Security Engineer

Functieomschrijving

De cyberweerbaarheid van de Rijksoverheid vergroten, dát is de missie van het Security Operations Center (SOC) van SSC-ICT. Als Security Engineer speel jij hierin een belangrijke rol. Je zorgt ervoor dat onze securitytechnologie, detectievoorzieningen en technische beveiligingsmaatregelen betrouwbaar functioneren en continu verbeteren. Met jouw technische kennis draag je bij aan de cyberveiligheid van 7 ministeries.
Je werkt binnen het SOC, onderdeel van het Chief Technology Office (CTO). Als Security Engineer ben je verantwoordelijk voor het technisch inrichten, beheren en verbeteren van onze securityplatformen en detectievoorzieningen. Je werkt met moderne securitytools, ontwikkelt en beheert detecties en automatiseert waar mogelijk terugkerende werkzaamheden. Zo bouw je mee aan een steeds slimmer, schaalbaarder en weerbaarder SOC.
Je vertaalt dreigingen en operationele behoeften naar technische oplossingen, zorgt voor betrouwbare koppelingen met databronnen en ondersteunt bij complexe security-incidenten. Hierbij werk je nauw samen met securityanalisten, beheerteams, architecten en leveranciers.
Een greep uit je werkzaamheden:

- Inrichten, beheren en optimaliseren van securityplatformen zoals SIEM-, EDR-, NDR- en SOAR-oplossingen.
- Ontwikkelen, testen en verbeteren van detectieregels, use-cases, dashboards en geautomatiseerde responsacties.
- Aansluiten en beheren van logbronnen en datakoppelingen.
- Bewaken van de kwaliteit, volledigheid en beschikbaarheid van securitydata.
- Technisch ondersteunen bij de analyse en afhandeling van security-incidenten, waaronder het uitvoeren van verdiepend onderzoek en het verzamelen van technische informatie.
- Automatiseren van terugkerende securitywerkzaamheden met scripts, API-koppelingen en playbooks.
- Signaleren en oplossen van technische knelpunten.
- Bijdragen aan de doorontwikkeling, documentatie en technische roadmap van het SOC.

Je werkt samen met securityanalisten, engineers en andere specialisten binnen een team met korte lijnen en veel kennisdeling. Jij zorgt voor een stevige technische basis, zodat analisten dreigingen sneller kunnen detecteren en incidenten effectief kunnen onderzoeken. Daarbij krijg je de ruimte om je verder te ontwikkelen op het gebied van detection engineering, security automation en incidentrespons.

Jouw werkzaamheden sluiten aan op het KWIV-profiel 4.1.3 CYBERSECURITY MANAGEMENT.
Meer informatie over KWIV-profielen vind je op: Kwaliteitsraamwerk Informatievoorziening (KWIV)

Functie-eisen

- Minimaal hbo-werk- en -denkniveau, bij voorkeur ondersteund met een opleiding in de richting van ICT, cybersecurity, informatica of informatiebeveiliging.
- Ervaring met het technisch beheren, implementeren en/of doorontwikkelen van securityoplossingen binnen een complexe IT-omgeving.
- Goede kennis van computernetwerken, Windows- en Linux-omgevingen en relevante

securityprincipes.
•Ervaring met securitytooling zoals SIEM-, EDR-, NDR- of SOAR-oplossingen, bijvoorbeeld Splunk, Microsoft Sentinel, Microsoft Defender of vergelijkbaar.
•Ervaring met scripting of automatisering, bijvoorbeeld met Python, PowerShell, Bash, API-koppelingen of vergelijkbare technieken.
•Goede beheersing van de Nederlandse en Engelse taal, zowel mondeling als schriftelijk.
Niet vereist, wel mooi meegenomen
•Certificeringen zoals Security+, SC-200, AZ-500, GSEC, CySA+ of vergelijkbaar.
•Ervaring met detection engineering, cloudsecurity, infrastructuurbeheer of DevSecOps.
•Kennis van querytalen en detectiestandaarden, zoals KQL, SPL, Sigma, YARA of vergelijkbaar.
Competenties
•Je bent technisch en analytisch sterk en weet complexe securityvraagstukken terug te brengen tot werkbare en betrouwbare oplossingen.
•Je werkt nauwkeurig en gestructureerd waardoor configuraties, scripts, wijzigingen en technische documentatie van hoge kwaliteit zijn.
•Je neemt initiatief en toont eigenaarschap bij het oplossen van technische knelpunten en het verbeteren van securityvoorzieningen.
•Je communiceert helder en weet technische keuzes begrijpelijk toe te lichten aan collega's en stakeholders.
•Je bent leergierig en blijft jezelf ontwikkelen op het gebied van securitytechnologie, automatisering en nieuwe vormen van dreigingen.
•Je stemt goed af met analisten, beheerders, architecten en leveranciers. Je zoekt hierbij actief de samenwerking op om tot duurzame oplossingen te komen.

Bijzonderheden

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 AIVD B-veiligheidsonderzoek is onderdeel van de procedure.

Meer over jouw toekomstige afdeling

Je gaat aan de slag bij het Security Operations Center (SOC), onderdeel van de Chief Technology Office (CTO). Met zo'n 16 collega's vormen we een divers team qua leeftijd en culturele achtergrond. Er heerst een informele werksfeer waarin mensen elkaar vertrouwen en op elkaar kunnen bouwen. In ons team streven we ernaar om elkaar te versterken en uit te dagen, zodat we continu groeien en scherp blijven. We hechten veel waarde aan een goede balans tussen werk en privé, waarbij we respect hebben voor ieders persoonlijke situatie. We hebben een hechte band en sluiten de week het liefst gezamenlijk af met een drankje.

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.