Titel van de bachelorproef.

Optionele ondertitel.

Ernst Aarden.

Scriptie voorgedragen tot het bekomen van de graad van
Professionele bachelor in de toegepaste informatica

Promotor: Dhr. F. Van Houte
Co-promotor: Mevr. S. Beeckman
Academiejaar: 2024–2025
Eerste examenperiode

Departement IT en Digitale Innovatie .

Woord vooraf

Samenvatting

De bescherming van vertrouwelijke bedrijfsgegevens vormt een cruciale uitdaging in de digitale wereld, vooral binnen de Belgische juridische context. Deze bachelorproef richt zich op de ontwikkeling en implementatie van een op maat gemaakte Netskope-gebaseerde Data Leakage Prevention (DLP) oplossing, specifiek afgestemd op de Belgische regelgeving. De hoofdonderzoeksvraag is hoe zo'n oplossing effectief kan worden ontworpen en toegepast om zowel te voldoen aan technische en juridische eisen. Met behulp van een combinatie van een literatuurstudie en een praktische Proof of Concept (PoC) worden de mogelijkheden van Netskope beoordeeld in het identificeren, beheersen en voorkomen van datalekken in een realistische testomgeving. Hierbij wordt rekening gehouden met wettelijke kaders zoals de Algemene Verordening Gegevensbescherming (AVG), de NIS2-richtlijn, evenals technische normen zoals PCI DSS en ISO 27001. De PoC zal worden uitgevoerd met realistische datascenario's om de oplossing te evalueren. Het onderzoek levert een werkend prototype van een DLP-oplossing op, samen met praktische aanbevelingen voor bedrijven die hun gevoelige data beter willen beschermen. De conclusie laat zien dat een goed uitgewerkte DLP-oplossing niet alleen helpt om aan de wetgeving te voldoen, maar ook zorgt voor een betrouwbare bescherming tegen datalekken, zelfs in ingewikkelde bedrijfsomgevingen.

Inhoudsopgave

Lijst van figuren

Lijst van tabellen

Lijst van codefragmenten

1

Inleiding

Datalekken zijn tegenwoordig een ernstige bedreiging voor industrieën en overheden. Cyberaanvallen, menselijke fouten en misconfiguraties kunnen leiden tot het verlies van gevoelige informatie. Een van de technologieën dat hierbij kan helpen, zijn Data Loss Prevention (dlp)-oplossingen. DLP-tools identificeren, monitoren en beschermen gevoelige gegevens, zoals **persoonlijke identificeerbare informatie** (pii) en **betalingsgegevens** (pci). De implementatie van DLP-oplossingen is niet alleen een best practice, maar vaak ook een **wettelijke vereiste** onder regelgevingen zoals de Algemene Verordening Gegevensbescherming (avg), de Payment Card Industry Data Security Standards (pcidss) en de nis2-richtlijn voor netwerk- en informatiebeveiliging. Hierdoor zijn DLP-oplossingen essentiële hulpmiddelen geworden om gevoelige informatie te beschermen en gegevensintegriteit te waarborgen. In deze bachelorproef zal een DLP-oplossing opgesteld worden voor **Evolane**, een bedrijf dat zich specialiseert in het optimaliseren en beveiligen van cloud- en enterprise-omgevingen voor organisaties. Evolane is een consultancybedrijf dat klanten helpt bij het implementeren van cloudoplossingen, zoals *Akamai*, *Dynatrace* en *Netskope*. Deze services staan op hun beurt in voor de beveiliging van bedrijfsgegevens en het voorkomen van cyberaanvallen van binnen- en buitenaf.
VerizonBusiness2025<empty citation> stelt in hun *Data Breach Investigations Report 2025* vast dat ransomware in **44%** van alle datalekken voorkwam. Deze aanvallen richten zich steeds meer op gevoelige bedrijfsdata. Aanvallers zullen na de exfiltratie van deze data de organisatie onder druk zetten om losgeld te betalen. Dit soort dubbele-afpersing-aanvallen worden ook wel *leakware* of *doxware* genoemd (**IBM2024**). Deze aanvallen sluiten aan bij enisa's bevindingen, dat het aantal incidenten met datadiefstal en afpersing jaar na jaar ziet toenemen (**EUAC2022**; **EUAC2023**). **IBMSecurity2024<empty citation>** gaven in hun *Cost of a Data Breach Report 2024* aan dat de gemiddelde schade van een ransomware-gerelateerde datalek in 2024 **4,37 miljoen** euro bedroegen (exclusief betaalde los-

gelden). Deze groei toont aan dat ransomware-aanvallen steeds vaker dienen als bewuste inkomstenbron voor cybercriminelen. Aangezien de aanvallen steeds vaker voorkomen, is het als bedrijf belangrijk om de juiste maatregelen te nemen om gevoelige data te beschermen. Evolane stelt vast dat, hoewel de bescherming van **extern** bereikbare applicaties via bijvoorbeeld *Akamai* op een geavanceerde en succesvolle manier gebeurt, de **interne risico's** niet voldoende worden aangepakt. Traditionele beveiliging richt zich voornamelijk op de *externe bezoeker* of *surfer*, maar wanneer een **aanval** via een **eigen medewerker** wordt ingezet, al dan niet bewust, verdwijnt die controle. Klantgesprekken tonen aan dat *phishingcampagnes steeds moeilijker te onderscheiden* zijn van legitieme communicatie. Zelfs goed opgeleide medewerkers kunnen slachtoffer worden van zulke aanvallen. In plaats van het vertrouwen op wantrouwen te baseren, implementeert Evolane een aanpak die medewerkers **ondersteunt** met technologie die hen **helpt fouten** te voorkomen.
Daarom kiest de organisatie voor een architectuur gebaseerd op Secure Service Edge (sse), waarin Data Loss Prevention (dlp) een centrale rol speelt. De keuze valt op Netskope vanwege zijn innovatieve visie op DLP, zijn financiële stabiliteit en zijn erkenning binnen het rechterkwadrant van het Gartner Magic Quadrant, zoals besproken in Hoofdstuk **??**. De technologische sterkte van Netskope sluit bovendien aan bij de klantgerichte aanpak van Evolane. Dit alles vormt de aanleiding om in deze bachelorproef de mogelijkheden van Netskope binnen een DLP-context te onderzoeken.

1.1. Probleemstelling

Evolane wilt de interne risico's van datalekken aanpakken door Netskope's DLP-oplossing te implementeren binnen hun sse-architectuur. Het probleem begint met het bekijken welke verschillende doelgroepen er bestaan binnen het bedrijf en welke confidentiële gegevens er het meest worden verwerkt per groep. Sales medewerkers komen bijvoorbeeld meer in contact met **klantinformatie**, terwijl security engineers meer bezig zijn met **technische configuraties**. Beide groepen verwerken gevoelige gegevens, maar de types gegevens zijn verschillend, net zoals de verwerking van deze gegevens. Tabel **??** geeft een overzicht van de verschillende doelgroepen en hun specifieke uitdagingen bij de implementatie van een DLP-oplossing binnen dit onderzoek. Om false positives te vermijden, zal er een uitgebreide evaluatieperiode moeten plaatsvinden, zoals verder uitgewerkt in Hoofdstuk **??**. Deze periode zorgt ervoor dat de DLP-regels correct worden ingesteld, verfijnt en geoptimaliseerd. De Security engineers zullen tijdens de evalutatieperiode feedback geven over de DLP-regels en de impact op hun workflows.

Doelgroep	Uitdaging(en)	Rol van DLP binnen de oplossing
Salesmedewerkers bij Evolane	Verwerken en delen van klantinformatie via e-mail, cloudopslag of SaaS zonder datalekken te veroorzaken.	Detecteert en blokkeert gevoelige klantgegevens bij ongeoorloofd delen. Verhoogt bewustzijn bij het verwerken van vertrouwelijke data.
Security en Observability engineers bij Evolane	Werken met configuratiebestanden, secrets en infrastructuurgegevens (zoals API keys, IP-adressen) zonder onbedoelde blootstelling.	Herkent technische datatypes (zoals API keys, wachtwoorden, configbestanden) en voorkomt dat deze uitlekken via niet-vertrouwde kanalen.
IT-afdelingen van klanten	Integreren van DLP-oplossing zonder grote architecturale wijzigingen of complexe opleidingsvereisten.	Biedt laagdrempelige integratie, inzichtelijke logging en rapportage met minimale operationele overhead. Evolane blijft implementatie ondersteunen.
Eindgebruikers bij klanten	Onbewuste blootstelling van gevoelige data door gebruik van cloudtools of misleidende phishing-aanvallen.	Intercepteert gevoelige handelingen in real-time en waarschuwt gebruikers bij risicovolle acties zonder workflows te blokkeren.

Tabel 1.1: Overzicht van doelgroepen, uitdagingen en rol van DLP

1.2. Onderzoeksvraag

De centrale vraag van dit onderzoek is: “Hoe kan een op Netskope gebaseerde DLP-oplossing worden ontworpen en geïmplementeerd om vertrouwelijke gegevens te beschermen en te voldoen aan de Belgische regelgeving?”. Vanuit deze hoofdvraag kunnen we een aantal deelvragen afleiden:

- Welke mogelijkheden biedt Netskope’s Secure Service Edge (sse) platform voor Data Leakage Prevention in de context van vertrouwelijke gegevensbescherming?
- Hoe kunnen regelsets en dataclassificatie in Netskope DLP worden afgestemd op de Belgische wetgeving, zoals de avg en nis2-richtlijn?
- Welke technieken en methoden kunnen worden toegepast om persoons- en betalingsgegevens effectief te detecteren en te beschermen binnen het Netskope-platform?
- Hoe kan een Proof of Concept (PoC) voor Netskope DLP worden opgezet in een testomgeving om de effectiviteit van de oplossing te evalueren?

- Welke juridische en technische normen moeten worden meegenomen bij het ontwerpen van een DLP-oplossing voor een Belgische organisatie, en hoe kan Netskope aan deze eisen voldoen?

1.3. Onderzoeksdoelstelling

In dit onderzoek wordt een Proof of Concept (PoC) klantomgeving ontwikkeld voor Evolane. In deze omgeving worden zowel confidentiële als niet-confidentiële gegevens verwerkt en opgeslagen. Door een Data Leakage Prevention-oplossing te implementeren, worden deze gegevens beveiligd tegen lekken. De DLP-oplossing moet voldoen aan de Belgische wetgeving, waaronder de Algemene Verordening Gegevensbescherming (avg) over persoonsgegevens (pii) en de pcidss met betrekking tot betalingsgegevens (pci). De DLP-oplossing moet verder rekening houden met de nis2-richtlijn en andere cybersecuritykaders, zoals het CCB-kader of iso. De PoC bevat een Netskope-gebaseerde DLP-oplossing die confidentiële gegevens beschermt en voldoet aan de Belgische regelgeving.
Om een breder inzicht te verkrijgen in de implementatie en optimalisatie van Data Loss Prevention (DLP)-oplossingen, wordt in deze bachelorproef verder onderzocht hoe DLP kan worden toegepast in verschillende contexten en omgevingen. De onderstaande gebieden vormen de focus van dit onderzoek:

- **saas** (Software as a Service): DLP-oplossingen richten zich op gegevens in beweging (*Data-in-Motion*), zoals bij het gebruik van forward proxies en bij statische gegevens (*Data-at-Rest*) voor APIs.
- **Web**: Hier wordt DLP toegepast op geëncrypteerd verkeer en voor alle poorten, met focus op gegevens in beweging tussen systemen.
- **iaas** (Infrastructure as a Service): Net zoals bij saas, wordt DLP toegepast op gegevens in beweging en in rust, respectievelijk voor forward proxies en APIs.
- **Email**: Bij het beheren van e-mailverkeer, zoals webmail, richt de uitgewerkte DLP-oplossing zich zowel op gegevens in beweging als op gegevens in rust.
- **Endpoint**: Endpoint Data Loss Prevention (DLP) richt zich op het beschermen van gegevens in gebruik (*Data-in-Use*) door middel van endpointbeveiliging. Dit houdt het volgende in: het monitoren en beperken van gegevensoverdracht via usb-opslagmedia, klemborden, printers en andere externe apparaten.

1.4. Opzet van deze bachelorproef

De rest van deze bachelorproef is als volgt opgebouwd: In Hoofdstuk **??** wordt een overzicht gegeven van de stand van zaken binnen het onderzoeksdomein, op basis van een literatuurstudie. In Hoofdstuk **??** komen de methodologie en de gebruikte

onderzoekstechnieken aan bod om een antwoord te kunnen formuleren op de onderzoeksvragen. In Hoofdstuk **??** wordt een risicoanalyse uitgevoerd om de impact van datalekken en de noodzaak van DLP-oplossingen te onderbouwen. In Hoofdstuk **??** wordt een Proof of Concept (PoC) opgezet om de effectiviteit van de Netskope DLP-oplossing te evalueren. In Hoofdstuk **??** wordt de PoC geëvalueerd door gebruikers. In Hoofdstuk **??** worden de resultaten van het onderzoek besproken en wordt een antwoord geformuleerd op de onderzoeksvragen. In Hoofdstuk **??** zal tenslotte de conclusie en de toekomstige onderzoeksmogelijkheden binnen dit domein worden besproken.

2

Stand van zaken

2.1. Data Leakage Prevention (DLP)

Een DLP-systeem heeft als doel drie soorten gegevens binnen een organisatie te beschermen: data-at-rest, data-in-motion en data-in-use. Data-at-rest verwijst naar statische informatie die is opgeslagen in bedrijfssystemen, zoals documentbeheersystemen, e-mailservers, bestandsservers, netwerkschijven, persoonlijke computers en opslagruimtenetwerken (san). Data-in-motion verwijst naar bedrijfsdata dat wordt verwerkt binnen het uitgaande netwerkverkeer, zoals e-mails en online verkeer. Data-in-use bestaat uit informatie die medewerkers gebruiken op eindgebruikersapparaten, zoals een bestand kopiëren naar een USB-schijf. De definitie van vertrouwelijkheid binnen een organisatie vereist een grondigere analyse. Soorten informatie zoals pii, inclusief namen, identiteitskaart- en creditcardgegevens, worden doorgaans in elke organisatie als vertrouwelijk beschouwd. Deze definitie krijgt echter ingewikkeldere aspecten bij bedrijfsgeheimen en interne communicatie, die vaak onregelmatig zijn. Vertrouwelijke informatie verwijst naar gegevens die binnen de organisatie zijn verzameld en niet algemeen toegankelijk zijn. Een DLP-systeem bevat de mogelijkheid om gevoelige gegevens te herkennen in een of meerdere van de genoemde datatypen.

2.1.1. PCI en PII

Persoonlijk identificeerbare informatie (pii), zoals namen, rijksregisternummers, e-mailadressen, telefoonnummers en dergelijke kunnen direct of indirect worden gebruikt voor de identificatie van een persoon. Met het oog op de avg zijn er strikte regels met betrekking tot toestemming en transparantie bij de verwerking van pii. Payment Card Industry (pci)-gegevens bevatten alle kaart- en betaalgegevens zoals debit-/creditcardnummers, Primary Account Numbers (pan) en andere confidentiële authenticatiegegevens zoals cvv. Om te voldoen aan de pcidss-norm,

moeten organisaties strenge maatregelen implementeren om deze kaartgegevens te beveiligen. Bedrijven die pii- en pci-data verwerken lopen het risico op zware sancties als deze gegevens niet voldoende beschermd worden.

2.1.2. Detectie methoden voor gegevensverlies

Identificatiemiddelen worden gebruikt om gevoelige informatie, zoals pii en pci, te detecteren. Dit gebeurt op basis van reguliere expressies (regex). Regex is een krachtig hulpmiddel dat DLP helpt specifieke gegevenstypen te herkennen door middel van uitdrukkingen, termen en patronen, zoals `BE\d{2}\s?\d{4}\s?\d{4}-\s?\d{4}` dat kan dienen voor Belgische iban-codes. Hoewel dit patroon effectief is voor standaard iban-formaten, kan het worden omzeild door een karakter toe te voegen in de invoer, wat het belang benadrukt van extra controles.
De aangemaakte identificatie voor confidentiële gegevens moet voldoen aan de volgende richtlijnen:

- Vooraf gedefinieerde en aanpasbare patronen voor datadetectie: Het is cruciaal om duizenden vooraf ingestelde regels voor het herkennen van gegevens beschikbaar te hebben en deze te kunnen aanpassen aan de behoeften van de organisatie.
- Ondersteuning voor verschillende soorten bestandstypen (Word, Excel, PDF, JPG, PNG, CSV, ZIP en RAR, enz.) en categorieën (afbeeldingen, databases, spreadsheets, enz.).
- Ondersteuning voor landspecifieke identificatienummers (iban's, postcodes, adressen, nationale identiteitskaarten, IP-adressen, paspoort- en telefoonnummers).
- Voldoen aan de wet- en regelgeving.

De bescherming van pii en pci-gegevens vormt een kernaspect van DLP. **Wason2020CASB<empty** legt de nadruk op het belang van de integratie van Cloud Access Security Brokers (casb) in cloudomgevingen. casb biedt organisaties de mogelijkheid om een uitgebreide zichtbaarheid te krijgen in het gebruik van cloudtoepassingen, inclusief goedgekeurde en ongeautoriseerde (shadow IT) diensten. Het houdt bij hoe de confidentiële data wordt opgeslagen en verplaatst/verwerkt, wat handig is voor het identificeren van deze data en het voorkomen van datalekken.

2.1.3. Regelsets

De regelsets binnen Netskope zijn de focus van dit onderzoek. Deze bestaan uit een combinatie van verschillende identificatiemethoden, zoals beschreven in de documentatie van **Netskope2025DLP<empty citation>**. Deze identificatoren of ook entiteiten genoemd, zijn de basis van DLP-regels en vormen samen een regelset. Meerdere regelsets kunnen worden gedefinieerd binnen een profiel (**Netskope2025Profiles**).

Tabel naar Nederlands

- **Predefined data identifiers**: Dit zijn vooraf gedefinieerde identificatoren die zijn ontworpen door Netskope.
- **Custom data identifiers**: Dit zijn op maat gemaakte identificatoren die organisaties kunnen definiëren om specifieke soorten gevoelige gegevens te herkennen die relevant zijn voor hun bedrijfsvoering.
- **Keyword identifiers**: Dit zijn specifieke woorden of zinnen die worden gebruikt om gevoelige gegevens te identificeren. Dit kan bijvoorbeeld een lijst zijn van veelvoorkomende achternamen die in combinatie met een rijksregisternummer kunnen worden gebruikt.
- **Regular expressions (RegEx)**: Dit zijn patronen die worden gebruikt om specifieke gegevensformaten te identificeren. RegEx kan worden gebruikt om complexe gegevensstructuren te herkennen, zoals iban-nummers of e-mailadressen.
- **Exact match criteria**: Dit zijn specifieke voorwaarden die moeten worden vervuld om te bepalen of een gegevenstype als gevoelig wordt beschouwd, zoals

Vooraf gedefinieerde regelsets

Netskope biedt een uitgebreide set vooraf gedefinieerde regelsets binnen zijn DLP-functionaliteit. Hiermee kan gevoelige informatie, zoals pii en pci, effectief worden gedetecteerd en beschermd. Volgens **brouwer2021cloud<empty citation>** heeft Netskope een uitgebreide lijst van DLP-profielen ontwikkeld die helpen bij het identificeren van allerlei soorten pii, verschillend van EU-identificatiegegevens tot Singaporese identificatiegegevens en medische rapporten. Deze regelsets zijn uitgebalanceerd en sluiten aan bij de regelgeving van de meeste westerse landen. Deze vooraf gedefinieerde regelsets zijn niet veranderbaar en kunnen niet verder worden gepersonaliseerd. Gebruikers kunnen echter wel hun eigen DLP-profielen definiëren voor specifieke use-cases, zoals in volgende sectie wordt besproken.
Een voorbeeld van een vooraf gedefinieerde regelset is de regelset voor 'DLP-PII', die is ontworpen om gevoelige persoonlijke informatie te identificeren en te beschermen. Deze regelset omvat gegevens zoals naam, adres, geboortedatum, e-mailadres, MedicareID, paspoortinformatie en sociale zekerheidsnummers. Alleen zijn deze specifiek gericht voor de Verenigde Staten en Canada. Aangezien dit onderzoek zich richt op de bescherming van Belgische persoons- en betalingsgegevens, voldoet deze regelset niet aan de vereisten van de Belgische wetgeving.
Daarnaast biedt Netskope ook de 'EU General Data Protection Regulation (GDPR)' regelset aan, die specifiek is ontworpen om te voldoen aan al de vereisten van de avg. Deze regelset richt zich op persoonsgegevens van een natuurlijk persoon binnen de Europese Unie. In Tabel **??** zijn de gegevenscategorieën weergegeven die Netskope heeft gedefinieerd voor deze regelset (**Netskope2023GDPR**). De entiteit/dataset zelf is niet publiek beschikbaar, dus zal deze aan de hand van een steekproefevaluatie worden beoordeeld.

Categorie	Gegevens
Adres	pan Vervaldatum, Naam, IP-adres, Telefoonnummer, E-mail, Region, Region-Date
Rijbewijs	Geboortedatum, Naam, Adres, Geslacht, Rijbewijsnummer, Uitgiftedatum, Vervaldatum
Identiteit	Biometrische gegevens, Geboortedatum, Naam, Geslacht, Etniciteit, Religie, Lengte, Gewicht, Haarkleur, Oogkleur, Gezondheidsgegevens, Handtekening, Nationaal Identificatienummer
Naam	pan, IP-adres, Telefoonnummer, E-mail, Politieke voorkeur, Criminele geschiedenis, Religie, Etniciteit, Geslacht, Lengte, Gewicht, Haarkleur, Oogkleur, Voorkeursnaam, Alias
Paspoort	Naam, Adres, Geboortedatum, Biometrische gegevens, Paspoortnummer, Uitgifteland, Uitgiftedatum, Vervaldatum

Tabel 2.1: Data categorieën van EU-AVG-ruleset (**Netskope2023GDPR**)

Aangepaste regelsets

De focus van dit onderzoek ligt op de aangepaste regelsets, zoals besproken in Hoofdstuk **??**. Elke regelset, oftewel profiel genoemd, bestaat uit DLP-regels, content classificaties of fingerprintregels (**Netskope2025CreateProfiles**). Elke regel bestaat uit een of meerdere entiteiten, die elk een specifiek type gegevens identificeren. Dit kan bijvoorbeeld een specifieke reeks cijfers zijn die overeenkomt met een rijksregisternummer of een reeks woorden die samen een bepaalde context vormen, zoals een naam in de buurt van een adres.

2.1.4. Entiteit

De entiteit is de basis van een DLP-regel. Deze entiteit houdt verschillende vormen van gegevens bij, zoals een reeks cijfers, woorden of zinnen. Dit onderzoek basseert zich op het gebruik van de entiteit 'Exact Match' en 'Regular Expression'. De configuratie gebruikt standaard de vooraf gedefinieerde entiteiten van Netskope. Als Netskope voor een specifieke behoefte geen vooraf gedefinieerde entiteit voorziet, dan zal een aangepaste entiteit worden aangemaakt. Deze aangepaste entiteiten zullen vooral bestaan uit 'Exact Match', aangezien regex-regels, dankzij hun complexiteit, meer false positives kunnen genereren.

2.1.5. Detectienauwkeurigheid

Detectienauwkeurigheid houdt in hoe goed het DLP-systeem in staat is om confidentiële gegevens te identificeren. Een hogere detectienauwkeurigheid wordt

bereikt door het gebruik van goed afgestemde regelsets en geavanceerde herkenningsmethoden, zoals reguliere expressies (regex), keywords en contextuele analyse. Netskope maakt gebruik van predefined datasets voor het verbeteren van de detectienauwkeurigheid. Deze datasets bevatten gestructureerde gegevens zoals pii en bieden ondersteuning voor verschillende soorten eisen, waaronder de avg (**Clementelli2023**). Netskope maakt ook gebruik van een vertrouwheidsscore om de betrouwbaarheid van de gedetecteerde data te bepalen. Deze score helpt bij het evalueren van de waarschijnlijkheid dat bepaalde gegevens confidentieel zijn, wat nodig is voor het verminderen van false positives en false negatives. Om deze nauwkeurigheid te verhogen, kunnen regelsets aangepast worden aan nieuwe typen confidentiële data of veranderende bedrijfsprocessen. In deze proof-of-concept wordt de detectienauwkeurigheid beoordeeld door de verhouding tussen true positives, false positives, false negatives en true negatives, samengevat in een Confusion Matrix (**Microsoftn.d.**). Bij de evaluatie van de detectienauwkeurigheid wordt er gebruik gemaakt van generieke datasets, zoals de *Enron Email Dataset* en de *CICIDS 2017* dataset.

2.1.6. Systeemimpact

De implementatie van een DLP-oplossing kan een merkbare impact hebben op de prestaties van een IT-systeem, wat invloed heeft op de workflow en gebruikerservaring van de eindgebruikers. Netskope heeft een cloudgebaseerde architectuur die het mogelijk maakt om DLP-regels in real-time toe te passen op zowel in- als uitgaand netwerkverkeer. Deze deep content inspection toepassing houdt in dat Netskope continu gegevens inspecteert en analyseert. Afhankelijk van de configuratie en de hoeveelheid netwerkverkeer kan dit leiden tot een verhoogd CPU- en geheugengebruik bij de eindgebruikers, vooral wanneer er meerdere complexe DLP-regels actief zijn. Volgens de documentatie van **Netskope2025Utilization<empty citation>** functioneert de DLP-oplossing stabiel onder productielast, zolang het correct is afgestemd op de infrastructuur en het netwerkverkeer. Tenslotte spelen netwerklatentie, throughput ook een belangrijke rol in de gebruikerservaring. **Netskope2021SLA<empty cita** heeft een Service Level Agreement (SLA) opgesteld die garandeert dat de latentie voor niet-gedecodeerd verkeer minder dan 10 milliseconden bedraagt. Voor gedecodeerd verkeer, zoals SSL/TLS-verkeer dat wordt ontsleuteld voor inspectie, is de latentie gegarandeerd onder de 50 milliseconden. Aangezien deze SLA-waarden bijzonder laag liggen, voert dit onderzoek hierover geen diepgaande technische analyse uit. In plaats daarvan evalueert dit onderzoek de impact vanuit het perspectief van de eindgebruikers en verwerkt deze in de gebruikersevaluatie.

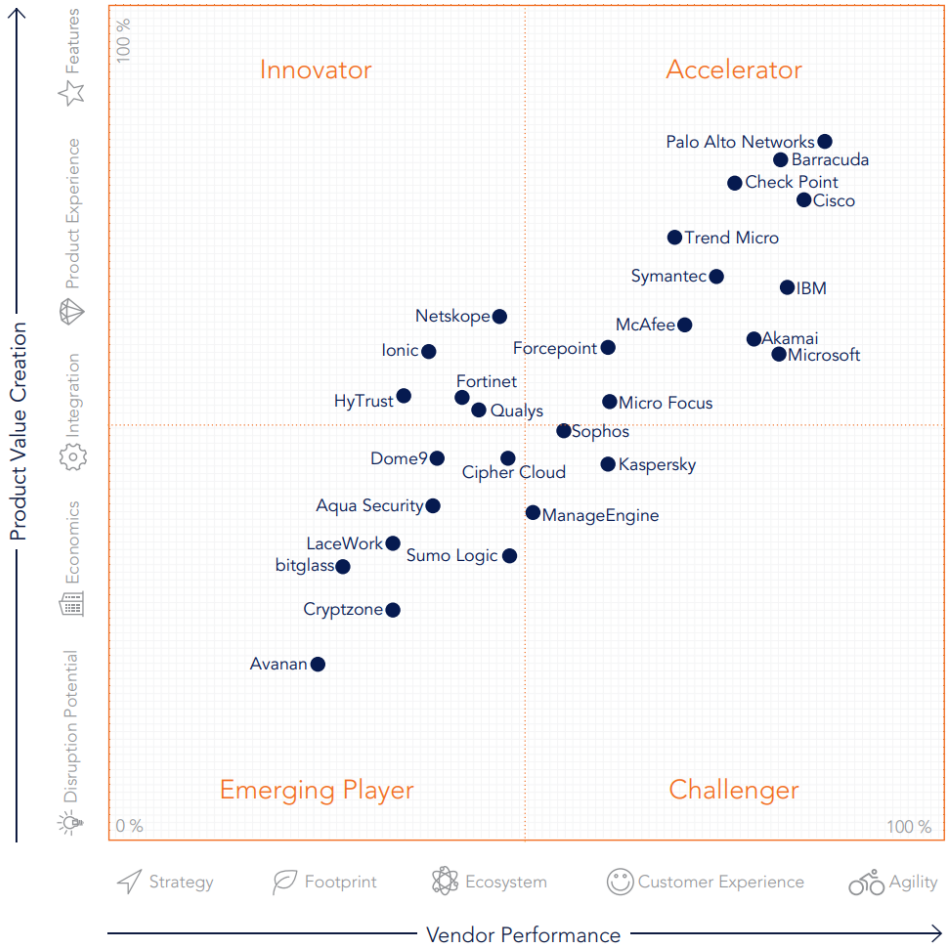
2.2. Netskope

Netskope heeft zich ontwikkeld tot een vooraanstaande speler in cloudbeveiliging door zijn geavanceerde Secure Service Edge (SSE)-platform. Het levert geïntegreerde

CASB- en DLP-mogelijkheden. Volgens **Riley2018<empty citation>** onderscheidt Netskope zich met functies zoals flexibele regelconfiguraties en realtime-detectie van gevoelige data. **VanDerWalt2022<empty citation>** identificeren belangrijke aspecten binnen Secure Access Service Edge (SASE) frameworks die nog onvoldoende onderzoek bevatten, onder meer netwerk- en beveiligingsdiensten in een cloudgebaseerde omgeving. Deze aspecten zijn onder andere de integratie van verschillende beveiligingscomponenten zoals Secure Web Gateways (SWG), CASB en Zero Trust Network Access (ZTNA). Hierbij dienen deze onderdelen samen te werken om een integrale beveiligingsstrategie te creëren. Om deze integratie van beveiligingscomponenten en Zero Trust-principes verder te versterken, is Netskope lid van de **SpectraAlliance2025<empty citation>**, een samenwerking tussen vier cybersecuritybedrijven: CrowdStrike, Okta, Proofpoint en Netskope. Deze alliantie is gericht op het bieden van een sterke Zero Trust-architectuur door verschillende beveiligingsdomeinen samen te laten werken. Netskope levert hierbij expertise op het gebied van cloud- en webbeveiliging, met een sterke focus op DLP en CASB-functionaliteiten. Bovendien is er een toenemende vraag naar het ontwikkelen van API-integraties voor Security Information and Event Management (SIEM)-systemen, zodat gegevens uit verschillende bronnen effectief kunnen worden verzameld en geanalyseerd.
Bij het evalueren van DLP-oplossingen binnen een SASE-architectuur is Netskope gekozen vanwege de unieke combinatie van functionaliteiten en prestaties die het biedt, evenals de verhouding ten opzichte van andere oplossingen. In 2018 werd Netskope door **Hille2018<empty citation>** beschreven als een van de innovators voor Cloud Security Management Platforms, zoals te zien in Figuur **??**. Toen waren ze volgens **Hille2018<empty citation>** nog relatief onder de radar, maar met een zeer aantrekkelijk productaanbod. Dit aanbod is sindsdien verder uitgebreid en omvat nu een breed assortiment aan functies die zijn ontworpen om cloudarchitecturen te beschermen.
In de meest recente Magic Quadrant voor Security Service Edge (SSE) positioneert Gartner Netskope opnieuw als Leader, zoals weergegeven in Figuur **??**.

2.3. False Positives

False positives bij een DLP-systeem ontstaan wanneer legitieme gegevens onterecht als confidentieel worden geclassificeerd. Dit kan leiden tot ***onnodige waarschuwingen***, ***vertragingen in bedrijfsprocessen*** en ***frustratie bij eindgebruikers***. **Lukas2023<empty citation>** legt uit dat dit probleem vooral voorkomt in systemen die gebruik maken van machine learning (ml) en natuurlijke taalverwerking (nlp). Dit komt doordat deze systemen vaak niet in staat zijn om de context van gegevens correct te interpreteren, wat leidt tot onjuiste classificaties. Concreet stelt **Lukas2023<empty citation>** dat deze false positives vooral voorkomen door:



Figuur 2.1: Quelle: Crisp Research AG, 2018 - Cloud Security Management Platforms (**Hille2018**)

- **Overmatige generalisatie van patronen**: Het taalmodel associeert bepaalde woordcombinaties, zoals e-mailadressen of namen, automatisch met gevoeligheid, zonder voldoende contextuele verificatie.
- **Gebrek aan semantisch onderscheid**: De modellen begrijpen onvoldoende het verschil tussen bv. een fictieve naam in een handleiding versus een echte naam in een medisch verslag.
- **Bias in trainingsdata**: Als de trainingsgegevens oververtegenwoordigd zijn met bepaalde formats of types van informatie, zal het model die patronen als gevoelig beschouwen, ook als dat in de praktijk niet klopt.

Olateju2024<empty citation> stelt vast dat DLP-systemen gemiddeld een false positive-percentage van 4% tot 5% vertonen, zelfs bij gebruik van geavanceerde deep learning-algoritmen. Dit lijkt misschien beperkt, maar in grote organisaties of cloudomgevingen met duizenden datatransacties per dag kan dit resulteren in een aanzienlijke hoeveelheid foutieve waarschuwingen.

Figuur 2.2: Gartner Magic Quadrant voor Security Service Edge (SSE) (**Gartner2024**)

2.4. Juridisch kader voor gegevensbescherming in België

De bescherming van persoonlijke en bedrijfsinformatie is een essentieel aspect van de hedendaagse digitale samenleving. Op zowel nationaal als Europees niveau zijn er wettelijke richtlijnen opgesteld om organisaties te ondersteunen bij het garanderen van de vertrouwelijkheid, integriteit en toegankelijkheid van gegevens.

2.4.1. Algemene Verordening Gegevensbescherming (AVG)

Dit onderzoek zal in overeenstemming zijn met de Algemene Verordening Gegevensbescherming (AVG of GDPR) 2016/679 van 27 april 2016 (**eu_avg2016**) en de Belgische wet van 30 juli 2018 (**BelgischeOverheid2018**). Volgens de **eu_avg2016<empty citation>**, overweging (78), moeten passende, technische en organisatorische maatregelen worden genomen om de rechten van natuurlijke personen te beschermen. Deze overweging zorgt ervoor dat persoonsgegevens op een veilige en verantwoorde manier worden verwerkt. Zo'n beveiliging kan gebeuren door middel van standaardinstellingen die erop zijn gericht om risico's in elke fase van de verwerking

van gegevens te minimaliseren. Op 25 juli 2024 publiceerde de Europese Unie haar tweede verslag over de toepassing van de AVG (**eu_avg2024**). Dit rapport legt de nadruk op het feit dat de AVG, ondanks verschillende uitdagingen, een goede basis is voor het veilig en transparant behandelen van persoonsgegevens.

2.4.2. Payment Card Industry Data Security Standard (PCI DSS)

De Payment Card Industry Data Security Standard (pcidss) bestaat uit een reeks richtlijnen en regels die ontworpen zijn voor organisaties die betalingsinformatie en kaartinformatie verwerken, zoals debit-/ creditcardnummers, Primary Account Numbers (pan) en Sensitive Authentication Data (sad), zoals Card Verification Value (cvv) en magnetische stripgegevens, van alle grote kaartschema's. Deze standaard is ontwikkeld om de veiligheid van kaartinformatie te garanderen en vereist dat organisaties maatregelen nemen om de gegevens van kaarthouders te beschermen (**Elluri2018**). pcidss vereist de implementatie van toegangscontroles, zoals dcs**-02** (toegangscontrole tot systemen en gegevens), dcs**-07** (beheer van gebruikersidentiteiten en -toegang), en dcs**-08** (toegangscontrole tot netwerken en systemen), om de veiligheid van kaartinformatie en de bescherming van kaarthoudergegevens te waarborgen (**Elluri2018**).

2.4.3. ISO 27001: Informatiebeveiliging

Bovendien moet de DLP-oplossing rekening houden met de vereisten van iso, de internationale norm voor het beheer van informatiebeveiliging. In dit verband bespreken **Alsanabani2020<empty citation>** de noodzaak van DLP-oplossingen die zowel detectie- als preventieve methoden samenbrengen. De preventieve aanpak probeert datalekken te vermijden door onder andere het gehele confidentiële bestand te versleutelen, toegangscontrole aan te passen en het labelen van de inhoud.

2.4.4. Nationale en Europese richtlijnen

Buiten de Belgische wetgeving zijn er ook tal van Europese richtlijnen en nationale standaarden die een belangrijke rol hebben in de bescherming van bedrijfsdata. Hierbij kan gedacht worden aan de Algemene Verordening Gegevensbescherming (avg), de EU Cybersecurity Act en belangrijke Europese richtlijnen, waaronder de nis2-richtlijn. Deze richtlijnen worden verder uitgebreid met specifieke normen, zoals de pcidss voor betalingsgegevens en internationale normen, zoals iso voor de beveiliging van informatie. De nis2-richtlijn (Richtlijn (EU) 2022/2555), die op 16 januari 2023 is aangenomen door de **nis2directive<empty citation>**, heeft als doel de cyberbeveiliging binnen de EU te versterken door een hoog niveau van beveiliging te waarborgen voor netwerken en informatiesystemen. Artikel 21 van de nis2-richtlijn richt zich op de beveiliging van netwerken en informatiesystemen en legt de verplichting op aan lidstaten om ervoor te zorgen dat aanbieders van essenti-

ële en belangrijke diensten passende technische en organisatorische maatregelen nemen. Maatregelen die over het DLP-systeem kunnen gaan, zijn onder andere:

- Risicoanalyse (lid 2, punten a en e): Organisaties moeten een risicobeheerproces implementeren dat hen in staat stelt om risico's voor de beveiliging van netwerken en informatiesystemen te identificeren, te evalueren en te beheersen.
- Encryptie en toegangscontroles (lid 2, punten h en i): Het gebruik van encryptie, toegangscontroles en regelmatige beveiligingstests en audits.
- Incidentenbehandeling (lid 2, punt b): Organisaties moeten procedures en mechanismen hebben voor het detecteren, melden en reageren op beveiligingsincidenten.
- Bewustwording en training (lid 2, punt g): Opleidingen om medewerkers te informeren over goede cyberhygiëne en risicomanagement (**nis2directive**). Het DLP-systeem van Netskope staat in voor het trainen van de eindgebruiker, mocht deze iets foutief doen.

De studie van **Nayak2020<empty citation>** geeft een uitgebreid overzicht van systemen voor het detecteren en voorkomen van datalekken, inclusief de indeling van systemen op basis van de status van de gegevens (data-at-rest, data-in-motion, data-in-use) en de detectietechnieken. Dit overzicht zal gebruikt worden voor het ontwikkelen van regex-gebaseerde regels in DLP-oplossingen. De studie legt de nadruk op het feit dat datalekken zowel onvoorzien als opzettelijk kunnen optreden en geeft uitdagingen aan, zoals het identificeren van gevoelige informatie, het balanceren van de detectienauwkeurigheid en de integratie van geavanceerde methodologieën.

2.4.5. Andere relevante wetgeving

Tabel **??** bevat de belangrijkste wettelijke richtlijnen en uitspraken die relevant zijn voor het ontwerp en de implementatie van een Data Leakage Prevention-oplossing voor Belgische bedrijven.

2.5. Ethische overwegingen

Een essentieel aspect van de implementatie van DLP is het vinden van de juiste balans tussen gegevensbeveiliging en gebruikersprivacy. Het gebruik van DLP-systemen kan leiden tot het monitoren van gebruikersgedrag, wat kan worden gezien als een inbreuk op de privacy van medewerkers. Om het vertrouwen bij medewerkers en klanten te behouden, is het belangrijk om transparant te zijn over het gebruik van DLP-systemen en de redenen daarvoor. Hierdoor weet elke gebruiker welke gegevens worden verzameld en hoe deze worden gebruikt (**Zaini2024**).

Wetgeving	Doel	Relevantie voor DLP
avg	Bescherming persoonsgegevens	Dataclassificatie en toegangscontrole
pcidss	Beveiliging van betalingsgegevens	Encryptie en toegangsbeheer
iso	Informatiebeveiliging	Risicoanalyse en ISMS-implementatie
ccb-framework	Strategie voor cybersecurity België	Aanbevelingen voor risicobeheer
nis2	Beveiliging netwerken en diensten	Incidentrapportage en risicoanalyse
EU Cybersecurity Act	Certificering van beveiligingstechnologie	DLP-oplossingen certificeren
Schrems II	Gegevensoverdracht naar niet-EU-landen	Beperking van cloud-gebaseerde opslag

Tabel 2.2: Overzicht van wetgeving en relevantie voor DLP

Deze regelsets moeten niet alleen voldoen aan de wettelijke vereisten, maar ook aan de ethische normen en waarden van de organisatie. Om monitoring van data en gebruikersgedrag te minimaliseren, zal de implementatie van de DLP-oplossing specifiek gericht zijn op het beschermen van gevoelige gegevens en het voorkomen van datalekken.
Tijdens het vak *IT Professional & Career Orientation (ITPCO)* kwam het belang van ethische en juridische aspecten binnen informatieveiligheid uitgebreid aan bod. Gastspreker **SoficoGuestLecture2024<empty citation>** van *Sofico* presenteerde een overzicht van hoe een internationaal bedrijf dat softwareoplossingen ontwikkelt voor autofinanciering, leasing, fleetmanagement en mobiliteitsbeheer, privacy en compliance structureel integreert in zijn processen (**SoficoGuestLecture2024**). Het gastcollege behandelde onder meer fysieke beveiligingsmaatregelen, toegangsbeheer tot ontwikkelomgevingen en de inzet van white hat hackers voor het identificeren van kwetsbaarheden. De organisatie gebruikt principes zoals *Privacy by Design* en *Security by Design* binnen de volledige ontwikkeling en implementatie van software. Deze principes staan in lijn met de avg en iso normen, waarbij de focus ligt op het minimaliseren van gegevensverwerking en het behouden van de privacy van gebruikers. De inzichten van Sofico zijn rechtstreeks van toepassing op dit onderzoek. *Privacy by Design* en *Security by Design* zijn namelijk gericht op minimale gegevensverwerking, transparantie, logging en traceerbaarheid. Binnen **Netskope2024PrivByDesign<empty citation>** worden deze principes toegepast via ***in-memory verwerking***, ***gegevensobfuscatie***, ***klantgecontroleerde datalokalisatie*** en ***uitgebreide transactie-logging***.

3

Methodologie

Het onderzoek naar de ontwikkeling en integratie van een Netskope-gebaseerde Data Leakage Prevention (DLP)-oplossing binnen de bedrijfsomgeving van Evolane. De onderzoeksmethode is een combinatie van een literatuurstudie en een praktische Proof of Concept (PoC).

3.1. Literatuurstudie

Het onderzoek begint met een uitgebreide literatuurstudie naar bestaande DLP-oplossingen, Netskope's Secure Service Edge (sse) platform en de relevante Belgische en Europese wetgevingen. Hierbij wordt gebruik gemaakt van academische artikelen, technische documentatie en juridische bronnen om een basis te leggen. Voor de literatuurstudie is ongeveer twee weken voorzien, waarin de focus ligt op het verder verzamelen en verwerken van recente bronnen over DLP-technologie, juridische eisen (avg, pcidss, nis2) en Netskope's DLP-oplossing.

3.2. Analyse en planning

Na de literatuurstudie volgt de selectie van specifieke datasets, zoals persoonlijk identificeerbare informatie (pii) en betalingsgegevens (pci), voor testen binnen de PoC. Een voorbeeld hiervan zijn de synthetische e-maildatasets van **Whelan2014<empty citation>**. Deze datasets bevatten in totaal 4796 e-mails, waarvan 4010 geen pii bevatten en 786 e-mails dit wel hebben, waaronder adressen, creditcardnummers en namen. De opgestelde testscenario's sluiten aan bij de bedrijfsprocessen van Evolane, zoals e-mailverkeer en bestandsoverdrachten naar cloudservices. Naast deze scenario's richt de analyse zich ook op de workflow van eindgebruikers, met als doel False Positives te beperken en de de workflow van de eindgebruikers niet te verstoren. Deze fase begint al deels tijdens de literatuurstudie en duurt ongeveer drie weken.

3.3. Risicoanalyse

Een belangrijk onderdeel van dit onderzoek is het uitvoeren van een risicoanalyse, waarbij mogelijke technische, juridische en organisatorische risico's worden geïdentificeerd en beoordeeld. Technische risico's kunnen bijvoorbeeld bestaan uit het niet volledig detecteren van gevoelige gegevens of prestatieproblemen van het DLP-systeem. Juridische risico's hebben te maken met het niet naleven van de avg-vereisten of andere relevante wetgeving. Organisatorische risico's omvatten mogelijke weerstand van medewerkers tegen nieuwe beveiligingsmaatregelen of een gebrek aan training, wat de effectiviteit van de DLP-oplossing kan verminderen. Voor elk vastgesteld risico worden geschikte maatregelen genomen om de gevolgen te beperken. Deze fase duurt ongeveer twee weken, overlappend met Analyse en Planning. Op het vlak van expertise zal hierbij de co-promotor van Evolane betrokken worden.

3.3.1. Technische risico's

Technische risico's zijn gerelateerd aan de operationele elementen van de DLP-oplossing en de technische infrastructuur van Evolane. Een van de belangrijkste technische risico's is de onvolledige detectie van confidentiële gegevens. Het DLP-systeem kan mogelijk niet alle vormen van pii en pci detecteren, vooral als er nieuwe of onbekende datatypes worden gebruikt. Daarnaast kan de implementatie van Netskope leiden tot prestatieproblemen, zoals vertragingen in netwerkverkeer of een verhoogd gebruik van systeemresources. Integratieproblemen vormen een ander potentieel risico, aangezien het DLP-systeem moet werken met bestaande IT-infrastructuren. Onverwachte compatibiliteitsproblemen kunnen de implementatie vertragen. Vervolgens kunnen verdere beveiligingslekken ontstaan door onvoldoende configuratie of zwakke punten in het DLP-systeem, waardoor confidentiële data alsnog kan worden gelekt. Om deze technische risico's te mitigeren, zullen uitgebreide tests worden uitgevoerd om de detectienauwkeurigheid van het DLP-systeem te waarborgen. Daarnaast zullen systeemprestaties worden gemonitord tijdens de implementatie en indien nodig optimalisaties worden doorgevoerd om prestatieproblemen te minimaliseren. Tenslotte zal een plan worden opgesteld hoe het DLP-systeem veilig geüpdatet kan worden om potentiële kwetsbaarheden te vermijden.

3.3.2. Juridische risico's

Juridische risico's hebben betrekking op de naleving van wet- en regelgeving, zoals de Algemene Verordening Gegevensbescherming (avg) en de NIS2-richtlijn. Onvoldoende naleving van deze wetten en richtlijnen (waaronder avg, pci DSS, ISO 27001, NIS2, Schrems II,..) kan leiden tot juridische sancties. Een belangrijk juridisch risico betreft onjuiste Data Processing Agreements (dpa) met dataverwerkers. Verkeerde of ontbrekende overeenkomsten met dataverwerkers kunnen juridische complica-

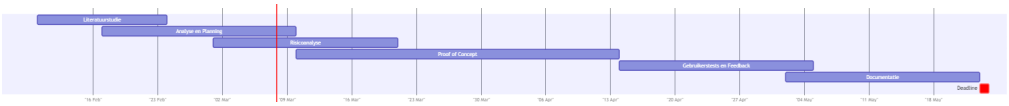
ties veroorzaken. Daarnaast kan het niet correct toepassen van dataminimalisatieprincipes of het verwerken van data voor andere doeleinden dan waarvoor ze zijn verzameld, ook leiden tot juridische gevolgen. Om deze juridische risico's te beperken, stellen betrokken partijen zorgvuldig dpa's op en voeren zij regelmatige herzieningen uit.

3.3.3. Organisatorische risico's

Organisatorische risico's hebben betrekking op de interne processen en procedures van Evolane en de acceptatie van de DLP-oplossing door medewerkers. Weerstand van medewerkers kan een belangrijk organisatorisch risico vormen, aangezien medewerkers mogelijk niet openstaan voor nieuwe beveiligingsmaatregelen. Een gebrek aan training kan bovendien leiden tot misbruik of onjuist gebruik van het DLP-systeem, wat de effectiviteit ervan zal verminderen. Om dan tenslotte deze organisatorische risico's te mitigeren, zullen workshops en informatiesessies worden georganiseerd om medewerkers te betrekken en het belang van de DLP-oplossing te benadrukken. Door medewerkers actief te betrekken en voldoende training te bieden, wordt het gebruik van de DLP-oplossing vergroot en wordt de effectiviteit ervan versterkt.

3.4. Proof of Concept

De PoC wordt opgezet in een interne testomgeving binnen het bedrijf, waarbij een Netskope-licentie wordt gebruikt om de DLP-service in te stellen. Deze omgeving zal verschillende datatypes bevatten (data-in-use, data-in-motion, data-at-rest), waarbij zowel vertrouwelijke als niet-vertrouwelijke bestanden worden gebruikt om te testen of de DLP-service alle vertrouwelijke data effectief kan identificeren en verdere verwerking kan blokkeren. De data bestaat voornamelijk uit persoonlijk identificeerbare informatie (pii) en betalingsgegevens (pci), die volgens de geldende wet- en regelgeving (zoals avg, pci DSS, ISO 27001, NIS2, Schrems II, enz.) beschermd moeten worden. Gebruikers met verschillende rechten zullen data doorsturen en verwerken binnen de testomgeving. De duur van de PoC is afhankelijk van de complexiteit van de testscenario's en de detectie van gevoelige gegevens, maar wordt geschat op 5 tot 6 weken. Na ongeveer 5 weken zou een eerste evaluatie van de effectiviteit van de DLP-oplossing mogelijk moeten zijn, en kan deze aan de eindgebruikers van Evolane worden gepresenteerd. Voor de technische uitvoering is expertise nodig in de configuratie van Netskope (bijvoorbeeld het instellen van detectie- en preventieregels met regex-patronen), evenals basiskennis van de netwerkinfrastructuur van de testomgeving om de dataflows goed na te bootsen.



Figuur 3.1: Gantt-diagram van de onderzoeksplanning van 10 februari 2025 tot 23 mei 2025.

3.5. Gebruikerstests en feedback

Na de initiële implementatie van de PoC worden gebruikers van Evolane betrokken bij het testen van de DLP-oplossing. Dit gebeurt, samen met mijn co-promotor, door middel van workshops en praktische tests waarbij eindgebruikers realistische scenario's simuleren waarin gevoelige data verwerkt en verplaatst wordt. De feedback van deze gebruikers is essentieel om inzicht te krijgen in de gebruiksvriendelijkheid en de invloed van de DLP-regelsets op de dagelijkse taken.

3.6. Evaluatie en meetbare criteria

De effectiviteit van de geïmplementeerde DLP-oplossing wordt geëvalueerd aan de hand van vooraf gedefinieerde Key Performance Indicators (kpi's). Deze kpi's dienen als indicator om te beoordelen in hoeverre de DLP-oplossing voldoet aan de gestelde vereisten en doelstellingen. Detectienauwkeurigheid meet het percentage correct geïdentificeerde confidentiële gegevens binnen de totale dataset, wat aangeeft hoe effectief de DLP-oplossing is in het herkennen van pii en pci. Het aantal false positives geeft aan hoeveel gegevens onterecht zijn geblokkeerd of gemarkeerd, wat inzicht geeft in de nauwkeurigheid van de detectiemethoden en helpt bij het finetunen van de regelsets. Dit zal in een Confusion Matrix worden weergegeven (**Microsoftn.d.**). Systeemimpact zal het effect van de DLP-implementatie op de algehele systeemprestaties beoordelen, zoals CPU- en geheugenverbruik, zodat de oplossing geen significante vertragingen of resource-uitputting zou veroorzaken.

3.7. Documentatie van resultaten

Alle bevindingen en conclusies worden grondig gedocumenteerd. In ongeveer twee weken tijd worden handleidingen, een schriftelijk evaluatierapport en het finale concept-bachelorproef geschreven.

3.8. Planning

De planning van het onderzoek, weergegeven in figuur **??**, is vastgelegd in een Gantt-diagram. De planning is opgesteld van 17 februari 2025 tot 24 mei 2025, met de laatste twee weken specifiek gereserveerd voor documentatie.

4

Conclusie

A

Onderzoeksvoorstel

Het onderwerp van deze bachelorproef is gebaseerd op een onderzoeksvoorstel dat vooraf werd beoordeeld door de promotor. Dat voorstel is opgenomen in deze bijlage.

A.1. Inleiding

In dit onderzoek wordt een klantomgeving voor Evolane ontwikkeld. In deze omgeving worden zowel confidentiële als niet-confidentiële gegevens verwerkt en opgeslagen. Door een Data Leakage Prevention-oplossing te implementeren, worden deze gegevens beveiligd tegen lekken. De DLP-oplossing moet ook voldoen aan de Belgische wetgeving, waaronder de Algemene Verordening Gegevensbescherming (AVG) over persoonsgegevens (PII) en de Payment Card Industry Data Security Standards (PCI DSS) met betrekking tot betalingsgegevens (PCI). De DLP-oplossing moet verder rekening houden met de NIS2-richtlijn en andere cybersecuritykaders, zoals het CCB-kader of ISO 27001. De centrale vraag van dit onderzoek is dus: "Hoe kan een op Netskope gebaseerde DLP-oplossing worden ontworpen en geïmplementeerd om vertrouwelijke gegevens te beschermen en te voldoen aan de Belgische regelgeving?". Vanuit deze hoofdvraag kunnen we een aantal deelvragen afleiden:

- Welke mogelijkheden biedt Netskope's Secure Service Edge (SSE) platform voor Data Leakage Prevention in de context van vertrouwelijke gegevensbescherming?
- Hoe kunnen regelsets en dataclassificatie in Netskope DLP worden afgestemd op de Belgische wetgeving, zoals de AVG en NIS2-richtlijn?
- Welke technieken en methoden kunnen worden toegepast om persoonsgegevens en betalingsgegevens effectief te detecteren en te beschermen bin-

nen het Netskope-platform?

- Hoe kan een Proof of Concept (PoC) voor Netskope DLP worden opgezet in een testomgeving om de effectiviteit van de oplossing te evalueren?
- Welke juridische en technische normen moeten worden meegenomen bij het ontwerpen van een DLP-oplossing voor een Belgische organisatie, en hoe kan Netskope aan deze eisen voldoen?

A.2. Literatuurstudie

A.2.1. Data Leakage Prevention (DLP)

Een DLP-systeem heeft als doel drie soorten gegevens binnen een organisatie te beschermen: data-at-rest, data-in-motion en data-in-use. Data-at-rest verwijst naar statische informatie die is opgeslagen in bedrijfssystemen, zoals documentbeheersystemen, e-mailservers, bestandsservers, netwerkschijven, persoonlijke computers en opslagruimtenetwerken (SANs). Data-in-motion verwijst naar bedrijfsdata dat wordt verwerkt binnen het uitgaande netwerkverkeer, zoals e-mails en online verkeer. Data-in-use bestaat uit informatie die medewerkers gebruiken op eindgebruikersapparaten, zoals een bestand kopiëren naar een USB-schijf. De definitie van vertrouwelijkheid binnen een organisatie vereist een grondigere analyse. Soorten informatie zoals PII, inclusief namen, identiteitskaart- en creditcardgegevens, worden doorgaans in elke organisatie als vertrouwelijk beschouwd. Deze definitie krijgt echter ingewikkeldere aspecten bij bedrijfsgeheimen en interne communicatie, die vaak onregelmatig zijn. Vertrouwelijke informatie verwijst naar gegevens die binnen de organisatie zijn verzameld en niet algemeen toegankelijk zijn. Een DLP-systeem bevat de mogelijkheid om gevoelige gegevens te herkennen in een of meerdere van de genoemde datatypen.

PCI en PII

Persoonlijk identificeerbare informatie (PII), zoals namen, rijksregisternummers, e-mailadressen, telefoonnummers en dergelijke kunnen direct of indirect worden gebruikt voor de identificatie van een persoon. Met het oog op de AVG zijn er strikte regels met betrekking tot toestemming en transparantie bij de verwerking van PII. Payment Card Industry (PCI)-gegevens bevatten alle kaart- en betaalgegevens zoals debit-/creditcardnummers, Primary Account Numbers (PAN) en andere confidentiële authenticatiegegevens zoals CVV. Om te voldoen aan de PCI DSS-norm (Payment Card Industry Data Security Standard), moeten organisaties strenge maatregelen implementeren om deze kaartgegevens te beveiligen. Bedrijven die persoonlijk identificeerbare informatie (PII) en PCI-data verwerken lopen het risico op zware sancties als deze gegevens niet voldoende beschermd worden.

Gegevensverlies detectie methoden

Identificatiemiddelen worden gebruikt om gevoelige informatie, zoals PII en PCI, te detecteren. Dit gebeurt op basis van reguliere expressies (regex). Regex is een krachtig hulpmiddel dat DLP helpt specifieke gegevenstypen te herkennen door middel van uitdrukkingen, termen en patronen, zoals `BE\d{2}\s?\d{4}\s?\d{4}\s?\d{4}` dat kan dienen voor Belgische IBAN-codes. Hoewel dit patroon effectief is voor standaard IBAN-formaten, kan het worden omzeild door een karakter toe te voegen in de invoer, wat de nood benadrukt van extra controles.
De aangemaakte identificatie voor confidentiële gegevens moet voldoen aan de volgende richtlijnen:

- Vooraf gedefinieerde en aanpasbare patronen voor datadetectie: Het is cruciaal om duizenden vooraf ingestelde regels voor het herkennen van gegevens beschikbaar te hebben en deze te kunnen aanpassen aan de behoeften van de organisatie.
- Ondersteuning voor verschillende soorten bestandstypen (Word, Excel, PDF, JPG, PNG, CSV, ZIP en RAR, enz.) en categorieën (afbeeldingen, databases, spreadsheets, enz.).
- Ondersteuning voor landspecifieke identificatienummers (IBAN's, postcodes, adressen, nationale identiteitskaarten, IP-adressen, paspoort- en telefoonnummers).
- Voldoen aan de wet- en regelgeving.

De bescherming van PII en PCI-gegevens vormt een kernaspect van DLP. **Wason2020CASB<empty** legt de nadruk op het belang van de integratie van Cloud Access Security Brokers (CASB) in cloudomgevingen. CASB biedt organisaties de mogelijkheid om een uitgebreide zichtbaarheid te krijgen in het gebruik van cloudtoepassingen, inclusief goedgekeurde en ongeautoriseerde (shadow IT) diensten. Het houdt bij hoe de confidentiële data wordt opgeslagen en verplaatst/verwerkt, wat handig is voor het identificeren van deze data en het voorkomen van datalekken.

False Positives

False positives ontstaan wanneer het DLP-systeem onterecht normale gegevens als confidentieel identificeert. Dit kan leiden tot onnodige waarschuwingen en vertragingen in de bedrijfsprocessen. Om false positives te vermijden, kan in Netskope bij custom identifiers worden aangegeven dat een bepaald keyword in de buurt moet staan, zoals 'RRN' of 'Rijksregisternummer'. Hierdoor ziet Netskope het niet als een match of zal het een lagere vertrouwheidsscore geven.

Detectienauwkeurigheid

Detectienauwkeurigheid houdt in hoe goed het DLP-systeem in staat is om confidentiële gegevens te identificeren. Een hogere detectienauwkeurigheid wordt

bereikt door het gebruik van goed afgestemde regelsets en geavanceerde herkenningsmethoden, zoals reguliere expressies (regex), keywords en contextuele analyse. Netskope maakt gebruik van predefined datasets voor het verbeteren van de detectienauwkeurigheid. Deze datasets bevatten gestructureerde gegevens zoals PII en bieden ondersteuning voor verschillende soorten eisen, waaronder de AVG (**Clementelli2023**). Netskope maakt ook gebruik van een vertrouwheidsscore om de betrouwbaarheid van de gedetecteerde data te bepalen. Deze score helpt bij het evalueren van de waarschijnlijkheid dat bepaalde gegevens confidentieel zijn, wat nodig is voor het verminderen van false positives en false negatives. Om deze nauwkeurigheid te verhogen, kunnen regelsets aangepast worden aan nieuwe typen confidentiële data of veranderende bedrijfsprocessen. In deze proof-of-concept wordt de detectienauwkeurigheid beoordeeld door de verhouding tussen true positives, false positives, false negatives en true negatives, samengevat in een Confusion Matrix (**Microsoftn.d.**).

Systeemimpact

Het meten van de systeemimpact is een belangrijk aspect van DLP-implementaties. Indicatoren hierbij zijn CPU-gebruik, geheugengebruik, netwerklatentie, throughput en systeemstabiliteit. CPU- en geheugengebruik toont aan hoeveel resources het DLP-systeem op de infrastructuur verbruikt. Netwerklatentie en throughput meten de invloed op de netwerkprestaties, terwijl systeemstabiliteit aangeeft of het DLP-systeem consistent functioneert zonder storingen. Voor het verzamelen en analyseren van deze gegevens kunnen tools zoals *Performance Monitor*, *Nagios*, *Zabbix* of de ingebouwde monitoringfunctionaliteiten van Netskope worden ingezet.

A.2.2. Netskope

Netskope heeft zich ontwikkeld tot een vooraanstaande speler in cloudbeveiliging door zijn geavanceerde Secure Service Edge (SSE)-platform. Het levert geïntegreerde CASB- en DLP-mogelijkheden. Volgens **Riley2018<empty citation>** onderscheidt Netskope zich met functies zoals flexibele regelconfiguraties en realtime-detectie van gevoelige data. **VanDerWalt2022<empty citation>** identificeren belangrijke aspecten binnen Secure Access Service Edge (SASE) frameworks die nog onvoldoende onderzoek bevatten. Dit combineert netwerk- en beveiligingsdiensten in een cloudgebaseerde omgeving. Deze aspecten zijn onder andere de integratie van verschillende beveiligingscomponenten zoals Secure Web Gateways (SWG), CASB en Zero Trust Network Access (ZTNA). Deze onderdelen dienen samen te werken om een integrale beveiligingsstrategie te creëren. Bovendien is er een toenemende vraag naar het ontwikkelen van API-integraties voor Security Information and Event Management (SIEM)-systemen, zodat gegevens uit verschillende bronnen effectief kunnen worden verzameld en geanalyseerd.
Bij het evalueren van DLP-oplossingen binnen een SASE-architectuur is Netskope

gekozen vanwege de unieke combinatie van functionaliteiten en prestaties die het biedt, evenals de verhouding ten opzichte van andere oplossingen. Netskope onderscheidt zich als een volledig geïntegreerd platform binnen het SASE-framework, met een Secure Service Edge (SSE)-oplossing die DLP, CASB, SWG en ZTNA naadloos combineert. Deze aanpak is waardevol in gedistribueerde werkomgevingen en bij toenemende cloudadoptie (**brouwer2021cloud**). Netskope biedt meer voordelen dan alternatieven zoals Symantec, Digital Guardian, Forcepoint, Microsoft en McAfee. Symantec en Digital Guardian richten zich bijvoorbeeld sterk op endpointbeveiliging, maar missen de cloudfunctionaliteiten die nodig zijn in moderne hybride werkomgevingen. Forcepoint staat bekend om krachtige gedragsanalyses, maar is minder effectief in het ondersteunen van complexe en dynamische cloudomgevingen. Microsoft biedt uitstekende integratie met Office 365, maar hierdoor mist het ook Netskope's cloud-agnostische aanpak, die een breder scala aan cloudapplicaties ondersteunt (**NetskopeTAP2024**). Tenslotte biedt McAfee een breed scala aan beveiligingsoplossingen, maar voor Evolane is Netskope een gebruiksvriendelijker platform met meer flexibiliteit bij het opstellen en aanpassen van regelsets.

A.2.3. Juridisch kader voor gegevensbescherming in België

De bescherming van persoonlijke en bedrijfsinformatie is een essentieel aspect van de hedendaagse digitale samenleving. Op zowel nationaal als Europees niveau zijn er wettelijke richtlijnen opgesteld om organisaties te ondersteunen bij het garanderen van de vertrouwelijkheid, integriteit en toegankelijkheid van gegevens.

Algemene Verordening Gegevensbescherming (AVG)

Dit onderzoek zal in overeenstemming zijn met de Algemene Verordening Gegevensbescherming (AVG of GDPR) 2016/679 van 27 april 2016 (**eu_avg2016**) en de Belgische wet van 30 juli 2018 (**BelgischeOverheid2018**). Volgens de **eu_avg2016<empty citation>**, overweging (78), moeten passende, technische en organisatorische maatregelen worden genomen om de rechten van natuurlijke personen te beschermen. Deze overweging zorgt ervoor dat persoonsgegevens op een veilige en verantwoorde manier worden verwerkt. Zo'n beveiliging kan gebeuren door middel van standaardinstellingen die erop zijn gericht om risico's in elke fase van de verwerking van gegevens te minimaliseren. Op 25 juli 2024 publiceerde de Europese Unie haar tweede verslag over de toepassing van de AVG (**eu_avg2024**). Dit rapport legt de nadruk op het feit dat de AVG, ondanks verschillende uitdagingen, een goede basis is voor het veilig en transparant behandelen van persoonsgegevens.

Payment Card Industry Data Security Standard (PCI DSS)

De Payment Card Industry Data Security Standard (PCI DSS) bestaat uit een reeks richtlijnen en regels die ontworpen zijn voor organisaties die betalingsinformatie en kaartinformatie verwerken, zoals debit-/ creditcardnummers, Primary Account

Numbers (PAN) en Sensitive Authentication Data (SAD), zoals Card Verification Value (CVV) en magnetische stripgegevens, van alle grote kaartschema's. Deze standaard is ontwikkeld om de veiligheid van kaartinformatie te garanderen en vereist dat organisaties maatregelen nemen om de gegevens van kaarthouders te beschermen (**Elluri2018**). PCI DSS vereist de implementatie van toegangscontroles, zoals DCS-02 (toegangscontrole tot systemen en gegevens), DCS-07 (beheer van gebruikersidentiteiten en -toegang), en DCS-08 (toegangscontrole tot netwerken en systemen), om de veiligheid van kaartinformatie en de bescherming van kaarthoudergegevens te waarborgen (**Elluri2018**).

ISO 27001: Informatiebeveiliging

Bovendien moet de DLP-oplossing rekening houden met de vereisten van ISO 27001, de internationale norm voor het beheer van informatiebeveiliging. In dit verband bespreken **Alsanabani2020<empty citation>** de noodzaak van DLP-oplossingen die zowel detectie- als preventieve methoden samenbrengen. De preventieve aanpak probeert datalekken te vermijden door onder andere het gehele confidentiële bestand te versleutelen, toegangscontrole aan te passen en het labelen van de inhoud.

Nationale en Europese richtlijnen

Buiten de Belgische wetgeving zijn er ook tal van Europese richtlijnen en nationale standaarden die een belangrijke rol hebben in de bescherming van bedrijfsdata. Hierbij kan gedacht worden aan de Algemene Verordening Gegevensbescherming (AVG), de EU Cybersecurity Act en belangrijke Europese richtlijnen, waaronder de NIS2-richtlijn. Deze richtlijnen worden verder uitgebreid met specifieke normen, zoals de PCI DSS voor betalingsgegevens en internationale normen, zoals ISO 27001 voor de beveiliging van informatie. De NIS2-richtlijn (Richtlijn (EU) 2022/2555), die op 16 januari 2023 is aangenomen door de **nis2directive**, heeft als doel de cyberbeveiliging binnen de EU te versterken door een hoog niveau van beveiliging te waarborgen voor netwerken en informatiesystemen. Artikel 21 van de NIS2-richtlijn richt zich op de beveiliging van netwerken en informatiesystemen en legt de verplichting op aan lidstaten om ervoor te zorgen dat aanbieders van essentiële en belangrijke diensten passende technische en organisatorische maatregelen nemen. Maatregelen die over het DLP-systeem kunnen gaan, zijn onder andere:

- Risicoanalyse (lid 2, punten a en e): Organisaties moeten een risicobeheerproces implementeren dat hen in staat stelt om risico's voor de beveiliging van netwerken en informatiesystemen te identificeren, te evalueren en te beheersen.
- Encryptie en toegangscontroles (lid 2, punten h en i): Het gebruik van encryptie, toegangscontroles en regelmatige beveiligingstests en audits.

- Incidentenbehandeling (lid 2, punt b): Organisaties moeten procedures en mechanismen hebben voor het detecteren, melden en reageren op beveiligingsincidenten.
- Bewustwording en training (lid 2, punt g): Opleidingen om medewerkers te informeren over goede cyberhygiëne en risicomanagement. (**nis2directive**) Het DLP-systeem van Netskope staat in voor het trainen van de eindgebruiker, mocht deze iets foutief doen.

De studie van **Nayak2020<empty citation>** geeft een uitgebreid overzicht van systemen voor het detecteren en voorkomen van datalekken, inclusief de indeling van systemen op basis van de status van de gegevens (data-at-rest, data-in-motion, data-in-use) en de detectietechnieken. Dit overzicht zal gebruikt worden voor het ontwikkelen van regex-gebaseerde regels in DLP-oplossingen. De studie legt de nadruk op het feit dat datalekken zowel onvoorzien als opzettelijk kunnen optreden en geeft uitdagingen aan, zoals het identificeren van gevoelige informatie, het balanceren van de detectienauwkeurigheid en de integratie van geavanceerde methodologieën.

Andere relevante wetgeving

De onderstaande tabel **??** bevat de belangrijkste wettelijke richtlijnen en uitspraken die relevant zijn voor het ontwerp en de implementatie van een Data Leakage Prevention-oplossing voor Belgische bedrijven.

Wetgeving	Doel	Relevantie voor DLP
AVG	Bescherming persoonsgegevens	Dataclassificatie en toegangscontrole
PCI DSS	Beveiliging van betalingsgegevens	Encryptie en toegangsbeheer
ISO 27001	Informatiebeveiliging	Risicoanalyse en ISMS-implementatie
CCB-framework	Strategie voor cybersecurity België	Aanbevelingen voor risicobeheer
NIS2	Beveiliging netwerken en diensten	Incidentrapportage en risicoanalyse
EU Cybersecurity Act	Certificering van beveiligingstechnologie	DLP-oplossingen certificeren
Schrems II	Gegevensoverdracht naar niet-EU-landen	Beperking van cloud-gebaseerde opslag

Tabel A.1: Overzicht van wetgeving en relevantie voor DLP (Voorstel)

A.2.4. Ethische overwegingen

Een essentieel aspect van de implementatie van DLP is het vinden van de juiste balans tussen gegevensbeveiliging en gebruikersprivacy. Het gebruik van DLP-systemen kan leiden tot het monitoren van gebruikersgedrag, wat kan worden gezien als een inbreuk op de privacy van medewerkers. Om het vertrouwen bij medewerkers en klanten te behouden, is het belangrijk om transparant te zijn over het gebruik van DLP-systemen en de redenen daarvoor. Hierdoor weet elke gebruiker welke gegevens worden verzameld en hoe deze worden gebruikt (**Zaini2024**). Deze regelsets moeten niet alleen voldoen aan de wettelijke vereisten, maar ook aan de ethische normen en waarden van de organisatie. Om monitoring van data en gebruikersgedrag te minimaliseren, zal de implementatie van de DLP-oplossing specifiek gericht zijn op het beschermen van gevoelige gegevens en het voorkomen van datalekken.

A.3. Methodologie

Het onderzoek naar de ontwikkeling en integratie van een Netskope-gebaseerde Data Leakage Prevention (DLP)-oplossing binnen de bedrijfsomgeving van Evolane. De onderzoeksmethode is een combinatie van een uitgebreide literatuurstudie en een praktische Proof of Concept (PoC).

A.3.1. Literatuurstudie

Het onderzoek begint met een uitgebreide literatuurstudie naar bestaande DLP-oplossingen, Netskope's Secure Service Edge (SSE) platform en de relevante Belgische en Europese wetgeving. Hierbij wordt gebruikgemaakt van academische artikelen, technische documentatie en juridische bronnen om een basis te leggen. Voor de literatuurstudie is ongeveer twee weken voorzien, waarin de focus ligt op het verder verzamelen en verwerken van recente bronnen over DLP-technologie, juridische eisen (AVG, PCI DSS, NIS2) en Netskope's DLP-oplossing.

A.3.2. Analyse en planning

Na de literatuurstudie worden specifieke datasetsspecifieke datasets, zoals persoonlijk identificeerbare informatie (PII) en betalingsgegevens (PCI), geselecteerd voor testen binnen de PoC. bijvoorbeeld de synthetische e-maildatasets van **Whelan2014<empty ci**
Deze datasets bevatten in totaal 4796 e-mails, waarvan 4010 geen PII bevatten en 786 e-mails dit wel hebben, waaronder adressen, creditcardnummers en namen. Ook worden realistische testscenario's opgesteld die aansluiten bij de bedrijfsprocessen van Evolane, zoals e-mailverkeer en bestandsoverdrachten naar cloudservices. Een projectplan zal hier ook uitgewerkt worden, waarin de benodigde middelen, zoals Netskope-licenties en testservers, worden geïdentificeerd. Verder zal hierin ook de tijdsplanning, inclusief de deliverables, worden opgenomen. Deze

fase begint al deels tijdens de literatuurstudie en duurt ongeveer drie weken.

A.3.3. Risicoanalyse

Een belangrijk onderdeel van dit onderzoek is het uitvoeren van een risicoanalyse, waarbij mogelijke technische, juridische en organisatorische risico's worden geïdentificeerd en beoordeeld. Technische risico's kunnen bijvoorbeeld bestaan uit het niet volledig detecteren van gevoelige gegevens of prestatieproblemen van het DLP-systeem. Juridische risico's hebben te maken met het niet naleven van de AVG-vereisten of andere relevante wetgeving. Organisatorische risico's omvatten mogelijke weerstand van medewerkers tegen nieuwe beveiligingsmaatregelen of een gebrek aan training, wat de effectiviteit van de DLP-oplossing kan verminderen. Voor elk vastgesteld risico worden geschikte maatregelen genomen om de gevolgen te beperken. Deze fase duurt ongeveer twee weken, overlappend met Analyse en Planning. Op het vlak van expertise zal hierbij de co-promotor van Evolane betrokken worden.

Technische risico's

Technische risico's zijn gerelateerd aan de operationele elementen van de DLP-oplossing en de technische infrastructuur van Evolane. Een van de belangrijkste technische risico's is de onvolledige detectie van confidentiële gegevens. Het DLP-systeem kan mogelijk niet alle vormen van PII en PCI detecteren, vooral als er nieuwe of onbekende datatypes worden gebruikt. Daarnaast kan de implementatie van Netskope leiden tot prestatieproblemen, zoals vertragingen in netwerkverkeer of een verhoogd gebruik van systeemresources. Integratieproblemen vormen een ander potentieel risico, aangezien het DLP-systeem moet werken met bestaande IT-infrastructuren. Onverwachte compatibiliteitsproblemen kunnen de implementatie vertragen. Vervolgens kunnen verdere beveiligingslekken ontstaan door onvoldoende configuratie of zwakke punten in het DLP-systeem, waardoor confidentiële data alsnog kan worden gelekt. Om deze technische risico's te mitigeren, zullen uitgebreide tests worden uitgevoerd om de detectienauwkeurigheid van het DLP-systeem te waarborgen. Daarnaast zullen systeemprestaties worden gemonitord tijdens de implementatie en indien nodig optimalisaties worden doorgevoerd om prestatieproblemen te minimaliseren. Tenslotte zal een plan worden opgesteld hoe het DLP-systeem veilig geüpdatet kan worden om potentiële kwetsbaarheden te vermijden.

Juridische risico's

Juridische risico's hebben betrekking op de naleving van wet- en regelgeving, zoals de Algemene Verordening Gegevensbescherming (AVG) en de NIS2-richtlijn. Onvoldoende naleving van deze wetten en richtlijnen (waaronder AVG, PCI DSS, ISO 27001, NIS2, Schrems II,..) kan leiden tot juridische sancties. Een belangrijk juridisch risico betreft onjuiste Data Processing Agreements (DPA) met dataverwer-

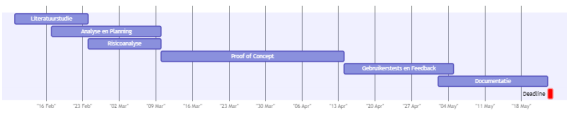
kers. Verkeerde of ontbrekende overeenkomsten met dataverwerkers kunnen juridische complicaties veroorzaken. Daarnaast kan het niet correct toepassen van dataminimalisatieprincipes of het verwerken van data voor andere doeleinden dan waarvoor ze zijn verzameld, ook leiden tot juridische gevolgen. Om deze juridische risico's te mitigeren, zullen DPA's zorgvuldig worden opgesteld en regelmatig worden herzien met alle betrokken derde partijen.

Organisatorische risico's

Organisatorische risico's hebben betrekking op de interne processen en procedures van Evolane en de acceptatie van de DLP-oplossing door medewerkers. Weerstand van medewerkers kan een belangrijk organisatorisch risico vormen, aangezien medewerkers mogelijk niet openstaan voor nieuwe beveiligingsmaatregelen. Een gebrek aan training kan bovendien leiden tot misbruik of onjuist gebruik van het DLP-systeem, wat de effectiviteit ervan zal verminderen. Om dan tenslotte deze organisatorische risico's te mitigeren, zullen workshops en informatiesessies worden georganiseerd om medewerkers te betrekken en het belang van de DLP-oplossing te benadrukken. Door medewerkers actief te betrekken en voldoende training te bieden, wordt het gebruik van de DLP-oplossing vergroot en wordt de effectiviteit ervan versterkt.

A.3.4. Proof of Concept

De PoC wordt opgezet in een interne testomgeving binnen het bedrijf, waarbij een Netskope-licentie wordt gebruikt om de DLP-service in te stellen. Deze omgeving zal verschillende datatypes bevatten (data-in-use, data-in-motion, data-at-rest), waarbij zowel vertrouwelijke als niet-vertrouwelijke bestanden worden gebruikt om te testen of de DLP-service alle vertrouwelijke data effectief kan identificeren en verdere verwerking kan blokkeren. De data bestaat voornamelijk uit persoonlijk identificeerbare informatie (PII) en betalingsgegevens (PCI), die volgens de geldende wet- en regelgeving (zoals AVG, PCI DSS, ISO 27001, NIS2, Schrems II, enz.) beschermd moeten worden. Gebruikers met verschillende rechten zullen data doorsturen en verwerken binnen de testomgeving. De duur van de PoC is afhankelijk van de complexiteit van de testscenario's en de detectie van gevoelige gegevens, maar wordt geschat op 5 tot 6 weken. Na ongeveer 5 weken zou een eerste evaluatie van de effectiviteit van de DLP-oplossing mogelijk moeten zijn, en kan deze aan de eindgebruikers van Evolane worden gepresenteerd. Voor de technische uitvoering is expertise nodig in de configuratie van Netskope (bijvoorbeeld het instellen van detectie- en preventieregels met regex-patronen), evenals basiskennis van de netwerkinfrastructuur van de testomgeving om de dataflows goed na te bootsen.



Figuur A.1: Gantt-diagram van de onderzoeksplanning van 10 februari 2025 tot 23 mei 2025.

A.3.5. Gebruikerstests en feedback

Na de initiële implementatie van de PoC worden gebruikers van Evolane betrokken bij het testen van de DLP-oplossing. Dit gebeurt, samen met mijn co-promotor, door middel van workshops en praktische tests waarbij eindgebruikers realistische scenario's simuleren waarin gevoelige data verwerkt en verplaatst wordt. De feedback van deze gebruikers is essentieel om inzicht te krijgen in de gebruiksvriendelijkheid en de invloed van de DLP-regelsets op de dagelijkse taken.

A.3.6. Evaluatie en meetbare criteria

De effectiviteit van de geïmplementeerde DLP-oplossing wordt geëvalueerd aan de hand van vooraf gedefinieerde Key Performance Indicators (KPI's). Deze KPI's dienen als indicator om te beoordelen in hoeverre de DLP-oplossing voldoet aan de gestelde vereisten en doelstellingen. Detectienauwkeurigheid meet het percentage correct geïdentificeerde confidentiële gegevens binnen de totale dataset, wat aangeeft hoe effectief de DLP-oplossing is in het herkennen van PII en PCI. Het aantal false positives geeft aan hoeveel gegevens onterecht zijn geblokkeerd of gemarkeerd, wat inzicht geeft in de nauwkeurigheid van de detectiemethoden en helpt bij het finetunen van de regelsets. Dit zal in een Confusion Matrix worden weergegeven (**Microsoftn.d.**). Systeemimpact zal het effect van de DLP-implementatie op de algehele systeemprestaties beoordelen, zoals CPU- en geheugenverbruik, zodat de oplossing geen significante vertragingen of resource-uitputting zou veroorzaken.

A.3.7. Documentatie van resultaten

Alle bevindingen en conclusies worden grondig gedocumenteerd. In ongeveer twee weken tijd worden handleidingen, een schriftelijk evaluatierapport en het finale concept-bachelorproef geschreven.

A.3.8. Planning

De planning van het onderzoek, weergegeven in Figuur 2, is vastgelegd in een Gantt-diagram. De planning is opgesteld van 17 februari 2025 tot 24 mei 2025, met de laatste twee weken specifiek gereserveerd voor documentatie.

A.4. Verwacht resultaat, conclusie

Dit onderzoek zal een volledig uitgewerkt Proof of Concept (PoC) opleveren van een Netskope-gebaseerde DLP-oplossing, die is ontworpen om vertrouwelijke gegevens, zoals PII- en PCI-gegevens, te beschermen volgens de Belgische wetgeving. De PoC zal datalekken identificeren en beschermen in een realistische testomgeving die door Evolane mede opgezet zal worden. De vertrouwelijke data zullen in alle mogelijke datatypen voorkomen, zoals data-in-use, data-in-motion en data-at-rest. De oplossing zal gericht zijn op het voorkomen van datalekken die kunnen optreden bij het verwerken en verplaatsen van gevoelige gegevens, zowel binnen als buiten de organisatie. De proof-of-concept zal een geconfigureerd DLP-platform opleveren dat PII- en PCI-gegevens kan identificeren en beschermen volgens de vooraf ingestelde parameters. Deze parameters zullen voldoen aan klantspecifieke dataclassificaties en zullen worden gevalideerd aan de hand van specifieke testscenario's. Het resultaat van deze tests wordt gepresenteerd in een evaluatierapport, dat de effectiviteit van de oplossing evalueert. Daarnaast zal het onderzoek aanbevelingen doen over hoe organisaties de Netskope DLP-oplossing kunnen implementeren om te voldoen aan zowel technische als juridische normen. Tijdens de gebruikers- en feedbacktests zullen medewerkers van Evolane betrokken worden bij het testen van de DLP-oplossing en het geven van feedback over de bruikbaarheid en effectiviteit ervan. Hierbij zullen hoogstwaarschijnlijk nog enkele aanpassingen aan de regelsets gebeuren om de detectienauwkeurigheid te verbeteren en het aantal false positives te verminderen. Het verwacht resultaat omvat een succesvolle implementatie van een DLP-oplossing die effectief de risico's van datalekken vermindert.