inzicht in de gevaren die uw IT-omgeving bedreigen, maar ook 24/7-monitoring van en respons op incidenten.

Het aantal cyberaanvallen blijft toenemen. De vraag is niet of ook u ermee geconfronteerd wordt, maar wanneer precies. Gelukkig zijn de meeste bedrijven zich intussen bewust van die **toenemende cyberdreiging** en proberen ze zich zo goed mogelijk tegen cybergevaren te wapenen. En mochten ze dat uit eigen beweging nog niet doen, dan is er altijd nog de groeiende druk van externe regelgevers.

NIS2 als gamechanger

Overheden, met de Europese Unie op kop, leggen bedrijven steeds meer eisen op, ook inzake cybersecurity. Een treffend voorbeeld is de uitgebreide Europese NIS2-richtlijn. Die zal de komende jaren als hefboom en accelerator dienen voor allerlei noodzakelijke investeringen in cybersecurity. Die moeten bedrijven helpen om ook op dat vlak een gemeenschappelijk minimumniveau of **veilige ondergrens** te bereiken.

NIS2 wordt in eerste instantie van kracht voor 180.000 bedrijven uit 18 sectoren binnen de Europese Unie. De kans is reëel dat uw bedrijf daartoe behoort – of deel uitmaakt van de supplychain van die organisaties. In dat geval zal ook u een aantal maatregelen moeten nemen om uw risico's op het gebied van cybersecurity voldoende te beheersen, incidenten zoveel mogelijk te voorkomen of de gevolgen ervan zoveel mogelijk te beperken.

Inzicht verwerven

Concreet gaat het om maatregelen in tien cybersecuritydomeinen. Een van die domeinen is **incidentafhandeling**: de **preventie en detectie van cyberincidenten en de reactie erop**.

Het goede nieuws is dat er tegenwoordig heel wat oplossingen op de markt voorhanden zijn die u bij die incidentafhandeling kunnen ondersteunen. Een van de bekendste is ontwikkeld door Microsoft. Met Microsoft Defender XDR verwerft u in de eerste plaats een beter inzicht in de talrijke gevaren die uw IT-omgeving bedreigen.

Maar er is ook minder goed nieuws. Bedrijven beschikken niet altijd zelf over het nodige personeel en de vereiste expertise om zo'n oplossing te implementeren en er vlot mee te werken. Investeren in die **gespecialiseerde kennis en profielen** is niet alleen duur, ze zijn ook gewoon heel moeilijk te vinden op onze arbeidsmarkt.

Microsoft Defender XDR: een betere kijk op gevaar

XDR (eXtended Detection and Response) breidt de basismogelijkheden van EDR (Endpoint Detection and Response) uit om **meer dan alleen eindpunten** te beschermen. Zo kan u met Microsoft Defender XDR ook uw **hybride identiteiten, e-mail, samenwerkingstools, apps en cloudomgeving** beveiligen, over **verschillende platformen** heen. De oplossing beperkt zich met andere woorden niet tot het Microsoft-platform alleen en strekt zich uit over uw gehele infrastructuur.

Doordat Microsoft Defender XDR de opname, analyse en workflows van beveiligingsdata stroomlijnt, vergroot de zichtbaarheid van verborgen en geavanceerde bedreigingen. De **betere en bijkomende inzichten** die u zo verwerft, helpen u om tijdig en gepast op die bedreigingen te reageren, al dan niet automatisch.

Actie ondernemen

Daar kunnen wij als **vertrouwde IT-partner** met onze **gecertificeerde Microsoft- en security-experts** het verschil voor u maken. Temeer omdat de implementatie van een oplossing als Microsoft Defender XDR niet volstaat, net zomin als het verwerven van inzichten via die oplossing.

Rapporten en automatische 'alerts' of waarschuwingen alleen volstaan niet. U moet ook **tijdig de gepaste acties** kunnen nemen om een incident te voorkomen of er succesvol op te reageren en zo ergere schade te vermijden. En dat moet bovendien **de klok rond** gebeuren, ook 's nachts en in het weekend.

XDR als managed service

Ook daarvoor heeft u misschien de mensen en de middelen niet in huis. Geen zorg: net daarom bieden wij u die onmisbare en op termijn - wie weet - zelfs verplichte incidentafhandeling nu ook als een **managed service** aan.

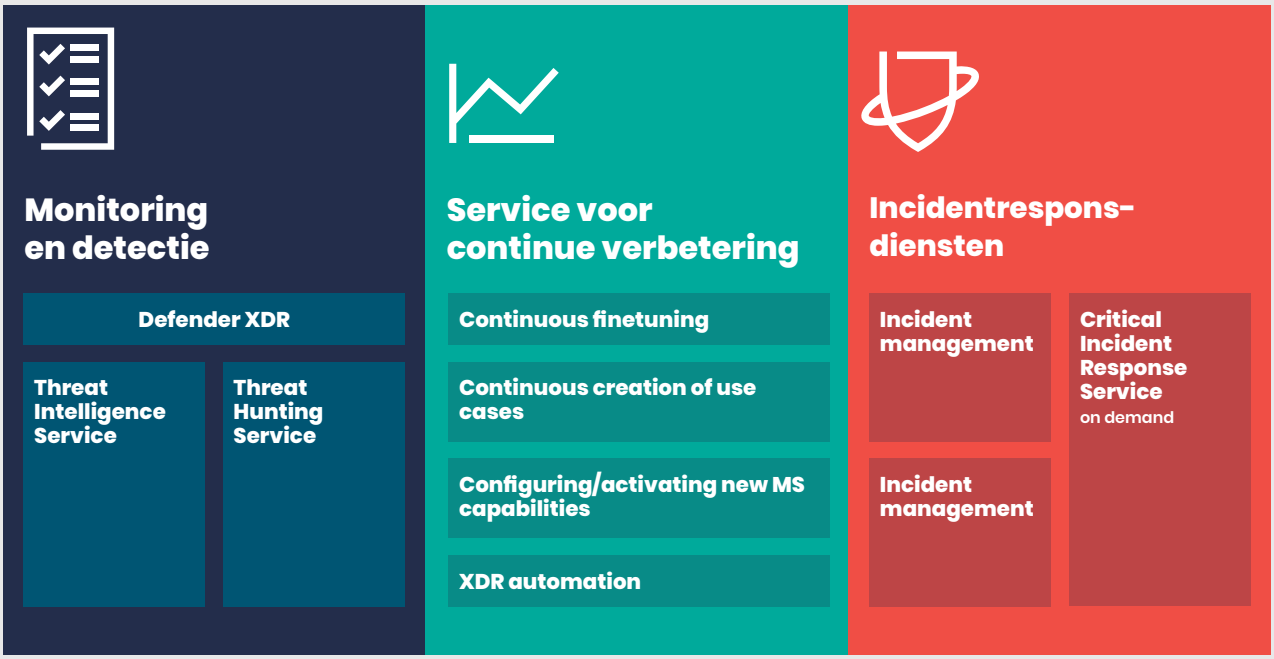
Die nieuwe managed service is gebaseerd op de bestaande oplossing van Microsoft voor eXtended Detection and Response (XDR), met inbegrip van het kritieke 'Incident Response'-luik. Ons eigen internationale **Security Operations Center (SOC)** staat daarbij garant voor **monitoring van en respons op incidenten, de klok rond.**

Tegelijk geniet u van de voordelen van een **lokale, nabije IT-partner** voor de eigenlijke implementatie van de XDR-oplossing. Een partner die uw ruimere IT-omgeving mee in rekening neemt. Zo kan u ook van deze nieuwe managed service gebruikmaken als uw omgeving niet hoofdzakelijk op Microsoft-technologie is gebaseerd.

Inetum LiveSOC MDR Service

Wij beschikken over een **netwerk van hoog gecertificeerde SOC's op drie locaties**. Doordat onze SOC's op gecoördineerde wijze en met hoge beschikbaarheidsprocedures werken, kunnen wij u de correcte levering garanderen van al onze diensten.

Onze dienst voor **Managed Detection and Response (MDR)** omvat verschillende diensten die elkaar aanvullen en voeden:



Meer weten?

Ook managed services zijn **maatwerk**. Uw bestaande IT-omgeving, de licenties waarover u al beschikt, uw maturiteit op het vlak van cybersecurity: al die elementen bepalen mee de dienstverlening die wij u kunnen bieden, altijd op maat van uw omgeving en organisatie.

Benieuwd wat wij voor u kunnen betekenen? Onze experts zoeken het samen met u uit. Via onze Cybersecurity Roadmap bepalen we de maturiteit van uw cyberbeveiliging en geven we aanbevelingen om uw risico's te minimaliseren. In lijn met de NIS2-regelgeving. Zij informeren u ook graag over andere diensten die wij u kunnen bieden.

Microsoft

Inetum
A. Vaucampslaan 42
1654 Huizingen, België
+32 2 801 55 55
www.inetum-realdolmen.world
info@inetum-realdolmen.world

inetum