

Security Engineer SOC

Functieomschrijving

Het SOC is de plaats waar Cybersecurity de buitenwereld ontmoet. Het RIVM als organisatie is een gewild doelwit vanwege de status en invloed haar producten op de nederlandse maatschappij. Het SOC is daarom de plek waar die het overzicht moet houden op alles dat er gebeurt en dat het hoofd koel moet houden. Begrijpen wat er gebeurt, inschatten wat de gevolgen zijn en dan de juiste acties nemen is daardoor het verschil tussen een succesvolle aanval of een mislukte aanval.

Werken bij het SOC van het RIVM betekent dat je je voor een groot deel van je tijd bezighoudt met het detecteren en mitigeren van activiteiten door kwaadwillende die het RIVM of de aangesloten organisaties schade willen berokkenen. Dat doen zij bijvoorbeeld door middel van phishingmails, pogingen tot binnendringen via een van onze honderden websites, of het detecteren en proberen te misbruiken van zwakheden in onze infrastructuur.

Naast het actief opsporen en tegengaan van dergelijke misbruikpogingen, behoort ook het -samen met anderen- technisch ontwerpen en inrichten van de securitytooling bij de functie. Evenals het adviseren van de beheerorganisatie over technische maatregelen die misbruik kunnen detecteren en waar mogelijk voorkomen.

Hoewel het merendeel van de infrastructuur van het RIVM zich bevindt in onze eigen gebouwen en datacenters, maakt het RIVM ook gebruik van cloudomgevingen. Kennis van, of de bereidheid om kennis op te doen van, de securityaspecten van Azure en AWS, met een focus op het detecteren van kwaadwillende activiteiten is belangrijk en zal in de toekomst steeds belangrijker worden. Dit alles vraagt in ons SOC een gedegen kennis van de technologie die wij gebruiken, want deze dient doorontwikkeld te worden.

Als SOC Engineer bij het RIVM speel je een kritieke rol in het versterken van onze cyberveiligheid. Je bent verantwoordelijk voor het ontwerpen, bouwen en optimaliseren van onze security monitoring-infrastructuur, terwijl je tegelijkertijd de SOC-analisten ondersteunt bij het detecteren, analyseren en mitigeren van bedreigingen. Je taken pakket is als volgt opgebouwd:

SOC Engineering (80%)

Bouwen en onderhouden van de security monitoring-omgeving:

- Microsoft Sentinel: Opzetten, configureren en optimaliseren van de inrichting van onze Microsoft Sentinel omgeving. Kennis van het werken met Biceps CI/Cd pipelines/GIT. Inrichten van de Defender XDR omgeving.
- Splunk: Inrichten van indexen, dashboards, alerts en correlation rules voor effectieve dreigingsdetectie.
- Logstroombeheer: Aansluiten, filteren en normaliseren van logs uit Windows, Linux, OpenShift, netwerkapparaten en cloudomgevingen (Azure) via Cribl naar diverse analysesystemen zoals Sentinel en splunk.

Automatisering & DevSecOps:

- Ontwikkelen en beheren van Azure DevOps-pipelines voor het automatisch uitrollen van configuraties en detectieregels.
- Git-repositories onderhouden (GitHub/Azure Repos) met consistente code, peer reviews en CI/CD-pipelines.
- Scripting & automatisering in Python, PowerShell, Bash, YAML (en optioneel Java/Go) voor logverwerking, detectieoptimalisatie en incidentresponse.

Detectie-engineering:

- Bouwen, testen en optimaliseren van detectieregels in Sentinel (KQL), Splunk (SPL) .
Dit op basis van eigen onderzoek en Threat Intel van andere partijen.

SOC Analistenondersteuning (20%)

- Samenwerken met analisten om logbronnen te prioriteren en kosteneffectieve analyse mogelijk te maken.
- Adviseren over welke loggebeurtenissen het meest relevant zijn voor dreigingsdetectie.
- Playbooks en runbooks ontwikkelen voor gestandaardiseerde processen.

Functie-eisen

Je werkt met een jong team, die in een dynamische omgeving waar proactieve beveiliging en snelle incidentresponse centraal staan. Je combineert technische expertise met een sterke analytische blik. In het team ben je communicatief sterk en de Nederlandse taal ook matig om de rapportages voor management en technische teams goed op te kunnen helpen stellen.

Verder heb je:

- Minimaal drie jaar Ervaring met SIEM/SOAR-platforms: Microsoft Sentinel, KQL, Log Analytics, Azure Monitor, Splunk,SPL, dashboards, alerts, index management;
- Aantoonbare ervaring met Cloud & DevSecOps: Infrastructure-as-Code, Azure Bicep, CI/CD: Azure DevOps, GitHub Actions, GitLab CI/CD;
- Kennis van Scripting & Automatisering met bijvoorbeeld Python, PowerShell, Bash, YAML, JSON, Ansible.

Je hebt de volgende opleidingen en certificeringen:

- Microsoft Certified: SC-200, AZ-500).
- Splunk Core Certified User/Administrator/Power User
- CISSP, CEH

Gewenste kennis van:

- Windows, Mac, Linux, OpenShift/Kubernetes, Netwerkkaparaatuur
- Threat Intelligence Platforms (TIP): MISP, OpenCTI.

Bij het RIVM hebben we één van de beste cao's van Nederland, namelijk die van de Rijksoverheid. Naast een goed salaris hebben we aantrekkelijke arbeidsvoorwaarden zoals een Individueel Keuzebudget van 16.5 % van je bruto jaarsalaris waarover je zelf de regie hebt. Je kunt iedere maand een deel laten uitbetalen of extra vrije dagen kopen of verkopen. Daarnaast bieden we fiscale voordelen om bijvoorbeeld je studieschuld af te lossen. Ook zijn we een mantelzorgvriendelijke organisatie. Meer weten? Lees er meer over onder de kop 'overige arbeidsvoorwaarden'.

Bijzonderheden

Veiligheid is niet een kantoorbaan van 8 tot 5. Daarom gelden de volgende eisen met betrekking tot jouw functie:

- Je bent beschikbaar voor standby diensten
- Je bent vrijdag beschikbaar voor werk
- Een veiligheidsonderzoek is noodzakelijk

Voor vragen over de inhoud van deze vacature kan je terecht bij Roel Vester via roel.vester@rivm.nl. Wil je telefonisch contact? Neem dan voor vragen even contact op met Guus Houdijk, Recruiter IV via 0620230816.

Vragen we in de vacaturetekst om een motivatiebrief en kun je wat hulp gebruiken om deze te schrijven? Lees dan deze 4 tips voor een goede motivatiebrief.

Informatie over solliciteren bij het RIVM:

- Wij begrijpen dat AI een handig hulpmiddel is voor jouw motivatiebrief en cv. We willen je adviseren om het enkel als hulpmiddel te gebruiken en vooral ook jouw unieke ik terug te laten komen in deze documenten.
- Bij je indiensttreding vragen we altijd om een Verklaring Omtrent Gedrag (VOG).

- Als je solliciteert als 'van-werk-naar-werkkandidaat' of als 'herplaatsingskandidaat', stuur dan een kopie van je aanwijzingsbrief mee.
- Werk je nu via een uitzend- detacheringsbureau bij de Rijksoverheid, vermeld dit dan in je brief.
- Het RIVM zet zich in om medewerkers in dienst te nemen die onder de doelgroep van de Wet Banenafpraak vallen. Meer informatie hierover vind je op de website van de Rijksoverheid.
- Bij het RIVM ben je welkom zoals je bent. Wij zijn ervan overtuigd dat diversiteit in een team de samenwerking en de uitkomst sterker maakt. Daarnaast wordt betrokkenheid van medewerkers bij medezeggenschap gewaardeerd.
- Wij volgen de Recruiter Code en gaan zorgvuldig met je persoonsgegevens om.
- Voor een volledig beeld van de zakelijke achtergrond van sollicitanten raadplegen we soms LinkedIn.
- Deze vacature gaat offline na de sluitingsdatum, vergeet dus niet om de tekst te downloaden en op te slaan. Het kan zijn dat na deze datum deze vacature nog (onbedoeld) vindbaar is op diverse jobboards. De sluitingsdatum op werkenvoornederland.nl is leidend.
- Het kan voorkomen dat de sollicitatiepagina niet werkt, het kan aan de browser liggen. Probeer in dat geval de sollicitatiepagina in een andere browser te openen.
- Wij maken geen gebruik van bureaus voor deze vacature. Mochten wij uiteindelijk hulp inschakelen, dan nemen wij hiervoor zelf contact op met bureaus.