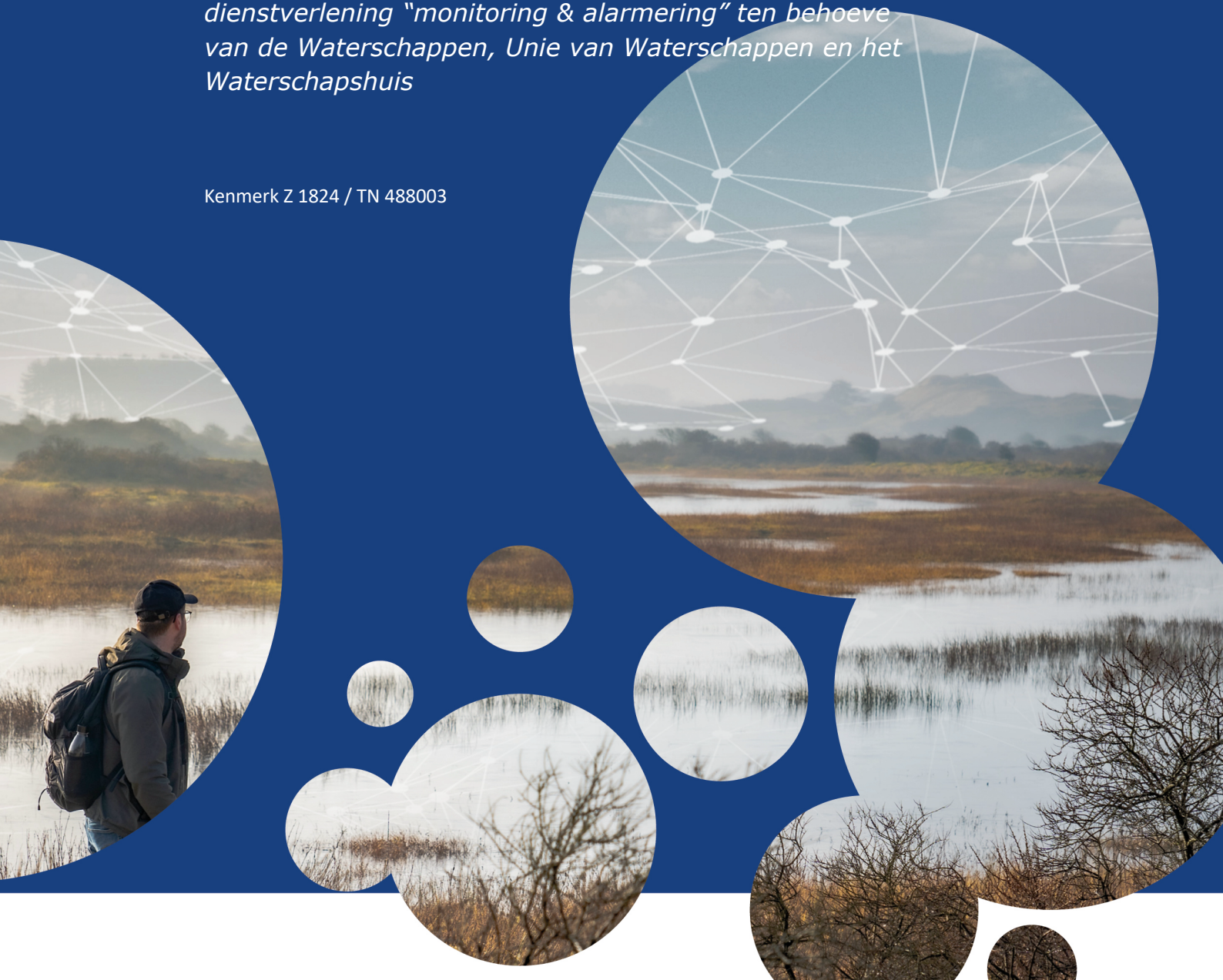
hetWaterschapshuis

De kracht van samen

Aanbestedings leidraad

Europese openbare procedure voor heraanbesteding SOC-dienstverlening "monitoring & alarmering" ten behoeve van de Waterschappen, Unie van Waterschappen en het Waterschapshuis

Kenmerk Z 1824 / TN 488003



Inhoud

INHOUD **2**

WOORD VOORAF **4**

1. OVER ONS, AANGENAAM **5**

1.1 Over het Waterschapshuis **5**

1.3 Opdrachtgever **5**

1.4 Deelnemers aan de aanbesteding **5**

1.5 Positie CERT-WM (Watermanagement) **7**

1.6 Afkortingen en terminologie **7**

1.7 Verkorte procedure **8**

2. WAAR ZIJN WE NAAR OP ZOEK? **10**

2.1. Context en scope **10**

2.2. Herzieningsclausule **11**

2.3. Buiten scope **12**

2.4. Contract **12**

3. HOE **13**

3.1. Aanbestedingsprocedure **13**

3.2. Aanbestedingsvoorwaarden **13**

3.3. Klagen mag **13**

4. HEEFT U INTERESSE? **14**

4.1. Nota van inlichtingen **14**

4.1.1 Voorbehouden, alternatieven, verbeteringen 14

4.2. Planning **14**

4.3. Uitsluitingsgronden 14

4.4 Geschiktheidseisen 15
4.4.1 Beroepsbevoegdheid 15
4.4.2 Technische en beroepsbekwaamheid 15
4.4.3 Kwaliteitsborging 18

4.5. Uw Inschrijving 21

4.6. Bewijsstukken 21

4.7. Standstill termijn 21

5. HOE BEPALEN WE DE WINNAAR? 22

5.1. Beoordelingscommissie 22

6. GUNNINGSCRITERIA 25

6.1 Prijs 26

6.2 Kwaliteit 28

6.3 Toelichting offerte door drie functionarissen 31

BEGRIPSBEPALINGEN M.B.T. PROCEDURE 32

BEGRIPSBEPALINGEN M.B.T. DIENSTVERLENING 34

BIJLAGEN EN FORMULIEREN: 39

Formulieren: 39

Woord vooraf

Deze aanbestedingsleidraad met bijlagen heeft betrekking op de heraanbesteding van de aanbesteding SOC-dienstverlening "monitoring en alarmering" met TenderNed kenmerk: TN 477772, die evenals als de eerdere aanbesteding met TenderNed kenmerk TN462385, heeft geresulteerd in ongeldige inschrijvingen.

Het Waterschapshuis heeft ernaar gestreefd in deze nieuwe aanbesteding zoveel mogelijk gebruik te maken van en aan te sluiten bij de documenten van de voorafgaande aanbesteding. Om de verschillen snel te kunnen herkennen, zijn toevoegde teksten in blauwe tekst weergegeven en zijn verwijderde teksten in ~~rood doorgestreepte tekst~~ weergegeven.

De aanbesteding zal middels verkorte termijnen worden doorlopen. De motivering voor die verkorte termijnen is in paragraaf 1.7 uitgewerkt.

EG

1. Over ons, aangenaam

1.1 Over het Waterschapshuis

Het Waterschapshuis is een gemeenschappelijke regeling van de 21 Waterschappen in Nederland (Scr. 2015, 7407 d.d. 13-03-2015). Doel van de regeling is een expertinstituut en service organisatie voor Waterschappen in het leven te roepen om voor de deelnemende Waterschappen en eventuele derden een renderende samenwerking op informatie- en bedrijfsprocessen te realiseren en daarmee de behoeften van algemeen belang van de watersector te behartigen. Het Waterschapshuis (hWh) is de regie-, beheer-, en uitvoeringsorganisatie op het gebied van digitale informatievoorziening van de Waterschappen. Het is een dienstverlenende organisatie van en voor de Waterschappen die verantwoordelijk is voor de aanschaf en het contractmanagement van (gezamenlijke) informatievoorzieningen en data. Het Waterschapshuis is van én voor alle Waterschappen samen.

Voor meer informatie zie https://www.hetWaterschapshuis.nl/.

1.3 Opdrachtgever

Het Waterschapshuis, tevens aanbestedende dienst, treedt op als formele Opdrachtgever en penvoerder namens de andere aanbestedende diensten. Aanbestedende diensten worden in deze aanbesteding gezamenlijk Deelnemers genoemd. Het Waterschapshuis wordt gemakshalve in deze aanbesteding als Opdrachtgever genoemd, waarbij Het Waterschapshuis ook een Deelnemer is. De Opdrachtgever sluit voor de SOC-dienstverlening ten behoeve van de Deelnemers een Hoofdovereenkomst (Bijlage D) af. De Deelnemers zullen binnen de kaders van deze Hoofdovereenkomst individueel een Deelnameovereenkomst (Bijlage J) afsluiten voor de te leveren diensten. Tijdens de looptijd van de Hoofdovereenkomst zal Het Waterschaphuis contractbeheer en Service Level Management uitvoeren voor alle Deelnemers.

1.4 Deelnemers aan de aanbesteding

Aan deze aanbesteding nemen de volgende (in tabel 1.4.1. genoemde) organisaties deel. Deze organisaties hebben Opdrachtgever gemachtigd namens hen onderhavige aanbesteding uit te voeren.

- Waterschappen
    1. Waterschap Aa en Maas
    2. Waterschap Amstel, Gooi en Vecht (incl. Waternet)
    3. Waterschap Brabantse Delta
    4. Hoogheemraadschap van Delfland
    5. Waterschap De Dommel
    6. Hoogheemraadschap de Stichtse Rijnlanden
    7. Hoogheemraadschap Schieland en de Krimpenerwaard
    8. Hoogheemraadschap van Rijnland
    9. Waterschap Hunze en Aa's
    10. Waterschap Limburg (incl. Waterschapsbedrijf Limburg)
    11. Waterschap Noorderzijlvest
    12. Waterschap Rijn en IJssel
    13. Waterschap Scheldestromen
    14. Waterschap Vallei en Veluwe
    15. Waterschap Drents Overijsselse Delta
    16. Wetterskip Fryslân

17. Waterschap Hollandse Delta 18. Waterschap Zuiderzeeland • Overige organisaties 19. Het Waterschapshuis 20. Unie van Waterschappen

Tabel 1.4.1. Lijst met initiële Deelnemers.

Bij deze initiële Deelnemers leeft een breed gedragen commitment ten aanzien van deze aanbesteding, in die zin dat zij hebben aangegeven SOC-dienstverlening af te willen nemen onder de gegunde Hoofdovereenkomst. Echter elke Deelnemer aan deze aanbesteding is vrij om deel te nemen en bepaalt zijn eigen instapmoment. De instapmomenten worden mede bepaald door nog lopende overeenkomsten. Deze initiële Deelnemers hebben de ambitie om in de hierna in tabel 1.4.2. genoemde tijdvakken te gaan deelnemen. Aan deze tabel kunnen geen rechten worden ontleend.

contractjaar	**1**	**2**	**3**	**4**
1e kwartaal	- Brabantse Delta - Hollandse Delta - Wetterskip Fryslân - Aa en Maas	- Hunze & Aa's - Limburg - Noorderzijlvest - Stichtse Rijnlanden	- Waternet	
2e kwartaal	- De Dommel - het Waterschapshuis	- Scheldestromen - Rijnland - Schieland en de Krimpener-waard - Delfland	- Vallei en Veluwe	
3e kwartaal	- Drents Overijsselse Delta	- Unie van Waterschappen		
4e kwartaal		- Zuiderzeeland - Rijn en IJssel		

Tabel 1.4.2. Beoogde tijdvakken van instappen door initiële Deelnemers.

Mogelijk toekomstige Deelnemers

Drie Waterschappen (zie tabel 1.4.3) behoren niet tot de initiële Deelnemers. Mogelijk wensen zij op een later tijdstip alsnog deel te nemen.

Gezien de ketenafhankelijkheden met o.a. andere Gemeenschappelijke Regelingen (zoals belastingsamenwerkingen en laboratoria; zie tabel 1.4.3), kunnen op enig moment mogelijk ook één of meer van de volgende (in tabel 1.4.3. genoemde) partijen toetreden (als nieuwe Deelnemer) tot de gezamenlijke SOC-dienstverlening:

Hoogheemraadschap Hollands Noorderkwartier	
Waterschap Vechtstromen	
Waterschap Rivierenland	
STOWA	https://www.stowa.nl/
Aquaminerals B.V.	https://aquaminerals.com/
Slibverwerking Noord-Brabant	https://www.snb.nl/
HVC-groep	https://www.hvcgroep.nl/
AEB Amsterdam	https://www.aebamsterdam.nl/
Belastingsamenwerking Gouwe Rijnland (BSGR)	https://www.bsgr.nl/
De Regionale Belastinggroep (De RBG)	https://www.derbg.nl/

Samenwerkingsverband Vastgoedinformatie Heffing en Waardebepaling (SVHW)	https://www.svhw.nl/
Belastingsamenwerking gemeenten en hoogheemraadschap Utrecht (BGHU)	https://bghu.nl/
Belastingsamenwerking West Brabant (BWB)	https://www.bwbrabant.nl/
Sabewa	https://www.sabewazeeland.nl/
Belastingsamenwerking Oost Brabant (BSOB)	https://www.bs-ob.nl/
Gemeenschappelijk Belastingkantoor Lococensus-Tricijn (GBLT)	https://gblt.nl/
Noordelijk Belastingkantoor (NBK)	https://noordelijkbelastingkantoor.nl/
Belastingsamenwerking Gemeenten en Waterschappen (BsGW)	https://www.bsgw.nl/
Aquon	https://www.aquon.nl/
Aqualysis	https://www.aqualysis.nl/

Tabel 1.4.3. Lijst met mogelijke toekomstige Deelnemers.

Wijze van instappen van Deelnemers

Om Deelnemer bij de Hoofdovereenkomst te worden stuurt elk Waterschap (en overige Deelnemers in tabel 1.4.1. en 1.4.3. een Verklaring van Deelname (Bijlage K) aan Opdrachtnemer en het Waterschapshuis. In de Verklaring van Deelname staat de aanvangsdatum van deelname aan de Hoofdovereenkomst. Nadat de Opdrachtnemer in kennis is gesteld van de deelname is de Deelnemer vanaf de in de Verklaring van Deelname genoemde ingangsdatum Partij bij de Hoofdovereenkomst en heeft de Hoofdovereenkomst rechtstreekse werking tussen Deelnemer en Opdrachtnemer. Deelnemer en Opdrachtnemer leggen uiterlijk binnen een maand na de Verklaring van Deelname de specifieke afspraken tussen Deelnemer en Opdrachtnemer vast in de Deelnameovereenkomst.
Opdrachtgever is het primaire interne en externe aanspreekpunt als het gaat om het gebruik en de uitleg van de Hoofdovereenkomst “SOC dienstverlening Monitoring & Alarmering”. Opdrachtgever voert namens de Deelnemers de centrale regie met betrekking tot het leveranciers-en contractmanagement.

1.5 Positie CERT-WM (Watermanagement)

De coördinatie van het CERT-WM (Watermanagement) wordt gedaan vanuit het Waterschapshuis, waar het CERT-WM valt onder het programma Informatiebeveiliging en Privacy. De medewerkers van het CERT-WM worden gedetacheerd vanuit de Waterschappen en zijn gestationeerd bij het Security Operations Centre van Rijkswaterstaat (SOC RWS) in Delft. Deze samenwerking met het SOC RWS bevordert de uitwisseling van kennis en versterkt de positie van het CERT-WM.

Het CERT-WM is 1 van de 4 aangewezen CERT’s door het ministerie van JenV. Met de komst van NIS2 gaat het CERT-WM doorontwikkelen naar een sectorale CSIRT/CERT binnen het ministerie van IenW. Het CERT-WM ondersteunt de Deelnemers bij preventie, detectie, coördinatie en fungeert als Computer Emergency Response Team op het gebied van kantoorautomatisering (hierna KA te noemen) en industriële automatisering, OT/Proces Automatisering/ICS/SCADA hierna PA te noemen, voor de aangesloten Deelnemers.

1.6 Afkortingen en terminologie

In dit document en aanbestedingsstukken worden begrippen met betrekking tot de dienstverlening gehanteerd. Aan deze begrippen komt de in het onderdeel "Begripsbepaling m.b.t. dienstverlening" (na hoofdstuk 6) genoemde betekenis toe.

1.7 Verkorte procedure

Waterschappen zijn kritieke entiteiten in de zin van de Europese Critical Entities Resilience (CER) richtlijn en essentiële entiteiten in de zin van de Europese Network Information Security (NIS2) richtlijn. Daarnaast zijn de waterschappen door de Nederlandse regering onder de noemer "vitale aanbieders" aangemerkt als beheerders van te beschermen vitale processen en vitale infrastructuur voor het proces Keren en beheren van waterkwantiteit. Onder andere vanuit de NIS2 blijkt dat de sector een aantrekkelijk doelwit voor cybercriminelen is. Dit wordt ook bevestigd door de AIVD in haar jaarverslag 2023. Daarin stelt de dienst in het hoofdstuk Cyberdreigingen het volgende: “De AIVD zag in 2023 wereldwijd verschillende buitenlandse cyberoperaties die waarschijnlijk sabotage als doel hadden.” En: “De operaties werden uitgevoerd door of in opdracht van statelijke actoren en waren specifiek gericht op de vitale infrastructuur in andere landen. Het doel was waarschijnlijk niet om meteen de communicatie te verstoren of het energienetwerk platleggen, maar om de mogelijkheid in te bouwen om dat later te kunnen doen. Bijvoorbeeld bij een conflict.”

Dat de sector gevoelig is voor cyberincidenten is al gebleken sinds 2020. In januari van dat jaar maakte softwarebedrijf Citrix bekend dat er een ernstige kwetsbaarheid was ontdekt. Daardoor konden buitenstaanders op het interne netwerk van verschillende organisaties komen. Als voorzorgsmaatregel werden een aantal systemen van de waterschappen tijdelijk uitgeschakeld. In 2021 werden bij Waterschap Amstel, Gooi en Vecht (Waternet) de persoonsgegevens van 48.000 bezoekers van de Amsterdamse Waterleidingduinen gestolen door hackers. Recent, in 2024, is het Hoogheemraadschap Hollands Noorderkwartier indirect door de cyberaanval getroffen door een Ransomeware-aanval. Door fysieke ketenafhankelijkheden kan een cyber veiligheidsincident bij één waterschap gevolgen hebben voor de hele waterschapsector.

Eén van de mitigerende maatregelen die de waterschappen sectorbreed willen inzetten tegen de cyberdreigingen, is het via een Security Operations Center (SOC) continu monitoren op, -en detecteren van- deze dreigingen in hun OT- & IT-domeinen. Dit zorgt voor structurele bewaking van kritische beheerprocessen en data.

Het doel van een gezamenlijke SOC-dienstverlening is om detectie van digitale dreigingen en/of afwijkend gedrag en de response hierop toekomstbestendig in te richten en de cyberweerbaarheid van de hele waterschapssector integraal te vergroten.

In april 2024 is hWh daartoe een Openbare Europese aanbestedingsprocedure (TenderNed kenmerk: TN 462385) gestart. Helaas heeft deze geleid tot enkel ongeldige inschrijvingen. Zo spoedig mogelijk is in juli 2024 een tweede Openbare Europese aanbestedingsprocedure gestart (TenderNed kenmerk: TN 477772), maar ook deze heeft tot ongeldige inschrijvingen geleid.

Hierdoor neemt de urgentie toe om een opdrachtnemer te contracteren, mede gelet op de eerdergenoemde cyberincidenten. Verdere vertraging kan ertoe leiden dat waterschappen zich alsnog gedwongen zien zelf hun SOC-diensten in te kopen, waardoor de sectorbrede kennis van cyberdreigingen en daarmee de sectorbrede cyberweerbaarheid afneemt. Dit is niet in het belang van de waterschappen en de waterschapssector als geheel.

In deze aanbesteding wordt daarom gebruik gemaakt van verkorte termijnen in de zin van artikel 2.74 Aanbestedingswet 2012. In beide voorafgaande aanbestedingen is er sprake geweest van ongeldigheid van de inschrijvingen met betrekking tot de geschiktheidseisen.

De ongeldigheid met betrekking tot de geschiktheidseisen heeft hWh niet kunnen voorkomen. Om redelijke geschiktheidseisen bij die eerdere aanbestedingen te kunnen vaststellen heeft hWh meerdere stappen doorlopen.

Allereerst is in 2023 een marktoriëntatie uitgevoerd. Daarin is een eerste analyse gemaakt van de essentiële ervaring, werkwijze, organisatorische structuur en bedrijfsprocessen die vereist zijn voor SOC-dienstverlening, gebaseerd op een brede en representatieve groep van mogelijk gegadigde

bedrijven. De marktoriëntatie is opgevolgd door een marktconsultatie (TenderNed kenmerk: TN 447227, d.d. 11 januari 2024) en een bijeenkomst met geïnteresseerden in februari 2024.

Na de eerste aanbesteding zijn de geschiktheidseisen met de inschrijvers geëvalueerd. Daarbij is niet aangegeven en is ook niet gebleken dat de geschiktheidseisen niet passend zouden zijn of dat inschrijvers niet aan de geschiktheidseisen konden voldoen. Wel zijn naar aanleiding van de evaluatie een aantal nuanceringen en verduidelijkingen in de geschiktheidseisen doorgevoerd.

Het is dan ook verrassend en tegen alle verwachtingen in dat bij de heraanbesteding wederom bij alle inschrijvers onregelmatigheden zijn vastgesteld met betrekking tot de geschiktheidseisen.

Inmiddels zijn sinds de aanvang van de eerste aanbesteding bijna zes maanden verstreken. Volgens de oorspronkelijke planning zou de dienstverlening vanaf medio september bij het eerste waterschap geïmplementeerd worden en vervolgens verder uitgerold worden. Met verkorte termijnen kan de vertraging beperkt blijven tot minder dan drie maanden.

2. Waar zijn we naar op zoek?

2.1. Context en scope

De Nederlandse Waterschappen hebben geconstateerd dat de digitale weerbaarheid vergroot dient te worden en dat daarvoor op individueel Waterschapniveau veelal de noodzakelijke kennis en personele capaciteit ontbreekt.

Eén van de mitigerende maatregelen die hWh wil inzetten tegen de cyberdreigingen, is het continu monitoren op, -en detecteren van- deze dreigingen in haar OT- & IT-domeinen. Dit zorgt voor structurele bewaking van kritische beheerprocessen en data.

hWh is voornemens om voor het monitoren en detecteren van deze dreigingen gezamenlijke Security Operations Center (SOC) dienstverlening "Monitoring & Alarmering" te realiseren. Deze gezamenlijke SOC-dienstverlening heeft als doel om detectie van digitale dreigingen en/of afwijkend gedrag, en de response hierop toekomstbestendig in te richten zodat de Deelnemers hiermee hun cyberweerbaarheid vergroten, voor nu en de komende jaren.

hWh wil de SOC-dienstverlening beleggen bij een externe partij, omdat hWh de specialistische kennis die in de markt aanwezig is, goed wil benutten.

De gevraagde SOC-dienstverlening omvat:

- Monitoring – Het vinden en analyseren van mogelijke cyberbeveiligingskwetsbaarheden, -aanvallen en -incidenten (cf. "Detect" uit het NIST Cybersecurity Framework 2.0[1]);
- Alarmering - Actie ondernemen met betrekking tot een gedetecteerd cyberbeveiligingskwetsbaarheid en -incident (cf "Respond" uit het NIST Cybersecurity Framework 2.0);
- Beheer en doorontwikkeling van voor de watersector relevante security use cases die voorzien zijn van een detectiemechanisme die de monitoring inhoud geven.

Daarnaast dient Opdrachtnemer te zorgen voor:

- Implementatie van de dienstverlening bij Deelnemers. De omvang van de implementatiewerkzaamheden varieert en is afhankelijk van de uitgangssituatie (kennis, inrichting en beschikbare capaciteit van de individuele Deelnemer.
- Opleiding en training van (interne) medewerkers van Deelnemers voor het effectief gebruik van de opgeleverde oplossingen.

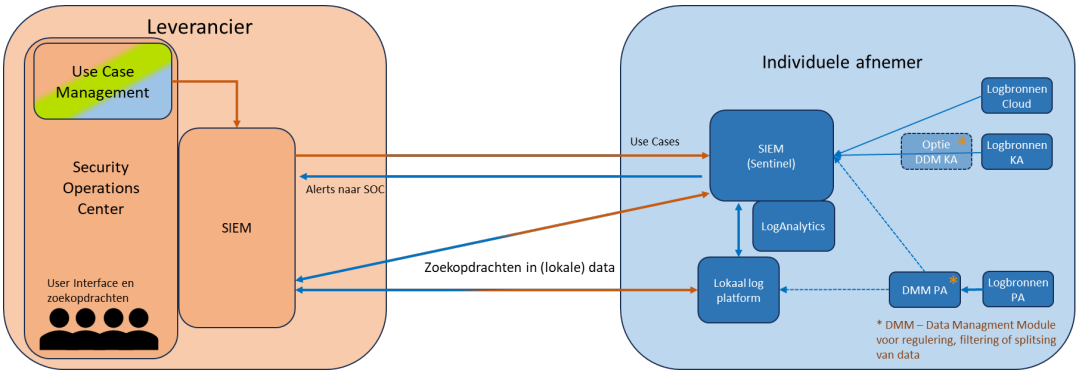
De eisen die aan de uitvoering van de opdracht worden gesteld, zijn nader uitgewerkt in Bijlage H, Programma van Eisen (met bijlagen).

De SOC-diensten dienen te worden uitgevoerd vanuit een "converged OT & IT SOC" (zie "Begripsbepalingen m.b.t. dienstverlening", aan het einde van deze leidraad).

In deze oplossing is in beginsel iedere individuele Deelnemer zelf verantwoordelijk voor het collecteren van de logdata die noodzakelijk zijn voor security monitoring. Deze data worden binnen de omgeving van de Deelnemer opgeslagen en zijn beschikbaar voor security monitoring. De PA-logdata zal voor security monitoring (bijna) real-time beschikbaar worden gesteld in de KA-omgeving van de Deelnemer. Er zijn echter Deelnemers die deze lokale opslag niet zelf kunnen regelen en de data naar een centraal aangeboden oplossing willen sturen. Bij die Deelnemers wordt de centrale opslag van de logdata tegen meerprijs, t.o.v. de oplossing met de eigen opslag van de logdata, verrekend.

[1] https://csrc.nist.gov/Projects/cybersecurity-framework/Filters#/csf/filters

Onderstaande figuur geeft schematisch de oplossing weer. Het blauwe vlak schetst de inrichting bij de individuele Deelnemers. Opgemerkt zij dat de individuele Deelnemer bepaalt of PA-data al dan niet in Sentinel wordt verwerkt. Opdrachtnemer dient zijn dienstverlening in te richten conform die keuze van de betreffende Deelnemer.



Figuur 2.1.1. Schematische weergave oplossing.

Van belang is dat Opdrachtnemer effectief en efficiënt (al dan niet lokale) logdata analyseert, waarbij onderscheid wordt gemaakt tussen de verschillende soorten data, waarbij op basis van een adequate risico-inventarisatie voor de verschillende soorten data wordt bepaald in welke mate zij dienen te worden gemonitord en geanalyseerd.

Alle 20 Deelnemers beschikken over een Microsoft E5 licentie en maken gebruik van de binnen deze licentie vallende Microsoftproducten. De werkstations zijn nagenoeg allemaal Windows gebaseerd. Een groeiend aantal Deelnemers heeft, in de Azure Cloud, Sentinel als SIEM geactiveerd. Er zijn ook Deelnemers die gebruik maken van een ander merk lokaal SIEM. De roadmap binnen de 20 Deelnemers geeft aan dat de producten uit de Microsoft E5 licentie in een steeds toenemende mate worden ingezet.

Om als Deelnemers op het gebied van informatiebeveiliging toekomstbestendig te zijn, dient de Opdrachtnemer zichzelf en zijn diensten proactief mee te ontwikkelen met de ontwikkelingen in de markt (zowel technisch als op basis van dreigingsbeelden). Opdrachtnemer dient de dienstverlening dynamisch en flexibel af te stemmen op deze ontwikkelingen in de markt en dient eveneens de dienstverlening flexibel en dynamisch af te stemmen op ontwikkelingen bij elke individuele Deelnemer. Er moet sprake zijn van een partnerschap waarin Opdrachtgever, de Deelnemers en de Opdrachtnemer gezamenlijk de digitale weerbaarheid blijven verhogen en de dienstverlening om dit te realiseren doorontwikkelen.

2.2. Herzieningsclausule

Opdrachtgever en/of individuele Deelnemers kunnen de dienstverlening uitbreiden met de volgende diensten:

- Uitbreiding van de SOC-dienstverlening:

    - Security Analysis;
    - Threat Hunting;
    - Threat Intelligence;
    - Vulnerability Management.
- Security adviesdiensten:
    - In de brede zin, ondersteuning en advisering bij informatiebeveiliging vraagstukken op zowel het OT als IT-landschap, waaronder:
        - Adviseren bij het opstellen en onderhouden van design en security architecturen;
        - Adviseren bij de inrichting of optimalisatie van securityprocessen en/of nieuwe security technologieën/ diensten;
        - Adviseren bij de (Europese) aanbesteding van specifieke security percelen.
- Awareness trainingen:
    - Het uitvoeren van periodieke phishing simulatieoefeningen op personeel van Deelnemers en Opdrachtgever inclusief het trainen van medewerkers om phishing emails te detecteren. In een later stadium kunnen hier algemene security awareness diensten aan toegevoegd kunnen worden zoals social engineering oefeningen, mystery man oefeningen enzovoorts.

2.3. Buiten scope

Buiten de scope van deze aanbesteding valt (onder meer, maar niet uitsluitend):

- Govern cf. NIST Cybersecurity Framework 2.0[2];
- Identify cf. NIST Cybersecurity Framework 2.0;
- Protect cf. NIST Cybersecurity Framework 2.0;
- Recover cf. NIST Cybersecurity Framework 2.0;
- Algemene ICT-adviesdiensten, hiervoor bestaan separate (raam)overeenkomsten.

2.4. Contract

Er is sprake van een Hoofdovereenkomst met een initiële looptijd van vier jaren. Na het verstrijken van deze periode heeft Opdrachtgever de mogelijkheid de Hoofdovereenkomst viermaal tegen dezelfde voorwaarden te verlengen voor een periode van telkens 24 maanden. De beoogde ingangsdatum van de Hoofdovereenkomst is 02-01-2025.

De dienstverlening dient binnen drie maanden nadat een Deelnemer Opdrachtnemer in kennis heeft gesteld van een verklaring van Deelname, operationeel te zijn bij Deelnemer.

Indien de implementatie van de dienstverlening aan de eerste 4 Deelnemers niet telkens binnen drie maanden nadat Opdrachtnemer in kennis is gesteld van de Verklaring van Deelname, niet is geaccepteerd, is Opdrachtnemer direct in verzuim (zonder dat een ingebrekestelling is vereist) en is Opdrachtgever en elke respectievelijke Deelnemer bevoegd de Hoofdovereenkomst en Deelnameovereenkomst met onmiddellijke ingang te beëindigen.

[2] https://csrc.nist.gov/Projects/cybersecurity-framework/Filters#/csf/filters

3. Hoe

3.1. Aanbestedingsprocedure

Voor deze Opdracht volgt het Waterschapshuis (hWh) de Europese openbare aanbestedingsprocedure volgens de Aanbestedingswet 2012.

De aankondiging en de bijlagen, behorend bij deze uitnodiging, maken onlosmakelijk onderdeel van deze aanbesteding.

Motivering samenvoeging

Opdrachtgever en Deelnemers hebben behoefte aan één Opdrachtnemer die de opdracht voor hen gezamenlijk de monitoring en alarmering van security incidenten uitvoert. De OT- en IT-processen bij de verschillende Waterschappen zijn heel erg vergelijkbaar. Er is dan ook een grote samenhang tussen de SOC-diensten voor de verschillende Waterschappen. Voor een zo adequaat mogelijk converged OT-en IT-SOC voor Waterschappen en daaraan gerelateerde organisaties is van belang dat kennis van OT- en IT-incidenten zo optimaal mogelijk wordt gedeeld tussen de Deelnemers. Door met één Opdrachtnemer in zee te gaan, neemt deze Opdrachtnemer zo breed mogelijk kennis van alle mogelijke OT- en IT-incidenten, hetgeen maximaal bijdraagt aan een zo adequaat mogelijke continue ontwikkeling van (het niveau en de omvang van) de SOC-dienstverlening voor de Waterschapssector. Indien er wordt gekozen voor meerdere verschillende Opdrachtnemers, worden ervaring en kennis verdeeld over deze Opdrachtnemers opgedaan, hetgeen ten koste gaat van het totaalbeeld van dreigingen voor de hele Waterschapssector en (de ontwikkeling van) effectieve integrale sectorbrede bestrijding ervan. Gelet op de hoedanigheid van de Waterschappen als vitale sector, is niet gewenst dat kennisdeling inzake monitoring en alarmering beperkt wordt. Samenvoeging levert een substantieel betere beveiliging op tegen security incidenten en daarmee beheersing van de risico's ervan.
In de markt zijn met name bedrijven actief die kwalificeren als grootbedrijf. Voor zover een gegadigde al niet kwalificeert als grootbedrijf kwalificeert deze als middelgroot MKB. De opdracht is door de samenvoeging niet minder toegankelijk voor de middelgroot MKB-bedrijven, dan voor grootbedrijven. In de marktconsultatie is bovendien gebleken dat samenvoeging voor de Opdrachtnemer juist leidt tot een betere beheersbaarheid van risico's ten aanzien van monitoring en alarmering van security incidenten.

Het is dan ook niet passend de opdracht op te delen in percelen.

3.2. Aanbestedingsvoorwaarden

Als u inschrijft voor deze Opdracht, dan verklaart u daarmee dat u onvoorwaardelijk akkoord gaat met alle gestelde eisen en dat u de Opdracht onvoorwaardelijk kunt uitvoeren volgens de gestelde eisen.

3.3. Klagen mag

Klachten kunnen, onderbouwd, gemeld worden bij inkoop@hetWaterschapshuis.nl onder vermelding van ‘Klacht aanbesteding SOC-monitoring en alarmering”.

4. Heeft u interesse?

Deze procedure verloopt digitaal via TenderNed. Een uitbreide instructie vindt u op www.tenderned.nl. Dit houdt het volgende in:

1. Alle Aanbestedingsstukken worden via TenderNed beschikbaar gesteld;

2. Inschrijvingen kunnen alleen via TenderNed worden aangeboden;

3. Alle communicatie verloopt via TenderNed t.a.v. mevrouw T. Duinkerken en vindt plaats in de Nederlandse taal. Aan mondelinge mededelingen kunnen geen rechten worden ontleend.

4.1. Nota van inlichtingen

Voorafgaand aan het indienen van de Inschrijving is er gelegenheid om vragen te stellen over deze uitvraag en de aanbestedingsstukken. Deze vragen kunnen uitsluitend worden gesteld via de vraag- en antwoordmodule op TenderNed. Wij verzoeken u per vraagregel in TenderNed maximaal één vraag in te dienen, het is vanwege de duidelijkheid niet toegestaan om binnen één vraag in TenderNed meerdere vragen te stellen. Uw vragen mogen geen bedrijfsnamen, merken of verwijzingen daarnaar bevatten.

Het is mogelijk vragen te stellen tot de in de planning aangegeven uiterste termijn. Na de uiterste termijn wordt de Nota van inlichtingen opgesteld en gepubliceerd. Vragen die daarna zijn ontvangen, worden niet beantwoord.

De Nota van Inlichtingen maakt integraal deel uit van de Aanbestedingsdocumenten.

De Nota van inlichtingen 2024-05-24 uit de voorafgaande eerste aanbesteding (TenderNed kenmerk: TN462385) is bijgevoegd en maakt onderdeel uit van de Overeenkomst, met uitzondering van de antwoorden op de vragen 5, 14, 16, 28, 29, 38, 39, 69, 92, 96, 134 en 137. Deze vragen vervallen (en zijn doorgestreept in de Nota van Inlichtingen 2024-05-24) en ~~worden~~ voor zover relevant zijn opnieuw beantwoord in de Nota van Inlichtingen 2024-08-13-1 of worden opnieuw beantwoord.

De Nota van inlichtingen 2024-08-13-1 en de Nota van inlichtingen 2024-08-27-1 uit de voorafgaande tweede aanbesteding (TenderNed kenmerk: TN 477772) zijn bijgevoegd en maken onderdeel uit van de Overeenkomst, met uitzondering van de antwoorden op de vragen 2, 3, 12, 13, 27 van Nota van inlichtingen 2024-08-13-1. Deze vragen vervallen (en zijn doorgestreept in de Nota van Inlichtingen 2024-08-23-1) en worden voor zover relevant opnieuw beantwoord of verwerkt in deze aanbestedingsleidraad, de overige aanbestedingsstukken of de Nota van Inlichtingen. In het laatste geval vindt de publicatie hiervan ~~vindt~~ direct na publicatie van de aankondiging op TenderNed plaats.

4.1.1 Voorbehouden, alternatieven, verbeteringen

Zitten er elementen in uw voorgenomen Inschrijving die niet zonder voorbehoud voldoen aan de gestelde eisen? Stel dan hierover een vraag tijdens de Nota van Inlichtingen. Door het indienen van uw Inschrijving verklaart u zich onvoorwaardelijk akkoord met alle aan de procedure en opdracht gestelde eisen.

4.2. Planning

De planning zoals opgenomen in TenderNed is leidend. Eventuele aanpassingen worden als rectificatie gecommuniceerd.

4.3. Uitsluitingsgronden

Door het ondertekenen van het Uniform Europees Aanbestedingsdocument (UEA) verklaart u dat geen van de uitsluitingsgronden genoemd in het UEA (zowel verplicht als facultatief) op u van

toepassing is. De van toepassing zijnde uitsluitingsgronden en de omschrijving daarvan vindt u terug in de aankondiging. Indien u gebruik maakt van onderaannemers, derden of combinanten, dienen die ook een UEA in te vullen en ondertekend in te dienen.

Het UEA moet volledig, juist, onvoorwaardelijk en zonder voorbehoud worden ingevuld en rechtsgeldig ondertekend.

4.4 Geschiktheidseisen

Inschrijver verklaart middels het UEA (Deel IV) aan de hierna gestelde geschiktheidseisen te voldoen alsmede de geschiktheidseisen genoemd in het programma van eisen (zie bijlage H eisen 6 Geschiktheid). Indien Inschrijver niet kan voldoen aan een of meer van de gestelde geschiktheidseisen, wordt de Inschrijver uitgesloten van (verdere) deelname aan de aanbestedingsprocedure.

Opdrachtgever is bevoegd de aangeleverde informatie te controleren, onder andere door contact op te nemen met opgegeven referenties en door een bezoek aan het bedrijf van inschrijver.

4.4.1 Beroepsbevoegdheid

Inschrijving beroeps- of handelsregister De onderneming van Inschrijver dient ingeschreven te staan in het beroeps- of handelsregister volgens de voorschriften van de lidstaat waar hij is gevestigd.

4.4.2 Technische en beroepsbekwaamheid

Inschrijver dient te voldoen aan de hierna volgende geschiktheidseisen met betrekking tot technische en beroepsbekwaamheid.

Kerncompetentie 1

De volgende kerncompetentie wordt gevraagd door middel van een referentie aan te tonen:

- Inschrijver dient te beschikken over de competentie om over een periode van minimaal ~~3 aaneengesloten jaren~~ 1 aaneengesloten jaar converged OT & IT SOC-diensten operationeel te verlenen (de implementatiefase telt niet mee) aan één Opdrachtgever, waarbij de OT-installaties worden gebruikt voor het beheer van operationele processen in de fysieke wereld voor het aansturen en monitoren van industriële apparatuur. De omzetwaarde van deze opdracht dient minimaal ~~€ 1.000.000~~ € 330.000 te zijn.

Kerncompetentie 2

De volgende kerncompetentie wordt gevraagd door middel van een referentie aan te tonen:

- Inschrijver dient te beschikken over de competentie om over een aaneengesloten periode van tenminste 3 jaren IT diensten te verlenen, waarop de Baseline Informatiebeveiliging Overheid (BIO) als onderdeel van de contractvoorwaarden van toepassing is. De totale omzetwaarde van de opdracht(en) bedraagt minimaal € 500.000.

Kerncompetentie 3

De volgende kerncompetentie wordt gevraagd door middel van een referentie aan te tonen:

- Inschrijver dient te beschikken over de competentie om over een aaneengesloten periode van tenminste 3 jaren IT diensten te verlenen, waarop de internationale norm IEC 62443 als onderdeel van de contractvoorwaarden van toepassing is. De totale omzetwaarde van de opdracht(en) bedraagt minimaal € 500.000.

Bij Inschrijving te overleggen bewijsstukken

Per referentie opdracht een volledig ingevuld en rechtsgeldig ondertekende referentieverklaring conform het format formulier 3 referentieproject kerncompetentie.

Een referentie opdracht dient te voldoen aan de volgende voorwaarden

- Indien er gebruik wordt gemaakt van referenties waarbij Inschrijver of onderaannemer samen met een andere ondernemer de referentie opdracht heeft uitgevoerd, moet duidelijk worden aangegeven welk deel door Inschrijver of onderaannemer is uitgevoerd. Alleen het daadwerkelijk uitgevoerde deel van de referentie opdracht mag als zodanig worden gebruikt. Indien Inschrijver toch gebruik wenst te maken van de volledige referentie dient de betrokken ondernemer van de referentie als onderaannemer te worden ingezet bij de uitvoering van de onderhavige opdracht.
- In het geval van een samenwerkingsverband dienen de combinanten gezamenlijk te voldoen aan de kerncompetenties. De combinant op wie inzake een kerncompetentie een beroep gedaan wordt, dient tijdens de uitvoering van de opdracht de werkzaamheden waarop deze kerncompetentie van toepassing zijn ook daadwerkelijk uit te voeren.
- Indien een Inschrijver zich voor de toetsing aan de technische bekwaamheid (referenties) deels op de technische bekwaamheid van derde(n) beroept, dient duidelijk te worden gemaakt in de overlegde referenties welk deel van de opdracht door Inschrijver en welk deel door de betreffende derde is uitgevoerd. Per referentie dient duidelijk aangegeven te worden door welke organisatie de referentie opdracht is uitgevoerd. De derde op wie inzake een kerncompetentie een beroep gedaan wordt, dient tijdens de uitvoering van de opdracht de werkzaamheden waarop deze kerncompetentie van toepassing zijn ook daadwerkelijk uit te voeren.
- De referentie opdracht is actueel. Dat wil zeggen dat de referentie opdracht op het moment dat de datum waarop de Inschrijving moet zijn ingediend niet langer dan zeven jaar geleden is uitgevoerd, of op het moment van uitbrengen van de Inschrijving in uitvoering is. Indien gebruik gemaakt wordt van een nog niet (geheel) afgeronde opdracht, mogen alleen de werkelijk behaalde resultaten van de lopende opdracht worden opgegeven.
- Inschrijver is ermee bekend en gaat ermee akkoord dat Het Waterschapshuis zich het recht voorbehoudt om zonder tussenkomst van Inschrijver de juistheid van alle verstrekte informatie omtrent de referentie(s) te verifiëren (bij de referent) en/of nadere bewijsstukken op te vragen bij de Inschrijver, zoals het bewijs van de duur van de referentie opdracht en bewijs van de omvang van de referentie opdracht.

Inschrijver beschikt over de benodigde technische bekwaamheid voor het uitvoeren van de Overeenkomst.

Technische bekwaamheid 1

- Inschrijver beschikt over een converged OT & IT SOC-team dat minimaal een jaar als zodanig functioneert.

Bij Inschrijving te overleggen bewijsstukken:

Technische bekwaamheid 1 wordt bij inschrijving aangetoond met een opgave van sinds wanneer het converged OT & IT SOC als zodanig functioneert, inclusief de organisatorische inbedding (waaronder een organogram) zoals die er minimaal een jaar geleden uitzag en hoe die op dit moment is. Indien tussen die twee momenten een verschil bestaat van de organisatorische inbedding, dan dient er tevens een beschrijving van de transitie van de inbedding tussen de twee momenten te worden opgegeven. Daarnaast dient de opgave onder andere te bevatten een beschrijving van de organisatie en het functioneren van het SOC-team.

Technische bekwaamheid 2

- Inschrijver beschikt over een converged OT & IT SOC-team waarbij de bezetting van het SOC-team 24 uur per kalenderdag bestaat uit minimaal 40 % niveau 2 (of hoger) analisten. Het niveau 1 en niveau 2 SOC-analisten zijn aantoonbaar gecertificeerde SOC-analisten via een marktconforme SOC-analistencertificering. De integriteit van alle SOC-analisten in het SOC-team dient door middel van een erkende screening te zijn vastgesteld.
  Zie de "Begripsbepalingen m.b.t. dienstverlening", aan het einde van deze leidraad, voor de definities van niveau 1, niveau 2 en niveau 3 SOC-analisten.

Bij Inschrijving te overleggen bewijsstukken:

Inschrijver overlegt een opgave van de bezetting van de SOC-analisten in het converged OT & IT SOC-team, waaruit blijkt dat er wordt voldaan aan de eis. Uit de opgave moet in ieder geval blijken:

- Het totaal aantal SOC-analisten;
- De voor- en achternaam van elke SOC-analist*;
- Het certificeringsniveau (1, 2 of 3) van de betreffende SOC-analist. Daarbij wordt aangegeven aan welke type certificering is voldaan en welke onafhankelijke opleidings-/certificeringsinstituten deze certificaten hebben afgegeven;
- Indien geen opleidingscertificaten van onafhankelijke opleidings-/certificeringsinstituten kunnen worden overlegd:
  - een beschrijving van de opleiding en het curriculum van de opleiding waarin aangetoond dient te worden dat de onderwerpen/inhoud overeenkomt met de in de definities voor SOC-analisten Niveau 1, 2 en 3 (zie "Begripsbepalingen m.b.t. dienstverlening", aan het einde van deze leidraad) genoemde certificeringen;
- Dat elke SOC-analist met goed gevolg is gescreend door een als Particulier Onderzoeksbureau gecertificeerde organisatie (POB) en welke POB's deze screeningsonderzoeken hebben uitgevoerd. In de screenings zijn minimaal de volgende onderdelen zijn opgenomen: financiële checks, social mediaonderzoek, verificatie strafblad en een persoonlijk interview. Indien er sprake is van een screening door een daartoe geëigende centrale overheidsinstantie, dient inschrijver middels de Nota van Inlichtingen procedure te vragen of de betreffende screening van de betreffende centrale overheidsinstantie als gelijkwaardig wordt beschouwd;
- De startdatum van de SOC-analist binnen het converged OT- & IT SOC.

Volg-nummer	Voor- en achternaam* analist	Level (1, 2 of 3)	Type certificering & instituut	Type Screening & POB	Datum start binnen converged OT- & IT SOC

* De kolom Voor- en achternaam kan bij inschrijving leeg blijven of geanonimiseerd zijn. hWh zal inschrijver na inschrijving verzoeken om dezelfde lijst maar dan met voor- en achternamen te tonen in een overleg met hWh. hWh krijgt geen afschrift van de getoonde lijst. De lijst moet behoudens de toegevoegde namen identiek zijn aan de bij inschrijving overlegde lijst. Vervolgens geeft hWh aan welke met voor- en achternaam genoemde SOC-analist Niveau 2 (of hoger) hWh wenst te spreken in de toelichting als bedoeld in paragraaf 6.3 van de Aanbestedingsleidraad. Het overleg waarin inschrijver de lijst met namen toont, kan naar keuze van inschrijver op locatie bij hWh in Amersfoort zijn of online. De voor- en achternaam van de analist is vereist ten behoeve van het uitnodigen van een SOC-analist in het kader van de toelichting van de inschrijving als bedoeld in paragraaf 6.3 van deze aanbestedingsleidraad.

Bijlage L bevat de belangenafweging in het kader van de AVG.

4.4.3 Kwaliteitsborging

Kwaliteitsborging

Met het doen van een Inschrijving verklaart Inschrijver dat zijn systeem van kwaliteitsborging voldoet aan de Europese normenreeks NEN/ISO 9001:2015 serie of een gelijkwaardig kwaliteitsborgingssysteem, waarbij SOC-dienstverlening binnen het toepassingsbereik valt.

Inschrijver kan dit aantonen door middel van:

- Een kopie van het meest recente, geldende certificaat met vermelding van het jaar van invoering en expiratie, afgegeven door een gecertificeerde instantie als bedoeld in artikel 2.96 Aw 2012; of,
- Indien Inschrijver een gelijkwaardig gecertificeerd informatiebeveiligingssysteem heeft, gebaseerd op een andere norm dan de ISO 9001:2015: Een kopie certificaat van de gecertificeerde instantie als bedoeld in artikel 2.96 van de Aanbestedingswet en een onderbouwde toelichting waaruit blijkt op welke punten en in welke mate het systeem overeenkomt en/of afwijkt van het van toepassing zijnde NEN/ISO 9001:2015 systeem. In deze toelichting dienen de volgende onderwerpen naar voren te komen:
    - Beoordeling van de context van de organisatie, klanteisen en risicoanalyse;
    - Betrokkenheid van leiderschap bij het vaststellen en borgen van het kwaliteitssysteem;
    - Planning van organisatie- en kwaliteitsdoelstellingen;
    - Beschrijving van middelen die noodzakelijk zijn om uitvoering te geven aan de bedrijfsprocessen;
    - Uitvoering en beheersing van de bedrijfsprocessen;
    - Evaluatie en continue verbetering van bedrijfsprestaties.
- Indien geen certificaat kan worden overlegd: een beschrijving van het kwaliteitsborgingsysteem. Het kwaliteitsborgingsysteem dient tenminste de bovengenoemde onderwerpen af te dekken.

Informatiebeveiliging

Met het doen van een Inschrijving verklaart Inschrijver dat zijn systeem van informatiebeveiliging voldoet aan de Europese normenreeks NEN/ISO 27001:2022 serie of een gelijkwaardig systeem van informatiebeveiliging, waarbij SOC-dienstverlening binnen het toepassingsbereik valt.

- Een kopie van het meest recente, geldende certificaat met vermelding van het jaar van invoering en expiratie, afgegeven door een gecertificeerde instantie als bedoeld in artikel 2.96 Aw 2012, of;
- Indien Inschrijver een gelijkwaardig gecertificeerd informatiebeveiligingssysteem heeft, gebaseerd op een andere norm dan de ISO 27001:2022: Een kopie certificaat van de gecertificeerde instantie als bedoeld in artikel 2.96 van de Aanbestedingswet en een onderbouwde toelichting waaruit blijkt op welke punten en in welke mate het systeem overeenkomt en/of afwijkt van het van toepassing zijnde NEN/ISO 27001:2022 systeem. In deze toelichting dienen de volgende onderwerpen naar voren te komen:
    - Aansturing en werking van geïmplementeerd informatiebeveiligingsbeleid;
    - Organisatie van informatiebeveiliging;
    - Classificatie en beheersing van informatie;
    - Beheer van bedrijfsmiddelen;
    - Veiligheid van personeel (voor, tijdens en na dienstverband);
    - Fysieke beveiliging en beveiliging van de omgeving in relatie tot informatiebeveiliging;
    - Toegangsbeveiliging tot informatie:
        - Toegang tot informatie- en informatie-verwerkende faciliteiten;

        - Beheer van toegangsrechten van gebruikers;
        - Gebruikersverantwoordelijkheden;
        - Toegang tot systemen en applicatieve toepassingen;
    - Beveiliging van communicatie en bedieningssystemen, inclusief cryptografische beheersmaatregelen;
    - Beveiliging bedrijfsvoering:
        - Bedieningsprocedures en verantwoordelijkheden;
        - Bescherming tegen malware
        - Back-up
        - Verslaglegging en monitoring
        - Beheersing van de operationele software
        - Beheer van technische kwetsbaarheden
        - Overwegingen betreffende audits van informatiesystemen
    - Bedrijfscontinuïteitsbeheer;
    - Naleving van wet- en regelgeving;
    - Evaluatie van de informatiebeveiliging binnen de organisatie;

Of;

- Indien geen certificaat kan worden overlegd: een beschrijving van het informatiebeveiligingssysteem. Het informatiebeveiligingssysteem dient tenminste de bovengenoemde onderwerpen af te dekken.

Informatiebeveiliging voor clouddiensten

Met het doen van een Inschrijving verklaart Inschrijver dat zijn systeem van informatiebeveiliging voor clouddiensten voldoet aan de Europese normenreeks NEN/ISO 27017:2015 serie of een gelijkwaardig systeem van informatiebeveiliging voor clouddiensten, waarbij SOC-dienstverlening binnen het toepassingsbereik valt.

- Een kopie van het meest recente, geldende certificaat met vermelding van het jaar van invoering en expiratie, afgegeven door een gecertificeerde instantie als bedoeld in artikel 2.96 Aw 2012, of;
- Indien Inschrijver een gelijkwaardig gecertificeerd informatiebeveiligingssysteem heeft, gebaseerd op een andere norm dan de ISO 27017:2015: Een kopie certificaat van de gecertificeerde instantie als bedoeld in artikel 2.96 van de Aanbestedingswet en een onderbouwde toelichting waaruit blijkt op welke punten en in welke mate het systeem overeenkomt en/of afwijkt van het van toepassing zijnde NEN/ISO 27017:2015 systeem. In deze toelichting dienen de volgende onderwerpen met betrekking tot clouddiensten naar voren te komen:
    - Aansturing en werking van geïmplementeerd informatiebeveiligingsbeleid;
    - Organisatie van informatiebeveiliging;
    - Classificatie en beheersing van informatie;
    - Beheer van bedrijfsmiddelen;
    - Veiligheid van personeel (voor, tijdens en na dienstverband);
    - Fysieke beveiliging en beveiliging van de omgeving in relatie tot informatiebeveiliging;
    - Toegangsbeveiliging tot informatie:
        - Toegang tot informatie- en informatie-verwerkende faciliteiten;
        - Beheer van toegangsrechten van gebruikers;
        - Gebruikersverantwoordelijkheden;
        - Toegang tot systemen en applicatieve toepassingen;
    - Beveiliging van communicatie en bedieningssystemen, inclusief cryptografische beheersmaatregelen;

- Beveiliging bedrijfsvoering:
  - Bedieningsprocedures en verantwoordelijkheden;
  - Bescherming tegen malware
  - Back-up
  - Verslaglegging en monitoring
  - Beheersing van de operationele software
  - Beheer van technische kwetsbaarheden
  - Overwegingen betreffende audits van informatiesystemen
- Bedrijfscontinuïteitsbeheer;
- Naleving van wet- en regelgeving;
- Evaluatie van de informatiebeveiliging binnen de organisatie;

Of;

- Indien geen certificaat kan worden overlegd: een beschrijving van het informatiebeveiligingssysteem voor clouddiensten. Het informatiebeveiligingssysteem voor clouddiensten dient tenminste de bovengenoemde onderwerpen af te dekken.

Beheersing uitbesteedde processen

Met het doen van een Inschrijving verklaart Inschrijver in bezit te zijn van een ISAE3402 Type 2 verklaring, Service Organisation Control 2 verklaring (SOC2-verklaring) of een ander gelijkwaardig certificaat, waarbij SOC-dienstverlening binnen het toepassingsbereik valt.

- Een kopie van het meest recente, geldende verklaring met vermelding van het jaar van invoering en expiratie, afgegeven door een gecertificeerde instantie als bedoeld in artikel 2.96 Aw 2012 inclusief een verklaring van toepasselijkheid, of;
- Indien Inschrijver een gelijkwaardige, verklaring heeft, gebaseerd op een andere norm dan de ISAE3402 Type 2 verklaring/ SOC2-verklaring: Een kopie verklaring van de gecertificeerde instantie als bedoeld in artikel 2.96 van de Aanbestedingswet en een onderbouwde toelichting waaruit blijkt op welke punten en in welke mate het systeem overeenkomt en/of afwijkt van de ISAE3402 Type 2 verklaring/ SOC2-verklaring.
  In deze toelichting dienen de volgende onderwerpen naar voren te komen:
  - Managementverklaring, scope van de dienstverlening en organisatorisch bereik (van toepassing zijnde 'Trust Service Criteria');
  - Relevante IT-architectuur en verantwoordelijkheden;
  - Invulling, toetsing en evaluatie van de klantvraag;
  - Risicoanalyses en -mitigatie. Zowel intern t.a.v. de dienstverlening als extern i.v.m. veranderende omgeving & -dreigingen en wet- en regelgeving;
  - Implementatie en continuïteit van beheersmaatregelen voor:
    - Organisatie van de dienstverlening, processen, procedures, verantwoordelijkheden, gedragsnormen en screening van medewerkers;
    - Beschikbaarheid en continuïteit van mensen, middelen, processen en herstelprocedures;
    - Vertrouwelijkheid (privacy-aspecten) t.a.v. data en de integriteit van het data-verwerkingsproces;
    - Communicatie m.b.t. beveiligingsbeleid, structuur, processen en bevoegdheden;
  - Afstemming tussen processen, systemen en maatregelen;
  - Monitoren uitvoering maatregelen (audits);

Of;

- Indien geen certificaat kan worden overlegd: een beschrijving van de beheersing van uitbestede processen. Het beheerssysteem van uitbestede processen dient tenminste de bovengenoemde onderwerpen af te dekken.

4.5. Uw Inschrijving

Dien uw Inschrijving in door deze, vóór de aangegeven tijd op de sluitingsdatum in TenderNed, in de digitale kluis te plaatsen. Na dit tijdstip is het niet meer mogelijk om de stukken in de kluis te plaatsen. hWh accepteert alleen Inschrijvingen die via TenderNed zijn ingediend.

Uw Inschrijving bevat de volgende documenten:

1. Uniform Europees Aanbestedingsdocument
   (indien van toepassing ook van derden en/of onder aannemer(s))
2. Verklaring derde en/ of verklaring onder aannemer(s)
3. Verklaring Rusland
4. Referentie verklaringen Kerncompetentie 1, 2 en 3
5. Bewijsstukken Technische Bekwaamheid 1 en 2
6. Bijlage G1 SOC Dienstverlening (uitwerking Gunningcriterium 1)
7. Bijlage G2 Samenwerking (Uitwerking Gunningcriterium 2)
8. Bijlage G3 Toekomstbestendigheid (Uitwerking Gunningscriterium 3)
9. Prijsinvulformulier
10. Uittreksel Kamer van Koophandel
11. Bewijs mandaat / machtiging (indien van toepassing).

Documenten die u niet aan een eis of gunningscriterium kan koppelen, kunt u in TenderNed uploaden bij de tab 'Overige documenten'.

4.5.1. (Rechtsgeldige) ondertekening

Op basis van artikel 2 lid 2 van het Aanbestedingsbesluit: indien de handtekening betrekking heeft op meerdere documenten waarvan de eigen verklaring er één is, is het niet verplicht om het UEA te ondertekenen. Bij deze aanbesteding geldt daarom de handtekening op Formulier 4 – Prijsformulier als een ondertekening van het UEA.

De ondertekening wordt geacht rechtsgeldig te zijn als deze gezet is door een tekenbevoegde of gemandateerde/ gemachtigde functionaris. Als er gebruik gemaakt wordt van een mandaat/ machtiging, dient deze bij de Inschrijving aangeboden te worden.

4.6. Bewijsstukken

Wij vragen de Gedragsverklaring Aanbesteden, een Uittreksel uit het handelsregister en een Verklaring betalingsgedrag nakoming fiscale verplichtingen als bewijsstukken op bij de voorlopig gegunde partij.

Let op: zorg dat u tijdig beschikt over de Gedragsverklaring Aanbesteden en de Verklaring betalingsgedrag nakoming fiscale verplichtingen.

4.7. Standstill termijn

Indien u bezwaar heeft tegen de Gunningsbeslissing, kunt u binnen 20 kalenderdagen na de dagtekening van de Gunningsbeslissing:

- Een kort geding aanhangig maken bij de civiele rechter te Utrecht.

De genoemde termijn van 20 kalenderdagen na de dagtekening van de Gunningsbeslissing, is een vervaltermijn wat betekent dat u daarna geen bezwaar meer kunt maken tegen de beslissing.

5. Hoe bepalen we de winnaar?

5.1. Beoordelingscommissie

De inhoudelijk beoordeling wordt gedaan door een beoordelingscommissie ~~bestaande uit 7 beoordelaars~~ onder leiding van de Inkoopadviseur. De commissie krijgt tijdens het beoordelen van de kwalitatieve gunningscriteria nog geen inzage in de inschrijvingsprijzen.

De beoordeling van de Inschrijvingen vindt plaats in fasen.

Fase 1: openen van de kluis

Na het verstrijken van de inschrijvingstermijn, wordt de digitale kluis geopend en worden de inschrijvingen gedownload. Hierbij zijn geen leden van de beoordelingscommissie betrokken. De inschrijvingen worden vertrouwelijk behandeld.

Na het openen van de digitale kluis wordt een automatisch gegenereerd proces-verbaal van kluisopening verstuurd aan alle Inschrijvers.

Fase 2: controleren of de inschrijving geldig is

In deze fase worden de Inschrijvingen gecontroleerd op volledigheid en geldigheid. Alle gevraagde bijlages/ formulieren dienen in uw inschrijving te zijn opgenomen, volledig te zijn ingevuld en indien van toepassing (rechtsgeldig) te zijn ondertekend. De bij deze Uitnodiging of latere versie bij de Nota van Inlichtingen beschikbaar gestelde formats dienen ongewijzigd te zijn.

Nadat is vastgesteld dat de Inschrijvingen volledig zijn, worden deze gecontroleerd op uitsluitingsgronden en wordt beoordeeld of aan de (geschiktheids)eisen is voldaan. Een Inschrijving die niet volledig is, waaruit blijkt dat uitsluitingsgronden van toepassing zijn of die niet voldoet aan de (geschiktheids)eisen, wordt als ongeldig beoordeeld en komt niet voor inhoudelijke beoordeling in aanmerking. Indien dit het geval is, wordt de betreffende Inschrijver hierover geïnformeerd.

Fase 3: beoordeling op de gunningcriteria

In fase 3 worden de inschrijvingen die in fase 2 als volledig en geschikt zijn aangemerkt, inhoudelijk beoordeeld op basis van de gunningscriteria. Uitgangspunten bij de beoordeling:

a) De beoordelaars hebben nog geen kennis van de ingediende prijzen;

b) De beoordelaars geven individueel voor elk onderdeel een beoordeling;

c) De toe te kennen beoordelingen zijn; verdere verfijning is niet toegestaan;

Zeer goed/ uitmuntend
Goed
Ruim voldoende
Voldoende
Matig/ onvoldoende

d) Vervolgens bespreekt het voltallige beoordelingsteam de individueel toegekende beoordeling en stelt de definitieve beoordeling voor elk kwalitatief subgunningscriterium in consensus vast;

e) Daarna wordt deze consensusbeoordeling omgezet naar een ‘waarde’ volgens de tabel bij de bijbehorende Gunningscriteria;

f) De totaal behaalde waarde wordt van de Inschrijfprijs afgehaald. Wat resulteert in een Fictieve laagste prijs ranking van de Inschrijvers.

Toelichting te behalen meerwaarde

De beoordeling op de kwalitatieve criteria kennen een maximaal aantal te behalen waarde.

Naarmate een plan van aanpak (als onderdeel van uw beantwoording) meer overtuigt dat de Inschrijver de doelstellingen beter weet te realiseren, wordt het betreffende plan hoger gewaardeerd.

Bij de beoordeling van uw Inschrijving op basis van de Gunningscriteria kan de beoordelingscommissie tot de conclusie komen dat een inschrijving inhoudelijk niet voldoet aan de eisen zoals die in de aanbestedingsstukken zijn opgenomen. Dit houdt in dat de Inschrijving alsnog als ongeldig kan worden beoordeeld, terzijde wordt gelegd en geacht niet inhoudelijk te zijn beoordeeld. Indien dit het geval is, wordt de betreffende Inschrijver hierover geïnformeerd.

Tegenstrijdigheden

In geval van tegenstrijdigheden in de uitwerking van de verschillende gunningscriteria kan de beoordelingscommissie uw invulling van een of meerdere wensen met een lagere waardering beoordelen.

Na vaststelling van de beoordeling op de kwalitatieve criteria worden de inschrijfprijzen geopend.

Gelijke laagste evaluatieprijs

Indien twee of meer Inschrijvers gelijkelijk als beste scoren, beslist

- De hoogste kwalitatieve score

Mocht deze score ook gelijk zijn dan beslist

- De hoogste kwalitatieve score op gunningscriterium G1, dan G2, dan G3.

Wie als best scorende eindigt. Indien de score dan ook gelijk is, beslist het lot wie de Economisch meest voordelige inschrijving heeft gedaan. De Inschrijvers worden tijdig van in kennis gesteld dat een loting zal plaatsvinden. Zie voor de lotingsprocedure Bijlage C.

Fase 4 Bekendmaking Gunningsbeslissing

Na beoordeling van de Inschrijvingen wordt de Gunningsbeslissing schriftelijk meegedeeld aan alle Inschrijvers. De Gunningsbeslissing aan de afgewezen Inschrijvers bevat naast hun eigen score de inhoudelijke motivering waarom de best scorende Inschrijver(s) de economisch meest voordelige inschrijving(en) heeft/ hebben gedaan.

Fase 5: Bezwaar tegen de Gunningsbeslissing

Indien u bezwaar heeft tegen de Gunningsbeslissing, kunt u binnen 20 kalenderdagen na de dagtekening van de Gunningsbeslissing:

c. een kort geding aanhangig maken bij de civiele rechter te Utrecht.

De genoemde termijn van 20 kalenderdagen na de dagtekening van de Gunningsbeslissing, is een vervaltermijn wat betekent dat u daarna geen bezwaar meer kunt maken tegen de beslissing.

Om te voorkomen dat een uitgebrachte dagvaarding ons niet tijdig bereikt, wordt de bezwaarmaker verzocht zo spoedig mogelijk een afschrift van de dagvaarding via de berichtenservice van TenderNed aan de contactpersoon te sturen.

Indien een kort geding is aangespannen, sluiten wij de beoogde Overeenkomst niet eerder dan nadat de rechter dan wel het scheidsgerecht een beslissing heeft genomen over het verzoek tot voorlopige maatregelen en de opschortende termijn is verstreken.

Fase 6: Bewijsmiddelen en Verificatie

Bewijsmiddelen

De bewijsmiddelen worden opgevraagd bij de Inschrijver die volgens de Gunningsbeslissing in aanmerking komt voor de opdracht. De verlangde bewijsmiddelen moeten, na een verzoek daartoe, binnen 10 kalenderdagen gerekend vanaf de dag van verzending van het verzoek, door HWh zijn ontvangen via de berichtenservice van TenderNed.

Indien de bewijsmiddelen niet tijdig en/of volledig zijn aangeleverd of niet de juistheid van de verklaringen aantonen, wordt de betreffende inschrijving alsnog ongeldig verklaard. De Gunningsbeslissing wordt dan ingetrokken en de procedure zal dan vanaf fase 4 als hierboven omschreven, opnieuw worden doorlopen.

Verificatie

Wij behouden ons het recht voor om een verificatiebespreking te houden met de Inschrijver waarmee wij voornemens zijn te contracteren. Blijkt tijdens de verificatiebespreking dat hij in zijn inschrijving onjuiste informatie heeft verstrekt, dan zal de betreffende inschrijving alsnog ongeldig worden verklaard. De Gunningsbeslissing wordt dan ingetrokken, de procedure zal dan vanaf fase 4 als hierboven omschreven, opnieuw worden doorlopen.

Fase 7: Sluiten Overeenkomst
Als binnen de opschortende termijn van 20 kalenderdagen na het verzenden van de Gunningsbeslissing niet door een Inschrijver bezwaar is gemaakt of een kort geding is aangespannen, kunnen wij besluiten de Overeenkomst met de best scorende Inschrijver aan te gaan.

6. Gunningscriteria

Gegund wordt aan de inschrijver met de economisch meest voordelige inschrijving (EMVI). Criterium voor de economisch meest voordelige inschrijving is de beste prijs – kwaliteitverhouding. De beste prijs – kwaliteitverhouding is de inschrijving met de laagste fictieve inschrijvingsprijs op basis van de volgende vier criteria:

Prijscriterium:

1. Inschrijvingsprijs;

~~2.~~ Kwalitatieve criteria:

2. SOC-dienstverlening;
3. Samenwerking;
4. Toekomstbestendigheid.

Deze criteria zijn nadere uitgewerkt in paragraaf 6.1 en 6.2.

Aan de inschrijving wordt per kwalitatief criterium een kwaliteitswaarde (in Euro) toegekend. De maximale toe te kennen kwaliteitswaarde staat vermeld in tabel 6.1 hieronder.

Gunningscriteria	Maximale Score	Score	Totaal Score (in Euro)
Prijs (inschrijvingsprijs)			**P**
Kwaliteit			
GC. 1 - SOC-dienstverlening	€ 1.200.000	**D**	
GC. 2 – Samenwerking	€ 600.000	**S**	
GC. 3 – Toekomstbestendigheid	€ 500.000	**T**	
Totale kwaliteitsscore			**D+S+T**
Fictieve inschrijvingsprijs (Totale Score)			**+P - (D+S+T)**

Tabel 6.1. EMVI rekentabel.

De economische meest voordelige inschrijving is de inschrijving met de laagste fictieve inschrijvingsprijs op basis van de berekening in tabel 6.1. Deze wordt verkregen door de inschrijvingsprijs te verminderen met de voor elk gunningscriterium aan de inschrijving toegekende kwaliteitswaarde.

6.1 Prijs

U gebruikt het prijsformulier (formulier 4) voor het indienen van uw inschrijvingsprijs.
Alleen de witte velden dienen te worden ingevuld.

Het prijsformulier bestaat uit een viertal categorieën kosten, zoals hierna toegelicht.

Alle genoemde aantallen en de indeling van de Waterschappen in categorie klein, middel en groot voor de tarieven van categorie 1. SOC diensten (regels 3 t/m 28) en categorie 3. Implementatiekosten (regels 38 t/m 43) zijn fictief en enkel ten behoeve van het bepalen van de inschrijvingsprijs.

Waterschappen zijn ingedeeld in de categorieën klein, middel en groot op basis van oppervlakte en aantal inwoners. Globaal genomen zit een relatie tussen de aantallen medewerkers, aantal KA-bronnen, aantal PA-bronnen en de daaraan gerelateerde benodigde hoeveelheid werk voor opdrachtnemer bij de implementatie. Omdat het aantal waterschappen dat tot elke categorie behoort vast is, kan op basis van die indeling ook een prijsopgave worden gemaakt voor de onderdelen in het prijsformulier waar die categorie-indeling wordt gehanteerd. Na opdrachtverlening wordt aan de Opdrachtnemer een overzicht verstrekt welke de Waterschappen tot welke categorie behoort. Het Waterschapshuis en de Unie van Waterschappen vallen onder de categorie klein.

1. Prijs SOC diensten

Facturatie bij Deelnemers van de per Deelnemer variabele aantallen medewerkers, KA-bronnen, PA-bronnen vindt, net als bij alle overige onderdelen in het prijsformulier, plaats op basis van de opgegeven tarieven.

Het doorontwikkelen, waaronder use case management en optimalisatie, van de dienstverlening dient te zijn inbegrepen in de tariefstelling van dit onderdeel 1. Prijs SOC diensten.

2. Prijs extra bronnen en use cases

Na de implementatiefase waarin die data ontsloten wordt die voor de SOC-dienst ‘Monitoring & Alarmering’ noodzakelijk is, gaan we over in een productionele situatie.
In de productiefase kunnen extra data noodzakelijk zijn, kan een wijziging plaatsvinden in de content, wijziging in de indeling van een databron of wisseling van een databron die niet automatisch kan worden verwerkt.
We onderkennen daarbij de volgende situaties:

- Een extra use case wordt gevraagd en daar is data voor nodig. Dat kan al beschikbare (ingelezen) data betreffen, maar ook data uit een extra databron;
- Er vinden wijzigingen in de infrastructuur van een Deelnemer plaats, kan het zijn dat een databron wisselt of een nieuwe databron ontstaat;
- Een databron wisselt van content of formaat waardoor deze niet meer werkt volgens het gehanteerde inlees- en indelings-automatisme.

Om deze handelingen uit te voeren onderkennen we extra variabele kosten, die van toepassing zijn per Deelnemer op het moment dat zich een dergelijke situatie voordoet. Dit zijn kosten voor het aansluiten van een nieuwe of gewijzigde databron of voor het implementeren van een nieuwe use case, situatie zoals hierboven omschreven.

Voor databronnen onderkennen we standaard databronnen en niet-standaard databronnen.

- Een standaard bron is data van een markconforme en bekende bron. Bijvoorbeeld een CISCO-component die veelvuldig bij organisaties wordt gebruikt en vergezeld gaat van een verklaring van CISCO over het formaat en de opmaak van de logdata;
- Een niet-standaard bron is een databron van een exotische component die niet gangbaar is in de markt en waarvoor extra werk nodig is om de data te kunnen duiden en analyseren.

Een use case implementeren definiëren we qua kosten op basis van de aan te sluiten databronnen. Voor een nieuwe use case rekenen we het aansluiten van 2 standaard databronnen en 1 niet-standaard databron. Dit betekent dat in deze databron-aansluitkosten, de kosten voor het creëren of herdefiniëren van bijbehorende detectieregels worden geacht te zijn opgenomen.

Het tarief voor deze wijzigingen dient te worden opgegeven in de regels 29 t/m 37 van het prijsformulier. Inschrijver dient er rekening mee te houden dat er tussen de Deelnemers een lage mate van standaardisatie van IT- en (met name) OT-componenten is. Dit brengt met zich mee dat voor de prijs(vorming) in het prijsformulier dient te zijn gebaseerd op het uitgangspunt dat elke niet-standaard bron uniek is en niet hergebruikt kan worden bij andere Deelnemers.

3. Prijs implementatiekosten

Inschrijver kan voor de verschillende categorieën klein, middel of groot verschillende prijzen voor de implementatie hanteren. De verschillen dienen onderling in redelijke verhouding tot elkaar te staan.

Inschrijver dient er rekening mee te houden dat er tussen de Deelnemers grote verschillen bestaan op het gebied van volwassenheid met betrekking tot informatieveiligheid. De implementatie betreft het aansluiten van de benodigde logbronnen, het implementeren danwel activeren van de use cases zoals benoemt in de bijlage M - 'Initiële use cases SOC', het afstemmen (tunen) van de use cases, het afstemmen van de SLA en DAP afspraken met de betreffende Deelnemer en het inregelen van de basisprocessen. Elke Deelnemer is verantwoordelijk voor:

- de kwaliteit van de aangeleverde logbronnen. Dit omvat een borging van de juistheid, volledigheid en tijdigheid, waarbij een foutmarge op de genoemde onderdelen van maximaal 10% toelaatbaar is;
- de kwaliteit van de binnen de Deelnemer ingerichte SIEM oplossing, indien van toepassing. De Deelnemer 'eigen' SIEM oplossing genereert niet meer dan 10% false positives naar het SOC van de opdrachtnemer.

Het optimaliseren van de use cases wordt gezien als een doorlopende operationele activiteit gedurende de dienstverlening en behoort bij prijsonderdeel 1. Prijs SOC-diensten te zijn inbegrepen.

4. Prijs consultancy voor ad hoc diensten

Bij de prijsstelling voor consultancy dient u zelf de onderlinge verhouding van de inzet tussen de verschillende categorieën consultants (junior, medior, senior) op te geven. De begrippen Security Consultant junior, respectievelijk medior en senior zijn uitgewerkt in de "Begripsbepaling m.b.t. dienstverlening" aan het einde van deze aanbestedingsleidraad. Bij de uitvoering van de opdracht dient u bij elke Deelnemer die onderlinge verhouding in de facturatie op jaarbasis voor ad hoc consultancy diensten in acht te nemen.

De tarieven en uren in hun onderlinge verhouding op een geschat jaartotaal van 350 uur per Waterschap per jaar (uitgaande van de eerste twee jaar) dient u in te vullen in de regels 48 t/m 50.

Facturatie vindt op maandelijkse basis plaats. Bij de inzet van consultancy uren, dient de opgegeven verhouding tussen de inzet van junior, medior, en senior consultant te worden toegepast. Jaarlijks wordt beoordeeld of de daadwerkelijk gerealiseerde consultancy-uren overeenkomen met de opgegeven verhouding. Afwijkingen worden jaarlijks gecorrigeerd.

Zoals onder prijsonderdeel 1. hierboven (Prijs SOC diensten) reeds valt af te leiden, vindt doorontwikkeling van dienstverlening niet plaats op basis van consultancy diensten. Na ommekomst van de eerste twee jaar van de SOC dienstverlening bij een waterschap zal de inzet van consultants voor ad hoc diensten naar verwachting beperkt zijn en zal in beginsel voornamelijk worden toegepast in het kader van werkzaamheden in het kader van de herzieningsclausule (als genoemd in paragraaf 2.2).

Algemeen

De Inschrijver kan geen rechten ontlenen aan de in het prijsformulier (of andere Aanbestedingsstukken) genoemde aantallen, cijfers, percentages en bedragen. Ten aanzien van de prognoses omtrent de omvang of de waarde van de levering en daaraan gerelateerde Dienstverlening geldt uitdrukkelijk dat het hier schattingen betreft.

De Prijsstelling moet "all-in" zijn, dat betekent dat de volgende kosten in ieder geval inbegrepen: de salariskosten, de overheadkosten, telefoonkosten/onlinekosten, de kosten voor ondersteunend werk, de kosten voor het gebruik van apparatuur, software, parkeer-, reisuren, reis-, installatie- en afleverkosten en logistieke kosten. Ook alle eventueel verdere bijkomende kosten moeten inbegrepen zijn. De Prijsstelling dient zowel inclusief als exclusief de van toepassing zijnde BTW te worden vermeld.

Afwijkingen van of aanvullingen op het prijsformulier zijn niet toegestaan. Verder dient u bij het invullen van het prijsformulier de volgende uitgangspunten te hanteren:

I. Alle prijzen dienen netto prijzen te zijn, afgerond op twee cijfers achter de komma. Eventuele kortingen dienen hierin te zijn verwerkt en mogen niet apart worden opgevoerd;
II. Alle prijzen en tarieven zijn marktconform;
III. Alle onderdelen van de prijzenbladen dienen met bedragen te worden ingevuld. Vermeldingen en/of afkortingen zoals bijvoorbeeld 'n.v.t.', 'n.t.b.' etc. zijn niet toegestaan;
IV. Negatieve bedragen zijn niet toegestaan;
V. De opgegeven prijzen dienen de volledige dienstverlening/ levering te dekken;
VI. Niet in de prijzen verdisconteerde kosten worden niet vergoed;
VII. Het is niet toegestaan te vermelden dat de gevraagde prijzen zijn opgenomen in andere prijsonderdelen van het prijsformulier.

6.2 Kwaliteit

Onderstaand vindt u de kwalitatieve gunningscriteria. U verplicht zich door het indienen van een inschrijving om de opdracht minimaal conform het gestelde in uw inschrijving uit te voeren.

Gunningscriterium 1 SOC-dienstverlening

Inschrijver dient een plan van aanpak SOC-dienstverlening in te dienen als bijlage G1 SOC Dienstverlening bij de inschrijving. Het Plan van Aanpak mag niet meer dan 4 pagina's (A4-formaat) bevatten.

De inschrijver dient in het plan van aanpak in te gaan op de hoofddoelstelling om de PA- en KA-omgevingen vanuit een converged OT & IT SOC optimaal te beschermen, rekening houdend met de situatie bij de Deelnemers en de onderliggende doelstellingen van de SOC-dienstverlening:

- Doelstelling 1: de dienstverlening dient vroegtijdig cyberbeveiligingskwetsbaarheden en bedreigingen te signaleren (cf. "Detect" uit het NIST Cybersecurity Framework 2.0);
- Doelstelling 2: de dienstverlening levert zo spoedig mogelijk een adequate reactie op cyberbeveiligingskwetsbaarheden, -aanvallen en -incidenten bij de Deelnemers en CERT-WM (cf "Respond" uit het NIST Cybersecurity Framework 2.0);
- Doelstelling 3: de dienstverlening zal effectief en efficiënt (al dan niet lokale) logdata analyseren;
- Doelstelling 4: meldingen worden in de context van een individuele Deelnemer en de Waterschapssector als geheel geanalyseerd en beoordeeld;
- Doelstelling 5: actuele specifieke dreigingsinformatie uit het cyber-ecosysteem (zoals andere SOC's, ISAC, OKTT, NCSC, PA/KA-leveranciers) wordt adequaat in de dienstverlening geïntegreerd.

Naarmate het ingediende plan van aanpak weet te overtuigen van een betere verwezenlijking van de doelstellingen, wordt het plan van aanpak hoger gewaardeerd. Aan het plan van aanpak wordt een kwaliteitsscore toegekend als volgt:

Beoordeling	**Kwaliteitsscore** (Punten)
Zeer goed/ uitmuntend	€ 1.200.000
Goed	€ 900.000
Ruim voldoende	€ 525.000
Voldoende	0
Matig/ onvoldoende	Ongeldige inschrijving

Een beoordeling "matig/ onvoldoende" leidt tot ongeldigheid van de inschrijving en derhalve tot uitsluiting van verdere deelname.

De kwaliteitsscore voor het plan van aanpak wordt in mindering gebracht op de inschrijvingsprijs overeenkomstig tabel 6.1. EMVI rekentabel.

Gunningscriterium 2 Samenwerking

Inschrijver dient een plan van aanpak Samenwerking te dienen als bijlage G2 Samenwerking bij de inschrijving. Het Plan van Aanpak uitvoering mag niet meer dan 2 pagina's (A4-formaat) bevatten.

Het plan van aanpak dient in te gaan op de volgende doelstellingen ten aanzien van samenwerking:

- Doelstelling 1: Opdrachtnemer doorgrondt de verwachtingen, behoeften en uitdagingen bij Opdrachtgever en de Deelnemers en adviseert op basis daarvan adequaat, proactief over relevante trends en ontwikkelingen op het gebied van cybersecurity;
- Doelstelling 2: Opdrachtnemer adviseert proactief over algehele cyberweerbaarheid van de (individuele) Deelnemers en de Waterschapssector als geheel;
- Doelstelling 3: Opdrachtnemer monitort en spiegelt op tactisch niveau structureel en proactief met betrekking tot de volwassenheid van de Deelnemers op het gebied van informatieveiligheid en privacy;
- Doelstelling 4: Opdrachtnemer voorziet in een adequate samenwerking met primaire stakeholders;

- Doelstelling 5: Opdrachtnemer acteert en communiceert jegens Opdrachtgever en de Deelnemers op een respectvolle en open toegankelijke en constructieve wijze, is flexibel en draagt er voor zorg dat hij continu de verwachtingen, behoeften en uitdagingen van Opdrachtgever en Deelnemers ten aanzien van cybersecurity begrijpt en doorgrondt en levert een constructieve en adequaat bijdrage aan het oplossen van gezamenlijke problemen.

Naarmate het ingediende plan van aanpak weet te overtuigen van een betere verwezenlijking van de doelstellingen, wordt het plan van aanpak hoger gewaardeerd. Aan het plan van aanpak wordt een kwaliteitsscore toegekend als volgt:

Beoordeling	**Kwaliteitsscore** (Punten)
Zeer goed/ uitmuntend	€ 600.000
Goed	€ 450.000
Ruim voldoende	€ 250.000
Voldoende	0
Matig/ onvoldoende	Ongeldige inschrijving

Een beoordeling "matig / onvoldoende" leidt tot ongeldigheid van de inschrijving en derhalve tot uitlsuiting van verdere deelname.

De kwaliteitsscore voor het plan van aanpak wordt in mindering gebracht op de inschrijvingsprijs overeenkomstig tabel 6.1. EMVI rekentabel.

Gunningscriterium 3 Toekomstbestendigheid

Inschrijver dient een plan van aanpak Toekomstbestendigheid in te dienen als bijlage G3 Toekomstbestendigheid bij de inschrijving. Het Plan van Aanpak mag niet meer dan 2 pagina's (A4-formaat) bevatten.

De inschrijver dient in het plan van aanpak in te gaan op de hoofddoelstelling om zorg te dragen voor een dienstverlening die gedurende de hele looptijd van de overeenkomst beschermt tegen actuele dreigingsbeelden en de onderliggende doelstellingen:

- Doelstelling 1: gedurende de looptijd van de overeenkomst zal de SOC-dienstverlening, met gebruikmaking van bewezen en gangbare kennis en technieken, flexibel meebewegen met, doorontwikkelen van en anticiperen op alle mogelijke toekomstige veranderingen, zowel op het gebied van cybersecurity alsook technische en organisatorische veranderingen bij de Deelnemers.
- Doelstelling 2: de dienstverlening wordt voortdurend aangepast zodat effectiviteit en de efficiëntie continu geoptimaliseerd wordt.

Naarmate het ingediende plan van aanpak weet te overtuigen van een betere verwezenlijking van de doelstellingen, wordt het plan van aanpak hoger gewaardeerd. Aan het plan van aanpak wordt een kwaliteitsscore toegekend als volgt:

Beoordeling	**Kwaliteitsscore** (Punten)
Zeer goed/ uitmuntend	€ 500.000
Goed	€ 375.000

Ruim voldoende	€ 200.000
Voldoende	0
Matig/ onvoldoende	Ongeldige inschrijving

Een beoordeling "matig/ onvoldoende" leidt tot ongeldigheid van de inschrijving en derhalve tot uitsluiting van verdere deelname.

De kwaliteitsscore voor het plan van aanpak wordt in mindering gebracht op de inschrijvingsprijs overeenkomstig tabel 6.1. EMVI rekentabel.

6.3 Toelichting offerte door drie functionarissen

De vijf inschrijvers die de hoogste totaalscore halen op de kwalitatieve criteria samen, worden uitgenodigd voor een toelichting van de offerte. In de toelichting wordt ingegaan op de inschrijving, waarbij Opdrachtgever de gelegenheid heeft hetgeen is aangeboden te verifiëren en waar nodig om verduidelijking te vragen.

De toelichting van de offertes vindt op de in de planning aangegeven data plaats.

De toelichting dient te geschieden door de volgende drie, bij de uitvoering van de opdracht in te zetten, functionarissen van inschrijver:

1. De sleutelfunctionaris die op tactisch niveau verantwoordelijk is voor (technisch inhoudelijke) service delivery richting Opdrachtgever en Deelnemers;
2. De sleutelfunctionaris die bij Opdrachtnemer op strategisch managementniveau verantwoordelijk is voor de services die worden geleverd aan Opdrachtgever en Deelnemers;
3. Een SOC-analist Niveau 2 (of hoger), naar keuze van Opdrachtgever uit het in het kader van technische bekwaamheid 2 opgegeven converged OT & IT SOC-team.

Afhankelijk van de antwoorden van deze functionarissen, kan het initiële oordeel over de verschillende plannen van aanpak naar boven of beneden worden bijgesteld. Het is dan van ook van belang dat deze functionarissen de aangeboden plannen van aanpak doorgronden.

Indien naar aanleiding van de toelichting het kwalitatieve oordeel van een of meerdere van deze inschrijvingen wijzigt, waardoor meer dan één van deze inschrijvingen niet meer bij de top vijf van inschrijvingen met hoogste totaalscore op de kwalitatieve criteria behoren, worden de inschrijvers die doorschuiven en vervolgens in deze top vijf zijn beland, uitgenodigd voor een toelichting.

De in deze alinea beschreven stap wordt net zo lang herhaald totdat er een top vier van inschrijvingen met de hoogste totaalscore op de kwalitatieve criteria is, die ook door inschrijvers zijn toegelicht.

Van deze top vier van inschrijvingen wordt vervolgens bepaald welke inschrijving de beste-prijs kwaliteitverhouding, aan de hand van de fictieve inschrijvingsprijs overeenkomstig de EMVI rekentabel in tabel 6.1. De inschrijving met de laagste fictieve inschrijvingsprijs is de winnende inschrijving.

Begripsbepalingen m.b.t. procedure

In de Leidraad hebben onderstaande vetgedrukte begrippen de betekenis die erachter staat vermeld. Gedefinieerde begrippen worden steeds met een hoofdletter geschreven. De begrippen kunnen, waar van toepassing, zonder verlies van betekenis zowel in enkelvoud als meervoud worden gebruikt.

Aanbestedende dienst
Het Waterschapshuis, verder ook te noemen, 'hWh', 'Opdrachtgever', 'wij'. Als er meerdere Aanbestedende diensten zijn, zijn deze hieronder inbegrepen.

Aanbestedingsprocedure
De Europese openbare procedure, waarbij Ondernemers worden uitgenodigd een Inschrijving in te dienen.

Aanbestedingsstukken
Alle stukken die door de Aanbestedende dienst worden opgesteld of vermeld ter omschrijving of bepaling van onderdelen van de aanbesteding of de procedure

Aanbestedingswet 2012
Wet van 1 november 2012, houdende regels omtrent aanbestedingen.

Algemene inkoopvoorwaarden
De algemene Waterschap voorwaarden voor: diensten (AWVODI-2018)

Beroepsfouten
Tekortkomingen, zoals vergissingen, onachtzaamheden, nalatigheden, verzuimen, onjuiste adviezen, die een vakbekwame en zorgvuldige Opdrachtnemer onder de gegeven omstandigheden met inachtneming van normale oplettendheid en bij een normale vakkennis en normale wijze van vak uitoefening, behoort te vermijden.

Economisch Meest Voordelige Inschrijving (EMVI)
Overkoepelend begrip voor de volgende drie gunningcriteria:

a. beste prijs-kwaliteitsverhouding (BPKV),
b. laagste kosten berekend op basis van kosteneffectiviteit, zoals de levenscycluskosten en
c. de laagste prijs.

Gunningsbeslissing
De keuze van hWh voor de Ondernemer met wie hij voornemens is de Overeenkomst waarop de procedure betrekking heeft, te sluiten, waaronder mede wordt verstaan de keuze om geen Overeenkomst te sluiten.

Gunningscriterium
Een inhoudelijk (gewogen) criterium ter bepaling van de Economisch Meest Voordelige Inschrijving.

Inschrijver
Ondernemer die een Inschrijving indient. Inschrijver kan een zelfstandige Ondernemer zijn die alleen voor zichzelf inschrijft, hij kan een Ondernemer zijn die als hoofdaannemer met Onderaannemers inschrijft en hij kan een Combinatie van Ondernemers zijn die inschrijft.

Inschrijving
Het document waarmee de Inschrijver meedingt naar de Overheidsopdracht die wordt aanbesteed.

Nota van inlichtingen
Document waarin de geanonimiseerde vragen van -potentiële- Inschrijvers en de antwoorden

daarop zijn opgenomen, evenals eventuele wijzigingen van het Beschrijvend document en/of andere Aanbestedingsstukken. De Nota van inlichtingen maakt integraal onderdeel uit van het Beschrijvend document.

Ondernemer
Een leverancier of dienstverlener, gegadigde, potentiële Inschrijver

Onderneming
De juridische vorm waarin de Ondernemer zijn zaak drijft.

Opdracht/ Overheidsopdracht
Een schriftelijke Overeenkomst onder bezwarende titel voor werken, leveringen of diensten, alsmede de Hoofdovereenkomst.

Opdrachtnemer
Inschrijver met wie de Overeenkomst is gesloten.

Overeenkomst
De bijgevoegde (concept-)Overeenkomst voor een Overheidsopdracht die hWh naar aanleiding van deze aanbesteding voornemens is te sluiten met de best scorende Inschrijver.

De overige Aanbestedingsstukken maken deel uit van de Overeenkomst.

Penvoerder
De Aanbestedende dienst die mede namens de andere Aanbestedende dienst(en) de Aanbestedingsprocedure leidt.

Uitnodiging
Het voorliggende Aanbestedingsstuk waarin de Overheidsopdracht en de wijze waarop deze Opdracht in de markt wordt gezet, wordt beschreven en toegelicht. Op basis van dit document wordt Ondernemers gevraagd een Inschrijving te doen.

Verwerkersovereenkomst
Overeenkomst om te zorgen voor de naleving van: artikel 28, leden 3 en 4, van Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming).

Begripsbepalingen m.b.t. dienstverlening

Converged OT & IT SOC

Een 'converged OT & IT SOC' is een SOC dat als één geïntegreerde organisatorische eenheid vanuit een integrale aanpak de OT- en IT-SOC diensten verleent en de OT- en IT-omgeving van de Afnemers beschermt, waarbij:

- Door de integratie van OT- en IT-SOC kennis en integratie van het OT- en IT-detectie en -reactieproces incidenten niet tussen separate IT- en OT-teams hoeven te worden overgedragen;
- Sprake is van een compleet situationeel bewustzijn van de SOC-teamleden om rekening te houden met de unieke kenmerken en kwetsbaarheden van beide soorten systemen; én
- Zowel met de bescherming van de OT als IT kant van de organisatie rekening wordt gehouden, om beveiligingsproblemen adequaat en snel op te lossen.

Automatisering

Automatisering definiëren we al het vervangen van menselijke arbeid door machines of computers en computerprogramma's. De drijfveer is economisch: de som van arbeid en grondstofverbruik is na automatisering kleiner dan daarvoor. Er zijn verschillende vormen van automatisering. In deze leidraad gebruiken we de vormen: kantoorautomatisering (KA) en Industriële automatisering (IA). De overige vormen van automatisering laten we buiten beschouwing.

Security Consultant junior

Een junior consultant in informatiebeveiliging is een beginnende professional die werkt onder toezicht van meer ervaren consultants of projectleiders. Ze ondersteunen bij het uitvoeren van analyses, het implementeren van beveiligingsmaatregelen en het verstrekken van advies aan klanten of interne teams.

Meetbare Kwalificaties:

- Opleiding: Afgeronde bacheloropleiding in Informatietechnologie, Informatica, Cybersecurity of een verwant veld.
- Certificeringen: Basiscertificeringen zoals CompTIA Security+, OT Security Essentials (ICS410), CEH (Certified Ethical Hacker), of vergelijkbaar.
- Ervaring: Minimaal 1-2 jaar ervaring in een relevante rol of stage in de cybersecuritysector.
- Vaardigheden: Basiskennis van netwerkbeveiliging, OT- en IT-componenten beveiliging, risicobeheer, incidentrespons en compliance. Goede analytische en probleemoplossende vaardigheden.
- Soft Skills: Goede communicatieve vaardigheden, vermogen om effectief in een team te werken en te leren van meer ervaren collega's.

Security Consultant medior

Een medior consultant in informatiebeveiliging heeft meer verantwoordelijkheid en zelfstandigheid dan een junior consultant. Ze zijn betrokken bij het ontwerpen en implementeren van beveiligingsoplossingen, het leiden van kleine teams en het adviseren van klanten over complexe vraagstukken op het gebied van cybersecurity.

Meetbare Kwalificaties:

- Opleiding: Afgeronde masteropleiding in Cybersecurity, Informatietechnologie of een gerelateerd vakgebied, of gelijkwaardige werkervaring.

- Certificeringen: Gevorderde certificeringen zoals CISSP (Certified Information Systems Security Professional), GICSP (Global Industrial Cyber Security Professional), CISM (Certified Information Security Manager) of vergelijkbaar.
- Ervaring: Minimaal 3-5 jaar relevante werkervaring, inclusief ervaring met projectmanagement en klantinteractie.
- Vaardigheden: Diepgaande kennis van beveiligingsarchitecturen, penetratietests, kwetsbaarheidsbeoordelingen, en ervaring met het implementeren van compliance-normen zoals AVG, ISO 27001, etc.
- Soft Skills: Leiderschapskwaliteiten, vermogen om zelfstandig te werken en effectief te communiceren met zowel technische als niet-technische belanghebbenden.

Security Consultant senior

Een senior consultant in informatiebeveiliging heeft een strategische rol en is verantwoordelijk voor het leiden van grote cybersecurity-projecten, het ontwikkelen van beleid en procedures, het adviseren van het management op C-niveau en het fungeren als een expert binnen het vakgebied.

Meetbare Kwalificaties:

- Opleiding: Geavanceerde academische graad zoals een master of PhD in Cybersecurity, Informatiebeveiliging of een gerelateerd veld.
- Certificeringen: Topcertificeringen zoals CISSP-ISSAP (Information Systems Security Architecture Professional), GSP (GIAC Security Professional), GSE (GIAC Security Expert), CCISO (Certified Chief Information Security Officer) of vergelijkbaar.
- Ervaring: Minimaal 5-10 jaar ervaring in cybersecurity, inclusief aantoonbare ervaring in senior advies- of leiderschapsrollen.
- Vaardigheden: Diepgaande technische expertise in alle aspecten van cybersecurity, inclusief strategische planning, risicomanagement, incidentrespons op hoog niveau, en compliance-advies op internationaal niveau.
- Soft Skills: Uitstekende communicatieve vaardigheden, sterke leiderschapskwaliteiten, vermogen om complexe concepten duidelijk uit te leggen aan niet-technische belanghebbenden, en ervaring met het adviseren van klanten op bestuurs- en directieniveau.

IA

Industriële Automatisering (IA) omvat de ICS/SCADA systemen en de ICT gerelateerde systemen en onderdelen (hardware en software), waarbij functioneel interactie plaats vindt met de fysieke omgeving of gebruikers (bijvoorbeeld een waterkering, zuiveringsinstallatie etc.). Dit omvat mede het verkrijgen van informatie over de fysieke omgeving (inwinnen) en het beïnvloeden van de fysieke omgeving (bedienen en besturen). PA en OT zijn synoniemen voor IA.

ICS

Industrial Control Systems (Proces Automatisering). Een industrieel besturingssysteem is een elektronisch besturingssysteem en bijbehorende instrumenten die worden gebruikt voor industriële procescontrole. Besturingssystemen kunnen in grootte variëren van enkele modulaire, op een paneel gemonteerde controllers tot grote onderling verbonden en interactieve gedistribueerde besturingssystemen met vele duizenden veldverbindingen.

ICT

Informatietechnologie of informatie- en communicatietechnologie is een vakgebied dat zich bezighoudt met informatiesystemen, telecommunicatie en computers. Hieronder vallen het ontwikkelen en beheren van systemen, netwerken, databases en websites, het onderhouden van computers en software en het schrijven van administratieve programma's.

KA

Kantoorautomatisering. De term "kantoorautomatisering" verwijst naar de uitrusting van een kantoor met moderne gegevensverwerking. Het gaat vooral om het rationaliseren van interne processen met behulp van software. Dit betekent het verhogen van de arbeidsproductiviteit en het verlagen van de totale kosten om de winst te maximaliseren. Het doel is om de efficiëntie van een bedrijf te verhogen door automatisering, mechanisatie en veranderingen in werkprocessen, waardoor kosten en uitgaven aanzienlijk worden verlaagd.

OT

Operational Technology (OT) is een verzamelnaam voor verschillende systemen die worden gebruikt voor het beheer van operationele processen in de fysieke wereld voor het aansturen en monitoren van industriële apparatuur. Het kan dan gaan om het uitlezen van sensoren of het inschakelen van een pomp of schakelaar op basis van een bepaalde conditie.

PA

Proces Automatisering. Hanteren we als algemene term. OT is een onderdeel van PA. IOT is afhankelijk van het object een onderdeel van PA of KA (denk aan HVAC of WIFI).

SCADA

Supervisory Control and Data Acquisition, is een controlesysteem dat data verzamelt, analyseert en visualiseert van OT-componenten en procesdata (PA).

SOC-analist Niveau 1

Ongeveer 0 tot 2 jaar werkervaring in een OT-/IT-analistenrol.

Niveau 1-analisten richten zich primair op basisbeveiligingsmaatregelen, zoals het monitoren van gebeurtenissen logs op verdachte activiteiten.

Als een niveau 1-analist verdachte activiteit in de gebeurtenissenlogs opmerkt, verzamelt hij of zij zoveel mogelijk informatie over de activiteit.

Vervolgens zal hij of zij het incident escaleren naar meer ervaren analisten op niveau 2.

Het kennis & kunde niveau wordt onderbouwd met 1 of meer van de volgende relevante opleiding, SOC-analisten certificering of aantoonbaar vergelijkbare certificering:

- afgeronde bachelor- of masteropleiding in Informatietechnologie, Informatica, Cybersecurity of een verwant vakgebied
- CompTIA A+
- CompTia Security+
- GIAC Security Essentials (GSEC)
- ICS/SCADA Security Essentials (ICS410)
- Essentials for NERC Critical Infrastructure Protection (OCS456)
- of een van de hierna beschreven certificeringen voor SOC-analist niveau 2 of 3

SOC-analist Niveau 2

Ongeveer 2 tot 5 jaar werkervaring in een OT-/IT-analistenrol.

Niveau 2-analisten hebben meer ervaring op het gebied van gegevensbeveiliging dan SOC-analisten van niveau 1 en gebruiken deze ervaring om meer geavanceerd werk op te pakken.

Het grootste deel van de taak van een niveau 2-analist bestaat uit incidentonderzoek na een inbreuk op de gegevensbeveiliging. Deze professionals beoordelen "de schade"; zij zullen het incident onderzoeken en bepalen in welke mate de hacker op het punt stond het systeem binnen te dringen. Als er sprake is van aanzienlijke schade aan het systeem (zoals gestolen gegevens of herschreven code), zijn niveau 2-analisten verantwoordelijk voor het oplossen van het probleem. Dit kan betekenen dat de configuratie van componenten moet worden aangepast om het beveiligingsnetwerk te herstellen, of zelfs dat er nieuwe configuratieregels moeten worden ontworpen om gaten in het systeem te dichten.

Het kennis & kunde niveau van de SOC-Analist niveau 2 wordt onderbouwd met minimaal 2 van de volgende relevante opleiding, SOC-analisten certificering of aantoonbaar vergelijkbare certificering of ervaring:

- afgeronde bachelor- of masteropleiding in Informatietechnologie, Informatica, Cybersecurity of een verwant vakgebied
- Cysa+ – Cyber Security Analyst (CompTIA)
- GCIH – GIAC Certified Incident Handler
- Kepner-Tregoe – Incident Management
- ICS515 – ICS Visibility, Detection and Response
- GICSP – GIAC Global Industrial Cyber Security Professional
- GCIA – GIAC Certified Intrusion Analyst
- of een van de hierna beschreven certificeringen voor SOC-analist niveau 3

SOC-analist Niveau 3

Ongeveer 5 tot 10 jaar werkervaring in een OT-/IT-analistenrol, vaak met gespecialiseerde certificeringen of diepgaande kennis van beveiligingsarchitecturen en -strategieën.

De niveau 3-analisten hebben als taak te leren over nieuwe beveiligingsbedreigingen om potentiële hackers een stap voor te blijven. Niveau 3-analisten zijn de meest ervaren professionals in een SOC-analyseteam.

In plaats van de huidige data- en eventlogs te monitoren, richten ze zich op het bestuderen van trends op het gebied van gegevensbeveiliging en het leren over nieuwe exploits die hackers kunnen gebruiken om het beveiligingsnetwerk van het bedrijf te doorbreken.

Bovendien besteden niveau 3-analisten tijd aan het ontwerpen van code om deze nieuwe beveiligingsbedreigingen tegen te gaan. Ze besteden ook een deel van hun tijd aan het onderzoeken van telemetriegegevens, waardoor het werk van de niveau 1-analisten een deskundige blik krijgt voor het geval ze verdachte activiteiten hebben gemist.

Het kennis & kunde niveau wordt onderbouwd met de niveau 2 certificering aangevuld met 1 of meerdere van de volgende opleiding, relevante SOC-analisten certificering of aantoonbaar vergelijkbare certificering of ervaring:

- afgeronde bachelor- of masteropleiding in Informatietechnologie, Informatica, Cybersecurity of een verwant vakgebied
- CASP – CompTIA Advanced Security Practioner

- CISSP – Certified Information Systems Security Professional
- GSP – GIAC Security Professional
- GSE – GIAC Security Expert
- CEH – Certified Ethical Hacker

Bijlagen en formulieren:

Bijlagen:

- A – Inkoopvoorwaarden AWVODI 2018
- B – e facturatie
- C – Lotingsprocedure
- D – Concept Hoofdovereenkomst
- E – Model Verwerkersovereenkomst
- F – Concept Dossier Afspraken Procedures (DAP)
- G – Concept Service level Agreement (SLA)
- H – Programma van Eisen
- I – STITCH eisen
- J – Deelnameovereenkomst
- K – Verklaring van Deelname
- L – Belangenafweging in het kader van de AVG
- M – Initiële Use Cases SOC
- N – Aansluitvoorwaarden SOC

Formulieren:

- Formulier 0 Uniform Europees Aanbestedingsdocument
- Formulier 1a Verklaring derde
- Formulier 1b Uitvoeringsverklaring onderaannemer
- Formulier 2 Rusland verklaring
- Formulier 3 Referentieproject kerncompetentie
- Formulier 4 Prijsformulier