

NORTHWAVE
Intelligent Security Operations

Afstudeerverslag

Auteur: Jasmine Fan, 458285
E-mail: 458285@student.saxion.nl | jasmine.fan@northwave.nl
Bedrijfsbegeleider: Julik Keijer
Afstudeerdocent: Arno Kromdijk

Versie: 1.0
Datum: 21 januari 2023

NORTHWAVE
Intelligent Security Operations

Managementsamenvatting

Northwave maakt momenteel gebruik van drie verschillende SIEM's, waarvan twee momenteel worden uitgefaseerd. Hierdoor houdt Northwave enkel Azure Sentinel als SIEM over. Om te voorkomen dat Northwave volledig afhankelijk is van Microsoft en om de kans op vendor lock-in te beperken, is de afstudeeropdracht ontstaan om onderzoek te doen naar welke SIEM voor Northwave het beste alternatief is voor Azure Sentinel met in achtneming van de requirements. Om deze hoofdvraag te beantwoorden is gebruik gemaakt van deelvragen, diverse analyses en onderzoeken.

Als eerste is een stakeholderanalyse uitgevoerd om de meest relevante en belangrijkste stakeholders voor de opdracht in kaart te brengen. Vervolgens zijn de behoeftes van deze stakeholders boven water gehaald met behulp van een behoefteanalyse. Deze behoeftes dienen als input voor de multicriteria-analyse, waarbij er op een zo objectief mogelijke manier een keuze tussen de verschillende SIEM's wordt gemaakt. Tevens is een literatuuronderzoek gedaan om meer kennis omtrent de afstudeeropdracht te vergaren en om antwoord te geven op de eerste deelvraag. Het literatuuronderzoek is in hoofdstuk 4 van het analyseverslag te vinden. Hierna is een impactanalyse uitgevoerd om de impact van een extra SIEM op de bestaande omgeving, op het gebied van zowel processen als techniek te onderzoeken. Deze impactanalyse is te lezen in hoofdstuk 2 van het ontwerprapport. Vervolgens is een high-level design gemaakt om een helikopterview van de huidige en nieuwe situatie te geven. Tot slot is het advies geschreven, waarbij diverse scenario's voor Northwave worden geschetst.

Deelvraag 1: "Wat is een SIEM?"
Een Security Information and Event Management (SIEM) is een reeks technologieën. Met een SIEM is het mogelijk om bedreigingen te detecteren en log events en andere gegevens uit bronnen te analyseren. Ook het naleven en beheren van security incidenten door het verzamelen en analyseren van security events behoort tot de mogelijkheden.

Deelvraag 2: "Wat zijn de requirements van Northwave waaraan een SIEM moet voldoen?"
Er zijn in totaal 43 criteria waaraan een SIEM moet voldoen. Deze zijn terug te vinden in hoofdstuk 3 van het analyserapport en in hoofdstuk 2 van dit adviesrapport.

Deelvraag 3: "Welke alternatieven zijn er voor Azure Sentinel die voldoen aan de requirements van Northwave?"
IBM, Exabeam, Elastic, Sumo Logic, Rapid7, Splunk, Securonix, Devo, Fortinet en Micro Focus zijn allemaal geschikte alternatieven voor Azure Sentinel die voldoen aan de requirements van Northwave. Hierbij is de volgorde aangehouden die op basis van de uitgevoerde multicriteria-analyse (MCA) naar voren is gekomen. IBM is volgens het MCA de meest geschikte alternatief en Micro Focus de minst geschikte.

Deelvraag 4: "Wat zijn de verschillen en overeenkomsten van de alternatieven ten opzichte van Azure Sentinel?"
Voor het beantwoorden van deze deelvraag is onderzoek gedaan naar de top drie meest geschikte SIEM's volgens de multicriteria-analyse. De top drie bestaat uit: IBM, Exabeam en Elastic. Op basis van de MCA scoort IBM op iedere behoefte gelijk of minder dan Azure

Sentinel. Exabeam scoort alleen op het gebied van ondersteuning vanuit het product beter, voor de rest scoort Exabeam gelijk of minder in vergelijking met Azure Sentinel. Elastic scoort op iedere behoefte gelijk of minder dan Azure Sentinel. Hierbij wordt wel de kanttekening geplaatst dat Sentinel volgens het Gartner Magic Quadrant een leader op de markt is en Elastic een visionary.

Deelvraag 5: "Wat is de impact op de bestaande omgeving, op het gebied van zowel processen als techniek?"
De impact op de bestaande omgeving, op het gebied van zowel processen als techniek is afhankelijk van het team. In hoofdstukken 2 en 3 van het ontwerprapport, en in hoofdstuk 2 van dit adviesrapport is meer informatie te vinden over de impact.

Antwoord op de hoofdvraag: "Wat is voor Northwave het beste alternatief voor Azure Sentinel met in achtneming van de requirements?"
Er zijn twee SIEM's geschikt als mogelijk alternatief voor Azure Sentinel, IBM QRadar en Elastic Security. In beide gevallen zorgt de aanschaf ervoor dat de kans op vendor lock-in kleiner is.

Er zijn verschillende scenario's voor Northwave met betrekking tot een tweede SIEM mogelijk. Als eerste kan Northwave ervoor kiezen om geen tweede SIEM aan te schaffen, waardoor de kans op vendor lock-in groot is. Tegelijkertijd scheelt het heel veel tijd, geld en moeite. Er hoeft namelijk geen tijdinvestering te worden gedaan om meer kennis te vergaren. De tweede optie is om IBM QRadar aan te schaffen, deze kwam als beste uit de multicriteria-analyse. IBM scoort op alle criteria even goed of minder dan Sentinel. Daarbij behoort IBM tot de "leaders" in het Gartner Magic Quadrant. Helaas bestaat de kans op weerstand onder Northwavers wanneer deze SIEM wordt aangeschaft. Een aantal hebben namelijk minder prettige ervaringen met dit product. Daarbij heeft een Northwaver gewerkt bij een bedrijf waar IBM werd uitgefaseerd omdat het te duur is en volgens dat bedrijf is het niet de beste op de markt. Tot slot kan Northwave kiezen voor Elastic Security, dit is de persoonlijke keuze van de studente op basis van de top drie uit de MCA. In het Gartner Magic Quadrant is Elastic een "visionary", maar scoort volgens het MCA op veel vlakken even goed of iets minder dan Sentinel. Daarbij gebruikt Northwave Elasticsearch, waardoor de engineers al kennis en ervaring hebben met Elastic. Dit leidt tot een hogere gebruikersadoptie en minder weerstand. Tevens is de tijdsinvestering in kennis minder lang in vergelijking met het aanschaffen van IBM.

De studente adviseert Northwave om voor het derde scenario te gaan en Elastic aan te schaffen. Hierbij wordt aanbevolen om een vervolgonderzoek te doen naar de volgende aspecten:

- Compatibiliteit van Elastic Security met het Northwave infrastructuur.
- De roadmap van de SIEM en toekomstige plannen.
- Prijs van aanschaf en licentiestructuur.
- Beveiliging van de SIEM.
- Northwave guidelines voor vendor criteria.

Voorwoord

Beste lezer,

Voor u ligt mijn afstudeerverslag dat bestemd is voor de bedrijfsbegeleider, afstudeerdocent en eenieder die betrokken is bij of belangstelling heeft voor de afstudeeropdracht. Dit afstudeerverslag is het resultaat van mijn twintig weken durende afstudeerperiode bij Northwave. Bij het opstellen van dit verslag is gebruik gemaakt van de overige opgeleverde documentatie, analyses, observaties en interviews. Het afstudeerverslag is door mijzelf geschreven, een vierdejaars HBO-ICT studente van de studierichting IT Service Management.

Graag wil ik Sjoerd van den Bedem, Rob Braun, Wouter van Kranenburg, Jair Santanna, Jaimy Thepass, Yazan Badin, Jochem Smit en Gilles Rauwerdink bedanken. In het bijzonder wil ik zowel mijn bedrijfsbegeleider Julik Keijer als afstudeerdocent Arno Kromdijk bedanken voor de goede begeleiding en ondersteuning.

Ik wens u veel leesplezier,

Jasmine Fan.
Utrecht, 16 januari 2022

Versiegeschiedenis

Versie	Datum	Veranderingen t.o.v. voorgaande versie
0.1	15-01-2023	Bestand is aangemaakt en een lay-out is gemaakt.
0.2	16-01-2023	Lay-out van dit bestand is met de afstudeerdocent en bedrijfsbegeleider besproken. De eerste hoofdstukken zijn gevuld.
0.3	17-01-2023	Deze conceptversie is met de bedrijfsbegeleider besproken en goedgekeurd. Deze versie is ingeleverd bij de afstudeerdocent voor feedback.
0.4	18-01-2023	Alle hoofdstukken zijn gevuld.
1.0	21-01-2023	Definitieve versie.

Tabel 1 Versiegeschiedenis

NORTHWAVE
Intelligent Security Operations

Inhoudsopgave

Managementsamenvatting ..... **II**

Voorwoord ..... **IV**

Versiegeschiedenis ..... **V**

1 Inleiding **8**

2 Probleemstelling en opdracht **9**

3 Methoden en procesmatige projectaanpak **10**

3.1 Methoden *10*

3.2 Procesmatige projectaanpak *11*

4 Resultaten en verantwoording keuzes **12**

4.1 Stakeholderanalyse *12*

4.2 Behoefteanalyse *15*

4.3 Multicriteria-analyse *19*

4.4 High-level design *22*

4.4.1 Huidige situatie (IST) 22

4.4.2 Nieuwe situatie (SOLL) 25

4.5 Advies *27*

5 Beantwoording hoofd- en deelvragen **32**

6 Discussie **36**

6.1 Evaluatie *37*

6.2 Aanbevelingen vervolgonderzoek *37*

Bibliografie **39**

Lijst van figuren

Figuur 1 Ingevulde stakeholdermatrix 13
Figuur 2 Behoeftes stakeholder Sjoerd van den Bedem 15
Figuur 3 Behoeftes stakeholder Rob Braun 16
Figuur 4 Behoeftes stakeholder Erwin Maas/Wouter van Kranenburg 16
Figuur 5 Behoeftes stakeholder Jair Santanna 17
Figuur 6 Behoeftes stakeholder Jaimy Thepass 17
Figuur 7 Behoeftes stakeholder Jochem Smit 18
Figuur 8 Proces SOC OPS shift huidige situatie 22
Figuur 9 Onboarding proces Engineering huidige situatie 23
Figuur 10 Alarm flow huidige situatie 24
Figuur 11 Use case deployment huidige situatie 24
Figuur 12 Proces SOC OPS shift nieuwe situatie 25
Figuur 13 Onboarding proces Engineering nieuwe situatie 25
Figuur 14 Alarm flow nieuwe situatie 26
Figuur 15 Use case deployment nieuwe situatie 26
Figuur 16 Veranderingen SOC-analist 29
Figuur 17 Veranderingen onboarding proces 29
Figuur 18 Veranderingen alarm flow 29
Figuur 19 Veranderingen use case deployment 29

Lijst van tabellen

Tabel 1 Versiegeschiedenis V
Tabel 2 Scrum-rollen 11
Tabel 3 Totaalscore per SIEM-oplossing 21
Tabel 4 Scenario 1 27
Tabel 5 Scenario 2 28
Tabel 6 Scenario 3 30
Tabel 7 Behoeftes m.b.t. een SIEM 33

1 Inleiding

Dit afstudeerverslag is geschreven om de belangrijkste resultaten van het complete onderzoek te geven. Om dit document tot stand te brengen, is gebruik gemaakt van alle overige opgeleverde documentatie, analyses, observaties en interviews. Daarbij is gebrainstormd over de inhoud en indeling van het afstudeerverslag.

In hoofdstuk 2 wordt de probleemstelling en afstudeeropdracht beschreven. Hoofdstuk 3 gaat in op de gebruikte methoden en procesmatige aanpak van het project. De belangrijkste resultaten van de uitgevoerde stakeholderanalyse, behoefteanalyse en multicriteria-analyse zijn te vinden in hoofdstuk 4. Dit hoofdstuk bevat tevens het high-level design en het advies. In hoofdstuk 5 worden de hoofd- en deelvragen beantwoord en in hoofdstuk 6 is de discussie, inclusief aanbevelingen voor een vervolgonderzoek, te lezen. Tot slot komt de bibliografie aan bod.

2 Probleemstelling en opdracht

Binnen Northwave wordt gebruik gemaakt van een aantal SIEM's (Security Information and Event Management), waarvan er twee momenteel worden uitgefaseerd. Dit zijn LogRythm en AlienVault, hierdoor houdt Northwave alleen Azure Sentinel over en dit is ook de enige SIEM die zij op dit moment actief (willen) gebruiken. Hier zijn twee redenen voor: enerzijds bij AlienVault is de kwaliteit van het softwareproduct ontoereikend, anderzijds bij LogRythm is het integreren met API's en het doorvoeren van automatische instellingen niet goed genoeg. Northwave ziet bij Azure Sentinel dat API's wel mogelijk zijn, wat Northwave de mogelijkheid heeft gegeven om heel hard te schalen. (van den Bedem, 2022)

Er kan eenvoudig een basis detectieregel worden aangemaakt, vervolgens wordt dit met een druk op de knop naar alle klanten gestuurd en geactiveerd. Voorheen was iemand nodig die iedere klantenportaal aanklikte en openzette, nu wordt dat automatisch gedaan. De enige manier om het gewenste schaalbaarheidsniveau wat betreft SIEM configuraties en detectieregels te kunnen behalen, is door middel van vergaande automatisering. Idealiter is er niemand die direct interacteert met de SIEM software voor configuratie doeleinden, het liefst wordt dit automatisch via code ingesteld. (van den Bedem, 2022)

Om vendor lock-in tegen te gaan wil Northwave graag weten wat het beste alternatief voor Azure Sentinel is met inachtneming van de eisen en wensen. Deze worden met behulp van een behoefteanalyse in kaart gebracht. Het afstudeerwerk wordt vanaf het begin gestart, aangezien er nog geen werk is verricht. (van den Bedem, 2022)

3 Methoden en procesmatige projectaanpak

In dit hoofdstuk worden de gebruikte methoden en procesmatige aanpak van het project beschreven.

3.1 Methoden

Tijdens het afstuderen is gebruik gemaakt van de volgende nieuwe methoden. Deze methoden zijn voornamelijk vergaard middels deskresearch en zijn gedurende de opleiding bij Saxion niet aan bod gekomen.

- **ASL-impactanalyse proces** wordt gebruikt om de gevolgen (impact) van voorgestelde wijzigingen te bepalen (ASL Foundation, z.d.).
- **BPMN** voor het ontwerpen van de impact op de huidige processen en techniek. Hier is voor gekozen, omdat het een gangbare methode is.
- **Bronnentriangulatie** om de betrouwbaarheid van bronnen te verhogen. Deze methode houdt in dat wanneer meerdere bronnen dezelfde informatie geven, de aanname kan worden gedaan dat deze bronnen betrouwbaar zijn (Scriptium, 2022).
- **Handy model** om de cultuur binnen Northwave te beschrijven. Bij deze methode wordt onderzoek gedaan naar hoe de machtsspreiding en samenwerkingsgraad zich tot elkaar verhouden (Mulder, 2018). Deze methode is gebruikt in het plan van aanpak.
- **Korthagen** voor het schrijven van de reflecties waarbij de samenhang tussen het gevoel en de handelingen centraal staat.
- **Model van Abell** om de behoeftes per stakeholder boven water te krijgen. Er is voor deze methode gekozen, omdat het goed aansloot op de behoeftes.
- **Multicriteria-analyse** om op een zo objectief mogelijke manier een keuze te kunnen maken.
- **STARR** voor het schrijven van de reflecties waarbij de samenhang tussen de situatie en de handelingen van belang is.

Gedurende de afstudeerperiode zijn de volgende methoden behandelt die tevens tijdens de opleiding zijn gebruikt. Er is gekozen om deze methoden te gebruiken, omdat de studente hier goede ervaringen mee heeft.

- **7s-model** om een interne analyse te maken en een goed beeld te krijgen over het bedrijf. Deze methode is gebruikt in het plan van aanpak.
- **APAv6** wordt gebruikt voor de bronvermelding.
- **Brainstormen** om zoveel mogelijk mooie ideeën uit te denken waarmee de antwoorden voor het vraagstuk worden verzameld (Impres, z.d.).
- **High-level design** om een helikopterview te geven (insign.it, z.d.).
- **Literatuuronderzoek** met behulp van deskresearch om meer kennis in het kader van de afstudeeropdracht te vergaren.
- **Matrix van Mendelow** om de definitieve lijst van relevante stakeholders te bepalen.
- **MoSCoW** wordt gebruikt voor de prioritering van de user stories.
- **Observaties** omdat wat mensen daadwerkelijk doen vaak verschilt van wat ze zeggen
- (HAN & HVA, z.d.).
- **Ontwerpprincipes** om, indien van toepassing, het ontwerp op te onderbouwen.

- **Semigestructureerde interviews** om gegevens voor het onderzoek te verzamelen (Genau, 2021).

3.2 Procesmatige projectaanpak

Gedurende het afstuderen is gebruik gemaakt van Scrum als projectmanagementmethodiek. Hiervoor is gekozen omdat binnen Northwave Scrum wordt gehanteerd. Binnen het Security Operations Center Operations (SOC OPS) wordt dagelijks tweemaal een stand-up gehouden. In de ochtend om half tien en in de middag om drie uur. Na iedere sprint heeft de studente een sprint review en retrospective met de bedrijfsbegeleider (Julik Keijer) gehouden. Daarbij zijn enkele user stories opgesteld met de bijbehorende Definition of Done (DoD), een product backlog en een sprint backlog. Dit is allemaal terug te vinden in het Scrum-document.

Binnen Scrum wordt gebruik gemaakt van een aantal rollen. Deze rollen worden overgenomen gedurende het uitvoeren van de afstudeeropdracht. Hierbij wordt het Blue Team als een geheel onder “Teamleden” verdeeld, aangezien dit team uit ongeveer 50-60 medewerkers bestaat is ervoor gekozen om deze niet allemaal te noteren. Daarbij zal de studente zelf de producten opstellen en opleveren, het Blue Team zal er enkel zijn ter ondersteuning.

Naam	**Scrum-rol**
Sjoerd van den Bedem	Product Owner
Julik Keijer	Scrum Master
Blue Team	Teamleden (ter ondersteuning)
Jasmine Fan	Teamlid

Tabel 2 Scrum-rollen

Toelichting op de rollen

- De **Product Owner** vertegenwoordigt de belangen van verschillende stakeholders, waaronder de klant. (Kooijman, z.d.)
- De **Scrum Master** is er om het team zo te begeleiden dat de samenwerking optimaal verloopt. De Scrum Master zorgt er in feite voor dat het Scrum Team ongestoord werk kan verzetten. (Kooijman, z.d.)
- Het **Scrum Team** is zelfsturend. De teamleden zorgen ervoor dat het product voldoet aan de wensen van de klant en dat het binnen de sprint wordt geproduceerd. (Kooijman, z.d.)

4 Resultaten en verantwoording keuzes

In dit hoofdstuk komen de belangrijkste resultaten van dit onderzoek naar voren. Als eerste wordt het resultaat van de stakeholderanalyse beschreven. Daarna komen de behoeftes van iedere stakeholder uit de behoefteanalyse aan bod. Vervolgens is het eindresultaat van de multicriteria-analyse te zien. Hierna komt het high-level design aan bod en tot slot is het advies te lezen.

Er zijn een aantal aspecten die wel zijn uitgevoerd, maar omwille van de grootte niet in dit verslag zijn opgenomen. Het literatuuronderzoek, waarin onderzoek is gedaan naar de volgende onderwerpen: “On-premise vs. Cloud SIEM”, “Managed vs. Co-managed vs. Self-managed SIEM” en “Alternatieven Azure Sentinel”, is terug te vinden in hoofdstuk 4 van het analyseverslag. Tevens is in hoofdstuk 5 van het analyseverslag de exacte opbouw van de multicriteria-analyse te lezen. De uitgevoerde impactanalyse wordt in hoofdstuk 2 van het ontwerprapport beschreven.

4.1 Stakeholderanalyse

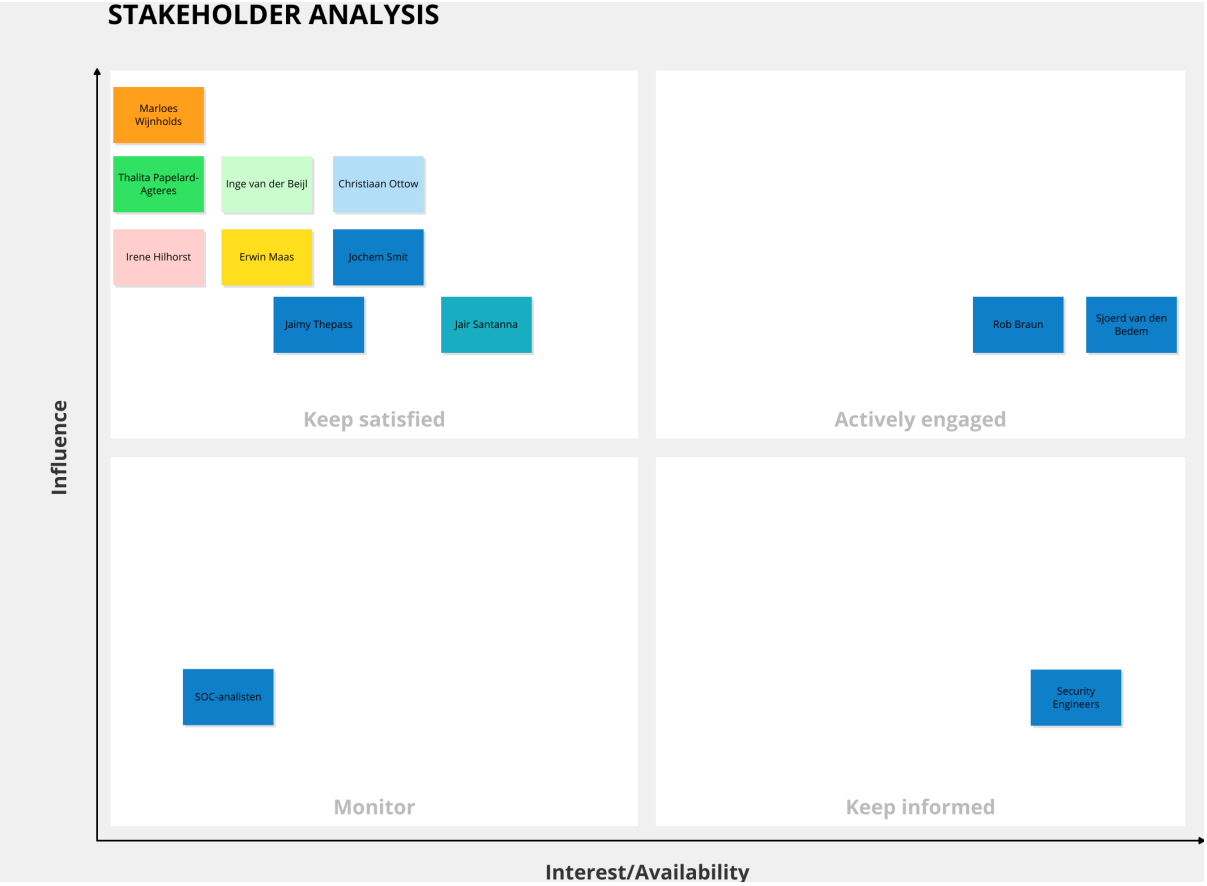
Er is een stakeholderanalyse uitgevoerd om de meest relevante en belangrijke stakeholders in kaart te brengen. De longlist met alle potentiële stakeholders en bijbehorende verantwoording is terug te vinden in hoofdstuk 2 van het analyseverslag.

De Mendelow-matrix is gebruikt om de definitieve lijst van relevante stakeholders te bepalen. Bij de matrix van Mendelow wordt gekeken naar vier aspecten.

- **Power** (macht): Hoeveel macht en invloed hebben ze op basis van hun posities?
- **Awareness** (bewustzijn): In hoeverre zijn ze zich bewust van de impact van het project?
- **Interest** (belang): Hoe groot is hun gevestigde belang bij het projectresultaat?
- **Support** (ondersteuning): Zijn ze ondersteunend of resistent tegen het project?

(Ondreicsik, 2021)

In onderstaand figuur is de ingevulde stakeholdermatrix te zien. De x-as verwijst naar de hoeveelheid macht die elke stakeholder heeft en de y-as naar de mate waarin ze geïnteresseerd zijn in de uitkomst van het project. Daarbij zijn er vier verschillende categorieën waartoe een stakeholder kan behoren. (Ondreicsik, 2021)



Figuur 1 Ingevulde stakeholdermatrix

Actively engaged (ook wel de "key players")
Deze stakeholders hebben veel macht en veel belang. Zij zullen de hoogste prioriteit vragen op het gebied van communicatie en betrokkenheid bij de besluitvorming. (Ondreicsik, 2021) In dit geval zouden dit zowel Sjoerd van den Bedem als Rob Braun zijn.

Keep satisfied
Deze stakeholders hebben veel macht maar weinig interesse. (Ondreicsik, 2021)
In deze situatie zijn dat Christiaan Ottow, Jaimy Thepass, Jair Santanna, Jochem Smit, Erwin Maas, Talitha Papelard-Agteres, Inge van der Beijl, Marloes Wijnholds en Irene Hilhorst.

Keep informed
Deze stakeholders hebben minder macht maar veel interesse. Ze zijn geïnteresseerd en moeten regelmatig op de hoogte worden gehouden. (Ondreicsik, 2021) De Security Engineers moeten regelmatig detectieregels schrijven voor de SIEM, waardoor zij zich bevinden tot de categorie "keep informed".

Monitor
Deze stakeholders hebben weinig macht en weinig interesse. Ze vergen minimale inspanning en aandacht, maar dienen in ieder geval gecontroleerd en geïnformeerd te worden. (Ondreicsik, 2021) De SOC-analisten behoren tot deze groep.

Om de scope en de haalbaarheid van de afstudeeropdracht te bewaken is ervoor gekozen om het resultaat van de stakeholdermatrix niet één op één over te nemen. Alleen de managers en leads van teams waar een nieuwe SIEM impact op zal hebben, zullen een stakeholder zijn. De vastgestelde stakeholders zijn als volgt.

- Sjoerd van den Bedem.
- Rob Braun.
- Erwin Maas.
- Jair Santanna.
- Jaimy Thepass.
- Christiaan Ottow.
- Jochem Smit.

Hierbij zijn zowel Sjoerd van den Bedem als Rob Braun de "key players" en daardoor de belangrijkste stakeholders. Zij zullen vaker op de hoogte worden gehouden dan de andere stakeholders. De teamleden van zowel Sjoerd als Rob gebruiken de SIEM dagelijks en een nieuwe SIEM zou de grootste impact op beide teams hebben. Sjoerd en Rob vertegenwoordigen daarbij de belangen van de SOC-analisten en Security Engineers. Hierdoor wegen hun behoeften zwaarder mee dan die van de andere stakeholders.

4.2 Behoefteanalyse

Naar aanleiding van de gehouden stakeholderinterviews zijn de behoeftes van de stakeholders in kaart gebracht. De behoeftes per stakeholder zijn door middel van het model van Abell genoteerd. De prioritering van behoeftes is gedaan met behulp van de MoSCoW-methode. Hierbij zijn de roodgekleurde behoeftes een must, oranje gekleurde behoeftes zijn een should, groen gekleurde zijn een could en de blauw gekleurde behoeftes zijn een would/won't. De behoeftes van de stakeholders dienen als input voor de multicriteria-analyse. Hierbij is besloten om de weging van de behoeftes van de "key players" (Sjoerd van den Bedem en Rob Braun) zwaarder mee te wegen dan die van de overige stakeholders.

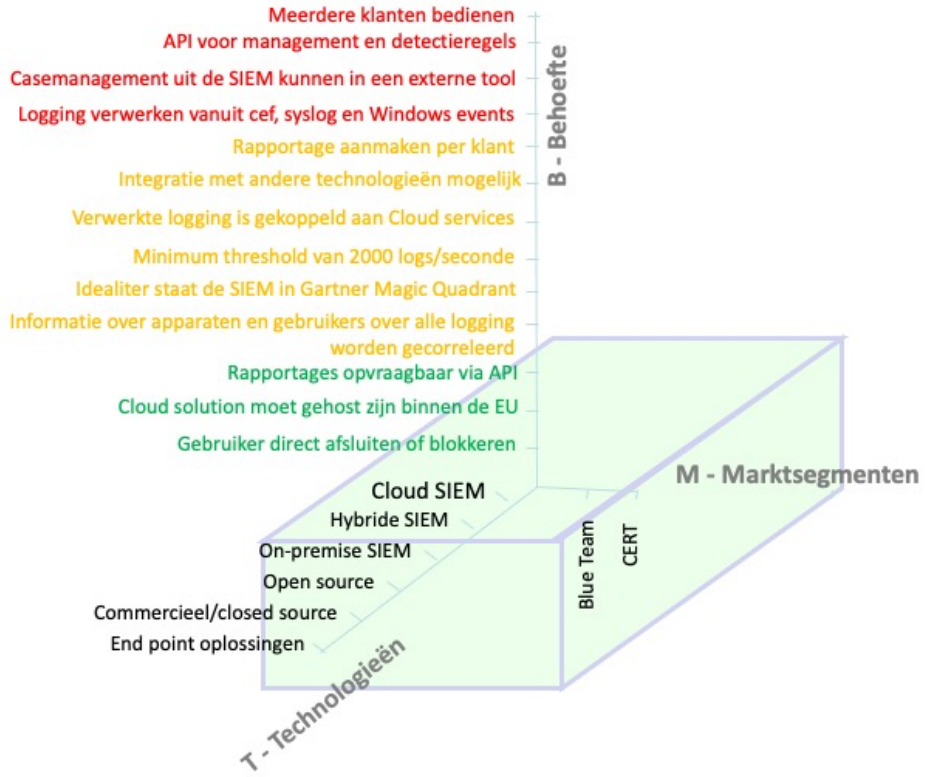
Het model van Abell geeft een duidelijk inzicht in het werkterrein. Het model bestaat uit de volgende drie verschillende dimensies.

- **Afnemers (Marktsegmenten)**
  De afnemers zijn diegene die het product of dienst aanschaffen. Dit wordt ook wel de "doelgroep" of "marktsegmenten" genoemd.
- **Behoeften**
  De behoeften zijn de zaken die afnemers belangrijk vinden aan een product of dienst.
- **Technologieën**
  Bij technologieën wordt er gekeken naar de manier waarop een bedrijf inspeelt op de behoeftes.

(Marketingscriptie, z.d.)

Teamlead Detection quality & stack

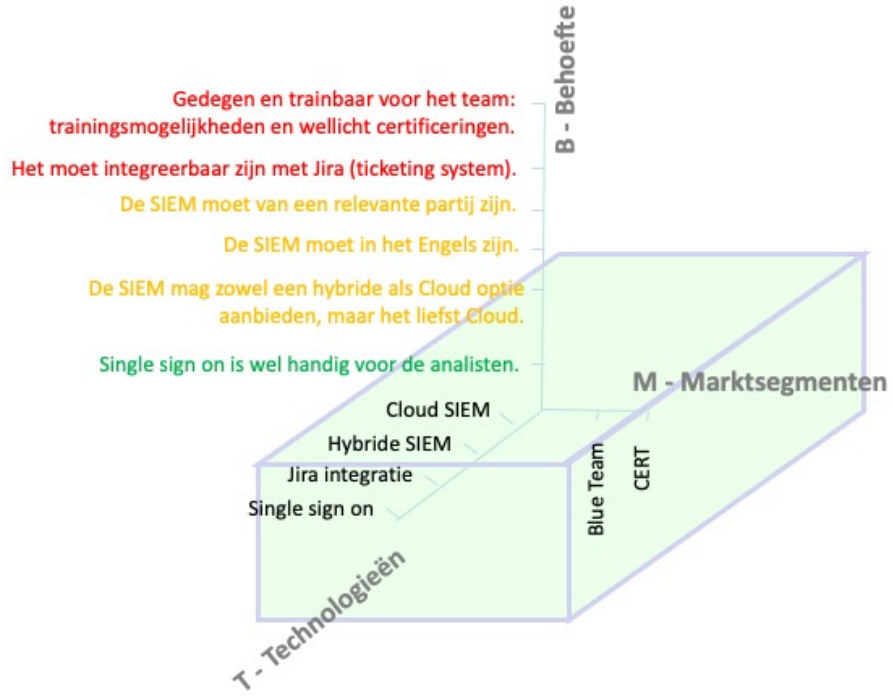
In onderstaand figuur is het model van Abell ingevuld met de behoeftes van Sjoerd van den Bedem. De prioritering van de behoeftes is samen bepaald.



Figuur 2 Behoeftes stakeholder Sjoerd van den Bedem

Teamlead Operations

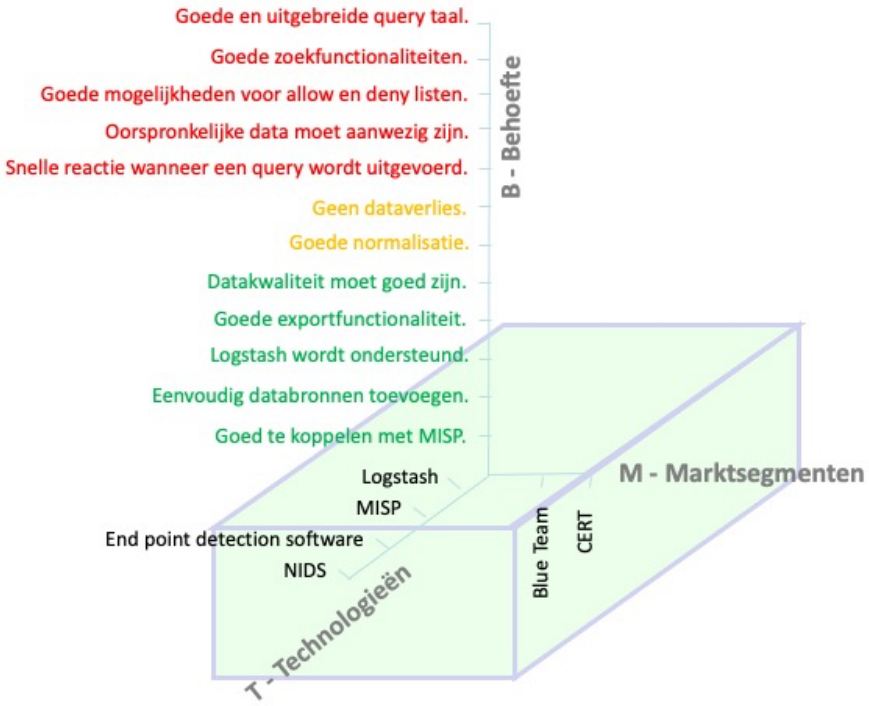
In onderstaand figuur is het model van Abell ingevuld met de behoeftes van Rob Braun. De prioritering van de behoeftes is samen bepaald.



Figuur 3 Behoeftes stakeholder Rob Braun

Manager CERT

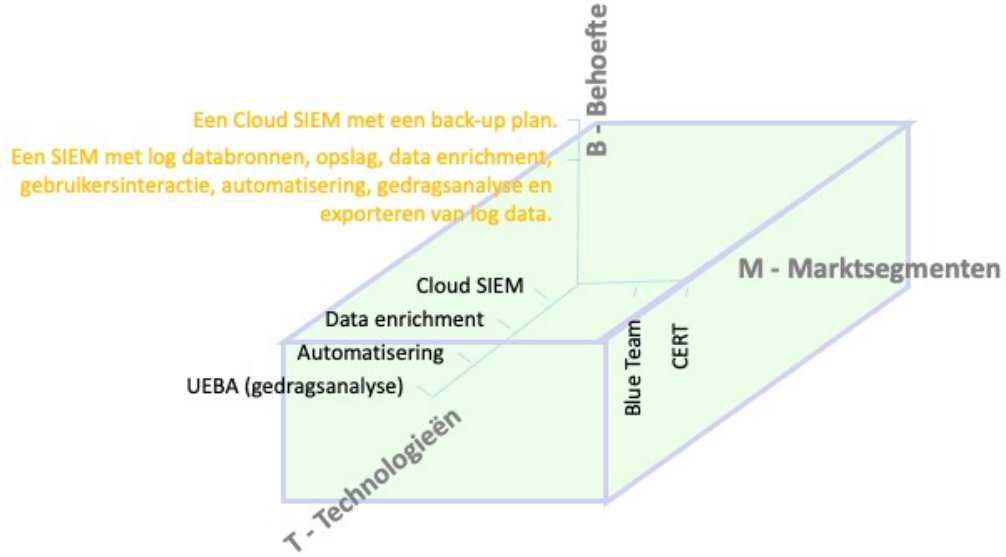
In onderstaand figuur is het model van Abell ingevuld met de behoeftes van Erwin Maas die vertegenwoordigd werd door Wouter van Kranenburg. De prioritering van de behoeftes is samen met Wouter bepaald.



Figuur 4 Behoeftes stakeholder Erwin Maas/Wouter van Kranenburg

Cloud Security Lead

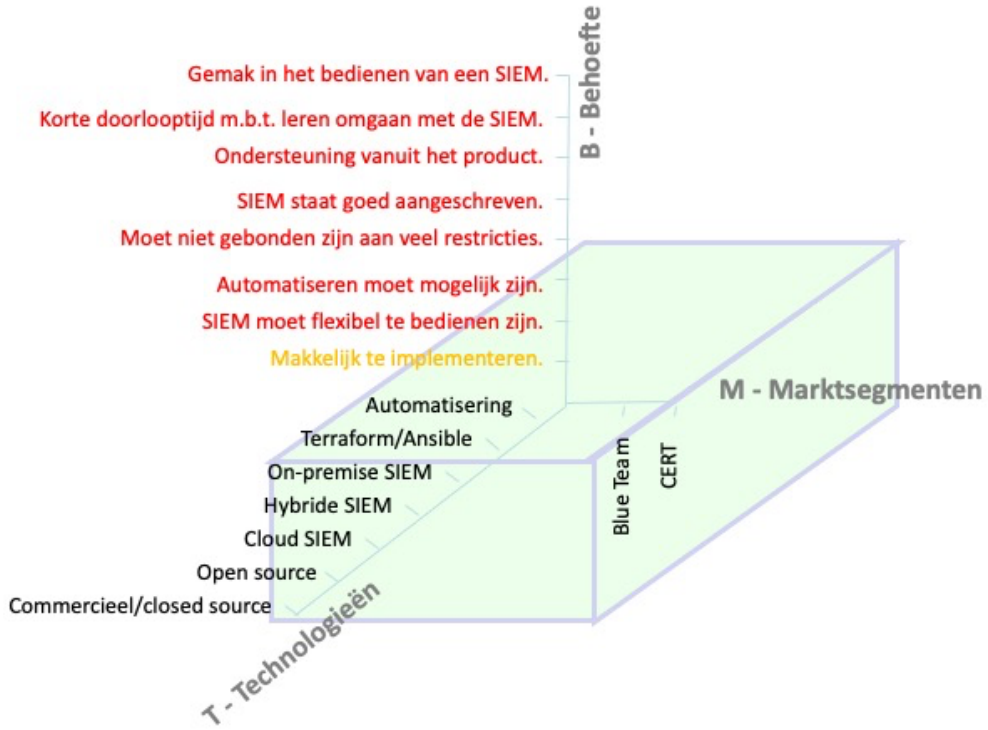
In onderstaand figuur is het model van Abell ingevuld met de behoeftes van Jair Santanna. De prioritering van de behoeftes is samen bepaald.



Figuur 5 Behoeftes stakeholder Jair Santanna

Teamlead Service delivery & sysadmin

In onderstaand figuur is het model van Abell ingevuld met de behoeftes van Jaimy Thepass. De prioritering van de behoeftes is samen bepaald. De behoeftes van Jaimy zijn aangevuld met behoeftes van Yazan Badin.

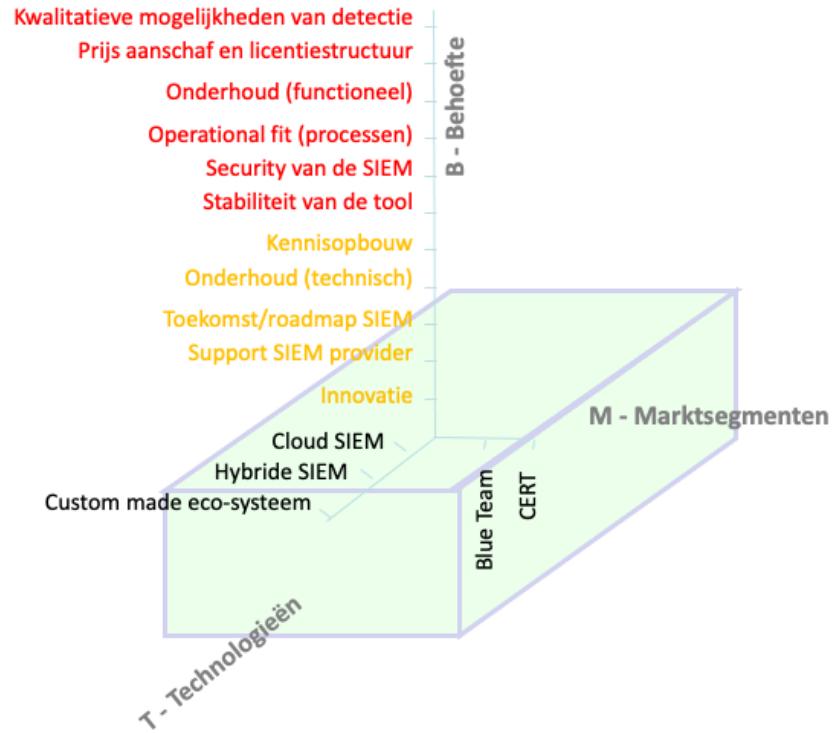


Figuur 6 Behoeftes stakeholder Jaimy Thepass

Chief Technology Officer (CTO)
Op 27 september 2022 is een mail gestuurd naar Christiaan Ottow met het stakeholderinterview in de vorm van een vragenlijst. Hier is geen reactie op gekregen, maar uit gesprekken met de andere stakeholders en de bedrijfsbegeleider is de aanname gedaan dat de behoeftes van Rob Braun en Sjoerd van den Bedem indirect ook de behoeftes van Christiaan Ottow vertegenwoordigen.

Manager Blue Team
Op 6 oktober 2022 is een mail gestuurd naar Jochem Smit met het stakeholderinterview in de vorm van een vragenlijst. Op 7 november 2022 is de ingevulde vragenlijst teruggestuurd, helaas was het multicriteria-analyse op dat moment net afgerond en zijn deze behoeftes niet één op één meegenomen. Echter, kwam een deel van Jochems requirements overeen met die van de andere stakeholders, dus dat deel is wel meegenomen.

In onderstaand figuur is het model van Abell ingevuld met de behoeftes van Jochem Smit. De prioritering van de behoeftes heeft Jochem zelf bepaald.



Figuur 7 Behoeftes stakeholder Jochem Smit

4.3 Multicriteria-analyse

In onderstaand tabel zijn de totale scores berekend en op basis van deze score heeft iedere SIEM-oplossing een bepaalde ranking gekregen. De scores zijn berekend door eerst de ingevulde scores in hoofdstuk 5.1.4 “Ingevulde scores” te koppelen aan de waardes in hoofdstuk 5.2.1 “Scores naar waarden tussen 0 en 1 vertalen”. Vervolgens zijn deze waardes vermenigvuldigd met de weging die terug te vinden is in hoofdstuk 5.2.2 “Het gewicht van elk criterium bepalen”. Deze hoofdstukken zijn te vinden in het analyseverslag.

	Devo	**Elastic**	**Exabeam**	**Fortinet**	**Gurucul**	**IBM**	**Micro Focus**	**Rapid7**	**Securonix**	**Splunk**	**Sumo Logic**
Meerdere klanten bedienen	0,4	0,4	0,4	0,4	0,4	0,4	0,4	0,4	0,4	0,4	0,4
API	0,4	0,4	0,4	0,4	0,4	0,4	0,4	0,4	0,4	0,4	0,4
Casemanagement in externe tool	0,4	0,4	0,4	0,4	0	0,4	0,4	0,4	0,4	0,4	0,4
Logging verwerken cef, syslog en Windows events	0,4	0,4	0,4	0,4	0,132	0,4	0,4	0,4	0,264	0,4	0,4
Integreerbaar Jira en andere technologieën	0,4	0,4	0,4	0,264	0,4	0,4	0,132	0,4	0,4	0,4	0,4
Korte doorlooptijd	0,3	0,3	0,3	0,3	0	0,3	0,3	0,3	0,3	0,3	0,3
Uitgebreide query taal	0,225	0,225	0,15	0,075	0,075	0,225	0,15	0,225	0,15	0,15	0,3
Goede zoekfunctionaliteiten	0,225	0,3	0,225	0,225	0,15	0,225	0,225	0,225	0,225	0,225	0,225
Goede mogelijkheden allow en deny listen	0,075	0,15	0,225	0,15	0,075	0,225	0,15	0,15	0,15	0,15	0,15
Raw data aanwezig	0,3	0,3	0,3	0,3	0	0,3	0,3	0,3	0,3	0,3	0,3

Ondersteuning vanuit het product	0,225	0,225	0,3	0,075	0,075	0,225	0,15	0,225	0,225	0,225	0,225
Gartner Magic Quadrant	0,3	0,3	0,3	0,3	0,3	0,3	0,3	0,3	0,3	0,3	0,3
Flexibel te bedienen	0,15	0,075	0,15	0,15	0,15	0,15	0,15	0,15	0,15	0,15	0,15
Rapportages aanmaken per klant	0	0,1	0,15	0,1	0	0,15	0,1	0,15	0,1	0,15	0,1
Logging gekoppeld aan Cloud services	0,15	0,15	0,15	0,1	0,15	0,15	0,1	0,15	0,1	0,15	0,15
Minimum threshold van 2000 logs/seconde	0,2	0,2	0,2	0,2	0	0,2	0	0	0,2	0	0
Informatie apparaten en gebruikers gecorreleerd	0,2	0,2	0,2	0,2	0,2	0,2	0,2	0,2	0,2	0,2	0,2
De SIEM is in het Engels	0,2	0,2	0,2	0,2	0,2	0,2	0,2	0,2	0,2	0,2	0,2
Cloud SIEM	0,2	0,2	0,2	0,2	0,2	0,2	0,2	0,2	0,2	0,2	0,2
Goede normalisatie	0	0,05	0,075	0,05	0,05	0,075	0,05	0,075	0,05	0,075	0,075
Eenvoudig te implementeren	0,025	0,05	0,025	0	0,025	0,075	0,025	0,075	0,075	0,075	0,075
Log databronnen, opslag, data enrichment, gebruikersinteractie, automatisering, gedragsanalyse en	0,084	0,084	0,1	0,084	0,084	0,1	0,084	0,1	0,084	0,1	0,084

exporteren van log data											
Totaalscore	4,859	5,109	5,250	4,573	3,066	5,300	4,416	5,025	4,873	4,950	5,034
Rank	8	3	2	9	11	1	10	5	7	6	4

Tabel 3 Totaalscore per SIEM-oplossing

Op basis van de uitgevoerde multicriteria-analyse is de volgende top drie naar voren gekomen.

1. IBM
2. Exabeam
3. Elastic

Deze top drie is in het analyseverslag verder uitgewerkt en waar mogelijk is er ook gekeken naar de “could have” requirements.
IBM is in hoofdstuk 5.4 van het analyseverslag te lezen, Exabeam in hoofdstuk 5.5 en Elastic in hoofdstuk 5.6.

De persoonlijke meningen met betrekking tot de verschillende SIEM’s zijn terug te vinden in hoofdstuk 5.7 van het analyseverslag. Deze meningen zijn gedurende de stakeholderinterviews naar voren gekomen.

4.4 High-level design

In deze paragraaf wordt de high-level design (HLD) beschreven. Het doel van een HLD is om een helikopterview te geven en biedt minder technische details (insign.it, z.d.). Hier is bewust voor gekozen, omdat Northwave bepaalde (technische) zaken intern wil houden. Als eerste komt de huidige situatie op het gebied van processen aan bod. Daarna wordt ingegaan op de huidige situatie van de techniek. Vervolgens wordt de nieuwe situatie voor de processen in kaart gebracht. Tot slot wordt de nieuwe situatie voor de techniek omschreven.

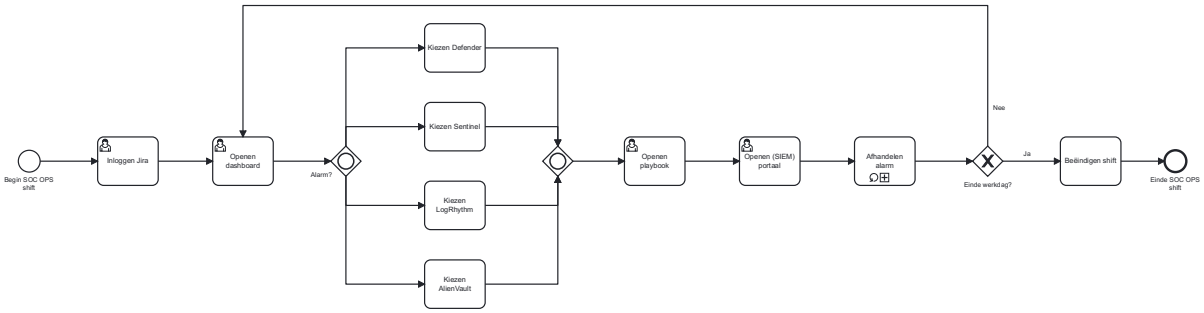
Op basis van de uitgewerkte impactanalyse wordt de conclusie getrokken dat een nieuwe SIEM nauwelijks impact heeft op huidige processen en techniek binnen het CERT. Hierdoor is besloten om het CERT niet mee te nemen in deze high-level design. De focus van de HLD ligt daardoor geheel op het Blue Team. Voor het uitwerken van de ontwerpen is gebruik gemaakt van de stakeholderinterviews (te vinden in het analyseverslag), de Northwave Knowledge Base, observaties, gesprekken met de bedrijfsbegeleider en opgedane ervaring gedurende de SOC OPS shifts. Verder is gebruik gemaakt van de BPMN Quick Guide (Gagné & Ringuette, z.d.)

4.4.1 Huidige situatie (IST)

In de huidige situatie worden twee processen en twee zaken met betrekking tot de techniek uitgewerkt. Als eerste wordt het proces met betrekking tot de SOC OPS shift van de SOC-analisten beschreven. Daarna wordt het onboarding proces van de engineers omschreven. Vervolgens wordt het alarm flow uitgelegd en tot slot komt de use case deployment aan bod.

Processen

In onderstaand figuur is het proces met betrekking tot de SOC OPS shift in de huidige situatie te zien.

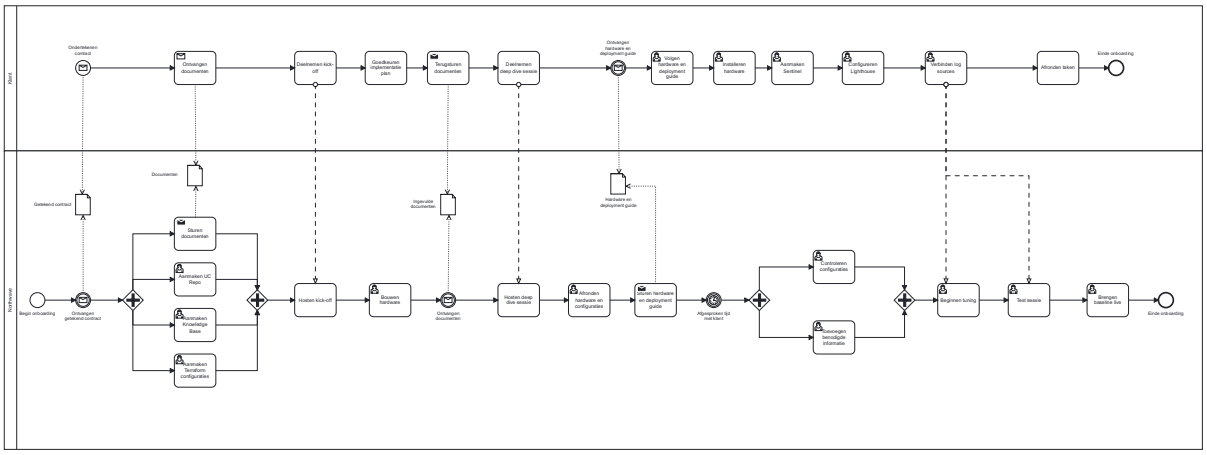


Figuur 8 Proces SOC OPS shift huidige situatie

Een SOC OPS shift begint als volgt. Een SOC-analist logt in op Jira en opent vervolgens het dashboard. Daarna wordt een alarm gekozen, waarbij er keuze is uit vier verschillende soorten: Defender, Sentinel, LogRhythm of AlienVault. Het is mogelijk om één of meerdere alarmen te kiezen. Wanneer een alarm is gekozen, wordt het playbook (UseCase Repo) geopend. Daarin staan de stappen die een analist kan nemen om het alarm te analyseren. Vervolgens wordt het (SIEM) portaal geopend, zodat de analist alle gegevens met betrekking tot het alarm kan inzien. Wanneer de juiste query wordt meegegeven, kan de analist alles bekijken wat hij/zij nodig heeft of wil zien. Na het openen van het portaal wordt het alarm afhandelingsproces gestart. Dit proces herhaalt zichzelf continu tijdens een SOC OPS shift.

Wanneer de werkdag nog niet klaar is, wordt het gehele proces herhaald door het dashboard te openen. Wanneer de werkdag tot een eind is gekomen, dan wordt de shift beëindigd en is het einde van de SOC OPS shift bereikt.

In onderstaand figuur is het onboarding proces in de huidige situatie te zien.



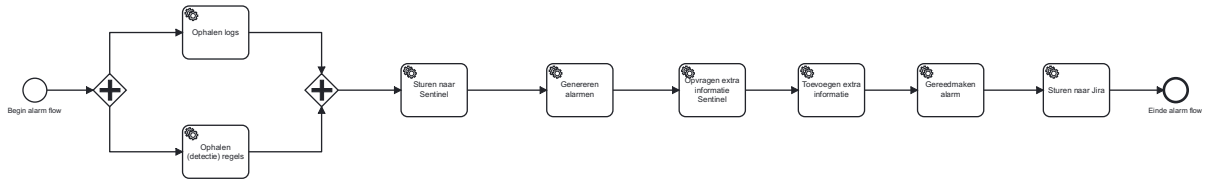
Figuur 9 Onboarding proces Engineering huidige situatie

Het onboarding proces begint als volgt. Vanuit Northwave begint het onboarding proces, waarbij er eerst wordt gewacht totdat het getekende contract van de klant is ontvangen. Daarna wordt er tegelijkertijd documenten naar de klant gestuurd en worden de UC Repo, Knowledge Base en Terraform configuraties aangemaakt. Daaropvolgend wordt een kick-off gehost, waar de klant aan deelneemt. Vervolgens wordt de hardware gebouwd en wordt er gewacht op de ingevulde documenten van de klant. Wanneer deze ontvangen zijn, host Northwave een deep dive sessie met de klant. Na deze sessie wordt de hardware en configuraties afgerond. Daaropvolgend wordt de hardware en deployment guide naar de klant gestuurd. Vervolgens wordt een bepaalde tijd gewacht, dit is een afgesproken tijd met de klant (bijvoorbeeld vijf dagen). Wanneer de klant klaar is met het installeren, implementeren en configureren, dan wordt tegelijkertijd de configuraties gecontroleerd en de benodigde informatie toegevoegd. Daarna wordt begonnen met tuning en een test sessie. Tot slot wordt de baseline live gebracht en eindigt het onboarding proces.

Voor de klant begint het proces bij het ondertekenen van het contract. Daarna worden de documenten van Northwave ontvangen en neemt de klant deel aan de kick-off. Na de kick-off keurt de klant het implementatieplan goed. Vervolgens worden de documenten ingevuld en naar Northwave teruggestuurd. Daaropvolgend wordt deelgenomen aan de deep dive sessie van Northwave. De klant wacht daarna totdat de hardware en deployment guide van Northwave is ontvangen. Eenmaal ontvangen volgt de klant deze guide en installeert de hardware. Vervolgens wordt Sentinel aangemaakt en Lighthouse geconfigureerd. De log sources worden daarna verbonden en samen met Northwave wordt er begonnen met tuning en de test sessie. Tot slot worden de taken afgerond en eindigt het onboarding proces.

Techniek

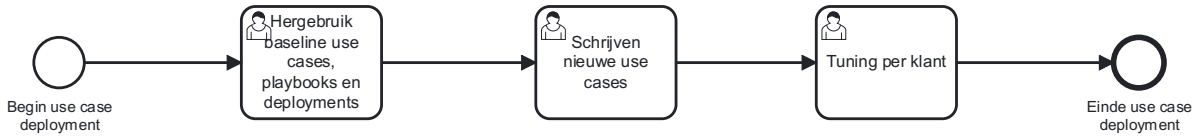
In onderstaand figuur is de alarm flow in de huidige situatie te zien.



Figuur 10 Alarm flow huidige situatie

De alarm flow begint en gelijktijdig worden logs en (detectie)regels opgehaald. Vervolgens worden deze doorgestuurd naar Sentinel, waarna alarmen worden gegenereerd. Daarna wordt extra informatie aan Sentinel opgevraagd en toegevoegd aan het alarm. Het alarm wordt gereedgemaakt en naar Jira gestuurd. Hierna eindigt de alarm flow. De alarm flow wordt geheel automatisch uitgevoerd, waarbij er gebruik wordt gemaakt van applicaties en services, waaronder API's.

In onderstaand figuur is de use case deployment in de huidige situatie te zien.



Figuur 11 Use case deployment huidige situatie

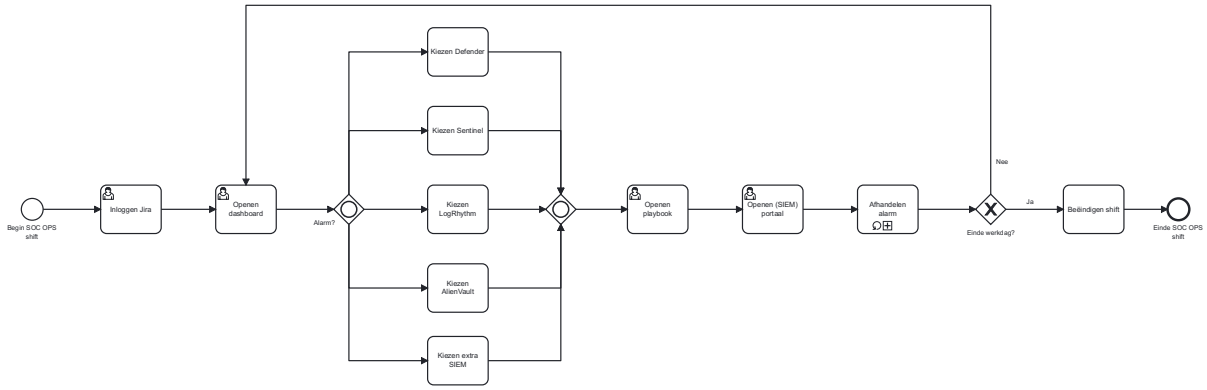
De use case deployment begint en de baseline use cases, playbooks en deployments voor Azure Sentinel worden hergebruikt. Vervolgens worden nieuwe use cases geschreven, deze worden over het algemeen naar de behoefte en/of op verzoek van de klant gedaan. Tot slot worden er kleine aanpassingen (tuning) per klant op basis van hun netwerk gedaan. Hierbij wordt gekeken naar welke regels er af gaan en wordt aan de klant gevraagd op dat legitiem is. Na de tuning wordt de use case deployment beëindigd.

4.4.2 Nieuwe situatie (SOLL)

In de huidige situatie worden twee processen en twee zaken met betrekking tot de techniek uitgewerkt. Als eerste wordt het proces met betrekking tot de SOC OPS shift van de SOC-analisten beschreven. Daarna wordt het onboarding proces van de engineers omschreven. Vervolgens wordt het alarm flow uitgelegd en tot slot komt de use case deployment aan bod.

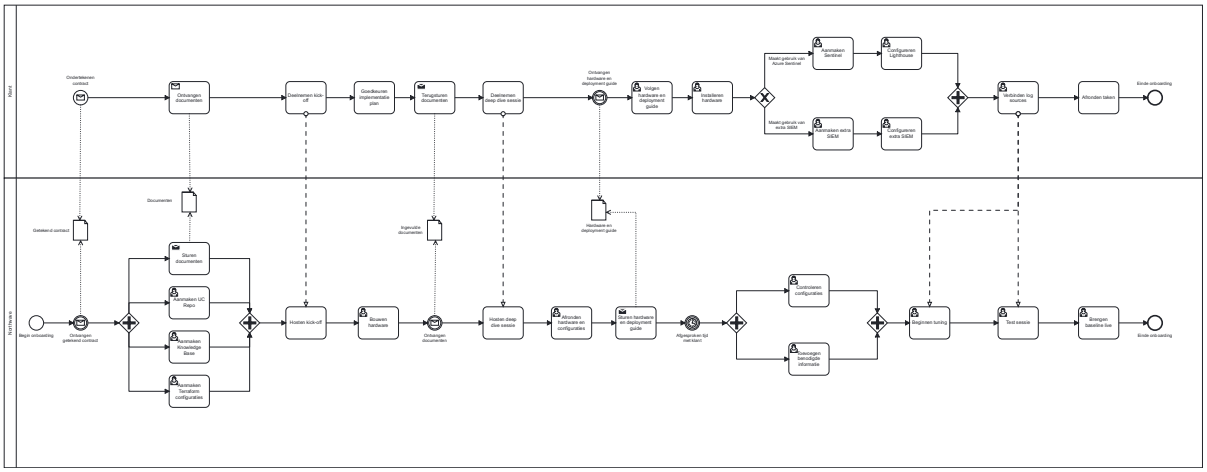
Processen

In onderstaand figuur is het proces met betrekking tot de SOC OPS shift in de nieuwe situatie te zien. In de nieuwe situatie verandert in principe één ding. De analist kan nu kiezen uit vijf mogelijkheden in plaats van vier. Hierbij is de vijfde mogelijkheid de extra SIEM.



Figuur 12 Proces SOC OPS shift nieuwe situatie

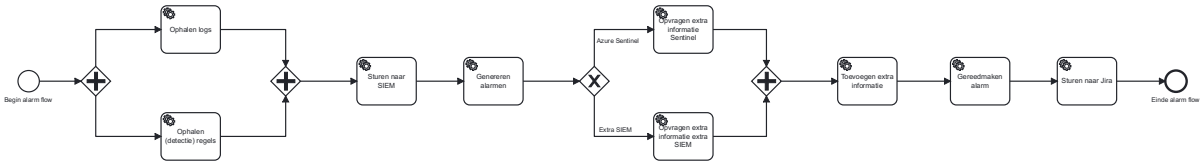
In onderstaand figuur is het onboarding proces in de nieuwe situatie te zien. In de nieuwe situatie wijzigt in principe één ding. Voor het aanmaken en configureren van de SIEM heeft de klant nu keuze tussen Azure Sentinel of de extra SIEM in plaats van alleen Sentinel.



Figuur 13 Onboarding proces Engineering nieuwe situatie

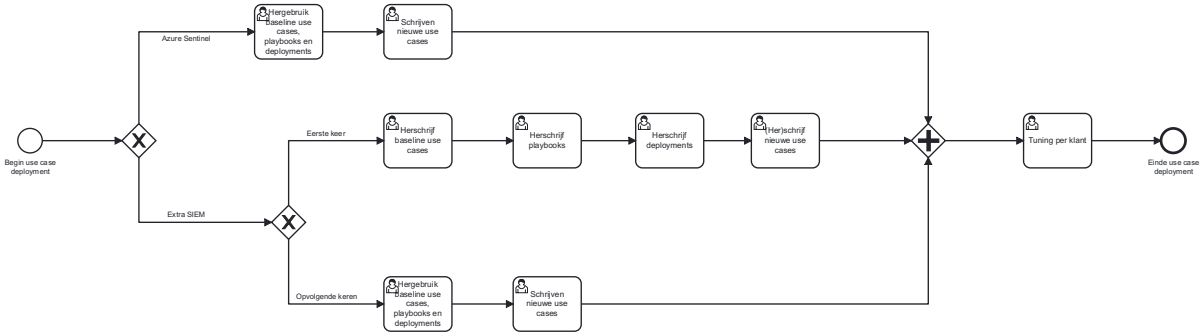
Techniek

In onderstaand figuur is de alarm flow in de nieuwe situatie te zien. In de nieuwe situatie wijzigt in principe één ding. Na het genereren van de alarmen wordt extra informatie opgevraagd aan Sentinel of de extra SIEM in plaats van alleen aan Sentinel.



Figuur 14 Alarm flow nieuwe situatie

In onderstaand figuur is de use case deployment in de nieuwe situatie te zien. De klant heeft nu keuze tussen Azure Sentinel of de extra SIEM. Wanneer er wordt gekozen voor de extra SIEM, dan zijn er twee opties. Als het de eerste keer is, dan worden de baseline use cases, playbooks en deployments herschreven. Deze aanpassingen hoeven in principe maar één keer worden gedaan en niet voor elke klant opnieuw. Dit resulteert in de optie “opvolgende keren”, waarbij de baseline use cases, playbooks en deployments net zoals bij Azure Sentinel worden hergebruikt.



Figuur 15 Use case deployment nieuwe situatie

4.5 Advies

In dit hoofdstuk komt het advies aan bod. Om het advies te ondersteunen, wordt gebruik gemaakt van diverse scenario's.

Scenario 1: Geen tweede SIEM aanschaffen

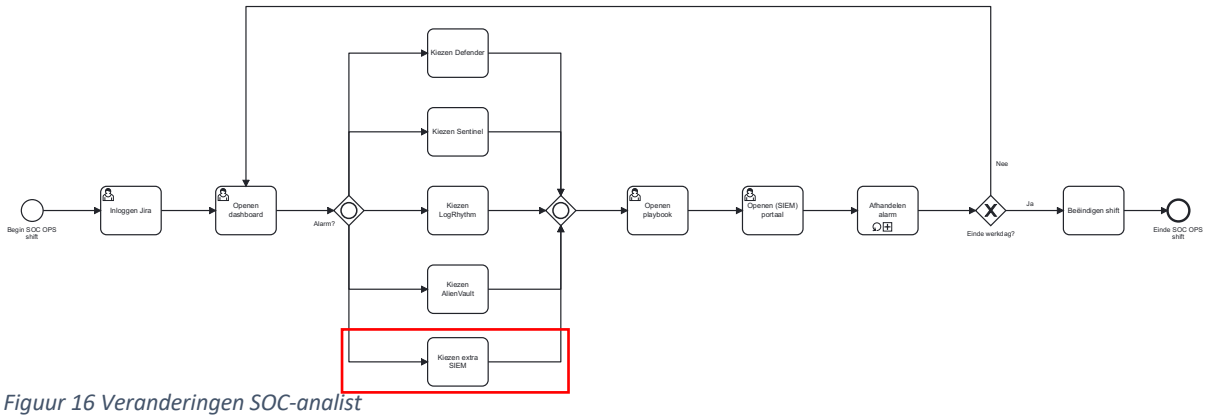
Omschrijving	Scenario 1 houdt in dat er niks wordt gedaan aan het huidige probleem. Nadat het uitfaseren van LogRhythm en AlienVault is voltooid, zal Northwave alleen gebruik maken van Azure Sentinel. Hierdoor blijft de kans op vendor lock-in bestaan. Daarbij kan aan potentiële klanten maar één SIEM mogelijkheid worden geboden. Als een bedrijf een sterke voorkeur heeft om Microsoft-producten te vermijden, kan dit de doorslaggevende reden zijn om niet met Northwave in zee te gaan.
Kosten	De kosten blijven gelijk, aangezien er geen veranderingen zijn. Wanneer LogRhythm en AlienVault volledig zijn uitgefaseerd, zullen de kosten dalen.
Tijd	Er hoeft geen investering te worden gedaan in tijd.
Processen	Zolang het uitfaseren van LogRhythm en AlienVault nog niet is voltooid, zal er geen impact zijn op de processen.
Techniek	Zolang het uitfaseren van LogRhythm en AlienVault nog niet is voltooid, zal er geen impact zijn op de techniek.
Beheer	Zolang het uitfaseren van LogRhythm en AlienVault nog niet is voltooid, zal het beheer gelijk blijven.

Tabel 4 Scenario 1

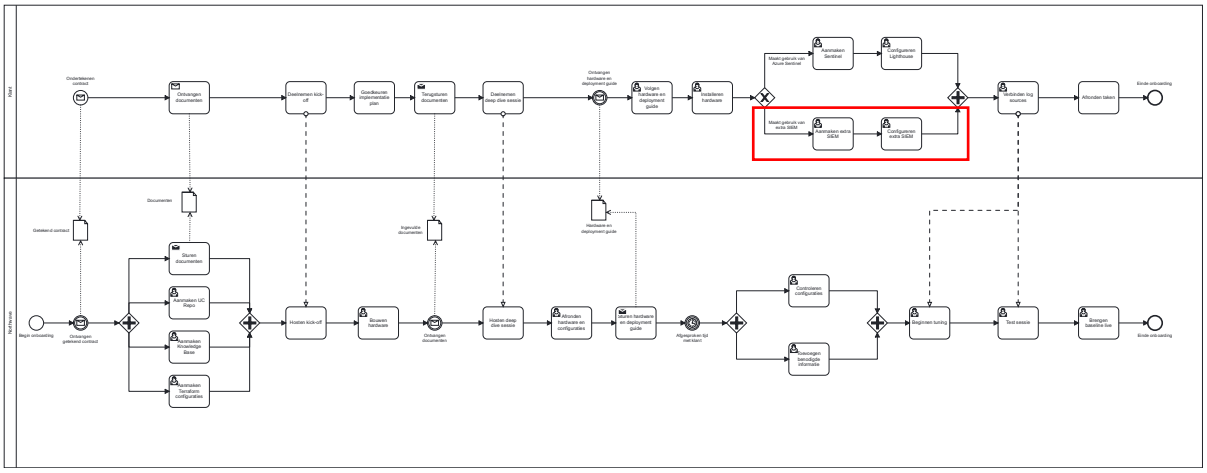
Scenario 2: Multicriteria-analyse winnaar

Omschrijving	Scenario 2 houdt in dat er wordt gekozen voor de SIEM die als beste uit de multicriteria-analyse (MCA) naar voren is gekomen. Het MCA is uitgevoerd op basis van verschillende criteria waaraan een SIEM volgens Northwave moet voldoen. IBM heeft in het MCA een score van 5,300 gekregen en is daarmee als beste uit de analyse gekomen. In dit scenario wordt IBM QRadar als extra SIEM aangeschaft. Hierdoor is Northwave minder afhankelijk van Microsoft en is de kans op vendor lock-in klein. Daarbij kan Northwave potentiële klanten naast Azure Sentinel een tweede mogelijkheid (IBM) aanbieden. IBM is tevens een "leader" in het Gartner Magic Quadrant en staat goed aangeschreven. Echter, bestaat de kans op weerstand onder verschillende Northwavers, aangezien een aantal slechte ervaringen hebben met IBM.
Kosten	De jaarlijkse kosten voor IBM QRadar zijn naar verwachting €125.000,- per jaar exclusief BTW. Hierbij wordt rekening gehouden met drie klanten à 2000 Events Per Second (EPS), dus 6000 EPS in totaal. Dit is slechts een indicatie en de daadwerkelijke kosten kunnen hoger of lager uitvallen. Als serviceprovider is er een "ESA-contract" beschikbaar, wat Northwave in staat stelt om de technologie van IBM "onder de motorkap" in hun eigen service aan te bieden. Dit contract wordt afgesloten voor een bepaald termijn; gedurende dat termijn liggen de prijzen vast, ongeacht IBM's tussentijdse prijsaanpassingen.
Tijd	Er moet een investering worden gedaan in tijd, om zowel het kennisniveau te verhogen als de SIEM te implementeren. Tevens is het nodig om tijd te steken in de wijzigingen met betrekking tot het onboarding proces.
Processen	In figuur 1 is te zien dat de Security Operations Center analist een extra keuze heeft met betrekking tot het kiezen en afhandelen van een alarm. Bij het onboarding proces wijzigt in principe ook één ding, zoals te zien is in figuur 2. De klant heeft keuze tussen Azure Sentinel of IBM (de extra SIEM). Op het gebied van processen zal de impact niet heel groot zijn.
Techniek	Figuur 3 laat zien dat er na het genereren van alarmen extra informatie wordt opgehaald van Azure Sentinel of IBM (de extra SIEM). Zoals in figuur 4 is te zien, moeten de baseline use cases, playbooks en deployments worden herschreven. Tot slot moeten nieuwe use cases worden geschreven. Op het gebied van techniek zal de impact wat groter zijn.
Beheer	IBM QRadar is een Cloud SIEM, waardoor het beheer naar verwachting grotendeels bij IBM zal liggen. Hierdoor zal er niet veel beheerwerk bijkomen. Wanneer LogRhythm en AlienVault zijn uitgefaseerd, is het beheerwerk zelfs minder wanneer IBM QRadar wordt geïmplementeerd.

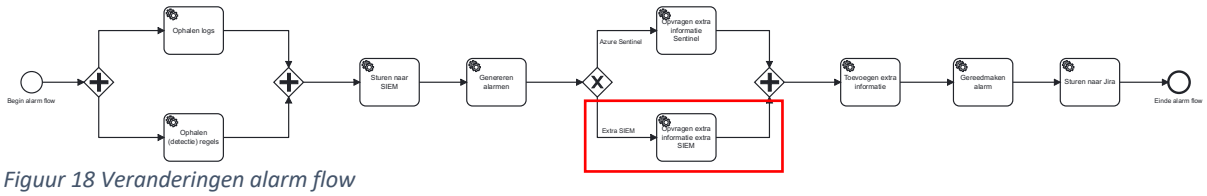
Tabel 5 Scenario 2



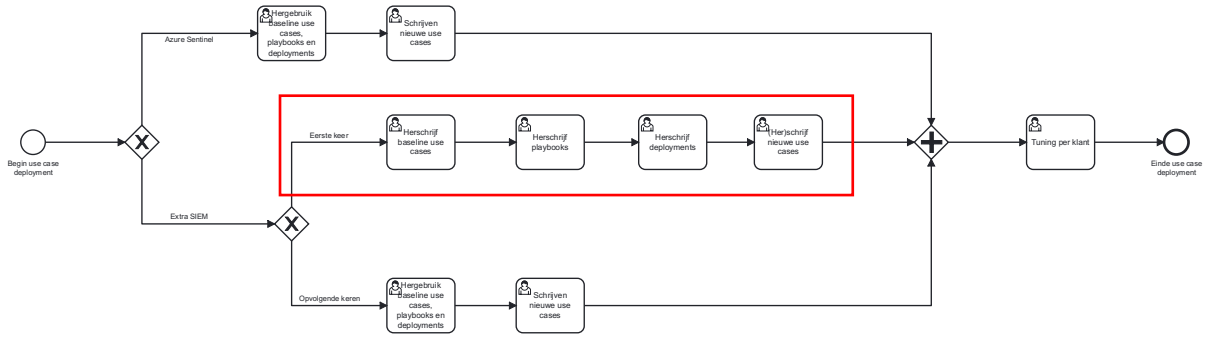
Figuur 16 Veranderingen SOC-analist



Figuur 17 Veranderingen onboarding proces



Figuur 18 Veranderingen alarm flow



Figuur 19 Veranderingen use case deployment

Scenario 3: Persoonlijke keuze op basis van multicriteria-analyse top 3

Omschrijving	Scenario 3 houdt in dat er wordt gekozen voor de persoonlijke keuze die is gemaakt op basis van de top 3 uit de MCA. De persoonlijke keuze van de afstudeerder is om voor Elastic te kiezen. In 2020 stond Elastic niet in het Magic Quadrant, in 2021 behoorde het tot de “niche players” en in 2022 is Elastic een “visionary” in het Gartner Magic Quadrant. Hiermee is te zien dat Elastic een goede ontwikkeling en groei doormaakt en dat er potentie in zit. Tevens wordt Elastic steeds populairder onder bedrijven en staat het goed aangeschreven. In dit scenario wordt Elastic Security als extra SIEM aangeschaft. Hierdoor is de kans op vendor lock-in kleiner en kan Northwave potentiële klanten een tweede SIEM-mogelijkheid aanbieden.
Kosten	Er is geen offerte van Elastic ontvangen, maar de prijsindicatie varieert tussen de $0,5174 per uur en minimaal $175 per maand.
Tijd	Northwave maakt momenteel gebruik van Elasticsearch voor de database van de alarmen, waardoor de Engineers al wat kennis en ervaring hebben met Elastic. Er moet echter wel tijd worden geïnvesteerd om het kennisniveau van het gehele Blue Team te verhogen en de SIEM te implementeren. Daarbij moet tijd worden gestoken in het wijzigen van het onboarding proces. In vergelijking met scenario 2 is een kleinere tijdsinvestering benodigd wanneer er wordt gekozen voor Elastic.
Processen	In dit scenario zal de impact op de processen niet heel groot zijn. Zoals in figuur 1 is te zien, heeft de SOC-analist een extra keuze bij het kiezen en afhandelen van een alarm. In figuur 2 is te zien dat bij het onboarding proces in principe één ding wijzigt. De klant heeft keuze tussen Azure Sentinel of Elastic (de extra SIEM).
Techniek	In vergelijking met de processen zal de impact op de techniek groter zijn. Figuur 3 laat zien dat er na het genereren van alarmen extra informatie wordt opgehaald van Azure Sentinel of Elastic (de extra SIEM). In figuur 4 is te zien dat het noodzakelijk is om de baseline use cases, playbooks en deployments te herschrijven. Tevens moeten nieuwe use cases worden geschreven.
Beheer	Het beheer zal naar verwachting grotendeels bij Elastic liggen, aangezien Elastic Security een Cloud SIEM is. Hierdoor zal er niet veel beheerwerk bijkomen. Wanneer LogRhythm en AlienVault volledig zijn uitgefaseerd, is het beheerwerk minder wanneer Elastic Security wordt geïmplementeerd.

Tabel 6 Scenario 3

Advies

LogRhythm en AlienVault zijn momenteel aan het uitfaseren, waardoor Northwave alleen Azure Sentinel als SIEM overhoudt. Hierdoor is Northwave zeer afhankelijk van Microsoft. Als hier niks aan wordt gedaan, dan is de kans op vendor lock-in reëel. Het voordeel van geen tweede SIEM aanschaffen is dat het heel veel tijd, geld en moeite scheelt. Er hoeft namelijk geen tijdinvestering te worden gedaan om meer kennis te vergaren. Tevens blijven de kosten gelijk en wanneer het uitfaseren voltooid is, zullen de kosten zelfs lager worden. Op vendor lock-in na, is er ook een kans dat Northwave potentiële klanten misloopt. Als een bedrijf een sterke voorkeur heeft om Microsoft-producten te vermijden, kan dit de doorslaggevende reden zijn om niet met Northwave in zee te gaan.

Uit het analyseverslag is gebleken dat Azure Sentinel nog steeds het beste past bij Northwave op basis van de verzamelde criteria. Uit het MCA blijkt dat IBM van alle andere onderzochte SIEM's het beste alternatief is voor Azure Sentinel. Echter, scoort IBM op alle vlakken even goed of minder dan Sentinel. Het aanschaffen van IBM kan de gedachte wekken dat het geen toegevoegde waarde heeft. Dit is echter niet terecht, aangezien Northwave niet verder afhankelijk wil zijn van Microsoft en vendor lock-in wil voorkomen. Dus zelfs als IBM QRadar volgens het MCA niet beter is dan Azure Sentinel, kan het alsnog de moeite waard zijn om hem aan te schaffen. Helaas hebben een aantal Northwavers minder prettige ervaringen met dit product, wat kan leiden tot weerstand. Tevens heeft een Northwaver gewerkt bij een bedrijf waar IBM werd uitgefaseerd, omdat het te duur is en volgens dat bedrijf niet de beste op de markt is.

Volgens het MCA heeft Northwave momenteel van de grote bekende vendors de beste SIEM. Hierdoor kan het aantrekkelijk zijn om naar de opkomende vendors te kijken. Elastic is in het Gartner Magic Quadrant een "visionary", maar scoort op veel vlakken even goed of iets minder dan Sentinel. Er lijkt veel potentie in Elastic te zitten, met name doordat een aantal producten van Elastic door andere grote bedrijven wordt gebruikt. Bedrijven zoals Amazon, Microsoft en Docker maken allen gebruik van Elasticsearch. Daarbij maken onder andere Slack en Cisco gebruik van Elastic Security. Northwave maakt zelf ook gebruik van Elasticsearch, de engineers hebben dus al kennis en ervaring met Elastic. Dit kan ervoor zorgen dat er minder weerstand is, wanneer er voor Elastic Security als SIEM wordt gekozen. Tevens is de tijdsinvestering in kennis minder lang in vergelijking met het aanschaffen van IBM.

Op basis van alle verzamelde informatie is de conclusie getrokken dat zowel IBM als Elastic beide goede en geschikte opties zijn. Echter, is het advies om voor scenario 3 te gaan en Elastic Security aan te schaffen. De kans op weerstand onder Northwavers is naar verwachting een stuk kleiner en er is al wat kennis en ervaring met Elasticsearch, waardoor er een hogere gebruikersadoptie is. Tot slot zorgt het aanschaffen van Elastic Security ervoor dat de kans op vendor lock-in kleiner is.

5 Beantwoording hoofd- en deelvragen

In dit hoofdstuk wordt eerst antwoord gegeven op de deelvragen en vervolgens wordt antwoord gegeven op de hoofdvraag.

Deelvraag 1: "Wat is een SIEM?"

Een Security Information and Event Management (SIEM) is een reeks technologieën. Met een SIEM is het mogelijk om bedreigingen te detecteren en log events en andere gegevens uit bronnen te analyseren. Ook het naleven en beheren van security incidenten door het verzamelen en analyseren van security events behoort tot de mogelijkheden.

Deelvraag 2: "Wat zijn de requirements van Northwave waaraan een SIEM moet voldoen?"

De behoeftes van de manager van het Blue Team zijn in de beantwoording van deze deelvraag meegenomen.

#	Requirement/Behoefte	MoSCoW prioritering
1.	Meerdere klanten bedienen	Must
2.	API voor management en detectieregels (automatiseren)	Must
3.	Casemanagement uit de SIEM kunnen in een externe tool.	Must
4.	Logging verwerken vanuit cef, syslog en Windows events.	Must
5.	Het is integreerbaar met Jira en andere technologieën.	Must
6.	Gedegen en trainbaar voor het team (korte doorlooptijd).	Must
7.	Uitgebreide query taal.	Must
8.	Goede zoekfunctionaliteiten.	Must
9.	Goede mogelijkheden voor allow en deny listen.	Must
10.	Oorspronkelijke (raw) data is aanwezig.	Must
11.	Ondersteuning vanuit het product.	Must
12.	Staat goed aangeschreven (Gartner Magic Quadrant).	Must
13.	Flexibel te bedienen, niet gebonden aan veel restricties.	Must
14.	Kwalitatieve mogelijkheden van detectie	Must
15.	Prijs aanschaf en licentiestructuur	Must
16.	Onderhoud (functioneel)	Must
17.	Operational fit (processen)	Must
18.	Security van de SIEM	Must
19.	Stabiliteit van de tool	Must
20.	Rapportage aanmaken per klant.	Should
21.	Verwerkte logging is gekoppeld aan Cloud services.	Should
22.	Minimum threshold van 2000 logs/seconde.	Should
23.	Informatie over apparaten en gebruikers over alle logging worden gecorreleerd.	Should
24.	De SIEM is in het Engels.	Should
25.	Cloud SIEM.	Should
26.	Goede normalisatie.	Should
27.	Eenvoudig te implementeren.	Should

28.	SIEM met log databronnen, opslag, data enrichment, gebruikersinteractie, automatisering, gedragsanalyse en exporteren van log data	Should
29.	Kennisopbouw	Should
30.	Onderhoud (technisch)	Should
31.	Toekomst/roadmap SIEM	Should
32.	Support SIEM provider	Should
33.	Innovatie	Should
34.	Rapportages zijn opvraagbaar via de API.	Could
35.	Cloud solution moet gehost zijn binnen de EU.	Could
36.	Gebruiker is direct af te sluiten of te blokkeren.	Could
37.	Het liefst een self-managed Cloud SIEM (SaaS).	Could
38.	Datakwaliteit is goed.	Could
39.	Goede exportfunctionaliteiten.	Could
40.	Logstash wordt ondersteund.	Could
41.	Databronnen zijn eenvoudig toe te voegen.	Could
42.	Goed te koppelen met MISP.	Could
43.	Single Sign-On voor de analisten.	Could

Tabel 7 Behoeftes m.b.t. een SIEM

Deelvraag 3: "Welke alternatieven zijn er voor Azure Sentinel die voldoen aan de requirements van Northwave?"
IBM, Exabeam, Elastic, Sumo Logic, Rapid7, Splunk, Securonix, Devo, Fortinet en Micro Focus zijn allemaal geschikte alternatieven voor Azure Sentinel die voldoen aan de requirements van Northwave. Hierbij is de volgorde aangehouden die op basis van de uitgevoerde multicriteria-analyse (MCA) naar voren is gekomen. IBM is volgens het MCA de meest geschikte alternatief en Micro Focus de minst geschikte.

Deelvraag 4: "Wat zijn de verschillen en overeenkomsten van de alternatieven ten opzichte van Azure Sentinel?"
Voor het beantwoorden van deze deelvraag is onderzoek gedaan naar de top drie meest geschikte SIEM's volgens de multicriteria-analyse. De top drie bestaat uit: IBM, Exabeam en Elastic. Op basis van de MCA scoort IBM op iedere behoefte gelijk of minder dan Azure Sentinel. Exabeam scoort alleen op het gebied van ondersteuning vanuit het product beter, voor de rest scoort Exabeam gelijk of minder in vergelijking met Azure Sentinel. Elastic scoort op iedere behoefte gelijk of minder dan Azure Sentinel. Hierbij wordt wel de kanttekening geplaatst dat Sentinel volgens het Gartner Magic Quadrant een leader op de markt is en Elastic een visionary.

Deelvraag 5: "Wat is de impact op de bestaande omgeving, op het gebied van zowel processen als techniek?"
De impact op de bestaande omgeving, op het gebied van zowel processen als techniek is afhankelijk van het team.

Uit de impactanalyse is gebleken dat de impact van een extra SIEM voor het CERT gering is. Op het gebied van processen zal de impact voornamelijk op het kennisniveau zijn, met name hoe er door data gezocht moet worden. Op het gebied van techniek is nauwelijks overlap.

Voor het blue team in het algemeen is de omvang van de veranderingen groot. Op het gebied van de processen moet binnen het blue team kennis worden opgebouwd. Daarbij moet de aansluiting van de nieuwe SIEM worden onderzocht en detectieregels worden gebouwd. De capaciteit moet tevens worden opgebouwd en het moet mogelijk zijn om de kosten door te belasten. Op het gebied van techniek moeten mensen stoppen met waar ze mee bezig zijn en zich focussen op het werkend krijgen van de hele infrastructuur. Verder moeten ook parses, connecties en configuratiescripts worden gebouwd.

De impact voor het SOC OPS zal voornamelijk zijn op kennisniveau, waarbij de veranderingen voor het SOC OPS tevens invloed gaat hebben op het cognitief vermogen van de analisten.

Voor de detection quality & stack engineers is de omvang van de veranderingen groot. Op het gebied van processen moeten mensen dubbel worden getraind. Op het gebied van techniek zullen de engineers vooral druk zijn met het uitzoeken hoe ze moeten communiceren met, en configureren van het systeem.

Voor de service delivery engineers is de omvang van de wijzigingen groot. Op het gebied van processen geldt dat hoe ingewikkelder een SIEM koppelt, hoe meer impact dit heeft op de processen. Op het gebied van techniek moeten een aantal zaken worden herschreven. Daarbij moeten alle werkzaamheden in alle waarschijnlijkheid twee keer uitgevoerd worden: dit geldt voor zowel de huidige- als de nieuwe SIEM.

Uit het High-Level Design is gebleken dat de impact op de processen “SOC OPS shift” en “onboarding proces Engineers” klein is. In beide gevallen komt een extra keuze erbij en hetzelfde geldt voor de “alarm flow” techniek. Voor de “use case deployment” techniek is de impact wat groter. Bij het gebruik van een extra SIEM moeten de baseline use cases, playbooks en deployments worden herschreven. Echter, kunnen deze daarna iedere keer worden hergebruikt zoals het momenteel bij Azure Sentinel het geval is.

Hoofdvraag: “Wat is voor Northwave het beste alternatief voor Azure Sentinel met in achtneming van de requirements?”
Er zijn twee SIEM’s geschikt als mogelijk alternatief voor Azure Sentinel, IBM QRadar en Elastic Security. In beide gevallen zorgt de aanschaf ervoor dat de kans op vendor lock-in kleiner is.

Uit het multicriteria-analyse is gebleken dat IBM QRadar het beste alternatief is voor Azure Sentinel met in achtneming van de requirements. IBM scoorde het beste in vergelijking met de overige tien alternatieven. IBM is al een aantal jaar een “leader” in het Gartner Magic Quadrant en doet het in dat opzicht zeer goed. Het nadeel van IBM dat een probleem voor Northwave kan vormen is weerstand onder Northwavers. Een aantal Northwavers hebben aangegeven dat zij minder prettige ervaringen hebben gehad met dit product. Tevens heeft een Northwaver gewerkt bij een bedrijf waar IBM werd uitgefaseerd omdat het te duur is en volgens dat bedrijf niet de beste op de markt is.

Op basis van de verschillende interviews met de stakeholders en dit onderzoek is de persoonlijke voorkeur van de studente om voor Elastic Security te gaan. Uit het multicriteria-analyse kwam Elastic Security als derde naar voren. In het Gartner Magic Quadrant is Elastic een “visionary”, maar scoort volgens het MCA op veel vlakken even goed of iets minder dan Sentinel. Daarbij gebruikt Northwave Elasticsearch, waardoor de engineers al kennis en ervaring hebben met Elastic. Dit leidt tot een hogere gebruikersadoptie en minder weerstand. Tevens is de tijdsinvestering in kennis minder lang in vergelijking met het aanschaffen van IBM.

6 Discussie

Uit de resultaten van het multicriteria-analyse is de volgende top drie naar voren gekomen. Op de eerste plaats staat IBM, op de tweede plek Exabeam en tot slot Elastic. Dit resultaat kwam niet overeen met de verwachting dat Splunk en Rapid7 hoger in de top zouden staan. Deze verwachting is geschept doordat er op sociale media veel te lezen is over Splunk. Rapid7 is de SIEM die bij het vorige stagebedrijf is gebruikt. Een mogelijke verklaring voor dit resultaat is dat de criteria die gebruikt zijn in het MCA specifiek voor Northwave is en dat andere bedrijven andere criteria gebruiken tijdens het aanschaffen en kiezen van een SIEM. Met dit resultaat is aangetoond dat het onderzoek onbevooroordeeld en correct is uitgevoerd.

Dit onderzoek is onderhevig aan diverse beperkingen. Deze worden beknopt beschreven en zijn als volgt.

Alleen Gartner Magic Quadrant SIEM's
Tijdens het beantwoorden van deelvraag 3: "Welke alternatieven zijn er voor Azure Sentinel die voldoen aan de requirements van Northwave?" zijn enkel de SIEM's die in het Gartner Magic Quadrant staan meegenomen. Hetzelfde geldt voor de multicriteria-analyse. Als tijdens het onderzoek ook SIEM's waren meegenomen die niet in het Gartner Magic Quadrant staan, was er wellicht een andere uitkomst geweest. Hierbij wordt wel de kanttekening geplaatst dat Northwave zelf aangaf dat zij graag wilde dat de SIEM goed stond aangeschreven en het liefst ook in het Gartner Magic Quadrant te vinden was.

Criteria manager Blue Team niet meegenomen
De behoeftes van Jochem Smit (manager van het Blue Team) zijn niet meegenomen tijdens het uitvoeren van de multicriteria-analyse. De oorzaak hiervan is dat de ingevulde vragenlijst net te laat was ontvangen en de MCA was al klaar. Als deze criteria wel op tijd waren ontvangen, dan was er wellicht een andere top drie uitgekomen.

Theoretische opdracht
De afstudeeropdracht was een theoretische opdracht, waardoor het lastig was om een concreet advies te geven. Het advies is gebaseerd op de gevonden literatuur en deze literatuur is niet gericht op de werkelijke situatie van Northwave, maar meer op de algemene best practices en de algemene infrastructuur.

Geen Proof of Concept (PoC)
Het maken van een PoC viel gedurende het afstuderen buiten de scope. Hierdoor is er niet diep ingegaan op de techniek en is het niet met zekerheid te stellen dat Elastic Security compatibel is met het Northwave infrastructuur. Als er wel een Proof of Concept was gemaakt, dan kon er met meer zekerheid worden gesteld of Elastic te implementeren is.

Criteria MCA
Uit de stakeholderanalyse zijn een aantal functies van stakeholders naar voren gekomen. De stakeholderinterviews zijn uitgevoerd met de medewerkers die momenteel deze functie beoefenen. Het resultaat is hierdoor een momentopname. Hetzelfde onderzoek op een later moment opnieuw uitvoeren, kan tot andere criteria in de multicriteria-analyse leiden. Andere criteria leidt mogelijk tot een ander resultaat.

6.1 Evaluatie
Volgende keer zou ik een combinatie van Prince2 en Scrum uitvoeren. Tijdens het afstuderen heb ik gemerkt dat ik een sprint pas wilde eindigen wanneer mijn product daadwerkelijk af was. Dit is niet geheel volgens de regels van Scrum, waar de lengte van de sprints altijd een vaste lengte moeten hebben. Bij Prince2 wordt gewerkt met fases, deze zijn flexibel van lengte. Het gebruik van een Scrumbord vond ik erg prettig werken, aangezien ik dan een goed overzicht had over wat ik nog moest doen, wat ik aan het doen was en wat al was afgerond.
Door Prince2 met Scrum te combineren, maak ik gebruik van het beste van beide methodes.

Met ongelimiteerde tijd had ik ook een Proof of Concept gemaakt, zodat ik het in de praktijk had kunnen testen en een sterker advies had kunnen geven.

6.2 Aanbevelingen vervolgonderzoek
Gedurende het onderzoek zijn een aantal aspecten niet onderzocht, enerzijds omdat het buiten de scope viel en anderzijds vanwege de beschikbare tijd. Daarom wordt aanbevolen om meer onderzoek te doen naar de volgende zaken. Deze aanbevelingen zijn gericht op Elastic Security, maar zijn ook toepasbaar op een andere SIEM vendor.

<u>Compatibiliteit met Northwave infrastructuur</u>
Het is sterk aan te raden om onderzoek te doen naar de compatibiliteit van Elastic Security met het Northwave infrastructuur om zeker te zijn dat het mogelijk is om deze SIEM te implementeren.

<u>Roadmap SIEM</u>
Een van de criteria van de manager van het Blue Team (Jochem Smit) was om naar de roadmap van de SIEM te kijken. Tijdens het maken van het MCA zijn deze criteria niet meegenomen, aangezien het net te laat was ontvangen. Het is echter wel belangrijk om dit te doen, aangezien het dan duidelijk is wat de toekomstige plannen en ontwikkelingen van Elastic Security zijn. Daarbij kan direct een inschatting worden gemaakt of de toekomst van deze SIEM past bij de toekomstplannen van Northwave.

<u>Prijs aanschaf en licentiestructuur</u>
Om een goed beeld te krijgen van de kosten is het verstandig om de prijzen voor de aanschaf van Elastic Security en de bijbehorende licentiestructuur te onderzoeken. Tevens kan dit helpen bij het bepalen van de rendabiliteit voor het aanschaffen van een tweede SIEM.

Beveiliging van de SIEM

De SIEM wordt gebruikt onder andere gebruikt om de infrastructuur van klanten te monitoren en in een zekere zin te beveiligen. Echter, is het ook belangrijk dat de SIEM zelf goed is beveiligd. Het is aan te raden om onderzoek te doen naar hoe Elastic Security wordt beveiligd.

Northwave guidelines voor vendor criteria

Uit het interview met de manager van het Blue Team (Jochem Smit) is gebleken dat Northwave zijn eigen guidelines voor vendor criteria heeft. Deze guidelines mochten in verband met “Traffic Light Protocol (TLP): Amber” niet gebruikt worden tijdens dit onderzoek. TLP: Amber houdt in dat de informatie binnen het bedrijf moet blijven. Mocht Northwave dit onderzoek gebruiken, dan is het aan te raden om de uitkomsten van het MCA alsnog te verifiëren met deze guidelines.

Bibliografie

ASL Foundation. (z.d.). *Proces Impactanalyse*. Opgehaald van ASL Foundation: https://aslfoundation.nl/model/procescluster-onderhoud-en-vernieuwing/proces-impactanalyse/

Gagné, D., & Ringuette, S. (z.d.). *BPMN Quick Guide; View it.* Opgehaald van BPMN Quick Guide: https://www.bpmnquickguide.com/view-bpmn-quick-guide/

Genau, L. (2021, september 8). *Semigestructureerd of half-gestructureerd interview | Voorbeeld*. Opgehaald van Scribbr: https://www.scribbr.nl/onderzoeksmethoden/semigestructureerd-interview/

HAN, & HVA. (z.d.). ICT Research Methods Pack. HBO-i.

Impres. (z.d.). *Brainstormsessie*. Opgehaald van Impres: https://www.impres.nl/strategie-en-advies/brainstormsessie/#:~:text=Brainstorming%20is%20een%20methode%20die,antwoorden%20verzamelt%20voor%20jouw%20vraagstuk.

insign.it. (z.d.). *High & Low-level Design*. Opgehaald van insign.it: https://www.insign.it/nl/concepts-projects/high-low-level-design

Kooijman, B. (z.d.). *Welke rollen & verantwoordelijkheden zijn er binnen Scrum? (+2min video uitleg).* Opgehaald van Agile Scrum Group: https://agilescrumgroup.nl/rollen-verantwoordelijkheden-scrum/

Marketingscriptie. (z.d.). *Het model van Abell maken en invullen*. Opgehaald van Marketingscriptie: https://www.marketingscriptie.nl/model-van-abell-maken/

Mulder, P. (2018, januari 8). *Handy model*. Opgehaald van Toolshero: https://www.toolshero.nl/management-modellen/handy-model/

Ondreicsik, A. (2021). *Create a stakeholder analysis with the Mendelow matrix | Free template*. Opgehaald van Conceptboard: https://conceptboard.com/blog/stakeholder-analysis-mendelow-matrix/

Scriptium. (2022, maart 31). *Triangulatie in je scriptie-onderzoek? Wat is het precies?* Opgehaald van Scriptium: https://www.scriptium.nl/triangulatie/

van den Bedem, S. (2022, april 26). SIEM afstudeeropdracht. (J. Fan, Interviewer)