Senior Adviseur Informatiebeveiliging

- WO
- Tilburg
- IT(/vakgebieden/ict)
- 32 tot 40 uur
- 5.236 - 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.
CZ IT is in beweging: het CIO Office houdt centrale regie zodat we aantoonbaar ‘in control’ blijven op onze informatievoorziening. Dat vraagt om duidelijke security-kaders én praktische toepassing daarvan in teams en leverancierssketens. In deze rol krijg je de ruimte om impact te maken op hoe CZ informatiebeveiliging organiseert, toetst en verbetert.
Als Senior Adviseur Informatiebeveiliging draag je bij aan een betrouwbare en veilige dienstverlening voor onze verzekerden. In een tijd van toenemende digitale dreigingen help jij CZ de vertrouwelijkheid, integriteit en beschikbaarheid van informatie te beschermen, zodat we onze ambities kunnen blijven realiseren. Je combineert kennis van security technologie met het vertalen en implementeren van beleid naar werkbare kaders, standaarden en richtlijnen. Vanuit jouw security-perspectief adviseer je over business- en IT-oplossingen en ben je in gesprek met collega’s uit alle bedrijfsonderdelen en lagen van de organisatie (o.a. IT-teams, Product Owners, Architectuur, Risk/Compliance/Privacy en leveranciers).
Waar jij impact maakt
Je brengt security verder van ‘afspraak’ naar ‘werkelijkheid’ door scherpe advisering, toetsing en opvolging in de keten. Denk daarbij aan:

- Security-by-design in veranderingen: van ontwerpkeuzes en risico-afwegingen tot concrete maatregelen en opvolging.
- Grip op controls en aantoonbaarheid: heldere normen, toetsing en een verbeterbacklog die echt wordt uitgevoerd.
- Derde partijen en ketenrisico’s: leveranciersbeoordelingen, eisen, afspraken en monitoring (o.a. met het oog op DORA).
- Je ontwikkelt en onderhoudt informatiebeveiligingsbeleid, standaarden en richtlijnen en vertaalt deze naar werkbare afspraken voor teams en leveranciers.
- Je toetst de inrichting en werking van security controls (o.a. ISO 27001/ISMS-principes) en maakt bevindingen concreet in prioriteiten, owners en termijnen.
- Je initieert verbeteringen in (cyber)beveiligingsmaatregelen en stimuleert waar passend de automatisering van controles (bijv. in cloud- en IAM-processen).

- Je voert leveranciersbeoordelingen uit (requirements, risico's, maatregelen) en zorgt voor duidelijke afspraken en opvolging op bevindingen.
- Je adviseert in initiatieven en changes (o.a. design reviews) en levert heldere adviezen/risico-afwegingen op die besluitvorming ondersteunen (incl. onderbouwing bij risico-acceptatie waar nodig).
- Je voert (of coördineert) risicoanalyses en assessments uit en vertaalt uitkomsten naar concrete verbeterplannen en een uitvoerbare backlog.
- Je volgt dreigingen en ontwikkelingen, deelt een actueel dreigingsbeeld en vertaalt dit naar risico's, maatregelen en prioriteiten voor opvolging binnen CZ.

Jouw team

Jij bent van groot belang

Je werkt in het Team Informatiebeveiliging. Samen stellen jullie kaders op en helpen jullie de organisatie om die kaders aantoonbaar na te leven. Vanuit deze regierol breng je security "by design" in de praktijk: je adviseert, toetst en faciliteert in samenwerking met IT-teams, Product Owners en architectuur. Je zorgt dat bevindingen niet blijven liggen, maar worden omgezet in concrete verbeteracties met duidelijke opvolging.

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

- Je hebt een achtergrond in informatiebeveiliging op tenminste HBO werk- en denkniveau en brengt minimaal 5 jaar relevante werkervaring mee (bijv. in een security-, IT-risk- of GRC-rol).
- Je hebt brede kennis van informatiebeveiliging (bijv. ISO 27001/ISMS) en kunt adviseren en toetsen op onderwerpen als cloud, IAM en netwerken. Ervaring met DORA is gewenst, maar geen vereiste.
- Je werkt risk-based: je kunt complexiteit terugbrengen tot scherpe keuzes, prioriteiten en trade-offs.
- Je bent stevig in stakeholdermanagement: je kunt adviseren, overtuigen én escaleren wanneer risico's of afspraken daarom vragen.
- Je schrijft heldere adviezen en rapportages die besluitvorming versnellen (managementniveau én uitvoering).
- Je combineert pragmatisme met kwaliteit: je kunt 'nee' verkopen met een haalbaar alternatief en je borgt opvolging op bevindingen.

Onze vragen

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

- Hoe ga jij in je dagelijkse werk om met snelle technologische ontwikkelingen op het gebied van informatiebeveiliging en AI, en hoe zorg je ervoor dat je zelf up-to-date blijft?
- Hoe draag jij vanuit jouw rol bij aan het actueel houden van het informatiebeveiligingsbeleid en het toepassen daarvan binnen de organisatie?
- Kun je beschrijven hoe jij vanuit een uitvoerende rol hebt bijgedragen aan het toepassen van ‘security by design’ binnen een organisatie die in waardestromen werkt?

Heb je vragen over deze vacature?

Neem dan gerust contact op met Rico via email rico.plomp@cz.nl(mailto:rico.plomp@cz.nl). **Acquisitie naar aanleiding van deze vacature wordt niet op prijs gesteld**.

Mail (mailto:rico.plomp@cz.nl)