Informatiebeveiligingsspecialist - Informatievoorziening

Functieomschrijving

Zorg jij er als Informatiebeveiligingsspecialist voor dat de tooling waarmee Logius werkt net zo veilig is als de diensten die we leveren?

Miljoenen Nederlanders vertrouwen dagelijks op DigiD, MijnOverheid en de andere voorzieningen van Logius. Om die diensten te bouwen, te beheren en te verbeteren, werken onze collega's zelf ook met tooling: van Jira en Confluence tot allerlei andere (SaaS)-toepassingen. Daar gaan bedrijfsgevoelige informatie en persoonsgegevens doorheen. Hoe zorg je ervoor dat die interne informatievoorziening veilig, betrouwbaar en compliant blijft, zonder dat security het werk afremt? Dat is waar jouw rol als Informatiebeveiligingsspecialist binnen team Informatievoorziening om de hoek komt kijken.

De afdeling Informatievoorziening (IV) levert de tooling waarmee Logius haar primaire en ondersteunende processen uitvoert. Zelforganiserende serviceteams leveren die tooling en ontwikkelen haar door. Dat doen ze volgens SAFe en in nauwe samenwerking met interne afdelingen en externe leveranciers. Nieuwe technologie biedt daarbij kansen, maar brengt ook nieuwe risico's mee. IV stelt voor de hele organisatie de kaders voor de ondersteunende informatievoorziening, en adviseert, toetst en ondersteunt daarbij. Als specialist informatiebeveiliging geef jij die rol invulling op het gebied van security en privacy.

Wil een team een nieuwe SaaS-toepassing in gebruik nemen of een bestaande tool flink aanpassen? Dan voer jij de risicoanalyse en waar nodig de DPIA uit, of je ondersteunt daarbij. Je zet standaard security-vragenlijsten uit bij leveranciers, beoordeelt hun TPM's en ISO-verklaringen en adviseert of zij aan de rijksbrede eisen voldoen. Bij audits en pentesten verzamel je de bewijsstukken. De bevindingen zet je als actiepunten in Jira, en je zorgt dat ze ook echt worden opgevolgd. Welke persoonsgegevens verwerkt deze tool, en waar staan ze? Voldoet de leverancier aan de BIO? Zijn de bevindingen uit de laatste pentest opgelost? Met dat soort vragen ben je dagelijks bezig.

Minstens zo belangrijk: je vertaalt het informatiebeveiligingsbeleid van Logius en wet- en regelgeving zoals de BIO, de AVG en NIS2 naar procedures en handleidingen. Daar moeten de serviceteams van IV in de praktijk echt iets mee kunnen. Je helpt IT-processen te verbeteren en houdt de risicoregisters en de backlog actueel. Ook organiseer je bewustwordingssessies, zodat informatiebeveiliging op de agenda blijft.

De uitdaging zit in de balans. Zelforganiserende teams zitten niet te wachten op een controleur met een checklist. Jij zoekt de vorm waarin kaders en praktijk samenkomen: je legt risico's helder uit, denkt mee over haalbare maatregelen en signaleert problemen voordat ze in een audit opduiken. Zo zorg je ervoor dat Logius van binnenuit veilig is, en daarmee ook de digitale overheid waarop burgers en bedrijven vertrouwen.

Je houdt je onder andere bezig met:

- **Risicoanalyses en DPIA's:** je voert ze uit of ondersteunt erbij voor tooling en applicaties binnen IV;
- **Leveranciers- en SaaS-toetsing:** je zet security-vragenlijsten uit en adviseert of leveranciers aan de rijksbrede eisen voldoen;
- **Audits en pentesten:** je levert bewijsstukken aan en bewaakt de opvolging van bevindingen in Jira;
- **Beleid naar praktijk:** je vertaalt kaders en wetgeving naar werkbare procedures en handleidingen;

•**Procesverbetering:** je helpt IT-processen te verbeteren volgens best practices;
•**Awareness:** je organiseert bewustwordingssessies over informatiebeveiliging en privacy;
•**Registratie en planning:** je houdt de backlog, risicoregisters en planningen in Jira en Confluence actueel.

Functie-eisen

Je bent een informatiebeveiligingsspecialist die de regels en kaders kent, maar vooral weet hoe je ze werkbaar maakt. Je legt risico's helder uit aan collega's in de teams en aan management en directie. Je weet mensen te overtuigen zonder met het vingertje te wijzen. Daarnaast beschik je over:
•Hbo-werk- en denkniveau, bij voorkeur aangetoond middels een relevant diploma;
•Minimaal één jaar ervaring in informatiebeveiliging, privacy of IT-compliance;
•Kennis van en ervaring met de BIO, ISO 27001 en de AVG;
•Een CISSP-certificering, of de bereidheid deze via Logius te behalen;
•Goede communicatieve vaardigheden in het Nederlands, mondeling en schriftelijk.
De Rijksoverheid streeft ernaar een werkgever te zijn waar iedere medewerker, ongeacht leeftijd, sekse, geaardheid, etnische afkomst en arbeidsbeperking voor wil werken. Werken aan maatschappelijke vraagstukken in divers samengestelde teams maakt ons effectiever en innovatiever. Bij Logius is daarom iedereen welkom!

Bijzonderheden

•Inschaling vindt plaats op basis van je opleiding, kennis en werkervaring;
•Een positief VOG is een vereiste voor deze vacature;
•Referenties kunnen worden opgevraagd als onderdeel van het sollicitatieproces, maar dit doen we altijd in overleg met jou;
•Logius is continu in ontwikkeling, ook nu. We verbeteren onze manier van samenwerken en richten onze organisatie toekomstbestendiger in. Voor de meeste functies heeft dit geen impact op het werk zelf, al kan de plek van teams in de organisatie veranderen. We vinden het belangrijk om hier eerlijk over te zijn. Je solliciteert bij een organisatie die continu professionaliseert én waar jouw expertise hard nodig blijft. Heb je vragen over de organisatieontwikkelingen binnen Logius? Wij beantwoorden deze graag tijdens het sollicitatiegesprek.

Meer over jouw toekomstige afdeling

De afdeling Informatievoorzieningen (IV) levert tooling ter ondersteuning van de primaire en secundaire processen van Logius. Met de tooling kunnen wij met elkaar en met onze externe omgeving op een excellente wijze de activiteiten binnen onze organisatie (bij)sturen, inrichten en verrichten en daarmee bijdragen aan de creatie van waarde voor burgers en bedrijven.
Dit doen wij door de tooling betrouwbaar, in samenhang en in eenvoud met vakkundige en zelforganiserende serviceteams te leveren en (door) te ontwikkelen. De (door)ontwikkeling van onze tooling doen wij samen met de organisatie en onze omgeving, zodat tegemoetgekomen kan worden aan de continu veranderende IV-behoeften en wij inspelen op de kansen en bedreigingen naar aanleiding van nieuwe technologische ontwikkelingen.
Wij bereiken dit door een excellente en efficiënte levering en (door)ontwikkeling van onze diensten middels de SAFe Agile werkwijze in nauwe samenwerking met interne afdelingen en externe partijen. IV is daarbij kaderstellend, adviserend, toetsend en ondersteunend naar de organisatie in relatie tot de ondersteunende informatievoorzieningen.

Dit bieden we nog meer

Naast het salaris ontvang je een Individueel Keuzebudget (IKB). Het IKB bestaat uit geld

(16,50% van je bruto jaarsalaris) en tijd. Met het IKB maak jij de keuzes die bij jou passen en kun je een deel van je arbeidsvoorwaarden zelf samenstellen. Je kunt er bijvoorbeeld voor kiezen om een deel van je maandinkomen te laten uitbetalen wanneer jij dat wenst. Ook kun je dit budget omzetten in verlof en andersom of besteden aan fiscaal vriendelijke doelen. De Rijksoverheid hecht sterk aan persoonlijke groei en loopbaanontwikkeling en biedt daarvoor tal van mogelijkheden. Tot de secundaire arbeidsvoorwaarden behoren onder meer verschillende studiefaciliteiten, bedrijfsfitness, volledige vergoeding van je OV-reiskosten woon-werkverkeer en gedeeltelijk betaald ouderschapsverlof.