Security Analist

Functieomschrijving

De cyberweerbaarheid van de Rijksoverheid vergroten, dát is de missie van het Security Operations Center (SOC) van SSC-ICT. Als Security Analist speel jij hierin een belangrijke rol. Met jouw analytische blik en communicatieve vaardigheden draag je bij aan de cyberveiligheid van 7 ministeries. Je werkt met moderne securitytools en houd je dagelijks bezig met het signaleren, analyseren en opvolgen van cyberdreigingen. Tegelijkertijd krijg je volop ruimte om je verder te ontwikkelen binnen het dynamische vakgebied van cybersecurity. Zo bouw je mee aan een steeds slimmer en weerbaarder SOC.

Je werkt binnen het SOC, onderdeel van het Chief Technology Office (CTO). Als Security Analist ben je verantwoordelijk voor het monitoren van cyberdreigingen, het analyseren van securitymeldingen en het ondersteunen bij de afhandeling van incidenten. Je onderzoekt verdachte activiteiten, brengt risico's in kaart en draagt bij aan het verbeteren van onze detectie- en responsprocessen.

Een greep uit je werkzaamheden:

- Monitoren en analyseren van securitymeldingen, afkomstig uit verschillende bronnen en securityplatformen.
- Onderzoeken van dreigingen, kwetsbaarheden en verdachte activiteiten binnen de ICT-omgeving van de Rijksoverheid.
- Uitvoeren van analyses op basis van logbestanden, security-events en andere beschikbare informatie.
- Ondersteunen bij de afhandeling van security-incidenten en het bepalen van de bijbehorende impact.
- Vastleggen en documenteren van bevindingen in rapportages en kennisbanken.
- Bijdragen aan de verbetering van detectieregels, werkprocessen en de verdere ontwikkeling van het SOC.

Je werkt samen met ervaren securityanalisten en specialisten binnen een team met korte lijnen en veel kennisdeling. Daarbij krijg je de mogelijkheid om je verder te ontwikkelen richting complexere analyses, incidentrespons en specialistische securitydomeinen.

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 of informatiebeveiliging.
- Ervaring met cybersecurity, security monitoring of incidentafhandeling binnen een IT-omgeving.
- Kennis van computernetwerken, Windows- en Linux-omgevingen.
- Ervaring met security tooling, zoals SIEM-oplossingen (bijvoorbeeld Splunk, Microsoft Sentinel of vergelijkbaar), is een pre.
- Affiniteit met thema’s als cyberdreigingen en incidentonderzoek.
- Bereidheid om 3 tot 4 keer per jaar piketdienst te draaien.
- Goede beheersing van de Nederlandse en Engelse taal, zowel mondeling als schriftelijk.

Niet vereist, wel mooi meegenomen

- Certificeringen zoals Security+, SC-200, GSEC, CySA+ of vergelijkbaar.

•Ervaring met EDR-, NDR- of SOAR-oplossingen.
•Kennis van relevante wet- en regelgeving op het gebied van informatiebeveiliging.
Competenties
•Je bent analytisch sterk en weet securitymeldingen en incidenten snel te doorgronden, zodat je risico's en impact goed kunt inschatten.
•Je werkt nauwkeurig en gestructureerd, waardoor jouw analyses, bevindingen en documentatie van hoge kwaliteit zijn.
•Je neemt initiatief en toont eigenaarschap bij het onderzoeken en opvolgen van securityvraagstukken.
•Je communiceert helder en weet technische informatie begrijpelijk over te brengen aan collega's en stakeholders.
•Je bent leergierig en blijft jezelf ontwikkelen op het gebied van cybersecurity, dreigingen en nieuwe technologieën.
•Je stemt goed af en zoekt actief de samenwerking op met collega's om kennis te delen en gezamenlijk resultaten te behalen.

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.