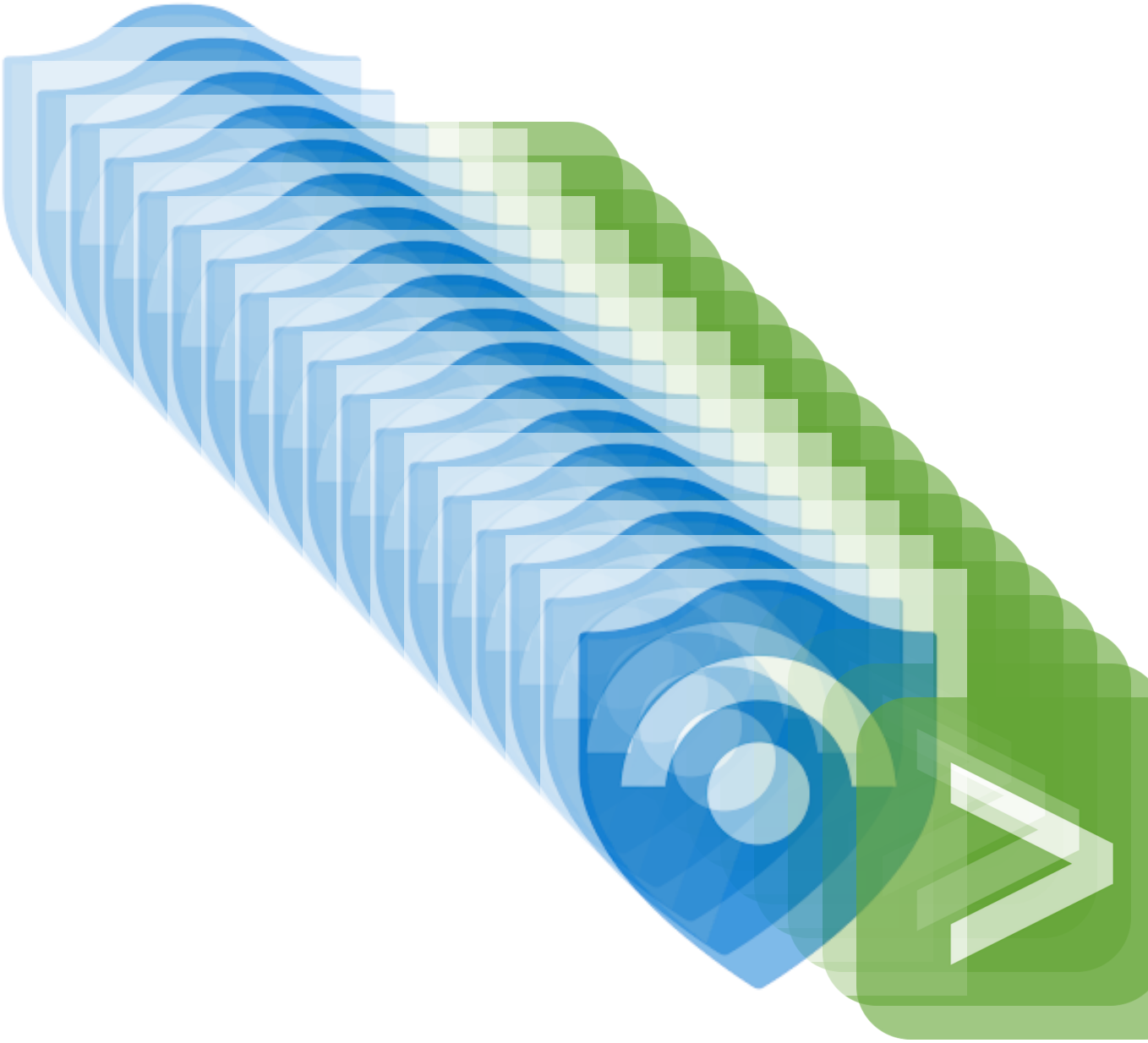
De 'hulp bij het kiezen van een SIEM' handleiding

henk-sjoerd hinrichs



Azure Sentinel & Splunk

Intro
handleiding

Deze handleiding is bedoelt als hulpmiddel bij het kiezen van een SIEM oplossing. Het gaat daarbij om de keuze tussen Splunk en Azure Sentinel. De handleiding is voorzien van informatie en werkbladen en daardoor een interactief document. De uitkomsten van de werkbladen spelen een adviserende rol in de keuze omtrent de SIEM oplossing. Deze handleiding is bedoelt voor de consultant van Avanade en de klant.

De opbouw van de handleiding is chronologisch en daarom adviseer ik om van voor naar achter te werken.

aanleiding

Recent heeft Microsoft Azure haar eigen SIEM (Security Information Event Mangement) gelanceerd, genaamd Azure Sentinel. Een SIEM is tooling (een gereedschap) voor een security team dat alle data op het netwerk, die een relatie heeft met informatiebeveiliging, verzamelt en analyseert. Het security team gebruikt deze analyses om kwetsbaarheden te ontdekken en mogelijke aanvallen te signaleren.

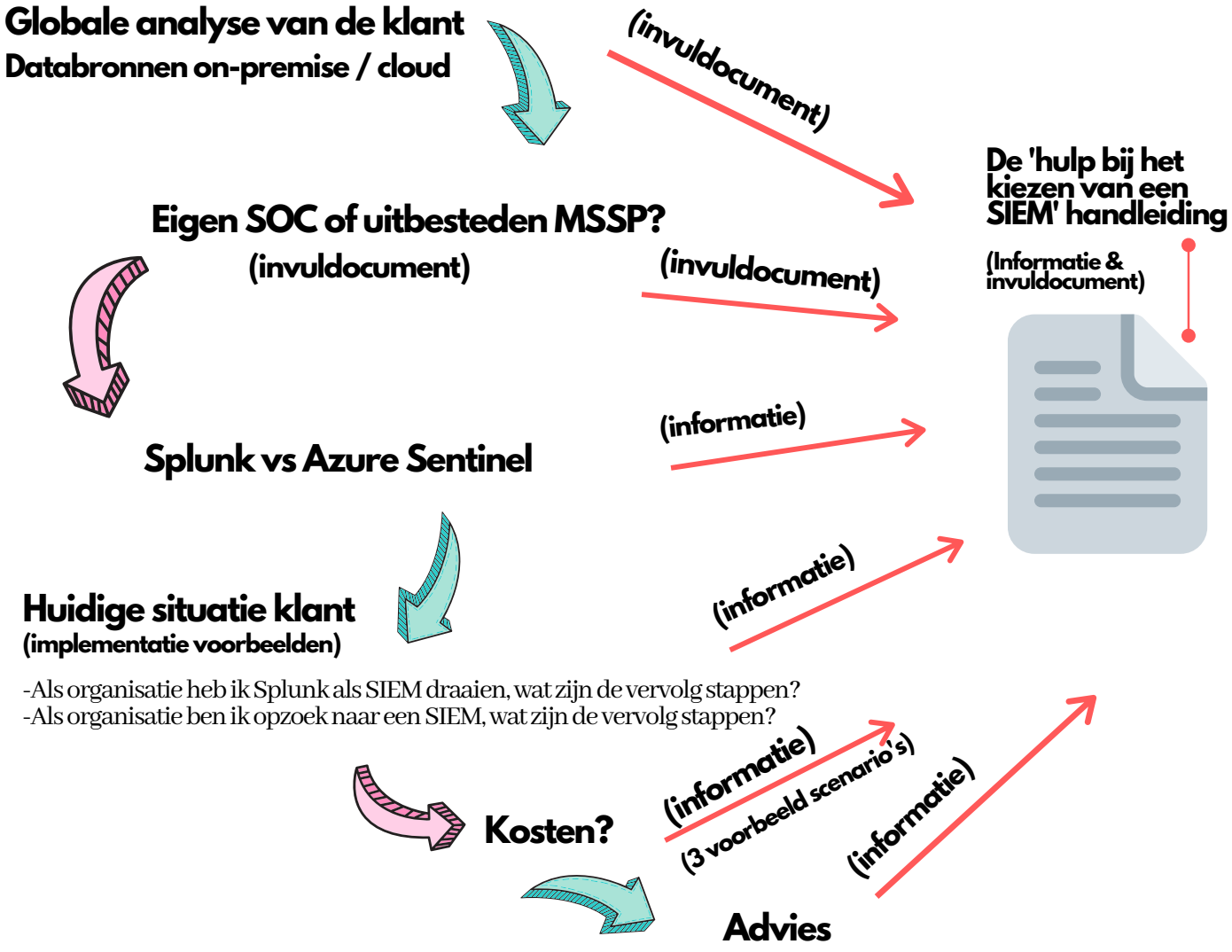
Hierboven beschreef ik al wat SIEM tooling betekent. Deze tool wordt gebruikt door het security team. Het security team bevindt zich in de SOC (Security Operations Center). De SOC is de plaats binnen een organisatie die alle IT-security gerelateerde zaken kan analyseren, begeleiden en uitvoeren.

Om een centraal inzicht te krijgen in security gerelateerde events uit verschillende omgevingen zijn klanten van Avanade meermaals op zoek naar een centrale oplossing. Op dit moment genereert Avanade zelf ongeveer 50% van de opdrachten en 50% komt bij Accenture vandaan. Er is dus een grote samenwerking tussen Accenture en Avanade. Accenture heeft een contract met Splunk> en Avanade met Azure Sentinel. De vraag is daarom ook om deze twee SIEM-oplossingen te vergelijken, zodat het inzichtelijker wordt welke SIEM het beste past bij de organisatie van de klant.

Workflow

overzicht

Deze handleiding is opgebouwd aan de hand van de onderstaande workflow. Via deze weg zal de consultant stap voor stap meer inzicht krijgen in de organisatie van de klant. Het doel is om uiteindelijk een aantal argumenten op tafel te krijgen die leiden tot de keuze van een SIEM oplossing.

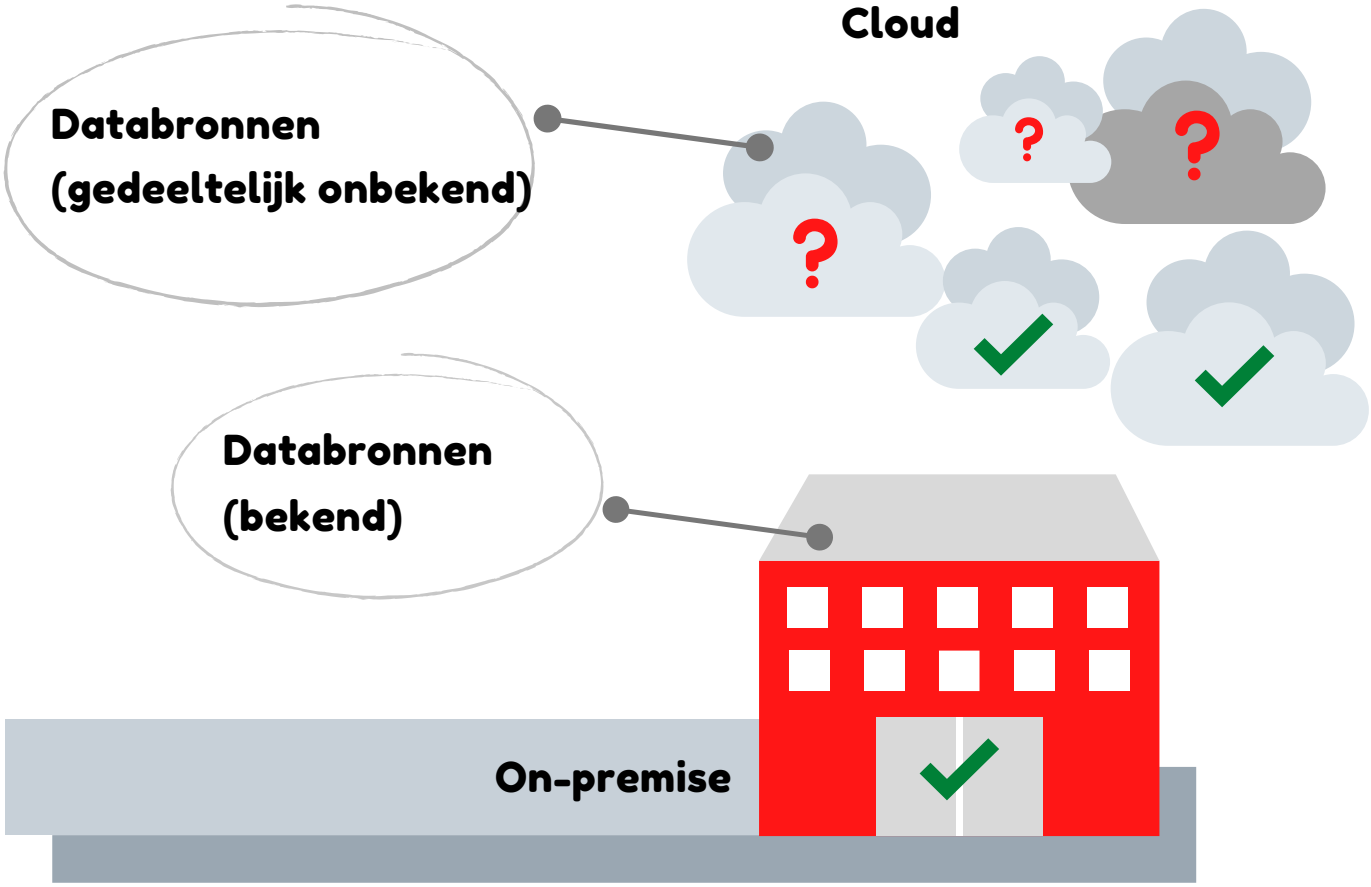


Globale analyse van de klant

Databronnen on-premise / cloud

De laatste 15 jaar hebben organisaties een grote digitale shift ervaren, vaak gedreven door de vraag naar efficiëntie en het reduceren van kosten. Het is een feit dat dit voor organisaties een groot voordeel heeft opgeleverd, maar het heeft ook de complexiteit van de IT-omgevingen enorm vergroot.

De databronnen voor organisaties zijn alleen maar toegenomen. Veel organisaties weten niet welke databronnen ze allemaal gebruiken, welke databronnen hun leveranciers beheren voor hen, of voor welke bedreigingen ze het meest moeten oppassen. Uiteindelijk weten ze niet aan welke risico's ze worden blootgesteld. Om de databronnen in kaart te brengen doen we een analyse op de on-premise & cloud databronnen van de klant.



Analyse on-premise databronnen

On-premise betekent 'ter plaatse'. In de bedrijfscontext hebben we het over de fysieke ruimte van het eigen bedrijf. Een paar voorbeelden van de databronnen die we in kaart willen brengen komen van eigen servers, routers, switches en firewalls.

Onderneem de volgende stappen

1. Verzamel de databronnen en begin klein
2. Als er bezorgdheden zijn omtrent specifieke data, begin dan daar
3. Welke databronnen zijn het belangrijkst en rangschik deze

Gebruik deze online calculator voor een schatting van de gegevensopname: https://siemsizingcalculator.logpoint.com/

De calculatie is gebaseerd op het aantal soort apparaten (knooppunten) in het netwerk. Dit omvat servers, routers, switches, firewalls en andere netwerkapparaten en applicaties.

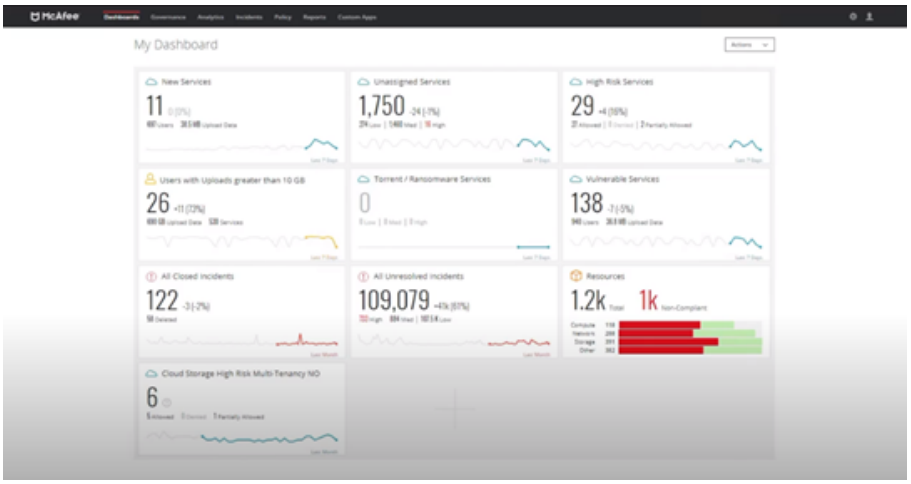
Checklist databronnen

Log types	**(aantal knooppunten)**
Windows Servers	
Windows Desktops (Laptops/ tablets)	
Network Switches	
Network Routers	
Network Firewalls (Layer 7 internal)	
Network VPN/ SSL VPN	
Network Flows (Netflow/S-Flow)	
Andere netwerkapparaten	
Linux/ Unix Servers	
Network IPS/IDS	
Network Firewalls (Layer 7 – DMZ)	
Network Wireless LAN	
Network Load-Balancers	
Network Firewalls (DMZ)	
Andere beveiligingsapparaten	
Network Web Proxy	
Network Firewalls (internal)	
HyperVisor (ESXi, Hyper-v etc)	
Eventueel zelf aanvullen*	

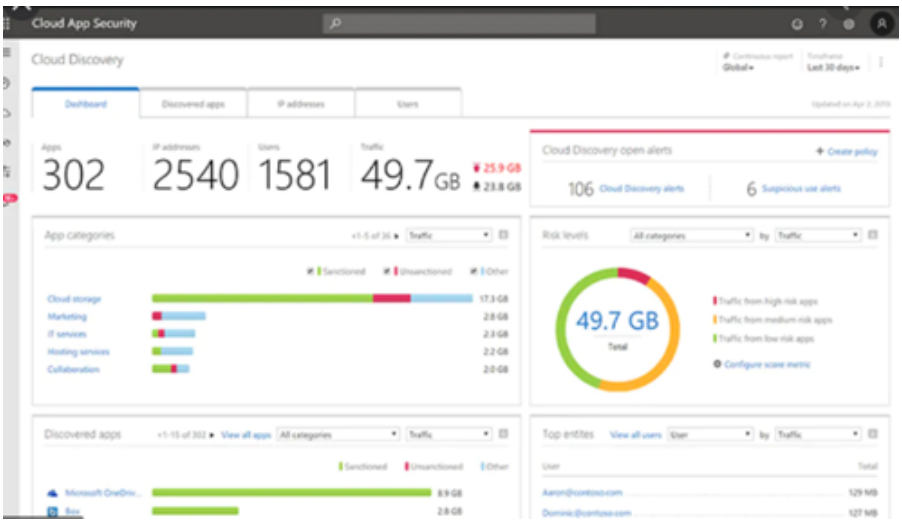
Analyse cloud databronnen
CASB (Cloud Access Security Broker)

Wat organisaties nodig hebben is het complete beeld van alle online databronnen. Een CASB wordt tussen het bedrijfsnetwerk en de cloudapplicaties gepositioneerd. Hierdoor wordt er inzicht in het gebruik van cloudapplicaties verkregen, de bedrijfsdata van en naar cloudapplicaties wordt beschermd en onder andere door de centrale policies (beveiligingsbeleid) wordt er controle verkregen vanuit één interface.

Hieronder is het dashboard te zien van McAfee MVISION Cloud, de CASB van McAfee.



Een andere optie is Microsoft Cloud App Security.



GB/dag (opname in de SIEM)

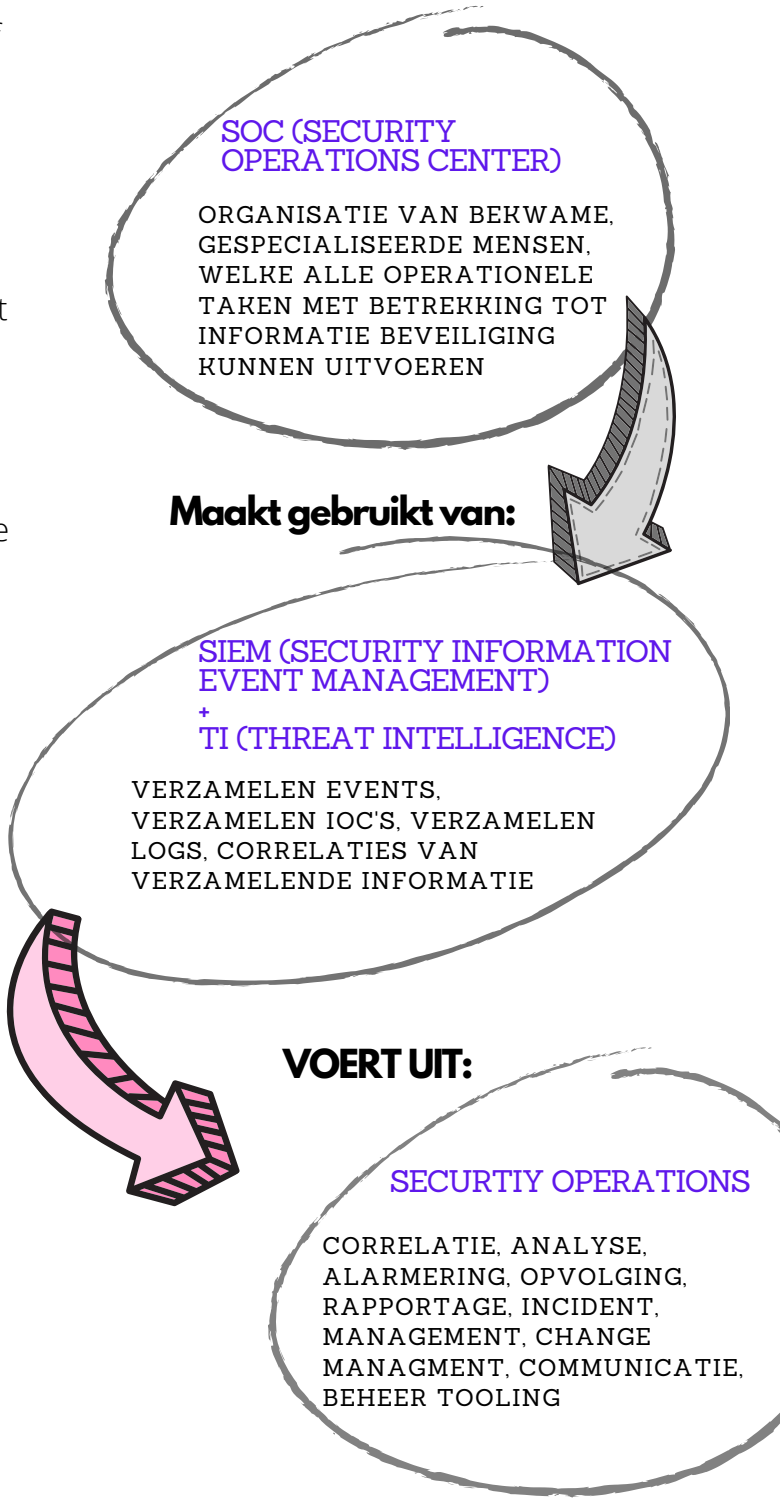
Maak een lijst van alle online databronnen die geanalyseerd moeten worden en maak een schatting van de gegevensopname in GB/dag.

SOC vs MSSP

Risicoanalyse van de klant

Voordat een SIEM voor de klant geadviseerd wordt zal er eerst bepaald moeten worden of de organisatie in staat is om zelf een SOC te hebben en te houden (aantrekken en behouden van het noodzakelijke talent en ze up to date te houden).

Niet elke organisatie heeft een eigen SOC met een security team nodig. Dit is afhankelijk van een aantal factoren, bijvoorbeeld de grootte van de organisatie, het IT-budget en de gevoeligheid van de data binnen de organisatie. Voor sommige kleinere bedrijven is een interne SOC geen optie en daarvoor zijn er ook outsourcing opties, zoals een MSSP (Managed Security Service Provider).



Werkblad

Aan de hand van dit werkblad wordt de klant geadviseerd een eigen SOC te nemen of te kiezen voor het outsourcen van de SOC d.m.v. een MSSP.

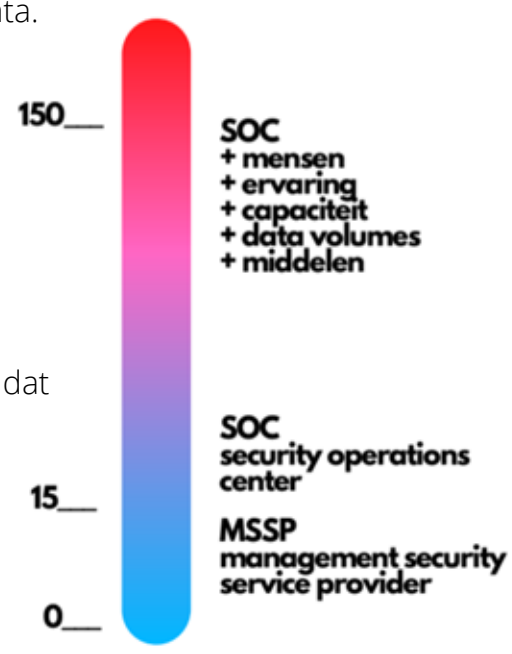
Uitleg werkblad

De vragen in het werkblad hebben als doel om het potentiele risico in te schatten op bedreigingsgevaar van hackers en datalekken voor een organisatie. Bij een verhoging van het risico is de vraag naar beveiliging steeds belangrijker. In het werkblad wordt de eindscore ook wel risicofactor genoemd, uitgedrukt in een getal.

Als de vragen 1-7 met 'ja' beantwoord kunnen worden dan geef je jezelf één punt. Bij een 'nee' geef je jezelf geen punten en komt er een 0 te staan. Onder de 7 vragen bij de titel subtotaal' moet de vraag beantwoord worden hoeveel IP hosts de organisatie telt in duizendtallen. De IP hosts zijn (de servers + de clients). De eindscore wordt berekend door de IP hosts in duizendtallen te vermenigvuldigen met de opgetelde punten.

Als leidraad wordt de drempel op 15 gezet. Organisaties die ver boven de 15 scoren zijn waarschijnlijk beter in staat een eigen SOC te bouwen en te laten functioneren. De organisaties die ver onder de 15 scoren zullen eerder in aanmerking komen voor een MSSP. Dan zijn er organisaties die rond de 15 schommelen. Deze organisaties kunnen andere factoren meenemen in het besluit, zoals in-house expertise of beschikbare middelen. We moeten ons bewust zijn dat de score een losse indicator is die niet rekening houdt met de grote van de SOC. Met andere woorden een organisatie met hoge score zal veel meer bedreigingen ervaren. Een bedrijf met een hoge score zal ook meer middelen nodig hebben, vakbekwame mensen, het behoud van mensen gaat een grote rol spelen, de verwerkingscapaciteit van data wordt groter en er is meer ervaring nodig als het gaat om de verwerking van grote volumes data.

Hiernaast is de schematische weergave van de scores en het daarbij horende advies. Hierboven heb ik aangegeven dat een grotere score ook vraagt om meer capaciteit op verschillende vlakken.



Voorbeeld werkblad

Dit is een ingevuld voorbeeld werkblad

Werkblad SOC - Formuleer de naam van de organisatie van de klant: Halfgeleiderbedrijf

Item	Vraag	Formuleer antwoord	Punten
1	Geef de organisatie 1 gratis punt, omdat de organisatie in de nabije toekomst een incident zal tegen komen.	Ja	1
2	Heeft de organisatie een incident gedetecteerd dat impact heeft op de doelen of de kosten van de organisatie in de afgelopen zes maanden?	Nee, er zijn geen grote incidenten geweest	0
3	Is het realistisch dat de organisatie wordt geconfronteerd met externe cyber dreiging naast de dagelijkse scriptkiddies?	Ja, het is een groot technologiebedrijf wat interessant is om te hacken	1
4	Biedt de organisatie producten met hoog risico of van grote waarde en is dit sterk afhankelijk van de IT, denk hierbij aan de bankenwereld, gezondheidszorg of energieproductie?	Nee, de fabriek (core business) draait op een apart netwerk	0
5	Biedt de organisatie IT-diensten rechtstreeks aan derde partijen?	Nee, er worden geen diensten geleverd	0
6	Biedt de organisatie gevoelige of privé gerelateerde data aan niet vertrouwelijke derde partijen via een publieke web interface, zoals een webapplicatie?	Nee, er worden geen gevoelige data aangeboden	0
7	Bewaart de organisatie gevoelige data van uzelf of van derde partijen, zodat uw organisatie aansprakelijk kan worden gesteld bij gestolen of verloren data?	Ja, een beperkte set van mijn persoonlijke gegevens zijn bekend	1
	Subtotaal		
	Hoeveel IP hosts (servers+clients) in duizendtallen telt de organisatie?	40000	40
	Vermenigvuldig het subtotaal in duizendtallen van hosts met punten. Dit is de totaalscore.	40 * 3 = **120**	

Deze organisatie scoort 3 van de 7 punten in combinatie met de grote van organisatie is de eindscore hoog. De organisatie wordt op basis van dit werkblad geadviseerd een eigen SOC te nemen. De hoge eindscore geeft de indicatie dat een ervaren security team nodig is die grote volumes data kan analyseren.

Werkblad voor de klant

Dit werkblad wordt ingevuld door de consultant in samenspraak met de klant.

Werkblad SOC - Formuleer de naam van de organisatie van de klant: .....

Item	Vraag	Formuleer antwoord	Punten
1	De organisatie krijgt één gratis punt, omdat de organisatie in de nabije toekomst met een incident te maken zal hebben.		1
2	Heeft de organisatie een incident gedetecteerd dat impact heeft op de doelen of de kosten van de organisatie in de afgelopen zes maanden?		
3	Is het realistisch dat de organisatie wordt geconfronteerd met externe cyber dreiging naast de dagelijkse script kiddies?		
4	Biedt de organisatie producten met hoog risico of van grote waarde en is dit sterk afhankelijk van de IT, denk hierbij aan de bankenwereld, gezondheidszorg of energieproductie?		
5	Biedt de organisatie IT-diensten rechtstreeks aan derde partijen?		
6	Biedt de organisatie gevoelige of privé gerelateerde data aan niet vertrouwelijke derde partijen via een publieke web interface, zoals een webapplicatie?		
7	Bewaart de organisatie gevoelige data van uzelf of van derde partijen, zodat uw organisatie aansprakelijk kan worden gesteld bij gestolen of verloren data?		
Subtotaal			
	Hoeveel IP hosts (servers+clients) in duizendtallen telt u organisatie?		
	Vermenigvuldig het subtotaal in duizendtallen van hosts met punten. Dit is de totaalscore.		

Bevindingen:

Splunk vs Azure Sentinel
voor- en nadelen

In mijn onderzoek heb ik geconcludeerd dan beide SIEM tools op basis van functionaliteiten aan elkaar gewaagd zijn. Hiermee zijn geen grote verschillen aan te tonen.

Het verschil gaat zitten in de benadering van de SIEM tools, in welke omgeving komt de SIEM te draaien, welke databronnen worden geanalyseerd en bijvoorbeeld hoe het zit met de expertise van medewerkers.

Hieronder zal ik een aantal onderzoeksresultaten delen en hier een score aan vast hangen die de sterktes en zwakheden van Splunk & Sentinel naar voren brengen. Veel van deze resultaten zijn verworven door een interview met Greg Peterson (Sr Director - IT Security Avanade) en een onderzoek van Accenture naar Splunk & Azure Sentinel.

Erg goed ++
Goed +
Neutraal 🤚
Slecht –
Erg Slecht – –

Onderzoeksresultaten

Azure Sentinel 🤚

Grote volumes SYSLOG & CEF (common event format) events en dan praten we over 13000 events/second waren tot begin 2020 lastig op te nemen door Azure Sentinel. Hier waren 20 Linux VM's voor nodig met elk een Microsoft mangement agent die 500 events/second konden verwerken. De agent is verbetert begin dit jaar en één Linux VM kan nu 10000 events/second verwerken. Op dit vlak is er verbetering, maar het staat nog in de kinderschoenen.

Splunk ++

Splunk is erg goed in het verwerken van grote volumes SYSLOG & CEF. Mocht de organisatie een groot percentage SYSLOG en CEF log data willen analyseren dan is Splunk hier geschrikt voor.

Onderzoeksresultaten

Azure Sentinel 

Azure Sentinel is recent op de markt en daarom zijn nog niet alle analyse mogelijkheden goed ontwikkelt. Als een organisatie overweegt Sentinel in huis te nemen dan kan het de volgende tactiek toepassen.

1. Bekijk de databronnen
2. Begrijp wat deze doen
3. Bekijk hoever Microsoft staat met de ontwikkeling van de databron die geanalyseerd moet worden.

Maak de organisatie bewust van de tekortkomingen van Azure Sentinel en de kwaliteiten.

Splunk Enterprise — —

Een SIEM die niet cloud native is heeft verzorging nodig in de vorm van upgraden en patching. Bij grote organisaties kan dat wel om 20 tot 30 VM's gaan verspreid over verschillende locaties. Upgraden en patching kost veel tijd/geld/mankracht en brengt verhoogde beveiligingsrisico's met zich mee bij nalatigheid. Daarnaast vergt het beheer van storage op de locaties ook tijd en geld.

Azure Sentinel ++

Splunk Cloud +

Bij een cloud native SIEM wordt upgraden en patching automatisch gedaan en daarnaast worden bij Microsoft nieuuwe updates en verbeteringen automatisch voorzien.

Azure Sentinel —
Splunk +

Data zoeken, maskeren en wijzigen om PCI of GDPR redenen.

Azure Sentinel —
Splunk +

De volwassenheid van alerting & ticketing en ticket tracking.

Azure Sentinel —

Splunk +

Splunk is goed in het geven en controleren van role based user access. Het is mogelijk om toegang te krijgen op verschillende indexen vanuit een groepsrol. In de praktijk zou het inhouden dat de netwerk mensen de netwerk indexen kunnen bekijken en de server mensen kunnen de server indexen zien. Dat zorgt voor overzicht en veiligheid.
Bij Azure Sentinel kan met via Azure Lighthouse queries en zoekopdrachten doen op de log analytics workspace, dit is een nieuwe manier en nog niet erg stabiel. Daarnaast is het mogelijk role based access te doen via Log Analtytics, maar dit functioneert nog niet naar behoren.

Implementatie scenario's

Wat is de volgende stap?

Als organisatie ben ik opzoek naar een SIEM, wat zijn de vervolg stappen?

Ik zou adviseren deze handleiding te gebruiken als startpunt, hier staat per stap uitgelegd hoe het keuzeproces van een nieuwe SIEM aangepakt kan worden.

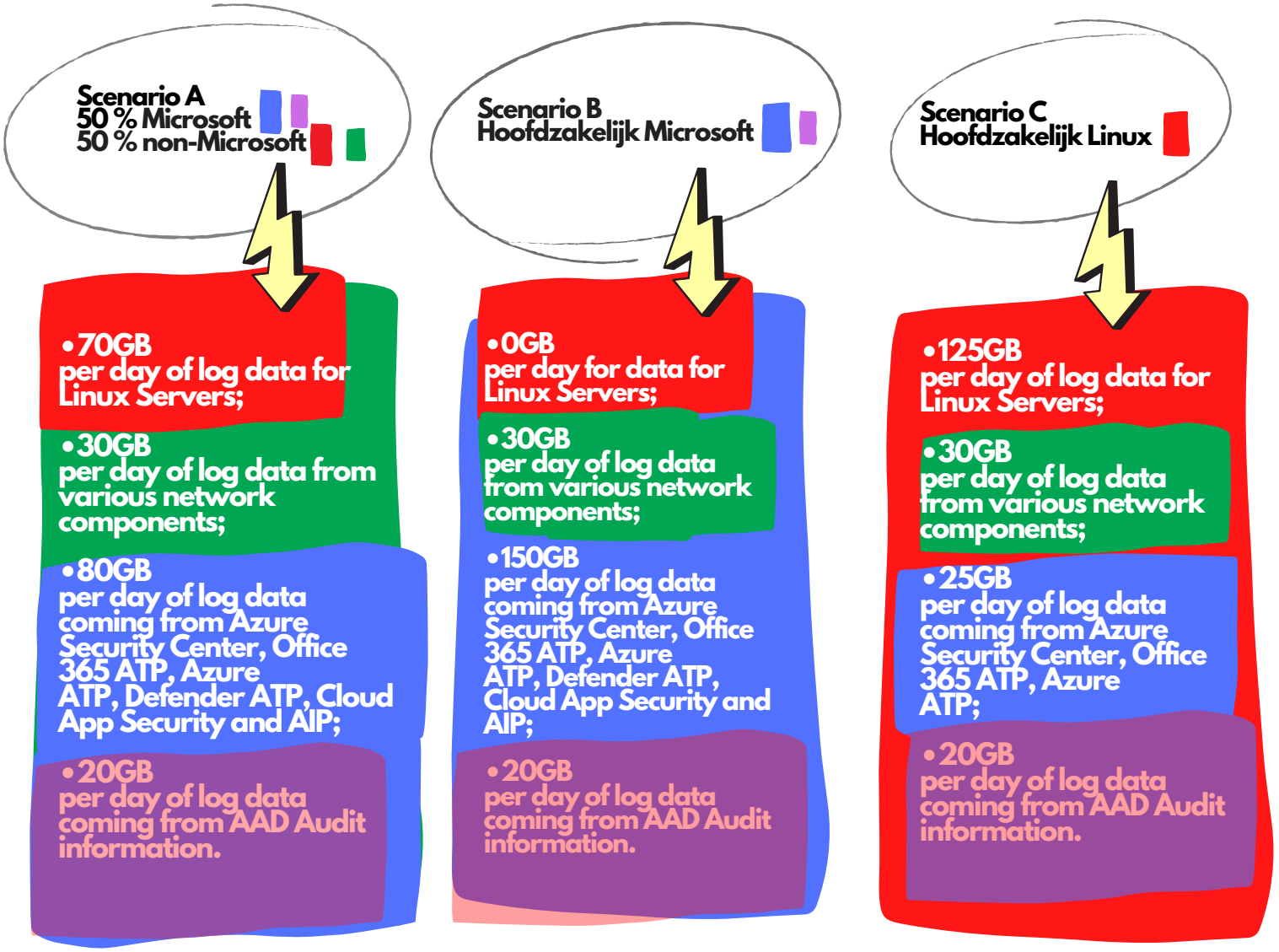
Als organisatie heb ik Splunk als SIEM draaien, wat zijn de vervolg stappen?

Het advies zou zijn de Splunk te houden en te optimaliseren. Het vooronderzoek van deze handleiding kan helpen bij het optimaliseren van de huidige SIEM. Denk daarbij aan de globale analyse. Het is het ook nog mogelijk om te kiezen voor een hybride oplossing waarbij Azure Sentinel de Microsoft workload overneemt. Vanwege de makkelijke integratie van Microsoft data in Azure Sentinel en de kostbesparing ten opzichte van Splunk is een hybride oplossing zeer aantrekkelijk. De belangrijke alerts worden dan doorgestuurd naar Splunk, zodat het security team de alerts vanuit één omgeving bekijkt.

Kosten Data Ingestion

gegevensopname uit databronnen

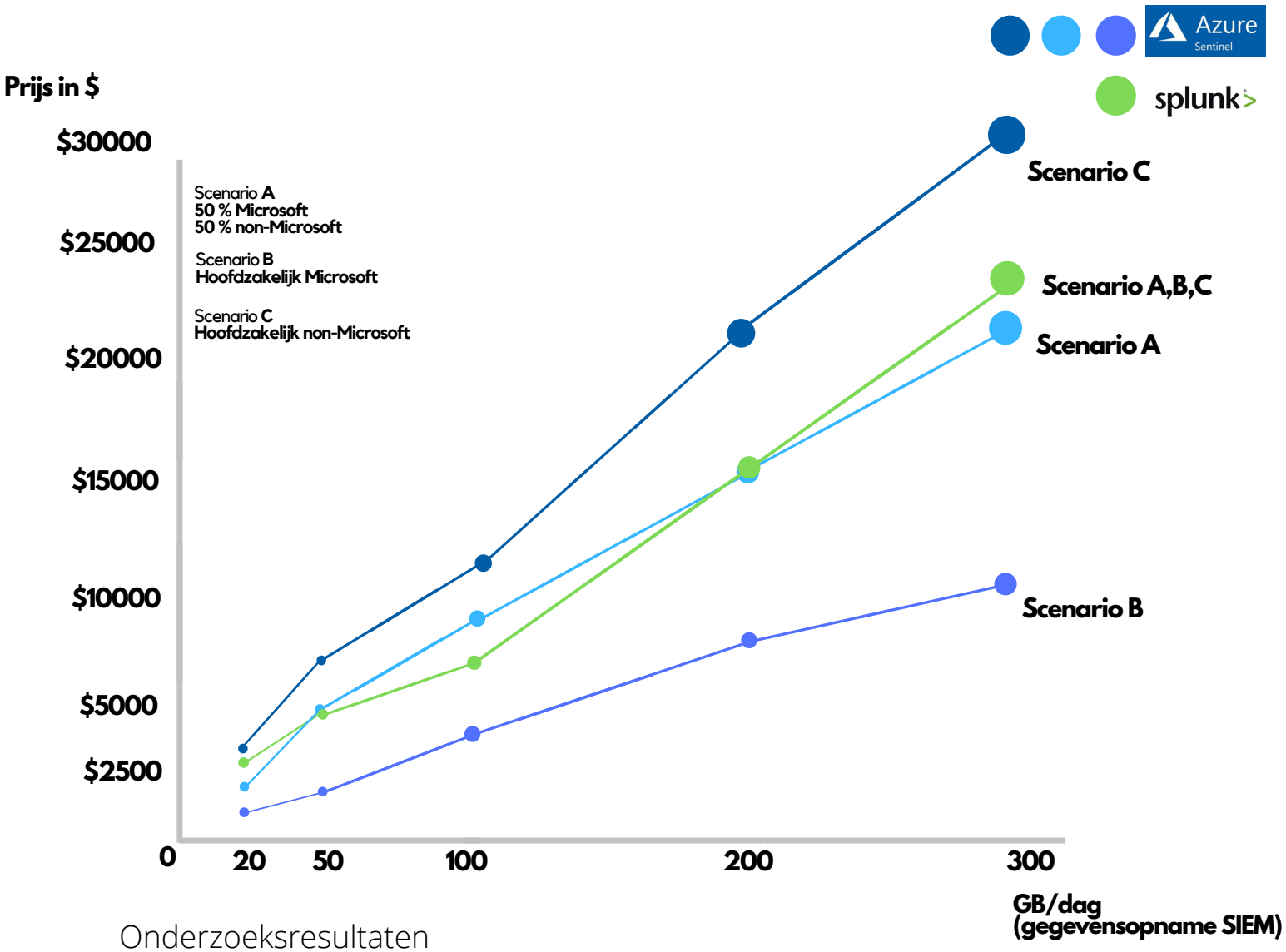
Hieronder zijn drie scenario's uitgeschreven voor de gegevensopname van 200GB/dag in de SIEM. Ik ga onderzoeken wat het verschil is in kost als we de input in de SIEM veranderen op basis van databronnen uit verschillende omgevingen. Het eerste scenario schets een gebalanceerde verdeling van Microsoft en non-Microsoft databronnen. Bij scenario B is het hoofdzakelijk Microsoft en bij scenario C hoofdzakelijk non-Microsoft.



Kost/maand in $ van de drie scenario's

De cijfers uit het diagram hieronder zijn gebaseerd op verschillende dagelijkse gegevensopnames in Splunk & Azure Sentinel. In het diagram zijn de volgende gegevensopnames in gigabyte 20GB, 50GB, 100GB, 200GB en 300 GB uitgezet tegenover de prijs in dollar per maand.

kostentabel



Onderzoeksresultaten

Alle databronnen die verbonden worden met Splunk komen van externe plaatsen. Of dat Microsoft, Linux of netwerkdata is. Bij Azure Sentinel is dit een ander verhaal, omdat Sentinel onderdeel uitmaakt van de Microsoft producten is het koppelen van Microsoft data relatief eenvoudig. De data van de volgende bronnen Azure Activity Logs, Office 365 Audit Logs en alerts, Microsoft Threat Protection producten (Azure Security Center, Office365 ATP, Azure ATP, Microsoft Defender ATP, Microsoft Cloud App Security en Azure Information Protection kunnen zonder extra kost opgenomen in Azure Sentinel en de Log Analytics workspace.

Hierdoor kan er een groot deel van de kost komen te vervallen als een organisatie veel gebruik maakt van deze Microsoft producten. Dit kan naar mijn idee ook een strategie zijn van een bedrijf, waarin het bedrijf hoog inzet op deze Microsoft producten en daarbij Azure Sentinel als SIEM gaat gebruiken om de kost te drukken.

Wat zijn dan de grote verschillen? Als we is inzoomen op scenario B waarin we hoofdzakelijk Microsoftdata de SIEM inpompen dan zien we een groot prijsverschil. Bij een opname van 300GB/dag betalen we bij Splunk $23.000,00 dollar. Bij dezelfde opstandigheden voor Azure Sentinel is het bedrag $10,612.55 voor de klant, dat is een verschil van ruim $12.000,00. Wel kunnen de cijfers 10 tot 20% lager uitvallen door kortingen vanuit Splunk & Microsoft, maar dat geld voor beide partijen. Mocht een klant dus veel data willen analyseren uit de hierboven genoemde Microsoft omgevingen dan kan dit grote prijsverschil een overtuigend argument zijn om voor Azure Sentinel te kiezen.

Prijs Azure Sentinel (scenario B)	Prijs Splunk (scenario B)	Verschil
300 GB - 10,612.55	300 GB – 23.000,00	$12.387,45
200 GB - 8,370.05	200 GB – 15,333.33	$6.963,28

Aan de andere kant zien we ook dat Azure Sentinel vele malen duurder kan uitvallen. In dit geval van scenario C wordt hoofdzakelijk non-Microsoft data in Azure Sentinel & Log Analytics opgenomen. Bij volumes lager dan 200GB zien we dat het grote prijsverschil afneemt.

Prijs Azure Sentinel (scenario C)	Prijs Splunk (scenario C)	Verschil
300 GB - 29,972.90	300 GB – 23.000,00	$6.971,9
200 GB - 21,261.60	200 GB – 15,333.33	$5.928,27

Als laatste, scenario A waarbij 50% Microsoft en 50 non-Microsoft data in de SIEM wordt opgenomen, zien we geen grote afwijkingen. Qua prijs blijven Splunk en Azure Sentinel om elkaar heen schommelen. Op basis van scenario A is er geen winnaar en zal gekeken moeten worden naar andere argumenten voor het kiezen van de SIEM.

Advies

op maat

Elke organisatie is anders en daar hoort een advies op maat bij. Deze handleiding geeft op een aantal onderwerpen een indicatie. Door middel van het invullen van onderstaande parameters zal het advies zichtbaar worden.

Databronnen

Eerder in de handleiding bij de "Globale Analyse' hebben we een analyse gedaan van de huidige databronnen van de klant. Bereken aan de hand van de GB/dag gegevensopname hoeveel procent van de databronnen Microsoft en non Microsoft zijn. Dit percentage geeft een indicatie welke SIEM oplossing in het geval de klant duurder zal zijn.

on-premise

.....GB/dag

cloud

.....GB/dag

Microsoft data

.....GB/dag = ...%

gratis Microsoft data

.....GB/dag = ...%

non-Microsoft data

.....GB/dag = ...%

SOC of MSSP

Noteer hier de score van het werkblad: .....
Als onder de 15 = MSSP
Als boven de 15 = SOC
Als de score ongeveer 15 maak de keuze dan op externe factoren, zoals in-house expertise, beschikbare middelen, budget en hou rekening met de toekomstvisie van het bedrijf.

Splunk vs Sentinel

Zoek tussen de onderzoeksresultaten bevindingen die van toepassing zijn op jouw organisatie en daardoor helpen bij de keuze. Noteer ze onder de lijn.

Implementatie scenario

Welk begin scenario past bij de organisatie van de klant? Kruis aan

Als organisatie ben ik opzoek naar een SIEM. ☑

Als organisatie heb ik Splunk als SIEM draaien. ☐

Kosten

Probeer op basis van de kostentabel een prijsschatting te doen, mocht het scenario van de klant totaal anders zijn, bereken dan de gegevensopname prijs in GB/dag eigenhandig via Splunk pricing en de Azure Microsoft calculator.

.....$

.....$

Succes met de SIEM implementatie

henk-sjoerd hinrichs