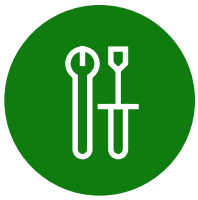
Microsoft Security

Drie redenen om over te stappen op geïntegreerde bedreigingsbeveiliging

Inhoudsopgave

Kennismaking



De gemiddelde onderneming gebruikt nu meer dan dertig verschillende beveiligingstools, vaak onsamenhangend en ‘toegevoegd’.

Beveiliging staat op een keerpunt. Cyberaanvallen worden steeds geavanceerder en organisaties blijven worstelen met uitdagingen zoals tekorten aan talent, kostenverdeling en de druk van hybride werken.

Ondertussen is de beveiligingsmarkt gefragmenteerder en complexer dan ooit. De gemiddelde onderneming gebruikt nu meer dan dertig verschillende beveiligingstools, vaak onsamenhangend en ‘toegevoegd’, waardoor beveiligingscentra (SOC’s) weinig zicht en onvoldoende inzichten hebben.

Beveiligings- en complianceleiders willen de nieuwste risico’s en bedreigingen beter begrijpen, maar ze moeten ook weten wat wel werkt, wat niet werkt en waar ze hiaten hebben.

Hoewel de omvang van de huidige beveiligingsuitdagingen soms overweldigend lijkt, is er reden voor optimisme voor CISO's die de efficiëntie en effectiviteit van hun beveiligingsactiviteiten willen verbeteren. Het antwoord ligt in een geïntegreerde, allesomvattende aanpak van de bescherming tegen cyberbedreigingen, wat organisaties helpt om:

Reden 1: Meer doen met minder

Consolideer puntoplossingen en verminder de overhead van beveiligingsactiviteiten (SecOps).

Reden 2: SecOps de mogelijkheid geven om zich op hoogwaardige taken te richten

Gebruik tools die de efficiëntie verbeteren en zelfs onervaren analisten capabeler dan ooit maken.

Reden 3: Werknemers productiever maken

Bescherm je organisatie op een manier waardoor je mensen zonder zorgen kunnen creëren en innoveren.

Deze aanpak wordt mogelijk gemaakt door een XDR-oplossing (uitgebreide detectie en respons) te integreren in een cloud-SIEM-systeem (beheer van beveiligingsinformatie en -gebeurtenissen) dat kunstmatige intelligentie (AI) en automatisering gebruikt. De geïntegreerde oplossing kan je SOC helpen betere voorspellingen te doen, proactiever te zijn en aanvallen in het hele bedrijf te voorkomen.

Reden 1

Meer doen met minder

Door tools te consolideren in de geïntegreerde oplossing van Microsoft, kun je ook besparen door alleen te betalen voor wat je gebruikt.

Veel organisaties hebben zich bij hun zoektocht naar beveiligingstools gericht op de allerbeste afzonderlijke oplossingen. Helaas kan die aanpak het voor beveiligers juist moeilijker maken om bedreigingen snel te herkennen en aan te pakken. Het kan ook een negatieve invloed op IT-uitgaven en de productiviteit van eindgebruikers hebben.

Omdat organisaties met minder meer willen bereiken, kan een geïntegreerde aanpak zoals Microsoft's SIEM en XDR helpen. Zo kun je de complexiteit verminderen door afzonderlijke tools te consolideren, en omdat het een geïntegreerde cloudoplossing is, kunnen ook de prestaties en schaal worden verbeterd.

Door tools te consolideren in de geïntegreerde oplossing van Microsoft, kun je ook besparen door alleen te betalen voor wat je gebruikt. Je kunt ook de SecOps-overhead van het beheren van oplossingen verlagen door meer te automatiseren en integreren.

> Het introductieproces voor nieuwe beveiligingstools begint makkelijk, omdat je verwacht dat je grote gaten hebt te vullen. Verderop in het proces zul je snel merken dat tools van verschillende leveranciers elkaar kunnen overlappen. Een dergelijke dubbele functionaliteit kan voor controles wenselijk zijn, **maar kan ook flinke financiële kosten met zich meebrengen.**"
>
> **Jonathan Cassar**
> Chief Technology Officer, MITA

USD 1,6 miljoen

per jaar bespaard door leveranciers te consolideren

Microsoft gaf Forrester Consulting de opdracht om een Total Economic Impact™-onderzoek (TEI) uit te voeren en het mogelijke investeringsrendement van het implementeren van Microsofts SIEM en XDR te onderzoeken. Dit zijn een paar van de belangrijkste bevindingen voor een hypothetische samengestelde organisatie met in totaal 8000 werknemers en 10 IT-beveiligers:

- **Een besparing van bijna USD 1,6 miljoen per jaar door leveranciers te consolideren.** Door in Microsofts SIEM en XDR te investeren, kon het samengestelde bedrijf de kosten besparen voor de oude SIEM (USD 560.000), de bijbehorende lokale infrastructuur (meer dan USD 360.000), drie losse XDR-oplossingen (USD 192.000) en de doorlopende arbeidskosten om die te beheren (USD 480.000).

- **60% kleiner risico dat materialen worden gelekt.** Met efficiëntere beveiligingsonderzoek- en reactieprocessen, verbeterde automatisering van beveiligingsreacties en het toegenomen vermogen om alle computeromgevingen te beschermen, waaronder multicloud, verkleinde het samengestelde bedrijf het risico op lekken, waardoor jaarlijks USD 1,6 miljoen aan kosten wordt bespaard.

- **Een investeringsrendement van 207%.** Uit de representatieve interviews en financiële analyses bleek dat een samengestelde organisatie in drie jaar tijd uit een investering van USD 5,76 miljoen USD 17,68 miljoen voordeel behaalt, wat neerkomt op een netto contante waarde van USD 11,92 miljoen.

Reden 2

SecOps de mogelijkheid geven om zich op hoogwaardige taken te richten

Het is essentieel om SIEM en XDR op elkaar af te stemmen om waarschuwingen te correleren, prioriteit te geven aan de grootste bedreigingen en maatregelen in de hele onderneming te coördineren.

SecOps-teams worden overweldigd door de hoeveelheid signalen die ze moeten analyseren, waaronder veel signalen met een lage waarschijnlijkheidsgraad die moeilijk, zo niet onmogelijk, handmatig kunnen worden gedetecteerd en verholpen. Als het aantal bedreigingen toeneemt, is het voor een overbelast SOC moeilijk om bij te blijven, vooral als ze data uit verschillende afzonderlijke oplossingen moeten analyseren. Het toewijzen van meer middelen om de hiaten op te vullen is niet het antwoord, want het blijft een uitdaging om voldoende beveiligers te vinden.

Daarom is het essentieel om SIEM en XDR te integreren, zodat meldingen kunnen worden gecorreleerd, de grootste dreigingen prioriteit kunnen krijgen en maatregelen in het hele bedrijf kunnen worden gecoördineerd, met geavanceerde AI en automatisering om dreigingen proactief te detecteren en verhelpen.

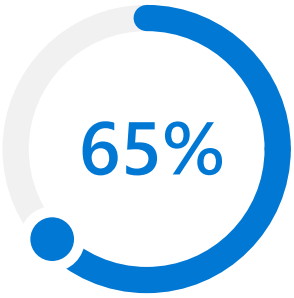
Bedenk bijvoorbeeld dat een enkel signaal op laag niveau van een traditionele SIEM niet veel aandacht kan krijgen. Maar met AI kan een cloud-SIEM dat signaal automatisch vergelijken met signalen van andere bronnen in de hele organisatie, waarbij het correleert tussen meerdere datasets om aanvallen te vinden die uit meerdere fasen bestaan.

Geïntegreerde SIEM en XDR maakt middelen vrij en geeft zelfs onervaren analisten meer mogelijkheden en vertrouwen.

Het systeem normaliseert, analyseert en correleert vervolgens de data, terwijl het context biedt over hoe de cyberaanval de infrastructuur binnenkwam, samen met de tijdlijn van de verspreiding. Hierdoor kunnen beveiligingsteams de inbreuk visualiseren en effectief vanaf een enkele console aanpakken.

> Veel CISO's realiseren zich niet **met hoeveel overhead ze hun teams opzadelen met twintig verschillende schermen** of puntoplossingen, en de bijbehorende jaarlijkse kosten … we hebben veel toolmoeheid weggenomen door één leverancier te nemen."
>
> **Terence Jackson**
> Chief Information Security and Privacy Officer, Thycotic

Om waarde uit een beveiligingsoplossing te halen, heeft een organisatie geen diepgravende expertise nodig. Geïntegreerde SIEM en XDR maakt middelen vrij en geeft zelfs onervaren analisten meer mogelijkheden en vertrouwen.



De geïntegreerde aanpak van Microsofts SIEM en XDR beperkte de tijd om dreigingen te onderzoeken met 65%.

In het Forrester Total Economic Impact™-onderzoek (TEI) in opdracht van Microsoft was deze SecOps-efficiëntie te zien in de samengestelde organisatie:

- **Onderzoeken naar dreigingen duren 65% korter en er wordt 88% sneller gereageerd.** De geïntegreerde aanpak van Microsoft's SIEM en XDR om dreigingen te onderzoeken en erop te reageren, maakt deze processen voor de beveiligers van de samengestelde organisatie efficiënter. Ze hoeven niet langer tussen verschillende tools te schakelen om dreigingen te detecteren en de beveiligingsautomatisering verbetert de reactieprocessen.
- **90% sneller een nieuwe werkmap aanmaken en 91% sneller nieuwe beveiligers inwerken.** De geïntegreerde aanpak van Microsoft's SIEM en XDR maakt ook aanvullende beveiligingsprocessen efficiënter. Omdat SIEM-logboeken in de hele suite oplossingen zijn geïntegreerd, wordt het maken van werkmappen bijna geautomatiseerd, en dankzij de enkele aanmelding kunnen nieuwe beveiligers bijna zestien weken sneller worden ingewerkt.

Reden 3

Werknemers productiever maken

Een geïntegreerde SIEM- en XDR-oplossing kan je organisatie helpen de productiviteit voor eindgebruikers te verbeteren.

Behalve dat je met minder meer kunt doen en SecOps efficiënter kunt maken, kan een geïntegreerde SIEM- en XDR-oplossing je organisatie ook helpen om eindgebruikers productiever te maken.

SecOps-teams weten dat als je beveiliging moeilijk maakt, gebruikers haar gaan omzeilen. Dus als de gebruikservaring de productiviteit van werknemers eerder belemmert dan ondersteunt, kan dit de organisatie blootstellen aan meer beveiligingsrisico's en hogere kosten. Zwakke of kwijtgeraakte wachtwoorden, onbeveiligde toegang via persoonlijke apparaten en het onbelemmerd delen van vertrouwelijke data zijn slechts een paar van de uitdagingen.

> [In het verleden] gingen we met de botte bijl te werk als iemand een probleem vermoedde. We zetten dingen uit en sloten de toegang af, wat een negatieve invloed had op ons bedrijf. En het was voor iedereen heel duidelijk, omdat dingen tijdelijk niet meer werkten. In Microsoft Sentinel hebben we een scalpel, zodat we heel chirurgisch kunnen reageren op wat er gebeurt. **Het bedrijf heeft het meestal niet eens door als we op een dreiging reageren** en dat is een heel duidelijk teken van succes."
>
> **Rick Gehringer**
> Chief Information Officer, Wedgewood

Bijna
68.000

Microsofts SIEM en XDR verbeterden de productiviteit van andere werknemers met in totaal bijna 68.000 uur per jaar.

Een geïntegreerde SIEM- en XDR-aanpak helpt je bij het leveren van naadloze gebruikerservaringen waarmee je je mensen in alle facetten van hun dagelijks werk productief en veilig kunt houden. Het kan negatieve gevolgen voor de productiviteit beperken, zoals het moeten uitzetten van diensten of het isoleren en opnieuw installeren van machines. Maar geïntegreerde SIEM en XDR kunnen ook nieuwe mogelijkheden creëren voor productiviteitsverbeteringen bij eindgebruikers, zoals meer self-service beveiligingssupport, betere dashboards en rapporten en meer responsiviteit en sneller opstarten omdat er minder beveiligingsservices draaien.

In het in opdracht van Microsoft uitgevoerde Forrester Total Economic Impact™-onderzoek (TEI) vertoonde de hypothetische samengestelde organisatie met in totaal 8000 werknemers meer productiviteit door Microsoft's SIEM en XDR te gebruiken:

- ✓ **In totaal bijna 68.000 uur meer productiviteit per jaar voor de andere werknemers.** Microsoft's SIEM en XDR voorkomen dat andere werknemers negatieve gevolgen van inefficiënte beveiligingsprocessen ondervinden. Het samengestelde bedrijf bespaart bijvoorbeeld 4000 uur per jaar omdat IT'ers zelf met beveiligingsupdates en -aanbevelingen aan de slag kunnen. Het maakt ook het op afstand oplossen van beveiligingsproblemen op machines van werknemers mogelijk en vermindert het aantal beveiligingsservices dat op die machines draait, wat per jaar bijna 64.000 uur aan eindgebruikersproductiviteit bespaart.

Beveiliging is een essentiële drijfveer achter technologisch succes geworden. Daarom hebben organisaties behoefte aan beveiligingsmaatregelen die zoveel mogelijk veerkracht tegen moderne aanvallen bieden, zodat ze de productiviteit en innovatie die groei mogelijk maken, kunnen beschermen.

Profiteer van geïntegreerde cyberbedreigingsbeveiliging met SIEM en XDR

Deze integratie van toonaangevende producten biedt preventie en detectie van en reactie op cyberbedreigingen in één allesomvattende oplossing.

Microsoft levert de eerste en enige geïntegreerde SIEM- en XDR-oplossing, die volledige zichtbaarheid in alle clouds en platformen biedt. Deze integratie van toonaangevende producten biedt preventie en detectie van en reactie op cyberbedreigingen in één allesomvattende oplossing.

Microsofts SIEM en XDR gebruiken de kracht van AI en automatisering, maar ook grote en voortdurende investeringen in cyberbedreigingsdetectie en -analyse, met inzichten van experts in zicht op 43 biljoen signalen per dag. Dankzij integratie van deze producten zijn SOC-teams gewapend met meer context dan ooit, zodat ze kritieke cyberbedreigingen sneller kunnen detecteren en oplossen:

Microsoft Sentinel

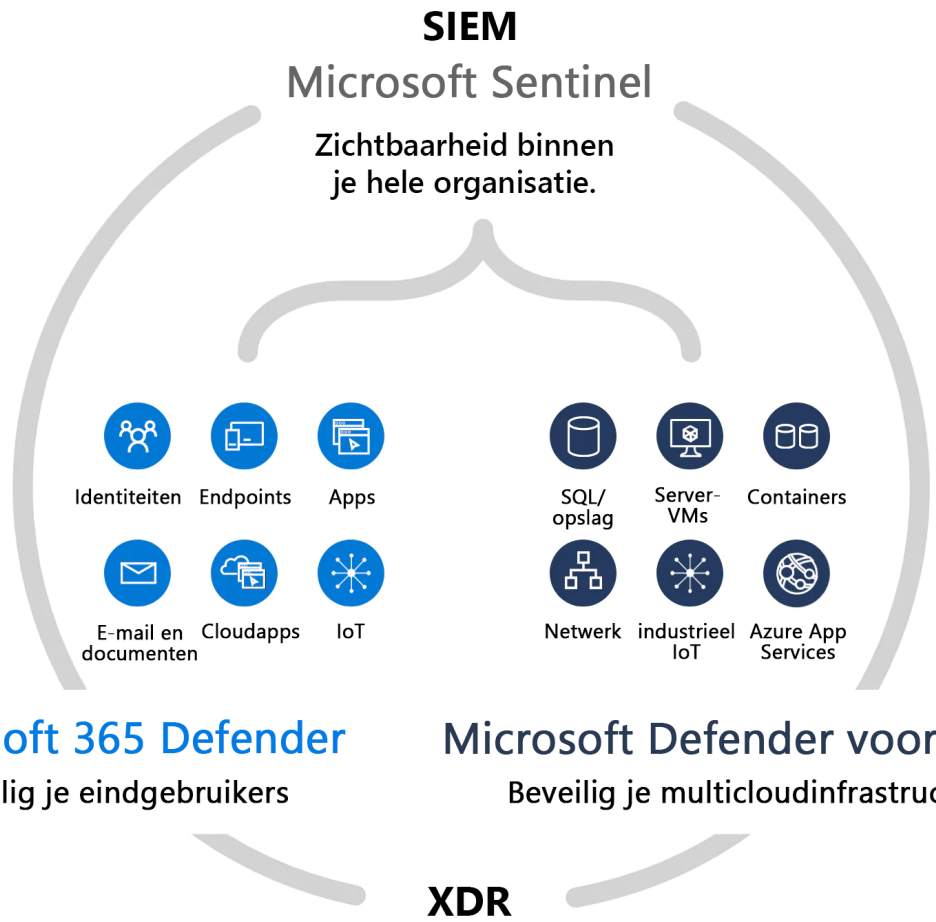
Krijg een totaaloverzicht van de onderneming met de cloud-SIEM van Microsoft. Verzamel beveiligingsdata uit vrijwel elke bron en gebruik AI om ruis te scheiden van legitieme gebeurtenissen, waarschuwingen in complexe cyberaanvalsketens te correleren en de reactie op cyberbedreigingen te versnellen met ingebouwde orkestratie en automatisering.

Microsoft Defender XDR

Voorkom en detecteer cyberaanvallen op je identiteiten, endpoints, apps, e-mails, data en cloudapps met XDR-mogelijkheden. Onderzoek en reageer op cyberaanvallen met kant-en-klare en eersteklas bescherming. Jaag op dreigingen en coördineer je reactie makkelijk vanaf een enkel dashboard.

Microsoft Defender voor Cloud

Bescherm je workloads in multi- en hybride clouds met ingebouwde XDR-mogelijkheden. Beveilig je servers, opslag, databases, containers en meer. Richt je met prioriteitsmeldingen op de belangrijkste zaken.



Voeg beveiliging niet toe. Bouw het in.

Geef de juiste mensen de juiste tools en informatie. Bescherm je tegen moderne aanvallen met een geïntegreerde totaaloplossing in de cloud.

Meer informatie over de geïntegreerde bescherming tegen cyberbedreigingen met Microsofts SIEM- en XDR-oplossingen >

Microsoft Security