Security Architect SOC

Functieomschrijving

Wil jij de architectuur achter de cyberbeveiliging van 7 ministeries vormgeven én betrokken blijven bij de dagelijkse securityoperatie? Als Security Architect binnen het Security Operations Center (SOC) van SSC-ICT in Den Haag combineer je strategische architectuur met diepgaande technische securitykennis.

Je bent de brug tussen visie en uitvoering. Je ontwikkelt en onderhoudt de SOC-architectuur en roadmap voor detectie, monitoring, log- en dataverzameling en incidentresponse. Daarbij zorg je dat architectuurkeuzes aansluiten op de SSC-ICT Enterprise Architectuur, actuele dreigingen, technologische ontwikkelingen en de behoeften van de organisatie.

Tegelijkertijd blijf je dicht bij de praktijk. Je draait mee als senior security analist en gebruikt inzichten uit complexe securitymeldingen en incidenten om de SOC-architectuur verder te verbeteren. Zo werk je op het snijvlak van security, architectuur, techniek en innovatie.

Een greep uit je werkzaamheden:

- Ontwikkelen en bewaken van de SOC-architectuurroadmap en adviseren van het management over prioriteiten en toekomstige ontwikkelingen.
- Opstellen van architectuurprincipes, standaarden, referentieontwerpen, baselines en integratiepatronen voor onder meer SIEM, monitoring, logmanagement en datapipelines.
- Uitvoeren van fit/gap-analyses voor bestaande en nieuwe on-premises- en cloudoplossingen, adviseren over technologische keuzes en vastleggen van ontwerpbesluiten in Architecture Decision Records (ADR's).
- Toetsen van ontwerpen en implementaties, ondersteunen bij audits en risicoanalyses en vertalen van kaders zoals BIO, NIS2 en AVG naar concrete architectuurrichtlijnen.
- Samenwerken met enterprise-, solution- en technische architecten, engineering, operations, compliance/privacy, threat intelligence en incidentresponse en creëren van draagvlak voor architectuurkeuzes.
- Volgen van nieuwe dreigingen en technologieën, waaronder AI/ML en behaviour analytics, en initiëren van proof-of-concepts en pilots die bij succes kunnen worden vertaald naar projectstartarchitecturen.
- Onderhouden van blauwdrukken, datastromen en integratieplannen en rapporteren over de roadmap, risico's, gaps en aanbevelingen.
- Analyseren van complexe securitymeldingen en incidenten en vertalen van bevindingen naar structurele verbeteringen in de SOC-architectuur.

Binnen het SOC werken collega's met verschillende ervaringsniveaus en specialismen. Schaal 11 richt zich voornamelijk op reguliere meldingen en incidenten. Schaal 12 heeft daarnaast een coachende en inhoudelijk sturende rol. Jij richt je op schaal 13-niveau op de meest complexe dossiers en architectuurvraagstukken.

Je vervult daarmee een belangrijke rol in de inhoudelijke richting van het SOC en bent sparringpartner voor securityspecialisten, architecten, stakeholders en management. Tegelijkertijd krijg je volop ruimte om je vakkennis verder te ontwikkelen en bij te dragen aan een SOC dat steeds slimmer en sneller cyberdreigingen detecteert en bestrijdt.

Jouw werkzaamheden sluiten aan op het KWIV-profiel 1.1.5 SYSTEEMARCHITECTUUR.

Meer informatie over KWIV-profielen vind je op: Kwaliteitsraamwerk Informatievoorziening (KWIV)

Functie-eisen

•Minimaal wo-werk- en denkniveau, bij voorkeur aangevuld met een afgeronde wo-opleiding in de richting van ICT, informatiebeveiliging of cybersecurity.
•Minimaal 5 jaar werkervaring in een vergelijkbare functie of in verschillende operationele rollen binnen een Security Operations Center (SOC).
•Ervaring met architectuurraamwerken zoals TOGAF, ArchiMate of SABSA.
•Relevante certificeringen, zoals CISSP, SABSA, CISM en/of CISA.
•Ervaring met Governance, Risk & Compliance (GRC), informatiebeveiliging en securityvraagstukken binnen publieke en private cloudomgevingen.
•Ruime ervaring met securitymonitoring, SIEM-tooling zoals Splunk en Linux- en Windows-omgevingen.
•Kennis van relevante wet- en regelgeving en het vermogen om deze te vertalen naar technische oplossingen.
•Ervaring met het begeleiden, coachen en ontwikkelen van medewerkers binnen een Security Operations Center (SOC).
•Goede beheersing van de Nederlandse en Engelse taal, zowel mondeling als schriftelijk.

Competenties

•Je beschikt over sterk strategisch en analytisch denkvermogen en vertaalt complexe securityvraagstukken naar heldere architectuurvisies en toekomstbestendige oplossingsrichtingen.
•Je legt snel verbanden tussen dreigingen, risico's en incidenten en weet hierin de juiste prioriteiten te stellen.
•Je neemt regie en durft beslissingen te nemen, ook onder druk en tijdens impactvolle cyberincidenten.
•Je deelt actief kennis, coacht collega's en draagt bij aan de verdere ontwikkeling van het team.
•Je communiceert helder en overtuigend met zowel technische specialisten als management en andere stakeholders.
•Je werkt resultaatgericht en draagt gericht bij aan het verbeteren van processen, detectiemethoden en de cyberweerbaarheid van de organisatie.
•Je bent samenwerkingsgericht en weet collega's, partners en andere betrokkenen effectief met elkaar te verbinden.

Bijzonderheden

De vermelde einddatum van de vacature is een richtlijn. Regelmatig wordt de einddatum van een vacature verlengd, maar dit heeft geen invloed op de beoordeling van kandidaten die al vóór die datum hebben gereageerd. In sommige gevallen wordt de vacature juist eerder gesloten. Wacht dus niet te lang en reageer snel!
Je wordt ingeschaald op basis van ervaring. Voldoe je nog niet volledig aan het profiel, dan begin je eerst in een aanloopschaal en krijg je de kans door te groeien naar het schaalniveau van deze functie.
De wederzijdse kennismaking en selectieprocedure bestaat uit twee gesprekken en mogelijk een assessment. Bij een positief verloop volgt een afrondend arbeidsvoorwaardengesprek.
Een Verklaring Omtrent het Gedrag (VOG) is nodig om te kunnen starten als medewerker bij SSC-ICT.
Een AIVD A-veiligheidsonderzoek is onderdeel van de procedure.

Meer over jouw toekomstige afdeling

Je gaat aan de slag bij het Security Operations Center (SOC), onderdeel van de Chief Technology Office (CTO). Met zo'n 16 collega's vormen we een divers team qua leeftijd en culturele achtergrond. Er heerst een informele werksfeer waarin mensen elkaar

vertrouwen en op elkaar kunnen bouwen. In ons team streven we ernaar om elkaar te versterken en uit te dagen, zodat we continu groeien en scherp blijven. We hechten veel waarde aan een goede balans tussen werk en privé, waarbij we respect hebben voor ieders persoonlijke situatie. We hebben een hechte band en sluiten de week het liefst gezamenlijk af met een drankje.

Dit bieden we nog meer

Naast het salaris ontvang je een Individueel Keuzebudget (IKB). Het IKB bestaat uit geld (16,50% van je bruto jaarsalaris) en tijd. Met het IKB maak jij de keuzes die bij jou passen en kun je een deel van je arbeidsvoorwaarden zelf samenstellen. Je kunt er bijvoorbeeld voor kiezen om een deel van je maandinkomen te laten uitbetalen wanneer jij dat wenst. Ook kun je dit budget omzetten in verlof en andersom of besteden aan fiscaal vriendelijke doelen. De Rijksoverheid hecht sterk aan persoonlijke groei en loopbaanontwikkeling en biedt daarvoor tal van mogelijkheden. Tot de secundaire arbeidsvoorwaarden behoren onder meer verschillende studiefaciliteiten, bedrijfsfitness, volledige vergoeding van je OV-reiskosten woon-werkverkeer en gedeeltelijk betaald ouderschapsverlof.