Algemene informatie

Aanbesteding:	Aanbesteding SOC - monitoring en alarmering - versie 2
Aanbestedende Dienst:	Het Waterschapshuis
Referentie:	Z1820

Toelichting:

Vraag en antwoord

Ref.nr. 1

Onderwerp:
Prijsformulier

Vraag:
Graag ontvangen wij een nadere toelichting hoe het Waterschapshuis het prijzenblad heeft opgebouwd en hoe de diverse onderdelen met elkaar samenhangen.

Antwoord:
Uit de marktconsultatie is gebleken dat leveranciers verschillende prijsmodellen hanteren voor de SOC-dienstverlening. Dit varieert van abonnementsvorm tot prijs per medewerker en/ of combinaties daarvan. Op basis hiervan en op basis van onze inkoopbehoefte hebben wij dit prijzenblad samengesteld. Zie voor een uitgebreide toelichting paragraaf 6.1 van de Aanbestedingsleidraad. De prijscomponenten zoals opgenomen in het prijzenblad dienen ingevuld te worden door inschrijver met dien voorstande dat het ook voldoet aan alle eisen en voorwaarden uit paragraaf 6.1 van Aanbestedingsleidraad.

Percelen:	P1 SOC dienstverlening Monitoring en Alarmering
Beantwoord op:	22 jul. 2024

Ref.nr. 2

Onderwerp:
Data

Vraag:
De hoeveelheden te analyseren data kunnen per logbron sterk variëren. Bijvoorbeeld een Netwerk flow monitoring tool in PA, geeft veel minder logs /alerts dan een Firewall. In het prijs formulier stelt u voor 1 prijs te hanteren voor logbronnen (één voor PA en en één voor KA logbronnen). Om dit te vertalen in de door het Waterschapshuis gevraagde prijsmodel, vragen wij u inzicht te geven in de samenstelling van de logbronnen. Indien het Waterschapshuis dit niet wenst te doen, dan stellen wij voor een aantal referentiebronnen te definiëren op basis waarvan gegadigden hun prijs bepalen en het Waterschapshuis een juist vergelijk tussen de gegadigden kan

maken.

Antwoord:
De hoeveelheid data per 24 uur verschilt per waterschap. Op basis van indicatoren die gebruikt worden om de omvang van een waterschap vast te stellen is de indeling gemaakt in klein, middel, groot zoals in het prijzenblad vermeld. De inschatting van de gemiddelde datastroom per 24 uur vanuit KA en PA binnen het waterschap (hoeveel data die richting Opdrachtnemer gaat is uiteraard geringer maar nu niet bekend) is vastgesteld op basis van:
• KA indicatoren, zoals servers, domein controllers, AD/Entra-ID, Linux, Syslog, Firewalls, Switches en externe koppelvlakken.
• PA indicatoren, IT componenten in PA, PLC's, HMI's , netwerk gekoppelde componenten en uitgebreid loggende componenten (SCADA, Historians, etc.)
Totale logdata binnen een waterschap wordt op basis hiervan geschat op:
• Klein: 90 GB
• Middel: 105
• groot: 115
Een Deelnemer is zelf verantwoordelijk om deze data te collecteren en gecentraliseerd ter beschikking te stellen van de dienst. Indien er hulp nodig is bij het collecteren en gecentraliseerd ter beschikking stellen, kan deze hulp als separate consultancy dienst worden afgenomen door de betreffende Deelnemer.

Percelen: P1 SOC dienstverlening Monitoring en Alarmering
Beantwoord op: 22 jul. 2024

Ref.nr. 3

Onderwerp:
Sentinel

Vraag:
Welke waterschappen hebben al Sentinel draaien en wat is de usage/log ingestion (GB per day)?

Antwoord:
Na het gunnen van de opdracht kan een overzicht worden vertrekt van de actuele situatie per waterschap. Sentinel is uitgerold en kan door alle waterschappen worden gebruikt. Een aantal heeft echter lopende contracten en gebruikt nog een andere SIEM oplossing in de praktijk. In de Sentinel uitrol zijn op dit moment de O365 en Azure logging geïmplementeerd.
Het aantal GB per 24 uur in Sentinel is momenteel niet representatief te noemen. Zie antwoord 2 voor hoeveelheden data per 24 uur.

Percelen: P1 SOC dienstverlening Monitoring en Alarmering
Beantwoord op: 22 jul. 2024

Ref.nr. 4

Onderwerp:
Certificering

Vraag:
U geeft in de leidraad op pagina 7 aan dat de eisen in het PvE uitvoeringseisen betreffen, echter vraagt u wel in deze fase al aantoonbaar te maken dat Inschrijver certificeringen kan overleggen van haar medewerkers. Inschrijver heeft een opleidingsplan klaar liggen en verwacht in de loop van dit jaar de eerste certificaten te kunnen overleggen. Kan AD ermee akkoord gaan dat Inschrijver de kennis van haar SOC analisten op een andere manier onderbouwd?

Antwoord:
De certificering van SOC-analisten betreft een geschiktheidseis. De SOC-analisten dienen aan de certificeringeisen te voldoen op het moment van inschrijving. In de aanbestedingsleidraad hoofdstuk 4.4.2 is dit onderwerp in meer detail beschreven.

Percelen: P1 SOC dienstverlening Monitoring en Alarmering
Beantwoord op: 22 jul. 2024

Ref.nr. 5

Onderwerp:
BIO

Vraag:
De oude vragen 5, 38, 39 en 69 komen houden kort samengevat in of de IEC 62443, respectievelijk BIO al dan niet nadrukkelijk in de contractvoorwaarden moeten zijn vermeld.

Antwoord:
De relativering in het antwoord op de oude vraag 38 is leidend. Dit betekent dat voldaan aan de eis indien bij de uitvoering van de opdracht IEC 62443, respectievelijk BIO in acht moet worden genomen, ook als dit niet nadrukkelijk in de overeenkomst is bepaald.

Percelen: P1 SOC dienstverlening Monitoring en Alarmering
Beantwoord op: 22 jul. 2024

Ref.nr. 6

Onderwerp:
Marktconsultatie

Vraag:
In vraag 28 van de NvI 2024-05-24 verwijst u naar de marktconsultatie. Kunt u het verslag van de marktconsultatie ter beschikking stellen ?

Antwoord:
Het verslag van de marktconsultatie wordt bij dit antwoord gepubliceerd op Tenderned. Het verslag maakt geen deel uit van de Overeenkomst of de Aanbestedingsstukken.

Percelen: P1 SOC dienstverlening Monitoring en Alarmering
Beantwoord op: 22 jul. 2024

Ref.nr.
7

Onderwerp:
4.4.2 Beroepsbekwaamheid

Vraag:
U vraagt met Kerncompetentie 2 specifiek om de BIO. Kunt u aangeven of certificering op ISO27001 voldoende is?

Antwoord:
Nee, dat is niet voldoende. ISO27001 betreft een managementsysteem. De BIO geeft een basisniveau voor informatiebeveiliging en stelt aan verschillende beheersmaatregelen aanvullende eisen. Daarnaast geldt de BIO specifiek voor alle Nederlandse overheidsorganisaties en aan de overheid gelieerde organisaties.

Percelen: P1 SOC dienstverlening Monitoring en Alarmering
Beantwoord op: 13 aug. 2024

Ref.nr.
9

Onderwerp:
Leidraad 4.4.2 Technische en beroepsbekwaamheid - kerncompetentie 2

Vraag:
De BIO wordt door overheden standaard als uitvoerings- en/of gunningseis opgenomen in aanvragen, maar het maakt geen onderdeel uit van het contract. Is onze aanname juist, dat als wij een referentie overleggen bij een overheid die moet voldoen aan de BIO, wij hiermee voldoen aan kerncompetentie 2? Zo nee, hoe kan inschrijver dan aantonen diensten te verlenen waarop de BIO van toepassing is?

Antwoord:
Indien bij de uitvoering van een referentieopdracht de BIO in acht dient te worden genomen en dus te worden toegepast, dan wordt voldaan aan de eis. Dat brengt met zich mee dat indien in een referentie opdracht IT diensten zijn verricht bij een opdrachtgever die moet voldoen aan de BIO, deze IT diensten eveneens moeten voldoen aan de BIO. Leidend is dat de BIO bij de uitvoering van de referentieopdracht van toepassing is (geweest). De referent moet dat kunnen bevestigen.

Percelen: P1 SOC dienstverlening Monitoring en Alarmering
Beantwoord op: 13 aug. 2024

Ref.nr. 10

Onderwerp:
Leidraad 4.4.2 Technische en beroepsbekwaamheid - kerncompetentie 3

Vraag:
Bij kerncompetentie 3 vraagt hWh aantoonbare ervaring met het IEC62443 framework. Veel van onze IT/OT-klanten werken met dit framework, maar is het geen onderdeel van het contract. Over het algemeen wordt ervaring met het IEC62443 framework gezien als een uitvoeringsvoorwaarde (veelal als eis/voorwaarde in de aanvraag). Is het voldoende als onze referenties bevestigen dat wij bewezen ervaring hebben met dit Framework? Zo nee, hoe kan inschrijver dan aantonen te beschikken over IEC62443 kennis?

Antwoord:
Indien bij de uitvoering van een referentieopdracht de IEC62443 in acht dient te worden genomen en dus te worden toegepast, dan wordt voldaan aan de eis. Leidend is dat de IEC62443 bij de uitvoering van de referentieopdracht van toepassing is (geweest). De referent moet dat kunnen bevestigen.

Percelen: P1 SOC dienstverlening Monitoring en Alarmering
Beantwoord op: 13 aug. 2024

Ref.nr. 11

Onderwerp:
Leidraad 6.1 Prijs - 3. Prijs implementatiekosten

Vraag:
Om de kwaliteit van de monitoring te kunnen waarborgen is de kwaliteit van de aan te sluiten logbronnen van belang. U geeft aan dat de deelnemers verantwoordelijk zijn voor de kwaliteit van de aan te sluiten logbronnen. Wij zien in de praktijk veelvuldig dat de kwaliteit van logbronnen sterk varieert. Welk proces hebben de deelnemers of het Waterschapshuis om de kwaliteit samen met de inschrijver te borgen indien blijkt dat een logbron niet de juiste kwaliteit biedt?

Antwoord:
Het is een expliciete keuze van de waterschappen om logmanagement zelf in te richten of te behouden (als het al is ingericht). In de aansluiteisen voor de waterschappen op de toekomstige SOC-dienstverlening is opgenomen dat zij logmanagement hebben ingericht. In de 3 maanden voordat een waterschap op de dienstverlening wordt aangesloten, starten we vanuit het Waterschapshuis met het ‘aansluit gereed maken’ van een waterschap. Hierbij is logmanagement een belangrijk onderdeel, waarin we volledigheid, juistheid en tijdigheid van logbronnen bespreken en controleren. De

inrichting van logbron-monitoring en het garanderen van een read-only opslag van deze data is daar een onderdeel van. Via het bewust maken van het belang van de logdata, daar waar nodig en het inrichten van logbronmonitoring inclusief de opvolging bij alarmeringen, is het uitgangspunt dat waterschappen in basis klaar staan om de vereiste kwaliteit van logdata te garanderen. Daarnaast zal het Waterschapshuis een service delivery rol vervullen en bewaken dat de voor beide zijden overeengekomen afspraken na worden geleefd.

Percelen: P1 SOC dienstverlening Monitoring en Alarmering
Beantwoord op: 13 aug. 2024

Ref.nr.
12

Onderwerp:
Leidraad 4.4.2 Technische en beroepsbekwaamheid - technische bekwaamheid 2

Vraag:
U vraagt o.a. 'De voor- en achternaam van elke SOC-analist'. Wij achten het niet proportioneel dat gevraagd wordt om van al onze analisten de gegevens te verstrekken. Enerzijds omdat niet alle analisten zullen werken voor hWh en de hun gegevens dus geen betrekking hebben op of relatie hebben tot de opdracht. Maar belangrijker, veel van onze medewerkers kiezen er juist voor om gegevens niet openbaar te delen gezien de aard van hun werkzaamheden. Wij delen derhalve het door u gestelde in bijlage L niet.

Wij stellen voor dat wij naast de (reeds in de eerste aanbesteding verstrekte) aantallen, de gegevens van de drie sleutelfiguren voor de toelichting verstrekken. Eventueel aangevuld met de gegevens van enkele andere cruciale rollen binnen ons SOC. Indien hWh hierin niet wenst mee te gaan, graag een nadere toelichting (anders dan bijlage L) waarom zij het proportioneel acht om de gegevens van al onze medewerkers op te vragen.

Antwoord:
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.

Percelen: P1 SOC dienstverlening Monitoring en Alarmering
Beantwoord op: 13 aug. 2024

Ref.nr. 13

Onderwerp:
Leidraad 6.3 Toelichting offerte door twee functionarissen

Vraag:
Is het met het oog op de vakantieperiode mogelijk om de toelichting een week eerder te plannen?

Antwoord:
Nee, dat is niet mogelijk, gelet inschrijftermijn.

Percelen: P1 SOC dienstverlening Monitoring en Alarmering
Beantwoord op: 13 aug. 2024

Ref.nr. 15

Onderwerp:
Aanbestedingsleidraad p.16

Vraag:
Wij hebben een vraag over de certificeringsvereisten van SOC analisten. Naast de analisten trainingen als SANS en COMPTIA en ons eigen opleidingsprogramma volgen onze analisten ook trainingen van leveranciers die gericht zijn op SOC analytische vaardigheden, denk hierbij aan Threat Hunting trainingen van Microsoft en Red Team Blue Team trainingen van Palo Alto Networks. Kan hWh aangeven hoe zij dergelijke trainingen gaat evalueren in het kader van de Technische bekwaamheid 2?

Antwoord:
Het kennis & kunde niveau wordt onderbouwd met de relevante SOC-analisten certificering zoals aangeven in de "Begripsbepalingen m.b.t. dienstverlening" van de Aanbestedingsleidraad óf met aantoonbaar vergelijkbare certificeringen. Het is aan de Inschrijver om inzichtelijk te maken dat de de onderwerpen/inhoud van de betreffende trainingen van leveranciers overeenkomt met de in de definities voor het betreffende niveau SOC-analisten genoemde certificeringen.

Percelen: P1 SOC dienstverlening Monitoring en Alarmering
Beantwoord op: 13 aug. 2024

Ref.nr. 16

Onderwerp:
Aanbestedingsleidraad p.30 (4.5.1)

Vraag:
hWh geeft het volgende aan: "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." Wij begrijpen dat het een harde eis is vanuit Europese aanbestedingsregels dat een UEA altijd rechtsgeldig ondertekend dient te worden. Kunt u bevestigen dat het rechtsgeldig ondertekenen van de UEA ook in deze fase een verplichting is?

Antwoord:
"De vraag is onbegrijpelijk. De geciteerde tekst uit § 4.5.1 van de Aanbestedingsleidraad stelt dat het, in lijn met artikel 2 lid 2 van het Aanbestedingsbesluit, niet vereist is om het UEA rechtsgeldig te ondertekenen. Desalniettemin staat het inschrijver vrij om het UEA rechtsgeldig te ondertekenen.

Percelen: P1 SOC dienstverlening Monitoring en Alarmering
Beantwoord op: 13 aug. 2024

Ref.nr. 17
Onderwerp: Aanbestedingsleidraad p.30 (6.3)

Vraag:
"hWh wenst zelf een keuze te maken voor de SOC analyst die men wenst te spreken. Hier hebben wij een vraag over:
Ivm vakantie kan het dat de geselecteerde analist niet beschikbaar is. Is het akkoord als de Aanbieder een paar L2/L3 analisten voorstelt en hWh daar de keuze uit maakt?"

Antwoord:
Nee, het gevraagde is niet akkoord.

Percelen: P1 SOC dienstverlening Monitoring en Alarmering
Beantwoord op: 13 aug. 2024

Ref.nr. 18
Onderwerp: Aanbestedingsleidraad p.30 (6.3)

Vraag:
hWh wenst zelf een keuze te maken voor de SOC analist die men wenst te spreken. Hier hebben wij een vraag over. Wij werken met de rol van Technical Delivery Manager (TDM). Dat is een ervaren analist die altijd het contact met de klant heeft over incidenten en andere operationele zaken. Voor een goed beeld van de te verwachten dienstverlening, procedures, kennisniveau en werkwijze is het van belang dat een TDM aanwezig is bij de presentatie. Is het akkoord als wij aangeven welke analisten een TDM rol vervullen en dat hWh hier een keuze uit maakt?

Antwoord:
Nee, het gevraagde is niet akkoord.

Percelen: P1 SOC dienstverlening Monitoring en Alarmering
Beantwoord op: 13 aug. 2024

Ref.nr. 19
Onderwerp: Aanbestedingsleidraad p.15

Vraag:
In de huidige tijd is er veel sprake van plaats onafhankelijk werken. Dit geldt ook voor medewerkers van het Converged SOC. Wat is de verwachting van hWh met betrekking tot een Converged SOC team, waarvan de verschillende analysten (mogelijk) niet altijd op fysiek dezelfde locatie zitten?

Antwoord:
Het converged OT & IT SOC-team dient op één fysieke locatie te zijn gehuisvest, waarbij de medewerkers ook fysiek bij elkaar zitten. Dat neemt niet weg dat medewerkers deels ook van uit huis (kunnen) werken.

Percelen: P1 SOC dienstverlening Monitoring en Alarmering
Beantwoord op: 13 aug. 2024

Ref.nr. 21
Onderwerp: Bijlage M - Initiële Use Cases SOC

Vraag:
Indien een Deelnemer reeds beschikt over een SIEM oplossing met daarin de benodigde use cases. Is het Inschrijver dan toegestaan deze use case te (her) gebruiken en alleen de alerts door te sturen naar het SIEM van de Inschrijver?

Antwoord:
De dienstverlening met betrekking tot use cases omvat onder andere de voorgeschreven use cases, de doorontwikkeling ervan en eventuele nieuwe use cases een en ander overeenkomstig de eisen die voortvloeien uit de overeenkomst. Het is aan opdrachtnemer om te bepalen of hij reeds bestaande use cases van opdrachtnemer (al dan niet aangepast) daartoe gebruikt.

Percelen: P1 SOC dienstverlening Monitoring en Alarmering
Beantwoord op: 13 aug. 2024

Ref.nr. **Onderwerp:**

22 Aanbestedingsleidraad p.16

Vraag:
In de aanbestedingsleidraad is aangegeven dat indien geen certificaten van onafhankelijke opleidings-/certificeringsinstituten kunnen worden overlegd: een beschrijving 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. Inschrijver beschikt over een intern opleidingsprogramma. Kan hWh bevestigen dat een dergelijk intern opleidingsprogramma, mits juist omschreven en van voldoende kwaliteit, gelijkwaardig zal worden beoordeeld als externe certificeringen?

Antwoord:
Dat hangt er van af in welke mate het intern opleidingsprogramma is gedocumenteerd en inschrijver aantoont dat de onderwerpen/ inhoud van de interne opleidingen overeenkomen met de in de definities voor SOC-analisten genoemde certificering. Vanzelfsprekend geldt een opleiding uit het programma alleen als de betreffende SOC-analist die opleiding ook heeft afgerond.

Percelen: P1 SOC dienstverlening Monitoring en Alarmering
Beantwoord op: 13 aug. 2024

Ref.nr. **Onderwerp:**
23 Aanbestedingsleidraad p.16

Vraag:
In technische bekwaamheid 2 vraagt hWh om screening door een gecertificeerd POB. Naast analisten die door een POB gescreend zijn, hebben we analisten in dienst die gescreend zijn door overheidsinstanties. Zoals bijvoorbeeld in Belgie door de Nationale Veiligheidsoverheid (NVO), waar de screening dan wordt uitgevoerd door de VSSE, ADIV en de Federale Politie. Gaat hWh ermee akkoord dat screening van dergelijke centrale overheidsinstantie als gelijkwaardig wordt beschouwd?

Antwoord:
Een screening door de Belgische Nationale Veiligheidsoverheid (NVO) uitgevoerd door de VSSE, ADIV en Federale Politie wordt als gelijkwaardig aan een POB screening beschouwd.

Percelen: P1 SOC dienstverlening Monitoring en Alarmering
Beantwoord op: 13 aug. 2024

Ref.nr. **Onderwerp:**
24 Data

Vraag:
Het antwoord op vraag 2 vervalt en wordt vervangen. De vraag luidt:
De hoeveelheden te analyseren data kunnen per logbron sterk variëren. Bijvoorbeeld een Netwerk flow monitoring tool in PA, geeft veel minder logs /alerts dan een Firewall. In het prijs formulier stelt u voor 1 prijs te hanteren voor logbronnen (één voor PA en en één voor KA logbronnen). Om dit te vertalen in de door het Waterschapshuis gevraagde prijsmodel, vragen wij u inzicht te geven in de samenstelling van de logbronnen. Indien het Waterschapshuis dit niet wenst te doen, dan stellen wij voor een aantal referentiebronnen te definiëren op basis waarvan gegadigden hun prijs bepalen en het Waterschapshuis een juist vergelijk tussen de gegadigden kan maken.

Antwoord:
De hoeveelheid data per 24 uur verschilt per waterschap. Op basis van indicatoren die gebruikt worden om de omvang van een waterschap vast te stellen is de indeling gemaakt in klein, middel, groot zoals in het prijzenblad vermeld.
Zoals aangegeven hebben de Waterschappen een E5 en P2 licentie. Zij gebruiken Microsoft Defender voor End-Points, Servers en Identities. Dit resulteert in het feit dat enkel alerts richting Sentinel worden gestuurd, i.p.v. hoeveelheden data. Detail analyse kan plaatsvinden aan de bron (Defender data). Daarnaast hebben we geconstateerd dat voor netwerkcomponenten de hoeveelheid data die voor security monitoring wordt gebruikt aanzienlijk kleiner is dan de bruto gegenereerde logfiles van bijvoorbeeld firewalls of switches. Ook dit heeft een direct invloed op de te verwerken hoeveelheid data door de opdrachtnemer.
De inschatting van de gemiddelde datastroom per 24 uur vanuit KA en PA voor een waterschap, met inachtneming van het feit dat enkel voor security monitoring relevante data wordt aangeboden, is:
• Klein: 10 GB
• Middel: 15 GB
• groot: 25 GB
Detail analyses (indien nodig) kunnen worden uitgevoerd op de ruwe logdata die binnen het waterschap aanwezig is en uiteraard omvangrijker van aard. Een Deelnemer is zelf verantwoordelijk om deze data te collecteren en gecentraliseerd ter beschikking te stellen van de dienst. Indien er hulp nodig is bij het collecteren en gecentraliseerd ter beschikking stellen, kan deze hulp als separate consultancy dienst worden afgenomen door de betreffende Deelnemer.

Percelen: P1 SOC dienstverlening Monitoring en Alarmering
Beantwoord op: 13 aug. 2024

Ref.nr.	**Onderwerp:**
25	Usage

Vraag:
Het antwoord op vraag 3 vervalt en wordt vervangen. De vraag luidt: Welke waterschappen hebben al Sentinel draaien en wat is de usage/log ingestion (GB per day)?

Antwoord:
Na het gunnen van de opdracht kan een overzicht worden verstrekt van de actuele situatie per waterschap. Sentinel is uitgerold en kan door alle waterschappen worden gebruikt. Een aantal heeft echter lopende contracten en gebruikt nog een andere SIEM oplossing in de praktijk. In de Sentinel uitrol in de Azure Cloud zijn op dit moment de O365 en Azure logging geïmplementeerd. Het aantal GB per 24 uur in Sentinel is momenteel niet representatief te noemen. Zie antwoord 2 voor hoeveelheden data per 24 uur. Waterschappen beschikken over de mogelijkheid om Defender in te zetten voor End-Points, Servers en Identities. Vanuit kosten overweging (deze onderdelen zijn al verdisconteerd in de bestaande licenties) zal een groot deel van de waterschappen deze producten gaan gebruiken.

Percelen: P1 SOC dienstverlening Monitoring en Alarmering
Beantwoord op: 13 aug. 2024

Ref.nr.
26

Onderwerp:
Contractduur

Vraag:
In uw referentie eis wordt gevraagd naar bewezen IT/OT-monitoring ervaring met een contractduur van minstens 3 jaar. Voor inschrijver geldt dat wij voor een van onze klanten gedurende de laatste 4 jaar IT/OT-monitoring verrichten. Echter deze klant heeft bijna 3 jaar geleden een onderdeel afgesplitst in een nieuwe onderneming. Voor inschrijver betekent dit 2 nieuwe contracten, waarbij we nu dezelfde diensten leveren voor twee in plaats van een entiteit. Deze nieuwe contracten hebben echter een looptijd korter dan 3 jaar. Mogen wij beide klanten zien als 2 klanten ieder met een contract vanaf de begindatum van 4 jaar in plaats van 2 klanten met maar een contractduur vanaf splitsing van 2 jaar?

Antwoord:
Er is in deze situatie sprake van herstructurering van de onderneming van de oorspronkelijke klant A, waarbij de overeenkomst met oorspronkelijke klant A vervolgens wordt omgezet in een nieuwe overeenkomst met oorspronkelijke (door herstructurering wellicht deels afgeslankte) klant A waarbij de overeengekomen dienstverlening voortduurt. Daarnaast duurt de dienstverlening aan de afgesplitste klant B eveneens voort. Dat voor de oorspronkelijke klant A na herstructurering en de afgesplitste klant B twee nieuwe overeenkomsten zijn gesloten in verband met de voortzetting van de

dienstverlening naar beide gespitste delen van oorspronkelijke klant A, maakt niet dat de oorspronkelijke overeenkomst en de na herstructurering opvolgende nieuwe overeenkomst (en) tezamen niet zouden kunnen worden beschouwd als één overeenkomst van vier jaar. In dat licht kunnen de twee contracten van klant A (voor herstructurering en na herstructurering) als één contract van vier jaar met een klant worden beschouwd. Zo ook kunnen de twee contracten van klant A (voor herstructurering) en van afsplitsing B als één contract van vier jaar met een klant worden beschouwd. Evenzo kunnen de drie contracten van klant A (voor herstructurering), van afgeslankte klant A en van afsplitsing B als één contract van vier jaar met een klant worden beschouwd.

Percelen: P1 SOC dienstverlening Monitoring en Alarmering
Beantwoord op: 13 aug. 2024

Ref.nr.
27

Onderwerp:
Persoonlijke gegevens

Vraag:
Wij hebben het beleid dat we geen persoonlijke gegevens verstrekken in deze fase van het traject. Dit heeft te maken met wettelijke bepalingen, AVG, kans op fraude en kans op chantage wanneer deze gegevens algemeen bekend worden. Zeker voor medewerkers van onze SOC's is dat het geval. Uiteraard begrijpen we de insteek van hWh en het belang voor hWh. We stellen voor om na gunning (indien positief) een kenningmaking te organiseren met een deel van onze SOC medewerkers. Gaat hWh akkoord met deze werkwijze?

Antwoord:
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.

Percelen: P1 SOC dienstverlening Monitoring en Alarmering
Beantwoord op: 13 aug. 2024