Security Analist - Level 3

Functieomschrijving

De Justitiële ICT Organisatie – een grote ICT-leverancier binnen de Overheid – is op zoek naar een **Security Analist Level 3**.

De kerntaak van de Security Analist Level 3 binnen het Security Operations Center is het opsporen, signaleren, analyseren en afhandelen van IT-beveiligingsincidenten binnen de door beheerder (klant)systemen en infrastructuur. Daarnaast ondersteunt de analist het SOC-team op 1e, 2e en 3e lijnsniveau bij cybersecurity-onderzoeken en draagt hij bij aan het verbeteren en ontwikkelen van de security monitoring-dienstverlening voor klanten en de onderliggende processen. Het SOC-team bevindt zich momenteel in een opbouwfase en bestaat uit een aantal analisten op verschillende niveaus, experts op het gebied van security monitoring, forensisch onderzoekers, en wordt aangestuurd door het hoofd SOC.

Als SOC Analist ben je verantwoordelijk voor het monitoren en analyseren van security events met behulp van SIEM/IDS en endpoint security systemen. Je houdt je bezig met het analyseren en opvolgen van beveiligingsmeldingen en incidenten, waarbij je nauw samenwerkt met verschillende oplospartijen binnen de organisatie. Dit omvat ook het beheer van openstaande meldingen en wijzigingen om de voortgang te waarborgen. Daarnaast ben je actief in het identificeren en analyseren van dreigingen die de organisatie kunnen beïnvloeden.

Een belangrijk onderdeel van je rol is het doorontwikkelen en implementeren van SIEM en monitoringtechnologie. Je zorgt ervoor dat logbronnen correct worden aangesloten en gemonitord op SOC-platformen om bedreigingen tijdig te detecteren. Tot slot werk je aan het ontwikkelen van SOC-werkprocessen, zodat de beveiligingsprocessen optimaal en efficiënt verlopen.

Naast de primaire taken draag je bij aan de beleids- en adviesvoorbereiding op het gebied van informatiebeveiliging, mede naar aanleiding van ontwikkelingen of incidenten. Je stelt adviezen en feitenrapportages op met betrekking tot securitymaatregelen en voorziet het security management en de beheerorganisaties van advies.

Ook ben je betrokken bij het scripten en automatiseren van SOC-platformen en voer je kwetsbaarheidsscans uit om zwakke plekken binnen de infrastructuur op te sporen. Waar nodig coördineer of voer je kwetsbaarheidsanalyses uit. Tot slot stel je rapportages op om inzicht te geven in de beveiligingsstatus en de uitgevoerde acties.

Ons hoofdkantoor is momenteel gevestigd in Gouda, maar medio 2027 verhuizen we naar Utrecht, direct achter Utrecht Centraal. Deze verhuizing biedt nieuwe kansen om onze samenwerking te versterken en innovatie te stimuleren. Bovendien komen we daarmee centraal in Nederland te liggen, wat onze bereikbaarheid voor zowel opdrachtgevers als collega’s verder vergroot.

Functie-eisen

- HBO- of academisch werk- en denkniveau met een sterk analytisch vermogen.
- Minimaal 5 tot 10 jaar ervaring in cybersecurity en operationele security monitoring.
- Diepgaande kennis van netwerktechnologie (routing, switching, TCP-IP, proxies, firewalls) en operating systemen (Windows en Linux) op gevorderd beheerdersniveau, inclusief beveiliging.
- Ervaring met SIEM- en logmanagementsystemen (bijv. Splunk, Elastic, Arcsight, IBM) en kennis van IDS, endpoint security (EDR) en pentesting-tools.
- Scripting- of programmeerkennis (bijv. Bash, Python, C#, PowerShell, Java, JavaScript, PHP) en basiskennis van toegepaste cryptografie.

•Bereidheid om intensieve technische trainingen te volgen en te specialiseren in operationele security en monitoring.

Overige arbeidsvoorwaarden

Naast het salaris ontvang je een individueel keuzebudget (IKB). Het IKB bestaat uit geld (16,5% 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 fiscaalvriendelijke 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. Daarnaast is er binnen de Justitiële ICT Organisatie een activiteitencommissie en zijn er werkgroepen op het gebied van “Vitaliteit” en “Werkgeluk” actief. Deze organiseren diverse activiteiten voor haar medewerkers om actief en energiek te blijven en verbinding te houden.

Bijzonderheden

Binnen de Rijksoverheid wordt er gebruik gemaakt KWIV-profielen.
Meer informatie kun je vinden op Kwaliteitsraamwerk Informatievoorziening (KWIV) - Functiegebouw Rijk (functiegebouwrijksoverheid.nl)
Een assessment kan onderdeel uitmaken van de selectieprocedure. Ben je in dienst van het Rijk en heb je een aanwijzing als VWNW- of (medisch) herplaatsingskandidaat? Voeg dan een voordracht van jouw leidinggevende of mobiliteitsadviseur én een kopie van de aanwijzingsbrief bij je sollicitatie.
Acquisitie naar aanleiding van deze vacature wordt niet op prijs gesteld