Security Analist SOC

Functieomschrijving

De cyberweerbaarheid van de Rijksoverheid vergroten, dát is de missie van het Security Operations Center (SOC) van SSC-ICT in Den Haag. Als security analist draag jij hier dagelijks aan bij. Met jouw analytische en communicatieve vaardigheden werk je aan de cyberveiligheid van 7 ministeries. Daarbij maak je gebruik van geavanceerde securitytools. Je krijgt volop ruimte om je vakinhoudelijk en persoonlijk verder te ontwikkelen. Zo word jij steeds beter in je vak, en wordt onze organisatie steeds slimmer en sneller in het detecteren en bestrijden van cyberdreigingen.

Je werkt binnen het SOC, onderdeel van het Chief Technology Office (CTO). Als security analist heb je een breed takenpakket met veel verschillende verantwoordelijkheden. Je monitort cyberdreigingen, analyseert securitymeldingen en bepaalt op basis van triage welke opvolging nodig is. Ook tijdens de verdere afhandeling van incidenten blijf je als inhoudelijk expert betrokken.

Je houdt je onder andere bezig met het:

- Identificeren van dreigingen zoals kwetsbaarheden en malware. Dit doe je op basis van rapportages van externe partijen, beheerteams en securitymanagement;
- Analyseren en opvolgen van securitymeldingen en incidenten aan de hand van onder andere logbestanden en veiliggesteld materiaal;
- Onderzoeken van de oorzaak en impact van securityincidenten;
- Vastleggen en documenteren van bevindingen in een knowledgebase;
- Verbeteren van detectieregels en bijdragen aan de verdere ontwikkeling van het SOC;
- Ondersteunen en begeleiden van collega’s bij complexere incidenten;
- Delen van kennis en het vertalen van technische bevindingen naar duidelijke adviezen voor verschillende stakeholders.

In deze functie werk je zelfstandig aan complexe securitymeldingen en incidenten. Je ondersteunt minder ervaren collega’s, neemt waar nodig complexere dossiers over en levert een actieve bijdrage aan de verdere professionalisering van het SOC. Ook kun je een coördinerende rol vervullen tijdens incidenten en weet je jouw kennis helder over te brengen. Je werkt in een deskundig team met korte lijnen, waarin iedere collega een eigen expertise meebrengt. Samen zorgen jullie ervoor dat dreigingen tijdig worden herkend, incidenten zorgvuldig worden afgehandeld. Zo versterken jullie de digitale weerbaarheid van 7 ministeries.

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 wo-werk- en -denkniveau en bij voorkeur een wo-diploma in de richting van ICT of security.
- Minimaal 3 jaar werkervaring in een vergelijkbare functie of in verschillende operationele functies binnen het domein van ICT-beveiliging.
- Ervaring met identificeren van dreigingen en risico’s met betrekking tot computernetwerken.
- Ervaring met Security Monitoring, SIEM-Tooling (zoals Splunk) en Linux- en Windowssystemen.
- Kennis van wet- en regelgeving die je kunt toepassen op de techniek.

•Ervaring met het herkennen van aanvalstechnieken (technisch en in de vorm van social engineering) en het overbrengen van deze informatie aan collega's.
•Bij voorkeur 1 of meerdere securitycertificeringen, zoals GIAC GSEC, GCIH, GMON, GCIA.
•Bereidheid om 3 tot 4 keer per jaar piketdienst te draaien.
•Goede beheersing van het Nederlands en Engels, zowel mondeling als schriftelijk.

Bijzonderheden

•De einddatum van de vacature is niet leidend. De selectie start wanneer geschikte kandidaten solliciteren. De vacature kan dus vóór de vermelde einddatum sluiten. Wees er daarom op tijd bij en reageer snel!
•De kennismaking en selectieprocedure bestaat uit 2 gesprekken en een assessment.
•Bij een positief verloop volgt een afrondend arbeidsvoorwaardengesprek.
•Een AIVD B-veiligheidsonderzoek is onderdeel van de procedure.
•Werk je, op afgesproken momenten, buiten de operatie aan de doorontwikkeling van het SOC? Dan is hybride werken wel bespreekbaar.
•Goed om te weten: in alle lagen van ons SOC hebben we een bereikbaarheidsdienst. Dit betekent dat iedereen af en toe een piketdienst draait. Bij een groter incident wordt de inzet van het hele team opgeschaald. Uiteraard blijft het bij incidentele gevallen en onze ervaring is dat onze professionals erbij willen zijn, als de nood zich aandient.

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 zestien 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. Bij ons hechten we 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.