unica ict solutions & Microsoft

E-book

Geef je beveiligings-activiteiten een boost met XDR.

Wij zijn er, altijd.

De huidige stand van zaken op het gebied van de veiligheidsoperaties

Toenemende frequentie, snelheid en verfijning van bedreigingen

Het huidige cyberbeveiligingslandschap kent nog steeds een toename van het aantal aanvallen in alle categorieën; meer phishing, meer ransomware-campagnes, meer identiteitsgerichte bedreigingen en ook een toename in de snelheid daarvan. Nu de Ransomware-as-a-Service (RaaS) economie in opkomst is, kan iedereen nu de beschikking krijgen over tools die zijn ontwikkeld door de meest productieve nationale aanvallers in de cyberwereld, waardoor hun slagingspercentages en schaalbaarheid toenemen.

Op zichzelf staande oplossingen vertragen de respons

Het is niet langer voldoende om alleen endpoints te beschermen en een volledig aparte e-mailbeveiligingsstrategie te hebben. Aanvallen richten zich op de gaten tussen deze geïsoleerde pointoplossingen en doorkruisen meerdere domeinen, waardoor verdedigers individuele waarschuwingen handmatig met elkaar moeten correleren om een bredere aanval te detecteren. Geavanceerde aanvallen vinden plaats via e-mail en endpoints, helemaal tot aan gebruikersidentiteiten, cloudapplicaties en uw gegevens. Bij een endpoints oplossingsstrategie moeten beveiligingsanalisten handmatig waarschuwingen met elkaar in verband brengen om aanvallen te identificeren, omdat ze nooit het grote geheel zien. Dit vertraagt niet alleen de detectie, maar ook het onderzoek en de sanering.

Volgens een onderzoek van Gartner worden besluitvormers op het gebied van beveiliging steeds ontevredener over de operationele inefficiëntie en het gebrek aan integratie die gepaard gaan met het gebruik van een breed scala aan traditionele beveiligingstools, en zoeken ze in plaats daarvan naar effectievere en geïntegreerde oplossingen.[1]

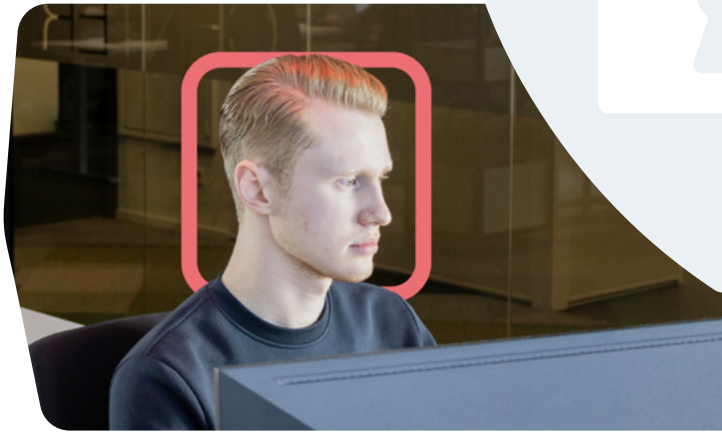
[1] Gartner: Top 5 Trends in Security Vendor Consolidation, 2022

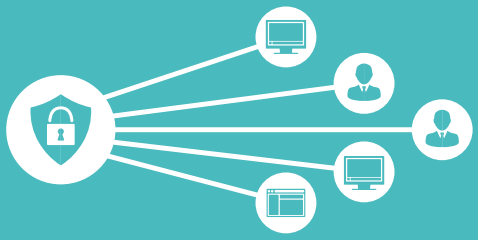
XDR, hét antwoord op moderne aanvallen.

Om de aard van moderne aanvallen die meerdere domeinen bestrijken aan te pakken, hebben beveiligingsteams een uniforme oplossing nodig waarmee ze bedreigingen efficiënter kunnen detecteren en erop kunnen reageren in het gehele digitale domein van een organisatie. XDR helpt jouw Security Operations Center (SOC), met krachtige intelligentie die de correlatie en analyse van gegevens automatiseert, bij de transitie van een reactieve benadering naar een proactieve verdedigingsstrategie.

Dat terwijl de detectie van bedreigingen wordt verbeterd, responstijden, en vooral het vrijmaken van tijd voor jouw SOC-analisten zodat zij zich kunnen concentreren op een proactieve jacht en preventie.

Extended Detection and Response (XDR)-oplossingen zijn ontworpen om een holistische, vereenvoudigde, en efficiënte aanpak om organisaties te beschermen tegen geavanceerde aanvallen. Ze geven SOC-teams een completer beeld van de kill-keten voor effectiever onderzoek en bieden automatisch herstel over meerdere domeinen met behulp van enorme sets van intelligentie en ingebouwde kunstmatige intelligentie (AI).





Uitgebreide detectie en respons (XDR)

- Holistische beveiliging en signaalcorrelatie tussen identiteit, e-mail, endpoint, cloud-app, beveiliging tegen gegevensverlies (DLP) en meer
- Ervaring op het gebied van onderzoek en respons op basis van incidenten
- Beschermt tegen geavanceerde aanvallen zoals ransomware en zakelijke e-mailcompromis (BEC)

VS

Endpointdetectie en respons (EDR)

- Alleen endpointbeveiliging
- Geïsoleerde endpointwaarschuwingen
- Kan alleen endpointspecifieke aanvallen helpen afweren en mist het grote plaatje om te helpen bij geavanceerde aanvallen

XDR biedt beveiligingsteams een nieuwe manier om de proces- en kostenefficiëntie binnen hun activiteiten te verbeteren. Wanneer je een XDR-oplossing voor jouw organisatie overweegt, let dan op deze essentiële reeks mogelijkheden:

1 Geavanceerde zichtbaarheid en bescherming van de kill chain

Om te beschermen tegen geavanceerde aanvallen moeten XDR-oplossingen verschillende soorten activa dekken en de beveiliging verenigen voor kritieke toegangspunten voor bedreigingen, zoals e-mail en identiteit, maar ook aanvalspunten verderop in de kill-keten beschermen, inclusief eindpunten, cloud-apps en DLP-gegevens. Door deze gegevensbronnen te consolideren, correleren XDR-oplossingen waarschuwingen op laag niveau tot één enkel incident en helpen ze de volledige kill-keten van een geavanceerde aanval bloot te leggen die door endpoint beveiligingsoplossingen over het hoofd zou worden gezien.

2 Uniform onderzoek en reactie

Effectieve XDR-oplossingen zijn ontworpen om beveiligingsanalisten effectiever te laten werken. Op incidenten gebaseerd onderzoek dat het end-to-end beeld van aanvallen laat zien, contextuele diepgaande analyses en respons-playbooks met best practices zijn allemaal van cruciaal belang om het voor SOC-teams gemakkelijker te maken om aanvallen efficiënter te onderzoeken en erop te reageren.

3 Automatisering

Het toenemende volume en de snelheid van geavanceerde aanvallen stellen de capaciteit van de meeste beveiligingsteams op de proef. XDR-oplossingen bieden op twee manieren automatisering. Ze gebruiken de breedte van hun onderliggende signaal en AI om ingebouwde automatisering te bieden om te reageren op geavanceerde aanvallen, maar bieden ook opties voor bedrijven om aangepaste automatiseringen te creëren. Beide helpen bij het schalen van de SOC-schaal.

4 Brede zichtbaarheid van inlichtingen en dreigingsvectoren

Een XDR-oplossing moet intelligentie bevatten. Het moet inzichten putten uit een breed scala aan bronnen om signalen te analyseren en het dreigingslandschap beter te begrijpen, evenals uit eigen onderzoek dat preventie-, detectie- en beschermingsmechanismen informeert. Een groter aantal en diversiteit aan signalen vergroot het vermogen om meer bedreigingsvectoren te zien en te begrijpen, waardoor de XDR-oplossing een aanval snel in een eerder stadium kan identificeren, het aantal waarschuwingen en incidenten kan verminderen en het SOC-team in staat stelt te reageren op de nieuwste ontwikkelingen om daardoor bedreigingen effectiever te bestrijden.

5 Verbeterde totale eigendomskosten

XDR maakt leverancierconsolidatie voor organisaties mogelijk door meerdere, in silo's geplaatste beveiligingstools te integreren die zijn aangeschaft in een uniforme oplossing. Het elimineert de noodzaak om bij verschillende leveranciers te kopen en het handmatige werk dat nodig is om signalen te correleren. In plaats daarvan biedt XDR een alomvattende oplossing voor detectie, respons en herstel, waardoor de acquisitiekosten en procesoverhead worden verlaagd.

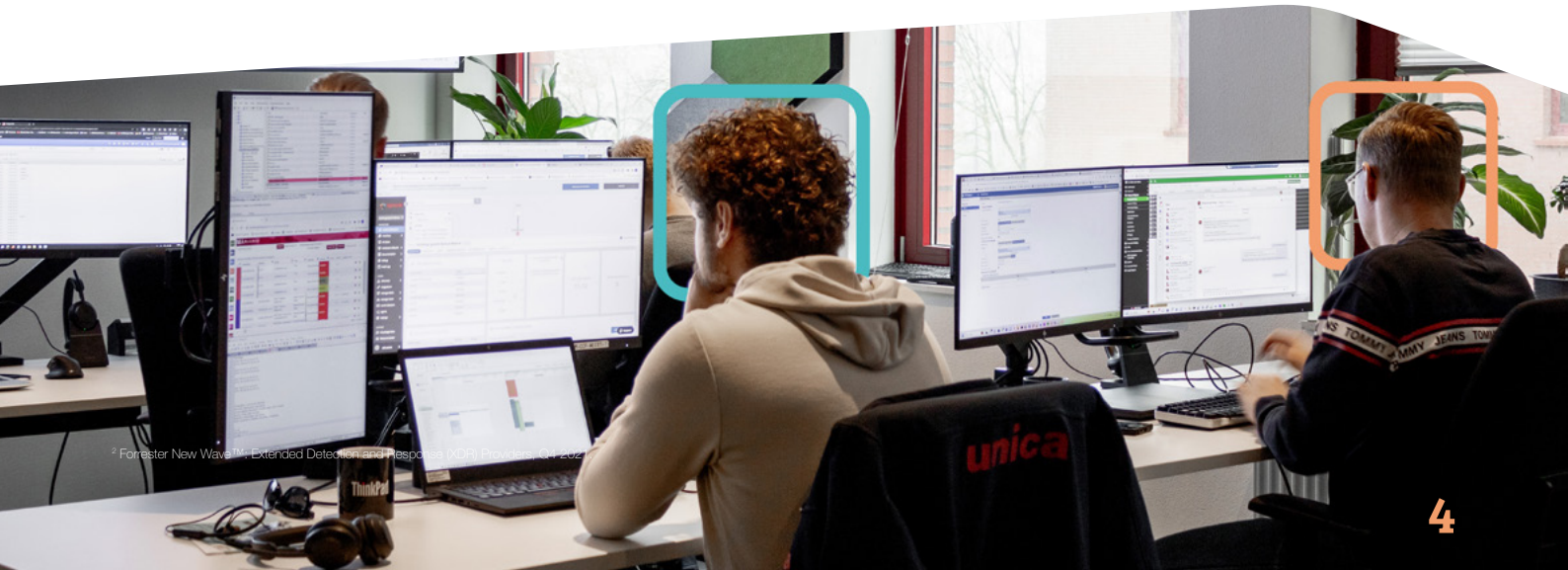
Geef jouw SOC-ervaring een boost met Microsoft 365 Defender, de Microsoft XDR-oplossing

Microsoft 365 Defender wordt erkend als een toonaangevende[2] XDR-oplossing en biedt een uniforme onderzoeks- en responservaring en biedt native bescherming voor eindpunten, hybride identiteiten, e-mail, samenwerkingstools en cloudapplicaties met gecentraliseerde zichtbaarheid, krachtige analyses en automatische verstoring van aanvallen. Met Microsoft 365 Defender kunnen organisaties beschikken over een bredere reeks beveiligingen, waaronder e-mailbeveiliging en identificatie- en toegangsbeheer als cruciale preventieve oplossingen, profiteren van automatische herstelmogelijkheden voor veelvoorkomende problemen, en SOC-teams schalen met XDR-geautomatiseerde verstoring om te beschermen tegen ransomware en andere geavanceerde aanvallen effectiever en tegelijkertijd de bedrijfscontinuïteit van organisaties waarborgen.

Microsoft 365 Defender biedt verdedigers een groot aantal belangrijke mogelijkheden om aanvallers een stap voor te blijven, waaronder:

1. Maak een snelle respons mogelijk met incidenten met XDR-prioriteit.

Microsoft 365 Defender correleert native signalen tussen multi-platform endpoints, hybride identiteiten, e-mail en samenwerkingstools, evenals SaaS-apps en DLP-inzichten om een compleet beeld van de keten te bieden. Dankzij deze diepe context kunnen SOC-teams onderzoek doen en reageren op incidentniveau, waardoor het stellen van prioriteiten eenvoudig wordt en het herstel sneller verloopt.



[2] Forrester New Wave™: Extended Detection and Response (XDR) Providers, Q1 202

Blijf geavanceerde aanvallen voor

Snelheid is van belang in de dagelijkse werkzaamheden van een beveiligingsanalist. Daarom biedt Microsoft 365 Defender uniform onderzoek en respons, ontworpen om de meest efficiënte ervaring voor SOC-teams te bieden voor snellere responstijden. Je kunt waarschuwingen onderzoeken in de context van het hele incident en gebruik maken van in-product herstel-playbooks om snel te reageren – allemaal als een verbonden ervaring zonder dat er van context wordt gewisseld. Je kunt zelfs deep diven met één enkele taal voor geavanceerd zoeken in alle services. Om ervoor te zorgen dat automatisering je helpen nog sneller te reageren, ondersteunt Microsoft 365 Defender bovendien realtime aangepaste detecties.

Voor een gestroomlijnd onderzoek biedt Microsoft 365 Defender een visuele grafiek van de aanval, waarin alle getroffen entiteiten worden weergegeven, zodat het SOC gemakkelijk kan begrijpen hoe de aanvaller van compromis naar doelwit is gegaan.

Een datacentrische SOC met DLP-signaal mogelijk maken

DLP is van cruciaal belang voor organisaties om gevoelige informatie te beschermen en het risico op gegevensverlies of lekken te beperken. Door DLP-waarschuwingen te integreren in de incidentonderzoekservaring krijgen SOC-analisten een geheel nieuwe manier om prioriteiten te stellen, gebaseerd op de gevoeligheid van de getroffen gegevens.

Microsoft 365 Defender biedt je de mogelijkheid om snel inzicht te krijgen in de impact van een datalek door DLP-waarschuwingen te correleren met de XDR-incidentweergave, de mogelijkheid om geavanceerde jacht uit te voeren en herstelacties rechtstreeks vanuit de Microsoft 365 Defender-portal te ondernemen. Door data-centriciteit toe te voegen aan jouw SOC-ervaring wordt de correlatie tussen een aanval en de detectie van datalekken vereenvoudigd, zodat je de impact van begin tot eind sneller en effectiever kunt begrijpen.

2. Onderbreek geavanceerde aanvallen met machinesnelheid.

Microsoft 365 Defender maakt gebruik van de breedte van ons XDR-signaal en onze op onderzoek gebaseerde, AI-gestuurde detectiemogelijkheden om geavanceerde aanvallen zoals ransomware te identificeren en biedt automatische respons op incidentniveau met automatische aanvalsonderbreking. Aanvalsverstoring omvat lopende aanvallen door apparaten en gebruikersaccounts die bij een aanval worden gebruikt automatisch uit te schakelen of te beperken, waardoor de voortgang wordt gestopt en de impact wordt beperkt.

Schaal jouw SOC-team op met automatische inperking van getroffen activa

Automatische aanvalsonderbreking is ontworpen om lopende aanvallen te beperken door deze automatisch uit te schakelen of het beperken van gecompromitteerde apparaten en gebruikersaccounts, waardoor de voortgang wordt gestopt en de impact voor organisaties wordt beperkt. Dit is een grote innovatie; tegenwoordig kunnen de meeste beveiligingsteams niet snel genoeg reageren op geavanceerde aanvallen zoals ransomware of BEC-campagnes en zijn ze doorgaans reactief door op te ruimen op basis van de impact. Bij verstoring van aanvallen blijven de aanvallen beperkt tot een klein aantal assets, waardoor de impact dramatisch wordt geminimaliseerd en de bedrijfscontinuïteit wordt verbeterd.

Bouw efficiëntie op basis van het breedste inzicht in de branche in aanvalsvectoren

Met 65 biljoen dagelijkse signalen en 8.500 beveiligingsprofessionals heeft Microsoft-beveiliging inzicht in meer bedreigingsvectoren dan welke andere leverancier dan ook. In combinatie met ons native geïntegreerde XDR-platform hebben SOC-teams een betere realtime bescherming tegen geavanceerde bedreigingen en kunnen ze sneller reageren.

43 trillion signals

worden dagelijks gesynthetiseerd, met behulp van geavanceerde data-analyses en AI-algoritmen om digitale dreigingen en criminele cyberactiviteit te begrijpen en ertegen te beschermen.[3]

[3] Microsoft, "Microsoft Digital Defense Report," November 2022

3. Integreer XDR-beveiliging en identiteitstoegangsbeheer.

Identiteiten vormen een kritische dreigingsfactor, omdat bij de meeste aanvallen gecompromitteerde identiteiten zich zijdelings verplaatsen. Microsoft combineert de mogelijkheden voor identiteitsbescherming van ons toonaangevende identiteitstoegang en -beheerplatform met onze XDR-oplossing, waardoor één geïntegreerde ervaring wordt geboden voor het beschermen van identiteiten en het verdedigen tegen bedreigingen. Deze krachtige combinatie biedt preventieve mogelijkheden zoals voorwaardelijke toegang, die rechtstreeks in het identiteitsplatform Azure AD zijn ingebouwd, terwijl het de volledige breedte van de mogelijkheden voor bedreigingsbescherming van Microsoft's XDR biedt. Dit geeft jouw organisatie een uniforme oplossing die hybride gebruikers- en werklastidentiteiten beschermt, evenals de onderliggende identiteitsinfrastructuur.

Creëer operationele efficiëntie en verlaag de kosten

Microsoft 365 Defender biedt een uniforme ervaring voor het beschermen van identiteiten op locatie en in de cloud en combineert deze signalen met alle andere bronnen voor de volledige XDR-weergave van de aanvalsketen, waardoor aanzienlijke efficiëntieverbeteringen voor het SOC worden gecreëerd. Bovendien realiseer je met Microsoft E5 Security een kosteneffectieve aanpak om leveranciers te consolideren en zowel toonaangevende identiteit als toonaangevende XDR-mogelijkheden in één pakket te krijgen.

Het beste van zijn soort, verenigd in een toonaangevende XDR-oplossing

Naast dat ze een toonaangevende aanbieder van identiteitsoplossingen zijn, zijn de andere oplossingen die zijn verenigd binnen Microsoft's XDR de beste in hun soort en is een endpoint beveiligingsoplossing vaak het startpunt voor een XDR-discussie. Gartner noemde Microsoft een leider in het Gartner® Magic Quadrant voor Endpoint Protection Platforms van 2022 met bescherming voor meerdere platforms, waaronder Linux, macOS, iOS en Android.[4]

Hoe Microsoft 365 Defender de efficiëntie van het SOC verbetert met een diep geïntegreerde beveiligingsstack.

>80%

vermindering van waarschuwingen in de SOC-wachtrij[5]

>75%

van de werkitems opgelost met automatisering[5]

242%

return on investment[5]

[4] Microsoft, "Microsoft is named a Leader in the 2022 Gartner® Magic QuadrantTM for Endpoint Protection Platforms," March 2, 2023.
[5] Forrester: The Total Economic Impact™ of Microsoft 365 Defender

Erkenning van de industrie

Forrester New Wave™: uitgebreide detectie en respons (XDR)

Microsoft werd uitgeroepen tot leider in de inaugurele Forrester New WaveTM: Extended Detection and Response (XDR), Q4, 2021,[6] en ontving één van de hoogste scores in de strategiecategorie. Microsoft 365 Defender werd beoordeeld als 'gedifferentieerd' op zeven criteria, waaronder detectie, onderzoek, respons en herstel.

MITRE Engenuity ATT&CK® evaluaties

Voor het vierde achtereenvolgende jaar demonstreerde Microsoft 365 Defender zijn toonaangevende bescherming in de onafhankelijke ATT&CK® Enterprise Evaluations[7] van MITRE Engenuity, waarin de waarde van een geïntegreerde, op XDR gebaseerde verdediging werd getoond. Microsoft demonstreerde volledige zichtbaarheid en analyses in alle stadia van de aanvalsketen.

Figuur 2

Forrester New wave™: Extended Detection And Response (XDR) Providers, Q4 2021

The Forrester New Wave

Extended Detection And Response (XDR) Providers

Gartner

Microsoft is uitgeroepen tot Leider in het Gartner® Magic Quadrant™ for Endpoint Protection Platforms van 2022 en kreeg de hoogste beoordeling op het gebied van uitvoering.[8,9] De Microsoft 365 Defender-portal verenigt de beste beveiliging in zijn soort voor endpoints, e-mail, identiteiten en SaaS-applicaties omzetten in een uitgebreide XDR-ervaring.

[6] The Forrester Wave™ is copyrighted by Forrester Research, Inc. Forrester and Forrester Wave™ are trademarks of Forrester Research, Inc. The Forrester Wave™ is a graphical representation of Forrester's call on a market and is plotted using a detailed spreadsheet with exposed scores, weightings, and comments. Forrester does not endorse any vendor, product, or service depicted in the Forrester Wave™. Information is based on best available resources. Opinions reflect judgment at the time and are subject to change.

[7] MITRE Engenuity ATT&CK® Evaluations, Wizard Spider + Sandworm Enterprise Evaluation 2022. The MITRE Corporation and MITRE Engenuity.

[8] Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose. Gartner is a registered trademark and service mark and Magic Quadrant is a registered trademark of Gartner, Inc. and/or its affiliates in the U.S. and internationally and are used herein with permission. All rights reserved.

[9] Gartner Magic Quadrant for Endpoint Protection Platforms, Peter Firstbrook, Chris Silva. 31 December 2022.

Klantervaring

ING maakt gebruik van de volledige reikwijdte van Microsoft 365 Defender om bankieren opnieuw vorm te geven voor een digitaal publiek. Het IT-team kan phishing-pogingen nu beter herkennen en vanaf het begin blokkeren, voortbouwend op zijn eigen intelligentie door querygegevens te gebruiken om extra risico's te identificeren.

"Eén enkele detectielaag is niet sterk genoeg en is gevoelig voor een zekere mate van valse positieven. Aan de andere kant correleert Microsoft 365 Defender signalen tussen endpoints, e-mail, documenten, identiteit, apps en meer.

We beschouwen het als een gamechanger dat Microsoft 365 Defender signalen combineert voor het opsporen van bedreigingen, omdat het gegevens vanuit het identiteits- en eindpuntperspectief verbindt om echt kwaadaardige gebeurtenissen op te sporen."

—Krzysztof Kuznik, Product Owner at ING

G&J pepsi

G&J Pepsi-Cola Bottlers had Microsoft 365 Defender geïmplementeerd en geprofiteerd, de basis die G&J Pepsi nodig had om de beveiliging uit te breiden na herstel van de ransomware-aanval. Microsoft 365 Defender is op unieke wijze in staat ransomware-bedreigingen, zoals die waar G&J Pepsi in 2021 mee te maken kreeg, te helpen detecteren en erop te reageren.

"Het hebben van een sterke beveiligingshouding gericht op het beschermen van de fysieke veiligheid en de beveiliging van apparaten, identiteiten en gegevens is van cruciaal belang voor de stabiliteit van het bedrijf en was een sleutelcomponent voor een succesvolle verdediging tegen cyberaanvallen.

—Eric McKinney, directeur Enterprise Infrastructure bij G&J Pepsi-Cola Bottlers

Samenvatting

XDR komt naar voren als een revolutionaire aanpak om cyberdreigingen te bestrijden en SecOps in staat te stellen meer te doen met een uniforme detectie- en responservaring. Geavanceerde aanvallen zoals ransomware verleggen de grenzen en benadrukken de tekortkomingen van geïsoleerde beveiligingsoplossingen. De behoefte aan een uitgebreidere en geïntegreerde oplossing is nog nooit zo duidelijk geweest; XDR biedt precies dat.

Microsoft 365 Defender wordt erkend als een toonaangevende XDR-oplossing en wordt gedefinieerd door zijn uniforme bescherming over endpoints, hybride identiteiten, e-mail, samenwerkingstools en cloudapplicaties. Naast op incidenten gebaseerd onderzoek en respons biedt het gecentraliseerde zichtbaarheid, krachtige analyses en automatische verstoring van aanvallen, om de SOC-efficiëntie te vergroten en ervoor te zorgen dat organisaties toegang hebben tot de nieuwste informatie en op onderzoek gebaseerde bescherming. Tot slot is Microsoft 365 Defender de enige XDR-oplossing die een toonaangevend identiteits-, toegangs- en beheerplatform combineert, voor een enkele, geïntegreerde ervaring om identiteiten te beschermen en zich te verdedigen tegen bedreigingen. Daardoor worden aanzienlijke voordelen op het gebied van de totale eigendomskosten voor de procesefficiëntie gecreëerd, maar ook het consolideren van de kosten bij één enkele leverancier.

XDR is een must-have voor elke moderne beveiligingsstrategie, dus SOC-teams zijn goed gepositioneerd om gelijke tred te houden met het zich ontwikkelende aanvalslandschap en worden geholpen door een op intelligentie gebaseerde en uniforme benadering van bedreigingsbescherming.

Heb je vragen of wil je meer informatie?

Hendry wil je graag verder helpen

Hendry is al jarenlang één van de specialisten bij Unica ICT Solutions als het gaat om Networking en Security. Met zijn enthousiasme en kennis geeft hij, vanuit zijn rol als Business Manager Digital Security & Networking, dagelijks advies aan de meest uiteenlopende organisaties, groot of klein. Hij deelt zijn jarenlange deskundigheid graag met zijn collega's en onze klanten en ondersteunt als adviseur ook bij het realiseren, onderhouden en beveiligen van netwerkinfrastructuren. Maar ook alles wat er bij een goede security van een organisatie komt kijken. Nu de infrastructuren het fundament worden voor elke organisatie waarop diensten zoals Microsoft Office365 worden geconsumeerd en ook slimme technologie wordt gekoppeld, is de beschikbaarheid maar ook beveiliging van deze infrastructuren van cruciaal belang. Gebruikers verwachten altijd en overal connectiviteit te hebben, zodat bedrijfsprocessen zo optimaal en veilig gefaciliteerd kunnen worden. Als Solution Specialist op het vlak van security en networking geeft hij een nuchter advies om de optimale, beveiligde en beheersbare infrastructuur voor onze klanten te kunnen realiseren.

Hendry

Business Manager Digital Security & Networking

hscholing@unica.nl

06-54651672

unica
ict solutions

&

Microsoft

Unica ICT Solutions

ictinfo@unica.nl

unica.nl/ict-solutions

Wij zijn er, altijd.