THOMAS MORE

Netleaf Adversary Emulation

Project Charter

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

2025 - 2026

Table of contents

1. Inleiding

Dit document beschrijft het project dat werd uitgevoerd in het kader van de stage bij Netleaf, met een focus op adversary emulation en detectievalidatie binnen een Security Operations Center (SOC). Binnen deze context wordt onderzocht hoe aanvalssimulaties kunnen worden ingezet om de effectiviteit van bestaande detectieregels te evalueren.

Het doel van dit document is om een duidelijk en gestructureerd overzicht te geven van de probleemstelling, de doelstellingen en de uitgewerkte oplossing. Hierbij wordt ingegaan op de huidige situatie binnen de SOC-omgeving, de gekozen aanpak en de gebruikte technologieën om een geautomatiseerde detectievalidatiepipeline te realiseren.

Daarnaast behandelt dit document de scope van het project, de belangrijkste stakeholders, mogelijke risico's en de planning. Op deze manier biedt het een volledig beeld van zowel de technische uitwerking als de organisatorische context van het project.

2. Achtergrond

In deze sectie wordt de context van het project toegelicht. Eerst wordt de organisatie waarin de stage plaatsvindt kort voorgesteld. Vervolgens wordt de huidige situatie binnen deze organisatie beschreven, met focus op het probleem dat aanleiding geeft tot dit project. Op deze manier wordt duidelijk waarom een nieuwe oplossing noodzakelijk is.

2.1. Netleaf

Netleaf is een organisatie die zich specialiseert in managed Security Operations Center (SOC)-diensten. Binnen deze B2B dienstverlening staat het continu monitoren van IT-omgevingen centraal, met als doel het detecteren en analyseren van mogelijke beveiligingsincidenten. Daarnaast ondersteunt Netleaf organisaties bij incident response en het optimaliseren van hun beveiligingsinfrastructuur.

Binnen het SOC maakt Netleaf gebruik van een SIEM-platform, namelijk Rapid7 InsightIDR, om logs te analyseren en verdachte activiteiten te detecteren aan de hand van vooraf gedefinieerde detectieregels. Deze regels vormen een essentieel onderdeel van de beveiligingsstrategie, aangezien ze bepalen welke activiteiten als potentieel kwaadaardig worden beschouwd.

2.2. Huidige situatie

Binnen de huidige SOC-omgeving van Netleaf zijn een groot aantal detectieregels geïmplementeerd binnen het SIEM-platform Rapid7 InsightIDR. Deze regels zijn bedoeld om verdachte activiteiten en mogelijke cyberdreigingen te detecteren. Hoewel deze detectieregels actief zijn, bestaat er momenteel geen gestructureerde manier om hun effectiviteit continu te valideren.

Daardoor is het onduidelijk welke detectieregels correct triggeren wanneer specifieke aanvalstechnieken worden uitgevoerd. Daarnaast is er beperkte zichtbaarheid op welke detectieregels verouderd zijn, niet langer relevant zijn of onvoldoende aansluiten bij de huidige dreigingen en infrastructuur. Hierdoor kunnen detection gaps ontstaan waarbij bepaalde aanvalstechnieken niet of onvoldoende worden gedetecteerd.

Momenteel gebeurt detectievalidatie voornamelijk manueel en ad hoc. Dit proces is tijdsintensief, moeilijk schaalbaar en afhankelijk van individuele controles.

Deze beperkingen zorgen ervoor dat het SOC-team geen volledig overzicht heeft van de actuele detectiedekking. Hierdoor wordt het moeilijker om de effectiviteit van detectieregels te beoordelen en detection gaps tijdig te identificeren.

3. Projectomschrijving

Dit project richt zich op het ontwikkelen van een geautomatiseerde oplossing voor het valideren van detectieregels binnen het SOC van Netleaf. De kern van de oplossing bestaat uit een geautomatiseerde oplossing waarmee aanvalssimulaties kunnen worden gekoppeld aan detectieregels. Op basis hiervan kan de effectiviteit van detecties worden geëvalueerd en kunnen detection gaps worden geïdentificeerd.

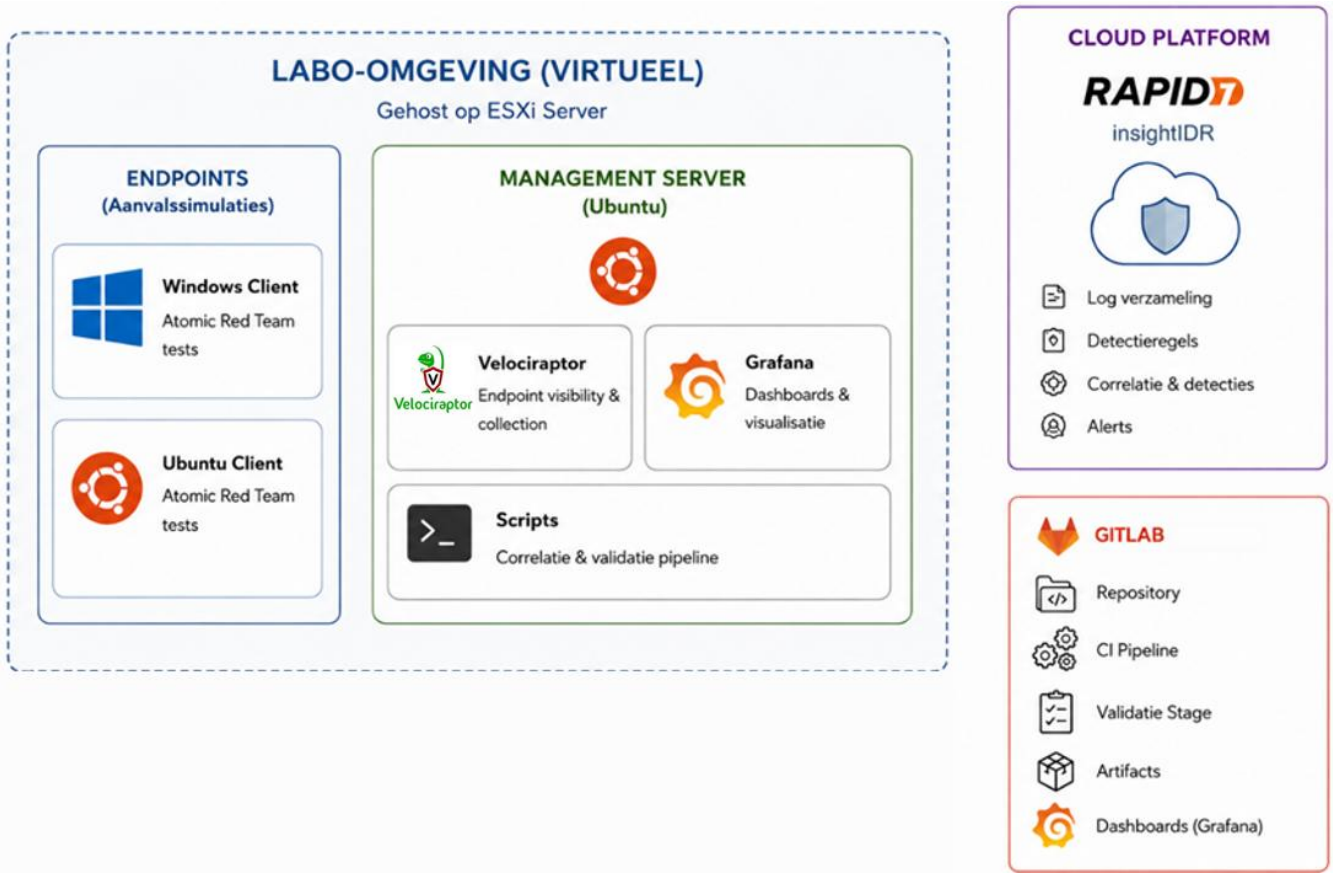
Om deze oplossing te realiseren, wordt het project opgebouwd uit drie opeenvolgende fases. In de eerste fase wordt een betrouwbare correlatiemethode ontwikkeld tussen uitgevoerde aanvalssimulaties en de gegenereerde detecties binnen het SIEM-platform. In de tweede fase wordt een Detection-as-Code pipeline uitgewerkt waarmee nieuwe detectieregels automatisch kunnen worden aangemaakt, gevalideerd en uitgerold. In de derde fase wordt een geautomatiseerde detectievalidatiepipeline ontwikkeld die bestaande detectieregels periodiek test en controleert of deze nog correct functioneren.

3.1. Labo-omgeving

Voor dit project werd een aparte labo-omgeving opgezet op een VMware ESXi-server. Deze omgeving bestond uit Windows- en Linux-endpoints voor aanvalssimulaties, een centrale managementserver en koppelingen met Rapid7 InsightIDR en GitLab.

Daarnaast werd een afzonderlijke Rapid7-omgeving voorzien, volledig los van de productieomgevingen van klanten, zodat testen en validaties veilig konden worden uitgevoerd.

Figuur 1 Architectuur van de labo-omgeving



Opmerking. Overzicht van de virtuele labo-omgeving. **Eigen werk.**

3.2. Fase 1: Correlatie tussen Atomic tests en detectieregels

In de eerste fase van het project ligt de focus op het ontwikkelen van een methode om Atomic Red Team-tests te koppelen aan detecties binnen Rapid7 InsightIDR. Er zal onderzocht worden hoe aanvalstechnieken, gebaseerd op het MITRE ATT&CK-framework, gelinkt kunnen worden aan specifieke detectieregels. Het MITRE ATT&CK-framework (Adversarial Tactics, Techniques & Common Knowledge) is een wereldwijd gebruikte kennisbank die aanvalstechnieken categoriseert op basis van het gedrag van cyberaanvallers.

Hierbij zullen verschillende correlatiemethoden worden geëvalueerd, zoals:

- Het gebruik van MITRE ATT&CK techniek-ID's in de vorm van Atomic Red Team-tests
- Tijds gebaseerde correlatie via batch gebaseerde validatie
- Filtering op specifieke hosts om ruis te beperken

Het doel van deze fase is het opzetten van een betrouwbare methode waarmee kan worden vastgesteld welke detectieregels effectief reageren op specifieke aanvalstechnieken.

3.3. Fase 2: Detection-as-Code Pipeline

In de tweede fase van het project wordt de ontwikkelde correlatielogica geïntegreerd in een geautomatiseerde Detection-as-Code pipeline. Deze pipeline maakt het mogelijk om detectieregels op een consistente, schaalbare en reproduceerbare manier aan te maken, valideren en beheren.

Wanneer een nieuwe detectieregel wordt ontwikkeld of aangepast, wordt de Detection-as-Code pipeline automatisch gestart via GitLab. De pipeline rolt de detectieregel uit naar de testomgeving en voert vervolgens de bijhorende Atomic Red Team-tests uit. Tijdens deze tests worden logs en detecties verzameld binnen Rapid7 InsightIDR.

Na afloop van de test haalt de pipeline de gegenereerde detecties op uit het SIEM-platform en correleert deze met de uitgevoerde aanvalssimulaties op basis van tijdsvensters, hostinformatie en MITRE ATT&CK-technieken. Op basis van deze correlatie wordt automatisch bepaald of de detectieregel correct heeft gereageerd op de gesimuleerde aanvalstechniek. Het resultaat wordt vervolgens opgeslagen en gerapporteerd als een PASS- of FAIL-validatie.

De pipeline automatiseert hierbij het volledige validatieproces:

- Het aanmaken en uitrollen van (nieuwe) detectieregels
- Het uitvoeren van Atomic Red Team-tests
- Het ophalen van detecties uit het SIEM-platform
- Het correleren van testen met deze detectieregels
- Het bepalen van een PASS/FAIL-validatiestatus

Detectieregels die succesvol worden gevalideerd kunnen behouden of verder uitgerold worden. Regels die niet correct functioneren worden automatisch afgekeurd, zodat deze verder geanalyseerd en verbeterd kunnen worden.

Deze fase resulteert in een geautomatiseerde kwaliteitscontrole voor nieuwe detectieregels, waardoor fouten vroegtijdig worden opgespoord en de betrouwbaarheid van detecties wordt verhoogd.

3.4. Fase 3: Continue detectievalidatie

In de derde fase van het project wordt een geautomatiseerde pipeline ontwikkeld voor bestaande detectieregels. Binnen een SOC-omgeving evolueren zowel aanvalstechnieken als IT-infrastructuren voortdurend, waardoor detectieregels na verloop van tijd minder effectief kunnen worden of zelfs volledig kunnen falen. Hierdoor ontstaat de nood om bestaande detectieregels periodiek te controleren en te valideren.

Deze fase richt zich op het continu testen van bestaande detectieregels aan de hand van aanvalssimulaties. Op basis van de resultaten kan worden vastgesteld welke detectieregels nog correct functioneren, welke mogelijk verouderd zijn en waar er detection gaps aanwezig zijn. Hierdoor krijgt het SOC-team meer inzicht in de actuele detectiedekking en kan sneller worden ingegrepen wanneer detecties niet langer werken zoals verwacht.

Hierbij zullen verschillende validatiemethoden worden toegepast, zoals:

- Het periodiek uitvoeren van Atomic Red Team-tests
- Het automatisch valideren van bestaande detectieregels
- Het identificeren van verouderde of niet-functionerende detecties
- Het rapporteren van detection gaps en resultaten

Het doel van deze fase is het realiseren van een continue kwaliteitscontrole op bestaande detectieregels, zodat de betrouwbaarheid en effectiviteit van de detectieomgeving op lange termijn gewaarborgd blijft.

4. Doelstellingen en belanghebbenden

In dit hoofdstuk worden de doelstellingen van het project beschreven. Eerst worden de functionele en niet-functionele vereisten van de oplossing toegelicht. Vervolgens worden de belangrijkste belanghebbenden geïdentificeerd en wordt de toegevoegde waarde van het project voor elke stakeholder besproken.

4.1. Functionele vereisten (op hoog niveau)

FV1: Correleren van aanvalssimulaties met detectieregels binnen het SIEM-platform.
FV2: Identificeren van detectiedekking en mogelijke detection gaps.
FV3: Automatisch valideren van detectieregels aan de hand van aanvalssimulaties.
FV4: Automatisch aanmaken en testen van nieuwe detectieregels via een Detection-as-Code aanpak.
FV5: Enkel gevalideerde detectieregels behouden of uitrollen.
FV6: Bestaande detectieregels periodiek controleren op correcte werking en veroudering.
FV7: Resultaten centraal visualiseren via dashboards en rapportages.

4.2. Niet-functionele vereisten/technische vereisten

NFV1: De oplossing moet schaalbaar zijn en meerdere validaties na elkaar kunnen verwerken.
NFV2: De correlatie tussen testen en detecties moet betrouwbaar en reproduceerbaar zijn.
NFV3: De oplossing moet grotendeels geautomatiseerd functioneren.
NFV4: De oplossing moet compatibel zijn met de bestaande SOC-infrastructuur.
NFV5: Validaties moeten binnen een aanvaardbaar tijdsvenster uitgevoerd kunnen worden.
NFV6: De oplossing moet eenvoudig uitbreidbaar en onderhoudbaar zijn.

4.3. Belanghebbenden en toegevoegde waarde

SOC-analisten

SOC-analisten zijn verantwoordelijk voor het monitoren en analyseren van beveiligingsincidenten. Dankzij de oplossing krijgen zij meer inzicht in de effectiviteit van detectieregels en de aanwezige detectiedekking. Vooral **FV1, FV2, FV3, FV6 en FV7** ondersteunen hen bij het identificeren van detection gaps en het opvolgen van detectiekwaliteit.

Netleaf (organisatie)

Voor Netleaf betekent dit project een verbetering van de kwaliteit en betrouwbaarheid van de SOC-diensten. Door detectieregels automatisch te valideren, nieuwe regels gecontroleerd uit te rollen en bestaande regels continu te testen, kan de organisatie haar dienstverlening verder professionaliseren. Netleaf profiteert hierbij van **alle functionele vereisten (FV1 t.e.m. FV7)**.

Klanten van Netleaf

De eindklanten profiteren indirect van dit project doordat hun IT-omgevingen beter beschermd worden tegen cyberdreigingen. Dankzij een betere detectiedekking, sneller geïdentificeerde detection gaps en continu gevalideerde detectieregels wordt de kans op onopgemerkte aanvallen verkleind. Hierbij leveren voornamelijk **FV2, FV3, FV5 en FV6** een meerwaarde.

5. Project scope

In dit hoofdstuk wordt de afbakening van het project vastgelegd. Dit maakt duidelijk welke onderdelen binnen het project worden gerealiseerd en welke expliciet buiten scope vallen. Daarnaast worden de verantwoordelijkheden van zowel de klant als het projectteam beschreven.

5.1. In-Scope

Binnen de scope van dit project valt het ontwerpen, implementeren en valideren van een geautomatiseerde oplossing voor detectievalidatie binnen een gecontroleerde testomgeving.
Concreet omvat dit:

- Het opzetten van een testomgeving waarin aanvalssimulaties kunnen worden uitgevoerd
- Het uitvoeren van Atomic Red Team-tests om aanvalstechnieken te simuleren
- Het ontwikkelen van een correlatiemethode tussen aanvalssimulaties en detecties binnen Rapid7 InsightIDR
- Het identificeren van detection gaps binnen de bestaande detectiedekking
- Het ontwikkelen van een Detection-as-Code pipeline voor het aanmaken en valideren van nieuwe detectieregels
- Het ontwikkelen van een geautomatiseerde pipeline voor continue detectievalidatie
- Het analyseren en visualiseren van resultaten via centrale dashboards

5.2. Out-of-Scope

De volgende onderdelen vallen buiten de scope van dit project:

- Implementatie van de oplossing in productieomgevingen van klanten
- Real-time automatisatie van incident response (bijvoorbeeld via SOAR-oplossingen)
- Het ontwikkelen van volledige detectiecontent voor alle MITRE ATT&CK-technieken
- Langdurig onderhoud en operationele opvolging na oplevering

5.3. Verantwoordelijkheden

Verantwoordelijkheden van het projectteam (stagiair):

- Ontwikkelen en implementeren van de verschillende projectcomponenten
- Opzetten en beheren van de labo-omgeving
- Ontwikkelen van correlatie- en validatielogica
- Uitvoeren van testen en analyseren van resultaten
- Documenteren van de oplossing en bevindingen

Verantwoordelijkheden van de klant (Netleaf):

- Aanleveren van toegang tot de nodige tools en infrastructuur
- Voorzien van begeleiding en technische ondersteuning
- Tijdige feedback geven op tussentijdse resultaten
- Valideren van de uiteindelijke oplossing

6. Risicoanalyse

In dit hoofdstuk worden de voornaamste risico's beschreven die een impact kunnen hebben op het succesvol verloop van het project. Hierbij wordt zowel gekeken naar risico's die binnen de verantwoordelijkheid van de klant liggen, als naar risico's die voortkomen uit de uitvoering van het project door de stagair. Door deze risico's tijdig te identificeren, kunnen gepaste maatregelen genomen worden om vertragingen, misverstanden of kwaliteitsverlies te beperken.

6.1. Risico's aan klantzijde (Netleaf)

Onvoldoende betrokkenheid van stakeholders
Een beperkte beschikbaarheid van betrokken medewerkers, zoals SOC-analisten of technische begeleiders, kan ervoor zorgen dat noodzakelijke input of feedback ontbreekt.

Voorgestelde maatregelen:

- Een vaste contactpersoon aanduiden
- Regelmatige opvolgmomenten inplannen
- Verwachtingen duidelijk communiceren
- Standup meetings met het team elke 2 weken

Beperkte toegang tot tools of infrastructuur
Toegang tot platformen zoals Rapid7 InsightIDR, testsystemen of dashboards is noodzakelijk om het project uit te voeren.

Voorgestelde maatregelen:

- Toegangen voorzien bij projectstart
- Accounts en rechten vooraf testen
- Technisch aanspreekpunt voorzien

Wijzigende prioriteiten binnen de organisatie
Operationele druk of dringende security-incidenten kunnen ervoor zorgen dat het project tijdelijk minder aandacht krijgt.

Voorgestelde maatregelen:

- Realistische planning voorzien
- Belangrijke beslissingen vroeg nemen
- Regelmatig prioriteiten afstemmen

6.2. Risico's aan projectzijde (stagiair)

Complexiteit van de technische integratie
Het project combineert verschillende technologieën, waaronder Atomic Red Team, Rapid7 InsightIDR, GitLab, Terraform en Grafana. De integratie tussen deze componenten brengt extra technische complexiteit met zich mee.

Voorgestelde maatregelen:

- Gefaseerd werken per component
- Wekelijkse meeting met stage mentor om de progressie te overlopen
- Regelmatig testen tijdens ontwikkeling en documenteren

Onbetrouwbare correlatie tussen testen en detecties
Het koppelen van Atomic tests aan detecties kan onnauwkeurig zijn door tijdsvertragingen, meerdere alerts of ruis in de logs.

Voorgestelde maatregelen:

- Gebruik maken van batchvalidatie
- Filteren op specifieke test hosts
- Correlatielogica iteratief verbeteren

Tijdsbeperking van de stageperiode
De beschikbare tijd binnen een stage is beperkt, waardoor niet alle gewenste functionaliteiten gerealiseerd kunnen worden.

Voorgestelde maatregelen:

- Prioriteiten bepalen vanaf de start
- Wekelijkse standup om de progressie te overlopen
- Extra functionaliteiten als uitbreidingen behandelen

Afhankelijkheid van externe systemen
Wanneer externe systemen storingen hebben of traag reageren (API's, agents, dashboards), kan testing tijdelijk onmogelijk zijn.

Voorgestelde maatregelen:

- Buffer voorzien in planning
- Logging, fallback-methodes en back-ups voorzien
- Testen op alternatieve momenten uitvoeren

7. Projectplanning

De uitvoering van het project verloopt over een periode van veertien weken en wordt opgedeeld in verschillende fasen. Elke fase bouwt verder op de resultaten van de vorige fase, zodat de oplossing op een gestructureerde manier kan worden ontwikkeld, gevalideerd en opgeleverd.

7.1. Week 1 – 2: Onboarding en opzetten van de labo-omgeving

Tijdens deze fase ligt de focus op het leren kennen van de organisatie, de gebruikte technologieën en de projectdoelstellingen. Daarnaast wordt een geïsoleerde labo-omgeving opgezet waarin aanvalssimulaties veilig kunnen worden uitgevoerd. De benodigde endpoints, tools en toegangen worden geconfigureerd zodat de verdere ontwikkeling van het project kan starten.

7.2. Week 3 – 5: Ontwikkeling van de correlatielogica

In deze fase wordt onderzocht hoe aanvalssimulaties kunnen worden gekoppeld aan detecties binnen Rapid7 InsightIDR. Verschillende correlatiemethoden worden geëvalueerd en getest om een betrouwbare koppeling te realiseren tussen Atomic Red Team-tests en detectieregels. Daarnaast wordt de detectiedekking geanalyseerd en worden eerste detection gaps in kaart gebracht.

7.3. Week 6 – 9: Ontwikkeling van de Detection-as-Code pipeline

Tijdens deze fase wordt een geautomatiseerde Detection-as-Code pipeline ontwikkeld. Nieuwe detectieregels kunnen hierbij automatisch worden aangemaakt, uitgerold en gevalideerd aan de hand van aanvalssimulaties. Op basis van de validatieresultaten wordt bepaald of een detectieregel correct functioneert voordat deze verder wordt gebruikt binnen de omgeving.

7.4. Week 10 – 11: Ontwikkeling van continue detectievalidatie

In deze fase wordt een geautomatiseerde pipeline ontwikkeld voor het periodiek testen van bestaande detectieregels. Door regelmatig aanvalssimulaties uit te voeren kan worden nagegaan welke detectieregels nog correct functioneren en welke mogelijk verouderd zijn. Daarnaast wordt gewerkt aan de rapportering en centrale visualisatie van de validatieresultaten.

7.5. Week 12 – 13: Documentatie en finale validatie

De focus verschuift naar documentatie en afronding van de oplossing. De architectuur, werking en belangrijkste componenten worden gedocumenteerd. Daarnaast worden finale validaties uitgevoerd om te controleren of alle projectdoelstellingen zijn gerealiseerd en correct functioneren.

7.6. Week 14: Oplevering en afsluiting

De laatste week staat in het teken van de oplevering van het project. De oplossing wordt overgedragen, de resultaten worden gepresenteerd en de projectdocumentatie wordt afgerond. Tot slot wordt gereflecteerd op de behaalde resultaten en mogelijke toekomstige uitbreidingen.

8. Glossary

Term	Uitleg
SOC (Security Operations Center)	Team dat beveiligingsincidenten monitort en analyseert.
SIEM (Security Information and Event Management)	Platform voor het verzamelen en analyseren van logs.
Rapid7 InsightIDR	Het SIEM-platform dat binnen Netleaf wordt gebruikt.
Atomic Red Team	Framework voor het simuleren van aanvalstechnieken.
MITRE ATT&CK Framework	Kennisbank die aanvalstechnieken categoriseert.
Velociraptor	Een geavanceerd, open-source platform voor endpoint bewaking, digitale forensische analyse en incidentrespons (DFIR).
Detectieregel	Regel die verdachte activiteiten detecteert.
Correlatie	Het koppelen van een aanvalssimulatie aan een detectie.
Detectiedekking	Overzicht van welke aanvalstechnieken worden gedetecteerd.
Detection gap	Ontbrekende of onvoldoende detectie voor een aanvalstechniek.
Detection-as-Code	Aanpak waarbij detectieregels via code worden beheerd en gevalideerd.
GitLab CI/CD	Functionaliteit voor het automatisch uitvoeren van pipelines.
Adversary Emulation	Het simuleren van aanvallersgedrag om detecties te testen.

9. Bronnen

9.1. Gebruik van AI

Tijdens het opstellen van dit document werd gebruikgemaakt van AI-ondersteuning voor het verbeteren van de structuur, formulering en leesbaarheid van de teksten. Daarnaast werd AI ingezet ter ondersteuning bij het visualiseren en verfijnen van diagrammen en architectuuroverzichten.

De technische inhoud, analyses, implementatie, configuraties en projectuitwerking werden zelfstandig uitgevoerd en gevalideerd tijdens de stage. AI werd uitsluitend gebruikt als ondersteunend hulpmiddel voor taaloptimalisatie, documentstructuur en visuele presentatie.

9.2. Literatuurlijst

Red Canary, R. (z.d.). *Atomic Red Team*. Opgehaald van https://github.com/redcanaryco/atomic-red-team
GitLab. (z.d.). *GitLab CI/CD Documentation*. Opgehaald van https://docs.gitlab.com/ee/ci/
Grafana Labs, G. (z.d.). *Grafana Documentation*. Opgehaald van https://grafana.com/docs/
MITRE. (z.d.). *MITRE ATT&CK Framework*. Opgehaald van https://attack.mitre.org/
Rapid7. (z.d.). *InsightIDR Documentation*. Opgehaald van https://docs.rapid7.com/insightidr/

9.3. Bijlagen

Figuur 1 Architectuur van de labo-omgeving