Security analist (aanmelden talentpool)

Functieomschrijving

Cyberveiligheid borgen op een plek waar het er écht toe doet. En in een uitdagend ICT-landschap. Dat doe je bij SSC-ICT, dé ICT-dienstverlener van en voor de Rijksoverheid. Binnen ons Security Operations Center zijn er doorlopend mogelijkheden voor medior en senior security analisten. Daarom zoeken we op voorhand alvast contact met ervaren specialisten zoals jij.

De Talentpool

Word jij onderdeel van onze talentpool? Meld je nu aan! Onze talentpool is een expertpool waarin jij als ICT-specialist je cv kan uploaden zonder motivatiebrief.

Sta vooraan in de rij

Bij een positieve beoordeling nemen we jouw cv op in ons recruitmentsysteem en gaan we voor je op zoek naar een passende functie. Hebben we een passende functie beschikbaar in de toekomst? Dan nemen we zo snel mogelijk contact met je op en gaan we in gesprek. Op deze manier ben jij altijd als eerste op de hoogte over ons functieaanbod en vergroot je de kans op een mooie en succesvolle vervolgstap in jouw ICT-loopbaan.

Hieronder lees je meer over wat een security analist doet bij SSC-ICT

In het kort: als security analist bij SSC-ICT ben jij de poortwachter die dreigingen signaleert en duidt voor maar liefst 7 ministeries. Je kunt je wel voorstellen hoe groot en complex het totale netwerk is dat jij en je collega's overzien. Als Rijksoverheid zijn we bovendien een doelwit van APTs.

Jouw baan als security analist

In het Security Operations Center (SOC) van SSC-ICT werk je midden in de actie. Uit enorme datastromen volgen meldingen die variëren van klein en onschuldig tot groot en urgent. Jij analyseert en duidt ze met geavanceerde SIEM-tooling. Ook neem je verantwoordelijkheid voor de opvolging door beheerteams mee te nemen in de juiste maatregelen. Daarnaast denk je mee over de doorontwikkeling van het SOC, bijvoorbeeld door detectieregels te verbeteren, rapporten over cyberdreigingen te analyseren of processen te automatiseren. Zo help je de Rijksoverheid structureel veiliger te werken.

Een greep uit jouw taken:

- Dreigingen zoals kwetsbaarheden en malware identificeren via onder meer meldingen uit SIEM-tooling en rapportages van het Nationaal Cyber Security Centrum of interne beheerteams.
- Meldingen beoordelen op basis van triage: inschatten van de risico's en bepalen van passende opvolging.
- Incidenten onderzoeken met veiliggesteld materiaal (zoals logfiles of malware) en uitvoeren van root-cause-analyses om de impact te bepalen.
- Bevindingen documenteren in de kennisbank van het SOC.
- Detectieregels verbeteren en meedenken over automatisering en scripting (bijvoorbeeld Python) om processen slimmer en sneller te maken.
- Als medior en zeker als senior pak je de zwaardere en complexe incidenten op. Ook draag je je kennis proactief over aan collega's. Daarnaast neem je ook coördinerende

taken op je tijdens shifts of grote incidenten.
Als medior en zeker als senior pak je de zwaardere en complexe incidenten op. Ook draag je je kennis proactief over aan collega's. Daarnaast neem je ook coördinerende taken op je tijdens shifts of grote incidenten.
Dit maakt jouw baan extra interessant:
•Impact: je draagt bij aan onze missie om de cyberweerbaarheid van de Rijksoverheid te vergroten. Met 7 ministeries en grote netwerken werk je op gigantische schaal.
•Uitdaging: aanvallen worden steeds geavanceerder en veranderen continu. In dit dynamische dreigingslandschap blijf je leren.
•Kans om te specialiseren: je krijgt de kans om je expertise voortdurend te verdiepen via trainingen en certificeringen, bijvoorbeeld in incident response, red teaming of forensische analyse.
Herken jij jezelf in dit profiel? Upload jouw cv in de talentpool!
Of je nu een ervaren security architect, -coördinator of -engineer bent: je kunt je cv altijd toevoegen aan de talentpool. Bij een positieve beoordeling nemen we contact met je op.

Functie-eisen

Om in te stromen in schaal 12 heb je in ieder geval:
•Hbo-niveau door opleiding of ervaring, en bij voorkeur een diploma in ICT of security.
•3 jaar ervaring in een vergelijkbare functie bij een Security Operations Center.
•Aantoonbare kennis van SIEM-tooling (bijv. Splunk), Linux- en Windows-omgevingen.
•Ervaring met het analyseren van dreigingen en risico's op het gebied van computernetwerken.
•Inzicht in wet- en regelgeving en de vaardigheid dit te vertalen naar techniek.
•Bekendheid met aanvalstechnieken (technisch én social engineering) en de vaardigheid om deze uit te leggen aan collega's.
•Een goede beheersing van de Nederlandse taal.
•Bij voorkeur één of meerdere securitycertificeringen (bijv. GIAC GSEC, GCIH, GMON, GCIA, Microsoft SC-200).
Om in te stromen in schaal 13 verwachten we – naast bovenstaande – dat je:
•Minimaal 5 jaar ervaring hebt in een vergelijkbare functie bij een Security Operations Center.
•In staat bent om het voortouw te nemen bij complexe dossiers, verbeteringen in het SOC, het coachen van collega's en het coördineren van incidentafhandeling.
Competenties
Verder is het fijn als je de volgende competenties bezit:
•Je doorziet complexe incidenten snel dankzij je sterke analytische vaardigheden.
•Je brengt bevindingen duidelijk over, ook aan niet-technische collega's, en neemt beheerteams en andere stakeholders overtuigend mee in je advies.
•Je zoekt actief de samenwerking op binnen het SOC, weet je kennis op een tactische en inspirerende manier over te brengen op collega's en draagt bij aan een cultuur van leren en verbeteren.

Word onderdeel van onze talentpool

Pak je kans en sluit je aan bij onze talentpool. Zo sta je straks vooraan wanneer er nieuwe en passende functies beschikbaar komen. Door je aan te melden via de knop 'solliciteren' upload je jouw cv in ons recruitmentsysteem. We beoordelen jouw cv en nemen bij een positieve beoordeling contact met je op om je te informeren over de actuele en aankomende functies. Zo weet je precies waar je aan toe bent. Uiteraard houden we ons aan de voorgeschreven privacywetgeving.

Belangrijk: het is voor de talentpool van belang dat je aangeeft dat we jouw gegevens

voor één jaar mogen bewaren. Dit kun je verderop in het proces aangeven.
Heb je vragen? Stuur ons gerust een bericht.

Meer over jouw toekomstige afdeling

Je gaat aan de slag in het Security Operations Center (SOC) van SSC-ICT: een hecht team van zo'n 16 collega's met verschillende leeftijden, achtergronden en expertises. We werken in een open en informele sfeer, waarin we elkaar vertrouwen, uitdagen en versterken.
Werk je aan procesverbeteringen of automatisering, dan is thuiswerken in overleg mogelijk. Operationeel werk doen we vooral vanuit het SOC, zodat we direct kunnen schakelen. We lunchen vaak samen en sluiten de week ook regelmatig samen af met wat gezelligheid. Zo combineren we een serieuze missie met een teamcultuur waarin veel ruimte is voor plezier. We hechten ook veel waarde aan een goede werk-privébalans, waarbij we respect hebben voor ieders persoonlijke situatie.

Draag bij aan ICT die Nederland vooruitbrengt

Bij SSC-ICT draait alles om slimme, veilige en betrouwbare digitale oplossingen voor de overheid. En daar hebben we de beste mensen voor nodig, zoals jij!

Bijzonderheden

- Goed om te weten: in alle lagen van ons SOC hebben we een bereikbaarheidsdienst. Dit betekent dat iedereen af en toe (ongeveer eens in de 3 à 4 maanden) een piketdienst draait. Bij een groter incident wordt het hele team ingezet.

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.