Insight®

Belangrijke uitdagingen oplossen voor Multi-vendor beveiligingsomgevingen

Een gids voor het overwinnen van een beveiligingsburn-out en het versterken van uw verdediging met Insight en Microsoft Sentinel

Beveiliging onder druk

van de respondenten in Cisco's 2020 CISO Benchmark Survey zegt dat ze lijden aan cyberbeveiligingsmoeheid (gedefinieerd als het vrijwel opgeven van proactieve verdediging tegen kwaadwillende partijen).

Van degenen die dit aangeven, **ontvangt 93% meer dan**

5.000 **waarschuwingen per dag,**

wat aangeeft dat complexiteit een van de belangrijkste oorzaken van een beveiligingsburn-out lijkt te zijn.[1]

De meeste organisaties maken gebruik van verschillende beveiligingsoplossingen om een complexe bedreigingsomgeving te beheren. Maar het beheren en orkestreren van waarschuwingen uit verschillende bronnen is niet alleen een uitdaging, het stelt organisaties ook bloot aan meer risico.

Een overdaad aan waarschuwingen betekent dat er simpelweg te veel zijn om aan te pakken, wat van invloed is op het bewustzijn en de zichtbaarheid van het team hierop, waardoor het bedrijf mogelijk wordt blootgesteld aan grotere, schadelijkere bedreigingen.

Volgens Fady Younes, directeur cybersecurity bij Cisco: "Het niet integreren van meerdere beveiligingsoplossingen kan ook gaps in de dekking achterlaten of een situatie creëren waarin het IT-team niet goed begrijpt welke bescherming een bepaalde oplossing biedt of hoe deze werkt, wat van invloed is op de zichtbaarheid en het bewustzijn van de daadwerkelijke beveiligingsstatus van het netwerk."[2]

Het is minder duidelijk welke risico's en waarschuwingen prioriteit moeten krijgen in deze omgevingen.

Niet alle waarschuwingen zijn even ernstig en de beste beveiligingsstrategieën passen beveiligingscontroles aan en wijzen middelen toe op basis van risiconiveau.

In diverse, multicloud-omgevingen wordt disaster recovery ongelooflijk complex, waardoor een proactieve in plaats van een reactieve beveiligingscultuur nodig is.

"Omgaan met integratie-issues en een hoog volume beveiligingswaarschuwingen kan beveiligingstechnici afleiden van het aanpakken van andere uitdagingen waar ze mee worden geconfronteerd..."

— **Fady Younes, Cybersecurity Director, Midden-Oosten en Afrika bij Cisco**

SIEM en SOAR

Beveiligingsteams hebben twee hoofddoelen: weten wat er gebeurt in hun IT-omgevingen en reageren op die informatie. Er bestaan oplossingen voor Security Information and Event Management (SIEM) en Security Orchestration, Automation and Response (SOAR) voor het bereiken van deze doelen.

SIEM-tools verzamelen en aggregeren gebeurtenisgegevens uit verschillende bronnen binnen een IT-omgeving en analyseren en rangschikken vervolgens gebeurtenissen in volgorde van prioriteit of belang. Beveiligingsteams dragen de verantwoordelijkheid voor het jagen en reageren op bedreigingen, evenals het afstemmen en corrigeren van het SIEM-platform.

SOAR-tools bieden geavanceerde analyses en automatisering die voortborduren op de capaciteiten van SIEM-tools, voor een meer autonome reactie op bedreigingen. SOAR-tools maken gebruik van zoveel mogelijk realtime gegevens en zijn gevoelig voor de capaciteit van degenen die ze beheren. De effectiviteit van deze tools is min of meer op basis van hoe ze worden gebruikt.

90%
van beveiligings-professionals

zegt dat SOAR zeer of extreem belangrijk is voor de algehele beveiligingsactiviteiten van hun organisatie.

Belangrijkste use cases voor SOAR:

- 65% SIEM triage
- 62% Phishingaanvallen
- 62% Informatie over bedreigingen

Uitkomsten van SOAR-implementaties:

- Snellere incidentenoplossing
- Verbeterde efficiëntie van personeel
- Lagere totale kosten[3]

Wat onderscheidt Microsoft Sentinel?

SOAR is de functionaliteit die Sentinel onderscheidt van de concurrentie. Het stelt beveiligingsteams in staat om code of draaiboeken binnen Sentinel te schrijven om automatisch te reageren op bedreigingen wanneer ze binnenkomen, waardoor het SOC-team waarschuwingsmoeheid kan verminderen en zich kan concentreren op dingen waar u zich daadwerkelijk op zou moeten concentreren.

Onze cliënten (klanten) vinden het prettig dat ze waarschuwingen en incidenten kunnen kruiscorreleren en elk incident in kaart kunnen brengen dat aan een specifieke entiteit is gekoppeld. Ik laat meestal een demo aan klanten zien op basis van een scenario waarin een willekeurige aanvaller toegang heeft gekregen tot de omgeving, zijn/haar privileges heeft verhoogd, een massale download van bedrijfsgegevens heeft uitgevoerd en vervolgens zijn/haar account heeft verwijderd. Dit zijn vier afzonderlijke waarschuwingen die u binnen elke SOAR of SIEM zou krijgen. Maar binnen Microsoft Sentinel ziet u een grafiek van één entiteit met vier verschillende lijnen voor elke waarschuwing die ze hebben gegenereerd, evenals een chronologische tijdlijn van die gebeurtenissen. Microsoft Sentinel maakt het jagen op bedreigingen echt gemakkelijker."

— Associate Consultant, InfoSec, Insight

Het voordeel van Microsoft Sentinel

Microsoft Sentinel™ combineert de kracht van een SIEM en een SOAR in één oplossing. Als u al hebt geïnvesteerd in Microsoft® Sentinel, bent u al op weg naar betere beveiliging.

Het Sentinel-platform kan u helpen:

Identificeer bedreigingen voordat ze impact hebben op uw bedrijf.

Reageer snel en nauwkeuriger.

Vereenvoudig de beveiliging in hybride, multicloud-, serverloze en andere moderne omgevingen.

Verlaag de kosten ten opzichte van verouderde SIEM-oplossingen voor bedreigingsonderzoek, licensing, opslag, infrastructuur, management en implementatie.

De tool is gebaseerd op de diepgaande ervaring van Microsoft op het gebied van beveiliging en de nieuwste mogelijkheden voor kunstmatige intelligentie, en werkt in harmonie met andere Microsoft-producten. Het is snel in te stellen en eenvoudig te schalen.

Eén hub, veel datapunten

Microsoft Sentinel maakt het minder complex om multi-vendor oplossingsomgevingen te beheren. De capaciteit van Sentinel om databronnen uit het hele ecosysteem van beveiligingsoplossingen van meerdere leveranciers te halen, biedt organisaties zichtbaarheid en controle waardoor ze eenvoudiger op jacht kunnen naar bedreigingen, waarschuwingsmoeheid kunnen verminderen en een betrouwbaar beeld van uw beveiligingspositie kunnen krijgen.

Best practices voor implementatie

Het is relatief eenvoudig om aan de slag te gaan met Microsoft Sentinel. We adviseren om duidelijke governance en beleid vóór de implementatie vast te stellen. Belangrijk om te overwegen zijn compliancenormen, kostenvereisten, plannen voor opslag, disaster recovery, de bezetting van het beveiligingsteam en incidentresponsplannen.

Dag 1:

Schakel Microsoft Sentinel in.

Verbind databronnen.

Begin met het bouwen van query's om de data te onderzoeken.

Syslog en CEF dienen, net als veel andere SIEM-tools, als ingestion points. U mag elke gewenste Linux®-distro gebruiken, inclusief de eigen Linux-distro van Microsoft, en CEF- en Syslog-forwarders installeren om logs door te sturen naar Microsoft Sentinel voor ingestion.

Microsoft heeft Sentinel gebouwd om ook algemene formatting-logs in een gemeenschappelijk event format te kunnen gebruiken, zodat zelfs logs van oudere of gespecialiseerde devices kunnen worden geïntegreerd en geanalyseerd.

Volledige beveiliging.

Microsoft Sentinel is het meest effectief als het deel uitmaakt van een bredere, programmatische benadering voor cyberbeveiliging. Zorg ervoor dat uw organisatie gebruikmaakt van best practices in het hele cyberbeveiligingsspectrum: Identificeren, beschermen, detecteren, reageren en herstellen.

INSIGHT-OPLOSSING

Beperk risico's en bescherm uw organisatie.

Insight heeft een robuuste beveiligingspractice en diepgaand inzicht in het IT-beveiligingslandschap. Wij helpen organisaties al meer dan 30 jaar bij het beveiligen van hun gegevens en netwerken. Als groep adviseurs, oplossingsleveranciers en technische specialisten onderhouden we certificeringen en bezitten we diepgaande kennis met betrekking tot de nieuwste beveiligingstechnologieën en best practices.

Dag 2 en daarna:

De flexibiliteit en dynamiek van het platform zal op dit moment duidelijk worden. Op dit moment zijn er verschillende manieren waarop u de voordelen van Microsoft Sentinel drastisch kunt maximaliseren voor de specifieke behoeften en het risicoprofiel van uw organisatie.

1.

Controleer uw logforwarders.

Als u niet goed let op de gezondheid van uw logforwarder en de capaciteit van uw VAR-logmap, kan het snel fout gaan en zal de ingestion van logbestanden stoppen. Wanneer Insight-consultants een Microsoft Sentinel-implementatie uitvoeren, gebruiken we Linux-distro's met een partitie voor het VAR-log-mountpoint dat los staat van het besturingssysteem. Op deze manier heeft het niet zoveel invloed op het besturingssysteem als de directory vol raakt.

2.

Kijk naar uw ingestion percentages.

Het inschatten van het aantal logs dat u aan het begin kunt laten opnemen is lastig, maar na een maand of twee beschikt u over voldoende historische gegevens om een betere besluitvorming rond een geschikt data ingestion percentage te ondersteunen. Dit helpt u een betere kostenoutput te bereiken.

3.

Minimaliseer valse positieve resultaten.

Veel out-of-the-box regels die rapporteren over administratieve functies met behulp van gedragsanalyse kunnen valse positieve resultaten genereren. Microsoft heeft een Sentinel-functie gepubliceerd, genaamd Watchlist, om deze valse positieve resultaten, de ruis die dit veroorzaakt en waarschuwingsmoeheid te helpen verminderen. Met Watchlist kunt u query's (of CSV's van verschillende kenmerken) onderdeel maken van analyseregels die een watchlist of key identifier-paar onderzoeken en niet waarschuwen voor specifieke activiteiten.

4.

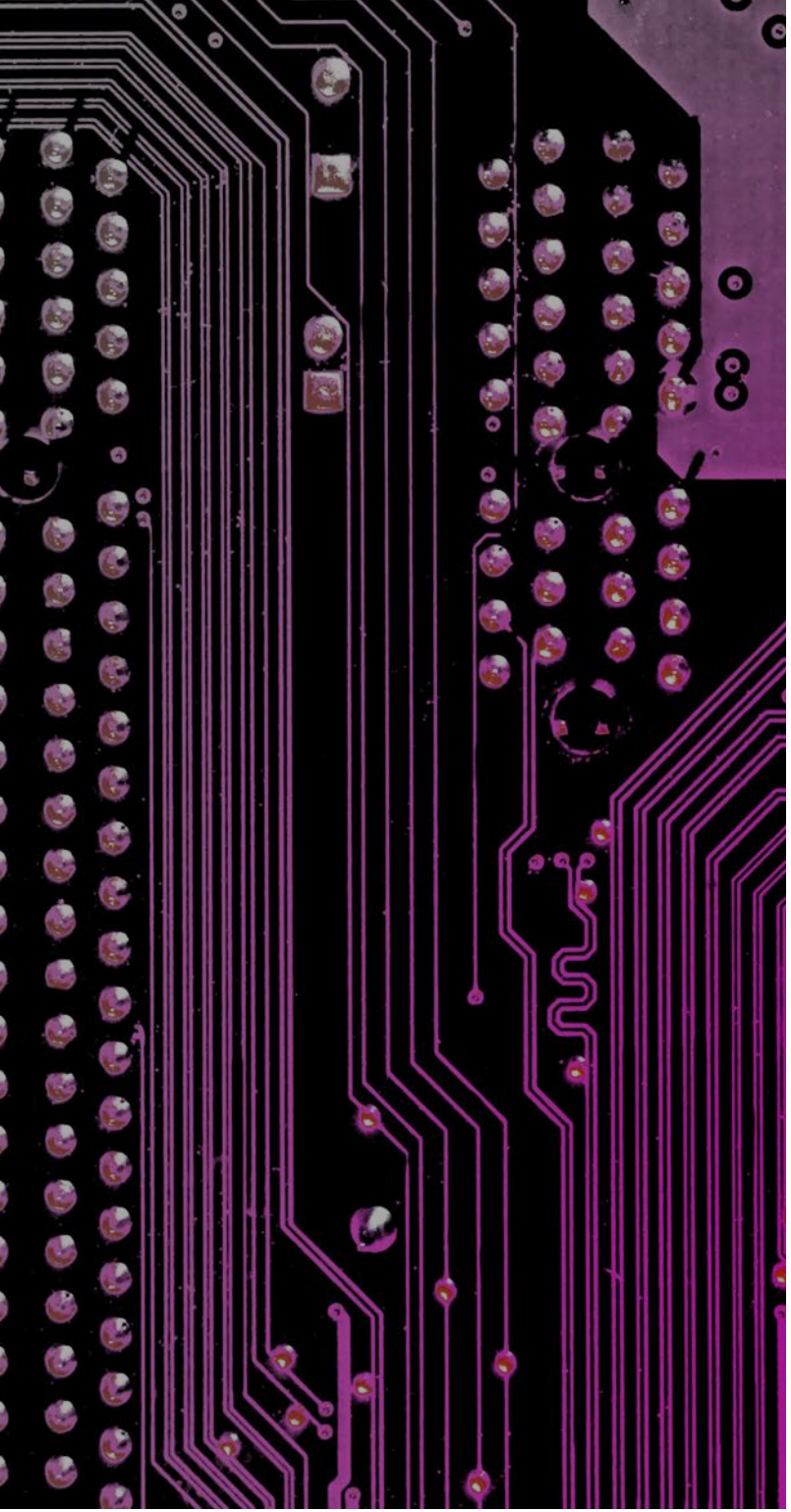
Gebruik een gecentraliseerde tenant.

Als u de monitoring voor verschillende Azure®-tenants uitvoert, moet u verschillende Microsoft Sentinel-installaties en loganalytics-werkplekken in elk van deze tenants maken. U kunt analytische regels instellen, de bron van de waarheid achterhalen en regels implementeren voor alle tenants door Azure Lighthouse te gebruiken om deze werkruimtes in een gecentraliseerde tenant te bewaken. Dit helpt bij het vaststellen van een consistente baseline voor drempels, gebruiksfrequentie en andere instellingen.

Wist u dat?

Als u Microsoft Sentinel gebruikt, hoeven gegevens uit Microsoft-infrastructuur, Office 365®, Microsoft Azure, enz., niet te worden opgenomen en zijn daarom gratis.

Dit is een groot prijsvoordeel ten opzichte van andere SIEM- en SOAR-oplossingen waarbij elk bericht kosten oplevert. Organisaties kunnen ook gebruikmaken van Microsoft-opslag voor meer betaalbare retentieoplossingen.



5.

Voer out-of-the-box detuning uit.

Microsoft Sentinel biedt het duidelijke voordeel van een soepele integratie met uw Microsoft-ecosysteem. Onze consultants adviseren klanten regelmatig om Microsoft Defender for Identity (MDI) te gebruiken voor, bijvoorbeeld, on-premise Active Directory® (AD). Echter, wanneer u MDI in Sentinel inplugt, zal de standaardinstelling automatisch alle waarschuwingen doorsturen die uit MDI komen. U kunt het best naar de plug-inconnector gaan en deze zodanig afstellen dat u niet wordt gewaarschuwd over niet-dringende informatie en alleen waarschuwingen ontvangt binnen een gespecificeerd ernstigheidsbereik.

Onderzoek ook de ernst van bestaande analytische regels en escaleer, de-escaleer of verwijder ze op basis van uw behoeftes. Veel out-of-the-box analytische regels draaien op een ingestelde frequentie die mogelijk te vaak beheerd zal moeten worden. We adviseren om analytische regels elke 15 of 30 minuten te gebruiken voor waarschuwingen met een hoge ernstigheidsgraad, en ze slechts eenmaal per dag uit te voeren voor waarschuwingen met een lage ernstigheidsgraad of informatieve waarschuwingen die weinig zakelijke impact hebben. Uiteindelijk helpt detuning u om waarschuwingsmoeheid en ruis te minimaliseren.

6.

Evalueer of u eruit haalt wat u nodig heeft.

Wat hebt u gebruikt om uw IT-omgeving te beveiligen voordat u gebruik ging maken van Microsoft Sentinel? Wat zijn de overeenkomsten en verschillen? Onze consultants adviseren om uw oude systeem en de Microsoft Sentinel-omgeving en visuele output, dashboards, waarschuwingen, logbronnen en andere belangrijke kenmerken te vergelijken om te controleren of u krijgt wat u nodig heeft. Er mag geen databron achterblijven. Dit helpt u er ook voor te zorgen dat u de nieuwe reikwijdte van dagelijkse taken, zorg en feeding, en personeelsvereisten voor het ondersteunen van het nieuwe platform volledig begrijpt.

7.

Overweeg de richtlijnen van Microsoft.

Microsoft heeft aanbevelingen gepubliceerd voor reguliere activiteiten om ervoor te zorgen dat Sentinel u de best mogelijke beveiliging biedt. Bekijk ze voor suggesties voor dagelijkse, wekelijkse en maandelijkse taken, integraties die u kunt instellen en processen voor het beheren van en reageren op incidenten.

Mogelijkheden voor automatisering

De automatiseringsmogelijkheden zijn een van de sterke punten van het Microsoft Sentinel-platform. Profiteer van automatisering voor optimale efficiëntie en beveiliging.

Hier zijn enkele manieren waarop u kunt automatiseren met Sentinel:

Retentie

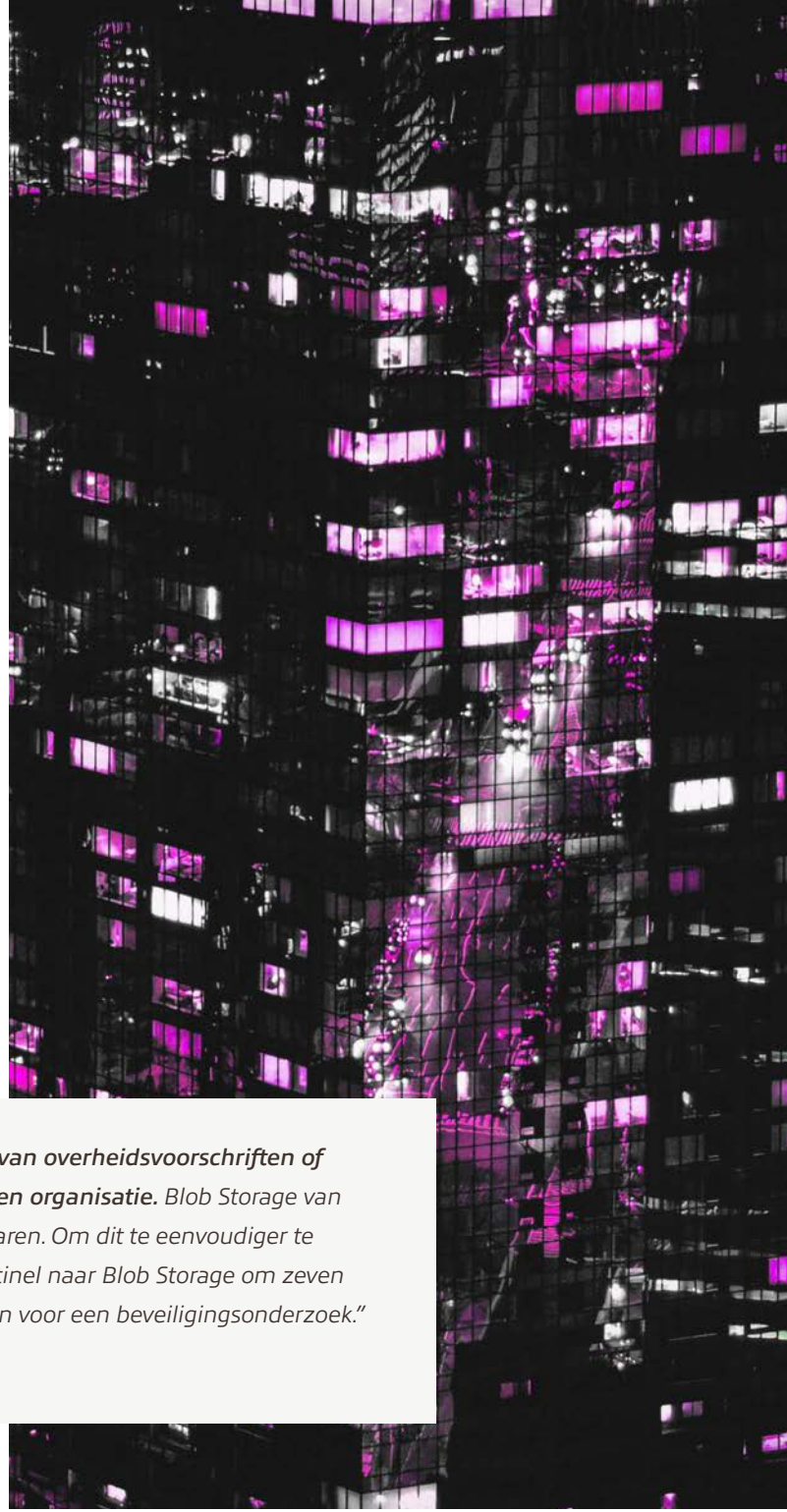
Elke organisatie heeft verschillende behoeftes met betrekking tot het bewaren van data, op basis van de sectorvereisten, de wettelijke eisen en de compliancevereisten. Microsoft Sentinel biedt de mogelijkheid om opslag voor bepaalde perioden te automatiseren, waardoor het ongelooflijk eenvoudig wordt voor uw team om dit te doen zonder herinneringen in te stellen of zich zorgen te maken over capaciteit.

Draaiboeken

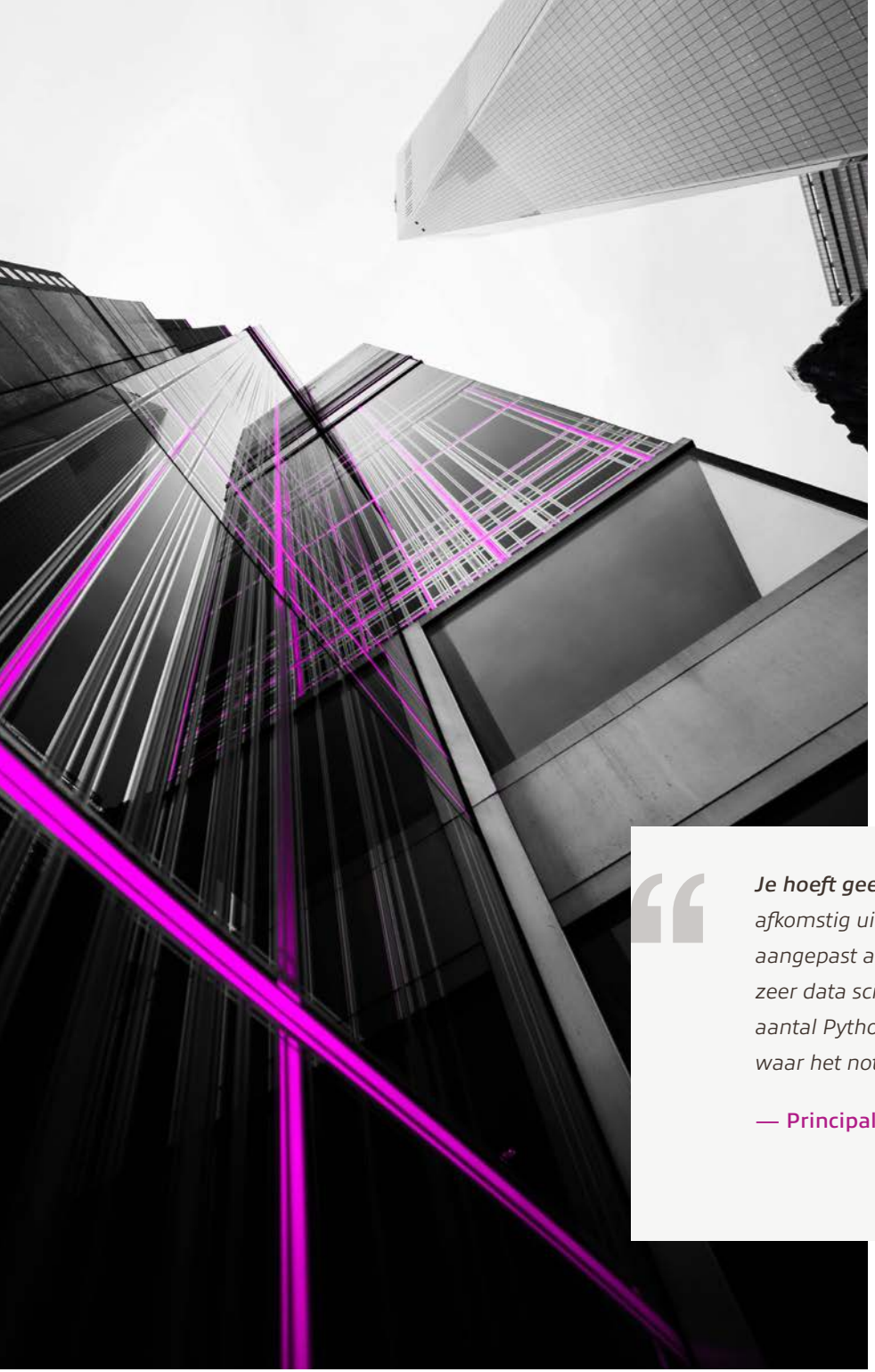
Draaiboeken zijn een uitstekende optie voor complexere automatiseringen. Draaiboeken kunnen binnen Microsoft Sentinel worden ingesteld voor verschillende taken, zoals:

- Een gebruiker blokkeren na een mislukte aanmeldingswaarschuwing
- Een ServiceNow®-incident aanmaken dat in uw ticketsysteem wordt ingevoerd
- De CMDB in ServiceNow aanpassen bij wijzigingen in geblokkeerde devices op het netwerk

GitHub, eigendom van Microsoft, host veel draaiboeken en ideeën voor aanpassingen, evenals leveranciersspecifieke automatiseringen binnen Microsoft Sentinel om te ontdekken.



> ***We hebben klanten die zeven jaar databewaring voor HIPAA willen, of één jaar voor compliance van overheidsvoorschriften of NIST, zogezegd. Het is een uitdaging om uit te zoeken welk bewaarschema het best werkt voor een organisatie.*** *Blob Storage van Microsoft is een goede optie. Hiermee kunt u op kosteneffectieve wijze logs tot zeven of acht jaar bewaren. Om dit te eenvoudiger te maken, creëren we Azure Logic Apps die automatisch opgenomen logs verplaatsen van Microsoft Sentinel naar Blob Storage om zeven jaar te worden bewaard. Organisaties hebben nog steeds toegang tot de logs als ze deze nodig hebben voor een beveiligingsonderzoek."*
>
> **— Associate Consultant, InfoSec, Insight**



Vooruitkijken

Er zijn ontelbare manieren om Microsoft Sentinel uit te breiden en te verbeteren, en de mogelijkheden blijven groeien naarmate het platform en de gebruikers-gemeenschap meer volwassen worden.

BYO ML

Bring Your Own Machine Learning (BYO ML) is een gebied dat veel aandacht krijgt. Deze Microsoft GitHub-pagina fungeert als een opslaglocatie voor de nieuwste informatie en een groeiende bibliotheek met voorbeeldtrainingsnotebooks. Organisaties gebruiken BYO ML om Databricks op te starten en training en analyse te brengen door een Spark-omgeving die alle data uit Sentinel haalt, modellen bouwt voor externe toegang of afwijkend gedrag, en nog veel meer.

> ***Je hoeft geen doctoraat te hebben om dit te kunnen doen.*** *Veel van de training en modellen afkomstig uit de community bieden een vrij goede benadering die alleen maar hoeft te worden aangepast aan uw omgeving. Andere SIEM's hebben iets vergelijkbaars, maar het idee dat u een zeer data science-native ervaring kunt hebben, waar u in principe een Jupiter-notebook hebt, een aantal Python-bibliotheken voor data science, en u gegevens rechtstreeks uit de omgeving haalt waar het notebook draait - dat is interessant voor mij."*
>
> **— Principal Architect (Cybersecurity, Networking, Data Science), Insight**

Geavanceerde visualisatie

Azure Monitor Workbooks bieden rijke datavisualisatie binnen Microsoft Sentinel. Dit is natuurlijk extreem nuttig voor beveiligingsteams. Het zien van de data kan het gemakkelijker maken om zwakke punten en kwetsbaarheden te identificeren, waardoor beveiligingsteams prioriteiten kunnen stellen. Visualisatie kan beveiligingsteams ook helpen bij het rechtvaardigen van budgetten voor de C-suite met een snelle impact. Wij denken dat datavisualisatie een belangrijke focus zal worden in de toekomst. Hierbij zullen communities gebruikers aangepaste workbooks ontwikkelen om aan elke beveiligings- of zakelijke behoefte te voldoen.

INSIGHT-OPLOSSING

Onze Security Services-consultants kunnen u helpen de beveiligingsimplicaties van uw bedrijfsactiviteiten te overwegen en oplossingen te adopteren die zijn afgestemd op uw behoeftes en doelstellingen. We beginnen met het beoordelen van uw huidige omgeving, uitdagingen en vereisten.

Managed Services

Door gebrek aan tijd en middelen kunnen organisaties van vandaag zich alleen

50% herstellen van legitieme beveiligingsbedreigingen.[1]

Veel organisaties vinden het lastig om ervaren beveiligingsprofessionals aan te trekken en te behouden die op de hoogte zijn van de nieuwste SIEM-, SOAR- en Security Operations Center (SOC)-toolsets. We zien al een algehele consolidatie van beveiligingstalent binnen serviceorganisaties die beveiligingsomgevingen op vakkundige wijze kunnen beheren, en cruciale ondersteuning kunnen bieden rond ransomware readiness, beveiligingsarchitectuur, incidentrespons en herstel.

In veel gevallen is tijd de centrale uitdaging. Meer inzicht krijgen in manieren om automatisering uit te breiden of machine learning te gebruiken om beter op jacht te kunnen gaan naar bedreigingen, kan worden overschaduwd door de ontelbare dagelijkse vereisten van het runnen van een beveiligingsteam.

De sleutel tot het verbeteren van uw beveiliging? Managed services.

Insight biedt Managed Security Services (MSS) die voortborduren op de capaciteiten van Microsoft Sentinel en 24/7 monitoring voor uw omgeving bieden. We helpen klanten bij het verminderen van de zware last van het zorgen voor en verbeteren van een dynamische beveiligingsomgeving door in de industrie gevormde best practices te combineren met geavanceerde technieken voor risicominimalisering.

Een geavanceerde aanpak.

Onze Security Services-consultants kunnen u helpen de beveiligingsimplicaties van uw bedrijfsactiviteiten te overwegen en oplossingen te adopteren die zijn afgestemd op uw behoeftes en doelstellingen. We beginnen met het beoordelen van uw huidige omgeving, uitdagingen en vereisten.

16 jaar
ervaring met incident- en bedreigingsbeheer

Meer dan 1500
architecten, technici en experts op het gebied van beveiliging en dienstverlening

Resultaten managed security:


Snellere reactietijden


Sterkere governance en compliance


Rijkere context en zichtbaarheid

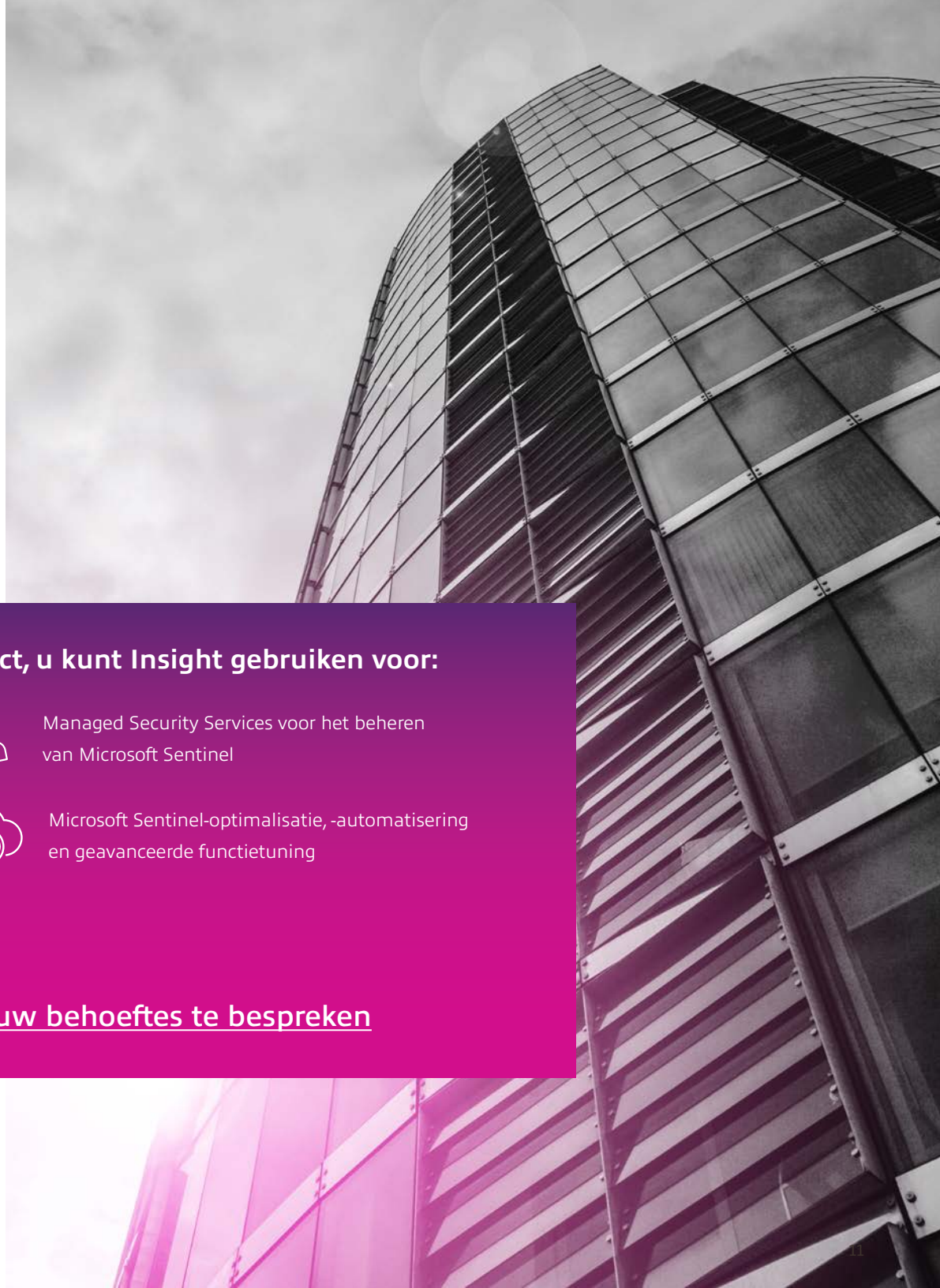

Verbeterde detectie van bedreigingen


Minder zware last voor het beveiligingsteam

De mogelijkheden zijn eindeloos

Microsoft Sentinel is eenvoudig te implementeren, maar vereist extra vaardigheden om goed te optimaliseren.

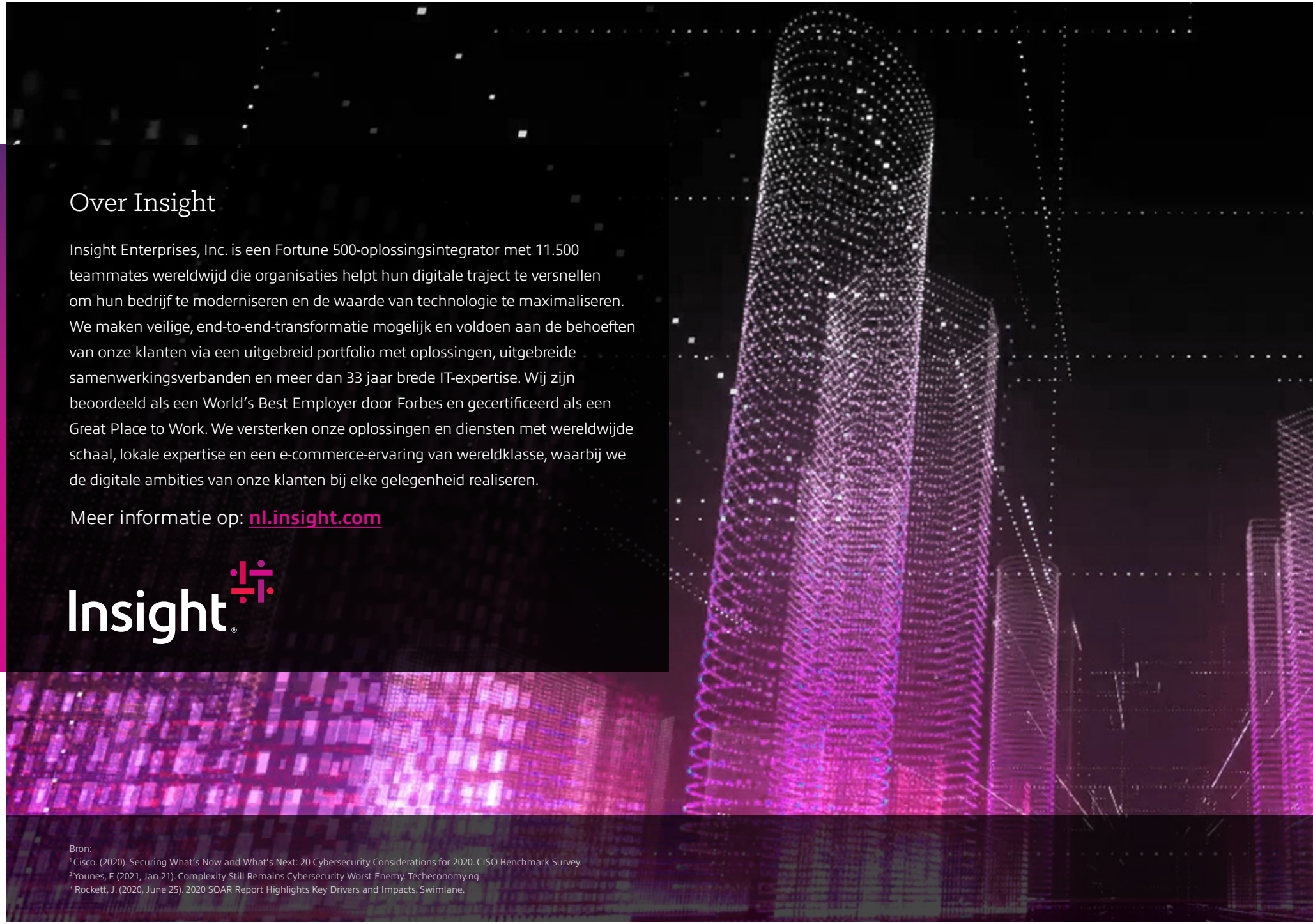
Gelukkig zijn er weinig beperkingen in hoe ver het platform u naar volledige beveiliging kan brengen, en met een vertrouwd team zoals Insight is het eenvoudiger dan ooit om de waarde van uw investering te optimaliseren. Onze consultants, technici en architecten beschikken over toonaangevende expertise voor Microsoft Sentinel in een brede variatie klantomgevingen.



Waar u zich ook bevindt op het Sentinel-traject, u kunt Insight gebruiken voor:

- Evaluatie van uw huidige beveiligingsomgeving
- Een assessment van de gereedheid van Microsoft Sentinel
- Implementatie, integratie en aanpassing van Microsoft Sentinel
- Managed Security Services voor het beheren van Microsoft Sentinel
- Microsoft Sentinel-optimalisatie, -automatisering en geavanceerde functietuning

Neem direct contact op met ons team om uw behoeftes te bespreken



Over Insight

Insight Enterprises, Inc. is een Fortune 500-oplossingsintegrator met 11.500 teammates wereldwijd die organisaties helpt hun digitale traject te versnellen om hun bedrijf te moderniseren en de waarde van technologie te maximaliseren. We maken veilige, end-to-end-transformatie mogelijk en voldoen aan de behoeften van onze klanten via een uitgebreid portfolio met oplossingen, uitgebreide samenwerkingsverbanden en meer dan 33 jaar brede IT-expertise. Wij zijn beoordeeld als een World's Best Employer door Forbes en gecertificeerd als een Great Place to Work. We versterken onze oplossingen en diensten met wereldwijde schaal, lokale expertise en een e-commerce-ervaring van wereldklasse, waarbij we de digitale ambities van onze klanten bij elke gelegenheid realiseren.

Meer informatie op: nl.insight.com

Insight®

Bron:
[1] Cisco. (2020). Securing What's Now and What's Next: 20 Cybersecurity Considerations for 2020. CISO Benchmark Survey.
[2] Younes, F. (2021, Jan 21). Complexity Still Remains Cybersecurity Worst Enemy. Techeconomy.ng.
[3] Rockett, J. (2020, June 25). 2020 SOAR Report Highlights Key Drivers and Impacts. Swimlane.

MKT6231