Hulp bij het kiezen van een SIEM

Plan van aanpak

Henk-Sjoerd Hinrichs

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

avanade

Document Titel

Project Title	Security Event Consolidation
Author	Avanade: Henk-Sjoerd Hinrichs
Reviewer	Thomas More: Liesbeth Kenens Avanade: Frank Molenaar
Current Version	Release 1.0
File Name	Plan van Aanpak
Publication Date	13-3-20

Revision History

Version	Date	Author	Changes
1.0	13-3-20	Henk-Sjoerd Hinrichs	
2.0	29-3-20	Henk-Sjoerd Hinrichs	Aanleiding, Doelstelling, Opdracht, Planning
3.0	22-4-20	Henk-Sjoerd Hinrichs	Stagebedrijf, Aanleiding, Doelstelling, Methodes en Technieken

Inhoudstabel

1 Stagebedrijf

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 daar ongeveer 400 medewerkers. Deze medewerkers waaronder ook de stagelopers zijn onder verdeelt in de zogeheten Talent Communities (TaCo'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 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 Event Mangement) 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 wat SIEM tooling was. 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. 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 werkt binnen de organisatie van de klant.

3 Opdracht

Om een centraal inzicht te krijgen in security gerelateerde events uit alle verschillende omgevingen is een klant van Avanade op zoek naar een centrale oplossing.

De oplossing moet in staat zijn de security gerelateerde events van verschillende Azure subscriptions samen te voegen en te analyseren, en eveneens van gehoste infrastructuur bij 3de partijen en on-premises netwerkapparatuur.

De security officer van de organisatie heeft behoefte naar een analyse van de mogelijkheden van Azure Sentinel in vergelijk met Splunk. Hierbij spelen ook de licentie kosten en complexiteit van implementatie een rol.

In deze opdracht vragen we je om na te denken en uit te zoeken hoe Azure Sentinel zich verhoudt tot een product zoals Splunk en in welke mate deze producten de organisatie inzichten kan bieden in de verschillende gerelateerde events uit verschillende Azure subscriptions, on-premises hardware en services bij nog andere cloud providers.

Breng op basis van je onderzoek een advies uit en beschrijf een referentie architectuur met stappenplan voor implementatie.

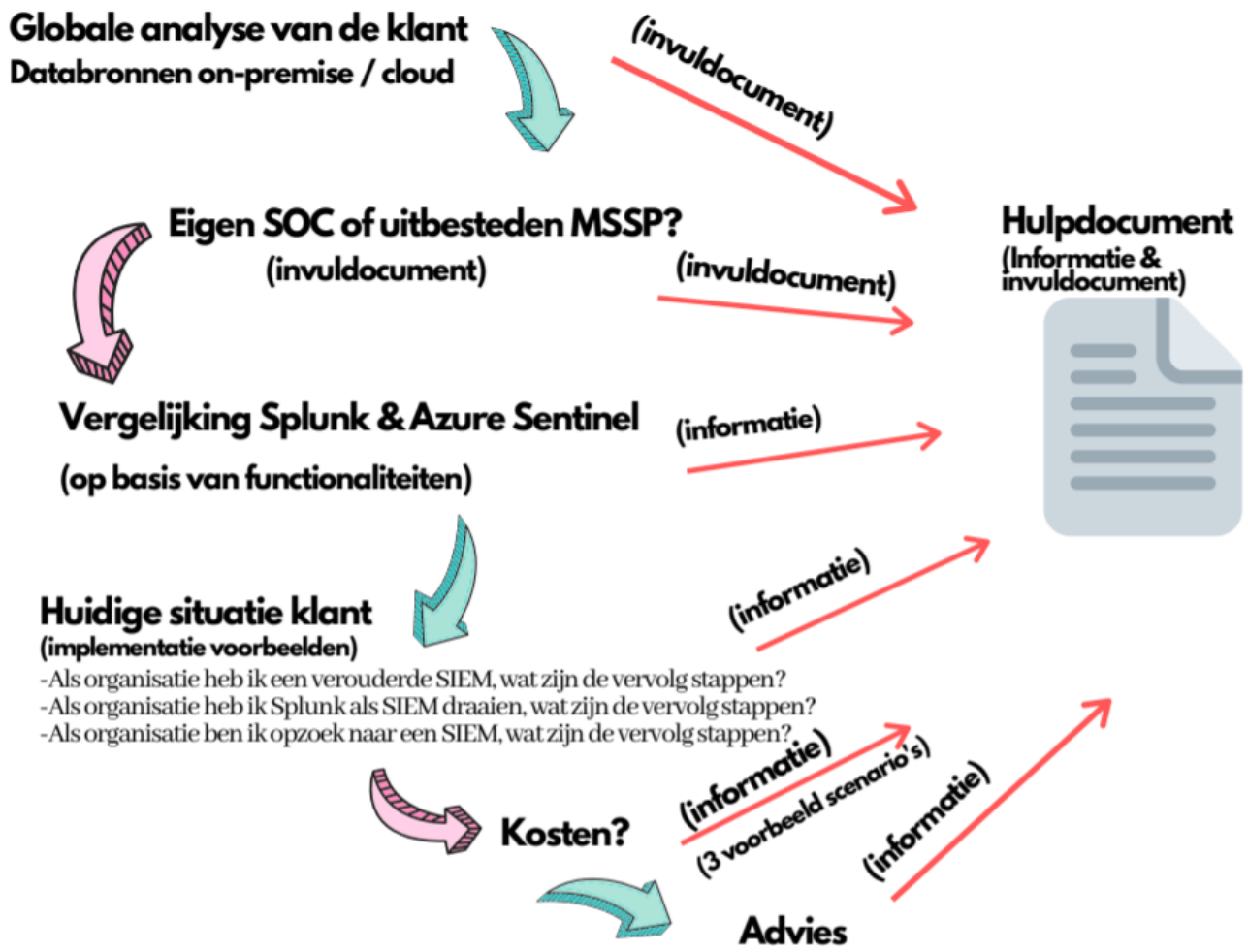
4 Doelstelling

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 advies op de vraag; ''Is een organisatie instaat een SOC intern te bouwen en onderhouden?", en het hulpdocument "Moet inzicht geven in het keuzeproces 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 IT gerelateerde zaken een aantal feiten over de organisatie samenbrengen in het hulpdocument. Deze analyse geeft de consultant een globaal overzicht van de organisatie.

Voordat er een SIEM gekozen kan worden moet het duidelijk zijn welke data de organisatie in de SIEM wil injecteren. Ik zal opzoek gaan naar een manier om de data van de klant in kaart te brengen.

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 voor de klant inzichtelijk?"** 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 bekijken en uitwerken. De drie scenario's staan opgesomd in de derde deelvraag.

5 Methodes & Technieken

5.1 Onderzoeksmethode

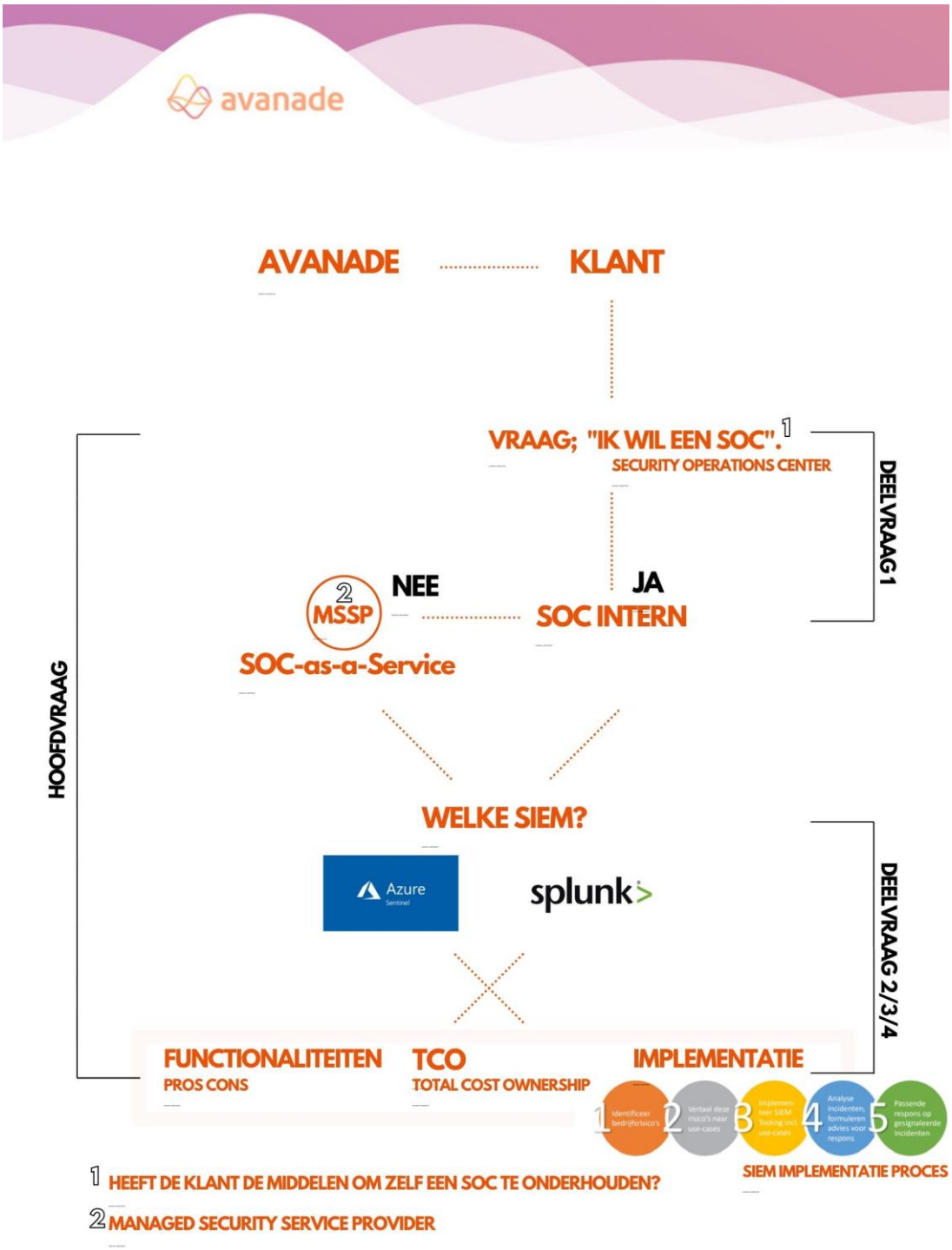
De meeste informatie zal verworven worden door een literatuuronderzoek. Verschillende collega's bij Avanade hebben goede kennis van Azure Sentinel en Splunk zowel in Nederland als internationaal. Ik zal met verschillende mensen in gesprek gaan voor advies, om vragen te stellen en daardoor kennis op te doen. De deelvragen zal ik beantwoorden door middel van bronnen op het internet en interviews.

De hoofdvraag die ik heb opgesteld; **'Hoe maakt de consultant van Avanade het proces voor het kiezen van een SIEM voor de klant inzichtelijk?'** 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 te houden) en voor welke organisaties is het verstandig om te kiezen voor een MSSP?	Literatuuronderzoek, vergelijkbaar onderzoek	Een invuldocument die 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 opzoek 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?

Om mijn hoofdvraag en deelvragen duidelijk te krijgen heb ik er een visuele component aangehangen. Door middel van een flowchart probeer ik iets meer inzicht te krijgen in mijn eindproduct.

(Deelvraag 1) -> We lezen van boven naar onder. De klant heeft een vraag. De klant wil een Security Operations Center. Het is de vraag of het bedrijf een eigen SOC wil laten bouwen of dat het bedrijf beter kan kiezen voor MSSP. eiden oplossingen kunnen aangeboden worden door Avanade.



(Deelvraag 2/3/4) -> Nadat de beslissing SOC intern/ SOC-as-a-Service is gemaakt kennen we gedeeltelijk de behoeften en de manier van werken van het bedrijf. Deze basiskennis kunnen we meenemen voor het kiezen van de juiste SIEM-oplossing.

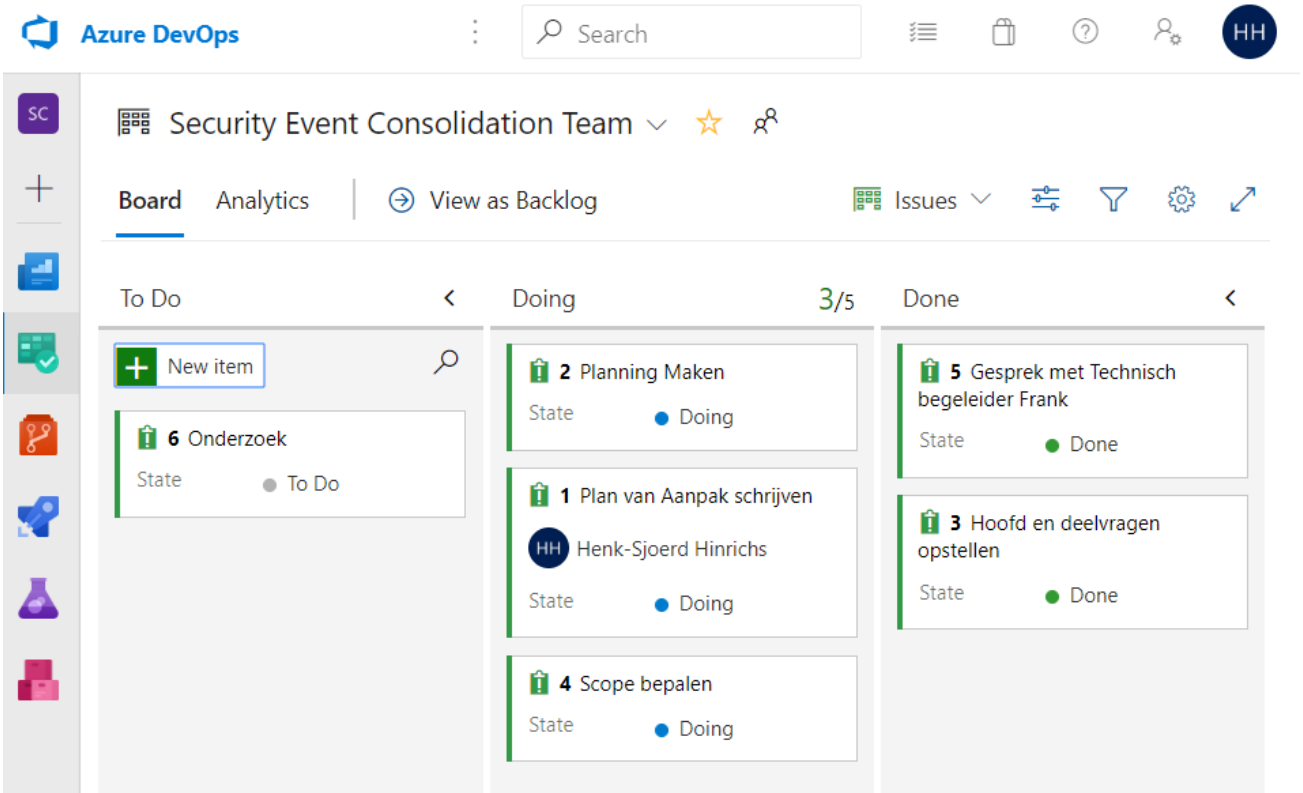
Om meer de diepte in te gaan zal ik onderzoek doen naar de functionaliteiten, Total Cost Ownership en de implementatie op basis van een gebouwde architectuur.

5.2 Projectmethode

Tijdens dit project zal ik Azure DevOps gebruiken voor een agile manier van werken. Binnen Azure DevOps bevindt zich Azure Boards. Dit is een plaats voor het plannen, bijhouden en bespreken van werkzaamheden. Ingebouwde scrumborden en planningshulpmiddelen helpen bijvoorbeeld bij het uitvoeren van sprints en het inplannen van vergaderingen. Azure Boards ondersteunt tracking met de Kanban-methode, backlogs, teamdashboards en custom reporting. [1]

Het is belangrijk dat ik dit project uitvoer in een Agile omgeving, omdat hierbij flexibel werken wordt ondersteund. Tijdens dit project zal ik bijsturen waar nodig en deze agile manier van werken leent zich daar goed voor.
In Azure Boards wordt gewerkt met een Kanban bord. In dit bord wordt een overzicht gegeven van de huidige status van het project.

Hieronder zien we een Collapse All titel, waar alle User stories onderstaan.
Daarnaast zijn er drie fases. De eerste is ***To Do***, de tweede is ***Doing*** en de laatste is ***Done***.



[1] David Oomen (Azure DevOps: niet alleen voor Microsoft developers).
Opgehaald van: https://www.computable.nl/artikel/blogs/cloud-computing/6530085/5260614/azure-devops-niet-alleen-voor-microsoft-developers.html

5.3 Technologieën

Ik zal voor dit project gebruik maken van Microsoft Azure. Binnen Microsoft Azure zal ik werken met Azure Security Center waarbinnen de SIEM valt van Azure genaamd Azure Sentinel. Hier zal ik mij vooral verdiepen in de mogelijke functionaliteiten en ik zal ermee werken als ik de PoC architectuur ga ontwerpen. Ook ga ik werken met Splunk om daar eveneens opzoek te gaan naar de mogelijke functionaliteiten en eveneens het ontwerpen van PoC architectuur.

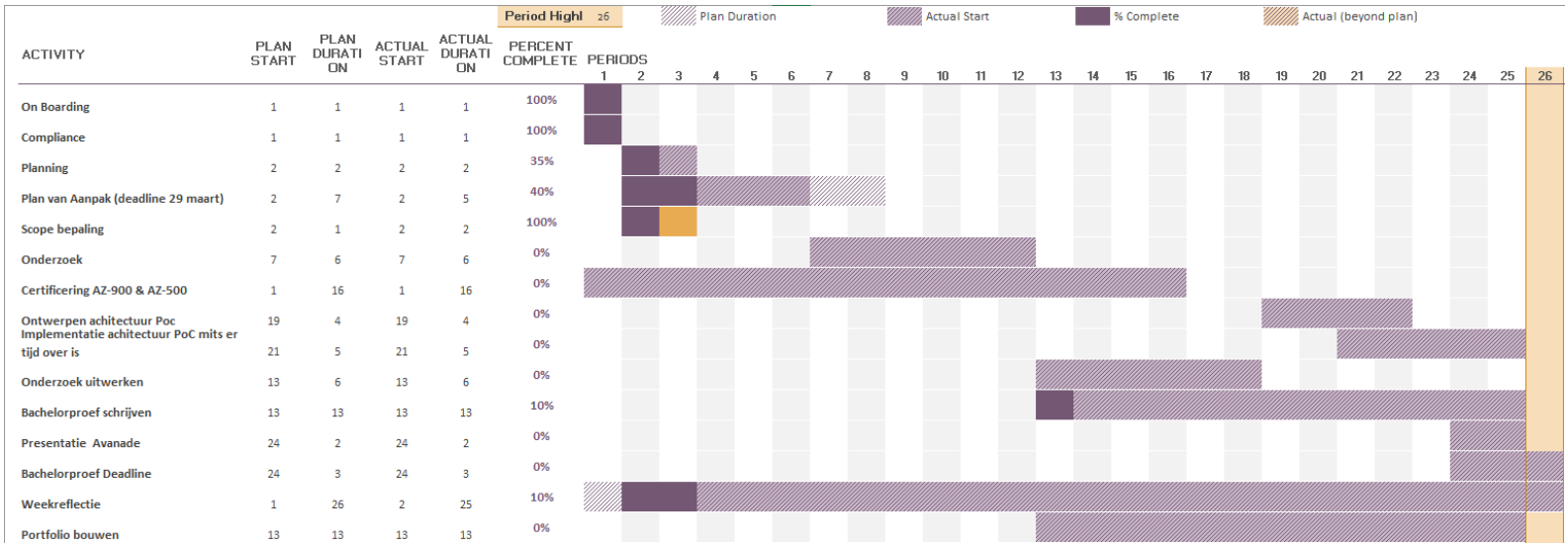
Daarnaast zal ik Azure DevOps gebruiken als projectmethode om een goed overzicht te bewaren in de vordering van het project.

6 Planning

Hieronder staat de globale planning voor de stageperiode. Om mijzelf 'on track' te houden zal ik deze planning goed moeten nastreven en de deadlines die daaraan vasthangen in het oog moeten houden.

Jaar	Maand	Week	Stageweek	Werkzaamheden
		10	1	
		11	2	
		12	3	
	Maart	13	4	On-boarding / Plan van Aanpak / AZ900
		14	5	Onderzoek -> Deelvraag 1 klaar met bijbehorend invuldocument
		15	6	Onderzoek functioniteiten SIEM -> Deelvraag 2
		16	7	Uitwerken functionaliteiten SIEM -> Deelvraag 2 met bijbehorend invuldocument
		17	8	Onderzoek & Uitwerken Implementatie architectuur Deelvraag 3 met bijbehorend invuldocument
	April	18	9	Onderzoek & Uitwerken TCO Deelvraag 4 met bijbehorend invuldocument
		19	10	Invuldocument samenvoegen en flowchart bouwen
		20	11	Onderzoekverslag samenvoegen / achterstanden bijwerken
		21	12	Presentatie Voorbereiden
2020	Mei	22	13	Presentatie Avanade
		23	14	Einde stage/ Controle Portfolio
		24	15	
		25	16	Presentatie Bachelorproef

Hieronder is een Gantt planning te zien in excel. Deze laat gedetailleerder zien hoe de voortgang van mijn project eruitziet. Ik kan in de kolom 'percent complete' aangeven hoeveel procent ik van deze taak al heb voltooid. Tevens kan ik ook aangeven als een deeltaak langer of korter duurt dan de oorspronkelijk planning. Dat zorgt ervoor dat je duidelijk ziet of je tijd over gaat hebben aan het einde of een paar overuren moeten maken om bij te benen.



6.1 Deadlines Thomas More

Een aantal afspraken die met mijn begeleider (Liesbeth Kenens) gemaakt zijn. Elke week maak ik ook een reflectieverslag in de vorm van een video. Deze zal in een gedeelde map zichtbaar zijn voor mijn begeleider.

Datum	Opdrachten
25-3-2020	Plan van Aanpak inleveren
31-3-2020	Presentatie via Skype voortgang project (nr1)
21-4-2020	Presentatie via Skype voortgang project (nr2)
3-6-2020	Link portfolio voor feedback
5-6-2020	Controle portfolio
Elke week	Reflectieverslag uploaden
19/22-6-2020	Bachelorproef presentatie

Risico's

Hier zal ik een aantal risico's uitwerken. Tijdens een project kunnen er problemen optreden. Hier zal worden uitgelegd hoe ik die problemen kan voorkomen.

Risico	Kans	Impact	Voorkomen
De documentatie is niet secuur genoeg geformuleerd.	1	1	Dit zou natuurlijk belangrijk zijn voor de persoon die het advies wil gebruiken voor keuzes. Ik zal het daardoor af en toe laten lezen door een technisch persoon en het zelf regelmatig herlezen.
Ik loop tegen technische problemen aan.	1	2	Vroegtijdig melden en hulp vragen, proactief reageren.
Verhinderd worden in het maken van de stageopdracht door ziekte (Corona bijvoorbeeld).	2	3	Extra tijd reserveren om eventuele problemen te tackelen.
Ik loop achter op schema.	2	2	Het kan zijn dat mijn planning niet helemaal synchroon loopt met huidige stand van zaken. Ik zal de planning dus goed in het oog moeten houden.