Security Event Consolidatie

Reflectie

Bachelor in de Elektronica-ICT
keuzerichting Cloud & Cybersecurity

Henk-Sjoerd Hinrichs

Academiejaar 2019-2020

Campus Geel, Kleinhoefstraat 4, BE-2440 Geel

LID VAN ASSOCIATIE KU LEUVEN

THOMAS MORE

1 INLEIDING

Tijdens mijn bachelor Elektronica-ICT aan de Thomas More-hogeschool krijgen de studenten aan het einde van het 3de jaar de mogelijkheid een stage te doen bij een bedrijf. Deze 13 weken durende stage geeft de student de gelegenheid ervaring op te doen in de bedrijf context. Aan de hand van een opdracht zal de student drie maanden lang werken binnen het stagebedrijf en begeleid worden door een technisch begeleider. Daarnaast heeft de student ook een begeleider vanuit het human resources team voor persoonlijke ontwikkeling en externe vragen. Deze reflectie opdracht zal opgedeeld worden in twee delen. Het eerste deel is een reflectie op de inhoudelijke stageopdracht en de tweede is een reflectie op de student zijn persoonlijke ontwikkeling gedurende de stageperiode. Voordat ik verder ga op de inhoudelijke reflectie van de stageopdracht bij Avanade, zou ik willen omschrijven hoe ik uiteindelijk bij Avanade terecht ben gekomen.

Een stagebedrijf zoeken leek mij de perfecte kans om verschillende bedrijven te leren kennen. Vanaf September 2019 was ik opzoek naar een geschikt bedrijf. Destijds realiseerde ik mij dat ik niet goed wist in wat voor bedrijf ik wou werken en waar ik goed zou passen. Door een selectie te maken van ongeveer 10 bedrijven begon ik mijn zoektocht. Deze 10 bedrijven waren klein, middel en grote bedrijven. Dan praat ik bij 15 personen over een klein bedrijf, 1000 over middel en 40.000 over een groot bedrijf. Eerst had ik een sollicitatie bij een middelgroot internationaal bedrijf in Lissabon. Daar was het nieuwe kantoor van Cloudfare geopend, met enig geluk werd ik door de Chief Security Officer doorverwezen naar een manager in Lissabon. Het eerste gesprek ging goed, maar het tweede deel was een online programmeer opdracht en die bleek in lijn te liggen met de stage opdracht. Ik wou niet mijn focus leggen op programmeren, maar juist op security. Vervolgens had ik sollicitaties bij een grote bank, een kleine cybersecurity bedrijf en een grote IT consultant. Door de diversiteit van verschillende bedrijven te ervaren, puur in het aanwerven en contact met werknemers kreeg ik inzicht in de manier van werken en kon ik inzien waar mijn voorkeur lag. Uiteindelijk heb ik gekozen voor een grote IT consultant genaamd Avanade. Het persoonlijke contact met verschillende medewerkers van Avanade, heeft ervoor gezorgd dat ik voor dit bedrijf heb gekozen. Daarnaast speelde ook mee dat de focus ligt op de ontwikkeling van de student, dat de stageloper de mogelijkheid krijgt certificaten te halen en het internationale karakter van het bedrijf.

2 INHOUDELIJKE REFLECTIE STAGEPROJECT

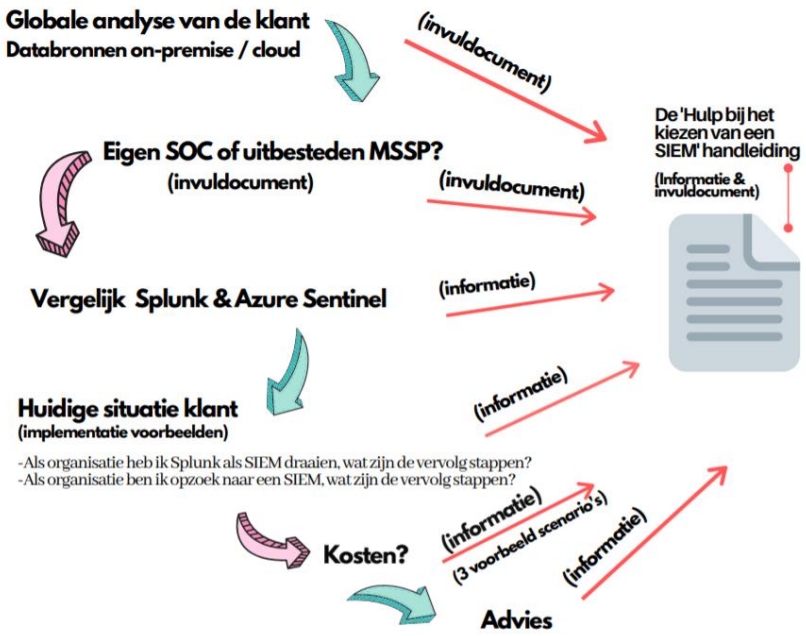
2.1 Wat heb je concreet gerealiseerd? Wat levert dit op voor de organisatie van de opdrachtgever en voor de gebruikers?

Eerst zal ik de stageopdracht toelichten, zodat de lezer de reflectie beter begrijpt. 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 de voorkeur van Avanade bij dit SIEM-product. Voordat Azure Sentinel bestond implementeerde Avanade vaak Splunk. Op dit moment wordt dat nog steeds gedaan, maar moet er een keuze tussen Splunk & Azure Sentinel worden gemaakt. Daarnaast wordt Splunk ook vaak door Accenture geïmplementeerd als SIEM-oplossing. Accenture is het moederbedrijf van Avanade.

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.

Het doel van dit onderzoek is om de consultant van Avanade te helpen bij het maken van keuzes omtrent de SIEM-oplossing. Ik heb gewerkt in de vorm van een handleiding voor de consultant van Avanade. De handleiding zal gedeeltelijk bestaan uit een invul deel, waarin gegevens van de organisatie van de klant worden verwerkt. Daarnaast zal ook een deel van de handleiding informatief zijn in de vorm van tekst en figuren.

Hieronder is de workflow uitgetekend om de handleiding op te bouwen.



De handleiding geeft antwoord 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. 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.

2.2 Huidige situatie stageproject

Het project is afgerond en kan als hulpmiddel gebruikt worden bij de volgende SIEM implementatie. Een aantal van de consultants van Avanade hebben persoonlijk gevraagd naar het document en deze toegestuurd gekregen.

2.3 Advies

Er zijn in het verleden veel implementaties gedaan, veel projecten en daardoor is veel kennis vergaard. Op dit moment zit de kennis in de werknemers, maar deze kennis blijft alleen bestaan binnen de projectgroepen en de mensen die met elkaar samen werken. De kennisdeling wordt op dit moment gedaan via presentaties op de zogenoemde talent community avonden Ik zou voorstellen om te focussen op meer kennisdeling, door middel van een ‘write up’ platform. Dit principen komt voort uit de ‘Capture the Flag’ community die opgeloste opdrachten uitschrijven aan de hand van tekst en screenshots. Als de werknemers na een project een write up schrijven over de bevindingen en oplossingen, dan kunnen de andere Avanade collega’s dit lezen en hier kennis uit putten. De write up database zal zich vullen met veel verschillende projecten, maar oude projecten kunnen ook als basis worden gebruikt om oplossingen te vinden voor nieuwe projecten. Dit write up platform zorgt er dan automatisch voor dat kennis behouden blijft en teruggekeken kan worden op eerdere successen. De handleiding die ik zelf heb geschreven is ook een soort write up van mijn scriptie. De kennis uit de handleiding kan gebruikt worden door andere Avanade collega’s.

3 PERSOONLIJKE REFLECTIE

3.1 Persoonlijke ontwikkeling

Stagelopen is de eerste stap naar een volwassen baan. De collega's om je heen verwachten dat je verantwoordelijk bent voor je eigen taken. Als er een probleem is moet jij zelf aan de bel trekken. Het vergt verantwoordelijkheid en eigen initiatief, dat zijn twee componenten die goed bijdragen aan de overstap richting mijn eerste baan. Tijdens mijn stage heb ik veel mensen leren kennen. Een groep van 25 stagelopers, daarnaast de mensen van human resources, recruitment, begeleiding, verschillende mensen van mijn talent community. Ik bouwde al snel een netwerk aan mensen op die ik af en toe spreekt. Tijdens de corona werkte wij veel met Microsoft teams voor meetings, gesprekken en lezingen. Daarin zit wel het nadeel dat je niemand meer treft tijdens een kopje koffie vanwege Covid19. Het is nodig zelf het initiatief te nemen en in contact te komen met collega's. Weliswaar ging dit goed. De bereidheid van mede collega's om even te bellen was groot. Als ik hulp zocht om verschillende redenen dan kreeg ik die vaak redelijk snel.

Een security architect van Avanade waar ik wel vaker wat vragen aan stelde vroeg vorige week nog wat mijn vervolg plannen zijn, waarop ik antwoorde; "ik zou het interessant vinden een baan te hebben als consultant met de focus op security". Ze stelde voor om te bellen en erover te sparren, aangezien ze veel in de security heeft gewerkt kan ze haar visie en ervaring delen. Ze stelde voor een open gesprek te hebben over de mogelijkheden voor mij. Dat waardeer ik enorm en dat zijn waardevolle contacten die je opdoet tijdens de stage periode.

3.2 Wat heb ik geleerd & waar ben ik in gegroeid

Ik heb geleerd de opdracht naar mijn eigen hand te zetten. Daar bedoel ik mee dat een opdracht op 100 verschillende manier uitgevoerd kan worden. Het is goed om te zoeken naar de manier die bij je past Als je weken aan een opdracht werkt dan is het goed als dat effectief en efficiënt gebeurd, dat bereik je door een format te kiezen die synchroon loopt met je eigen manier van werken.

Op technisch vlak heb ik veel bijgeleerd over Security Information and Event Mangement systemen met in het bijzonder Splunk & Azure Sentinel. Daarnaast heb ik het proces inzichtelijk gemaakt voor het kiezen van een SIEM. Dit zorgde ervoor dat ik een manier heb gehanteerd die ik kan gebruiken bij het uitvoeren van opdrachten voor mijn nieuwe werkgever. Op gebied van cloud technologie heb ik in het bijzonder een certificaat behaald van Microsoft genaamd AZ900. Dit is het Azure Fundamentals certificaat. Dat betekent dat ik een aantal dagen heb gespendeerd om te leren over cloud technologie met de focus op Azure.

Een andere les die ik heb getrokken uit de stage is lef hebben. Gedurende mijn stage periode was het niet altijd makkelijk online bruikbare informatie te vinden. In een gesprek met mijn begeleider vroeg ik of hij iemand kende met technische expertise in mijn onderwerp. Mijn begeleider stelde voor om Greg Peterson te mailen. Greg is sr Director Security van Avanade en gevestigd in Seattle(USA). Deze meneer had de migratie gedaan van Splunk naar Azure Sentinel voor Avanade, die expertise en kennis was bruikbaar voor mijn onderzoek. Ik had een interview met hem geregeld waarin hij op een open en zeer begrijpbare wijze mijn vragen beantwoorde. Een internationale organisatie als Avanade heeft expertise over de hele wereld zitten en die kan benut worden. Door middel van Microsoft teams kan videobellen met alle collega's over de hele wereld.

3.3 Problemen

Halverwege mijn stage periode kreeg ik te horen dat mijn technisch begeleider een andere baan zou krijgen. Twee weken later zou hij vertrekken en dit betekende voor mij dat ik geen technisch begeleider meer had voor de laatste vier weken mijn stage. Na het horen van deze informatie heb ik met iemand van personeelszaken gebeld en deze persoon heeft ervoor gezorgd dat ik op tijd een nieuwe technisch begeleider kreeg.