INSIGHT'S CYBERBEVEILIGING MOGELIJKHEDEN OVERZICHT

Insight

Introductie

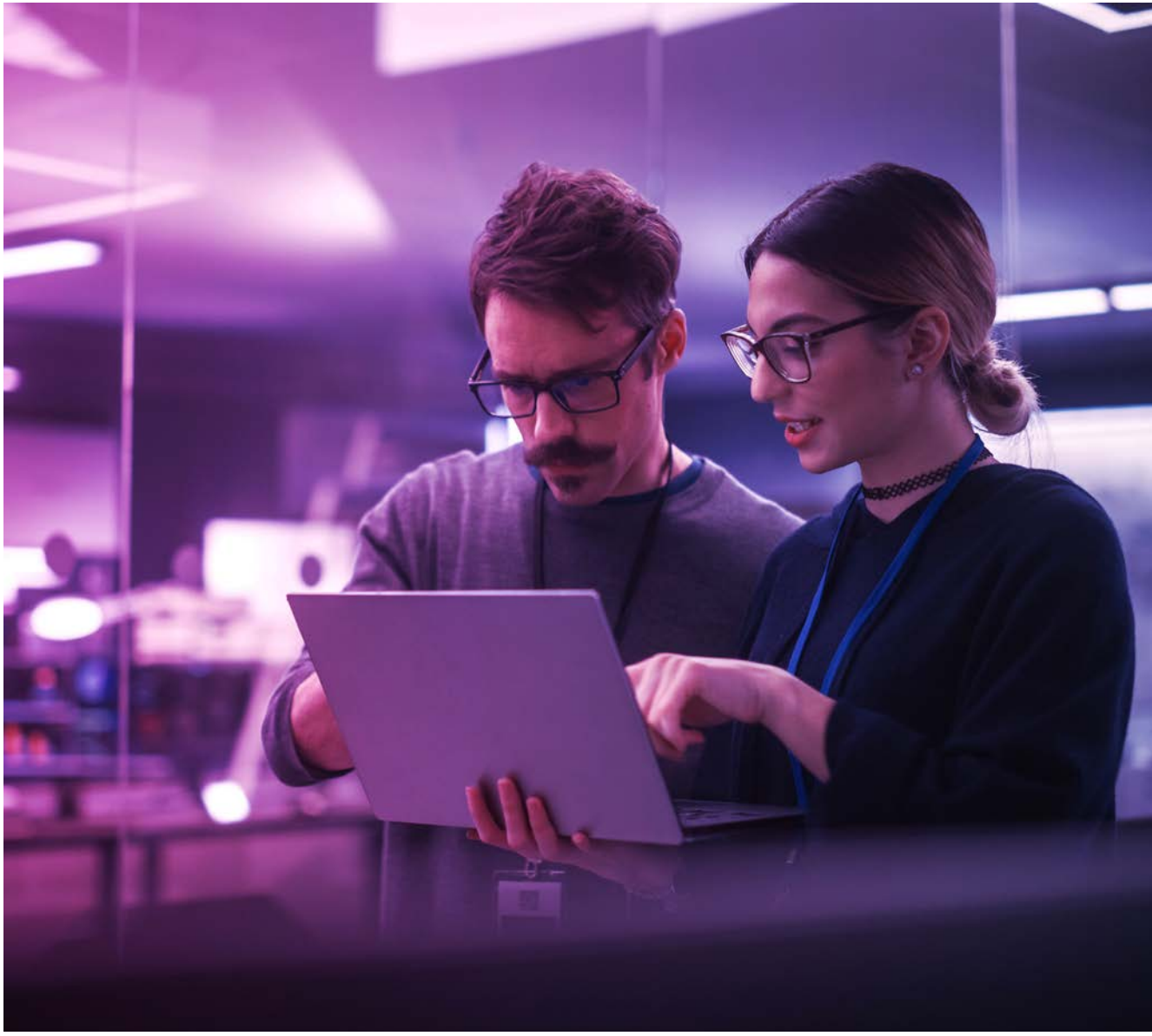
Cyberbeveiliging is belangrijker dan ooit voor bedrijven van elke omvang, omdat cyberdreigingen steeds frequenter en complexer worden. Cyberbeveiligingsinbreuken kunnen verwoestende gevolgen hebben, waaronder financieel verlies, juridische aansprakelijkheid, schade aan het merkimago en verlies van vertrouwen van klanten.

Uw bedrijf beschermen tegen cyberdreigingen is niet alleen een kwestie van compliance of goede praktijken; het is essentieel om uw activiteiten te beschermen en zakelijke continuïteit te waarborgen.

Investeren in robuuste cyberbeveiligingsmaatregelen is een investering in de toekomstige veerkracht en het succes van uw bedrijf. Door effectieve cyberbeveiligingsstrategieën te implementeren, kunt u risico's beperken, dreigingen tijdig detecteren en erop reageren en een sterke verdediging tegen cyberaanvallen opbouwen.

Cyberbeveiliging is niet alleen een noodzaak; het is een strategische noodzaak voor bedrijven die willen gedijen in een veilige en veerkrachtige omgeving.

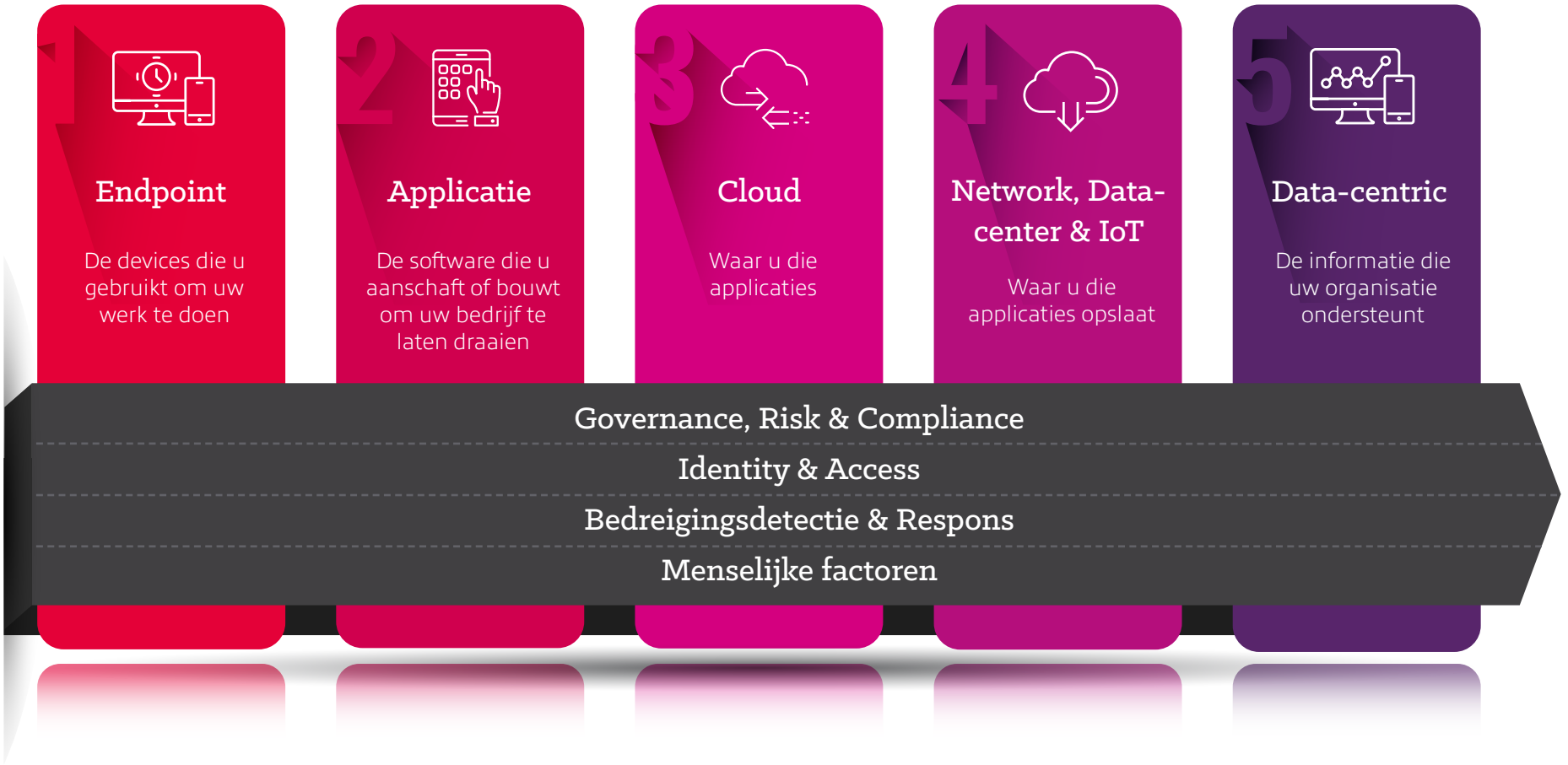
Bij Insight begrijpen we de noodzaak van een uitgebreide aanpak van beveiliging.



De aanpak van Insight voor cyberbeveiliging

Cyberbeveiliging is ingewikkeld – het vereist een complete aanpak van uw eindgebruikers, beveiligingsteams en tools. Daarom hanteren wij een holistische benadering van cyberbeveiliging, zowel op technologisch als op integratiegebied. Deze benadering wordt gerealiseerd via herhaalbare methoden en bewezen processen die succesvolle resultaten opleveren. Onze specialisten begeleiden u van begin tot eind, wat leidt tot verbeterde efficiëntie, effectiviteit en strategische afstemming.

Het totaalconcept van Insight



De aanpak van Insight voor cyberbeveiliging

We beschikken over uitgebreide technische vaardigheden in de vijf technologiedomeinen::

- Endpoints
- Applicaties
- Cloud
- Network, Datacenter & IoT
- Data-centric

Maar als toonaangevende solution integrator begrijpen we dat technische uitmuntendheid in deze domeinen niet voldoende is. Beveiliging moet holistisch worden aangepakt, zodat alle beveiligingsgebieden geïntegreerd en gecoördineerd zijn. Wij doen dit door de toepassing van:

- Governance & compliance
- Identiteit & toegang
- Detectie en respons op bedreigingen
- Menselijke factoren

De hiaten waar de technologiedomeinen met elkaar in verbinding staan, zijn vaak de plekken waar extra waarde kan worden behaald, waardoor uw algehele security-houding op een kosteneffectieve manier kan worden verbeterd.

Wij kunnen u helpen met:

- Het vertrouwen in cyberveiligheid te verbeteren
- De risico's te identificeren en te beperken
- Het verminderen van de complexiteit door overlappende technologieën tot een minimum te beperken.
- De beveiligingsactiviteiten te optimaliseren
- Ervoor te zorgen dat beveiligingscontroles waarde toevoegen en het rendement op uitgaven verbeteren.

Technologiepijlers

Endpoints

De dagen van één device per gebruiker in een bedrijf zijn voorbij, het is meer dan waarschijnlijk dat uw werknemers meerdere devices gebruiken. Endpoints spelen een cruciale rol in cyberbeveiliging voor organisaties en dienen als ingangen voor cyberdreigingen en kwetsbaarheden. De uitdagingen bij het beveiligen van endpoints zijn toegenomen door de snelle toename van verschillende devices, werkomgevingen op afstand en de toenemende verfijning van cyberaanvallen op endpoints. Veelvoorkomende uitdagingen zijn endpoint zichtbaarheid, kwetsbaarheidsmanagement, gegevensbescherming en applicatiecontrole.

Deze devices moeten worden managed, hun beveiligingspositie moet worden bewaakt en bijgewerkt en actieve verdedigingen voor het blokkeren van malware en exploits moeten worden geïmplementeerd en onderhouden. Onze endpoint Security Solutions richten zich op het proces van het beveiligen van endpoints zoals notebooks, desktops, servers en mobile devices, die worden gebruikt om toegang te krijgen tot bedrijfsnetwerken en data.

Wij kunnen u helpen met:

- Inzicht verkrijgen in uw endpoint estate, op device- en applicatie-level.
- Detecteren en reageren op cyberdreigingen in realtime.
- Beschermen van gevoelige gegevens op devices tegen onbevoegde toegang.
- Voorkomen van malware-infecties en cyberaanvallen op endpoints.
- Inzicht krijgen in endpointactiviteiten voor effectieve monitoring.
- Beveiliging van devices voor remote werkomgevingen.

Applicaties

Nu cyberdreigingen voortdurend evolueren, staan bedrijven voor grote problemen. Dit wordt nog verergerd door het feit dat de hedendaagse applicaties steeds complexer worden, met tal van onderling verbonden zaken en integraties met derden, wat resulteert in een breder aanvalsoppervlak Hackers en kwaadwillenden werken voortdurend aan nieuwe technieken om kwetsbaarheden in applicaties te benutten.

Alle organisaties gebruiken applicaties die gepatcht moeten worden om kwetsbaarheden onder controle te houden – zowel op de endpoints van gebruikers als op de serverinfrastructuur. Veel organisaties zullen ook hun eigen applicaties creëren, hetzij via low/no code, hetzij via traditionele ontwikkeling of DevOps. Beveiliging en privacy door ontwerp integreren in de levenscyclus van softwareontwikkeling is cruciaal voor deze organisaties.

Bij Insight kan ons team van ervaren beveiligingsconsulenten u helpen de risico's in uw applicatie-infrastructuur te verminderen. Wij helpen u up-to-date te blijven met kwetsbaarheids- en patchmanagement voor uw off-the-shelf-applicaties en bieden penetratietesten voor alle interne webapplicaties.

Vertrouw op Insight om uw uitdagingen op het gebied van applicatiebeveiliging direct aan te pakken, zodat u verzekerd bent van stevige bescherming en interne gemoedsrust.

Wij kunnen u helpen met:

- Beheren van uw applicatieomgeving om de kwetsbaarheids- en patchcyclus in de gaten te houden.
- Integratie van beveiligingscontroles in uw DevOps-processen zonder afbreuk te doen aan de ontwikkelingssnelheid.
- Detectie en herstel van bedreigingen die via shift-left worden uitgevoerd, waardoor de kosten voor herstel worden verlaagd.

Cloud

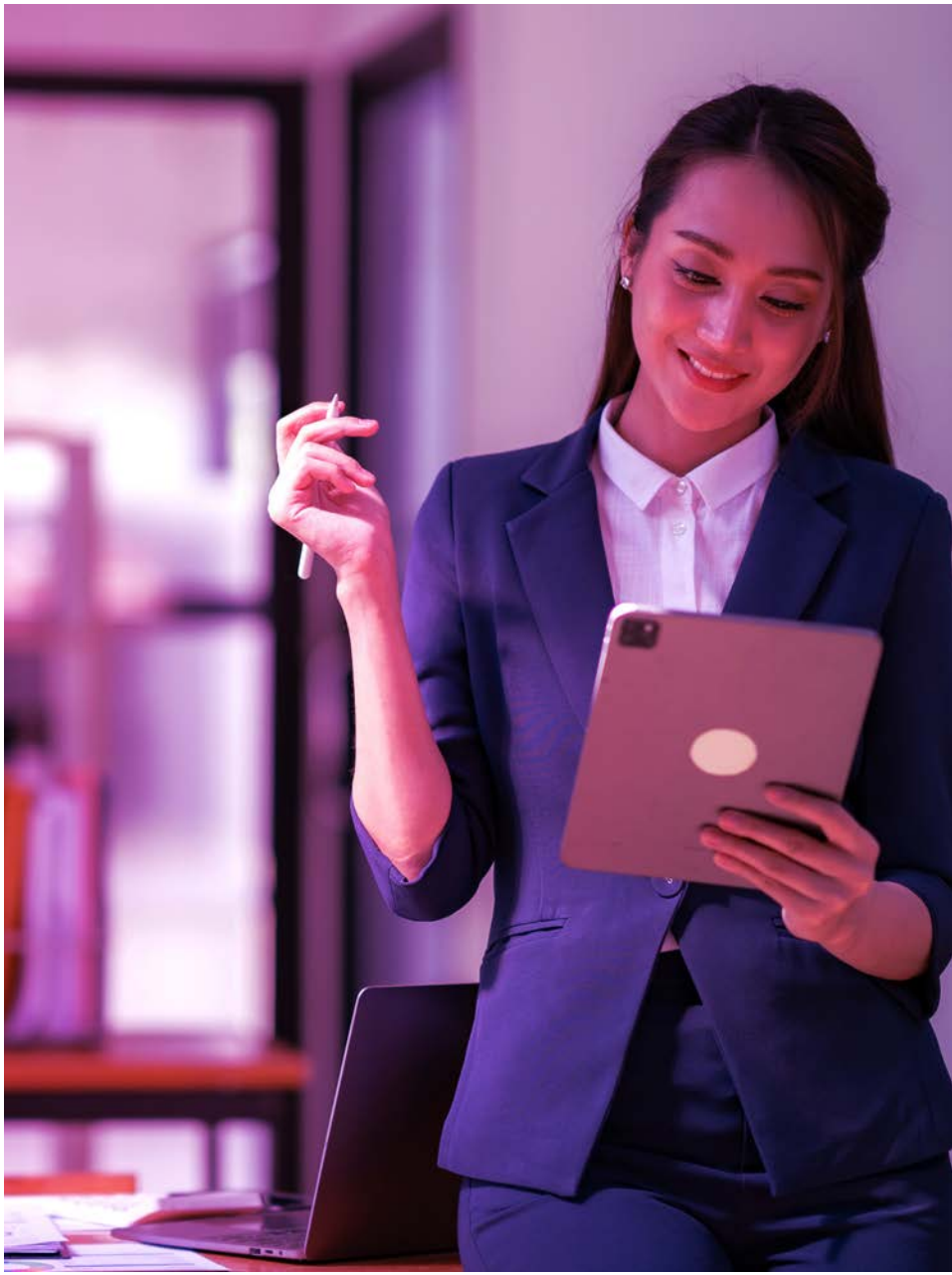
Cloud computing biedt een ongeëvenaarde schaalbaarheid en doeltreffendheid, maar ook grote security challenges. Organisaties moeten hun vertrouwelijke gegevens beschermen tegen ongeoorloofde toegang, inbreuken en kwetsbaarheden en tegelijkertijd de regels naleven en de reputatie van het bedrijf beschermen.

U moet proactief en risicogebaseerd werken en samenwerken met uw cloudproviders om een degelijk beveiligingsframework op te zetten.

De cloud- en beveiligingsspecialisten van Insight hebben jarenlange ervaring met het bouwen, beveiligen en uitvoeren van multi-cloudomgevingen voor bedrijven van elke omvang en complexiteit. We creëren een allesomvattend beveiligingsframework met proactieve bewaking zodat u zich kunt richten op groei, schaalbaarheid en vernieuwingen.

Wij kunnen u helpen met:

- Visibiliteit in uw multicloudomgeving te bereiken.
- Workloads te beveiligen, waar ze ook worden gecreëerd.
- De compliance met de security frameworks te bewaken en te monitoren.



Datacenter, netwerk & IoT

In de moderne, onderling verbonden wereld breidt het digitale landschap zich razendsnel uit. Hierdoor is een complex technologisch web ontstaan dat de deur opent voor toenemende cyberdreigingen, datalekken en ongeautoriseerde toegang.

Om de beveiligingsmaatregelen en veerkracht te creëren die bedrijven vandaag de dag nodig hebben, is een gelaagde aanpak nodig. Een combinatie van firewalls, encryptie,
toegangscontroles en regelmatige beveiligingsaudits is nog maar het begin. U moet de dreigingen voortdurend voor blijven met geavanceerde dreigingsdetectiesystemen en specialistische analyses om potentiële risico's proactief te herkennen en te beperken.

Wij denken met u mee over het oplossen van uw datacenter, networking en IoT security challenges. Met een diepgaande kennis van business, technologie en security creëren we de juiste oplossing voor uw bedrijf – van strategie tot planning en ontwerp, implementatie en managed services. Onze beveiligingsspecialisten kunnen u helpen bij het omgaan met de complexe technologie die nodig is om effectieve cyberbeveiliging te ontwikkelen en te managen, waarbij overlappingen tot een minimum worden beperkt en kosteneffectieve cyberbeveiliging wordt geboden.

We helpen u met:

- Zichtbaarheid in complexe hybride architecturen
- Verbeterde bedrijfscontinuïteit.
- Beveiligingscontroles die werken binnen zowel uw on-premises- als cloudnetwerken.
- Uw gegevens veilig houden van bron tot bestemming.

Data-Centric

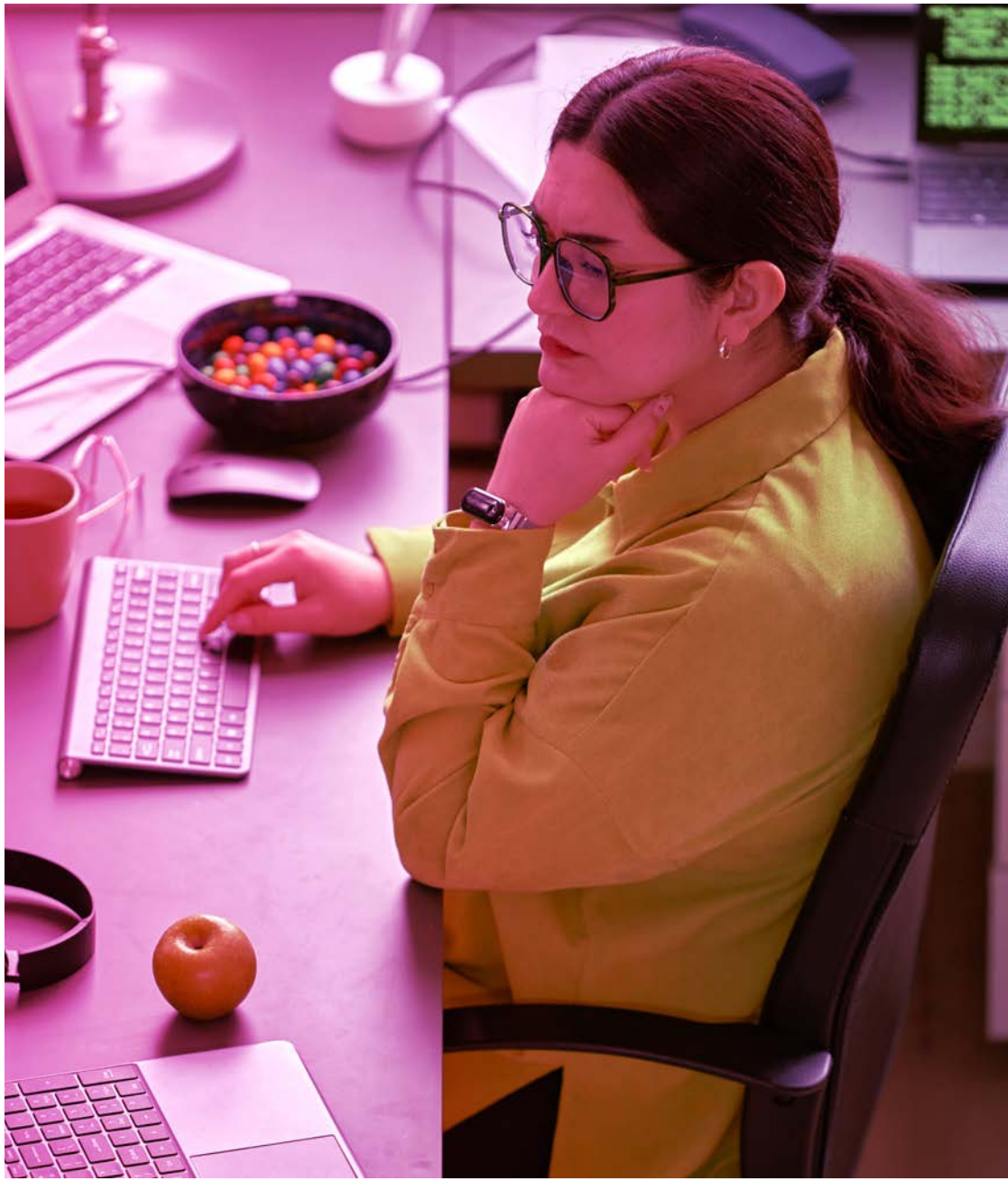
Terwijl beveiligingsprofessionals veel tijd besteden aan het beveiligen van applicaties en infrastructuur, komt bijna alles wat we doen neer op het beveiligen van gegevens. Of het nu gaat om werknemersinformatie, orders van klanten, productiecijfers of intellectuele eigendom, het zijn de gegevens die zich door uw bedrijf bewegen die waarschijnlijk de meeste waarde toevoegen voor uw eindklanten en uw bedrijf.

Een goede plek om te beginnen bij het nadenken over uw totale beveiligingsstrategie is met data. Een datagerichte aanpak moet beginnen met het betrekken van uw businessstakeholders, niet met technologie.

Onze aanpak is gericht op het beschermen van de gegevens zelf, in plaats van alleen het beveiligen van de systemen of netwerken die deze opslaan en verzenden. Wij helpen u voorop te blijven lopen en de meest waardevolle asset van uw bedrijf – uw data – doeltreffend te beschermen.

We helpen u met:

- Detectie van gevoelige en verouderde gegevens in uw gehele omgeving.
- Het classificeren van gegevens om ervoor te zorgen dat de juiste hoeveelheid controle wordt toegepast.
- Naleving van de privacybepalingen.
- Auditeerbaarheid van datagebruik



Integratiedomeinen

Governance, Risico en Compliance (GRC)

Governance, risico en compliance zijn essentiële componenten van cyberbeveiliging voor bedrijven en omvatten het beleid, de procedures en de mechanismen om cyberbeveiligingsrisico's te beheren en naleving van wettelijke vereisten zoals de AVG en NIS2 te garanderen. Organisaties staan voor uitdagingen bij het opzetten van effectieve governancestructuren, het identificeren en beoordelen van cyberbeveiligingsrisico's en het implementeren van robuuste controles om bedreigingen te beperken.

Effectieve GRC-praktijken leggen duidelijke rollen vast, stroomlijnen processen en beperken cyberrisico's. Een solide aanpak verhoogt uw cyberbeveiligingsvolwassenheid, vermindert de legale en financiele verplichtingen , verbetert het vertrouwen van uw klanten en zorgt voor naleving van de regels. Met Insight weet u zeker dat de beveiliging aansluit bij de behoeften van uw bedrijf en deze niet beperkt. Met behulp van risicobeoordelingen op het gebied van beveiliging kunt u de kosten van dat risico berekenen en bepalen waar controles moeten worden geplaatst voor het beste effect. Tegelijkertijd zorgt u ervoor dat de door u geselecteerde controles hun werk effectief doen.

Wij helpen u met:

- Risico's te evalueren
- De meest effectieve controles te bepalen
- Beleid en processen ontwikkelen
- Experts op alle niveaus van de organisatie tot CISO-level

- NIS / NIS2
- DORA
- EU AI act
- ISO27001
- Cyber Essentials/+
- CIS18
- NIST CSF
- PCI-DSS

Identiteit & toegang

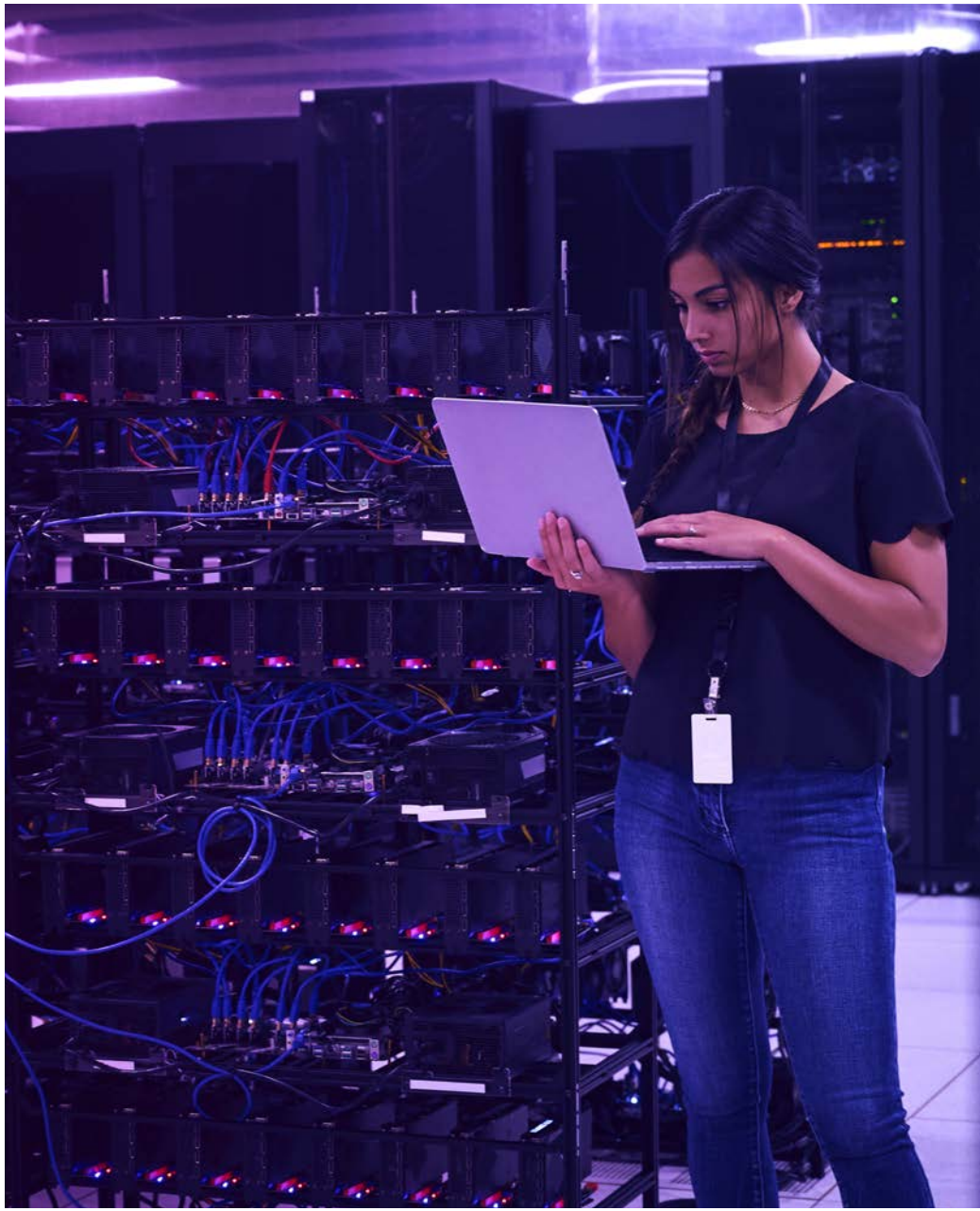
Identiteits- en toegangsmanagement is een cruciaal aspect van cyberbeveiliging voor bedrijven en omvat de processen en technologieën die worden gebruikt om digitale identiteiten te beheren en te beveiligen en de toegang tot resources te controleren. Organisaties staan voor uitdagingen bij het garanderen van veilige en efficiënte praktijken voor identiteits- en toegangsmanagement, zoals het beheren van gebruikersidentiteiten in meerdere systemen, het afdwingen van toegangscontroles met de minste privileges en het voorkomen van ongeautoriseerde toegang.

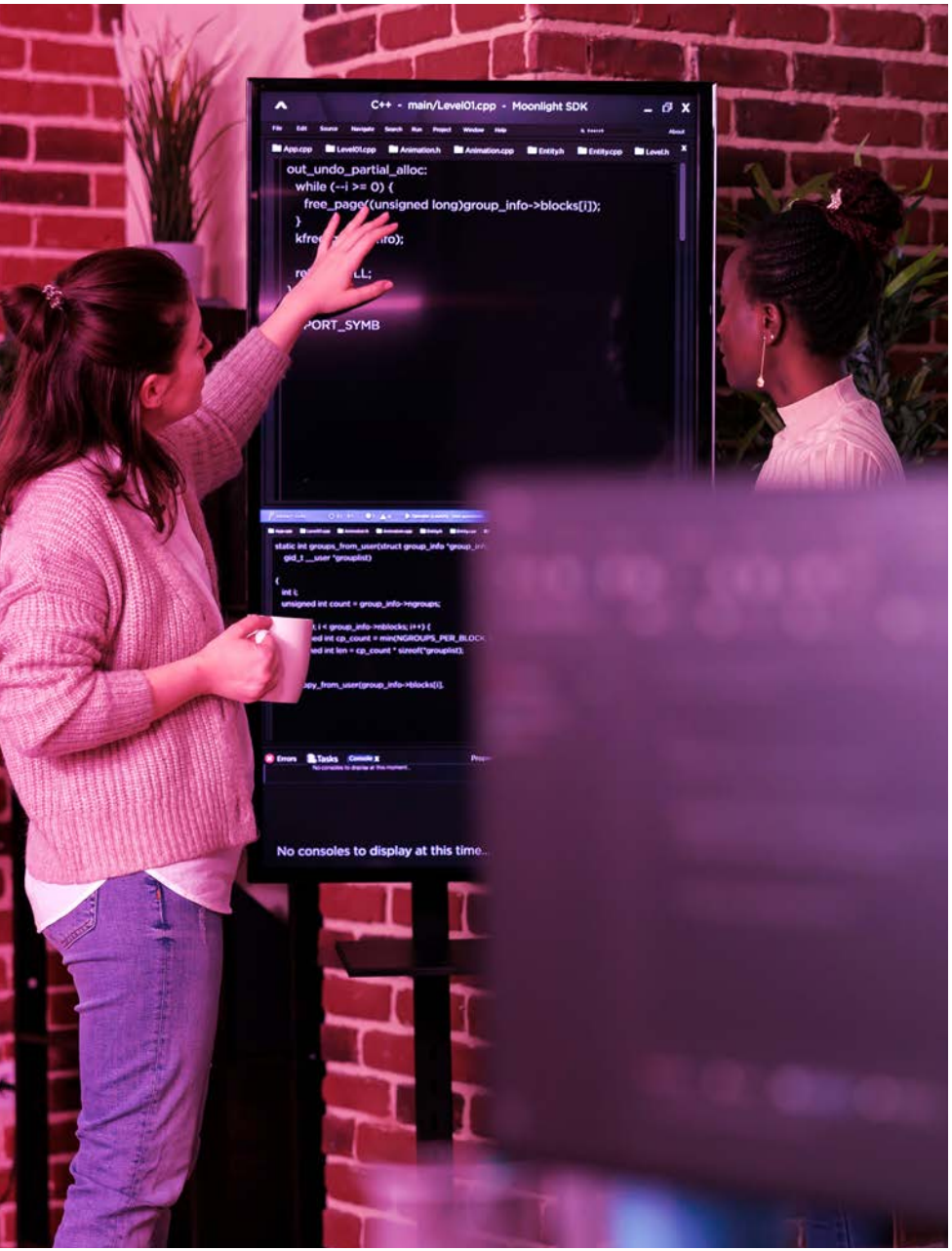
Daar biedt een naadloze identity- en acces-managementoplossing die in al uw technologiepijlers wordt ingezet, een solide en veelomvattende oplossing.

Wij helpen u bij het focussen op het identificeren en beperken van risicogebieden en ondersteunen u vervolgens bij het creëren van kosteneffectieve oplossingen die voldoen aan de vereisten van het beleid en de processen van uw organisatie. U ervaart een verhoogde beveiliging, verminderde risico's en verbeterde efficiëntie met de aanpak van Insight, afgestemd op uw bedrijf.

Dit doen we door:

- De zero-trust-benadering toe te passen
- Te zorgen voor een zakelijke benadering van toegang tot data en applicaties
- Te zorgen dat de juiste mensen toegang hebben tot uw applicaties en gegevens.





Bedreigingsdetectie & Respons

Bedreigingsdetectie en -respons zijn cruciale componenten van een robuuste cyberbeveiligingsstrategie voor bedrijven. Organisaties staan voor talloze uitdagingen bij het identificeren en beperken van cyberdreigingen, waaronder de evoluerende aard van aanvallen, de complexiteit van IT-omgevingen en het tekort aan gekwalificeerde cyberbeveiligingsprofessionals. Effectieve dreigingsdetectie vereist realtime monitoring, analyse van beveiligingsgebeurtenissen en snelle incidentrespons om de impact van beveiligingsinbreuken te minimaliseren.

De security-specialisten van Insight kunnen u helpen bij een meerlagige aanpak van beveiligingsdetectie- en respons-oplossingen binnen de technologiedomeinen in uw bedrijf.

Wij creëren oplossingen met behulp van geavanceerde tools, technologieën en de expertise van onze beveiligingsadviseurs om risico's te identificeren en te beperken voordat ze aanzienlijke schade aan uw bedrijf toebrengen. Insight maakt gebruik van technologie zoals SIEM en XDR, geoptimaliseerd door beveiligingsanalisten die de enorme hoeveelheden data die door uw beveiligingstools worden gegenereerd samenbrengen, om intelligente beslissingen te nemen over bedreigingen in uw hele omgeving.

Wij kunnen u helpen met:

- Bedreigingen eerder te herkennen
- Risico's in uw hele netwerk te verminderen
- U te voorzien van bruikbare informatie over bedreigingen
- Bedreigingsbescherming automatiseren

Menselijke factoren

Hoewel de beveiligingsinfrastructuur, tools en controles voortdurend worden verbeterd en er voortdurend in wordt geïnvesteerd, vinden er nog steeds inbreuken plaats die niet eenvoudig te identificeren en op te lossen zijn. Er zijn veel gespecialiseerde beveiligingscontroles voor verschillende soorten bedreigingen, van aanvallen op endpoints tot aanvallen op supply chains – maar als je bekijkt hoe deze aanvallen daadwerkelijk zijn gebeurd, zijn de drie belangrijkste redenen:

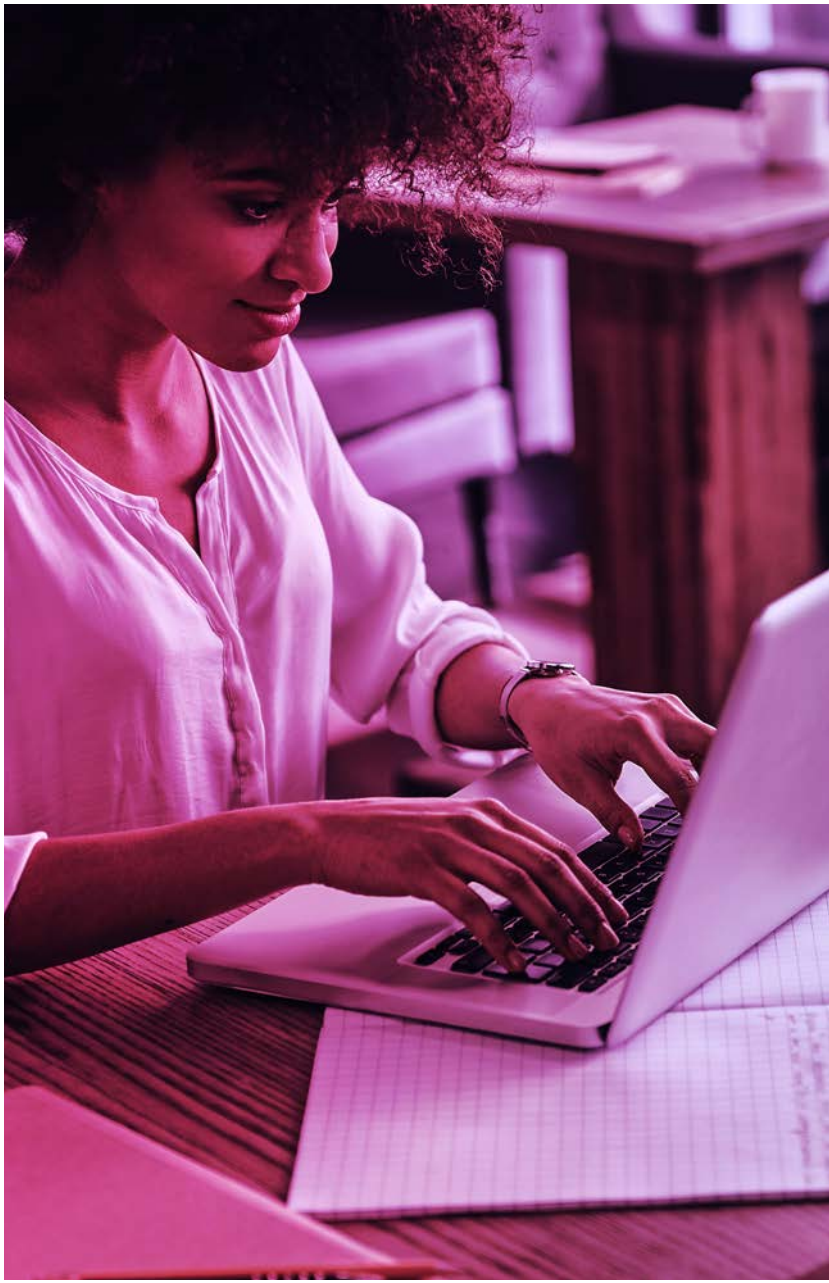
- Wachtwoorden
- Phishing
- Patching

IT-teams kunnen technologie gebruiken om de kans op inbreuken te verminderen, maar eindgebruikers zullen altijd een rol spelen bij de ondersteuning van de beveiliging van een organisatie.

IT -teams concentreren zich vaak op de technologie, en soms het proces, en vergeten de menselijke kant, terwijl mensen het falen of succes van een project kunnen bepalen.
Stel uw werknemers in staat om een ondoordringbare eerste verdedigingslinie tegen cyberdreigingen te worden met Insight. Door een mensgerichte aanpak te hanteren, kunnen we u helpen om kwetsbaarheden snel aan te pakken, uw beveiligingshouding te versterken en risico's te minimaliseren.

Wij helpen u:

- Het bewustzijn van de cyberbeveiliging van eindgebruikers te verbeteren.
- Training te geven aan ontwikkelaars over het coderen met beveiliging in het achterhoofd.
- Ervoor te zorgen dat uw beheerders over de nodige vaardigheden beschikken om een cyberaanval te detecteren en erop te reageren.
- De risico's van succesvolle aanvallen te verminderen.
- Kosten te besparen door datalekken te voorkomen.



Managed security

De grote hoeveelheid veiligheidsuitdagingen is niet-aflatend. Organisaties worden geconfronteerd met een toename van cyberdreigingen, van geavanceerde hackpogingen tot ransomwareaanvallen. Organisaties moeten ingewikkelde wettelijke compliancevereisten naleven, gevoelige gegevens beschermen en de steeds veranderende cyberbeveiligingsrisico's voorblijven. Beveiligingsoplossingen bieden tal van waarschuwingen, maar het is van essentieel belang om te weten op welke u moet reageren om grotere schade aan uw bedrijf te voorkomen.

Deze uitdagingen samen creëren de behoefte aan alomvattende en pro-actieve cyberbeveiligingsoplossingen om bedrijven te beschermen tegen de diverse en complexe dreigingen waarmee ze dagelijks worden geconfronteerd. Weerbaarheid van cyberbeveiliging is van het grootste belang om de continuïteit en het succes van elk modern bedrijf te beschermen.

Dat is waar Insight kan helpen – ons team van ervaren beveiligingsspecialisten is 24/7 beschikbaar, met ondersteuning om uw cyberbeveiliging te verbeteren met proactieve threat monitoring, detection en response met toegang tot geavanceerde technologieën.

Ons Security Operations Centre (SOC) biedt twee managed services met geavanceerde functies voor het opsporen, onderzoeken en reageren op dreigingen:

- **Managed Endpoint Detection en Response (MEDR)** Voor notebooks, desktops en mobile devices.
- **Managed Extended Detection en Response (MXDR)** Waarbij logs en feeds uit allerlei bronnen worden verzameld en de beste detectiemogelijkheden biedt voor uw omgeving.
- Combining technologies such as AI, threat intelligence and analytics, our team of expert security analysts can detect and respond to threats to your environment in real-time.

Dit doen we door:

- Proactief threat management
- Specialistische beveiligingsanalyses en incident response.
- Toegang tot geavanceerde beveiligingstechnologieën.
- Beveiligingsstrategie en roadmapbegeleiding.
- Een schaalbaar, kostenefficiënt model

Het proces

Helpt u bij het strategiseren, implementeren en beheren van toekomstbestendige IT-beveiligingsoplossingen.

Assessment

- Helpt u bij het verkrijgen van accreditatie volgens industriekaders zoals ISO27001 of NIS2.
- Bekijk uw bestaande beveiligingsmaatregelen en identificeer resterende risico's.
- Help bij het opstellen van een geprioriteerde roadmap om uw gewenste security level te bereiken.

Planning en ontwerp

- Helpen bij het vertalen van uw zakelijke uitdagingen naar beveiligingsprojecten.
- Ondersteuning en begeleiding bij het selecteren van de juiste leveranciers, producten en diensten.
- Envisioning Workshops en technisch ontwerp.

Bouwen & Implementeren

- Plannen omzetten in realiteit – van ontwerp tot volledig gebouwde en gedocumenteerde beveiligingscontroles
- Insight bekijkt elk project in de context van uw algemene roadmap
- Overdracht aan uw interne teams voor management of transitie naar onze Managed Services

Security Operations Management

- Support services zorgen ervoor dat uw beveiligingscontroles optimaal werken.
- Managed Services waarbij Insight de verantwoordelijkheid neemt voor uw beveiligingscontroles.

Onze Security Technology Partners

IT-modernisering is een teaminspanning. We bundelen de capaciteiten van 6.000+ software-, hardware- en cloudpartners en -uitgevers met de uitgebreide branche-expertise van ons team onder één dak om de beste oplossingen te creëren die uw transformatietraject versnellen.

Wij werken rechtstreeks samen met toonaangevende technologiebedrijven, zodat u kunt profiteren van:

- Eén aanspreekpunt voor toegang tot de nieuwste producten en oplossingen op het gebied van technologie.
- Een ecosysteem van samenwerkende, zeer bekwame teams om uw IT-omgeving uit te rusten en te beheren.
- Concurrerende prijzen en gestroomlijnde contractonderhandelingen.
- Partneronafhankelijke oplossingen op maat van uw specifieke behoeften.

Microsoft · cisco · aws · Google · paloalto NETWORKS · FORTINET · KnowBe4 · Barracuda · Check Point SOFTWARE TECHNOLOGIES LTD.

Waarom samenwerken met Insight?

Cyberbeveiliging is ingewikkeld – het vereist een complete aanpak van uw eindgebruikers, beveiligingsteams en tools. Daarom hebben we herhaalbare methoden en bewezen processen ontwikkeld die succesvolle resultaten opleveren. Onze specialisten begeleiden u van begin tot eind, wat leidt tot verbeterde efficiëntie, effectiviteit en strategische afstemming.

We hebben:

20+ jaar kennis en ervaring in beveiligingstransformatie

Diepgaande partnerschappen met topleveranciers

Oplossingsonafhankelijke aanpak om oplossingen te vinden die het beste zijn afgestemd op uw behoeften.

Member of Microsoft Intelligent Security Association

Microsoft Security

Microsoft Verified Managed XDR Solution

Cisco Partner

Advanced Security Architecture Specialized
SASE Specialized
XDR Specialized

Gold Microsoft Partner

Microsoft

Azure Expert MSP

Microsoft Solutions Partner
Microsoft Cloud

Microsoft Solutions Partner
Security

Specialist
Cloud Security
Identity and Access Management
Information Protection & Governance
Threat Protection

Volgende stappen

Neem contact op met Insight om uw cyberbeveiligingsstrategie en dagelijkse activiteiten te verbeteren. Nu cyberbeveiligingsbedreigingen toenemen, is het beschermen van uw bedrijf cruciaal voor continuïteit en succes. Onze uitgebreide aanpak verbetert de cyberbeveiligingspositie, identificeert en beperkt risico's, stroomlijnt activiteiten, optimaliseert beveiligingscontroles en maximaliseert investeringen. Vertrouw op de bewezen methoden en deskundige begeleiding van Insight om uw cyberbeveiliging te versterken en de veerkracht en groei van uw bedrijf te stimuleren.