

Information Security Officer 32-36 uur

Wij zijn Solido, een organisatie die veiligheid en innovatie hoog in het vaandel draagt. Ons securityteam is continu bezig met het versterken van onze digitale weerbaarheid. Om deze missie voort te zetten, zoeken we een ervaren en gedreven Information Security Officer (ISO) met een affiniteit voor IT die ons helpt bij het versterken van onze securitymaatregelen en processen.

Bij Solido waarderen we collegialiteit en expertise. We bieden een dynamische werkomgeving met ruimte voor eigen inbreng en initiatief. Daarnaast zorgen we voor een goede balans tussen werk en privé, met flexibele werktijden en mogelijkheden voor thuiswerken. Voor de verdere professionalisering van onze organisatie zijn wij op zoek naar een Security Officer (32-36 uur).

Sta jij sterk in je schoenen en wil je meebouwen aan de afdeling security van onze organisatie? Dan is de functie van Information Security Officer bij Solido misschien wel iets voor jou.

Wat ga je doen

We zoeken een Information Security Officer met ervaring die zaken helder kan uiteenzetten en waar nodig daadkrachtig kan optreden. Je kerntaken zijn:

- Stuurt informatiebeveiligingsprojecten en adviseert over selectie, effectiviteit en praktische toepassing;
- Adviseert over beveiligingseisen, begeleidt risicoanalyses en evalueert prestaties;
- Coördineert afhandeling informatiebeveiligingsincidenten;
- Stelt plannen en rapportages op inzake informatiebeveiliging;
- Draagt het informatiebeveiligingsbeleid uit;
- Uitvoering van taken die cruciaal zijn voor de dienstverlening binnen Solido.

Als Information Security Officer ben je verantwoordelijk voor het verbeteren en bewaken van onze informatiebeveiliging. Je zult nauw samenwerken met verschillende teams binnen de organisatie en richt je onder andere op:

- Security intake op hard- en software: Beoordelen van nieuwe en bestaande oplossingen op securityrisico's en compliance-eisen.
- Advies bij projecten: Begeleiden en adviseren van teams over informatiebeveiliging bij implementatie van nieuwe technologieën en processen.
- Ondersteuning bij cyberincidenten: Bijdragen aan de analyse en coördinatie van incidentrespons, inclusief forensisch onderzoek en rapportage.
- Hardenen van bestaande configuraties: Actief adviseren en begeleiden van verbeteracties zoals het versterken van O365 Conditional Access, netwerksegmentatie en endpointbeveiliging.
- Bewustwording en advies: Adviseren van management en medewerkers over best practices op het gebied van security.
- Compliance en beleid: Helpen bij het naleven van beveiligingsnormen en regelgeving (zoals ISO 27001, NIST, CIS Controls).

Dit betekent in de praktijk dat je intake doet van projecten/hardware/software. Je overleg voert met de beheerders over securitybeleid en keuzes hieromtrent in de doorontwikkeling van de techniek en de infrastructuur. Je doet interne controles/audits om vast te stellen dat beleid ook wordt nageleefd en neemt indien nodig hierop actie. Daarnaast biedt je ondersteuning aan je collega's binnen het security domein in de afhandelingen van de taken die er liggen.

Een typische werkdag begint met een overleg binnen het securityteam om de lopende dreigingen en prioriteiten te bespreken. Daarna voer je een intake uit op nieuwe software of hardware die binnen de organisatie wordt geïntroduceerd. Je adviseert een projectteam over de implementatie van beveiligingsmaatregelen en helpt met het hardenen van bestaande configuraties. Halverwege de dag neem je deel aan een incidentrespons-simulatie, waar je samen met het SOC werkt aan het testen van de organisatie brede weerbaarheid tegen cyberdreigingen. In de middag evalueer je lopende securityacties en bespreek je nieuwe beleidsmaatregelen met het management. Je sluit de dag af met een update naar de IT-experts over recente bedreigingen en best practices.

Wat vragen wij van jou

Je bent nieuwsgierig en beschikt over daadkracht. Je herkent jezelf in onze KECS (Klantgericht, Eigenaarschap, Communicatie en Samenwerken) Het coördineren van werkzaamheden en het doorhakken van knopen gaat je gemakkelijk af. Je signaleert kansen en risico's. Je bent proactief en weet hoe je een advies goed moet onderbouwen. Maar wat vooral belangrijk is: je staat stevig in je schoenen en je blijft kalm.

Je bezit kennis en kunde over de volgende onderwerpen:

- WO werk- en denkniveau, bij voorkeur aangetoond middels een diploma;
- Minimaal twee jaar relevante werkervaring in een soortgelijke functie;
- Een relevante opleiding en/of technische kennis op het gebied van Informatiebeveiliging. Bij voorkeur aantoonbaar door certificeringen zoals CISSP of CISA;
- Kennis van securitystandaarden zoals ISO 27001, NIST en CIS Controls.
- Ervaring met hardening van systemen en cloud omgevingen (o.a. Microsoft 365, Azure).
- Goede beheersing van de Nederlandse taal in woord en geschrift.
- Kennis over de BIO is een pré.
- Ervaring met incidentrespons is een pré.

Waarom bij Solido werken

Je komt terecht in een innovatieve omgeving waar jouw expertise het verschil maakt. Wij bieden volop ruimte voor persoonlijke ontwikkeling en een sleutelrol in een organisatie die meebeweegt met de toekomst. Samen bouwen we aan een efficiënte en veilige IT-dienstverlening voor onze deelnemers en klanten.

De functie is ingeschaald in salarisschaal 10 (afhankelijk van opleiding en ervaring, bij een fulltime dienstverband). We starten met een arbeidsovereenkomst voor bepaalde tijd met de intentie om deze op vaste basis te continueren. Het gaat om een structurele formatieplaats.

Verder ontvang je een individueel keuze budget (IKB). Dit is 17.05% van jouw salaris. Daarnaast bieden wij mogelijkheden om opleidingen te volgen, flexibel te werken en hebben wij verschillende vitaliteitsregelingen, waaronder onze eigen sportstimuleringsregeling en een flexibel vitaliteitsbudget in de vorm van een digitale munt (Vitknip) die je in Heerlen op veel plekken kan inzetten om jouw vitaliteit te vergroten. Je pensioen wordt opgebouwd bij het ABP. Onze arbeidsvoorwaarden zijn geregeld volgens de cao sgo.

Solliciteer

Wil jij samen met ons de toekomst van Solido verder vormgeven? Stuur dan je CV en een motivatiebrief per mail voor vrijdag 28 maart 2025 aan secretariaat@solido-it.nl en vergeet de naam van de positie niet te vermelden.

Indien je nog verdere vragen hebt, Wil je meer weten over Solido of over de inhoud van deze functie? Neem dan contact op met de teammanager Valerie Jammertzheim-de Beaumont. Zij is bereikbaar via ons algemene nummer 045 560 5111. Voor overige vragen kunt u contact opnemen met ons secretariaat via email: secretariaat@solido-it.nl of via telefoonnummer 045 211 6117

Voor deze functie wordt intern én extern geworven. Bij gelijke geschiktheid gaat de voorkeur uit naar de interne kandidaat. Acquisitie naar aanleiding van deze vacaturetekst wordt niet op prijs gesteld.