Security Specialist

- HBO
- Tilburg
- IT(/vakgebieden/ict)
- 32 tot 38 uur
- 4.554 - 7.480

Jouw baan

Bij CZ werken we met betekenis, daadkracht en als één team.

We nemen verantwoordelijkheid, tonen lef, blijven leren en maken impact. Samen zetten we ons elke dag in voor toegankelijke en betaalbare zorg voor iedereen.
Cyberdreigingen ontwikkelen zich iedere dag. Daarom zoeken we een securityprofessional die niet alleen zal reageren op incidenten, maar ook wil begrijpen hoe aanvallers te werk gaan én actief bijdraagt aan de verdere professionalisering van ons Security Operations Center. Je onderzoekt dus meldingen, verrijkt analyses met relevante context en helpt bij het verbeteren van detectie(mogelijkheden) en monitoring. Tegelijkertijd kijken we nadrukkelijk verder dan de dagelijkse operatie. We zoeken iemand die kansen ziet om processen, werkwijzen en tooling slimmer en effectiever in te richten. In deze rol ben je dus een belangrijke schakel in het signaleren, analyseren en beheersen van securityrisico's. Naast de dagelijkse SOC-werkzaamheden neem je deel aan consignatiediensten en lever je een actieve bijdrage aan het verbeteren van de security posture van CZ door betrokkenheid bij vulnerability- en patchmanagementprocessen. We zoeken iemand die dus zowel defensief als offensief kan denken én handelen. Je houdt je onder andere bezig met:

- Het onderzoeken, analyseren en opvolgen van securitymeldingen en incidenten.
- Het uitvoeren van loganalyses en threat hunting activiteiten om dreigingen vroegtijdig te signaleren.
- Het deelnemen aan consignatiediensten en het adequaat opvolgen van security-incidenten buiten reguliere kantooruren.
- Het verzamelen en verrijken van context rondom verdachte activiteiten.
- Het verbeteren en ontwikkelen van detectieregels, use cases en monitoring(mogelijkheden).
- Het vertalen van dreigingsinformatie naar concrete acties en verbeteringen binnen CZ.
- Het actief bijdragen aan de verdere professionalisering van het SOC op het gebied van processen, samenwerking, kennisdeling (in- en extern) en kwaliteit.
- Het meedenken en handelen naar nieuwe ontwikkelingen op het gebied van AI, automatisering en cybersecurity.
- Het automatiseren van terugkerende werkzaamheden met behulp van scripting en tooling.

- Het monitoren, analyseren en verbeteren van het vulnerability management proces, inclusief het beoordelen van kwetsbaarheden, prioriteren van risico's en afstemmen van patchactiviteiten met beheerteams.

- Het adviseren over en volgen van patch management activiteiten om de security posture van CZ verder te versterken.

Binnen CZ zien we AI en automatisering als belangrijke ontwikkelingen binnen cybersecurity. Tegelijkertijd geloven we dat succesvolle inzet daarvan begint met een sterke basis in mensen, processen en detectiekwaliteit. Juist daar lever jij een belangrijke bijdrage aan.

Jouw team

Jij bent van groot belang

Je komt terecht in het Security Operations Center (SOC) van CZ, onderdeel van Tech Enablement. Het SOC speelt een cruciale rol in het beschermen van de informatie, systemen en dienstverlening van CZ. Het team bevindt zich in een fase waarin verdere professionalisering centraal staat. Er liggen mooie uitdagingen op het gebied van detectie, monitoring, procesverbetering, kennisontwikkeling en samenwerking met andere teams binnen Security en IT. Daardoor krijg je veel ruimte om mee te denken, invloed uit te oefenen en zichtbaar bij te dragen aan de ontwikkeling van security gerelateerde aspecten binnen CZ. Je werkt dagelijks samen met securityspecialisten, infrastructuurspecialisten, architecten en andere IT-teams. Daarbij combineren we een pragmatische aanpak met de ambitie om onze securityoperatie steeds verder te verbeteren.

Dit krijg je van ons

- **Focus op opleiding en ontwikkeling**
  Binnen CZ krijg je wekelijks ruimte om je te verdiepen in je vak om zo te werken aan je eigen ontwikkeling.

- **Flexibel werken**
  Jij bepaalt waar en wanneer je werkt om zo de beste werk-prive balans te bieden. Natuurlijk wel zo dat je ook nog bereikbaar bent voor je team.

- **Keuzesysteem arbeidsvoorwaarden**
  Ieder mens is anders dus jij bepaalt welke arbeidsvoorwaarden voor jou het best passen.

Jouw profiel

Dit neem je mee naar onze organisatie

- Hbo werk- en denkniveau, bij voorkeur richting IT of cybersecurity.

- Ervaring binnen een SOC, Security Operations, Incident Response of vergelijkbare omgeving.

- Ervaring met SIEM-oplossingen, securitymonitoring, incidentanalyse, loganalyse en threat intelligence.

- Kennis van Windows-, Linux- en netwerkomgevingen, aangevuld met brede securitykennis.

- Ervaring met detectieontwikkeling en het verbeteren van monitoring- en securityprocessen.

- Kennis van scripting (bijvoorbeeld PowerShell of Python); ervaring met Microsoft Sentinel, Defender XDR of vergelijkbare platformen is een pré.

- Relevante certificeringen zoals AZ-500, SC-200, Security+, GCIH of vergelijkbaar zijn een pré.

- Je bent analytisch, nieuwsgierig, communicatief sterk, werkt graag samen en denkt in verbeteringen.

Herken je jezelf niet in alle punten? Geen probleem. Motivatie, leervermogen en de juiste mindset vinden wij minstens zo belangrijk als specifieke ervaring.

Onze vragen

Een motivatiebrief is niet nodig, in plaats daarvan ontvangen we graag jouw antwoord op de volgende drie vragen:

- Hoe zou je te werk gaan als je een melding ontvangt van verdacht gedrag op een endpoint, maar de beschikbare informatie beperkt is?
- Cybersecurity verandert continu. Kun je een voorbeeld geven van een nieuwe ontwikkeling (bijvoorbeeld AI, een aanvalstechniek of tooling) die je recent hebt onderzocht?
- Welke taak binnen een SOC zou jij direct automatiseren als je morgen zou beginnen? (Op basis van huidige kennis die je hebt).

Heb je vragen over deze vacature?

Neem dan gerust contact op met Evie via email evie.vermeltfoort-moeskops@cz.nl (mailto:evie.vermeltfoort-moeskops@cz.nl). **Acquisitie naar aanleiding van deze vacature wordt niet op prijs gesteld**.

Mail (mailto:evie.vermeltfoort-moeskops@cz.nl)