4 manieren waarop Microsoft Sentinel de belangrijkste IT-beveiligingsproblemen aanpakt

Maximaliseer de voordelen en capaciteiten van uw beveiligingsinvestering.

Insight

Microsoft

Goed kijken naar het dreigingslandschap

Het vinden van de juiste combinatie van tools, technologieën en vaardigheden is cruciaal voor het runnen van een succesvol Security Operations Centre (SOC). Dit geldt met name omdat het aantal cyberaanvallen recentelijk snel is toegenomen. Houd er nu rekening mee dat de gemiddelde kosten van een inbreuk veroorzaakt door ransomware in 2021 $ 4,62 miljoen bedroegen.[1] Dat is veel potentiële schade. Het is dus geen verrassing dat IT-beveiligingsteams over de hele wereld onder druk staan om de responstijd te verbeteren en toekomstige verliezen te voorkomen.

Om deze groeiende trend tegen te gaan, is de verwachting dat bedrijven in 2022 gemiddeld $ 24,4 miljoen uitgeven aan IT-beveiligingsbudget.[2] Iedereen die data op locatie en in de cloud wil onderbrengen, zal de bestaande oplossingen opnieuw moeten beoordelen om volledige dekking te kunnen garanderen voor alle operationele locaties, thuiskantoren, communicatiesystemen en alles daartussenin.

De groei van eindpoints en datavolumes vereist schaalbare beveiliging.

Pointoplossingen bieden beperkte reikwijdte en extra integratie-uitdagingen.

Het vinden en behouden van cruciaal beveiligingstalent is lastiger geworden.

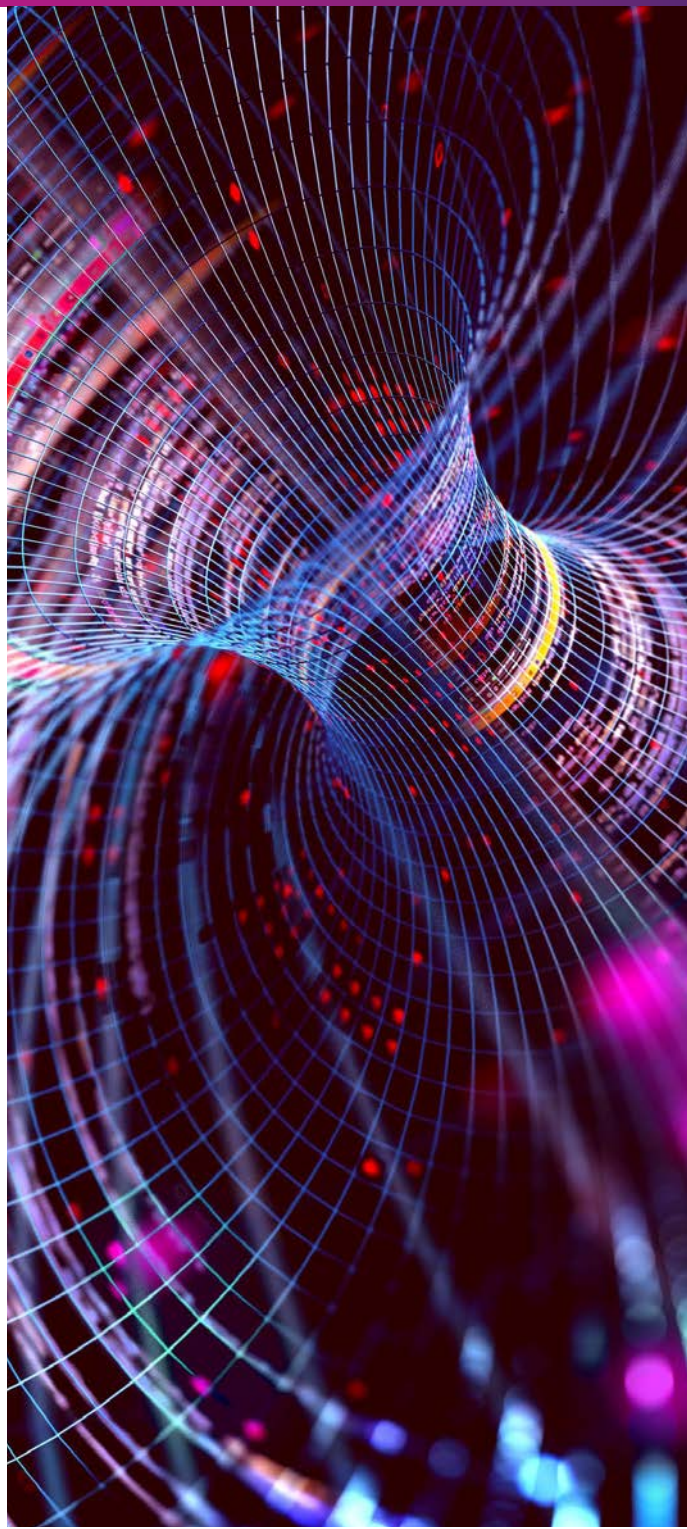
IT-omgevingen worden steeds complexer waardoor talloze vectoren voor aanvallen ontstaan.

Denk goed na over uw data, gebruikers en systemen.

Volledige zichtbaarheid is van cruciaal belang voor het detecteren en voorkomen van potentiële schade, evenals het kunnen exploiteren van meerdere systemen vanaf één enkel beginpunt en het verkrijgen van controle over de gehele IT-omgeving. Wanneer het bedrijven gemiddeld 280 dagen kost om een inbreuk te detecteren, kan een ontelbare hoeveelheid data, dossiers en systemen worden aangetast voordat er überhaupt stappen worden ondernomen om de inbreuk te bestrijden. De implementatie van identiteits- en toegangsbeheer is een manier om de zichtbaarheid te verbeteren en deze roadblock minder groot te maken. De capaciteit om gebruikersgedragstrends te volgen en patronen te ontdekken, biedt bedrijven de mogelijkheid om het herstelvenster te sluiten en gaps aan te pakken die voorheen onopgemerkt bleven.

Stel uzelf de volgende vragen bij het implementeren van identiteits- en toegangsbeheer:

- Hoe gevoelig is uw data?
- Wie heeft echt toegang nodig tot specifieke bestanden?
- Wanneer en voor hoe lang is toegang nodig?
- Moet u een dataclassificatieprogramma starten?
- Hebt u gebruikerstypen ingesteld?
- Wanneer hebt u de machtigingen voor het laatst gecontroleerd?
- Hoe verifieert u identiteiten en toegangspunten?
- Welke alternatieven hebt u overwogen voor authenticatie?
- Zou biometrie een zinvolle keuze zijn?
- Hebt u duidelijke gaps of patronen opgemerkt?
- Hoe zou u uw huidige aanpak veiliger kunnen maken?



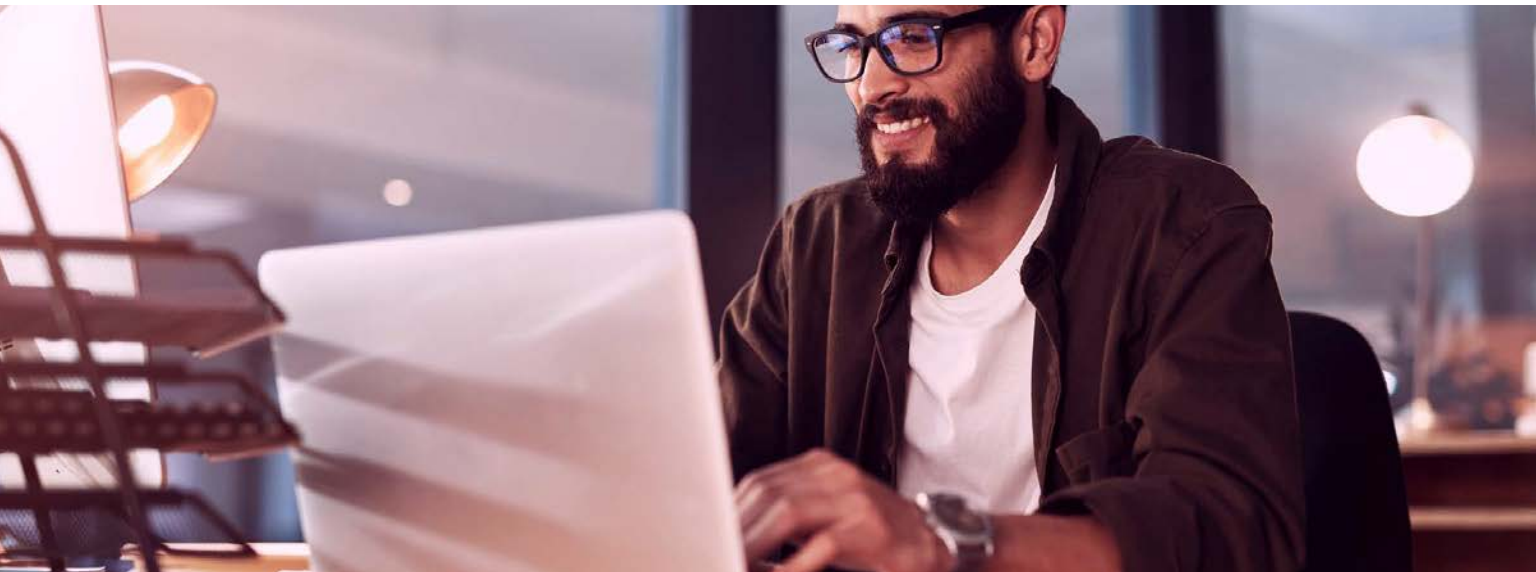
Het begin van een modern beveiligingsprogramma

Het kan nuttig zijn om op te merken dat 89% van de bedrijven al een multicloud-aanpak in gebruik heeft genomen of van plan is om deze te implementeren.[4] Als uw bedrijf onderdeel is van deze meerderheid, hebt u mogelijk een diverse IT-omgeving bij de hand. Als u gegevens, kwaadwillende hackers en meer succesvol kunt volgen, zal dit de effectiviteit van de preventie-inspanningen van uw IT-beveiligingsteam vergroten. Een ander belangrijk kenmerk van een robuust programma is uitgebreide governance dat is gericht op verantwoordelijkheid en aansprakelijkheid. Bedrijven kunnen richtlijnen en training beter organiseren en gebruikers en processen valideren door beveiligingsdoelstellingen, rollen en processen duidelijk te definiëren.

Iets anders om rekening mee te houden is dat 57% van de ondervraagde bedrijven in het rapport "The State of IT Modernisation 2020" zei dat het upgraden van beveiligingsinfrastructuur en -processen een groot obstakel was bij hun streven naar de modernisering van hun IT-bedrijfsomgevingen.[3] Een externe partner kan hier mogelijk toegevoegde waarde bieden via automatiseringsdiensten.

Automatisering binnen het SOC levert:

- Snellere detectie-, respons- en herstelmogelijkheden
- Minder fouten en minder "waarschuwingsmoeheid"
- Beveiligingsmiddelen bevrijd van repetitieve taken
- Verbeterde gebruikerservaring en tevredenheid



Investeren in een cloud-native SIEM-oplossing

Microsoft Sentinel is een cloud-native oplossing voor Security Information and Event Management (SIEM) en Security Orchestration Automation and Response (SOAR) die wordt geleverd als een cloudservice. Bedrijven kunnen bedreigingen stoppen voordat ze schade veroorzaken door gebruik te maken van de capaciteit om intelligente beveiligingsanalyses te bieden voor de hele omgeving. Als schaalbare, evergreen-oplossing verbetert of vervangt Microsoft Sentinel uw bestaande beveiligingstools om de zichtbaarheid van uw bedreigingslandschap te vergroten.

- Krijg een volledig perspectief op uw hele bedrijf.
- Stroomlijn detectie en respons met Artificial Intelligence (AI).
- Elimineer het instellen en onderhoud van de beveiligingsinfrastructuur.
- Schaal om te voldoen aan veranderende beveiligingsbehoeften.

Als extra bonus verlaagt deze oplossing de kosten met 48% en kan 67% sneller worden geïmplementeerd dan traditionele SIEM's.[5] Hierdoor kunnen bedrijven meer tijd besteden aan het snel vinden van de echte bedreigingen door gebruik te maken van meer strategische beveiligingsactiviteiten. Dus hoe werkt het precies? Hoe maakt het gebruik van AI en machine learning om bedreigingen te detecteren, analyseren en onderzoeken? We gaan op de volgende pagina verder in op het vierstappenproces.

4 stappen naar next-gen beveiligingsactiviteiten

1. Verzamelen

Bedrijven hosten tegenwoordig documenten, data, records en meer op een groot aantal devices, toepassingen en infrastructuur, zowel on-premise als in meerdere clouds. Bovendien hebben gebruikers vrijwel altijd en overal toegang tot al deze gevoelige bestanden. Microsoft Sentinel verzamelt data op cloudschaal, waarbij infrastructuur- en beveiligingsdevices zoals firewalls worden samengevoegd.

2. Detecteren

Het vinden van reguliere voorvallen en cyberaanvallen kan bedrijven helpen om iets te doen aan specifieke bedreigingen. Analyse en ongeëvenaarde informatie over bedreigingen helpen bedrijven zelfs om eerder niet-detecteerbare bedreigingen te ontdekken en de kans op valse positieve resultaten te minimaliseren. Stelt u zich eens voor dat u miljoenen afwijkingen tegelijkertijd kunt monitoren en verbanden kunt leggen, en vervolgens snel waarde uit het rapport kunt halen. Dat is wat deze oplossing biedt.

3. Onderzoeken

Microsoft Sentinel maakt gebruik van tientallen jaren ervaring met cyberbeveiliging bij Microsoft en gaat met behulp van AI op schaal op jacht naar verdachte activiteiten, waardoor hardware of virtuele machines niet meer nodig zijn. Het leert van dagelijkse logs wat belangrijk is, zodat beveiligingsteams zich kunnen concentreren op de essentiële signalen.

4. Reageren

Met ingebouwde orkestratie en de automatisering van veelvoorkomende taken kunnen bedrijven snel reageren op incidenten. Het gebruik van intelligente technologie bespaart uw IT-beveiligingsteam niet alleen tijd, maar verbetert ook de nauwkeurigheid. Draaiboeken die worden geactiveerd door analyse- of automatiseringsregels kunnen bijvoorbeeld binnen Microsoft Sentinel worden uitgevoerd om de responstijd te stroomlijnen en kwaadwillende partijen te blokkeren.

Waarom Insight voor Microsoft Sentinel?

Bij Insight geloven we dat dit hét moment is om uw beveiligingsstatus te verbeteren, vooral met de toename van werken op afstand en hybride werken. Vertrouw op onze jarenlange ervaring om uw bedrijf te beschermen tegen groeiende cyberdreigingen. Samen helpen we uw bedrijf bij het verkrijgen van een flexibele, schaalbare oplossing die gebruikmaakt van geavanceerde AI- en machine learning-capaciteiten. Het doel: verbeterde beveiliging, zichtbaarheid en controle over uw gehele IT-omgeving.

We zijn een toppartner van Microsoft en een van de slechts 12 partners die door Microsoft publiekelijk worden genoemd voor advies en het leveren van Microsoft Sentinel-diensten:

- 18 Microsoft Gold- en Silver-competenties
- Meer dan 25 jaar als Microsoft-partner
- Meer dan 1000 op Azure gerichte technici en serviceprofessionals
- Een Azure Expert Managed Services Provider (MSP) en grootste Azure-partner
- Winnaar van de Microsoft Security 20/20 Award voor de categorie Azure Security Deployment Partner of the Year
- Ondersteuning tijdens het volledige proces en levering van consultatiediensten

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.

Insight®

nl.insight.com

Bron:

[1] IBM Security. (2021). Cost of a Data Breach Report.

[2] Channel Futures. (Februari 2022). The High Cost of Ransomware.

[3] Insight. The State of IT Modernisation 2020.

[4] Flexera. (Maart 2022). 2022 State of the Cloud Report.

[5] Forrester. (November 2020). The Total Economic Impact™ of Microsoft Sentinel. Cost Savings and Business Benefits Enabled By Microsoft Sentinel.

MKT6231