THOMAS MORE

SOC MPI Oosterlo

Reflectiedocument

Michiel Kuyken
Student Bachelor in de Elektronica-ICT – Cloud & Cyber Security

2024 - 2025

Inhoudsopgave

1. Inleiding

In dit reflectiedocument kijk ik terug op mijn stage bij MPI Oosterlo VZW**,** waar ik gewerkt heb aan het opzetten van een Security Operations Center. Tijdens deze stage kreeg ik de kans om mijn kennis en vaardigheden op het gebied van cybersecurity toe te passen in een echte werkomgeving. Het was een leerrijke ervaring waarin ik niet alleen technisch veel heb bijgeleerd, maar ook als persoon sterk ben gegroeid.

Het document bestaat uit twee delen. In het eerste deel blik ik terug op de technische uitvoering van mijn project. Ik leg uit wat ik precies heb gerealiseerd, welke tools en systemen ik gebruikt heb, wat het resultaat betekent voor de organisatie en de gebruikers, en welke zaken nog openstaan. Ook geef ik enkele aanbevelingen mee voor de toekomst, zodat het SOC verder kan worden uitgebouwd.

In het tweede deel reflecteer ik op mijn persoonlijke leerproces. Ik sta stil bij de competenties die ik ontwikkeld heb, de obstakels die ik tegenkwam en hoe ik daarmee omging. Daarnaast beschrijf ik hoe ik ben gegroeid als IT-student, hoe ik heb samengewerkt met collega's, en wat deze stage voor mij betekend heeft op professioneel en persoonlijk vlak.

Met dit document wil ik niet alleen laten zien wat ik heb gedaan, maar ook hoe ik het ervaren heb. Zo krijgt u als lezer een goed beeld van het project en van mijn ontwikkeling tijdens deze stageperiode.

2. Inhoudelijke reflectie

Ik begin met een reflectie over mijn project dat ik heb uitgewerkt voor het MPI Oosterlo. Het opstellen van een SOC ging met vallen en opstaan, zoals alle projecten gaan. In onderstaande tekst kijk ik terug op dit proces en haal ik aan wat er moeilijk was, wat er goed ging en wat ik heb geleerd.

2.1. Concrete realisatie

2.1.1. Korte beschrijving project

Voor de realisatie van mijn SOC heb ik gebruik gemaakt van verschillende tools. Een alert wordt gedetecteerd met Wazuh en deze wordt naar Shuffle gestuurd, waar er vervolgens een workflow start. Deze workflow maakt alerts en cases aan in TheHive en voegt hier observables aan toe. Deze worden gecontroleerd door analyzers die zich in Cortex bevinden. Ten slotte krijgt het IT-team een melding in een Teams-chat die verteld wat er aan de hand is. Voor de volledige uitleg van het project verwijs ik u graag naar mijn realisatiedocument.

2.1.2. Relevantie voor MPI

Het project is van grote relevantie voor het MPI, omdat het kritieke servers beschermd tegen aanvallen. Het MPI beschikt over veel servers, waaronder ook fileservers en active directories waarop gevoelige informatie staat. Hierop worden nu aanvallen proactief gedetecteerd en kunnen ernstige lekken voorkomen worden.

2.1.3. Technische problemen + oplossingen

Een project gaat zelden in een keer goed. Hieronder bespreek ik enkele van de problemen die ik ondervond tijdens mijn stage en de oplossing die ik hiervoor gebruikt heb.

Een van de eerste problemen die ik ben tegengekomen, gebeurde bij het opzetten van Shuffle. Ik kreeg het niet opgezet met het volgen van de installatiegids. Na veel zoeken bleek uiteindelijk dat het probleem zich bevond in het virtueel netwerk dat door Shuffle werd opgezet. Na het IP-subnet hiervan aan te passen, werkte alles wel naar behoren.

De licentie van TheHive is nodig om aanpassingen te kunnen maken in het platform. Dit betekent dat er helemaal niks gedaan kan worden, totdat er een licentie toegekend is. TheHive heeft een gratis licentie, maar ik heb gewacht tot ik nog maar zeven dagen had van mijn testlicentie om deze aan te vragen. Ik dacht dat ik deze licentie snel zou ontvangen. Ik heb gewacht tot ik deze licentie had vooraleer ik verdere aanpassingen maakte, omdat ik geen onnodige tijd wou steken in het opzetten van iets waar ik geen toegang meer tot kon krijgen. Na een week zonder enige reactie en mijn licentie nu op zijn einde, ben ik gaan experimenteren met DFIR IRIS. Ik heb hier echter nooit veel mee gedaan omdat ik niet zoveel ervaring met deze tool. Gelukkig kreeg ik na 12 dagen eindelijk mijn licentie van TheHive. Het antwoord op dit probleem was dus veel geduld hebben.

Het laatste probleem dat ik aanhaal, is een probleem wat op het einde van mijn project naar boven kwam. Het ophalen van observables van cases om te laten analyseren door Cortex was volgens verschillende tutorials mogelijk. Dit bleek echter niet het geval te zijn omdat Shuffle sindsdien enkele updates heeft gehad. Ik heb hier uiteindelijk nooit een goede oplossing voor gevonden, enkel een tijdelijke oplossing die ongeveer hetzelfde resultaat bereikt. Deze oplossing is te uitgebreid om hier te beschrijven, hiervoor verwijs ik u graag door naar mijn realisatiedocument.

2.2. Toekomstplannen

2.2.1. Gebruiksinname + toekomstadviezen

Momenteel is mijn SOC actief in gebruik door mijn collega's. In mijn laatste week van mijn stage heb ik een live-demo gegeven waarin ik de functionaliteiten liet zien. Tijdens deze demo hebben ze de mogelijkheid gekregen om vragen te stellen en verduidelijkingen te vragen. Ik heb hier alle vragen beantwoord en mijn collega's weten dat ze mij altijd mogen contacteren bij eventuele vragen.

Mijn SOC heeft nog veel groeipotentie. In de toekomst is het nuttig voor mijn collega's om alerts te onderzoeken. Momenteel worden alerts ingedeeld in vier grote groepen: critical, high, medium en low. Critical en high staan al ingesteld om een melding te maken in Teams. Dit betekent niet dat er in de medium en low categorieën geen belangrijke alerts meer zitten. Mijn advies is om de categorie medium onder de loep te nemen en eerst te proberen zoveel mogelijk alerts op te lossen. Dit heb ik tijdens mijn stage al voor enkele vaak herhaalde alerts gedaan. Als dit ook voor andere alerts gedaan kan worden, worden ze al minder overrompeld door de hoeveelheid meldingen in de categorie medium. Zonder de opgeloste alerts, wordt het duidelijk welke andere minder kritieke alerts ze kunnen verwijderen. Uiteindelijk kunnen ze dan ook het meldingsniveau vanwaar alerts naar Teams worden gestuurd, verlagen. Positief is dat ze dan ook niet overrompeld worden door alerts die minder dringend zijn.

Een ander probleem waar ik mee gekaapt heb tijdens mijn stage is het maken van uniforme alerts. Dit houdt in dat elke alert die op Wazuh binnenkomt, dezelfde syntax volgt. Ik heb hier tijdens mijn stage veel onderzoek naar gedaan, maar geen goede oplossing gevonden om dit probleem aan te pakken. Voor mijn collega's is het handig om te proberen dit toch toe te passen. Dit zou de workflow in Shuffle makkelijker maken om op te stellen en uit te breiden. Momenteel heb ik hier tijdelijke oplossingen voor, maar deze kunnen het best weggewerkt worden voor meer duidelijkheid.

3. Persoonlijke reflectie

3.1. Persoonlijke groei en inzichten

3.1.1. Omgeving

Voor het vak Project 4.0 had ik al een voorproef gekregen van het leven in een IT-bedrijf. Dit beviel me niet helemaal, dus was ik blij dat ik mijn stage kon doen bij een organisatie waar de focus niet op IT lag. De sfeer lag hier helemaal anders. Het was een rustigere en fijnere omgeving waar de druk niet constant lag op het vervullen van deadlines, maar op het draaiende houden van de organisatie.

Het meedraaien op de servicedesk haalde me telkens uit mijn comfortzone die in school is opgesteld. We worden opgeleid om een specialist te worden in een bepaalde tak, maar hier komen alle soorten problemen aan bod. Dit zorgde ervoor dat ik veel kennis op kon doen, waar ik later op terugkom. Gelukkig hielp hier de steun van mijn collega's van de IT-dienst en het geduld van mijn andere collega's enorm.

Tenslotte heb ik tijdens mijn stage ook de mogelijkheid gekregen om een presentatie over grensoverschrijdend gedrag bij te wonen. Het was een interessante kijk op de verschillende vormen waarin dit kan voorkomen, die niet seksueel hoeven te zijn. Dit bracht me ook weer uit mijn comfortzone: ik was hier niet enkel om een IT-project op te zetten. Ik werd meegetrokken in de algemene werking van een organisatie waar er ook onderlinge problemen zich kunnen voordoen. Weten waar je terecht kunt is dan heel belangrijk en het was fijn om te zien dat een organisatie zo betrokken is bij het welzijn van zijn medewerkers.

3.1.2. Collega's

Op de IT-dienst heb ik geleerd hoe ik met collega's binnen mijn branche moest omgaan. De onderlinge dynamiek in een klein team heeft zijn voor- en nadelen. De drempel om mensen aan te spreken ligt veel lager omdat iedereen veel losser is. Mijn stagementor was ook de leidinggevende van ons team en iedereen kon hem op elk moment storen als we met vragen zaten. Dit hielp mij ook om naar andere te gaan als ik met problemen zat of niet wist hoe ik iets moest oplossen.

Een nadeel is natuurlijk dat als er problemen zijn tussen collega's, je elkaar niet uit de weg kunt gaan. Ik heb de pech gehad dat de onderlinge dynamiek tussen mijn twee collega's tijdens mijn stageperiode op zijn ergst was. Dit zorgde voor afwezigheid van één van de twee waardoor ik een hele week enkel met mijn andere collega doorbracht. Hoewel ik het goed met beide kon vinden, merkte je toch de spanningen. Dit is uiteraard jammer, zeker omdat ik maar zo'n korte periode aanwezig was.

3.2. Praktische groei

Voor mijn SOC heb ik vanuit school al een brede basis meegekregen waar ik op verder kon bouwen. Ik kende al veel zaken en wist hoe ik in theorie met de verschillende tools kon omgaan om een mooi SOC op te zetten. Hoewel ik hier ook veel bijgeleerd heb door dieper in te gaan op deze tools, wil ik vooral focussen op de servicedesk waar ik op meedraaide.

Tijdens mijn opleiding ben ik in contact gekomen met Windows Server en Active Directory. Deze vakken miste echter veel praktijk en waren vooral theoretisch. Kleine projecten kwamen niet in de buurt van wat ik tijdens mijn stage hierover heb bijgeleerd. Ik ben meer zelfzeker in het werken in een Active Directory en kan rechten toepassen volgens de richtlijnen van de organisatie. Ik herkende hierin veel zaken die we ook gezien hebben tijdens de lessen, maar waar we nooit echt mee in aanraking zijn gekomen.

Ook het oplossen van problemen op printers was compleet nieuw voor mij. Ik was nog nooit in aanraking gekomen met een printserver, maar naar het einde van mijn stage kon ik zelfstandig verschillende problemen oplossen. Een echte meerwaarde dus.

3.3. Werkpunten

Tijdens mijn stage ben ik veel over mezelf te weten gekomen, zowel op positief als negatief vlak. Beginnen doe ik met mijn zwaktes. Eén van mijn grootste werkpunten is mijn perfectionisme. Ik heb dit eerder tijdens de opleiding ook al gemerkt. Ik stel onrealistische deadlines voor mezelf waarin ik zaken perfect wil afhebben. Dit zorgt vaak voor stress, wat me tot mijn volgende punt brengt.

Mijn stressbestendigheidsniveau ligt vrij laag. Ik heb moeite met het omgaan met stress, wat gelukkig al een deel verholpen werd door in een werksfeer te zijn waar ik me op mijn gemak voelde. Toch merkte ik naar het einde toe dat ik soms dichtklapte en geen vooruitgang kon maken. Dit omwille van de stressreactie die mijn lijf en hoofd geeft. Dit is een probleem waar ik in de toekomst rekening mee moet houden, niet alleen voor toekomstige projecten maar ook het type werk dat ik kies.

3.4. Kwaliteiten

Natuurlijk heb ik ook veel sterke kanten van mezelf ontdekt. Graag haal ik hiervoor vier belangrijke eigenschappen aan. Ik ben er namelijk achter gekomen dat ik heel klantvriendelijk kan zijn. Ik kreeg vaak van anderen te horen dat ik vriendelijk overkom en altijd probeer te helpen waar ik kan. De blijdschap die ik mensen kon geven met het oplossen wat voor mij soms simpele problemen zijn, deed me realiseren dat dit hetgeen is waar energie uit haal en wat ik graag doe.

Een tweede eigenschap die bij mij sterk is, is het omgaan met tegenslagen. Regelmatig stootte ik op problemen tijdens mijn project. Ik merkte hier dat ik een goed doorzettingsvermogen had en dat ik altijd bleef proberen om toch het probleem op te lossen. Als ik er even niet uit kon komen, ging ik iets anders doen om me af te leiden. Hierna kon ik me met een fris hoofd terug achter het probleem zetten om het verder op te lossen. Dit heeft me door veel problemen gesleurd waar ik soms wel dagen achter zat.

Ook heb ik ontdekt dat ik flexibel kan zijn. Mijn werken aan mijn SOC werd regelmatig onderbroken door andere problemen die zich voordeden. Het wisselen van werkhouding om van mijn project naar het probleem ter handen te gaan, verliep vlot en soepel.

Dit brengt mij ook mooi bij mijn laatste eigenschap, probleemoplossend denken. Hoewel ik in de eerste weken van mijn stage moest wennen aan de nieuwe problemen die mijn kant op werden gegooid, is dit toch iets wat na verloop van tijd wende. Naar het einde van mijn stage toe stond ik er één dag per week alleen voor en moest ik proberen om alle problemen zelf op te lossen. Een belangrijke tip die ik heb meegenomen was dat het oké is om niet alles te weten. Je mag gerust iets opzoeken als je twijfelt en niet alles moet van de eerste keer goed gaan.