SOC Analyst
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 SOC Analyst (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 SOC Analyst die zaken helder kan uiteenzetten en waar nodig daadkrachtig kan optreden. Je werkt met de beste middelen in een complexe IT-omgeving. Dankzij jou kunnen ruim 20 lokale overheidsorganisaties en meer dan 250.000 inwoners vertrouwen op veilige digitale dienstverlening.
Je kerntaken zijn:

- Monitoren en borgen van technische beveiligingsmaatregelen voor ICT. Analyseren en evalueren van ICT-beveiligingsrisico's. Testen van onderdelen van het incident response- en/of continuïteitsplan.
- Volgen van technologische ontwikkelingen op het gebied van ICT-beveiliging. Beoordelen van actuele dreigingen en trends (o.a. via NCSC en IBD) en de impact hiervan op Solido. Documenteren van kennis voor ICT-beveiliging.

- Adviseren en presenteren van ICT-beveiligingsoplossingen en risico's aan het lijnmanagement en collega's. Opstellen van verbetervoorstellen voor ICT-beveiliging.
- Realiseren van technische beveiligingsmaatregelen en updates in systemen en netwerken. Onderhouden en door ontwikkelen van SOC-systemen. Selecteren en implementeren van beveiligingshulpmiddelen. Uitvoeren van assessments, tests en reviews.
- Bijdragen aan digitaal forensisch onderzoek bij integriteitskwesties, beveiligingsincidenten of op verzoek van het MT.
- Adviseren over en monitoren van maatregelen bij informatiebeveiligingsincidenten. Deelnemen aan het Security Incident Response Team en bijdragen met informatieverzameling, risicoanalyses en advies.

Wat vragen wij van jou

Je bent intelligent, nieuwsgierig en beschikt over daadkracht. Je herkent jezelf in onze KECS-kernwaarden (Klantgericht, Eigenaarschap, Communicatie en Samenwerken). Je signaleert kansen en risico's, weet goed te adviseren en blijft kalm onder druk. Daarnaast breng je mee:

- HBO werk- en denkniveau, bij voorkeur aangetoond met een diploma in de richting van IT of cybersecurity.
- Vermogen om verbanden te leggen en dreigingen te correleren.
- Sterk analytisch vermogen en het kunnen stellen van prioriteiten.
- Affiniteit met en oprechte interesse in informatiebeveiliging.
- Kennis van SIEM-software en andere beveiligingstools.
- Bij voorkeur relevante certificeringen zoals Security+, CySA+, SC-200, BTL1, CSA of OSCP.
- Ervaring met tools zoals Microsoft Defender suite, Exabeam, Nessus, Darktrace of SentinelOne is een pre.

Hoe ziet een werkdag eruit?

Geen dag is hetzelfde. Je start met een teamoverleg met 10 andere specialisten over nieuwe risico's en verbetervoorstellen. Daarna check je binnengekomen signaleringen van onder andere het NCSC, de IBD en Darktrace, analyseer je potentiële dreigingen en vertaal je die naar concrete acties. Je doet nog een threathunt naar aanleiding van wat tips van de IBD.

In de ochtend werk je daarna aan hardening van systemen en software. Tussendoor heb je overleg met een toonaangevend cybersecuritybedrijf ter voorbereiding van een realistische cyberoefening die onze paraatheid test.

Na de lunch analyseer je alerts in onze SIEM-omgeving. Bij incidenten schakel je snel en werk je samen met het Security Incident Response Team aan containment, analyse en herstel. Aan het eind van de dag bespreek je de resultaten van de laatste PEN-test met de CISO's en ISO's van de aangesloten organisaties.

Waarom bij Solido werken

Je komt terecht in een innovatieve en interessante grootschalige omgeving waar jouw expertise het verschil maakt. Wij bieden volop ruimte voor persoonlijke ontwikkeling en je krijgt 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 9/10 (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 en we zijn bereid om in je te investeren.

Verder ontvang je een individueel keuze budget (IKB). Dit is 17.05% van jouw salaris. We bieden de 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 e-mail voor 30 april 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 51 11. Voor overige vragen kunt u contact opnemen met ons secretariaat via email: secretariaat@solido-it.nl of via telefoonnummer 045 211 61 17

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.