DevSecOps Engineer Vlam

Functieomschrijving

Wil jij bouwen aan de toekomst van veilige, soevereine AI voor de Rijksoverheid? Bij SSC-ICT werk je aan *vlam*: een schaalbaar, veilig AI-platform dat volledig on-premise draait. Als DevSecOps-engineer ben jij verantwoordelijk voor de ontwikkeling, beveiliging én compliance van dit AI-platform. Met jouw technische expertise en scherpe blik op security en compliance zorg je dat *vlam* voldoet aan de geldende overheidsnormen.
In deze rol vorm je de brug tussen enerzijds ontwikkeling en anderzijds security en compliance. Ongeveer 70% van je tijd besteed je aan technische ontwikkeling – zoals GitOps, Argo CD en automatisering – en 30% aan het opzetten, onderhouden en automatiseren van compliance-documentatie en -processen.
Dankzij jouw werk voldoen zowel het platform als alle applicaties aan de gestelde eisen, zonder dat papierwerk het tempo vertraagt. Je weet precies welke informatie vastgelegd moet worden en hoe je die zo efficiënt en geautomatiseerd mogelijk genereert en up-to-date houdt.

Belangrijke focusgebieden

- GitOps & geautomatiseerde deployments: Je speelt een sleutelrol in de transitie naar GitOps en richt Argo CD zo in dat AI-applicaties en -infrastructuur continu, veilig en betrouwbaar worden uitgerold.
- Automatische compliance-documentatie: Je ontwikkelt oplossingen waarmee beveiligingsplannen, risicoanalyses en auditrapportages automatisch – met behulp van AI – worden gegenereerd op basis van de actuele staat van het platform.
- Security by Design: Je borgt security en compliance in elke fase, van code tot productie, conform BIO2, ISO 27001 en de eisen die horen bij het niveau departementaal vertrouwelijk.

Jouw werkzaamheden

- Ontwikkelen en beheren van Infrastructure as Code met tools zoals Terraform, met nadruk op security en compliance.
- Inrichten en beheren van GitOps-pijplijnen met Argo CD, inclusief veilige workflows voor automatische deployments en rollbacks.
- Automatiseren van compliance-checks en -documentatie, onder andere via Open Policy Agent (OPA) of vergelijkbare tools in de deployment-pijplijn en AI-gedreven rapportages.
- Meedenken over én implementeren van Kubernetes security controls (zoals Pod/Network Policies en RBAC) en monitoren van de veiligheidspostuur.
- Samen met het team security- en compliance-eisen vertalen naar concrete technische oplossingen en deze verankeren in architectuur en processen.
- Ondersteunen bij audits en het opstellen van beveiligingsdocumentatie, zoals threat models, risicoanalyses en compliance-matrices.
- Doorontwikkelen van de CI/CD-pijplijn voor snelle, veilige releases binnen de kaders van de overheidsnormen.

Jouw werkzaamheden sluiten aan op het KWIV-profiel 5.3.1 INFORMATIEMANAGEMENT.
Meer informatie over KWIV-profielen vind je op: Kwaliteitsraamwerk Informatievoorziening (KWIV)

Functie-eisen

- Hbo- of wo-werk- en -denkniveau.

•Ervaring als DevOps/SecDevOps-engineer in een complexe omgeving met verhoogde beveiligingseisen.
•Ervaring met automatisering en je hebt sterke scriptvaardigheden.
•Diepgaande kennis van Kubernetes (inclusief security-hardening, multi-node clusters, on-premise deployments) en Helm, aangevuld met ervaring met GitOps-tools zoals Argo CD of Flux.
•Kennis van Infrastructure as Code (Terraform, Ansible) en versiebeheer (Git).
•Ervaring met security-tools zoals OPA, Trivy, Falco, of vergelijkbare oplossingen voor container- en Kubernetes-security.
•Begrip van compliance-kaders zoals BIO2 en ISO 27001 en de vertaling hiervan naar technische maatregelen.
•Kennis van AI/ML-infrastructuur (bijv. LLM-deployments, GPU-clusters) is een pre, maar niet vereist.

Competenties

•Je hebt een proactieve en verantwoordelijke houding en neemt initiatief om security en compliance te borgen in alle ontwikkelprocessen.
•Je denkt analytisch en oplossingsgericht, met een sterke focus op risicominimalisatie en het voorkomen van security-incidenten.
•Je bent pragmatisch en hands-on, met een passie voor automatisering en het elimineren van handmatige processen.
•Je communiceert helder en effectief met technische teams, compliance-officers en stakeholders, en je kunt complexe security- en compliance-vraagstukken begrijpelijk uitleggen.
•Je hebt oog voor duurzaamheid en schaalbaarheid en zorgt ervoor dat oplossingen toekomstbestendig zijn.
•Je bent nieuwsgierig en blijft op de hoogte van de laatste ontwikkelingen in DevOps, Security en AI.

Bijzonderheden

Een AIVD B-veiligheidsonderzoek is onderdeel van de procedure.
De vermelde einddatum van de vacature is een richtlijn. Regelmatig wordt de einddatum van een vacature verlengd, maar dit heeft geen invloed op de beoordeling van kandidaten die al vóór die datum hebben gereageerd. In sommige gevallen kan de vacature juist eerder worden gesloten. Wacht dus niet te lang en reageer snel!
Je wordt ingeschaald op basis van ervaring. Voldoe je nog niet volledig aan het profiel, dan begin je eerst in een aanloopschaal en krijg je de kans door te groeien naar het schaalniveau van deze functie.
De wederzijdse kennismaking en selectieprocedure bestaat uit twee gesprekken en mogelijk een assessment. Bij een positief verloop volgt een afrondend arbeidsvoorwaardengesprek.
Een Verklaring Omtrent het Gedrag (VOG) is nodig om te kunnen starten als medewerker bij SSC-ICT.

Meer over jouw toekomstige afdeling

Je komt te werken bij het AI Competence Center (AICC), een hecht en ambitieus team binnen de Chief Technology Office (CTO). Het AICC is volop in ontwikkeling en biedt jou de kans om vanaf de basis mee te bouwen aan de toekomst van AI binnen SSC-ICT. Je werkt samen met 9 collega’s: een diverse groep professionals die intensief samenwerkt met andere afdelingen.
Het AICC heeft drie kerndoelen: AI integreren in bestaande diensten, AI inzetten in interne processen en tools, en nieuwe AI-specifieke diensten ontwikkelen die SSC-ICT toekomstbestendig maken. Daarbij staan veilig, verantwoord en waardegedreven gebruik

van AI altijd centraal. Het team combineert een sterke compliance-kant (wet- en regelgeving, ethiek, risicobeheersing) met een technische kant (innovatie, implementatie, schaalbaarheid). Door deze twee werelden te verbinden, realiseren we AI-oplossingen die zowel juridisch zorgvuldig als technisch robuust zijn.
De sfeer in het team is energiek en collegiaal: samenwerken, leren en innoveren staan voorop. Er wordt hard gewerkt, maar er is ook ruimte voor creativiteit, experimenteren en het vieren van successen. Of het nu gaat om een complex vraagstuk oplossen, een nieuwe toepassing lanceren of kennis delen met collega's: je merkt de drive om samen impact te maken. Je komt in een omgeving terecht waar groei wordt gestimuleerd, waar jouw ideeën welkom zijn en waar je bijdraagt aan betere overheidsdienstverlening met behulp van AI.
Let op: Het AICC is een tijdelijk team voor maximaal twee jaar. Daarna worden de taken geïntegreerd in de lijnorganisatie, waardoor je de mogelijkheid hebt om je werk binnen SSC-ICT voort te zetten. Dit betekent dat je werkt met een duidelijke deadline én de kans krijgt om blijvende impact te maken op hoe AI binnen SSC-ICT wordt vormgegeven.

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.