SOC Analist

Functieomschrijving

Ben jij een ervaren SOC Analist die alles weet over informatiebeveiliging? Wil jij werken in het hart van de digitale overheid?

Dan gaan we graag met jou in gesprek!

Als SOC Analist werk je in het hart van de digitale overheid. Samen met je collega's bewaak je de digitale veiligheid voor producten en diensten zoals DigiD, MijnOverheid en Digipoort. Dankzij deze diensten van Logius kunnen mensen veilig hun belastingaangifte doen, kan een overheidsorganisatie digitaal post sturen naar burgers en kan de Douane miljoenen berichten over inkomende en uitgaande goederen verwerken.

Je bent verantwoordelijk voor de ontwikkeling, inrichting en verbetering van monitoring- en detectie middelen. Je analyseert cyberdreigingen, onderzoekt securitymeldingen en adviseert over passende maatregelen.

Daarbij schakel je met technisch specialisten, data-analisten, fraudespecialisten, product owners en management. Ook denk je proactief mee over de verdere ontwikkeling van de monitoring- en detectiearchitectuur van Logius.

Logius wil sneller inspelen op veranderingen in de samenleving, die staat nooit stil en wij ook niet. Daarom werken wij met het SAFe-raamwerk als best practice om Agile werken toe te passen waardoor wij als organisatie wendbaar en flexibel kunnen inspelen op deze veranderlijke samenleving. Samenwerken staat daarbij voorop in onze manier van denken, werken en organiseren.

Jouw werkzaamheden:

- Monitoren en analyseren van security events met SIEM en endpoint securitysystemen
- Analyseren en opvolgen van security meldingen- en incidenten
- Identificeren en analyseren van dreigingen voor de Logius organisatie
- Uitvoeren van kwetsbaarheidsscans en analyseren van de resultaten, inclusief het opstellen van adviesrapportages.
- Doorontwikkelen van SOC-processen en aansluiten van de nieuwe Logius producten en diensten op het SIEM
- Inhoudelijk verantwoordelijk voor de juiste inrichting van Monitoring & detectie middelen
- Zelfstandig ontwikkeling en realisatie van complexe technische monitoring en detectie middelen
- Zelfstandig technische analyse kunnen opzetten en opvolgen m.b.t. cybersecurity

Je persoonlijke ontwikkeling vinden we erg belangrijk. Daar krijg je bij ons alle ruimte en diverse mogelijkheden voor om te groeien in de richting die bij jou past.

Functie-eisen

Je hebt minimaal vijf jaar relevante werkervaring op hbo- of wo-niveau en beschikt over brede kennis van informatiebeveiliging en IT-systemen. Je bent analytisch sterk, doorgrondt complexe systemen en netwerken en weet technische bevindingen te vertalen naar heldere adviezen voor managers en bestuurders. Ook onder druk behoud je het overzicht en werk je effectief samen met collega's en leveranciers aan de veiligheid en continuïteit van de Logius-dienstverlening.

Verder heb jij:

- Aantoonbare kennis van IP-netwerken, securitymonitoring, aanvalstechnieken, malware en Linux- en Windows-systemen.
- Ervaring met SOC-werkzaamheden en SIEM-tools, zoals Splunk, QRadar of ArcSight.

•Ervaring met beveiligingstools, zoals IDS/IPS, firewalls, vulnerability scanning en DDoS-mitigatie.
•Ervaring met scripting, loganalyse en het zelfstandig onderzoeken en rapporteren van cybersecurityincidenten.
•Bereidheid om technische trainingen te volgen en je verder te specialiseren in operationele security en monitoring.

Voor deze functie zijn tevens de volgende competenties van belang:

•Analyseren
•Creativiteit
•Netwerken
•Omgevingsbewustzijn
•Organisatiesensitiviteit
•Overtuigingskracht
•Plannen en organiseren

De Rijksoverheid streeft ernaar een werkgever te zijn waar iedere medewerker, ongeacht leeftijd, sekse, geaardheid, etnische afkomst en arbeidsbeperking voor wil werken. Werken aan maatschappelijke vraagstukken in divers samengestelde teams maakt ons effectiever en innovatiever. Bij Logius is daarom iedereen welkom

Bijzonderheden

•Een referentiecheck maakt onderdeel uit van het sollicitatieproces. Dit doen we altijd in overleg met jou.
•Voor deze functie is een Verklaring Omtrent het Gedrag (VOG) vereist.
•Logius is continu in ontwikkeling, ook nu. We verbeteren onze manier van samenwerken en richten onze organisatie toekomstbestendiger in. Voor de meeste functies heeft dit geen impact op het werk zelf, al kan de plek van teams in de organisatie veranderen. We vinden het belangrijk om hier eerlijk over te zijn!

Meer over jouw toekomstige afdeling

Om beschermd en weerbaar te zijn tegen digitale aanvallen, is het nodig om zicht en grip te hebben op de digitale dienstverlening binnen Logius en op alles wat daarbinnen gebeurt. De afdeling Security Operations Center (SOC) monitort daartoe de GDI-dienstverlening en activiteiten van Logius en afnemers en onderzoekt afwijkende zaken. Het SOC richt zich daarmee op relevante informatie over de beveiliging van alle systemen en apparaten. Deze informatie leidt tot inzicht in hoe veilig het netwerk, de systemen en hard- en software binnen Logius functioneren. Daarnaast kijkt het SOC ook naar informatie over kwetsbaarheden en dreigingen in cybersecurity. De risico’s van geavanceerde digitale dreigingen en de eigen kwetsbaarheden worden steeds groter. Je komt te werken in een team van SOC/ security professionals waarbij we van elkaar willen leren. Bij het SOC werken we afwisselend thuis en op kantoor.

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.