

'Hulp bij het kiezen van een SIEM'

Henk-Sjoerd Hinrichs

Bachelor Elektronica-ICT in Cloud & Cyber Security
Thomas More Hogeschool te Campus Geel

Document Title

Project Title	Security Event Consolidation
Author	Avanade: Henk-Sjoerd Hinrichs
Reviewer	Thomas More: Liesbeth Kenens Avanade: Frank Molenaar, Ruud Gijsbers, Michael Zimmerman
Current Version	Release 1.0
File Name	Onderzoeksverslag
Publication Date	16-4-2020

Revision History

Version	Date	Author	Changes
1.0	16-4-2020	Henk-Sjoerd Hinrichs	
2.0	27-5-2020	Henk-Sjoerd Hinrichs	Globale analyse, implementatie, conclusie, vergelijking Splunk /Sentinel.

Table of Contents

1	Begrippenlijst	1
2	Inleiding	2
2.1	Stage bedrijf.....	2
2.2	Aanleiding	2
2.3	Opdracht.....	3
2.4	Afbakening van het project.....	3
2.5	Doelstelling.....	3
2.6	Hoofd en deelvragen.....	5
3	Globale analyse van de klant	6
3.1	Waar is de data van de klant?	6
3.2	Hoe krijgt de klant overzicht op de databronnen van de on-premise omgeving?	7
3.2.1	Checklist van mogelijke databronnen van de klant om inzicht te krijgen in de on-premise omgeving.	8
3.3	Hoe krijgt de klant een overzicht in de zijn cloud omgeving?.....	8
4	Heeft de klant een SOC nodig?	9
4.1	Inleiding	9
4.2	Een SOC bouwen binnen de organisatie of is uitbesteden een betere optie?	10
4.2.1	De schematische weergave van een eigen SOC.....	10
4.2.2	De schematische weergave van een MSSP (Managed Security Service Provider).....	11
4.2.3	Advies door middel van invuldocument.....	12
4.2.4	Beoordelingsdocument	12
4.2.5	Opties voor het outsourcen van de SOC.....	15
4.3	Tips bij het opzetten van een SOC.....	15
5	Welke SIEM is geschikt voor de klant? "It's easy to buy 'Technology', but the always evolving threat landscape demands mature 'People' and 'Processes' as well to be on top of the game."	16
5.1	Wat is een SIEM? 'In the cloud, things aren't always what they SIEM'	16
5.2	Splunk & Azure Sentinel vergelijken aan de hand van requirements	17
5.2.1	Inleiding	17
5.2.2	MosCow Methode	17
5.2.3	Requirements	17
5.2.4	Requirements uitgeschreven.....	18
5.3	SIEM Tooling Capabilities	20
5.3.1	Globaal overzicht	20
5.3.2	Beslissingsmatrix op basis van output MosCow.....	23
6	Drie implementatie scenario's	24
6.1	Inleiding	24
6.2	Twee implementatie scenario's beschreven	25
6.2.1	Scenario 1; "Als organisatie ben ik opzoek naar een SIEM, wat zijn de vervolg stappen?"	25
6.2.2	Scenario 3 "Als organisatie heb ik Splunk als SIEM draaien, wat zijn de vervolg stappen?"	28
7	Kosten Data Ingestion (gegevensopname)	30
7.1	Inleiding	30
7.2	Drie scenario's	30
7.3	Azure Sentinel & Splunk Cloud ingestion prijs	31
7.3.1	Scenario A (50% Microsoft 50% non-Microsoft)	31
7.3.2	Scenario B (Hoofdzakelijk Microsoft)	32

7.3.3	Scenario C (Hoofdzakelijk non-Microsoft)	33
7.3.4	Alle prijzen samengevoegd in één tabel	34
7.3.5	Kost/maand in dollar van de verschillende scenario's in één diagram	34
7.3.6	Bevindingen	35
8	Conclusie	36
9	Bronnen	37
10	Bijlage Hoogtepunten interview Greg Peterson (Sr Director – IT Security Avanade) Over de producten Splunk en Azure Sentinel en de migratie van Splunk Enterprise naar Azure Sentinel bij Avanade (Seattle, USA)	38
10.1	Highlights - Interview Greg Peterson (Sr Director – IT Security Avanade) 23-04-2020	38

1 Begrippenlijst

TI	Threat Intelligence
SOC	Security Operations Center
SIEM	Security Information Event and Management
SOAR	Security Orchestration Automation and Response
UEBA	User and Entity Behavior Analytics
AI	Artificial Intelligence
SaaS	Software as a Service
MSSP	Managed Security Service Provider
IT	Informatietechnologie
TCO	Total Cost of Ownership
TaCo	Talent Community

2 Inleiding

2.1 Stage bedrijf

De stage opdracht zal worden uitgevoerd bij Avanade, een IT-consultancy bedrijf dat gespecialiseerd is in Microsoftoplossingen. Op dit moment heeft Avanade 36.000 werknemers in dienst verspreid over 24 landen. Het bedrijf is opgericht door Accenture en Microsoft in het jaar 2000.

Het Nederlandse kantoor is gesitueerd in Utrecht, op dit kantoor werken ongeveer 400 medewerkers. Deze medewerkers, waaronder ook de stagelopers, zijn onderverdeeld in de zogeheten TaCo's (Talent Community's). De TaCo's hebben gespecialiseerde kennis van een bepaald gebied binnen de IT en vormen samen een bron van kennis die met elkaar wordt gedeeld. Vaak werken de medewerkers uit TaCo's in teams aan opdrachten.

Zelf ben ik gesitueerd binnen de Infrastructure TaCo die overlap toont met de Security TaCo, nog niet zolang geleden heeft Security zijn eigen Talent Community gekregen, omdat de vraag naar security in de IT-wereld alleen nog maar groeit.

2.2 Aanleiding

Met betrekking tot dit onderzoek is het Microsoft-verhaal belangrijk. Avanade werkt namelijk hoofdzakelijk met Microsoft-technologie en dit is de core business van het bedrijf. Op dit moment is Microsoft bezig zich verder te ontwikkelen op het gebied van cybersecurity.

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

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

Om een centraal inzicht te krijgen in security gerelateerde events uit verschillende omgevingen is een klant van Avanade op zoek naar een centrale oplossing. Op dit moment genereert Avanade zelf ongeveer 50% van de opdrachten en 50% komt bij Accenture vandaan. Deze opdrachten zijn bijvoorbeeld Microsoft implementaties. 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 goed past binnen de organisatie van de klant.

2.3 Opdracht

Avanade is een Microsoft georiënteerd bedrijf en één van de grote business drivers is het implementeren van Microsoftproducten. Anderhalf jaar geleden is Microsoft met een nieuw product gekomen genaamd Azure Sentinel. Azure Sentinel is de nieuwe cloud native SIEM van Microsoft. Aangezien Azure Sentinel een Microsoftproduct is, ligt nu de prioriteit bij dit SIEM-product. Voordat Azure Sentinel bestond implementeerde Avanade vaak Splunk. Op dit moment wordt dat nog steeds gedaan. Daarnaast wordt Splunk ook vaak door Accenture geïmplementeerd als SIEM-oplossing.

Azure Sentinel is recentelijk op de markt gekomen en vanwege dit feit is de kennis nog beperkt. De vraag vanuit Avanade is; "wanneer kan de consultant beter Azure Sentinel adviseren en wanneer Splunk". Zoek uit waar de voordelen liggen en hoe de consultant van Avanade kan beoordelen welke organisatie geschikt is voor één van de SIEM-oplossingen.

2.4 Afbakening van het project

Tijdens een gesprek op 8 april '20 met Luka Kolb, een medestudent uit België, werd duidelijk wat er met mijn onderzoek niet mogelijk is. Luka bouwt een SIEM-oplossing voor zijn stage bedrijf met de ELK stack (Elasticsearch, Kibana, Beats & Logstash). Door een uitgebreide briefing van het stagebedrijf werd Luka geïnstrueerd in de specifieke monitoring eisen. Het bedrijf beschrijft aan Luka waar hij rekening mee moet houden met het bouwen van de SIEM. Het bedrijf kent haar eigen visie en doel.

Mijn oorspronkelijke idee was om vrij realistische scenario's te schetsen en daar een passende SIEM-oplossing bij te zoeken. Dit blijkt niet haalbaar te zijn vanuit mijn positie, omdat ik de 'requirements' moet kennen van de organisatie met betrekking op hun nieuwe SIEM-oplossing. Daarnaast moet je inzicht hebben in de ICT-infrastructuur en de databronnen. Een volledige SIEM-oplossing adviseren voor een fictief scenario is niet herbruikbaar. Mijn benadering moet bruikbaar zijn voor de consultant van Avanade.

Dit betekent dat ik dit onderzoek op een globaler niveau moet onderzoeken en in mijn achterhoofd moet houden waar dit onderzoek een meerwaarde kan bieden voor de consultant van Avanade. Het globalere karakter van dit onderzoek zal duidelijk worden in de volgende alinea 'Doelstelling'.

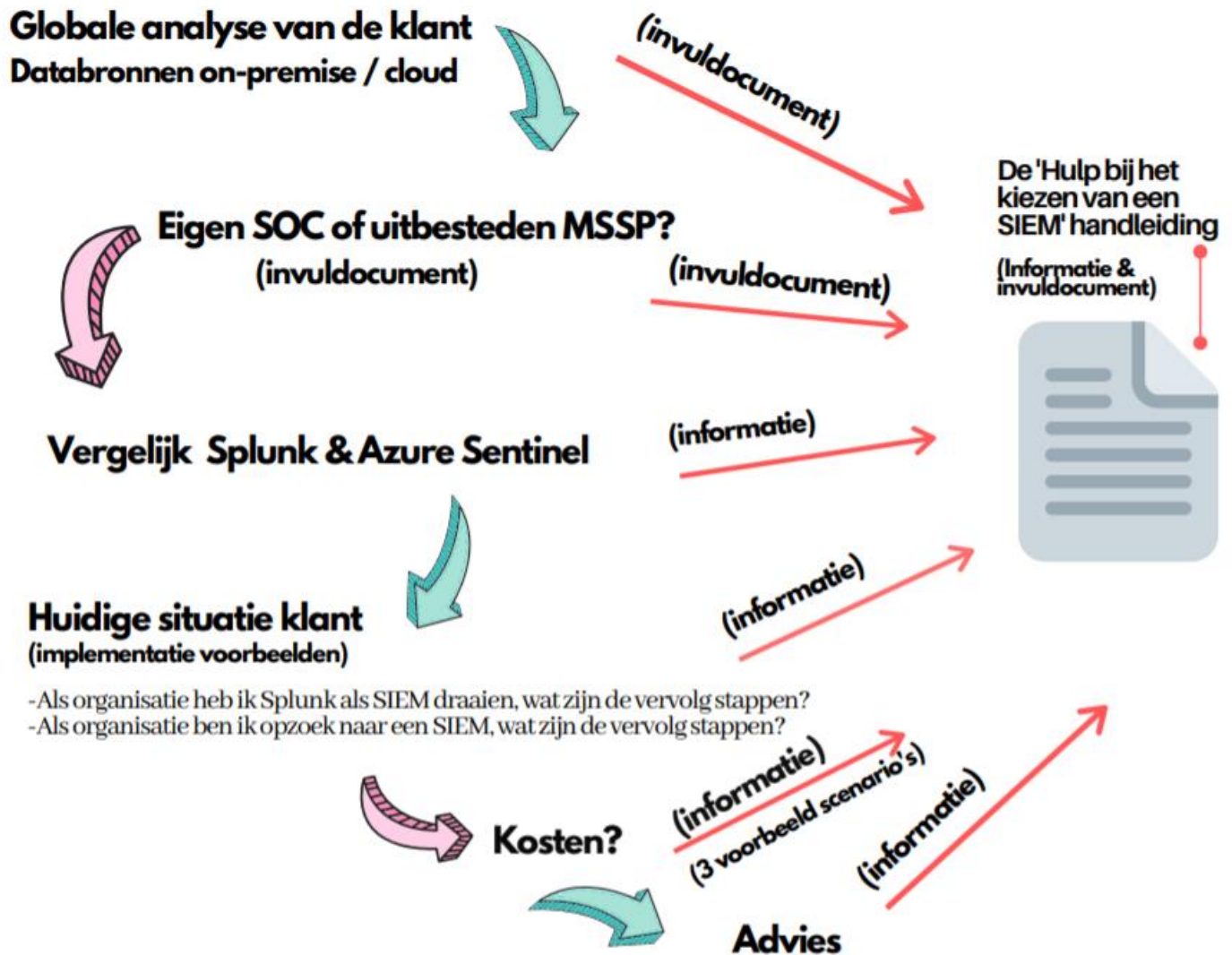
2.5 Doelstelling

De klant vraagt Avanade na te denken over een SIEM-oplossing voor zijn of haar organisatie. Het doel van dit onderzoek is om de consultant van Avanade te helpen bij het maken van keuzes omtrent de SIEM-oplossing. Ik ga werken in de vorm van een hulpdocument voor de consultant van Avanade. Het hulpdocument zal gedeeltelijk bestaan uit een invul deel, waarin gegevens van de organisatie van de klant worden verwerkt. Daarnaast zal ook deel van het hulpdocument informatief zijn in de vorm van tekst en figuren.

Het hulpdocument geeft onder andere advies op de vraag; "Is een organisatie in staat een SOC intern te bouwen en onderhouden?", en het hulpdocument "Moet inzicht geven in het keuzeprocess voor een SIEM-oplossing". Om tot dit doel te komen is het belangrijk eerst een analyse te doen op de organisatie van de klant. Deze analyse zal zich focussen op de on-premise en cloud databronnen van de klant.

Deze analyse geeft de consultant een overzicht van de klant zijn dataflow.

Hieronder is de workflow uitgetekend om het hulpdocument op te bouwen.



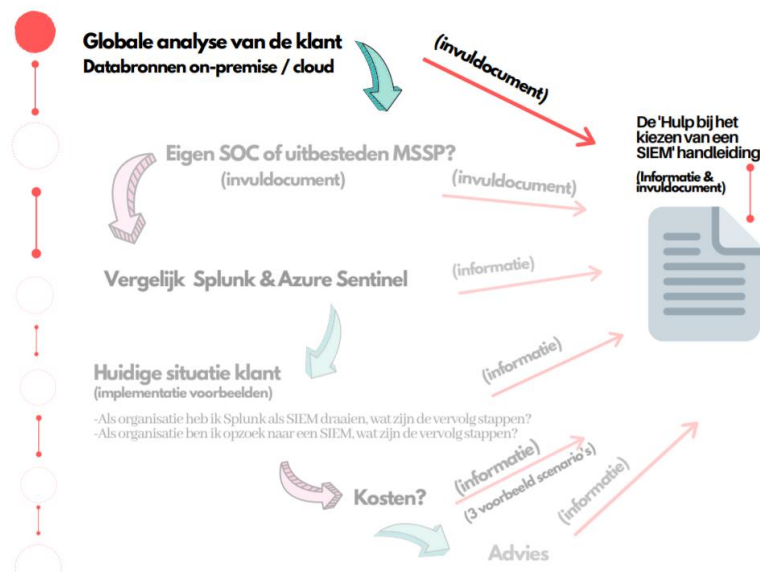
De bovengenoemde doelen zullen helpen een antwoord te geven op de hoofdvraag. "Hoe maakt de consultant van Avanade het proces voor het kiezen van een SIEM inzichtelijk voor de klant?" Om de hoofdvraag te beantwoorden maak ik gebruik van een aantal deelvragen. Ik zal de belangrijke functionaliteiten van Splunk en Azure Sentinel onderzoeken. Om deze te bepalen ga ik aan de hand van Moscow-methode kijken welke SIEM-functionaliteiten belangrijk zijn. Er hangt ook een prijskaartje vast aan een SIEM. Deze bepalen we door een TCO (Total Cost of Ownership) te maken. Ook zal ik vanuit drie scenario's het implementatieproces onderzoeken. De drie scenario's staan opgesomd in de derde deelvraag in de tabel hieronder.

2.6 Hoofd en deelvragen

De hoofdvraag die ik heb opgesteld; **‘Hoe maakt de consultant van Avanade het proces voor het kiezen van een SIEM inzichtelijk voor de klant?’** zal ik kunnen beantwoorden met behulp van verschillende deelvragen die ik heb opgesteld.

Deelvraag	Onderzoeksmethode	Eindresultaat
1. Welke organisaties zijn in staat om zelf een SOC te hebben en te houden (aantrekken en behouden van het noodzakelijke talent en ze up to date houden) en voor welke organisaties is het verstandig om te kiezen voor een MSSP?	Literatuuronderzoek, vergelijkbaar onderzoek	Een invuldocument dat advies geeft op basis van informatie die de klant heeft gegeven.
2. Wat zijn de belangrijke functionaliteiten van Azure Sentinel en Splunk?	Literatuuronderzoek, expertise collega's	De belangrijke functionaliteiten vergeleken in een vergelijkingsmatrix.
3. Onderzoek de volgende drie scenario's die een consultant van Avanade kan tegenkomen bij een SIEM-implementatie. -Als organisatie heb ik een verouderde SIEM, wat zijn de vervolg stappen? -Als organisatie heb ik Splunk als SIEM draaien, wat zijn de vervolg stappen? -Als organisatie ben ik op zoek naar een SIEM, wat zijn de vervolg stappen?	Literatuuronderzoek, online tutorial, interview	Een stappenplan voor het bouwen van de architectuur van een SIEM-oplossing.
4. Wat is de TCO (Total Cost of Ownership) van Azure Sentinel en Splunk vanuit 3 scenario's bekeken?	Literatuuronderzoek	Een duidelijk overzicht van de Total Cost of Ownership 3 scenario's?

3 Globale analyse van de klant



3.1 Waar is de data van de klant?

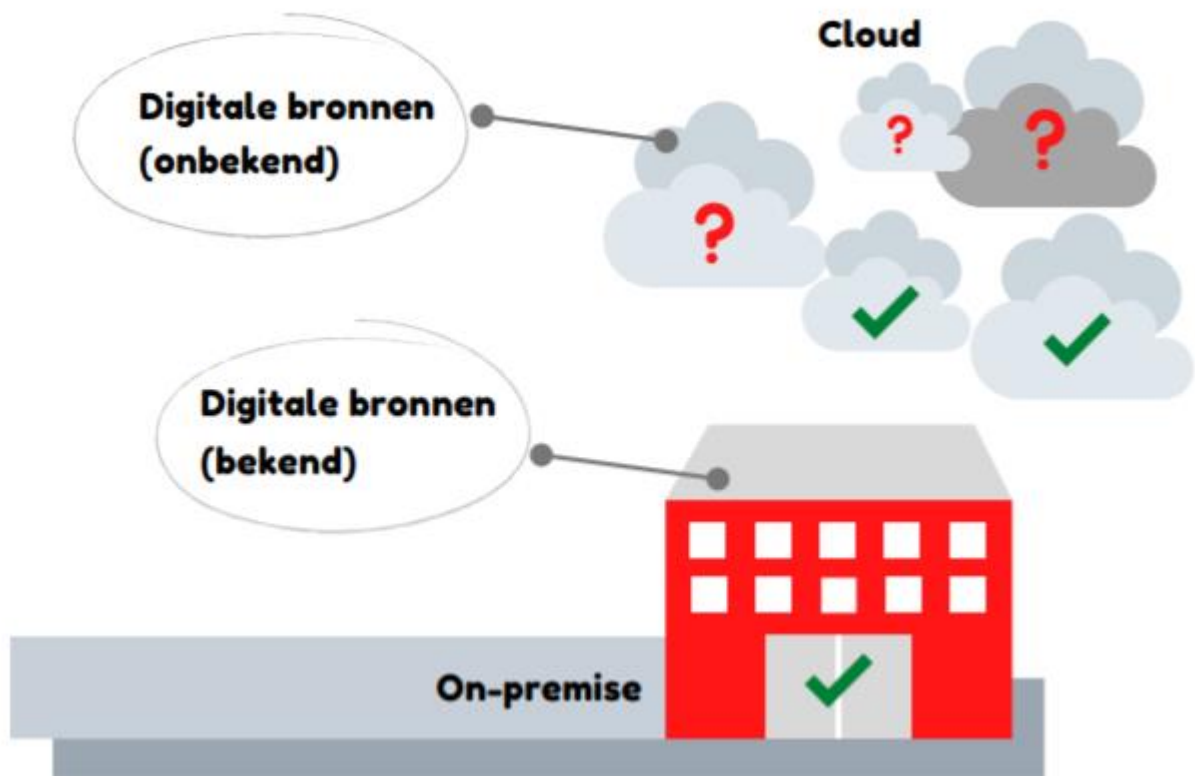
De laatste 15 jaar hebben organisaties een grote digitale shift ervaren, vaak gedreven door de vraag naar efficiëntie en het reduceren van kosten. Het is een feit dat dit voor organisaties een groot voordeel heeft opgeleverd, maar het heeft ook de complexiteit van de IT-omgevingen enorm vergroot.

De databronnen voor organisaties zijn alleen maar toegenomen. Voordat ik verder ga in dit verhaal zal ik eerst opsommen welke databronnen relevant zijn in dit verhaal. Hierbij een lijst van kritieke databronnen.

Categorie	Voorbeeld
Host/Endpoint Logs	Windows Event Collection, Syslog, Log Analytics Agent
Authenticatie Logs	AWS CloudTrail, Azure Active Directory
Cloud Infrastructure	AWS CloudTrail, Azure Storage, Azure Activity
Cloud Application Logs	Office 365
Netwerk Infrastructuur en Device Logs	Syslog, CEF, Azure Network Analytics, OMS Wiredata

Azure Sentinel Teminus Board Here (bron)

Voorheen waren dit databronnen die vooral uit on-premise omgevingen kwamen. De toename in het gebruik van cloud omgevingen heeft ervoor gezorgd dat data bij en onbekende vendors terecht is gekomen met hun eigen beveiligingsuitdagingen en bedreigingen, waar de meeste organisaties geen zicht op hebben.



Veel organisaties weten niet welke online databronnen ze allemaal gebruiken, welke online databronnen hun leveranciers beheren voor hen, of voor welke bedreigingen ze het meest moeten oppassen. Uiteindelijk weten ze niet aan welke digitale risico's ze worden blootgesteld. De digitale footprint van de organisatie moeten we in beeld krijgen om alle essentiële data in de SIEM te krijgen. Ik maak hier een opsplitsing in de on-premise databronnen en de cloud databronnen.

Digitale bronnen onbekend bekend

3.2 Hoe krijgt de klant overzicht op de databronnen van de on-premise omgeving?

Het is belangrijk om inzichtelijk te hebben wat er allemaal gebeurt op het netwerk van de klant. Het netwerk zou op elk moment van de dag geraadpleegd moeten kunnen worden. In het oog houdende dat de medewerkers van de organisatie niet door verschillende tools en processen moet graven om inzicht te krijgen. Waarschijnlijk lukt dit nog niet als de consultant aankomt bij de klant, maar daarom hebben ze ook bij Avanade aangeklopt.

Het is optie de klant te vragen of er al een centraal logging platform draait. Dit kan bijvoorbeeld SYSLOG zijn of iets in die trant. Natuurlijk kan de klant ook een SIEM hebben draaien, maar is hij niet tevreden met zijn huidige SIEM. Andere vragen die je kan stellen zijn; "of ze individueel de logs op machines bekijken?", "wanneer hebben ze voor het laatst naar Windows server logs gekeken?". De kans is aanwezig dat de klant stuit op een onoverzichtelijke berg data. Daarom is SIEM, een centrale plek voor monitoring van security gerelateerde events in het leven geroepen.

“Welke databronnen zijn belangrijk?”.

Stap 1 -> Verzamel de databronnen eerst en begin klein.

Stap 2 -> Als er bezorgdheden zijn omtrent specifieke data, begin dan daar.

Stap 3 -> Welke data is het belangrijkste en rangschik deze.

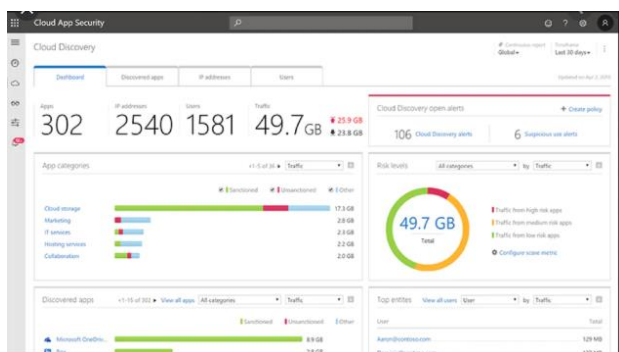
3.2.1 Checklist van mogelijke databronnen van de klant om inzicht te krijgen in de on-premise omgeving.

Log types	Ja / Nee in aantallen
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)	

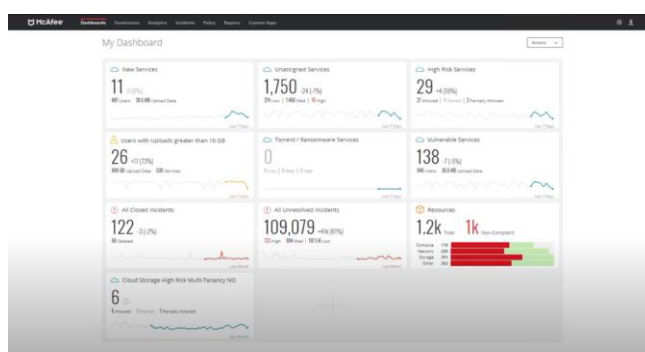
3.3 Hoe krijgt de klant een overzicht in de zijn cloud omgeving?

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.

Door middel van cloud discovery is het mogelijk om via traffic logs de onlinedatabronnen in beeld te krijgen. Hieronder twee voorbeeld van CASB-tools.

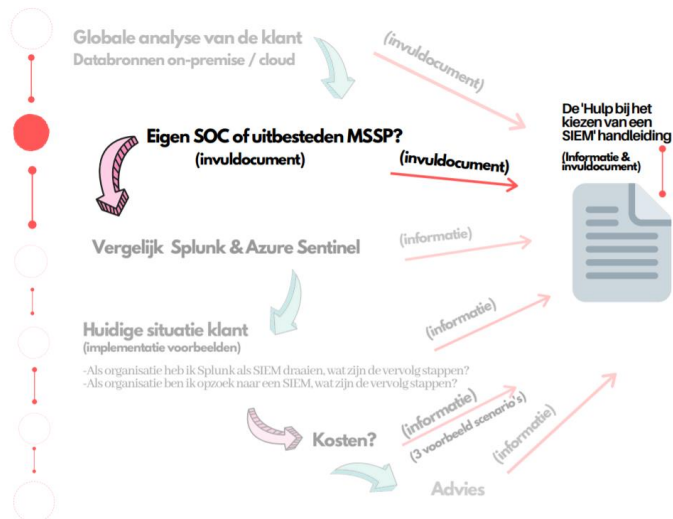


Microsoft Cloud App Security



McAfee MVISION Cloud

4 Heeft de klant een SOC nodig?



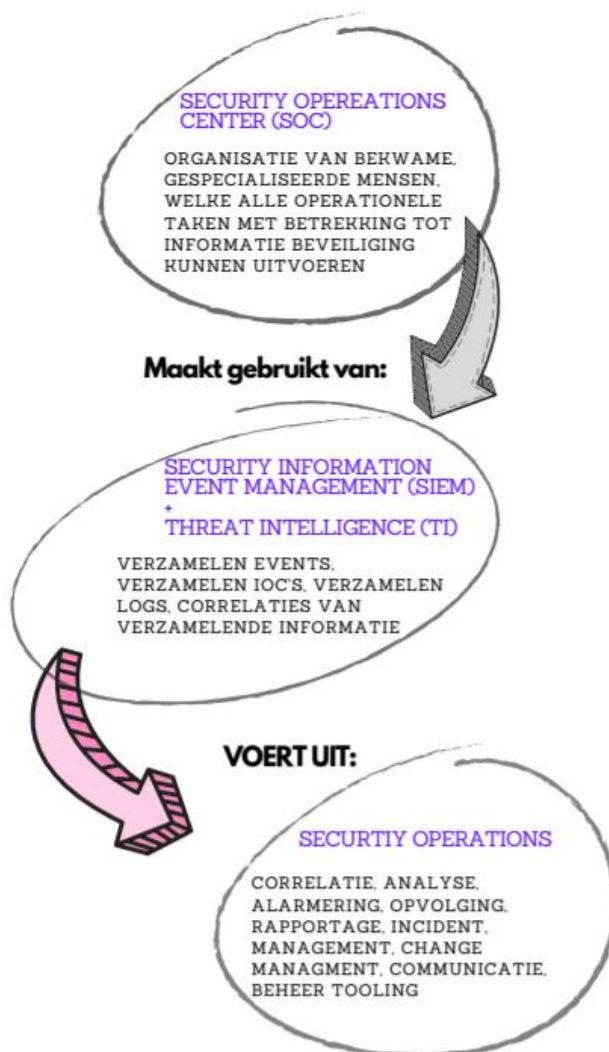
4.1 Inleiding

SOC is de afkorting voor Security Operations Center. De SOC is de plaats binnen de organisatie die alle IT-security gerelateerde zaken kan begeleiden en uitvoeren.

De medewerkers van een SOC hebben specifieke, diepgaande kennis van informatiebeveiliging, zowel op het gebied van technologie als ook processen en bedrijfsvoering.

Controle op de IT-infrastructuur is belangrijk voor organisaties die afhankelijk zijn van het digitale landschap. Deze controle kan worden uitgevoerd door een SIEM (Security Information Events and Management). Een goed geconfigureerde SIEM werkt als een zeef, waarin het veilige water wordt doorgelaten, maar de onveilige steentjes als alerts blijven hangen in de zeef.

Deelvraag 1; **'Welke organisaties zijn in staat om zelf een SOC te hebben en te houden (aantrekken en behouden van het noodzakelijke talent en ze up to date te houden) en voor welke organisaties is het verstandig om te kiezen voor een MSSP (SOC-as-a-Service)?'**



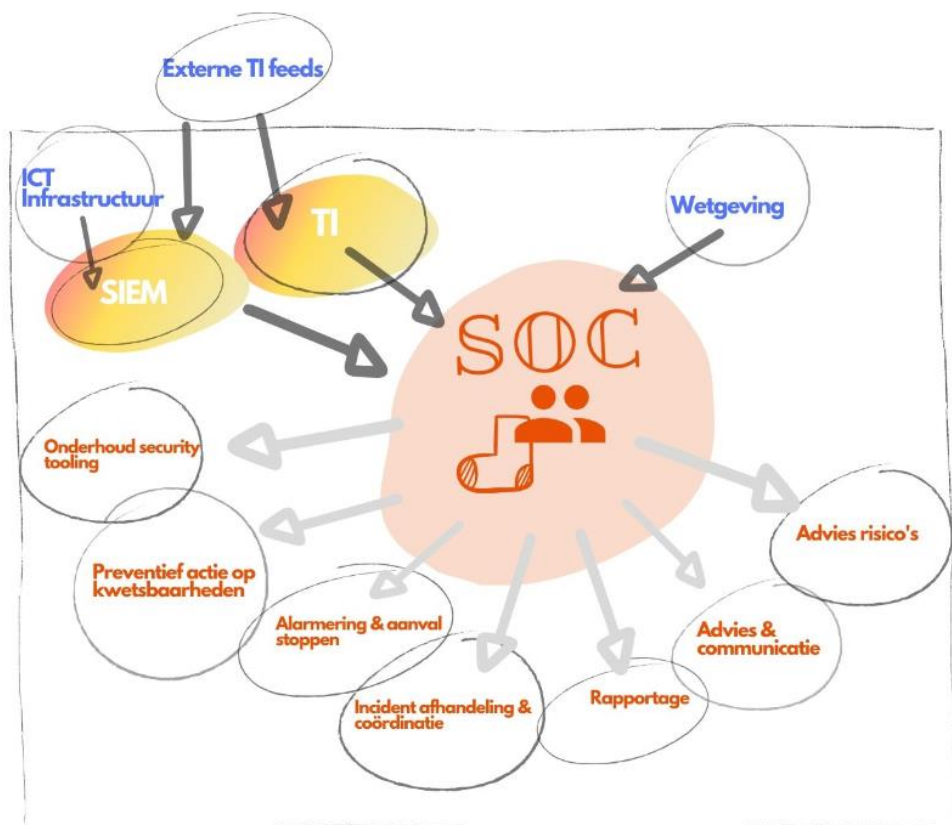
4.2 Een SOC bouwen binnen de organisatie of is uitbesteden een betere optie?

Niet elke organisatie heeft een eigen incident response 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 daarom is het ook nodig om naar outsourcing opties te kijken, zoals een MSSP (Managed Security Service Provider). Verder in het hoofdstuk wordt uitgelegd wat de verschillen zijn tussen een SOC intern en een MSSP.

4.2.1 De schematische weergave van een eigen SOC

Hieronder is een schematische weergave van de SOC te zien. De ICT-infrastructuur stuurt zijn data naar de SIEM en daar wordt het geanalyseerd. Alerts worden door het securityteam in de SOC gecategoriseerd op risico. Mocht het risicogehalte hoog genoeg zijn dan wordt er actie ondernomen. Daarnaast kan de SIEM worden ondersteund/aangevuld door (TI) Threat Intelligence. TI analyseert feeds en vergelijkt deze met eerdere gebeurtenissen. Als TI iets detecteert dan wordt het doorgestuurd naar de SOC.

De taken van het securityteam worden hieronder aangegeven in de wolkjes met oranje tekst.



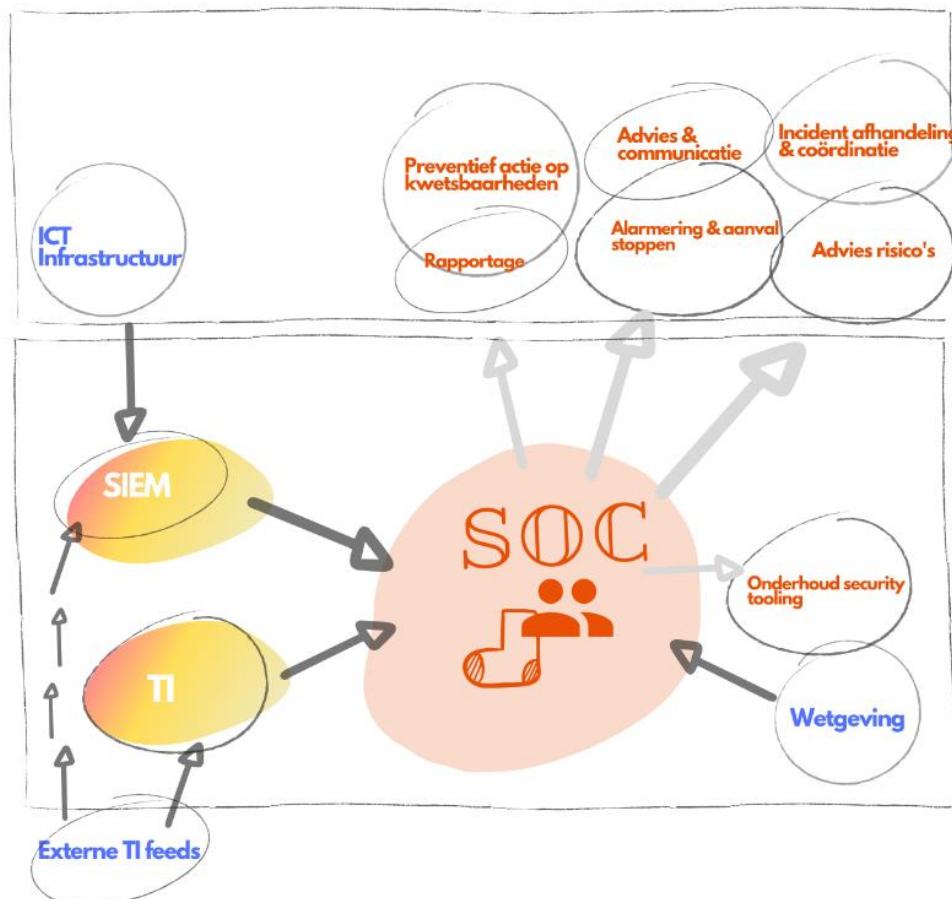
SOC intern

Een aantal belangrijke punten om rekening mee te houden als de organisatie intern een eigen SOC wil:

- Zijn er mensen met de juiste expertise en hoe behouden we deze binnen de organisatie, of kunnen deze mensen geworven worden?
- Heeft de organisatie use cases klaarliggen die demonstreren welke informatie/data inzichtelijk moet worden?
- Zijn er wettelijke (dwingende) redenen die van invloed zijn op de inrichting van het SOC?

4.2.2 De schematische weergave van een MSSP (Managed Security Service Provider)

Hieronder is een schematische weergave te zien van een SOC die is geoutsourced. Deze SOC wordt door een securityteam van een MSSP bemand en onderhouden. De bovenste rechthoek is het vak van de organisatie en de onderste rechthoek van de MSSP. De organisatie en de MSSP hebben interactie met elkaar. We zien dat de organisatie zijn data richting de SIEM van de MSSP stuurt. Het securityteam van de MSSP voert zijn taken uit om de organisatie te beschermen.



MSSP (SOC-as-a-Service)

Een aantal belangrijke punten om rekening mee te houden bij het outsourcen van de SOC:

- Hoe gaat de MSSP om met vertrouwelijke informatie en mag dat door de klant gecontroleerd worden in de vorm van een audit?
- Zijn er wettelijke (dwingende) redenen die van invloed/ belemmering zijn op de inrichting van een externe SOC?
- Blijft de verzamelde informatie, meestal met een privacygevoelig karakter, in Nederland, of in een ander land? En wat voor wettelijke impact heeft dat?
- Hoe gaat de MSSP om met de data die tijdelijk behouden moet worden van de klant?

4.2.3 Advies door middel van invuldocument

4.2.3.1 Inleiding

Er bestaat geen industrie standaard die de hamvraag van dit hoofdstuk beschrijft, omdat er geen industrie handleiding bestaat was het nodig opzoek te gaan naar betrouwbare informatie om de kwaliteit van dit onderzoek te waarborgen. Een onderzoek van MITRE gaf ondersteuning.

De MITRE Cooperation is een Amerikaanse not-for-profit organisatie. MITRE bestaat uit verschillende FFRDCs (federally funded research and development centers). Een aantal van deze centers zijn Defense & Intelligence, Healthcare en ook Cybersecurity. Carson Zimmerman werkt binnen de cybersecurityafdeling als cybersecurity engineer en heeft in naam van MITRE het boek; *“Ten Strategies of a World-Class Cybersecurity Operations Center”* geschreven. Verschillende informatie uit het boek heb ik toegepast in dit hoofdstuk.

4.2.4 Beoordelingsdocument

4.2.4.1 Inleiding beoordelingsdocument

Om de consultant van Avanade bij te staan in de zoektocht naar de SIEM-oplossing is het beoordelingsdocument samengesteld die als startpunt dient voor het SOC onderzoek en daarnaast de consultant aan het denken zet en adviseert. Dit document zal bestaan uit werkbladen, informatie en tips. Het doel van dit werkblad is om te bepalen of de organisatie geschikt is voor een eigen SOC of dat de organisatie beter voor een andere oplossing kan kiezen. De andere opties worden verder in dit hoofdstuk besproken. Dit werkblad laat de consultant en zijn klant nadenken over de beveiligingsrisico's van zijn of haar bedrijf. De waarde van dit document voor de klant is een stuk bewustwording over wie zij zijn en waar zij staan in het informatie beveiligingslandschap.

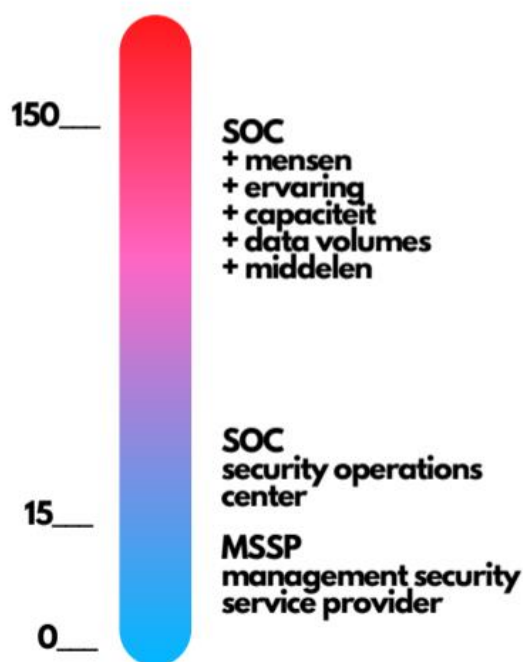
4.2.4.2 Uitleg werkblad

De vragen in het werkblad hebben als doel om het potentiële risico in te schatten op bedreigingsgevaar van hackers en datalekken voor een organisatie. Kritieke data, zoals persoonsgegevens en bedrijfsgeheimen zullen het risico op schade van hackers vergroten. 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. Hieronder volgt verdere uitleg.

Het is belangrijk om de kwaliteiten van de organisatie in het oog te houden bij het invullen van het werkblad. Als de vraag 1-7 met 'ja' beantwoordt is dan wordt één punt toe bedeed. Bij een 'nee' zijn er geen punten te verdienen = 0. 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 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 geen rekening houdt met de grootte 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 grote volumes data.

Hieronder 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. Dat zien we ook terug in figuur 4.



Figuur 4

4.2.4.3 Werkblad

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.		

4.2.4.4 Voorbeeld 1,2,3

Introductie scenario 1

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.	$40 * 3 = 120$	

4.2.5 Opties voor het outsourcen van de SOC

Op het moment dat de score lager is dan 15 dan zijn er aantal scenario's denkbaar. De keuze die hierin wordt gemaakt hangt af van de belangen van de organisatie. Hier volgen een paar opties.

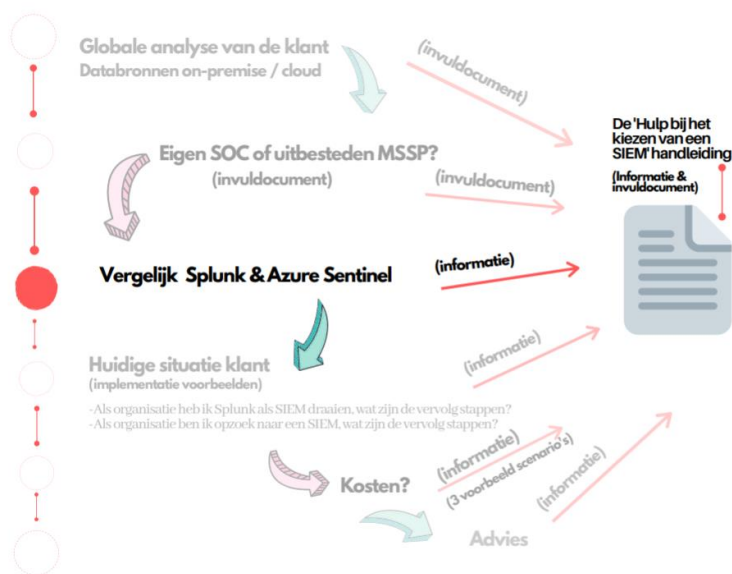
1. Een eerste optie is het outsourcen van de SOC aan een MSSP (Management Security Service Provider). In deze constructie betaalt de organisatie een derde partij voor het monitoren van zijn/haar organisatie en andere services terug te vinden bij 4.2.2 in de schematische tekening. Het securityteam van de MSSP heeft de technische vaardigheden om een SOC te laten functioneren, maar waarschijnlijk kennen zij niet de missie en de interne regelgeving van de organisatie. Daarnaast is de SOC van de MSSP vaak niet gepositioneerd in hetzelfde land als de organisatie. Het securityteam van de MSSP heeft de technici vaardigheden, maar een SOC outsourcen kan de reactietijd verlagen, de MSSP kan zich minder goed mengen in het politieke debat van de organisatie en daardoor kan de interne missie van de organisatie leiden onder deze oplossing.
2. Als de organisatie deel uitmaakt van een overkoepelde organisatie, zoals verschillende universiteiten of een overheidsbedrijf dan is er de mogelijk de SOC onder te brengen in de overkoepelende organisatie. Dit kan je zien als een soort outsourcing, maar in sommige omstandigheden hoeft dit relatief weinig geld te kosten.
3. Het inhuren van een MSSP die opereert vanuit de organisatie zelf. In dit scenario is de SOC gepositioneerd in de organisatie, maar wordt volledig bedient door medewerkers van de MSSP. Bij dit scenario is het belangrijk dat er goede contracten worden opgesteld en dat de bevoegdheden van de medewerkers in de SOC duidelijk zijn.

4.3 Tips bij het opzetten van een SOC

- Focus op een paar punten en voer die goed, in plaats van meerdere punten half uit te voeren. Probeer daarnaast activiteiten te vermijden die beter door andere organisaties uitgevoerd kunnen worden.
- Probeer het wiel niet opnieuw uit te vinden;
 - Reconstrueer bestaande formaten die bruikbaar zijn voor de SOC
 - Maak gebruik van bestaande technologieën en middelen om op te starten.
 - Laat de huidige toestroom van middelen binnen de organisatie je niet afleiden voor het inrichten van de SOC.
- Focus op technologieën die het dreigingsrisico aankunnen en haal het maximale uit een beperkte set van tools.
- Geef de meest bekwame analisten de verantwoordelijkheid om continu te verbeteren en te automatiseren.
- Zorg van het eerste moment voor een sterke kwaliteitscontrole binnen de SOC.
- Houdt de missie van de organisatie in de gaten met betrekking tot monitoring.

5 Welke SIEM is geschikt voor de klant?

"It's easy to buy 'Technology', but the always evolving threat landscape demands mature 'People' and 'Processes' as well to be on top of the game."



5.1 Wat is een SIEM?

'In the cloud, things aren't always what they SIEM'

Het is belangrijk eerst te begrijpen wat een SIEM (Security Information and Management) en SOAR (Security Orchestration, Automation en Response) is en betekent. De hoeveelheid informatie die gegenereerd wordt op het netwerk van de klant kan qua volume angstaanjagend veel zijn, maar door de informatie goed te organiseren kunnen we de angst inzichtelijk maken, begrijpen en omzetten in waardevolle informatie. Een SIEM kan het verschil maken en Gigabytes aan data filteren naar waardevolle informatie die de bescherming van het netwerk kan waarborgen.

Aan de andere kant is een SOAR een harmonieuze samenkomst van componenten. Het 'orchestration' deel is het deel waar verschillende componenten integreren en samenwerken onder gecentraliseerd beheer. Het is een beetje de juf op een schoolreisje die alle kinderen bij elkaar probeert te houden. Het automation component is een actie gedreven onderdeel dat zijn werk gaat doen als het wordt getriggerd. Via een vooropgestelde workflow voert het zijn beveiligingstaak uit.

Een SIEM bestaat uit twee delen. Aan de ene kant de Security Event Manager (SEM) dat zich focust op real-time events op het netwerk (data verzameling). Aan de andere kant hebben we de Security Information Manager (SIM) die zich meer richt op lange termijn data behoud en analyse (Data omzetten naar informatie\filteren). Een SIM is ook belangrijk voor breaches die op een later tijdstip gedetecteerd worden, zo is het mogelijk om met terugwerkende kracht informatie uit de data te filteren.

5.2 Splunk & Azure Sentinel vergelijken aan de hand van requirements

5.2.1 Inleiding

Deze requirements worden opgesteld om te beoordelen hoe ver de ontwikkeling van opties binnen Azure Sentinel staan ten opzichte van Splunk. Wat is er allemaal mogelijk? Splunk is opgericht in 2003 en richt zich als 17 jaar op analyse software. Azure Sentinel is 1.5 jaar op de markt. Met de requirements kijken we naar de basale eigenschappen van de twee SIEM-tools. Wat hebben ze allemaal in huis, niet meer niets minder. Hiermee zal niet worden uitgezocht hoe de werking is van de functionaliteiten. Dat zal ook geen volledig antwoord geven op de deelvraag. Later in het onderzoek zal een specialist meer diepgang geven in de werking van de functionaliteiten.

Aan de hand van de requirements ga ik beide tools testen op de functionaliteiten. Deze requirements heb ik opgesteld aan de hand van informatie van Frank Molenaar, het afstudeeronderzoek van Justin van Cromberge en literatuuronderzoek. Justin heeft 10 verschillende SIEM-tools onderzocht bij Avanade onder begeleiding van Frank Molenaar in periode van eind 2019 begin 2020. De kennis die Justin heeft verworven is relevant voor mijn onderzoek en deze zal ik raadplegen waar nodig.

Tijdens mijn studieperiode aan de Thomas More in Geel heb ik een aantal keer gewerkt met de MoSCoW-methode. Deze methode zal ik ook gebruiken en inzetten om Splunk en Azure Sentinel te vergelijken.

5.2.2 MosCow Methode

De MosCoW-methode is een manier om de opgestelde requirements te rangschikken op prioriteit. Het wordt vaak gebruikt in de IT-wereld om software/hardware te vergelijken. Het rangschikken gaat als volgt.

- M – must have: de requirements zijn noodzaak in het eindresultaat terug te komen, zonder deze eisen is het product niet bruikbaar.
- S – should have: deze requirements zijn zeer gewenst, maar zonder het product is het wel bruikbaar.
- C – could have: deze requirements komen alleen aan bod als er genoeg tijd is.
- W – won't have: deze requirements komen in dit project niet aan bod, maar kunnen bij een vervolgproject, interessant zijn.

5.2.3 Requirements

#REQ	Onderwerp	Prioriteit
REQ-01	Centralized monitoring	Must have
REQ-02	SOAR (Security, Orchestration, Automation and Response)	Must have
REQ-03	Scalability	Must have
REQ-04	Cross-platform	Must have
REQ-05	Integration (common and other data sources)	Must have
REQ-06	Implementation	Should have
REQ-07	UEBA (User and Entity behavior analytics)	Should have
REQ-08	Shadow IT-monitoring	Should have
REQ-09	AI & Machine Learning	Should have
REQ-10	Threat Intelligence sources	Should have
REQ-11	Community	Could have
REQ-12	One platform (for Log Management, SIEM, UEBA and SOAR)	Could have
REQ-13	SaaS (Software as a platform)	Could have

5.2.4 Requirements uitgeschreven

REQ 1 – Centralized Monitoring: Het is de bedoeling dat log bestanden van zowel on-premises en die van cloud services bij elkaar komen in een centraal systeem. Dit zorgt voor overzicht en is hanteerbaar voor het securityteam.

REQ 2 – SOAR (Security, Orchestration, Automation and Response): Een SOAR maakt het verschil op de SIEM-markt; het heeft de mogelijkheid om automatisch actie te ondernemen op basis van verworven informatie. Er is de mogelijkheid veelvoorkomende acties te automatiseren en het orkestratie gedeelte vereenvoudigt dit door middel van playbooks. In de volgende link wordt uitgelegd hoe jezelf een playbook aanmaakt in Azure Sentinel vanaf 10:00 min (<https://www.youtube.com/watch?v=oiWlnLYvnUk>)

REQ 3 – Scalability: Een product is schaalbaar als het de mogelijkheid heeft zich aan de passen naar de wensen van de gebruiker. Schaalbaarheid is noodzakelijk vanuit verschillende standpunten. Op het moment dat de organisatie groeit dan moet de SIEM-tool de groeiende datastroom aankunnen. Daarnaast moet er de mogelijkheid zijn nieuwe databronnen te koppelen. Vanuit het perspectief dat een organisatie krimpt moet het ook mogelijk zijn dat er terug geschaald kan worden.

REQ 4 – Crossplatform: Als het systeem op zowel Windows als Linux platformen kan draaien.

REQ 5 – Integration (Out of the box data connector – common and other data sources): Het centraal monitoren van data kan alleen gebeuren als data uit verschillende bronnen wordt samengebracht in de SIEM. De brug die gebouwd moet worden van de databronnen naar de SIEM wordt gedaan met data connectoren. De datalogs die hier binnenkomen zijn bijvoorbeeld Host/Endpoint Logs, Authentication Logs, Cloud Infrastructure Logs, Cloud Application Logs of Network Infrastructure and Device Logs.

Hieronder een overzicht van landschappen waar men connectoren voor nodig heeft.

- Cloud omgevingen:
 - Amazon Web Services (AWS)
 - Microsoft Azure
 - Google Cloud
- Besturingssystemen (zowel server als client):
 - Windows
 - Linux
 - Apple OS X
- Software:
 - SaaS oplossingen
 - Dropbox
 - Office 365
 - ServiceNow
 - On-premises software

REQ 6 – Implementation (moeilijkheidsgraad): Het implementeren van een SIEM-oplossing is complex en kostbaar. Daarnaast vraagt het een stevig doorzettingsvermogen van alle betrokkenen. Het traject vereist expertise en een stevig mandaat vanuit het hogere management. Als een SIEM van de IT-afdeling van een bedrijf wordt geïnitieerd leidt dit meestal tot onvoldoende mandaat, budget, tijd en een tekort aan medewerking.

REQ 7 – UEBA (User and Entity behavior analytics): UEBA analyseert de “entiteiten” en “events” uit routers, servers en endpoints. UEBA-oplossingen zijn krachtiger dan UBA-oplossingen, omdat ze complexe aanvallen van meerdere gebruikers, IT-apparaten en IP-adressen kunnen detecteren.

PROS:	CONS:
Automatisch detecteren (verschillende interne en externe cyberaanvallen)	Kosten Kleinere organisaties hebben waarschijnlijk niet zo'n complex systeem nodig
Reduceren van security analisten (minder mensen in dienst)	Complexiteit ten opzichte van UBA neemt toe (analisten hebben eventueel extra training nodig)
Het naar beneden schroeven van het budget (voor cybersecurity)	Het is geen totale vervanging voor je cyber verdediging

REQ 8 – Shadow IT-monitoring: Dit is een manier om in kaart te krijgen welke applicaties er allemaal worden gebruikt door de werknemers. Wanneer IT-beheerders wordt gevraagd hoeveel Cloud-apps ze hun werknemers laten gebruiken, is het gemiddeld 30 tot 40, in werkelijkheid is het gemiddelde meer dan 1000 apps die worden gebruikt door werknemers in de organisatie.

Fase1: schaduw IT detecteren en identificeren

Fase2: evalueren en analyseren

Fase3: uw apps beheren

Fase4: advanced shadow IT discovery-rapportage

In fase 4 gaan we de Cloud Discovery logboeken integreren in de SIEM voor verder onderzoek en analyse.

REQ 9 – AI & Machine Learning: Machine learning verwijst naar een tak van kunstmatige intelligentie (AI). Machine learning binnen een SIEM zorgt ervoor dat analyses binnen de SIEM eenvoudig en makkelijker gedaan worden door automatisering. Dit resulteert in werkontlasting voor werknemers van het securityteam. Als machine learning modellen goed functioneren binnen een SIEM dan kan het op basis van gegevens die het ontvangt beslissingen nemen.

REQ 10 – Threat Intelligence: Bij TI worden kenbare bedreigingen gebruikt om vergelijkbare dreigingen te vinden in de datastroom. IoC's (indicator of compromise) zijn TI-feeds die organisaties gebruiken om bedreigingen op te sporen. Het gebeurt ook dat organisaties nieuwe IoC's vinden. Het is belangrijk dat organisaties deze nieuwe IoC's met elkaar delen, zodat de beveiliging bij organisaties gewaarborgd blijft. Een SIEM kan verbinden met verschillende TI-sources en TI kan als bron functioneren. Verwacht wordt dat door een toenemende complexiteit van cyber aanvallen een combinatie van TI en SIEM noodzakelijk is.

REQ 11 – Community: Een online community is een essentieel onderdeel van het dagelijkse werk voor IT'ers. Het communiceren met mensen uit hetzelfde werkveld. Het lezen van reviews en oplossingen van andere technici. Het helpen van mensen en geholpen worden. Een actieve community kan het dagelijks leven een stuk aangenaamer maken. De boodschap is; “maak gebruik van het collectieve geheugen.”

REQ 12 – One platform: Voor de gebruikersvriendelijkheid en efficiëntie is het goed als de SIEM, SOAR, log management en UEBA op één platform werken. Zonder dat het cybersecurityteam niet voor elke tool een ander platform moet gebruiken en daardoor het overzicht sneller kwijtraakt.

REQ 13 – SaaS (Software as a Service):

Dit is software dat als dienst online wordt aangeboden. De SaaS-aanbieder zorgt voor installatie, onderhoud en beheer, de gebruiker benadert de software over het internet bij de SaaS-aanbieder.

5.3 SIEM Tooling Capabilities

5.3.1 Globaal overzicht

Hieronder zijn de requirements in een tabel gegoten en vergeleken met Splunk en Azure Sentinel.



Voldoet aan requirement






















Voldoet gedeeltelijk aan requirement





Voldoet niet aan requirement

	REQ#	Splunk>	Microsoft Azure Sentinel
Centralized monitoring	REQ-1	Splunk is een SIEM-product die logs centraal uit on-premises en cloud omgevingen samen laat komen voor analyse. ✓	Met dit cloud native SIEM-product als Azure Sentinel kunnen organisaties logs van zowel on-premises als uit de cloud analyseren. ✓
SOAR (Security, Orchestration, Automation and Response)	REQ-2	Splunk Phantom is de SOAR van Splunk. Het automatiseren van taken kan gedaan worden via Python playbooks. Phantom draait op een aparte virtuele machine in een AWS EC2 instance. Het vergt technische kennis om dit op te zetten. Via de Phantom Add-On is mogelijk de Splunk Phantom te configureren met je Splunk account. ✓	Azure Sentinel biedt goede SOAR-mogelijkheden aan door middel van een Fusion en Jupyter notebook integratie. Het automatiseren van de taken kan gedaan worden door zogenaamde playbooks. Deze playbooks kunnen ook worden aangemaakt door non-developers aangezien er een goede GUI beschikbaar is. ✓
Scalability	REQ-3	Splunk is schaalbaar naar de wensen van de klant. De organisatie biedt een capacity planning guide aan die de gebruiker helpt bij het maken van hardware keuzes. Als een Splunk server niet genoeg dan heb je de mogelijkheid er één toe te voegen. Binnenkomende data wordt automatisch verdeeld en zoekopdrachten worden naar alle	Azure Sentinel is cloud native SIEM die schaalbaar is naar de vraag van de klant. Met de Pay-As-You-Go betaal je gewoonweg voor het gebruik van resources. ✓

		<p>Splunk-instanties verzonden. Dit zorgt ervoor dat de opdrachtverwerking toeneemt in snelheid met het toevoegen van meer machines. Optioneel kan redundantie worden ingeschakeld zodat elke gebeurtenis op twee of meer Splunk-servers wordt opgeslagen.</p> 	
Cross-platform	REQ-4	<p>Splunk kan geïnstalleerd worden op verschillende platformen (Windows, iOS, Linux). Splunk is gemakkelijk te installeren en te gebruiken.</p> 	<p>Azure Sentinel is een cloud native SIEM vanwege dit feit is het niet afhankelijk van een OS. Azure Sentinel is te bereiken via een browser met internetverbinding.</p> 
Integration (Out of the box data connectors - common and other data sources)	REQ-5	<p>400</p> 	
Implementation (moeilijkheidsgraad)	REQ-6	<p>Splunk moet geïnstalleerd worden op een OS naar keuze. Splunk biedt een handige installatie gids die je stap voor stap meeneemt in dit verhaal. Er is ook nog een optie voor Splunk Cloud, maar deze moet altijd geconfigureerd worden aan Splunk Enterprise Security. Dit zorgt ervoor dat Splunk nooit helemaal in de cloud draait. Het kopen en installeren van Splunk is eveneens niet het moeilijke gedeelte. Het wordt ingewikkeld bij configuratie, integratie en het dagelijkse analyseren door het securityteam.</p> 	<p>De implementatie van Azure Sentinel is redelijk eenvoudig binnen de Azure portal. Eerst maak je een Log Analytics workplace aan en daarboven op komt Azure Sentinel te draaien. De implementatie van de SIEM is niet het moeilijke vraagstuk, maar het configureren ervan is het lastige karwei.</p> 
UEBA (User and Entity behavior analytics)	REQ-7	<p>Een Splunk add-on maakt het mogelijk om Splunk Enterprise Security en Splunk User Behavior (UBA) te integreren in je SIEM-oplossing. Aan deze add-on zitten kosten verbonden. Om deze add-on aan te schaffen moet je wel extra kosten bestalen.</p> 	<p>Microsoft Cloud App Security zorgt voor entiteit gedragsanalyse (UEBA) in de Cloud. Deze kan geconnecteerd worden via een Data connector met Azure Sentinel.</p> 
Shadow IT-monitoring	REQ-8	<p>Dit zit niet standaard in Splunk het is wel mogelijk te connecteren met een</p>	<p>Met Cloud App Security Platform (CASP) is Shadow IT native ingebouwd in Azure Sentinel.</p>

		Cloud App Security Platform (CASP) om het doel te bereiken. 																			
AI & Machine Learning	REQ-9	De Splunk Machine Learning Toolkit maakt het mogelijk om incidenten in de organisatie te detecteren, voorspellen en te voorkomen. Het is mogelijk je eigen machine learning modellen te integreren met de toolkit. In deze toolkit zitten standaard 25 Python algoritmes en het geeft toegang tot 300 andere op source bibliotheken. 	Azure Sentinel maakt gebruik van schaalbare algoritmen voor machine learning die zijn gebaseerd op tientallen jaren ervaring van het Microsoft securityteam dat echte bedreigingen binnen enkele minuten kan vinden, onderzoeken en kan oplossen. Deze ingebouwde modellen brengen miljoenen laagdrempelige afwijkingen met elkaar in verband en verbinden deze om een paar serieuze beveiligingsincidenten aan de analist te presenteren. Het is ook mogelijk om Azure Machine Learning te gebruiken voor het bouwen van eigen modellen of aan te passen. 																		
Threat Intelligence sources	REQ-10	Splunk beschikt over standaard 17 Threat Intelligence sources. Hier tussen staat I-Blocklist, SANS, abuse.ch. Andere TI sources kunnen handmatig worden toegevoegd.  https://docs.splunk.com/Documentation/ES/6.1.0/Admin/Includedthreatintelsources Included threat intelligence sources <small>The threat intelligence sources are parsed for threat indicators and added to the relevant KV Store collections.</small> <table><thead><tr><th>Threat source</th><th>Threat list provider</th><th>Website for the threat source</th></tr></thead><tbody><tr><td>Emerging Threats compromised IPs blocklist</td><td>Emerging Threats</td><td>https://rules.emergingthreats.net/blockrules</td></tr><tr><td>Emerging Threats firewall IP rules</td><td>Emerging Threats</td><td>https://rules.emergingthreats.net/firewallrules</td></tr><tr><td>Malware domain host list</td><td>Hail o TAXII.com</td><td>http://hailoatxii.com</td></tr><tr><td>iBlocklist Logmein</td><td>iBlocklist</td><td>https://www.i-blocklist.com/lists</td></tr><tr><td>iBlocklist Prolebay</td><td>iBlocklist</td><td>https://www.i-blocklist.com/lists</td></tr></tbody></table>	Threat source	Threat list provider	Website for the threat source	Emerging Threats compromised IPs blocklist	Emerging Threats	https://rules.emergingthreats.net/blockrules	Emerging Threats firewall IP rules	Emerging Threats	https://rules.emergingthreats.net/firewallrules	Malware domain host list	Hail o TAXII.com	http://hailoatxii.com	iBlocklist Logmein	iBlocklist	https://www.i-blocklist.com/lists	iBlocklist Prolebay	iBlocklist	https://www.i-blocklist.com/lists	Met Threat Intelligence in Azure Sentinel wordt vaak gerefereerd aan Palo Alto Networks MineMeld. Daarnaast de open-source tool MISP (Malware Information Sharing Platform) en ThreadConnect. Andere TI sources kunnen handmatig worden toegevoegd. https://www.inspark.nl/misp-threat-intelligence-azure-sentinel/ 
Threat source	Threat list provider	Website for the threat source																			
Emerging Threats compromised IPs blocklist	Emerging Threats	https://rules.emergingthreats.net/blockrules																			
Emerging Threats firewall IP rules	Emerging Threats	https://rules.emergingthreats.net/firewallrules																			
Malware domain host list	Hail o TAXII.com	http://hailoatxii.com																			
iBlocklist Logmein	iBlocklist	https://www.i-blocklist.com/lists																			
iBlocklist Prolebay	iBlocklist	https://www.i-blocklist.com/lists																			
Community	REQ-11	Splunk heeft een grote community, ook met community groups over de hele wereld. Op github is veel info en voorbeelden te vinden. 	Microsoft Tech Community is een plek waar je vragen kan stellen en informatie kan vinden. De pagina voor Azure Sentinel is nog niet super actief evenals de github pagina en reddit fora. Natuurlijk is het overkoepelende platform Azure wel erg actief, daar zijn veel mensen te vinden die graag helpen. 																		
One platform (for Log Management, SIEM, UEBA and SOAR)	REQ-12	Nee UEBA draait op een aparte AWS EC2 instance. 	Ja dit is te vinden op de Azure Portal. 																		

SaaS (Software as a Service)	REQ-13	Gedeeltelijk (Geen SaaS voor UEBA) 	Ja het is volledig SaaS. Eerst zetten we Log Analytics workspace op in Azure. Dan integreren we Sentinel met de Analytics workspace. Dit gebeurt allemaal in de Azure portal. Log Analytics kan je zien als de motor van Sentinel. (Zelf playbook)  https://www.youtube.com/watch?v=oiWInLYvnUk
-------------------------------------	--------	---	--

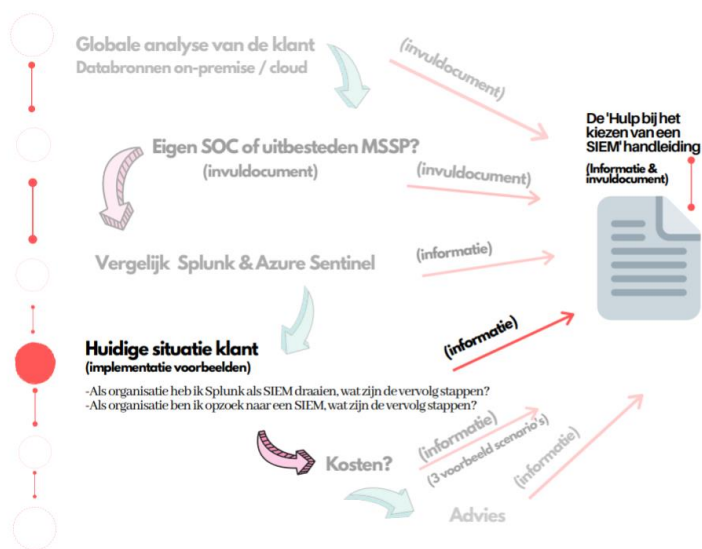
5.3.2 Beslissingsmatrix op basis van output MosCow

Hieronder is een beslissingsmatrix te zien waarin de weegfactor wordt afgetoetst tegen de behaalde score en wordt vermenigvuldigd. De conclusie is dat Splunk> en Azure Sentinel op het gebied van functionaliteiten erg aan elkaar gewaagd zijn.

Het grote verschil gaat hem niet zitten in de mogelijkheden van beide SIEM-oplossingen, maar juist in de benadering van de SIEM-oplossing. Hoe gaat er met deze SIEM gewerkt worden? Welke mensen gaan ermee werken en wat is hun expertise en ervaring? Welke data komt er binnen? In de bijlage onderaan in dit document staan de highlights van een diepte-interview met Greg Peterson, hier komen feiten over Splunk en Sentinel naar boven op basis van ervaring en onderzoek

		splunk>		Azure Sentinel	
		Wegingsfactor	Score	Weging Score	Weging Score
Centralized monitoring	REQ-1	3	3	9	3
SOAR (Security, Orchestration, Automation and Response)	REQ-2	3	3	9	3
Scalability	REQ-3	3	3	9	3
Cross-platform	REQ-4	3	3	9	3
Integration (common and other data sources)	REQ-5	3	3	9	2
Implementation	REQ-6	2	1	2	1
UEBA (User and Entity behavior analytics)	REQ-7	2	2	4	2
Shadow IT-monitoring	REQ-8	2	1	2	2
AI & Machine Learning	REQ-9	2	2	4	2
Threat Intelligence sources	REQ-10	2	2	4	2
Community	REQ-11	1	1	1	1
One platform (for Log Management, SIEM, UEBA and SOAR)	REQ-12	1	0	0	1
SaaS (Software as a platform)	REQ-13	1	0.5	0.5	1
				53.5	54
					Totaal

6 Drie implementatie scenario's



6.1 Inleiding

Het implementeren van een SIEM-oplossing kan vanuit een paar perspectieven worden gedaan in de Avanade context. In de hoofdstuk ga ik er twee behandelen.

- Als organisatie ben ik opzoek naar een SIEM, wat zijn de vervolg stappen?
- Als organisatie heb ik Splunk als SIEM draaien, wat zijn de vervolg stappen?

Hieraan is de volgende deelvraag gekoppeld; **"Onderzoek drie scenario's die een consultant van Avanade kan tegenkomen bij een SIEM-implementatie?"**

Maar om alvast een beeld te schetsen van de **moeilijkheidsgraad** van een implementatie zal het eerste deel van dit hoofdstuk gaan over de migratie van Splunk naar Azure Sentinel bij Avanade. Dit gebeurde ongeveer een jaar geleden en werd gestuurd vanuit Seattle (USA). Ik was in het volgende fragment in gesprek met Greg Peterson, een van de leidinggevende omtrent de implementatie. Ik stelde de volgende vraag; "Can you maybe take me a bit on the journey of the migration from Splunk to Sentinel you did at Avanade, maybe share a bit of your experiences?". Ik zal drie quotes geven uit het antwoord dat Greg gaf; "Could we at least get to the same of what we were doing in Splunk or better or close enough. So one was log ingestion and retention. So we talked a lot about log ingestion. And we got to a point again, that was our longest pole or critical path item. Can we actually get those logs in a sustainable fashion? The other bit would be. Can we do similar sets of correlation rules or use cases? So once you get all the data into this and can you actually alert and respond to it? We did it with similar use cases and we probably had thirty or thirty-five different use cases in Splunk. Custom rules, looking for various different things and providing alerts based on what we saw, which I would call just because I, my own worst critic would call it immature. But nevertheless, it was what we were doing."

De tweede quote; "So from using, you know, Splunk query language to Kusto query language within Sentinel. Then there's also a bit of cross training. And our team was all trained in Splunk and they're intended to be trained in Splunk. So when we started talking about moving to a Microsoft solution, we actually switched teams within Accenture. So they had another team that while Sentinel is still relatively new and they didn't have much experience. Accenture did have a solution for security monitoring built on top of log analytics. And it's ultimately the same

substrate, right?

De derde quote; "And so we had a transition period for them where again, we cross-trained, we got them up to speed on our use cases. We also threw in some additional sort of fresh look at how we do security incident response and monitoring. **So it's not just a migration to Sentinel.** We also heavily leverage MTP. So Microsoft Threat Protection, which provides actually lots of SIEM like features in advanced hunting features using the same languages, but potentially against different sets of data that's correlated together. So over time we're working with Microsoft to let them or help them make all of those data sources more easily consumable in Sentinel."

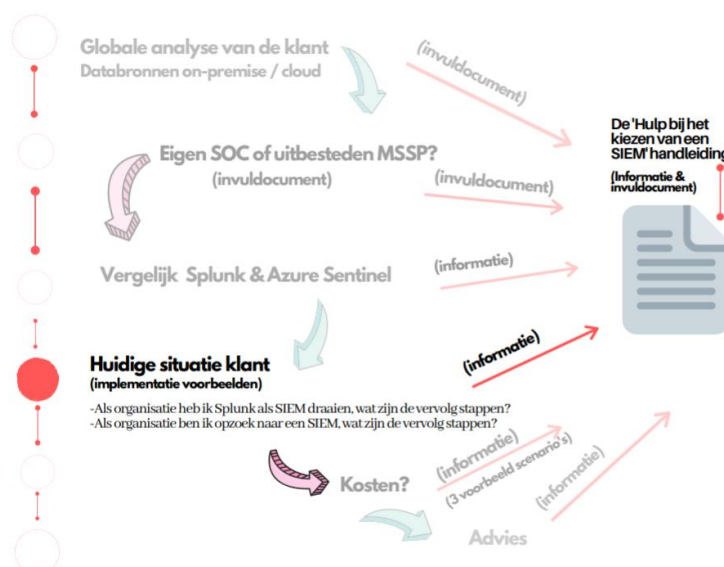
Er komen hier een paar interessante migratie verhalen naar boven. Een kritieke vraag van Greg bij de migratie was; "Kunnen we log ingestion and retention, oftewel opname en behoud van logs goed uitvoeren en belangrijker nog omzetten naar een duurzame gebruiksvorm?", "Kunnen we de use cases die we in Splunk gebruikten overzetten naar Sentinel?"

Het team dat voor Avanade werkte aan Splunk, was getraind in Splunk en werkte hier graag mee. Op het moment dat Avanade aankondigde dat ze de overgang zouden maken naar de Microsoft oplossing zou er heel wat cross training gedaan moeten worden om de nieuwe query taal Kusto te leren. Dit is de taal die wordt gebruikt in Sentinel. De oplossing hiervoor was een team ruil met Accenture. Accenture had een team dat werkte met security monitoring dat gebouwd was boven op Log Analytics, dezelfde onderliggende tool wordt ook gebruikt bij Sentinel. Hier blijkt uit dat een migratie veel meer is dan alleen de vervanging van software. De reden van deze introductie om een bewustwording te creëren van de complexiteit van een SIEM-implementatie.

6.2 Twee implementatie scenario's beschreven

6.2.1 Scenario 1; "Als organisatie ben ik opzoek naar een SIEM, wat zijn de vervolg stappen?"

Om een centraal inzicht te krijgen in security gerelateerde events uit verschillende omgevingen is een klant van Avanade op zoek naar een centrale oplossing. In deze situatie zal de consultant van Avanade de verschillende stappen doorlopen die terugkomen in dit onderzoek. Deze verschillende stappen zijn in de figuur hieronder terug te vinden. De vetgedrukte 'Huidige situatie klant (implementatie voorbeelden)' is de huidige stap die in dit hoofdstuk wordt uitgewerkt. Voordat we uiteindelijk bij deze stap zijn aangekomen zien we dat er al heel wat vooronderzoek gedaan is.



Hieronder worden (twee) focus punten aangehaald die een grote rol spelen bij het kiezen van Splunk dan wel Azure Sentinel als SIEM-oplossing. Dit zal ik onderbouwen door de ervaring van Greg Peterson en een onderzoek van Accenture naar Splunk & Azure Sentinel.

Als we kijken naar organisaties die nieuw zijn op het gebied van security. Dan is Azure Sentinel een interessante keuze, omdat de volwassenheid van de organisatie en Azure Sentinel gelijktijdig groeien. Op het moment dat de volwassenheid van de organisatie groeit zal Sentinel meer geavanceerde features releasen die in het beginstadia van het bouwen van de SIEM-oplossing nog geen belangrijke rol spelen. Die nieuwe features die gedurende tijd gereleased worden komen in preview modus bij Sentinel en kunnen zo uitgetest worden door de klant. Daarnaast kan de klant zijn nieuwe producten baseren om Microsoft omgeving om een makkelijke integratie te hebben met Sentinel en goedkoper uit te zijn.

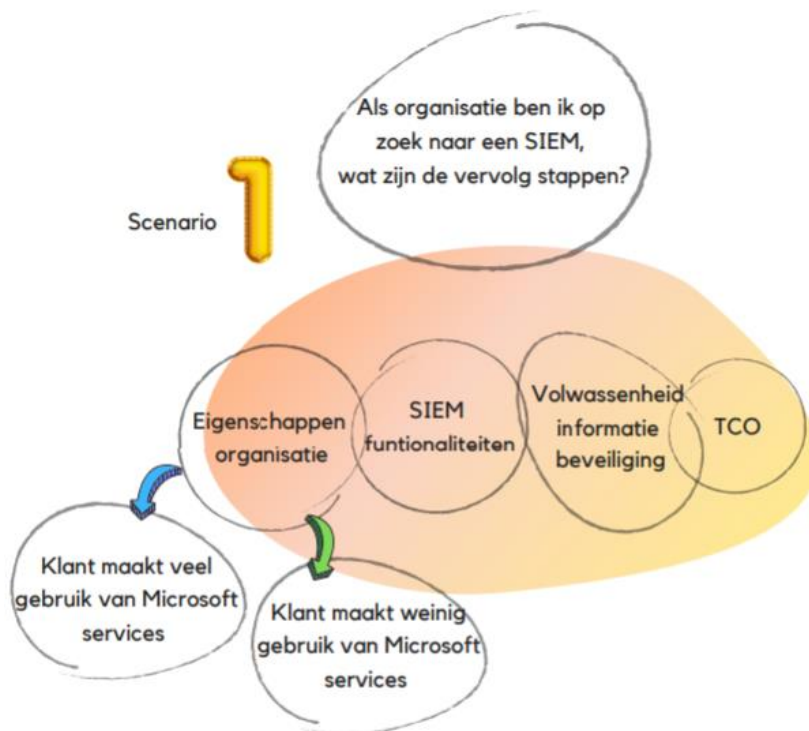
Een erg belangrijk aandachtspunt is het implementeren van Sentinel aangezien dit *gemakkelijker* en *sneller* is, mits de organisatie Microsoft georiënteerd is.

Dat zou voor een organisatie een erg belangrijk punt kunnen zijn voor de besluitvorming m.b.t. een SIEM-oplossing.

Als in het databron onderzoek (hoofdstuk 3) is uitgewezen dat grote volumes CEF & SYSLOG opgenomen zullen worden door de SIEM dan is Splunk waarschijnlijk een goede keus. Tot het begin van 2020 probeerde Greg Peterson met zijn team grote volumes SYSLOG en CEF data Sentinel binnen te krijgen.

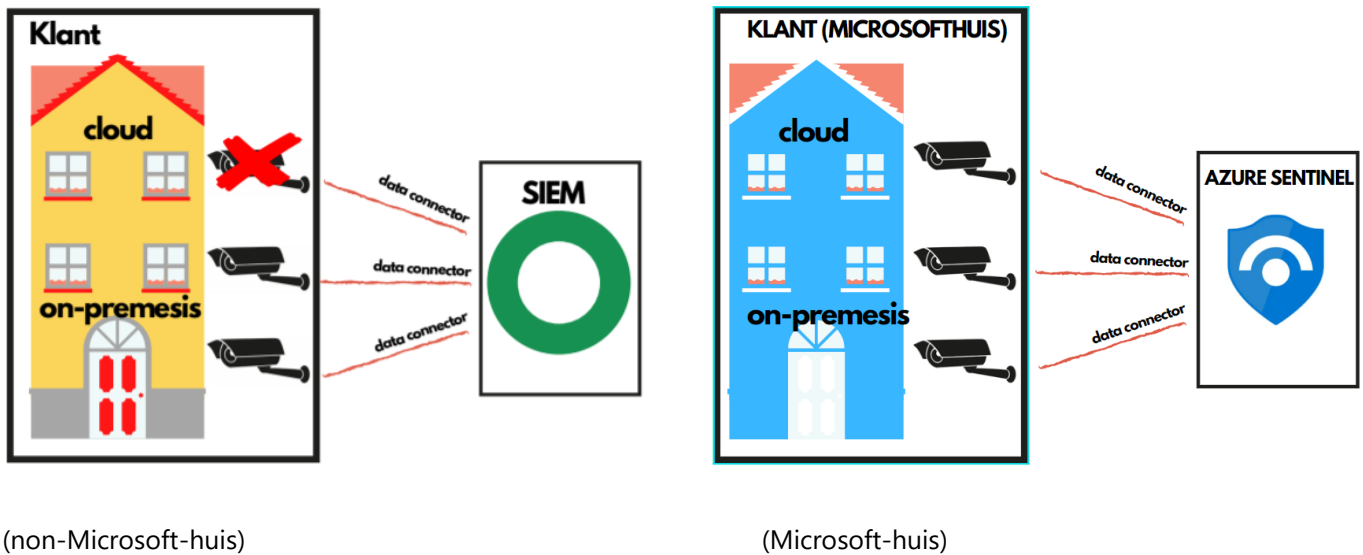
Grote volumes SYSLOG & CEF (common event format) events en dan praten we over 13000 events/second waren tot begin 2020 lastig op te nemen door Azure Sentinel. Hier waren 20 Linux VM's voor nodig met elk een Microsoft management agent die 500 events/second konden verwerken. De agent is verbeterd begin 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 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 geschikt voor.



Een ander focus punt heeft betrekking op de hoeveelheid Microsoftservices die wordt gebruikt binnen de organisatie van de klant. Als de organisatie grotendeels Microsoft georiënteerd is dan het zeker de overweging waard om te kijken naar Sentinel. Databronnen connecteren gaat dan relatief makkelijk en er is een beter overzicht. Dit overzicht zal ik schetsen aan de hand van een analogie geïnspireerd door Rhesa Baar (Security architect Avanade).

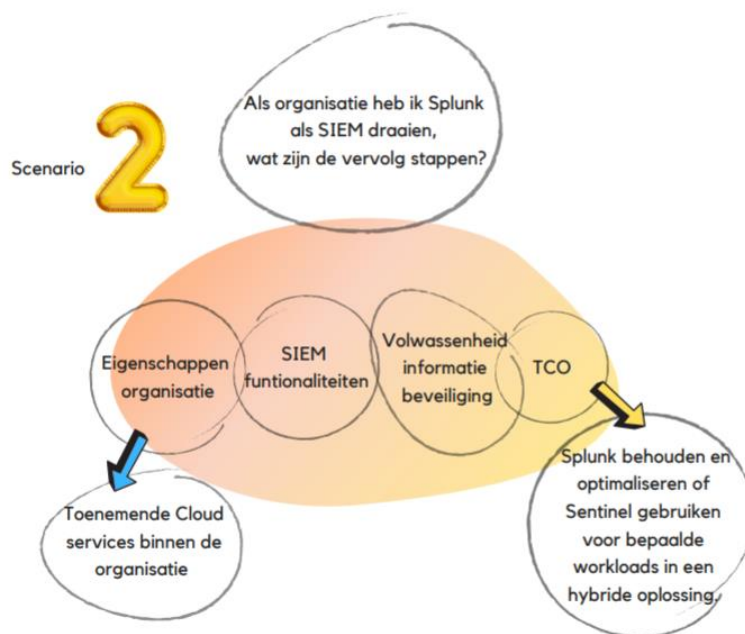
"Beschouw de SIEM als een groepje beveiligingscamera's die een huis met verschillende verdiepingen observeert. Elke verdieping staat voor een bepaalde databronnen die geobserveerd moeten worden. Het is belangrijk alle databronnen en dus alle verdiepingen te observeren om de beveiliging te kunnen garanderen. Als een databron niet in beeld is en daarmee niet wordt gemonitord, dan keldert de beveiliging garantie enorm. Je kan alsnog zo goed beveiligd zijn op de eerste twee verdiepingen, maar als de derde verdieping niet wordt beveiligd dan kan de inbreker alsnog ongezien binnenkomen. Als een organisatie veel verschillende databronnen moet analyseren van diverse landschappen dan kan het zijn dat er een databron wordt vergeten of dat het lastig is de data van de databron in de SIEM te krijgen. Hiermee heeft een Microsoft georiënteerde organisatie een voordeel. Doordat veel databronnen van Microsoft zijn is het makkelijk het overzicht te bewaren, de data te connecteren en te analyseren. Hieronder zien we een figuur van een Microsofthuis die door Azure Sentinel wordt gemonitord en een non-Microsoft huis die wordt eveneens wordt gemonitord door een SIEM. Hiermee geef ik aan dat een huis met een grote diversiteit aan databronnen van verschillende omgevingen moeilijker in kaart te brengen is en daarom moeilijker te analyseren is."



6.2.2 Scenario 3 “Als organisatie heb ik Splunk als SIEM draaien, wat zijn de vervolg stappen?”

De laatste jaren nemen bij veel bedrijven de cloud services toe en dit zal komende jaren blijven stijgen. Als een organisatie bij Avanade aanklopt met een reeds draaiende Splunk dan is het veel te kostbaar om deze volledig te vervangen voor Sentinel. Eveneens zou dit een slecht idee zijn, want qua functionaliteiten zijn de twee SIEM-oplossingen aan elkaar gewaagd. Als de groeiende cloud services vooral uit Microsoft omgevingen komen dan is de mogelijkheid om te kiezen voor hybride oplossing, waarin Splunk side-by-side naast Sentinel draait. Ik stelde Greg Peterson hierover de volgende vraag; “If a company is running Splunk and they use quite a few Microsoft services would a hybrid SIEM be a good solution?”

Greg: Yeah and that's something that we're proposing for Accenture to possibly do as well, where they say it's expensive to put microsoft data in Splunk. So it does make sense for us to monitor some chunk of that data? We put the Microsoft data in Sentinel and then feed just the biggest alerts into Splunk or to sort of do a side by side.



Een hybride oplossing kan volgens Greg waardevol zijn als een deel van workload wordt overgenomen door Sentinel. Deze workload komt voort uit Microsoftservices uit de volgende omgevingen Azure Activity Logs, Office 365 Audit Logs en alerts van Microsoft Threat Protection producten (Azure Security Center, Office365 ATP, Azure ATP, Microsoft Defender ATP, Microsoft Cloud App Security en Azure Information Protection). De reden die Greg hier geeft heeft te maken met kosten. Het zou erg duur zijn data in Splunk te krijgen. Een kleine kanttekening vanuit mijn perspectief; "Als data in Splunk krijgen duurder is en je zou deze data in Sentinel stoppen, dan moet je SOC-team alsnog training volgen en de hybride implementatie zal ook tijd kosten." In het volgende hoofdstuk zal duidelijk worden of het duurder is om bepaalde Microsoft data in Splunk te stoppen in tegenstelling tot Azure Sentinel.

Een aantal voordelen om Azure Sentinel als cloud native SIEM aan je huidige SIEM te koppelen voor een hybride oplossing.

- Eenvoudig binnenhalen van cloud sources
- Oneindig schaalbaar
- Geïntegreerde automatiseringsmogelijkheden
- Patching en updates worden automatisch gedaan

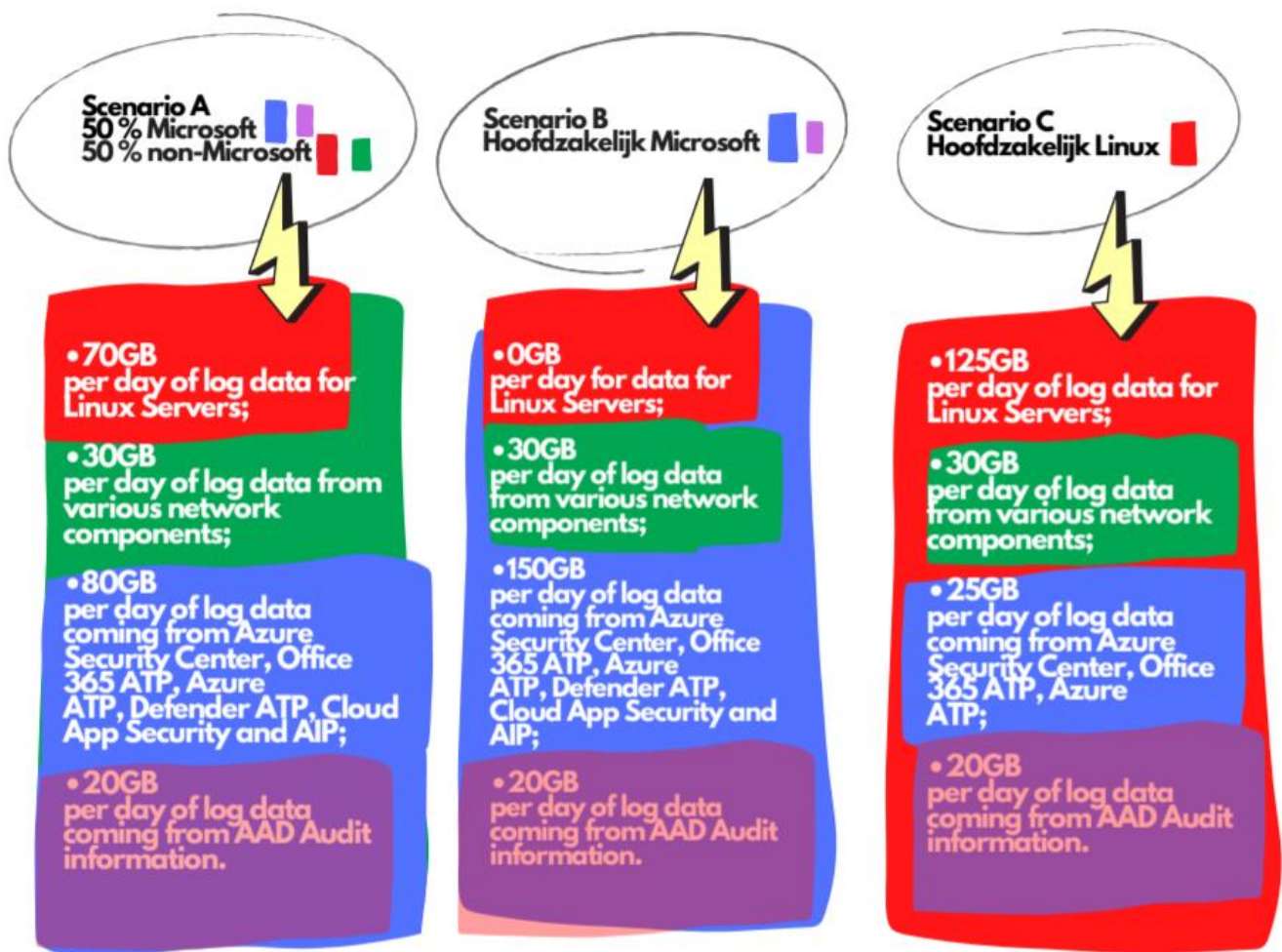
7 Kosten Data Ingestion (gegevensopname)

7.1 Inleiding

Data ingestion is een proces waarbij data wordt verplaatst van een of meerdere bronnen naar een bestemming waar de data kan worden opgeslagen en verder geanalyseerd. De bestemming in dit onderzoek is de SIEM. De data kan verschillende formaten hebben en afkomstig zijn van verschillende bronnen.

7.2 Drie scenario's

Hieronder zijn drie scenario's uitgeschreven voor de gegevensopname van 200GB per/dag. Ik ga onderzoeken wat het verschil is in kost als we de input in de SIEM veranderen op basis van databronnen. Ik onderzoek een scenario waar hoofdzakelijk Microsoft wordt opgenomen door de SIEM, een scenario waar 50% Microsoft en 50% non Microsoft wordt opgenomen en als laatste een scenario waar hoofdzakelijk non-Microsoft binnenkomt.



Prijs Splunk Enterprise link https://www.splunk.com/en_us/products/pricing/calculator.html#tabs/tab1-collapse

Prijs Splunk Cloud link https://www.splunk.com/en_us/products/pricing/calculator.html#tabs/tab2

Prijs Azure Sentinel link <https://azure.microsoft.com/en-us/pricing/calculator/?service=azure-sentinel#azure-sentinel974427f3-131b-4d00-9a6f-a2875965625c>

7.3 Azure Sentinel & Splunk Cloud ingestion prijs

7.3.1 Scenario A (50% Microsoft 50% non-Microsoft)

7.3.1.1 Azure Sentinel

Hieronder één uitgewerkt voorbeeld voor de berekening van de maandprijs. Azure Activity Logs, Office 365 Audit Logs en alerts van Microsoft Threat Protection producten (Azure Security Center, Office365 ATP, Azure ATP, Microsoft Defender ATP, Microsoft Cloud App Security, Azure Information Protection kunnen zonder extra kosten opgenomen worden door Azure Sentinel en Azure Monitor Log Analytics.

Audit informatie van Azure Active Directory (AAD) zijn **niet gratis** en worden gefactureerd voor opname in zowel Azure Sentinel als Azure Monitor Log Analytics.

Parameters	Aantal	Prijs Component	Prijs/Unit	Prijs/Maand
Totaal Sentinel Ingestion volume (GB/dag)	20	N/A	\$ -	\$ -
O365/ASC/ATP/AIP/CAS/.. volume (GB/dag)	8	Inclusief	\$ -	\$ -
Totaalprijs = Sentinel Workspace Storage (GB) +Log Analytics ingestion volume (GB/dag)	12	Azure Sentinel	\$ 166,45	\$ 1,997.45

De aantallen hieronder zijn de gehalveerd, omdat dit scenario 50% Microsoft bedraagt en deze helft wordt gratis opgenomen door Azure Sentinel.

Parameters	Aantal	Prijs Component	Prijs/Unit	Prijs/Maand
Totaalprijs = Sentinel Workspace Storage (GB) +Log Analytics ingestion volume (GB/dag)	12	Azure Sentinel	\$ 166,45	\$ 1,997.45
Totaalprijs = Sentinel Workspace Storage (GB) +Log Analytics ingestion volume (GB/dag)	30	Azure Sentinel	\$ 167,20	\$ 5,016.05
Totaalprijs = Sentinel Workspace Storage (GB) +Log Analytics ingestion volume (GB/dag)	60	Azure Sentinel	\$ 154,46	\$ 9,268.05
Totaalprijs = Sentinel Workspace Storage (GB) +Log Analytics ingestion volume (GB/dag)	120	Azure Sentinel	\$ 123,53	\$ 14,824.25
Totaalprijs = Sentinel Workspace Storage (GB) +Log Analytics ingestion volume (GB/dag)	190	Azure Sentinel	\$ 111,90	\$ 21,261.60

7.3.1.2 Splunk

Parameters	Aantal	Prijs Component	Prijs/Unit	Prijs/Maand
Totaal Splunk Ingestion volume (GB/dag)	20	Splunk Cloud	\$ 138	\$ 2760
Totaal Splunk Ingestion volume (GB/dag)	50	Splunk Cloud	\$ 95,88	\$ 4.791,66
Totaal Splunk Ingestion volume (GB/dag)	100	Splunk Cloud	\$ 76,66	\$ 7.666,66
Totaal Splunk Ingestion volume (GB/dag)	200	Splunk Cloud	\$ 76,66	\$ 15.333,33
Totaal Splunk Ingestion volume (GB/dag)	300	Splunk Cloud	\$ 76,66	\$ 23.000,00

7.3.2 Scenario B (Hoofdzakelijk Microsoft)

7.3.2.1 Azure Sentinel

Parameters	Aantal	Prijs Component	Prijs/Unit	Prijs/Maand
Totaalprijs = Sentinel Workspace Storage (GB) + Log Analytics ingestion volume (GB/dag)	5	Azure Sentinel	\$ 164,71	\$ 823,55
Totaalprijs = Sentinel Workspace Storage (GB) + Log Analytics ingestion volume (GB/dag)	12,5	Azure Sentinel	\$ 166,50	\$ 2.081.30
Totaalprijs = Sentinel Workspace Storage (GB) + Log Analytics ingestion volume (GB/dag)	25	Azure Sentinel	\$ 167,10	\$ 4.177.55
Totaalprijs = Sentinel Workspace Storage (GB) + Log Analytics ingestion volume (GB/dag)	50	Azure Sentinel	\$ 167,40	\$ 8.370.05
Totaalprijs = Sentinel Workspace Storage (GB) + Log Analytics ingestion volume (GB/dag)	75	Azure Sentinel	\$ 167,36	\$ 10.612.55

7.3.2.2 Splunk Cloud

Parameters	Aantal	Prijs Component	Prijs/Unit	Prijs/Maand
Totaal Splunk Ingestion volume (GB/dag)	20	Splunk Cloud	\$ 138	\$ 2760
Totaal Splunk Ingestion volume (GB/dag)	50	Splunk Cloud	\$ 95,88	\$ 4.791,66
Totaal Splunk Ingestion volume (GB/dag)	100	Splunk Cloud	\$ 76,66	\$ 7.666,66

Totaal Splunk Ingestion volume (GB/dag)	200	Splunk Cloud	\$ 76,66	\$ 15.333,33
Totaal Splunk Ingestion volume (GB/dag)	300	Splunk Cloud	\$ 76,66	\$ 23.000,00

7.3.3 Scenario C (Hoofdzakelijk non-Microsoft)

7.3.3.1 Azure Sentinel

Parameters	Aantal	Prijs Component	Prijs/Unit	Prijs/Maand
Totaalprijs = Sentinel Workspace Storage (GB) + Log Analytics ingestion volume (GB/dag)	17,5	Azure Sentinel	\$ 166,84	\$ 2919,80
Totaalprijs = Sentinel Workspace Storage (GB) + Log Analytics ingestion volume (GB/dag)	43,75	Azure Sentinel	\$ 167,15	\$ 7,321.93
Totaalprijs = Sentinel Workspace Storage (GB) + Log Analytics ingestion volume (GB/dag)	87,5	Azure Sentinel	\$ 131,25	\$ 11,485.20
Totaalprijs = Sentinel Workspace Storage (GB) + Log Analytics ingestion volume (GB/dag)	175	Azure Sentinel	\$ 121,49	\$ 21,261.60
Totaalprijs = Sentinel Workspace Storage (GB) + Log Analytics ingestion volume (GB/dag)	262,5	Azure Sentinel	\$ 114,18	\$ 29,972.90

7.3.3.2 Splunk Cloud

Parameters	Aantal	Prijs Component	Prijs/Unit	Prijs/Maand
Totaal Splunk Ingestion volume (GB/dag)	20	Splunk Cloud	\$ 138	\$ 2760
Totaal Splunk Ingestion volume (GB/dag)	50	Splunk Cloud	\$ 95,88	\$ 4.791,66
Totaal Splunk Ingestion volume (GB/dag)	100	Splunk Cloud	\$ 76,66	\$ 7,666,66
Totaal Splunk Ingestion volume (GB/dag)	200	Splunk Cloud	\$ 76,66	\$ 15.333,33
Totaal Splunk Ingestion volume (GB/dag)	300	Splunk Cloud	\$ 76,66	\$ 23.000,00

7.3.4 Alle prijzen samengevoegd in één tabel

Azure Sentinel	20 GB/dag	50 GB/dag	100 GB/dag	200 GB/dag	300 GB/dag
Scenario A	\$1,997.45(12)	\$5,016.05 (30)	\$9,268.05 (60)	\$14,824.25 (120)	\$21,261.60(190)
Scenario B	\$823,55(5)	\$2,081.30 (12,5)	\$4,177.55(25)	\$8,370.05 (50)	\$10,612.55(75)
Scenario C	\$2919,80(17,5)	\$7,321.93(43.75)	\$11,485.20(87.5)	\$21,261.60 (175)	\$29,972.90(262,5)

Achter de bedragen staan de GB te niet gratis zijn voor Azure Sentinel en dus moeten worden betaald per maand.

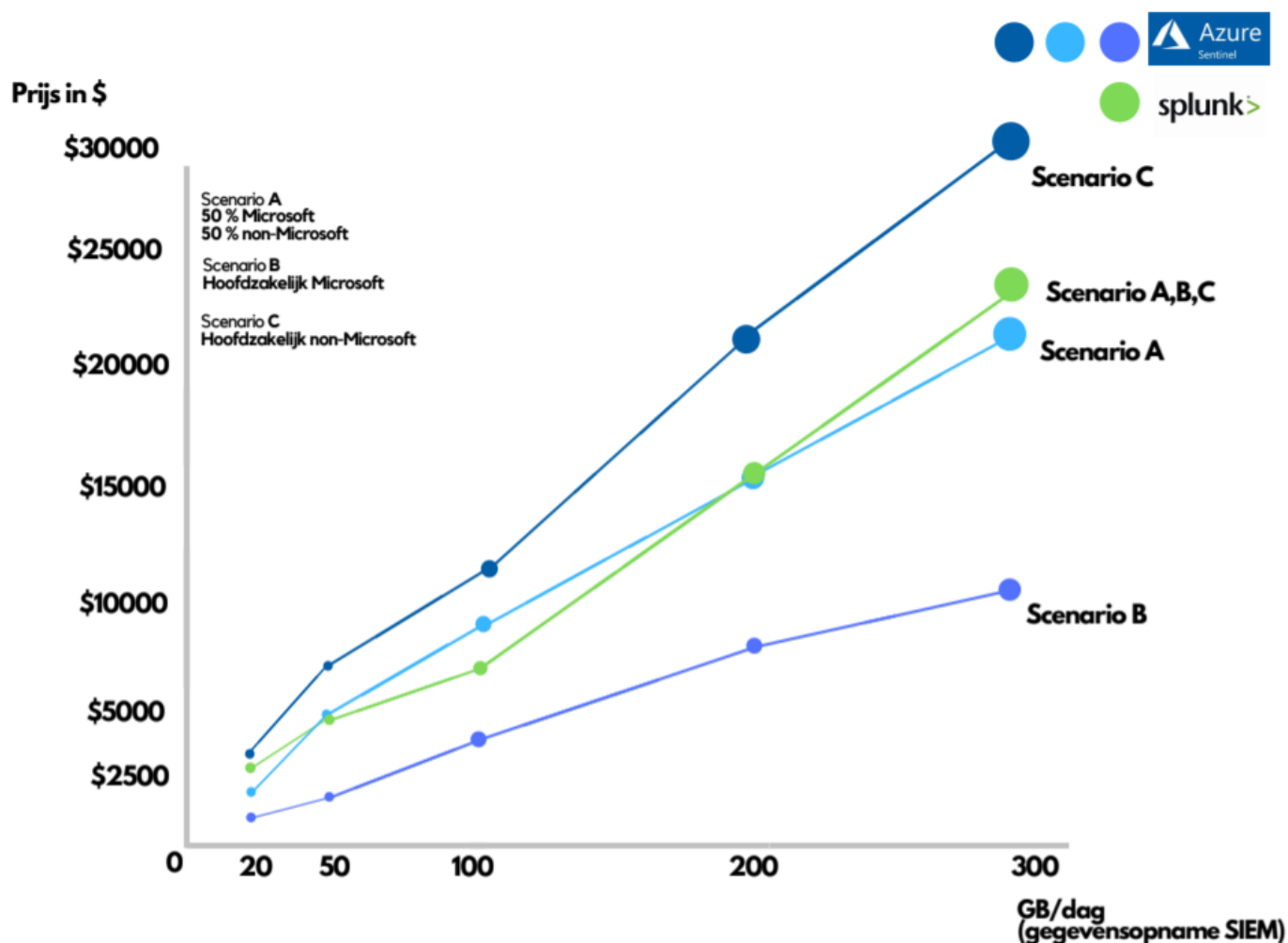
<https://azure.microsoft.com/en-us/pricing/calculator/?service=monitor>

Splunk Cloud	20 GB/dag	50 GB/dag	100 GB/dag	200 GB/dag	300 GB/dag
	\$2760	\$4.791,66	\$7,666,66	\$15,333,33	\$23.000

https://www.splunk.com/en_us/products/pricing/calculator.html#tabs/tab2

7.3.5 Kost/maand in dollar van de verschillende scenario's in één diagram

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.



7.3.6 Bevindingen

Wat als eerst opvalt is dat een paar prijzen enorm uit elkaar lopen, ook al stoppen we dezelfde hoeveelheid GB in de SIEM. Hoe kan dit verschil zijn ontstaan? Splunk is in deze analyse een stabiele factor. Bij de drie scenario's die we hier uittesten, waarin data van verschillende databronnen door Splunk wordt opgenomen zien we geen verschil in de kost. Wel wordt het duurder naarmate we meer GB's reserveren voor de opname in de SIEM, maar niet als we data uit verschillende databronnen in Splunk stoppen.

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 beide bedrijven, maar dat geldt 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)	Vershil
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. In de tabel hieronder dan kan dat in grote mate van non-Microsoft data flink oplopen in kosten. Bij volumes lagen dan 200GB zien we dat het grote prijsverschil afneemt.

Prijs Azure Sentinel (scenario C)	Prijs Splunk (scenario C)	Vershil
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 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.

8 Conclusie

Om dit onderzoek af te ronden, zal er antwoord gegeven moeten worden op de hoofdvraag; **“Hoe maakt de consultant van Avanade het proces voor het kiezen van een SIEM inzichtelijk voor de klant?”**. De handleiding die ik heb geschreven genaamd “Hulp bij het kiezen van een SIEM” vormt de basis van het antwoord op deze vraag. De handleiding is een product die de consultant van Avanade mee kan nemen naar de klant, digitaal of uitgeprint. De consultant gaat samen om de tafel zitten met de klant en gebruikt de interactieve handleiding om verschillende vragen te beantwoorden en inzicht te krijgen in de organisatie. Door de handleiding compleet door te werken krijgt de klant inzicht in het keuzeproces omtrent de SIEM. Door dit transparante proces kan de consultant goed uitleggen wat de mogelijkheden zijn en kan de klant duidelijk maken waar de wensen liggen. Het document is als volgt opgebouwd. Als eerste wordt de workflow getoond van de handleiding, die een goed beeld geeft wat er allemaal in de handleiding te vinden is. Vervolgens een introductie wat betreft de databronnen. Het is de taak van de consultant om samen de klant inzicht te krijgen in alle databronnen, zowel de on-premise als de cloud databronnen. Vervolgens moet er beoordeeld worden of de organisatie instaat is een eigen SOC te hebben en te behouden. Door middel van een invuldocument dat gemaakt is door Carson Zimmerman krijgen we risicoscore uit het invuldocument. Deze score vormt een goede indicatie die antwoord geeft op de vraag of de klant een eigen SOC moet bouwen of dat de organisatie de SOC beter kan uitbesteden aan een derde partij in dit geval een MSSP (Managed Security Service Provider). De volgende onderdelen zijn informatief en beginnen bij de voor- en nadelen van Splunk en Sentinel gebaseerd op antwoorden van Greg Peterson (sr Director Security – Avanade, Seattle (USA)). Dan krijgen we een hoofdstuk over implementatie scenario's en vervolgens een kostentabel. Deze kostentabel toont de kosten per maand in \$ van drie scenario's waarbij verschillende hoeveelheden GB/dag worden opgenomen door de SIEM. Als laatste zal het 'advies op maat' gedeelte de ruimte bieden om verschillende bevindingen en getallen van de organisatie in te voeren. Doordat de consultant en de klant samen de organisatie inzichtelijk maken door middel van de handleiding zal het keuzeproces voor het kiezen van een SIEM worden blootgelegd. Dit inzicht is een win win voor beide partijen.

9 Bronnen

Cynthia Gonzalez (What is SIEM? Security Information & Event Management Explained) Opgehaald van <https://www.youtube.com/watch?v=GbFtSDnPZBQ>

Helge Klein (Whats is Splunk and How Does it Work?) Opgehaald van <https://helgeklein.com/blog/2014/09/splunk-work/>

Ian Helle (Azure Sentinel Resource Terminus – board here!) Opgehaald van <https://techcommunity.microsoft.com/t5/azure-sentinel/azure-sentinel-resource-terminus-board-here/ba-p/1269252>

Jeff Petters (What is UEBA? Complete Guide to User and Entity Behavior Analytics) Opgehaald van <https://www.varonis.com/blog/user-entity-behavior-analytics-ueba/>

Docs.microsoft (Zelf studie: schaduw vinden en beheren in uw netwerk) Opgehaald van <https://docs.microsoft.com/nl-nl/cloud-app-security/tutorial-shadow-it>

Logan Daley (Make your SIEM SOARlike an eagle with Microsoft Sentinel) Opgehaald van <https://medium.com/@digitallyvicarious/make-your-siem-soar-like-an-eagle-with-microsoft-sentinel-da0efce56cbf>

Carson Zimmerman ("*Ten Strategies of a World-Class Cybersecurity Operations Center*") Opgehaald van <https://www.mitre.org/sites/default/files/publications/pr-13-1028-mitre-10-strategies-cyber-ops-center.pdf>

Kwaliteitsinstituut Nederlandse gemeenten in opdracht van vereniging van Nederlandse gemeente (Security Information & Event Management (SIEM) en Security Operations Center (SOC) binnen uw gemeente) opgehaald van <https://www.informatiebeveiligingsdienst.nl/wp-content/uploads/2017/04/201704-Factsheet-SIEM-SOC-v1.00.pdf>

AGconnect (SIEM waakt over uw netwerk) opgehaald van <https://www.agconnect.nl/artikel/siem-waakt-over-uw-netwerk>

10 Bijlage

Hoogtepunten interview Greg Peterson (Sr Director – IT Security Avanade)

Over de producten Splunk en Azure Sentinel en de migratie van Splunk Enterprise naar Azure Sentinel bij Avanade (Seattle, USA)

10.1 Highlights - Interview Greg Peterson (Sr Director – IT Security Avanade) 23-04-2020

00:00:39 Henk-Sjoerd: Can you tell me a little bit about yourself and what your role is at Avanade.

00:01:01 Greg: Yeah, absolutely. So, uh, Greg Peterson, I run our security technology and ops team for Avanade. I report to our CSO and CIO Bob Bruns, and I've been with Avanade since forever now. So, since, January 2001 in a number of different roles. So, and then for the last several years I have been running, you know, again, internal security, technology and ops team. So, anything that we do from a Security operations perspective like building and managing our SIEM and supporting tools, the security operations team in conjunction with Accenture. So, we leverage a managed security service from Accenture for sort of Level 1 Level 2 monitoring.

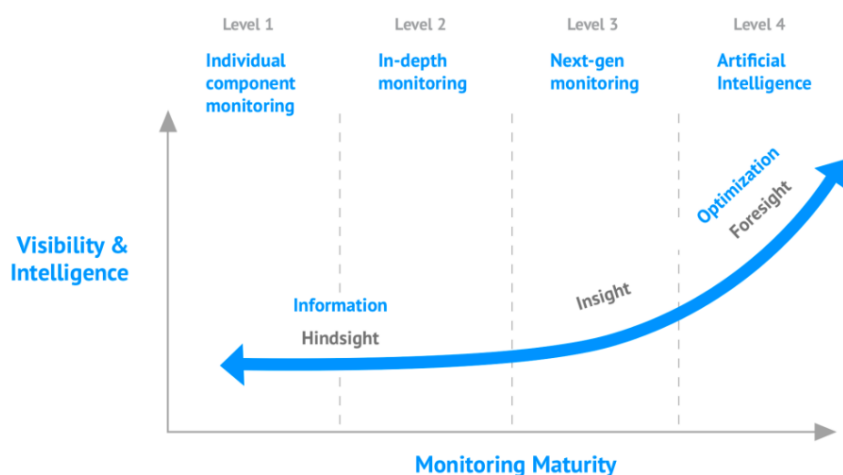


Figure 1 Levels in monitoring

00:06:03 Henk-Sjoerd: I am trying to get more insight in the process of choosing a SIEM solution. That is the main question in my research, and I am looking for answers that point to whether it is better for the company to choose for Splunk or Azure Sentinel. I prepared some questions and I will just start with the first one. When did you do the migration of Splunk to Sentinel for Avanade?

00:06:49 Greg: So, I think we started working with her to understand Sentinel about a year ago. We had some pain around collecting our non-Microsoft events and logs. So in a SIEM there's a very fairly common format for syslogs called syslog and then a more specific format or type of just log messages called CEF (common event format). So, getting all of that syslog and CEF messages into Sentinel early on, was fairly difficult, at least at the volume that we had. For example, our Palo Alto firewalls and the logging turned up fairly high to the point where we're seeing, you know, across our environment over 10000 events per second. And I think there's something closer to like 12000 or 13000. So not way over, but over.

And the Microsoft management agent, which is essentially the tool or part of the tool chain that reads logs from various formats on the machine. So it could be just Windows event logs or in this case syslog and sends it to Sentinel. That tool until late last year was unable to keep up with the log volume that we have.

I think it was something closer to 500 events per second. And it would start creating problems. So we had to have 20 something Linux boxes running Microsoft management agent and listening on syslog in order to catch all those logs

and send them the Sentinel, which wasn't very stable nor very useful. What Microsoft did recently, towards the end of the year was improve that agent to nail and to process about 10000 logs or events per second.

And so now it's I think we have three or four machines just for you to know, we don't want to be running them at maximum to be able to handle the load across the twelvish thousand events per second that we have coming out of those boxes.

Conclusie: Grote volumes syslog & CEF (common event format) events, tot 13000 events/second was sinds kort moeilijk op te nemen door Azure Sentinel. Hier waren 20 Linux VM's voor nodig met elk een Microsoft management agent die 500 events/second konden verwerken. Begin 2020 heeft Microsoft deze agent verbeterd en kan één Linux VM 10000 events verwerken. Avanade heeft ervoor gekozen 4 VM's te draaien om de load te verdelen. Kortom er is verbetering, maar grote volumes SYSLOG en CEF-data in Azure Sentinel krijgen is niet eenvoudig.

00:09:27 Henk-Sjoerd: Can you say that Splunk had less issues with handling syslog and CEF logs?

00:09:42 Greg: Yeah. So Splunk. That was sort of their bread and butter. Right. They've started with an everything that you feed into Splunk. For the most part ends up being a system hugger off messages that then gets sort of consumed and indexed and Splunk, whereas Microsoft has at least for their cloud native services or capabilities, connectors that you just flip a switch. And now all of a sudden you're collecting office activity logs. Right. It's just a switch. Whereas if you're going to ingest that into Splunk, you'd have to subscribe to the API or have some box. But Splunk from a syslog perspective natively handles logs easier and at scale easier. Mm hmm. But again, Microsoft's catching up.

Conclusie: Vanuit nature verwerkt Splunk syslog & CEF logs gemakkelijker dan Azure Sentinel.

00:11:57 Henk-Sjoerd: Can you maybe take me a bit on the journey of the migration from Splunk to Sentinel you did at Avanade, maybe share a bit of your experiences?

00:12:08 Greg: Sure. So, a super high level as we're looking at how to how to migrate or I guess whether we should migrate. Was it to get our decision to move may be influenced by different factors than some other customers or clients, because again, one of our primary motivators is to help showcase new Microsoft tools, whereas other companies might not have that.

00:12:37 Henk-Sjoerd: The primary motivator where you talk about, was the main business driver to migrate?

00:12:43 Greg Exactly. Getting there first and early was important for us and is probably less important to other customers.

Conclusie: De grote business driver van Avanade is om Microsoftproducten te tonen aan het grote publiek. Dit is ook de reden waarom juist Avanade als eerst een grote Azure Sentinel migratie wou doen, mede door het feit dat dit Avanade zou helpen in het vergaren van kennis omtrent Azure Sentinel. Deze kennis zou potentiële klanten weer kunnen helpen bij hun Azure Sentinel migratie.

00:12:43 Greg: We also had a minimum bar of can we at least do the things that we were doing in Splunk? Not that we were doing everything you could do with Splunk, but could we at least get to the same of what we were doing in Splunk or better or close enough. And that's across a few different areas. So one was log ingestion and retention. So we talked a lot about log ingestion. And we got to a point again, that was our longest pole or critical path item. Can we actually get those logs in a sustainable fashion? The other bit would be. Can we do similar sets of correlation rules or use cases? So once you get all the data into this and can you actually alert and respond to it? It with similar use cases and we probably had thirty or thirty five different use cases in Splunk. Custom rules, looking for various different

things and providing alerts based on what we saw, which I would call just because I, my own worst critic would call it immature. But nevertheless it was what we were doing. We were able to transition many of those use cases over to Sentinel or translate them. So from using, you know, Splunk query language to Kusto query language within Sentinel. Then there's also a bit of cross training. You know, everyone has to go learn that new language and learn the new method to do hunting or searching or querying all the new gnome and culture, all that stuff. So that was a big piece. Ah, L1 L2 team is again, it's a managed service with Accenture and they are technology specific. So what they provide for us again is that 24/7 coverage. So you've got. Was it 16, 18 people that work shifts around the clock so we can have eyes on glass on the consoles? And our team was all trained in Splunk and they're intended to be trained in Splunk. So when we started talking about moving to a Microsoft solution, we actually switched teams within Accenture. So they had another team that while Sentinel is still relatively new and they didn't have much experience. Accenture did have a solution for security monitoring built on top of log analytics. And it's ultimately the same substrate, right? It's the same tools underneath. So that team is within it sensors or it evolved into the Sentinel managed security services team. And so we had a transition period for them where again, we cross-trained, we got them up to speed on our use cases. We also threw in some additional sort of fresh look at how we do security incident response and monitoring. So it's not just a migration to Sentinel. We also heavily leverage MTP. So Microsoft Threat Protection, which provides actually lots of SIEM like features in advanced hunting features using the same languages, but potentially against different sets of data that's correlated together. So over time we're working with Microsoft to let them or help them make all of those data sources more easily consumable in Sentinel. But there are a few, for example, today that aren't fully there right now. So. One example is Defender ATP sends all the alerts and we can get those alerts in Sentinel in an MTP. But what we don't get is incidents. So an incident being some correlation was done across to help group a bunch of alerts into a single incident. And there's a few different ways that you can think about that or go about that. And MTP does it one way. Sentinel does it another way. And while we have a API to get into and interact with sentinel incidents, we don't have any API is to interact with MTP incidents. We can get the alert data, but we can't get the incident data out of an API yet.

Conclusie: Er komen hier een paar interessante migratie verhalen naar boven. Een kritieke vraag van Greg bij de migratie was; "Kunnen we log ingestion and retention, oftewel opname en behoud van logs goed uitvoeren en belangrijker nog omzetten naar een duurzame gebruiksvorm?", "Kunnen we de use cases die we in Splunk gebruikten overzetten naar Sentinel?"

Het team dat voor Avanade werkte aan Splunk, was getraind in Splunk en werkte hier graag mee. Op het moment dat Avanade aankondigde dat ze de overgang zouden maken naar de Microsoft oplossing zou er heel wat cross training gedaan moeten worden om de nieuwe query taal Kusto te leren. Dit is de taal die wordt gebruikt in Sentinel. De oplossing hiervoor was een team ruil met Accenture. Accenture had een team dat werkte met security monitoring dat gebouwd was boven op Log Analytics, dezelfde onderliggende tool wordt ook gebruikt bij Sentinel. Hier blijkt uit dat een migratie veel meer is dan alleen de vervanging van software.

Microsoft moet het mogelijk maken dat data sources makkelijker bruikbaar zijn, maar hier is ook nog wel wat te winnen. Bijvoorbeeld bij Defender ATP

00:19:31 Henk-Sjoerd: Did you did you migrate everything at once or was Splunk still running on this side?

00:19:39 Greg: So, we had Splunk in Sentinel running side-by-side for some time. And then once we migrated or flipped the switch to start monitoring primarily in Sentinel. We essentially were able to start turning down our our Splunk instance to be more historical. Right. So we have a policy that says we need to keep logs for six months, 180 days and just given the sheer volume of content. We ran both side by side. We shrank our Splunk deployment such that we because we were actively using it for queries or monitoring that we didn't need all the same compute power or even

all the same redundancy. And so we were able to shrink that quite considerably and keep it around simply for retention. And then we've gotten to the point last month where we know the likelihood of us needing to go back and query for things from December or before is so low that it's not worth us keeping that environment viable. So we're keeping logs or keep we've got the system, some of it still up and running. But our Splunk licenses lapsed.

Conclusie: Splunk heeft nog voor een jaar side by side gedraaid met Azure Sentinel. Dit zegt ons dat een migratie een erg lang proces is. Er moesten nog verschillende query's gedaan worden tot voorkort op de Splunk instance. Sinds December was niet minimaal geworden en is het abonnement afgebroken.

00:22:03 Henk-Sjoerd: Did you faced any limitations with getting the data in Sentinel?

00:22:19 Greg: I think large log volumes syslog stuff, so just if you're thinking about producing some guidance on how to choose Sentinel versus something else, that would be something to look at the other, I guess perspective would be yes. Most of the logs from Microsoft systems were able to turn on and turn on more easily. But as they make better logs or have different systems, we can't get all of them yet. Right. So we're a little bit dependent on Microsoft to do it. But once they do it, it'll be easy for us just to flip in. One of the examples is like the Office 365 advanced threat protection logs. Right. So essentially doing email security, there's a ton of data and telemetry that exists in office 365. And while we can get some of that information into Sentinel, some of it is and some of it has been plumbed to MTP. Not all of it is one to one. And so we just kind of have to look at each one of your log sources and say. Does this work? Does this work now? And I think there are even some that we had problems with which have already since been addressed. So while I could get into more specifics, I would probably say go look at each one of your log sources and understand what it is and understand where the current state of Microsoft is.

Conclusie: Quote van Greg; "I would probably say go look at each one of your log sources and understand what it is and understand where the current state of Microsoft is". Dit houdt in dat als een organisatie overweegt om Azure Sentinel in huis te nemen ze deze tactiek kunnen toepassen.

1. Bekijk je databronnen
2. Begrijp wat deze doen
3. Bekijk hoever Microsoft staat met ontwikkeling van deze specifieke databron

00:27:03 Henk-Sjoerd: Which is your favorite, Splunk or Sentinel and why?

00:27:24 Greg: Yeah, I think for us Sentinel is our way forward. So if we think about the care and feeding and management overhead because we were in this, this may be different with Splunk Cloud. We know it probably is somewhat different response cloud, but we weren't using that. But as compared to our on premise SIEM, we don't have to worry about the care and feeding patch management upgrades, any of that stuff. And we are. And I'm talking. 20 to 30 VMs. To manage across multiple sites. And being able to manage the storage and all the backhands, like all of that stuff that we have to do with Splunk. We don't have to do it all with Sentinel. That's just part of the service that we buy with Sentinel. So that's huge, though.

The other one would be we get all those benefits of new upgrades or updates or improvements to the product without trying. Right. So Microsoft's constant it's the software as a service versus, you know, roll your own infrastructure. It's just better. Is the product as mature? No. So being able to do like the language is good, but there's still some limitations around how we do searches or how we get data into the platform. That, you know, with Splunk. They've lived with this problem much longer and they're their solutions a bit more elegant.

Conclusie: Een SIEM heeft natuurlijk verzorging nodig in de vorm van upgraden en patching. Bij Avanade gaat dat om 20 tot 30 VM's verspreid over verschillende locaties. Dit vergt ook tijd m.b.t. het beheer van de storage. Dit bij elkaar kost gewoon veel tijd en geld. Bij Splunk Enterprise werd dit dus uitgevoerd door medewerkers van Avanade, maar

door de overstap naar Azure Sentinel is dit niet meer nodig aangezien Azure Sentinel een cloud native SIEM is en patching, upgraden automatisch wordt uitgevoerd. Dat is een groot verschil. Wat ook nog een groot voordeel is dat nieuwe updates of verbeteringen door Microsoft worden toegevoegd aan Azure Sentinel. Het is het SaaS versus beheer je eigen infrastructuur verhaal.

Is Sentinel volwassen? Nee, er zijn limieten op het gebied van zoeken en data in het platform krijgen, Splunk heeft hier een streepje voor.

00:36:03 Henk-Sjoerd: So you were talking about this paper what Accenture put together to compare Splunk with Azure Sentinel. Can you tell me a little but about it?

00:36:23 Greg: Let's see the overall tone of the paper from Accenture. And again, they've got a slightly different perspective than we have.

00:36:51 Greg They wouldn't recommend Sentinel over Splunk for mature clients. OK. Right. And I might even agree with that in some circumstances for some period of time. Right. So if you have a super, highly mature Splunk implementation at a client or a very mature SIEM, that is not Splunk or Sentinel, but you're choosing between Splunk or Sentinel. Splunk might be the right answer for you right now because it's able to do you know, it's just more mature across the board.

Conclusie: Accenture zou bij een grote SIEM implementatie kiezen voor Splunk. Splunk is gewoonweg over de hele line volwassener, Greg is het hier ook mee eens.

00:37:29 Greg: If you're a company that's relatively new to a scene, you know, I would probably go all in with Sentinel and by the time you're mature enough to leverage, the more advanced features. So while the product would probably be one and again, it's just not a secret, right? Sentinel is new. Yeah, I would say it would be faster and easier to implement if you were largely a Microsoft shop.

Conclusie: Voor een organisatie die nog niet volwassen is lijkt Azure Sentinel in eerste instantie interessanter, tegen de tijd dat de klant volwassen is geworden zou Azure Sentinel dat ook moeten zijn. Daarnaast is het makkelijker en sneller om Azure Sentinel te implementeren, mits deze organisatie Microsoft georiënteerd is.

00:38:52 Greg: Yeah, we already talked about it. Data collection from hosts, data masking, so that was an area. It sounded like Splunk has a few different options to. Find and mask or change data for things like PCI or GDPR. I'd like to go find data that you've already collected. Change it or tweak it is a little bit more. That's much more mature in the Splunk world.

Conclusie: Op het gebied van data zoeken, maskeren en wijzigen om PCI of GDPR redenen zou Splunk veel volwassener zijn dan Sentinel. Het gaat hier om data die al eerder is verzameld door de SIEM.

00:39:39 Greg: Oh, alerting or ticketing, ticket tracking. So just from a SIEM workflow perspective, you go for Splunk. More mature in that area as well. What we do internally is leverage Sentinel and service now. So we have our team that will create service now tickets or incidents based on stuff that they see in the empty console versus the sentinel console.

Conclusie: Vanuit een SIEM workflow perspectief is alerting, ticketing of ticket tracking beter ontwikkeld in Splunk.

00:40:03 Henk-Sjoerd: If a company is running Splunk and they are use quite a few Microsoft services would a hybrid SIEM be a good solution?

00:40:54 Greg: Yeah. And that's something that we're proposing for Accenture to possibly do as well, where they say it's expensive to put data in Splunk. So does it make sense for us to monitor some chunk of that data? Right. The Microsoft data in Sentinel and then feed just the biggest alerts into Splunk or to sort of do a side by side. I think there was even a blog article on that from Microsoft that came out not too long ago and sort of a better together story.

Conclusie: Een hybride oplossing tussen Splunk en Azure Sentinel kan waardevol zijn als een gedeelte van de logs uit Microsoftservices komt. Het is namelijk erg duur om de data in Splunk te krijgen, dan zou het alternatief zijn dan de Microsoftdata wordt geanalyseerd door Azure Sentinel en dat de grote alerts door worden gegeven naar Splunk.
'Greg is continuing the Accenture file.'

00:43:22 Greg: So, you know, the problem space is changing rapidly. Where do you put all your data and how do you consolidate it and assign role based user access control to it. So in Splunk, there's the concept of. Shoot, I've now forgotten the term, but different indexes or workspaces where you store different data about different things and then you can easily search across those indexes. If you have the rights per index, right. What we did is, you know, our internal I.T. team had a set of indexes for like network here, for example, and then we had some other devices that was non network. You're going to like the Windows Server Logs Index. And then there's the DC's group had some DC's indexes and we could even set up Splunk to say the DC people can see the DC's ones, the network people can see the network ones, the server people can see the server ones and the security people can see all of them.

Conclusie: Splunk kan rechten geven aan groepen om bepaalde indexen met data te bekijken. Ik zie het zelf als een soort Active Directory waarin je personeel in Global Groups zit en via een soort Domain Local group recht krijgt op een index. Hieronder staat uitgelegd wat het verschil is met Sentinel.

00:49:22 Greg: That is not as easy to do in Sentinel. In the beginning, like they don't, it's changing, but they don't fully understand that model. So they have lighthouse, which is sort of an event bus that you can look at using to do searches and queries across the workspaces. But for our implementation, we essentially landed on all the data for Sentinel goes into one workspace, which in Splunk claims to be kind of like one index, right, for us to be able to find and search across the stuff. But that's a new one. They are changing or implementing additional ways to do like role based access control on queries or on fields within log analytics as monitor log analytics. But that's still new and we haven't fully explored yet.

Conclusie: In Sentinel kan men via Azure Lighthouse queries en zoekopdrachten doen op de workspace, dit is een nieuwe manier en daarom nog niet erg stabiel. Daarnaast is er nog een manier om via log analytics role based access te doen, maar daar heeft Greg en zijn team nog niet echt veel mee gewerkt. Laat ik concluderen dat role based access nog niet erg volwassen is in vergelijking met Splunk.

