Opening Statement

Interviewer:
Goedemorgen. Ten eerste wil ik u bedanken dat u bereid bent deel te nemen aan het interview. Mijn naam is Imane, ik doe momenteel mijn master aan de Universiteit van Amsterdam in de richting Information Studies. Dit interview maakt deel uit van mijn scriptieonderzoek bij Kouters van der Meer. Het onderzoek gaat over hoe kunstmatige intelligentie effectief kan worden geïntegreerd in het cybersecurity-risicomanagement, met name bij financiële instellingen. Het interview duurt ongeveer 60 minuten. Alles wordt anoniem verwerkt en er wordt alleen een transcript gemaakt, dat daarna wordt verwijderd.

Het interview bestaat uit twee delen. Eerst is een korte introductie van ongeveer 5 minuten en daarna ga ik naar de kernvragen.

Respondent:
Ja, klinkt goed

Interviewer:
Ik had gisteren ook een mail gestuurd met het framework, ik weet niet of u die al gezien had?

Respondent:
Ja, ik heb het gezien, maar nog niet volledig doorgenomen.

Interviewer:
Dat geeft niet, we gaan er niet te veel in detail op in. Want de vragen zijn combinaties van verschillende elementen uit tot framework. Dus de vragen die ik hier stel worden uiteindelijk verwerkt in het framework. Zijn er verder nog vragen.

Respondent:
En ja, en Ik was nog wel benieuwd waarom je voor het bedrijf hebt gekozen

Interviewer:
[Naam bedrijf] was onderdeel van de thesis market bij de UvA en ze hadden dus een onderwerp over AI hoe je het best kan gebruiken in risicomanagement. Ze hadden het nog heel breed gelaten, zodat de studenten dan zelf een idee mochten bedenken. Nou, ik had mijn bachelor aan de VU gedaan en mijn bachelor is AI en daarom trok dit onderwerp me wel aan.

Respondent:
En wat voor mensen interview je verder?

Interviewer:
Ik interview mensen uit cybersecurity, risicomanagement, governance en gerelateerde domeinen. Zo krijg ik verschillende perspectieven. Twee van de geïnterviewden zijn intern bij [Naam bedijf], de rest zijn externen.

Respondent:
Oke ja, helder.

Sectie 1: Achtergrond van de geïnterviewde

Interviewer:
Nou dan ga ik de eerste introductie vraag stellen:

Q1.1: Kunt u kort iets over uzelf vertellen en uw rol binnen de organisatie?

Respondent:
Ja nee, zeker met naam is [NAAM] Nou, ik heb dezelfde master gedaan. Ik heb ook de bachelor informatiekunde gedaan, is ook de Universiteit van Amsterdam.
Eerst is mijn werkzame leven gestart in de public policy rondom internet en internet governance en later heb ik mezelf verdiept in AI risicomanagement. En zit ik momenteel in een team bij [NAAM BEDRIJF] waar ik nu 3,5 jaar werkzaam ben.

Interviewer:
Wat is belangrijk aan uw rol voor AI en risicomanagement?

Respondent:
We hebben een divers klantenbestand, van overheden tot bedrijven. We adviseren hen over verantwoord gebruik van AI.

Interviewer:

Q1.3: In hoeverre bent u bekend met LLMs of andere AI-technologieën?

Respondent:
Nou, Ik ben daar zeer bekend mee, want wij adviseren onze klanten over het verantwoord gebruik daarvan. Ja, Ik vind wel dat ik meer dan gemiddeld weet over AI. Maar ik weet niet veel over LLMs specifiek.

Interviewer:

Q1.4: Bent u bekend met regelgeving zoals DORA of de AI Act?

Respondent:
Van DORA heb ik kennisgenomen, maar niet inhoudelijk. De AI Act ken ik goed en gebruiken we ook met de klanten.

Sectie 2: Thematische verdieping

Interviewer:
Q2.1 :Op welke punten in het cybersecurityrisicomanagementproces ziet u volgens u de grootste potentie voor AI, met name grote taalmodellen (LLM's), om toegevoegde waarde te creëren binnen financiële instellingen?

Respondent:

Zo, dat is wel een mond vol haha. Als ik jou vraag ff opsplits dan gaat het over het gebruik van LLM's in het identificeren van risico's bij financiële instellingen.

Imane Akhyar:

Ja dat klopt

Respondent:

Vind ik lastig, ik heb geen idee. Deze vraag kan ik niet beantwoorden op dit moment.

Interviewer:

Geen probleem!

FQ2.1: Zijn er bepaalde uitdagingen of barrières bij het adopteren van AI-oplossingen voor cybersecurity en risicomanagement die u zelf heeft ervaren of bij andere heeft gezien?

Respondent:

Een groot risico is gebrek aan educatie. Veel mensen gebruiken AI zonder de juiste kennis. Ik denk dat het gevaar nu is, dat er niet meer kritisch wordt nagedacht. Daarnaast zijn er problemen zoals bias in trainingsdata en gebrek aan transparantie. Wat we zien is dat de data waarop getraind wordt vaak niet voldoende is om het grootste stuk bias er uit te halen.

Ook synthetische data kan nieuwe vormen van bias introduceren, met name hoe het is gecreëerd. En ik denk dat we die ook nog wel even houden, omdat we steeds meer synthetische data aan het genereren zijn.

Interviewer:

Oke, dus eigenlijk, wat ik hier vanuit haal is dat vooral educatie een belangrijke rol is, maar dat het ook risico is omdat mensen gewoon te weinig kennis hebben daarvan en dan nog bias en transparantie in AI.

Respondent:

Ja dat klopt.

Interviewer:

Q2.2: Hoe wordt in uw organisatie toezicht gehouden op AI-systemen?

Respondent:

Binnen onze organisatie werken we in multidisciplinaire teams, bestaande uit technische experts, juristen en adviseurs. Wij fungeren vaak als verbindende schakel tussen deze disciplines. Vanuit die positie adviseren we klanten over het verantwoord gebruik van AI en geven we aan welke toepassingen wel of niet geschikt zijn binnen hun context. Hoewel er nog geen formeel toezichtsmechanisme is, ontstaat toezicht impliciet via deze samenwerking en afstemming.

Interviewer:

FQ1.2: Ervaart u weerstand bij die samenwerking?

Respondent:

Nee, eerder zien we dat AI te snel wordt toegepast. Wij adviseren juist de klanten terughoudendheid en alternatieve oplossingen waar mogelijk. Vaak wordt er gedacht dat hun werkwijze klopt en dat bespreken we dan samen met het team voordat er een final besluit wordt gemaakt.

Interviewer:

Mijn volgende vraag gaat over de regelgeving:

Q2.3: Hoe beïnvloeden regelgevingen zoals GDPR, DORA, NIS2 of de AI Act de toepassing van LLMs in cybersecurity?

Respondent:

Onze klanten willen uiteraard voldoen aan wet- en regelgeving zoals de AI Act, GDPR en DORA. Deze regelgevingen hebben directe invloed op hoe organisaties omgaan met AI, vooral op het gebied van transparantie, risicoclassificatie en verantwoord datagebruik. Wij ondersteunen klanten hierin op verschillende manieren: door het geven van educatiesessies, het uitvoeren van modelreviews, en het helpen bij het classificeren van AI-systemen op basis van risiconiveaus. Daarnaast adviseren we over welke documentatie, beleid en controles vereist zijn om aantoonbaar compliant te zijn. In die zin zijn we actief betrokken bij het vertalen van abstracte regelgeving naar werkbare richtlijnen en processen die passen bij de organisatiecontext van de klant.

Interviewer:

En dan heb ik nog vragen over de ethische en de privacy zorgen.

Nou u had net al wat verteld over de bias and fairness punten,

Q2.4: zijn er nog andere ethische en privacy zorgen bij AI-gedreven cybersecurity oplossingen en hoe zouden die volgens u aangepakt moeten worden om vertrouwen en transparantie te waarborgen?

Respondent:

Welke precies kan ik nu niet opkomen maar wat je wel vaak ziet is het gebrek aan inzicht in metrieken. Dus dat een partij heel overtuigend is dat de toepassingen die zij gebruiken correct is. Vandaar dat ik dan denk dat het belang van frequente review processen nodig is.

Interviewer:

En wat bedoelt u daar precies mee? De review processen?

Respondent:

Ik zou bij elke stap een review laten plaatsvinden, zodat je zeker weet dat wat je gebruikt ook correct wordt ingezet. Een soort vierogenprincipe dus: AI kan iets aanleveren of analyseren, maar er moet bijna altijd een tweede controle plaatsvinden voordat er iets daadwerkelijk wordt toegepast. Zeker bij gevoelige toepassingen in cybersecurity is dat essentieel om fouten of verkeerde aannames te voorkomen. Het gaat erom dat je AI niet blind volgt, maar er bewust checks op opbouwt.

Interviewer:

Oke ja, top, want dat was ook gelijk mijn volgende vraag:

Q2.4a: Vindt u dat er altijd menselijke controle nodig is, of kunnen bepaalde beslissingen volledig geautomatiseerd worden?

Respondent:

Ik denk dat er een risico-inschatting moet worden gemaakt, welke laat je specifiek wel door AI en welke niet, dat is nog een grijs gebied. AI-besluitvorming moet altijd menselijke controle behouden. Sommige beslissingen zijn zelfs verboden in sommige contexten.

Interviewer:

FQ1.5a: En zijn er ook bepaalde taken die u nooit zou automatiseren?

Respondent:

Bepaalde taken, zoals juridische beslissingen, zouden nooit door AI mogen worden genomen. AI kan hoogstens voorstellen doen met begeleidende waarschijnlijkheden.

*Interviewer***:**

Als laatst had ik nog een vraag over de data-invoer.
Q2.5: Hoe belangrijk vindt u de kwaliteit, herkomst en controle van de data die gebruikt wordt in AI-toepassingen zoals LLMs? En welke aanpak hanteert uw organisatie daarin?
U had eerder al genoemd dat synthetische data nieuwe vormen van bias kan introduceren.

*Respondent***:**

Ja, dat klopt. Datakwaliteit speelt een enorm belangrijke rol, zeker bij AI-toepassingen. Wat we vaak zien is dat organisaties wel met AI willen werken, maar onvoldoende zicht hebben op waar de gebruikte data vandaan komt of hoe die is samengesteld. Dat geldt zowel voor echte datasets als voor synthetisch gegenereerde data. Zeker bij LLMs is dat een risico, omdat je model dan iets leert op basis van potentieel foutieve aannames of gebrekkige representatie. Wij proberen

dat zoveel mogelijk te ondervangen door bij klanten aan te geven dat je eigenlijk nooit zomaar een model moet voeden met ongescreende data. Er moet eerst een stap voorafgaan: wat voor data is dit, hoe is het verzameld, en wat zit er niet in?Idealiter zou je die input data ook classificeren op kwaliteit of betrouwbaarheid. In de praktijk doen we dat nog niet altijd gestructureerd, maar we bespreken het wel bewust in elk project waar AI een rol speelt. Daarnaast merk je ook dat veel bedrijven modellen inzetten die getraind zijn op open datasets of publieke bronnen, en daar zit weinig transparantie in. Dat proberen we ook bespreekbaar te maken – bijvoorbeeld dat synthetische data een oplossing lijkt, maar ook nieuwe vertekeningen kan veroorzaken.

Interviewer:
Dus als ik het goed begrijp, wordt datakwaliteit steeds meer een onderwerp van gesprek, maar is er nog geen vaste aanpak of standaard?

Respondent:
Precies. Het besef is er, en we nemen het mee in de overwegingen, maar ik denk dat het nog verder moet worden ingebed in processen en beleid. Zeker als AI breder ingezet gaat worden, moet dat deel structureel worden geregeld.

Interviewer:

Dat waren de kernvragen van dit interview. Nu wil ik u graag nog enkele vragen stellen over het voorlopige framework dat ik heb meegestuurd.
Q2.7: Wat zou u nodig hebben om vertrouwen te hebben in een AI-ondersteund framework voor cybersecurity-risicomanagement? En hoe zou zo'n framework idealiter getoetst of verbeterd moeten worden in de praktijk?

Respondent:
Binnen onze organisatie hebben we zelf een framework ontwikkeld dat we gebruiken in onze AI- en risicoadviestrajecten. Dat kan ik eventueel met je delen. Wat mij opvalt is dat er een aantal elementen overeenkomen met jouw voorstel, wat positief is. Tegelijkertijd zie ik ook een aantal onderdelen die ik mis. Zo vind ik dat het aspect explainability explicieter opgenomen moet worden. Daarnaast mist er nog aandacht voor sustainability, bijvoorbeeld in de zin van langetermijneffecten van AI-systemen of het energieverbruik van bepaalde modellen. Dat zijn wat mij betreft belangrijke toevoegingen om het framework sterker te maken en toekomstbestendiger.

Interviewer:
Ooh top dank u wel! En dan had ik nog een vraag over mijn voorlopige framework.
Q2.8: Als u kijkt naar het framework in zijn geheel, welke onderdelen vindt u het meest relevant in uw praktijk?

Respondent:
Het meest relevant vond ik de focus op risicoclassificatie en governance, dat zijn onderwerpen die in onze dagelijkse praktijk voortdurend terugkomen. Die componenten sluiten goed aan bij hoe wij momenteel AI en risicobeheersing benaderen binnen organisaties. Ze vormen wat mij betreft de kern van een werkbaar framework.

Afsluiting

Interviewer:

Dit brengt ons ook gelijk aan het eind van het interview en nogmaals, bedankt voor die tijd en uw antwoorden. En zoals eerder al vermeld, alles wordt geanonimiseerd en vertrouwelijk behandeld. Ik zal het alleen in het transcript gebruiken voor de zinnen en het verwerken in de scriptie. En na de scriptie wordt alles verwijderd.

Zijn er nog andere vragen of opmerkingen?

Respondent:

Nee verder geen vragen meer

Imane Akhyar:

En na het verwerken van de resultaten van de interviews stuur ik nog een Google Survey op naar alle kandidaten van het interview. Dit bevat ook meteen het final framework en vragen over of het klopt met wat er vandaag is besproken. Zo kan ik gelijk met iedereen valideren. Die kunt u dan de tweede week van juni ongeveer verwachten.

Respondent:

Top! Veel succes nog met de interviews en het schrijven van je scirptie!