Security analist

FF09 ICT-infrastructuur, beheer en security · ISCO-08 2529 · CBS 0812 Systeembeheerders en netwerkspecialisten · senioriteit medior · Ook bekend als: Securityanalist, SOC analist, Cybersecurity analist, Security operations analist, Beveiligingsanalist

Onderzoekt meldingen en logging op tekenen van aanvallen, bepaalt de ernst daarvan en zet de vervolgstappen bij incidenten in gang.

De security analist werkt in de monitoringketen en beoordeelt de stroom van meldingen die uit detectiesystemen komt. Anders dan de security engineer bouwt hij de detectie niet, en anders dan de security officer werkt hij op incidentniveau in plaats van op beleid. In de selectie wordt vooral naar toolervaring gevraagd, terwijl de functie afhangt van onderzoekshouding en kalmte: het merendeel van de meldingen is ruis, en wie onder tijdsdruk moet beslissen welke melding wel echt is, heeft bronbeoordeling en dossieropbouw nodig in plaats van routine.

Kerncijfers van dit profiel

25 skills · 4 te meten competenties · 5 knockout-skills · zwaartepunt: Digitaal, data en AI 57%, Cognitief vermogen en probleemoplossing 18%, Zelfmanagement, drive en veerkracht 9%

1 Te meten competenties

Dit zijn de gedrags- en capaciteitsconstructen in dit profiel. Per competentie staat erbij met welke hrmforce-vragenlijst je die meet.

Te meten competenties	Streefniveau	hrmforce instrument	Meetmethode	Gedragsanker op streefniveau
Stressbestendigheid Competentie (50-framework): Stressbestendigheid	N4	Big Fifty, 15PF, Mentale Weerbaarheid (4C)	Persoonlijkheidsvragenlijst	Blijft bij piekdrukte gestructureerd werken, houdt afspraken met opdrachtgevers helder en signaleert vroegtijdig welke resultaten in gevaar komen.
Nauwkeurigheid en aandacht voor detail Competentie (50-framework): Nauwkeurigheid	N4	Big Fifty, 360 Feedback	Persoonlijkheidsvragenlijst	Bouwt in het eigen proces controlemomenten in, houdt fouten bij en voorkomt herhaling door de werkwijze aan te passen.
integriteit en betrouwbaarheid Competentie (50-framework): Integriteit	N4	Big Fifty (schaal Integriteit), 360 Feedback, Structureerd interview	Persoonlijkheidsvragenlijst	Meldt uit eigen beweging een mogelijke belangenverstrengeling en vraagt om toetsing voordat er een besluit wordt genomen.

Te meten competenties	Streefniveau	hrmforce instrument	Meetmethode	Gedragsanker op streefniveau
Discipline en afspraken nakomen Competentie (50-framework): Discipline	N4	Big Fifty, 15PF, 360 Feedback	Persoonlijkheidsvragenlijst	Zegt alleen toe wat haalbaar is, houdt de eigen toezeggingen bij en informeert betrokkenen zodra een datum onder druk staat.

2 Volledig skillprofiel

Alle skills van dit profiel, op gewicht gesorteerd. Het gedragsanker onder elke skill hoort bij het streefniveau.

T	Skill	Streefniveau	Gewicht	Knockout	Meetmethode	hrmforce instrument
V	Respons op beveiligingsincidenten Leidt de organisatiebrede responsorganisatie, beslist over communicatie naar buiten en verbetert het draaiboek na elke oefening.	N5	5	ja	Simulatie	Kennistoets (klantspecifiek), Werkproef
V	Probleemanalyse Splitst een terugkerende klacht in mogelijke oorzaken, toetst die met eigen gegevens en benoemt de meest waarschijnlijke oorzaak.	N4	5	ja	Assessment center	Competency Check, Ability Scan
V	Kritisch denken en bronbeoordeling Ontdekt in rapporten drogredenen en selectief bewijs, en benoemt welke conclusie de gegevens wel dragen.	N4	5	nee	Werkproef	Competency Check, Werkproef
G	Stressbestendigheid Blijft bij piekdrukte gestructureerd werken, houdt afspraken met opdrachtgevers helder en signaleert vroegtijdig welke resultaten in gevaar komen.	N4	5	nee	Persoonlijkheidsvragenlijst	Big Fifty, 15PF, Mentale Weerbaarheid (4C)
V	Data-analyse Kiest zelf analysemethoden bij een open vraag, bewerkt ruwe gegevens tot een werkbestand en onderbouwt elke conclusie met cijfers.	N4	5	nee	Werkproef	Ability Scan, Werkproef
K	Netwerkbasiskennis Leidt uit symptomen af in welke laag van het netwerk een probleem zit en onderbouwt dat met eigen metingen.	N4	5	ja	Kennistoets	Kennistoets (klantspecifiek)

T	Skill	Streefniveau	Gewicht	Knockout	Meetmethode	hrmforce instrument
V	Incidentbeheer en storingsoplossing Stelt bij een onbekende storing zelf een onderzoekslijn op, herstelt de dienst en legt oorzaak en oplossing vast voor hergebruik.	N4	5	ja	Werkproef	Werkproef, Kennistoets (klantspecifiek)
V	Dreigings- en risicoanalyse Voert zelfstandig een dreigingsanalyse uit op een toepassing, prioriteert risico's en adviseert over maatregelen met kosten en effect.	N4	5	nee	Werkproef	Kennistoets (klantspecifiek), Werkproef
V	Toegangsbeheer en identiteitsbeheer Ontwerpt rollen en rechten voor een applicatie, voert de periodieke controle uit en corrigeert te ruime toegang.	N4	5	ja	Werkproef	Kennistoets (klantspecifiek), Werkproef
V	Informatie verzamelen en filteren Kiest zelf bronnen bij een open vraag, filtert dubbele en verouderde gegevens weg en verantwoordt die keuze.	N4	4	nee	Werkproef	Competency Check, Werkproef
G	Nauwkeurigheid en aandacht voor detail Bouwt in het eigen proces controlemomenten in, houdt fouten bij en voorkomt herhaling door de werkwijze aan te passen.	N4	4	nee	Persoonlijkheidsvragenlijst	Big Fifty, 360 Feedback
G	integriteit en betrouwbaarheid Meldt uit eigen beweging een mogelijke belangenverstrengeling en vraagt om toetsing voordat er een besluit wordt genomen.	N4	4	nee	Persoonlijkheidsvragenlijst	Big Fifty (schaal Integriteit), 360 Feedback, Structureerd interview
G	Discipline en afspraken nakomen Zegt alleen toe wat haalbaar is, houdt de eigen toezeggingen bij en informeert betrokkenen zodra een datum onder druk staat.	N4	4	nee	Persoonlijkheidsvragenlijst	Big Fifty, 15PF, 360 Feedback

T	Skill	Streefniveau	Gewicht	Knockout	Meetmethode	hrmforce instrument
V	Informatiebeveiliging in het werkproces Weegt bij nieuwe werkafspraken de beveiligingsrisico's mee, past maatregelen aan en spreekt collega's aan op onveilig gedrag.	N4	4	nee	Kennistoets	Kennistoets (klantspecifiek)
V	Cloudplatformen benutten Richt zelfstandig clouddiensten in voor een toepassing, regelt rechten en back ups en houdt kosten en verbruik in beeld.	N4	4	nee	Kennistoets	Kennistoets (klantspecifiek)
K	Informatiebeveiligingsbewustzijn Legt collega's uit hoe dreigingen werken, beoordeelt twijfelgevallen zelf en past het eigen gedrag aan nieuwe dreigingen aan.	N4	4	nee	Kennistoets	Kennistoets (klantspecifiek)
V	Leren van fouten en incidenten Analyseert eigen fouten en die van het team, bespreekt de oorzaak open in het werkoverleg en past afspraken aan.	N3	3	nee	Situational Judgement Test	360 Feedback, Competency Check
V	Professioneel bijblijven en vakliteratuur Houdt structureel bronnen en richtlijnen bij, weegt de kwaliteit ervan en past de eigen werkwijze aan nieuwe inzichten aan.	N3	3	nee	Portfolio/bewijsstuk	Portfolio, Kennistoets (klantspecifiek)
V	Technische documentatie schrijven Schrijft complete documentatie voor een systeem of proces, test die met een onbekende lezer en houdt versies bij.	N3	3	nee	Werkproef	Werkproef, Portfolio
V	Systeembeheer en monitoring Beheert een systeemomgeving zelfstandig, stelt bewakingsdrempels in en verbetert terugkerende oorzaken van verstoringen.	N3	3	nee	Werkproef	Kennistoets (klantspecifiek), Werkproef

T	Skill	Streefniveau	Gewicht	Knockout	Meetmethode	hrmforce instrument
V	Releasebeheer en deployment Stelt zelf een uitrolplan met terugvaloptie op, stemt af met betrokkenen en controleert na uitrol of de dienst goed werkt.	N3	3	nee	Werkproef	Kennistoets (klantspecifiek), Werkproef
V	Procesautomatisering Beschrijft een proces in stappen, automatiseert de herhaalbare stappen en bouwt controles in op fouten en uitzonderingen.	N3	3	nee	Werkproef	Werkproef, Portfolio
V	Calamiteiten- en crisisorganisatie Vervult zelfstandig een rol in een crisisteam, houdt het beeld actueel en zorgt dat besluiten worden vastgelegd.	N3	3	nee	Simulatie	Werkproef, Competency Check
V	Servicegesprekken en telefonie Handelt afwijkende vragen in één gesprek af, houdt de gesprekstijd in de hand en vat de afspraak hoorbaar samen.	N3	2	nee	Werkproef	Werkproef, Communicatiestijlen
V	Dataclassificatie en bewaartermijnen Stelt voor een informatiestroom de classificatie en bewaartermijn vast en controleert of opschoning volgens plan gebeurt.	N3	2	nee	Kennistoets	Kennistoets (klantspecifiek), Werkproef

3 Niveaus per senioriteit

Hetzelfde profiel, met de senioriteitsbijstelling van de functiefamilie toegepast. De streefniveaus zijn begrensd op 1 tot 5.

Skill	junior	medior	senior
Respons op beveiligingsincidenten	N5	N5	N5
Probleemanalyse	N3	N4	N5
Kritisch denken en bronbeoordeling	N3	N4	N5
Stressbestendigheid	N4	N4	N4
Data-analyse	N3	N4	N5
Netwerkbasiskennis	N3	N4	N5
Incidentbeheer en storingsoplossing	N3	N4	N5
Dreigings- en risicoanalyse	N4	N4	N4
Toegangsbeheer en identiteitsbeheer	N3	N4	N5
Informatie verzamelen en filteren	N3	N4	N5
Nauwkeurigheid en aandacht voor detail	N3	N4	N5
integriteit en betrouwbaarheid	N3	N4	N5
Discipline en afspraken nakomen	N3	N4	N5
Informatiebeveiliging in het werkproces	N3	N4	N5
Cloudplatformen benutten	N3	N4	N5
Informatiebeveiligingsbewustzijn	N3	N4	N5
Leren van fouten en incidenten	N2	N3	N4
Professioneel bijblijven en vakliteratuur	N2	N3	N4
Technische documentatie schrijven	N2	N3	N4
Systeembeheer en monitoring	N3	N3	N3
Releasebeheer en deployment	N2	N3	N4
Procesautomatisering	N2	N3	N4
Calamiteiten- en crisisorganisatie	N2	N3	N4
Servicegesprekken en telefonie	N2	N3	N4
Dataclassificatie en bewaartermijnen	N2	N3	N4

4 De niveauschaal

Niveau	Label	Autonomie	Complexiteit	Bereik	Kennisdiepte
N1	**Begeleid**	werkt onder toezicht en volgt instructie	routinematig, een variabele tegelijk	eigen taak	basisbegrip, kent de termen
N2	**Toepassend**	werkt zelfstandig binnen vastgestelde kaders	bekende situaties met beperkte variatie	eigen rol	werkkennis, past standaardaanpak toe
N3	**Zelfstandig**	stelt de eigen aanpak vast en vraagt zelf om input	meerdere variabelen, enige ambiguïteit	eigen team of proces	grondige kennis, weegt alternatieven
N4	**Sturend**	geeft anderen richting en beslist over de aanpak	complex, met tegenstrijdige belangen	meerdere teams of een afdeling	diepgaande kennis, adviseert anderen
N5	**Toonaangevend**	zet de standaard en het beleid	strategisch, met hoge onzekerheid	organisatie, keten of vakgebied	autoriteit, ontwikkelt het vakgebied

5 Gedragsankers per skill

Ankers staan op N1, N3 en N5. N2 en N4 zijn bewust niet geankerd: beoordelaars plaatsen die daartussen, conform de O*NET-conventie.

Skill	N1	N3	N5
Respons op beveiligingsincidenten Handelt bij een beveiligingsincident volgens draaiboek door te beperken, bewijs te bewaren, te herstellen en de juiste partijen tijdig te informeren.	Meldt een vermoed incident onmiddellijk, raakt niets aan en volgt de aanwijzingen van de coördinator.	Beperkt zelfstandig de schade bij een incident, bewaart bewijsmateriaal en levert een navolgbare tijdlijn van gebeurtenissen op.	Leidt de organisatiebrede responsorganisatie, beslist over communicatie naar buiten en verbetert het draaiboek na elke oefening.
Probleemanalyse Ontleedt een vraagstuk in onderdelen, scheidt oorzaken van gevolgen en benoemt welke informatie nodig is om verder te komen.	Benoemt bij een storing wat er precies afwijkt en welke gegevens ontbreken, en legt dit voor aan de begeleider.	Splitst een terugkerende klacht in mogelijke oorzaken, toetst die met eigen gegevens en benoemt de meest waarschijnlijke oorzaak.	Herleidt hardnekkige organisatieproblemen tot een klein aantal grondoorzaken en legt de analysemethode vast die andere teams gaan gebruiken.
Kritisch denken en bronbeoordeling Toetst beweringen op logica, bewijs en belang van de bron en onderscheidt daarbij feiten van meningen en aannames.	Vraagt bij een bewering waar die op gebaseerd is en controleert of de bron genoemd en vindbaar is.	Ontdekt in rapporten drogredenen en selectief bewijs, en benoemt welke conclusie de gegevens wel dragen.	Stelt de toetsingscriteria voor bronnen en claims op, ook voor door kunstmatige intelligentie gemaakte teksten, en handhaaft die organisatiebreed.
Stressbestendigheid Blijft bij tijdsdruk, tegenspraak of onverwachte wendingen dezelfde kwaliteit werk leveren en houdt in het contact met anderen een zakelijke toon.	Werkt bij oplopende drukte door aan de lopende taak en vraagt de begeleider welke taak kan wachten.	Blijft bij piekdrukte gestructureerd werken, houdt afspraken met opdrachtgevers helder en signaleert vroegtijdig welke resultaten in gevaar komen.	Houdt in crisissituaties de organisatie werkbaar, neemt onder hoge onzekerheid besluiten en zet de norm voor kalm handelen onder druk.

Skill	N1	N3	N5
Data-analyse Bewerkt en analyseert gegevensbestanden om patronen, verbanden en afwijkingen te vinden en verbindt de uitkomsten aan de oorspronkelijke vraag.	Voert een vooraf beschreven analysestap uit op een aangeleverd bestand en legt de uitkomst vast in het afgesproken format.	Kiest zelf analysemethoden bij een open vraag, bewerkt ruwe gegevens tot een werkbestand en onderbouwt elke conclusie met cijfers.	Bepaalt de analysestandaarden van de organisatie, beoordeelt analyses van anderen en zet nieuwe analysemethoden in het vakgebied neer.
Netwerkbasiskennis Kent de werking van netwerken op hoofdlijnen zoals adressering, routering, poorten en naamsopvraging en benoemt waar een verbindingsprobleem kan ontstaan.	Legt uit welke onderdelen een verbinding vormen en voert een aangereikte controle zoals een verbindingstest uit.	Leidt uit symptomen af in welke laag van het netwerk een probleem zit en onderbouwt dat met eigen metingen.	Draagt de netwerkkennis in de organisatie uit, stelt de ontwerpuitgangspunten vast en beoordeelt netwerkontwerpen van leveranciers.
Incidentbeheer en storingsoplossing Neemt storingen aan, stelt de oorzaak vast via gerichte stappen, herstelt de dienst en houdt melders en betrokkenen op de hoogte.	Registreert een storing volledig, doorloopt de standaardstappen en schaalt op zodra de eigen stappen niet werken.	Stelt bij een onbekende storing zelf een onderzoekslijn op, herstelt de dienst en legt oorzaak en oplossing vast voor hergebruik.	Richt het incidentproces van de organisatie in, leidt de aanpak bij zware verstoringen en verantwoordt die naar directie en klanten.
Dreigings- en risicoanalyse Brengt dreigingen, zwakke plekken en gevolgen voor een systeem of proces in kaart, weegt kans tegen impact en benoemt passende maatregelen.	Vult een risico-inventarisatie in aan de hand van een gegeven lijst dreigingen en legt de uitkomst voor aan de specialist.	Voert zelfstandig een dreigingsanalyse uit op een toepassing, prioriteert risico's en adviseert over maatregelen met kosten en effect.	Bepaalt de risicobereidheid en analysemethode van de organisatie en verantwoordt het beveiligingsrisicobeeld aan de directie.
Toegangsbeheer en identiteitsbeheer Kent rechten toe op basis van rol en noodzaak, controleert periodiek wie waar bij kan en trekt rechten in bij wijziging of uitstroom.	Verwerkt aanvragen voor toegang volgens het vastgestelde rollenschema en legt elke wijziging vast.	Ontwerpt rollen en rechten voor een applicatie, voert de periodieke controle uit en corrigeert te ruime toegang.	Bepaalt het toegangsbeleid van de organisatie en verantwoordt de beheersing van rechten bij audits.
Informatie verzamelen en filteren Zoekt gericht naar gegevens in meerdere bronnen, selecteert wat relevant is voor de vraag en laat overige informatie weg.	Zoekt in aangewezen bronnen de gevraagde gegevens op en levert die volledig en met bronvermelding aan.	Kiest zelf bronnen bij een open vraag, filtert dubbele en verouderde gegevens weg en verantwoordt die keuze.	Richt de informatiestromen voor het hele vakgebied in, bepaalt welke bronnen gezaghebbend zijn en schrapt overbodige rapportages.
Nauwkeurigheid en aandacht voor detail Werkt zorgvuldig, controleert het eigen werk op fouten en houdt zich aan afspraken over volledigheid en juistheid van gegevens.	Loopt het eigen werk na met een checklist en herstelt gevonden fouten voordat het werk wordt doorgegeven.	Bouwt in het eigen proces controlemomenten in, houdt fouten bij en voorkomt herhaling door de werkwijze aan te passen.	Stelt de normen voor volledigheid en juistheid vast, laat steekproeven uitvoeren en spreekt teams aan op structurele slordigheid.
integriteit en betrouwbaarheid Handelen volgens geldende normen en afspraken, ook zonder toezicht, en transparant zijn over eigen belangen, gemaakte fouten en twijfelgevallen.	Houdt zich aan gemaakte afspraken en gedragsregels en meldt een eigen fout bij de leidinggevende.	Meldt uit eigen beweging een mogelijke belangenverstrengeling en vraagt om toetsing voordat er een besluit wordt genomen.	Stelt de integriteitsnormen van de organisatie vast, handhaaft die ook bij invloedrijke betrokkenen en legt keuzes in het openbaar uit.

Skill	N1	N3	N5
Discipline en afspraken nakomen Houdt zich aan gemaakte afspraken, procedures en toezeggingen, ook zonder controle, en meldt tijdig wanneer een afspraak niet haalbaar blijkt.	Komt op de afgesproken tijd met het afgesproken werk en meldt vertraging bij de begeleider.	Zegt alleen toe wat haalbaar is, houdt de eigen toezeggingen bij en informeert betrokkenen zodra een datum onder druk staat.	Legt de norm voor betrouwbaar nakomen vast in werkafspraken en spreekt op elk niveau aan wie die norm structureel laat lopen.
Informatiebeveiliging in het werkproces Past beveiligingsmaatregelen toe in dagelijkse werkzaamheden zoals veilig delen, classificeren en opslaan van informatie en signaleert risicovolle werkwijzen.	Volgt de beveiligingsregels voor delen en opslaan van informatie en meldt een vermoedelijk incident direct.	Weegt bij nieuwe werkafspraken de beveiligingsrisico's mee, past maatregelen aan en spreekt collega's aan op onveilig gedrag.	Stelt het beveiligingsbeleid voor informatie vast en bewaakt organisatiebreed dat processen aan de gestelde eisen voldoen.
Cloudplatformen benutten Zet diensten in een cloudomgeving op en beheert die, richt rechten en kosten in en kiest tussen beschikbare dienstvormen op basis van eisen.	Gebruikt bestaande clouddiensten volgens werkinstructie en meldt afwijkend gedrag of onverwachte kosten aan de beheerder.	Richt zelfstandig clouddiensten in voor een toepassing, regelt rechten en back ups en houdt kosten en verbruik in beeld.	Bepaalt de cloudstrategie van de organisatie en beslist welke werklasten waar worden ondergebracht.
Informatiebeveiligingsbewustzijn Kent de meest voorkomende dreigingen zoals phishing, gijzelsoftware en misleiding, herkent signalen ervan en weet welke handeling dan verwacht wordt.	Herkent een duidelijk phishingbericht, klikt niet en meldt het bericht via het aangewezen kanaal.	Legt collega's uit hoe dreigingen werken, beoordeelt twijfelgevallen zelf en past het eigen gedrag aan nieuwe dreigingen aan.	Ontwerpt het bewustzijnsprogramma van de organisatie, meet het effect en stuurt de aanpak bij op basis van meetresultaten.
Leren van fouten en incidenten Onderzoekt na een fout of incident wat er is gebeurd, benoemt de oorzaak zonder de schuld te verplaatsen en verandert de werkwijze op dat punt.	Meldt een eigen fout direct bij de begeleider en herhaalt de taak volgens de gecorrigeerde instructie.	Analyseert eigen fouten en die van het team, bespreekt de oorzaak open in het werkoverleg en past afspraken aan.	Zorgt dat incidenten organisatiebreed veilig gemeld worden, laat oorzaken structureel uitzoeken en verwerkt de lessen in beleid en standaarden.
Professioneel bijblijven en vakliteratuur Volgt ontwikkelingen in het eigen vak via literatuur, richtlijnen en netwerken en verwerkt relevante nieuwe inzichten in de eigen werkwijze.	Leest de toegestuurde vakinformatie en benoemt welk onderdeel voor het eigen werk van belang is.	Houdt structureel bronnen en richtlijnen bij, weegt de kwaliteit ervan en past de eigen werkwijze aan nieuwe inzichten aan.	Beoordeelt de stand van het vakgebied, weegt tegenstrijdig onderzoek en bepaalt welke richtlijnen de organisatie voortaan volgt.
Technische documentatie schrijven Schrijft handleidingen, beheerdocumentatie en beslisverantwoording die een lezer zonder voorkennis stap voor stap kan volgen en die actueel blijft.	Vult een documentatiesjabloon aan met de stappen van een taak en laat de tekst controleren door een collega.	Schrijft complete documentatie voor een systeem of proces, test die met een onbekende lezer en houdt versies bij.	Stelt de documentatiestandaard van de organisatie vast en zorgt dat documentatie onderdeel is van elke oplevering.
Systeembeheer en monitoring Houdt systemen werkend door instellingen, updates en rechten te beheren, richt bewaking in en handelt op signalen voordat gebruikers hinder ondervinden.	Voert geplande beheertaken en updates uit volgens draaiboek en meldt afwijkingen in de bewakingssignalen.	Beheert een systeemomgeving zelfstandig, stelt bewakingsdrempels in en verbetert terugkerende oorzaken van verstoringen.	Bepaalt de beheer en bewakingsstandaarden van de organisatie en beslist over de inrichting van de systeemomgeving.

Skill	N1	N3	N5
Releasebeheer en deployment Plant en voert het uitrollen van nieuwe versies uit, controleert vooraf en achteraf op werking en zorgt dat terugdraaien mogelijk blijft.	Voert de stappen van een uitrolplan uit en meldt direct wanneer een stap niet het verwachte resultaat geeft.	Stelt zelf een uitrolplan met terugvaloptie op, stemt af met betrokkenen en controleert na uitrol of de dienst goed werkt.	Bepaalt het releasebeleid van de organisatie, beslist over uitrolvensters en verbetert de doorlooptijd van wijzigingen structureel.
Procesautomatisering Analyseert een terugkerend werkproces, bouwt of laat bouwen dat stappen automatisch verlopen en controleert of de uitkomst betrouwbaar blijft.	Voert een bestaande automatisering uit en meldt wanneer de uitkomst afwijkt van wat verwacht werd.	Beschrijft een proces in stappen, automatiseert de herhaalbare stappen en bouwt controles in op fouten en uitzonderingen.	Bepaalt de automatiseringsagenda van de organisatie en beslist welke processen wel en niet worden geautomatiseerd.
Calamiteiten- en crisisorganisatie Werkt volgens crisisplannen bij incidenten, vervult een rol in de crisisorganisatie en zorgt voor beeldvorming, besluitvorming en verslaglegging.	Kent de eigen rol in het calamiteitenplan en voert bij een oefening de opgedragen taken volgens instructie uit.	Vervult zelfstandig een rol in een crisisteam, houdt het beeld actueel en zorgt dat besluiten worden vastgelegd.	Ontwerpt de crisisorganisatie en de opleidings- en oefencyclus en leidt de evaluatie na een echte calamiteit.
Servicegesprekken en telefonie Klantcontacten via telefoon en chat afhandelen met een vaste opbouw, een gecontroleerde uitvraag en een afsluiting met een concrete afspraak.	Meldt zich volgens het script, registreert de vraag in het systeem en verbindt door naar de juiste collega.	Handelt afwijkende vragen in één gesprek af, houdt de gesprekstijd in de hand en vat de afspraak hoorbaar samen.	Ontwerpt gespreksmodellen en kwaliteitsnormen voor het klantcontactcentrum en beoordeelt opnames om coaching en systeemkeuzes te onderbouwen.
Dataclassificatie en bewaartermijnen Rubriceert informatie naar gevoeligheid en belang, koppelt daaraan bewaartermijnen en zorgt dat verwijdering en archivering daadwerkelijk plaatsvinden.	Kent een classificatielabel toe volgens het schema en legt onduidelijke gevallen voor aan de beheerder.	Stelt voor een informatiestroom de classificatie en bewaartermijn vast en controleert of opschoning volgens plan gebeurt.	Ontwerpt het classificatie en bewaarbeleid van de organisatie en verantwoordt dit bij audits en toezicht.

6 Meetmethoden en validiteit

De validiteiten zijn de gecorrigeerde meta-analytische schattingen van Sackett, Zhang, Berry en Lievens (2022) in het Journal of Applied Psychology. Die vervangen de oudere cijfers van Schmidt en Hunter (1998). De spreiding is even belangrijk als het gemiddelde: bij een hoge SD varieert de validiteit sterk per context.

Meetmethode	rho	SD	Wat het is
Simulatie	-	-	Nagebootste werksituatie, meestal digitaal, met gestandaardiseerde scoring.
Assessment center	**0.29**	**0.09**	Meerdere oefeningen, meerdere beoordelaars, dimensiegewijze scoring.
Werkproef	**0.33**	**0.09**	De kandidaat voert een representatief werkfragment uit onder gestandaardiseerde condities.
Persoonlijkheidsvragenlijst	**0.40**	**0.15**	Zelfrapportage van gedragsvoorkeuren. Bij hrmforce de Big Fifty en de 15PF.
Kennistoets	**0.40**	**0.13**	Toets van declaratieve vakkennis, meestal klantspecifiek samengesteld.
Situational Judgement Test	**0.12**	**0.11**	Scenario met responsopties, gescoord op kennis of op gedragstendens.
Portfolio/bewijsstuk	-	-	Verzameling van eerder werk of resultaten, beoordeeld tegen vaste criteria.

7 Meetinstrumenten voor deze functie

hrmforce instrument	Skills	Wat het meet
Werkproef	**14**	Representatief werkfragment onder gestandaardiseerde condities
Kennistoets (klantspecifiek)	**12**	Toets van vakkennis, per klant samengesteld
Competency Check	**5**	Competentiebeoordeling op gedragsniveau
360 Feedback	**4**	Meervoudige beoordeling op gedragsankers
Big Fifty	**3**	Persoonlijkheidsvragenlijst, 150 items, 25 factoren
Portfolio	**3**	Beoordeling van eerder werk tegen vaste criteria
Ability Scan	**2**	Capaciteitentest: verbaal, numeriek en abstract redeneervermogen
15PF	**2**	Persoonlijkheidsprofiel, korter alternatief voor de Big Fifty
Mentale Weerbaarheid (4C)	**1**	Mentale weerbaarheid volgens het 4C-model
Big Fifty (schaal Integriteit)	**1**	
Structureerd interview	**1**	Gedragsgericht interview met vaste opzet
Communicatiestijlen	**1**	Voorkeursstijl in communicatie

8 Hoe je dit profiel gebruikt

1. Stel het profiel vast met de leidinggevende voordat de eerste kandidaat wordt gemeten. Gewichten die je achteraf verschuift, maken de uitkomst onverdedigbaar.

2. Kies per skill de meetmethode uit kolom Meetmethode. Combineer maximaal drie methoden per kandidaat.
3. Kalibreer de beoordelaars in een sessie van twee uur met de gedragsankers uit hoofdstuk 5. Ankers zonder beoordelaarstraining leveren weinig op.
4. Vul de matchcalculator en bespreek de gaps in het ontwikkelgesprek. Type A en type G zijn selectiecriteria, geen ontwikkeldoelen van een kwartaal.

Bron: hrmforce Skills Framework 2.0, versie 2.0.0, gebouwd op 2026-09-08. Crosswalks naar ESCO v1.2.1, O*NET 31.0, Lightcast Open Skills, SFIA 9, DigComp 3.0, EntreComp, LifeComp, GreenComp, AILit, WEF Future of Jobs 2025, ISCO-08 en de Beroepenindeling ROA-CBS 2014 editie 2025. Dit profiel is een startpunt, geen norm: stem het af op de eigen organisatie voordat je ermee selecteert.