THOMAS MORE

Netleaf Adversary Emulation

Reflectie

Siebe Moeskops
Student Bachelor in de Toegepaste Informatica – Applicatieontwikkeling
Student Bachelor in de Elektronica-ICT – Cloud & Cyber Security

2025 – 2026

Inhoudsopgave

1. Inleiding

Dit reflectiedocument vormt het sluitstuk van de stageperiode bij Netleaf. Waar in het project charter de doelstellingen werden vastgelegd en in het realisatiedocument de technische uitwerking van het project werd toegelicht, wordt in dit document teruggeblikt op zowel de inhoudelijke als persoonlijke aspecten van de stage. (Moeskops, 2026)

Eerst wordt gereflecteerd op de gerealiseerde projectdoelstellingen, de meerwaarde van de ontwikkelde oplossing en de mogelijke toekomst van het project binnen de organisatie. Vervolgens wordt stilgestaan bij de persoonlijke leerervaringen, de verworven competenties en de uitdagingen die tijdens de stageperiode werden ervaren.

2. Inhoudelijke reflectie

Tijdens de stage bij Netleaf werden alle vooropgestelde doelstellingen succesvol gerealiseerd. Het project resulteerde in een geautomatiseerde oplossing voor detectievalidatie binnen hun Security Operations Center (SOC). Hierbij werden drie belangrijke onderdelen ontwikkeld: een detection coverage mapping, een Detection-as-Code pipeline voor nieuwe detectieregels en een oplossing voor continue validatie van bestaande detecties.

Deze oplossing biedt Netleaf meer inzicht in de effectiviteit van detectieregels binnen Rapid7 InsightIDR en maakt het mogelijk om mogelijke detection gaps sneller te identificeren. Daarnaast zorgt de automatisatie ervoor dat nieuwe detectieregels op een consistente en reproduceerbare manier getest kunnen worden alvorens ze in gebruik worden genomen. Ook de continue validatie levert een belangrijke meerwaarde doordat afwijkingen of verouderde detectieregels sneller zichtbaar worden.

Hoewel de basis van het project volledig gerealiseerd werd, zijn er nog verschillende uitbreidingsmogelijkheden. De oplossing kan verder uitgebreid worden met bijkomende aanvalstechnieken, extra validatiecriteria en een bredere integratie binnen de bestaande processen van het SOC. Daarnaast dient de oplossing nog officieel binnen de operationele omgeving uitgerold te worden.

Op het moment van afronding van de stage is de oplossing nog niet actief in productie genomen. Wel werd aangegeven dat de ontwikkelde oplossing voldoende potentieel heeft om verder gebruikt en uitgebreid te worden binnen de organisatie. Ik kreeg bovendien de mogelijkheid aangeboden om dit traject verder te zetten binnen Netleaf na afloop van de stage, en vast te werken bij hun team als junior SOC analist.

Voor de toekomst raad ik aan om de opgebouwde documentatie, architectuur en ontwikkelde scripts zorgvuldig te behouden. Daarnaast hebben de wekelijkse standup momenten tijdens de stage bewezen dat regelmatige opvolging en kennisdeling een belangrijke bijdrage leveren aan het succes van technische projecten. Het behouden van dergelijke overlegmomenten kan toekomstige ontwikkelingen verder ondersteunen.

3. Persoonlijke reflectie

Deze stage betekende voor mij een belangrijke stap in de overgang van student naar professional. Tijdens de stage kreeg ik de kans om zelfstandig een technisch project uit te werken binnen een professionele cybersecurityomgeving. Het feit dat ik na afloop van de stage een jobaanbieding ontving, beschouw ik als een bevestiging dat ik klaar ben om de volgende stap in mijn carrière te zetten.

Op technisch vlak heb ik veel nieuwe kennis opgedaan. Ik maakte kennis met technologieën zoals Rapid7 InsightIDR, Velociraptor, Atomic Red Team, GitLab CI/CD, Terraform en Grafana. Daarnaast leerde ik hoe verschillende systemen met elkaar geïntegreerd kunnen worden binnen één geautomatiseerde workflow. Ook mijn kennis rond detectieregels, adversary emulation en Security Operations Centers werd aanzienlijk uitgebreid.

Naast de technische vaardigheden heb ik vooral geleerd om zelfstandig te werken. Tijdens het project moest ik vaak zelf onderzoek uitvoeren, documentatie raadplegen en oplossingen uitwerken voor problemen waarvoor geen kant-en-klare oplossing beschikbaar was. Hierdoor heb ik mijn probleemoplossend vermogen en zelfredzaamheid verder ontwikkeld.

Gedurende de stage werd ik geconfronteerd met verschillende uitdagingen. Zo bleek het correleren van aanvalssimulaties met detecties complexer dan eerst verwacht. Daarnaast zorgden vertragingen in logverwerking, integratieproblemen tussen verschillende tools en het opzetten van een betrouwbare automatisatiepipeline voor bijkomende uitdagingen. Door systematisch te testen, problemen op te splitsen in kleinere onderdelen en regelmatig feedback te vragen aan mijn stagebegeleider konden deze problemen telkens succesvol opgelost worden.

Wanneer ik terugkijk op deze stage, overheerst vooral een gevoel van tevredenheid. Ik heb niet alleen mijn technische kennis aanzienlijk uitgebreid, maar ook geleerd hoe projecten in een professionele omgeving worden aangepakt. De combinatie van zelfstandigheid, verantwoordelijkheid en technische diepgang maakte deze stage bijzonder leerrijk en vormt een sterke basis voor mijn verdere professionele carrière.

LITERATUURLIJST

Moeskops, S. (2026). *Moeskops_Siebe_Project_Charter*.