hetWaterschapshuis
De kracht van samen

BIJLAGE H
Programma van Eisen

Ten behoeve van Europese openbare procedure voor SOC-dienstverlening “monitoring & alarmering” ten behoeve van de Waterschappen, Unie van Waterschappen en het Waterschapshuis.

Colofon

Titel: Programma van Eisen SOC-dienstverlening “Monitoring & Alarmering”
Auteur(s): / Farisha Koerban
Contactpersoon: Farisha Koerban
Vervangend contactpersoon: Tina Duinkerken
Kenmerk: Z1814
Het Waterschapshuis, 19 april 2024
Stationsplein 89, 3818 LE Amersfoort
Postbus 2180, 3800 CD Amersfoort
T: 033 460 31 00, F: 033 460 31 01
www.hetwaterschapshuis.nl, inkoop@hetwaterschapshuis.nl

Eisen 1. Algemeen	
A1.1	Inschrijver verklaart door Inschrijving zich te onthouden van gedragingen die de mededinging tussen de Inschrijvers kan beperken.
A1.2	Opdrachtnemer gaat door Inschrijving akkoord met de inhoud van alle Aanbestedingsstukken, de beoordelings-en waarderingssystematiek, de gekozen Aanbestedingsprocedure en alle bepalingen en voorbehouden die hiermee samenhangen.
A1.3	Inschrijver verklaart dat alle bij Inschrijving overlegde gegevens juist, volledig en naar waarheid zijn ingevuld en gestand worden gedaan gedurende de gehele looptijd van de Hoofdovereenkomst inclusief eventuele verlengingen.
A1.4	Opdrachtgever behoudt zich het recht voor op ontbinding van de Hoofdovereenkomst en/of een schadevergoeding in geval van onjuiste en/of onvolledige informatie en/of het niet kunnen nakomen hetgeen bij Inschrijving aangeboden is.
A1.5	Opdrachtnemer is in staat en bereid om de gevraagde dienstverlening ten behoeve van de Opdrachtgever, conform de in de Aanbestedingsstukken gestelde eisen te verzorgen.
A1.6	Opdrachtnemer handelt (aantoonbaar) conform de (Uitvoeringswet) Algemene Verordening Gegevensbescherming ((U)AVG) en aanverwante wetgeving. De Opdrachtgever behandelt alle door Opdrachtnemer verstrekte persoonsgegevens eveneens conform de in Nederland geldende Wet- en regelgeving.
A1.7	Opdrachtnemer voert alle werkzaamheden uit met inachtneming van de vigerende Nederlandse wet- en regelgeving (zoals de CSIR voor PA).
A1.8	Mondelinge communicatie van de Opdrachtnemer naar de Opdrachtgever en Deelnemers vindt plaats in de Nederlandse taal (C1; zie ook https://detaalbrigade.nl/taalniveaus/).
A1.9	(Technische) documentatie is opgesteld in de Nederlandse of Engelse taal (C1; zie ook https://detaalbrigade.nl/taalniveaus/). Documentatie wordt continu up-to-date gehouden en de laatste versie wordt actief gedeeld met hWh en Deelnemers.
A1.10	Voor het definiëren van dienstverlening, de benodigde security functies en gebruik van best practices hanteert deze uitvraag het NIST-CSF 2.0 model: - De gevraagde dienstverlening 'Monitoring & Alarmering wordt gedefinieerd conform de definitie van 'Detect en Respond' - Opdrachtnemer kan de dienstverlening formuleren en aanbieden conform het NIST-CSF model
A1.11	Opdrachtnemer levert één (1) vast aanspreekpunt voor de contractmanager van Het Waterschapshuis voor de looptijd van de Hoofdovereenkomst.
A1.12	Opdrachtnemer verplicht zich vertrouwelijk om te gaan met de informatie die in het kader van de uitvoering van deze Hoofdovereenkomst hem ter kennis komt. Het niet vertrouwelijk omgaan met deze informatie kan leiden tot een ontbinding van de Hoofdovereenkomst.
A1.13	Het Waterschapshuis heeft het recht om maximaal één (1) maal per jaar een audit te laten uitvoeren, door een externe onafhankelijke partij. Deze audit

	wordt in overleg met de Opdrachtnemer ingepland en omvat zowel bestaan als werking.
A1.14	Opdrachtnemer biedt de dienstverlening aan conform de standaard verwerkersovereenkomst van het Waterschapshuis.
A1.15	Opdrachtnemer stelt na gunning een plan van aanpak op voor implementatie van de dienstverlening, dat rekening houdt met: - Verschillen tussen individuele Deelnemers - Bestaande contracten bij Deelnemers voor monitoring en alarmeringsdiensten - een aansluitperiode van 4 jaar vanaf datum gunning waarin Deelnemers gefaseerd kunnen aansluiten
A1.16	De Opdrachtnemer borgt aantoonbaar de integriteit van haar medewerkers door hen te laten screenen door een als Particulier Onderzoeksbureau gecertificeerde organisatie. In de screenings zijn minimaal de volgende onderdelen zijn opgenomen: financiële checks, social media onderzoek, verificatie strafblad en een persoonlijk interview.
A1.17	Opdrachtnemer kan aantonen dat de dienstverlening compliant is met de minimale beveiligingseisen voor de relevante inkoop onderdelen uit de Inkoopeisen Cybersecurity Overheid (https://www.bio-overheid.nl/ico-wizard). Opdrachtnemer kan dit voor definitieve gunning van de opdracht aantonen. Minimaal zijn de volgende Inkoop-onderdelen in scope: - Algemeen Ketenpartners (voor alle percelen) - Clouddiensten (alleen voor de percelen waarbij de inschrijver clouddiensten inzet) - Softwarepakketten (alleen voor de percelen waarbij de inschrijver specifieke software inzet) - Toegangsbeveiliging (alleen voor de percelen waarbij de inschrijver diensten levert waar data van Deelnemers bij opgeslagen wordt)
A1.18	Na definitieve gunning wordt er samen met Opdrachtnemer een SLA document gemaakt en vastgesteld. In deze SLA komen minimaal de volgende onderwerpen terug: - Heldere dienstbeschrijving; - Communicatiematrix met de gegevens van de contactpersonen van Opdrachtgever en Opdrachtnemer met onderverdeling naar functies/ verantwoordelijkheden/escalatieniveau ’s - Overlegmatrix - KPI's - Evaluaties/prestatiemeting Additioneel voor specifieke security percelen: - Rapportages die geleverd worden - Technische/ functionele ondersteuning over de dienstverlening
A1.19	Opdrachtnemer voldoet aantoonbaar aan de 8 STITCH eisen (zie bijlage I-STITCH EISEN)

Eisen 2. Juridisch	
J2.1	Op deze Dienstverlening zijn de Algemene Waterschapsvoorwaarden voor het verstrekken van opdrachten tot het verrichten van diensten 2018 (AWVODI-2018) van toepassing. De algemene voorwaarden, productvoorwaarden, verkoopvoorwaarden en/of andere voorwaarden van Opdrachtnemer worden

	nadrukkelijk van de hand gewezen. In de Inschrijving wordt niet (deels) naar andere juridische voorwaarden verwezen.
J2.2	Opdrachtnemer brengt de contactpersoon van de Opdrachtgever, zodra Opdrachtnemer weet of behoort te weten dat de nakoming van de Diensten niet of niet tijdig of niet naar behoren plaatsvindt, onmiddellijk schriftelijk én telefonisch op de hoogte onder vermelding van de omstandigheden.
J2.3	Indien de Hoofdovereenkomst of Deelnameovereenkomst binnen de looptijd wordt ontbonden, om reden van een onjuiste calculatie, op grond van een onvoldoende prestatie of andere tekortkomingen die aan Opdrachtnemer kunnen worden toegerekend, is Opdrachtnemer verplicht tot vergoeding van de schade die door de annulering ontstaat. Onder schade wordt in dit verband mede verstaan het verschil tussen de met Opdrachtnemer overeengekomen prijs en de eventueel hogere prijs, verbonden aan het doen uitvoeren van de Diensten door een derde, zulks te berekenen over de nog resterende looptijd van de Hoofdovereenkomst. Indirecte- en gevolgschade zoals bedrijfsstagnatie vallen hier niet onder.
J2.4	Door het indienen van een Inschrijving maken de door Opdrachtnemer opgegeven antwoorden op de kwalitatieve sub-gunningcriteria automatisch en direct deel uit van de eisen die gesteld worden aan de uitvoering van de dienstverlening.

Eisen 3. Commercieel	
C3.1	De door Inschrijver aangeboden tarieven zijn 'all-in', dat wil zeggen inclusief (niet gelimiteerd) salariskosten, overheadkosten, kosten voor gebruik apparatuur/software/hardware (die nodig zijn bij het in het kaart brengen en oplossen van een informatieveiligheid incident), verzekeringen, reis- en verblijfskosten, reistijd, belasting, heffingen, administratieve kosten, kosten voor overleg etc.
C3.2	Verlagingen van wettelijke heffingen zoals het btw-percentage dient Opdrachtnemer te allen tijde te melden en de tarieven dienen in een dergelijk geval verplicht te worden herzien.
C3.3	Alle in de Aanbestedingsstukken en de daarbij behorende bijlagen genoemde bedragen en/of aantallen zijn indicatief. Opdrachtnemer kan aan deze bedragen en/of aantallen geen rechten in termen van (minimaal en maximaal) afzet/omzet ontlenen.

Eisen 4. Algemeen t.a.v. de Dienstverlening	
D4.1	De Opdrachtnemer kan haar SOC-analisten classificeren volgens de marktdefinities voor SOC-Analisten niveau 1, niveau 2 of niveau 3.
D4.2	De Opdrachtnemer levert 24 uur per dag bemenste SOC-dienstverlening, zogeheten 'eyes-on-screen', gedurende 7 dagen per week, m.a.w. inclusief weekenden en feestdagen.
D4.3	Het SOC, de door de Opdrachtnemer gebruikte software (o.a. SIEM) en de datacenters waar de data opgeslagen en verwerkt wordt, moeten binnen de EER gevestigd zijn (ook redundante systemen).
D4.4	Het SOC team is werkzaam en werkt binnen de EER.

D4.5	Inzage van logdata is alleen mogelijk voor Deelnemer en bevoegde medewerkers bij Opdrachtnemer, tenzij vooraf uitdrukkelijk en schriftelijk toestemming is gegeven door Deelnemer of als de rechter daar opdracht toe geeft.
D4.6	Bevoegde medewerkers: De organisatie behoort verwerkers gescheiden en beperkt toegang te verlenen tot logdata, op basis van uit te voeren activiteiten die binnen een specifieke rol worden uitgevoerd en in te trekken, indien de activiteiten, noodzaak of vastgestelde doelbinding niet meer geldt voor deze persoon of rol; de verstrekte toegang is toetsbaar.
D4.7	Het SOC-team van de Opdrachtnemer bestaat uit niveau 1 en niveau 2 SOC-analisten, waarbij het SOC-team gedurende de 24 uur per dag op elk moment bestaat uit minimaal 40% niveau 2 analisten (Definities niveau 1,2 en 3 opgenomen in integraal ontwerp).
D4.8	Het SOC-team bestaat gedurende de 24 uur per dag op elk moment uit minimaal 2 personen.
D4.9	De SOC-teamleden van de Opdrachtnemer zijn aantoonbaar gecertificeerde SOC-analisten via een marktconforme certificering (bijvoorbeeld CompTIA, SANS of ISACA, CEH, OSCP, CISSP).
D4.10	De Opdrachtnemer levert SOC-dienstverlening. Het collecteren en opslaan van de vereiste logdata is verantwoordelijkheid van de Deelnemers. Opslag van de logdata vindt plaats binnen de netwerkgrenzen van iedere individuele Deelnemer, tenzij een individuele Deelnemer anders overeenkomt met de Opdrachtnemer. Zie ook 5.4 Ontsluiting van de data ten behoeve van de SOC-dienstverlening, m.a.w. de benodigde data voor security monitoring feitelijk kunnen benutten voor deze monitoring, is verantwoordelijkheid van de Opdrachtnemer. Deelnemers zorgen dat zij voldoen aan de overeengekomen aansluitcriteria ten aanzien van het beschikbaar stellen van logdata.
D4.11	Opdrachtnemer sluit aan op de bestaande security capabilities en bestaande log analytics omgeving van Deelnemers.
D4.12	Opdrachtgever houdt een overzicht bij waarop een mapping is gemaakt van de gebruikte use cases op het Mitre ATT&CK framework, voor zowel IT als voor OT (ICS).
D4.13	Opdrachtgever analyseert proactief op afwijkingen in gedrag op zowel IT als OT-componenten, naast de gedefinieerde use cases.
D4.14	Opdrachtnemer implementeert, beheert en optimaliseert de te gebruiken security use cases en alle benodigde detectieregels. Indien een Deelnemer over een lokale SIEM-oplossing beschikt, worden de use cases ook in dit lokale SIEM geimplementeerd. Operationalisatie van deze uitrol vindt plaats in overleg met de betreffende Deelnemer. De security use cases bestaan minimaal uit: - Bescherming tegen bekende generieke aanvallen - Bescherming tegen specifieke aanvallen op Deelnemers - Bescherming tegen aanvallen die gedetecteerd zijn bij andere klanten van Opdrachtnemer en relevant zijn voor de Deelnemers
D4.15	Interne en externe dreigingsinformatie wordt continue gemonitord op relevantie voor de Deelnemers. Deze dreigingsinformatie voorziet minimaal in: - dreigingsinformatie specifiek voor de sector - dreigingsinformatie specifiek voor IT en OT landschappen - dreigingsinformatie voor andere klanten van Opdrachtnemer die ook relevant zijn voor de Deelnemers - Opdrachtnemer gebruikt deze informatie om de detectie mogelijkheden van dreigingen te verbeteren
D4.16	Opdrachtnemer heeft partnerships met diverse partijen om markt specifieke dreigingsinformatie te ontvangen, in ieder geval met het NCSC, Team Hightech Crime en OKTT.

D4.17	De Opdrachtnemer stelt op basis van de overeengekomen generieke SLA individueel met elke Deelnemer een onderliggende SLA op een stelt een dossier afspraken en procedures (DAP) op. In de specifieke SLA komen minimaal de volgende onderwerpen terug: - Overeengekomen dienstverlening en de status van deze dienstverlening - het dreigingslandschap van de Deelnemer - KPI's - Evaluaties/prestatiemeting - Rapportages die geleverd worden In het DAP komen minimaal de volgende onderwerpen terug: - Communicatiematrix met de gegevens van de contactpersonen van Opdrachtnemer en de Deelnemer met onderverdeling naar functies/ verantwoordelijkheden/escalatieniveau 's - Technische/ functionele ondersteuning over de dienstverlening - Procesafspraken t.a.v. het Incident-, Problem, Change en Configuratiemanagementproces
D4.18	Opdrachtnemer draagt zorg voor de classificatie van alarmen en maakt hierbij tenminste onderscheid in: - True Positive - False Positive - Benign Positive - Vulnerability
D4.19	Opdrachtnemer levert rapportages in een digitale vorm via een dashboard- of portalfunctie op basis van een (near) real time rapportage. Deze rapportage bevat minimaal de onderdelen: - Kwaliteit van de dienstverlening, inclusief te verwachten ontwikkelingen op korte termijn (1 kwartaal vooruit kijkend) - Incidenten - alle benodigde informatie voor sturing op incidenten (o.a. opgetreden, afgesloten en openstaand) - Waarschuwingen ter voorkoming van incidenten - Time to respond van incidenten en waarschuwingen - False positives - alle benodigde informatie voor sturing op reductie - Brondata - alle benodigde informatie voor optimalisatie van- en continuïteit in brondata aanlevering - Trends in de markt - Lifecycle Management t.a.v. use cases en detectiemechanismen - Dekkingsgraad van de security monitoring - Verbetermogelijkheden van de monitoring en response processen
D4.20	Opdrachtnemer draagt zorg voor een tijdige prioritering van- en respons op- security incidenten door melding aan de betreffende Deelnemer en het CERT-WM. Hierbij voldoet Opdrachtnemer aan de volgende richtlijn: Time to respond: - Critical (P1). - 10 min - High (P2) - 1 uur - Medium (P3) - 4 uur - Low (P4). - 16 uur *onder time to respond wordt hier verstaan: de maximale tijd tussen het (automatisch) genereren van een alarm, en het melden van een (mogelijk) incident bij de desbetreffende Deelnemer.
D4.21	De Opdrachtnemer laat minimaal één (1) maal per jaar de dienstverlening testen d.m.v. een penetratietest (PenTest), door een externe onafhankelijke partij.

D4.22	Opdrachtnemer dient op verzoek Deelnemers te kunnen ondersteunen bij het aansluiten op de SOC-dienstverlening. Dit omvat zowel de configuratie van de lokale componenten van een Deelnemer binnen haar eigen netwerkgrenzen als het aansluiten op de converged SOC-dienstverlening.
D4.23	De Opdrachtnemer verzorgt training/opleiding van (interne) medewerkers van Deelnemers voor het effectief gebruik van de dienstverlening.
D4.24	Op eerste aangeven van een Deelnemer stelt Opdrachtnemer, binnen 3 maanden, een Exit-plan op voor de Deelnemer. Het verzoek kan ook worden ingediend door Opdrachtgever voor een of meerdere Deelnemers. Het Exit-plan dient goedkeuring aan de verzoeker te worden voorgelegd.
D4.25	De Opdrachtnemer zal op verzoek van Opdrachtgever of Deelnemer de uitvoering van de Deelnemingsovereenkomst onder dezelfde condities, prijzen en tarieven voortzetten na de einddatum daarvan tot het moment dat de continuïteit van de Diensten en de uitvoering van de Hoofdovereenkomst door een andere opdrachtnemer wordt gewaarborgd (de "retransitie" periode) hetgeen uitsluitend door Opdrachtgever kan worden beoordeeld. De transitieperiode wordt gesteld op maximaal 6 (zes) maanden.
D4.26	Bij beëindiging van de Hoofdovereenkomst of beëindiging van de deelname door een Deelnemer ongeacht de reden of wijze van beëindiging, zal Opdrachtnemer aan de betrokken Deelnemer(s) alle noodzakelijke medewerking verlenen zodat de betrokken Deelnemer(s) op een soepele wijze kan (kunnen) overstappen naar een andere opdrachtnemer. Opdrachtnemer zal gedurende de retransitie alle ter hand gestelde documenten, goederen en data van een Deelnemer ter beschikking stellen aan die Deelnemer of een door die Deelnemer of Opdrachtgever aan te wijze derde, inclusief bijbehorende meta-data. Dit ter hand stellen dient te gebeuren in een gangbaar en voor Opdrachtgever/Deelnemer bruikbaar en gedocumenteerd elektronisch formaat. Opdrachtgever/Deelnemer zal de ontvangen gegevens controleren en verifiëren of de data in goede orde, dus leesbaar, bruikbaar, volledig en juist zijn. Indien de gegevens in goede orde zijn ontvangen, stuurt Opdrachtgever/Deelnemer hiervan een bevestiging aan Opdrachtnemer.
D4.27	Na ontvangst van bevestiging als hiervoor (in D4.26) bedoeld zal Opdrachtnemer overgaan tot vernietiging van onder hem bevindende gegevens, waarbij de vernietigingshandelingen gedocumenteerd zullen worden en een rapportage hiervan aan Opdrachtgever/Deelnemer ter hand gesteld zal worden. Een afwijkende afspraak kan worden gemaakt, indien daartoe aanleiding bestaat (bijv. in het kader van het eerbiedigen van een wettelijke bewaartermijn).

Eisen 5. Technisch	
T5.1	De IT-infrastructuur van de Waterschappen is sterk Microsoft georiënteerd. Alle diensten die ingezet worden voor de dienstverlening Monitoring en Alarmering moet derhalve compatibel zijn met Microsoft producten en diensten.
T5.2	Binnen de IT-infrastructuur van de Waterschappen wordt ook gebruik gemaakt van Linux systemen. Alle diensten die ingezet worden voor de dienstverlening Monitoring en Alarmering moet derhalve compatibel zijn met Linux producten en diensten.
T5.3	De Opdrachtnemer draagt zorg dat er geen hardware van de Opdrachtnemer geïnstalleerd hoeft te worden in de netwerken van de waterschappen om de SOC dienst te doen laten functioneren. Zie ook T5.4.
T5.4	De Deelnemers zijn zelf verantwoordelijk voor het verzamelen van logdata en het ter beschikking stellen van die data aan de Opdrachtnemer. Indien additionele sensoren/ systemen benodigd zijn voor het ontsluiten van benodigde logdata dan zal de betreffende Deelnemer deze aanschaffen, in gebruik nemen en beheren. Zie ook T5.3 Indien een Deelnemer de data niet zelf kan of wil verzamelen, zal de Opdrachtnemer deze taak tegen meerprijs uitvoeren voor de Deelnemer
T5.5	Als het verdienmodel van de dienstverlening gebaseerd is op de hoeveelheid te verwerken data, moeten de maandelijkse dataverbruikskosten gebaseerd zijn op de daadwerkelijk

	noodzakelijke data om monitoring effectief en efficiënt te laten zijn. Opdrachtnemer adviseert periodiek of optimalisatie mogelijk is en neemt hierin ook proactief stappen.
T5.6	De dienstverlening dient aantoonbaar 99,99% per maand beschikbaar te zijn.
T5.7	Opdrachtnemer maakt gebruik van artificial intelligence (AI) en machine learning (een specifieke subset van AI) om onbekende bedreigingen en afwijkend gedrag op te sporen.
T5.8	Opdrachtnemer dient een SOAR-platform (Security Orchestration, Automation and Respons) aan te bieden als aanvulling op de SIEM oplossing. Waarbij de randvoorwaarde geldt dat er enkel geautomatiseerd ingegrepen wordt in overeenstemming met expliciete toestemming van de betreffende Deelnemer. Dit is een toekomstbestendigheidseis.
T5.9	Het gebruik van de dienstverlening mag nagenoeg geen nadelige invloed hebben op de prestaties van de te monitoren omgeving.
T5.10	Opdrachtnemer is verantwoordelijk voor het, in afstemming met Opdrachtgever, opleveren van Playbooks t.b.v. incidentafhandeling. Deze worden beschikbaar gesteld aan alle Deelnemers.
T5.11	Opdrachtnemer moet uitwisselingsprotocollen voor dreigingsinformatie ondersteunen (zoals STIX / TAXII). Hiermee moet Opdrachtnemer in staat zijn dreigingsinformatie met de Deelnemers te delen, of van Deelnemers te ontvangen voor verdere analyse binnen de dienstverlening.
T5.12	Opdrachtnemer sluit aan op het incident response proces van individuele Deelnemers en het CERT-WM (bijvoorbeeld technische aansluiting op Topdesk, of een veilige email). Informatie-uitwisseling vindt op een veilige manier plaats.
T5.13	Opdrachtnemer dient zorg te dragen voor een alarmeringsmechanisme dat is toegespitst op de impact van een melding (bijv. sms bij een critical, mail bij een lagere prioriteit).
T5.14	Toegang voor de Deelnemers tot de oplossing en bijbehorende functionaliteit zoals dashboards of rapportages wordt ingericht volgens een Role Based Access Control Model (RBAC).
T5.15	Toegang voor Deelnemers tot het monitoringsplatform geschiedt op basis van Single-Sign-On, incl. MFA.
T5.16	De interface van het aan te bieden dashboard dient te functioneren zonder noodzaak voor het installeren van plug-ins bij gebruikers en geheel op basis van gangbare veilige technologie.
T5.17	Opdrachtnemer stelt na monitoring een baseline (=normaal gedrag van apps en netwerkverkeer) vast voor iedere Deelnemer. Voor wijzigingen in infrastructuur en inrichting bij een Deelnemer, zal een change management proces gevolgd worden.
T5.18	Opdrachtnemer detecteert afwijkingen van de baseline en signaleert dit bij de desbetreffende Deelnemer inclusief context en analyse. minimaal, maar niet uitsluitend: - lateraal verkeer tussen endpoints - a-specifiek serververkeer (DNS request naar een niet DNS-server bijv.) - scanactviteiten (bijv. nmap) - detectie op afwijkend aansturingsgedrag in OT* - detectie op toevoegen van machines in OT - detectie op internetverkeer uit OT (layer 0, 1 en 2 indien afwijkend van de baseline) - detectie op basis van configuratiehandelingen in OT (afwijkend van de baseline) zoals het uploaden en downloaden van configuraties of het aanmaken van admin accounts. Dit alles bij unencrypted communicatieverkeer! - detecteren & signaleren op onion exit (TOR) nodes - detectie van traffic flooding / DOS aanvallen
T5.19	Opdrachtnemer kan Enduser Behavior Analythics (UEBA) capabilities leveren als onderdeel van de dienstverlening.
T5.20	Opdrachtnemer voert (waar gewenst) threat hunting uit op het digitale landschap van de waterschappen als onderdeel van de overeenkomst.
T5.21	Opdrachtnemer adviseert Opdrachtgever continu over het toevoegen van security sensoren of het her-configureren van systemen in de Deelnemer's (IT-/ OT-) infrastructuur om blinde vlekken in de security monitoring te adresseren.
T5.22	Opdrachtnemer heeft de mogelijkheid om eventuele output te gebruiken van vulnerability management, configuratie management en risk management processen van de

	waterschappen in de dienstverlening om de detectie mogelijkheden van dreigingen en incidenten te verbeteren.
T5.23	De SOC-dienst dienstverlening wordt door de Opdrachtgever flexibel aangeboden, dat wil zeggen: Uitbreidbaar wanneer het IT-/ OT-landschap van de Opdrachtgever groeit of migreert (on-prem naar Cloud bijv) of wanneer er (nieuwe) bronnen bij komen of worden vervangen.
T5.24	Opdrachtnemer geeft in de aanbieding aan in hoeverre zij de logdata, die wordt gegenereerd door producten en diensten in gebruik bij de Deelnemers, kunnen opnemen in de dienstverlening.
T5.25	De standaard retentietijd van log- en eventdata en het auditlog is minimaal cf. wet- en regelgeving. Op basis van de BIO geldt een retentietijd van minimaal 6 maanden. Opdrachtnemer zorgt er ook voor dat informatie over security incidenten en betrokken data niet verloren gaan, hiertoe zijn aantoonbaar afdoende maatregelen genomen om verlies van informatie te voorkomen.
T5.26	Indien een Deelnemer gebruik maakt van de optie om de log – en event data op te slaan bij Opdrachtnemer, wordt deze zodanig opgeslagen dat de beschikbaarheid, integriteit en vertrouwelijkheid gegarandeerd is, deze gedeeld kan worden voor analyse van historische data (forensisch en post-mortem) en als bewijsmateriaal gebruikt kan worden in strafzaken.
T5.27	Indien een Deelnemer gebruik maakt van de optie om de log – en event data op te slaan bij Opdrachtnemer, dienen analyse danwel delen van de (eigen) log- en eventdata geëxporteerd te kunnen worden voor archivering buiten de systemen van de Opdrachtnemer.
T5.28	De dienstverlening moet in staat zijn om de event tijd te corrigeren voor systemen met een onjuiste tijdaanduiding, bijvoorbeeld door een foutieve tijdzone instelling. De integriteit van de timestamp moet gegarandeerd blijven.
T5.29	Log- en eventdata met een onjuiste tijdsaanduiding moet worden gesignaleerd als incident.
T5.30	Normaliseren van de door Deelnemers aangeleverde logging aan de Opdrachtnemer, is een verantwoordelijkheid van de Opdrachtnemer.
T5.31	Indien een Deelnemer gebruik maakt van de optie om de log – en event data op te slaan bij Opdrachtnemer, dient deze op een veilige en versleutelde wijze verzonden te kunnen worden naar de Opdrachtnemer.
T5.32	De Opdrachtnemer is in staat om een netwerkvisualisatie op te leveren op basis van de ontsloten logdata.
T5.33	Opdrachtnemer zal als onderdeel van de dienstverlening op zowel IT als op OT data Deep Packet Inspection (DPI) analyse uitvoeren.

Eisen 6. Geschiktheid	
G6.1	De Opdrachtnemer heeft minimaal 3 jaar ervaring bij Opdrachtgevers met de Baseline Informatiebeveiliging Overheid (BIO).
G6.2	De Opdrachtnemer heeft minimaal 3 jaar ervaring bij Opdrachtgevers met IEC 62443. De Opdrachtnemer heeft minimaal 3 jaar ervaring bij Opdrachtgevers met IEC 62443.
G6.3	De Opdrachtnemer is gecertificeerd conform ISO27001 (of gelijkwaardig), waarbij SOC-dienstverlening binnen het toepassingsbereik valt.
G6.4	De Opdrachtnemer is gecertificeerd conform ISO27017 (of gelijkwaardig), waarbij SOC-dienstverlening binnen het toepassingsbereik valt.
G6.5	De Opdrachtnemer is gecertificeerd conform ISO9001 (of gelijkwaardig), waarbij SOC-dienstverlening binnen het toepassingsbereik valt.
G6.6	De Opdrachtnemer is in bezit van een ISEA3402 Type 2 verklaring, SOC2 verklaring of een ander gelijkwaardig certificaat, waarbij SOC-dienstverlening binnen het toepassingsbereik valt.
G6.7	Opdrachtnemer levert de dienst vanuit een 'converged OT & IT SOC'. 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 Deelnemers beschermt, waarbij: a. 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; b. 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 c. Zowel met de bescherming van de OT als IT kant van de organisatie rekening wordt gehouden, om beveiligingsproblemen adequaat en snel op te lossen.
G6.8	De Opdrachtnemer heeft minimaal 3 jaar aaneengesloten ervaring, bij 1 Opdrachtgever, met converged OT/IT SOC-dienstverlening, waarbij de OT-installaties van eenzelfde categorie zijn als die van Waterschappen.
G6.9	Opdrachtnemer dient meerjarige ervaring en kennis te hebben met het verzamelen van informatie uit OT netwerken. De dienstverlening dient o.a. deze OT protocollen te kunnen analyseren (zoals, maar niet beperkt tot: ModBus, Profinet, ProfiBus, S7, Ethernet/IP, HART, AMQP, Bluetooth, CAN en BACNet). Daarnaast dient de SOC-analist dit verkeer te begrijpen om deze afdoende te kunnen analyseren. Intelligentie uit OT omgevingen kan worden gecorreleerd met informatie uit de Email, IT en SaaS omgeving als één samenwerkend platform en in één unified-view, waardoor dreigingen die zich verspreiden vanuit de KA/SaaS naar de PA/IA omgeving inzichtelijk worden en tijdig gestopt kunnen worden.

Eisen 7. Privacy	
PR7.1	Opdrachtnemer zal de toegang en de autorisaties die zijn verleend ten behoeve van de uitvoering van de dienst(en) enkel voor die doeleinden gebruiken en niet voor enig ander doeleinde.
PR7.2	Privacyverklaring: De organisatie heeft een privacyverklaring waarin is beschreven op welke wijze persoonsgegevens worden verwerkt en hoe een betrokkene, zijn of haar rechten kan uitoefenen.
PR7.3	Opdrachtnemer draagt er zorg voor dat bij de uitvoering van de werkzaamheden niet meer persoonsgegevens of andere gevoelige gegevens worden ingezien of anderszins verwerkt dan werkelijk noodzakelijk voor het correct uitvoeren van de Opdracht.
PR7.4	Privacybeleid: De organisatie heeft privacybeleid en procedures ontwikkeld en vastgesteld, waarin de verantwoordelijkheid is vastgelegd op welke wijze persoonsgegevens worden verwerkt, invulling wordt gegeven aan de wettelijke beginselen en hoe in een cyclisch proces wordt vastgelegd op welke wijze transparant aan de wet- en regelgeving wordt voldaan en afwijkingen worden opgelost.
PR7.5	Privacy-organisatie: De verdeling van de taken en verantwoordelijkheden, de benodigde middelen en de rapportagelijnen, zijn door de organisatie vastgelegd en vastgesteld, inclusief die bij uitwisseling van persoonsgegevens tussen organisaties, zodat ook bij doorgifte van persoonsgegevens de privacybelangen van de betrokkenen, waarvan de persoonsgegevens worden verwerkt, zijn gewaarborgd.
PR7.6	Privacy-bewustzijn: De organisatie waarborgt dat eenieder die persoonsgegevens verwerkt of een verwerking voorbereidt zich bewust is van

	de belangen van de betrokkenen, waarvan de persoonsgegevens worden verwerkt, en beschouwt dit conform de verwachtingen als hoogste prioriteit om deze overtuiging toe te passen; deze betrokkenen hebben daarvoor de benodigde kennis en zijn op de hoogte van grote veranderingen in de verwachtingen.
PR7.7	Formele vastlegging handelen verwerkingsverantwoordelijke: De organisatie heeft van eenieder, die persoonsgegevens verwerkt of een verwerking voorbereidt, een actuele VOG, een actuele verklaring terzake het naleven en de kennisname van de regels omtrent privacy en het bewijs van op de hoogte zijn van de disciplinaire procedure; hiervan bestaat een overzicht.
PR7.8	Privacy in de levenscyclus: Vooraf aan het ontwerp van een gegevensverwerking en bij een verandering wordt een inschatting gemaakt van de privacy-risico's en wordt bepaald welke passende maatregelen nodig zijn; hiervoor zijn de verantwoordelijkheden duidelijk en is een proces ingeregeld voor het kunnen aantonen van het passend zijn van deze maatregelen.
PR7.9	Register van verwerkingsactiviteiten: De verwerkingsverantwoordelijke(n) en de verwerker(s) hebben hun gegevens over de gegevensverwerkingen in een register vastgelegd, daarbij biedt het register een actueel en samenhangend beeld van de gegevensverwerkingen, processen en technische systemen die betrokken zijn bij het verzamelen, verwerken en doorgeven van persoonsgegevens en dat voldoet aan de vereisten van de AVG.
PR7.10	Datalekken: De organisatie heeft de kennis georganiseerd om de oorzaak van een datalek te kunnen vaststellen en te onderzoeken, heeft daarvoor de benodigde loggegevens om herhaling te voorkomen en heeft de stakeholders vastgesteld om ze te kunnen informeren.
PR7.11	Datalekken: Opdrachtnemer meldt binnen 24 uur na ontdekken van datalek aan Opdrachtgever/Deelnemer dat er een datalek heeft plaatsgevonden waarbij persoonsgegevens van Opdrachtgever/Deelnemer betrokken zijn.
PR7.12	Doelbinding op rolniveau: De organisatie behoort verwerkers gescheiden en beperkt toegang te verlenen tot persoonsgegevens, op basis van uit te voeren activiteiten die binnen een specifieke rol worden uitgevoerd en in te trekken, indien de activiteiten, noodzaak of vastgestelde doelbinding niet meer geldt voor deze persoon of rol; de verstrekte toegang is toetsbaar.
PR7.13	Toegang op taakniveau: Het verlenen van toegang tot persoonsgegevens wordt beperkt op basis van duidelijke en afgebakende taken en het doel en de verstrekte toegang is toetsbaar.
PR7.14	Logging en monitoring uitgeven toegangsrechten: De verwerking behoort op verwerkers/persoonsniveau te loggen, zodat direct of periodiek kan worden beoordeeld welke persoonsgegevens de medewerker heeft opgevraagd, ingezien en aangepast.
PR7.15	Opdrachtnemer zal bij de uitvoering van de Diensten alle noodzakelijke zorg betrachten om te vermijden dat (nader) forensisch onderzoek niet goed meer kan worden uitgevoerd of de resultaten daarvan niet goed (meer) zouden kunnen worden vertrouwd.
PR7.16	Indien de Dienst bestaat uit het uitvoeren van forensisch (digitaal) onderzoek, zal Opdrachtnemer zorgdragen voor het aantoonbaar maken van de bevindingen om als bewijsmateriaal te kunnen dienen in strafrechtelijke of civielrechtelijke rechtszaken en op een voor dat doeleinde deugdelijke en betrouwbare wijze bijhouden wie op ieder moment toegang had tot of beschikking had over het bewijsmateriaal ('chain of custody').
PR7.17	Na afloop van een incident zal Opdrachtnemer alle gegevens over Deelnemer, diens werknemers of overige relaties die Opdrachtnemer heeft verwerkt, vernietigen of terug leveren aan Deelnemer, met uitzondering van gegevens die (a) Opdrachtnemer nodig heeft om zich gereed te houden om bij een volgend

	incident zo snel en effectief mogelijk op te treden en (b) Opdrachtnemer op grond van de wet verplicht is te bewaren. Op verzoek van Deelnemer verstrekt Opdrachtnemer inzage in de gegevens die Opdrachtnemer bewaart om zich gereed te houden om bij een volgend incident zo snel en effectief mogelijk op te treden. Voor zover Opdrachtnemer verplicht is om na afloop van de opdracht dergelijke gegevens te bewaren, zal Opdrachtnemer Deelnemer deugdelijk informeren over welke (categorieën) gegevens bewaard moeten worden en op grond van welke specifieke wettelijke verplichtingen.
PR7.18	Opdrachtnemer dient aan te tonen dat hij passende technische en organisatorische beveiligingsmaatregelen heeft geïmplementeerd om persoonsgegevens en andere gevoelige gegevens van (medewerkers, klanten of andere relaties van) Opdrachtgever/Deelnemer te kunnen verwerken.
PR7.19	De organisatie waarborgt dat eenieder die persoonsgegevens verwerkt of een verwerking voorbereidt zich bewust is van de belangen van de betrokkenen, waarvan de persoonsgegevens worden verwerkt, en beschouwt dit conform de verwachtingen als hoogste prioriteit om deze overtuiging toe te passen; deze betrokkenen hebben daarvoor de benodigde kennis en zijn op de hoogte van grote veranderingen in de verwachtingen.
PR7.20	Vertrouwelijkheid/Integriteit: Opdrachtnemer zal bij de uitvoering van de Diensten geen handelingen verrichten die de vertrouwelijkheid, integriteit en/of beschikbaarheid van de systemen van Deelnemer(s) en/of de daarop verwerkte gegevens in gevaar kan brengen.
PR7.21	DPIA (data protection impact assessment): Inschrijver kan een actuele DPIA overleggen op de SOC-dienst waarin: • Minimaal wordt beschreven welke risico's en kwetsbaarheden voor de vrijheden en rechten van betrokkenen bij de verwerking verwacht worden/ontstaan. • Welke maatregelen kunnen worden genomen om bovengenoemde risico's en kwetsbaarheden te mitigeren. • De DPIA dient minimaal 1 keer per jaar te worden her beoordeeld. De DPIA dient minimaal 1 keer per 3 jaar te worden herhaald.
PR7.22	Inschrijver kan aantonen de maatregelen benoemd in de eigen DPIA te hebben geïmplementeerd.
PR7.23	Inschrijver zal kosteloos meewerken aan de uit te voeren DPIA door Deelnemers.
PR7.24	Inschrijver zal kosteloos meewerken aan de uit te voeren IAMA door Deelnemers.

Eisen 8. Bereikbaarheid	
B8.1	Opdrachtnemer beschikt over een primair aanspreekpunt voor administratieve, - en contractzaken, dat op werkdagen beschikbaar is tussen 08.30 en 17.00 Nederlandse tijd.

Eisen 9. Facturatie	
F9.1	Onder vermelding van de Raamovereenkomst verzendt Opdrachtnemer na volledige verrichting en acceptatie een factuur per uitgebrachte offerte met betrekking tot de werkzaamheden.
F9.2	Facturen dienen te voldoen aan de wettelijke vereisten (zie www.belastingdienst.nl). Een factuur bevat minimaal de volgende gegevens: Gegevens Opdrachtnemer · Bedrijfsnaam · Adres · Telefoonnummer · KvK-nummer · Btw-nummer · IBAN-rekeningnummer · Debiteurnummer Gegevens de Aanbestedende dienst · Organisatienaam · Adres · Contractnummer Factuur gegevens · Factuurdatum · Factuurnummer · Ordernummer · Periode waar de factuur betrekking op heeft · Totaal factuurbedrag exclusief btw · Btw-percentage · Btw-bedrag factuur · Totaal factuurbedrag inclusief btw · Btw-nummer
F9.3	Een kostenoverzichten bevat minimaal de volgende gegevens: • Factuurdatum • Factuurnummer • Ordernummer • Periode waar de factuur/kostenoverzicht betrekking op heeft • Naam van de opdrachtverstrekker (indien van toepassing) • Prijs per onderdeel zoals opgenomen in het prijzenblad (of de offerte in het geval van aanvullende werkzaamheden) • Aantal per onderdeel zoals opgenomen in het prijzenblad (of de offerte in het geval van aanvullende werkzaamheden) • Totaal kosten (incl. en excl. btw) • In het geval van aanvullende werkzaamheden een kopie van de door de Deelnemer goedgekeurde offerte • Naam en telefoonnummer contactpersoon Opdrachtnemer
F9.4	Indien een factuur niet voldoet aan de in de Overeenkomst genoemde voorwaarden wordt de Opdrachtnemer hiervan binnen 30 kalenderdagen na ontvangst schriftelijk op de hoogte gebracht. De betreffende factuur wordt pas in behandeling genomen op het moment dat deze voldoet aan de in de Overeenkomstgenoemde voorwaarden.

F9.5	De Deelnemer is gerechtigd om indien er sprake is van door Opdrachtnemer verschuldigde bedragen (crediteringen) deze te verrekenen met bedragen die Opdrachtnemer verschuldigd is aan de Deelnemer.
F9.6	Indien de Deelnemer niet tijdig betaalt en de vertraging niet te wijten is aan Opdrachtnemer, kan Opdrachtnemer aanspraak maken op de wettelijke rente van het bedrag, met de betaling waarvan de Deelnemer in gebreke is, met ingang van de dag, volgend op die, waarop de betaling uiterlijk diende te geschieden. Rente van rente kan Opdrachtnemer niet vorderen.
F9.7	De kosten van het accountantsonderzoek komen voor rekening van de Opdrachtgever of Deelnemer, tenzij uit het onderzoek van de accountant blijkt dat de factu(u)r(en) niet juist dan wel onvolledig is/zijn, in welk geval bedoelde kosten voor rekening van Opdrachtnemer komen.

Eisen 10. Personeel	
P10.1	Opdrachtnemer beschikt over voldoende medewerkers om de Diensten conform de Aanbestedingsstukken uit te voeren.
P10.2	Opdrachtnemer ziet erop toe dat de uitvoering van de Dienstverlening ongestoord voortgang vindt en conform de daaraan gestelde eisen wordt uitgevoerd. Opdrachtnemer draagt er zorg voor dat de voortgang niet door o.a. ziekte, vakantie of andere redenen van afwezigheid van haar medewerkers wordt onderbroken. Opdrachtnemer neemt in voorkomende gevallen onverwijld de nodige maatregelen tot het doen van de vereiste voorzieningen c.q. inzet van vervangend gelijkwaardig personeel (zowel qua werk- en denkniveau als aantoonbare relevante werkervaring).
P10.3	Alle medewerkers van en namens Opdrachtnemer welke in een gebouw van de Deelnemer komen houden zich aan de geldende huisregels en kunnen zich op verzoek legitimeren.
P1404	Opdrachtnemer verklaart dat alle medewerkers welke gedurende de looptijd van de Raamovereenkomst bij Opdrachtnemer in dienst zijn aan alle wettelijke voorschriften voldoen van het land (of de landen) waar de medewerker gecontracteerd en werkzaam is. Opdrachtnemer is volledig verantwoordelijk voor het naleven van de wet- en regelgeving met betrekking tot aanstelling, tewerkstelling, betrouwbaarheid, gedrag en andere relevante zaken met betrekking tot haar medewerkers.
P10.5	De Opdrachtgever kan nimmer aansprakelijk gesteld worden voor het inlenen van illegale werknemers. De door de overheid aan de Opdrachtgever opgelegde boetes zullen worden vergoed door Opdrachtnemer.
P10.6	Indien de Opdrachtgever niet tevreden is over de inzet van een medewerker van Opdrachtnemer kan de Opdrachtgever verzoeken om vervanging van de desbetreffende medewerker. De Opdrachtgever zal tijdig Opdrachtnemer op de hoogte stellen en zal geen vervanging eisen op basis van ongegronde redenen.