Nota van Inlichtingen Selectiefase niet-openbare aanbesteding SIEM-SOC

Nvl # 2
Datum 10 juni 2024

Vraag	Document	Hoofdstuk, paragraaf	Pagina	Onderwerp	Vraag of opmerking Gegadigde	Antwoord provincie Noord-Holland
1	Selectieleidraad	2.5	13	Taal	U geeft aan " Vooruitlopend op de Inschrijvingsleidraad eist Aanbestedende dienst dat de Ondernemer het SOC heeft gevestigd binnen de EER en dat de contactpersonen en de met de uitvoering van de werkzaamheden belaste personen van de Ondernemer de Nederlandse taal (B1) in woord en geschrift machtig zijn". MSSP leveren hun SOC-diensten meestal vanuit centrale locaties, vanwege beperkte beschikbaarheid van gespecialiseerde resources en om maximaal gebruik te maken van ervaringen bij andere klanten. De voertaal is dan vooral Engels. Inschrijver ziet dan ook dat Engels in dit soort dienstverlening door klanten steeds meer geaccepteerd wordt. De hele cybersecuritydienstverlening bestaat ook uit Engelse vaktermen. Inschrijver geeft aan dat in haar dienstverlening de primaire technische en commerciële contactpersoon Nederlands spreken. De dienst zelf (operationele zaken zoals gemelde incidenten, rapportages, handleidingen, serviceportal e.d. zijn in het Engels (op minimaal C1 niveau). Kunt u de zin aanpassen naar " Vooruitlopend op de Inschrijvingsleidraad eist Aanbestedende dienst dat de Ondernemer het SOC heeft gevestigd binnen de EER en dat de contactpersonen en de met de uitvoering van de werkzaamheden belaste personen van de Ondernemer de Nederlandse of Engelse taal (B1) in woord en geschrift machtig zijn".	**Aanvulling van het antwoord gegeven in Nvl 1:** Alle communicatie met Aanbestedende dienst of één van haar leveranciers, verloopt in het Nederlands. **Antwoord gegeven in Nvl 1:** De Aanbestedende dienst vindt het belangrijk deze vraag vooruitlopend op de geplande Nota van Inlichtingen te beantwoorden. Nee, de Aanbestedende dienst past de eis niet aan. Het is voor de Aanbestedende dienst essentieel dat tijdens crisissituaties en/ of calamiteiten geen interpretatieverschillen ontstaan door taal- en/ of interpretatieverschillen. Daarom eist de Aanbestedende dienst dat er altijd gecommuniceerd wordt in de Nederlandse taal (B1).
2	Selectieleidraad	4.4.2	30	Darktrace	U maakt gebruik van Darktrace. Is het een vereiste of een wens om Darktrace te blijven voeren?	Dit is een wens. Vooruitlopend op de inschrijffase geeft de Aanbestedende dienst mee dat een sleuteloverdracht naar een opdrachtnemer met Darktrace de voorkeur heeft. Aanbestedende dienst heeft veel geïnvesteerd voor de implementatie van Darktrace. Ervaring met Darktrace is een selectiecriterium op basis waarvan de provincie de Gegadigden beoordeelt. Dit is van toepassing wanneer er meer dan 5 geschikte Gegadigden zijn. Ervaring met Darktrace is voor de Aanbestedende dienst onderscheidend. De selectiefase richt zich op de geschiktheid als organisatie. In de inschrijffase beoordeelt de Aanbestedende dienst hoe inschrijvers invulling geven aan de opdracht. In de inschrijffase gaat de Aanbestedende dienst in op de eisen en wensen voor de opdracht.

Nota van Inlichtingen Selectiefase niet-openbare aanbesteding SIEM-SOC

NvI # 2
Datum 10 juni 2024

Provincie Noord-Holland

3	Selectieleidraad	4.4.2	30	Darktrace	Als geen Darktrace maar een alternatief met vergelijkbare kwaliteiten wordt gebruikt door inschrijver, komt dit alternatief wel in aanmerking voor de te verdienen punten?	Nee. Ervaring met Darktrace is een selectiecriterium op basis waarvan de provincie de Gegadigden beoordeelt. Dit is van toepassing wanneer er meer dan 5 geschikte Gegadigden zijn. Ervaring met Darktrace is voor de Aanbestedende dienst onderscheidend. De selectiefase richt zich op de geschiktheid als organisatie. In de inschrijffase beoordeelt de Aanbestedende dienst hoe inschrijvers invulling geven aan de opdracht. In de inschrijffase gaat de Aanbestedende dienst in op de eisen en wensen voor de opdracht.
4	n.v.t.	-	-	Gunningsfase	Deze aanbesteding betreft een niet-openbare Europese aanbesteding. Deelnemer houdt het ervoor dat vragen/voorstellen t.a.v. de toepasselijke contractuele voorwaarden in de gunningsfase dienen/kunnen worden gesteld/gedaan. De gunningsfase biedt ook ruimte voor het stellen van vragen en de voorwaarden zullen daarnaast in samenhang met de nadere specificaties/details van de opdracht dienen te worden beoordeeld. Graag uw bevestiging.	Ja, dit klopt.
5	Selectieleidraad	4.3.1		Financiele en economische draagkracht	U vraagt een afschrift van de meest recente premiebetaling. Dit is hoogst ongebruikelijk. We verzoeken u dit bewijsstuk te laten vervallen.	Het bewijsstuk "Een afschrift van de meest recente premiebetaling (niet ouder dan één jaar)." vervalt. Een aangepaste Selectieleidraad is als bijlage bij deze Nota van Inlichtingen gevoegd.
6	Bijlagen	2 en 3	34		Wilt u de bijlagen (2 en 3) in .docx vrijgeven? Zo kan leverancier gemakkelijker deze documenten invullen.	Ja. De Selectieleidraad in .docx is bijgevoegd.
7	Selectieleidraad	4.4.2	31	Selectie-criteria S2 Bewaken van OT	Kijkt Aanbestedende dienst bij OT-monitoring naar Device Discovery en netwerkanalyse of worden er andere activiteiten verwacht? Zo ja, welke?	Ja, de Aanbestedende dienst verwacht onder OT monitoring Device Discovery en netwerkanalyse. § 2.5 "Aard van de opdracht" beschrijft de andere activiteiten die de Aanbestedende dienst verwacht.
8	Selectieleidraad	4.3.1	27	Financiële en economische draagkracht	Aanbestedende dienst vraagt na de selectiebeslissing de meest recente jaarrekening op. Inschrijver maakt gebruik van de accountantsverklaring uit het geconsolideerde jaarverslag van haar moedermaatschappij en publiceert geen zelfstandige cijfers. Inschrijver voldoet zelfstandig aan de gestelde selectiecriteria en doet geen beroep op de draagkracht van haar moedermaatschappij om te voldoen aan de selectiecriteria. Accepteert Aanbestedende dienst de accountantsverklaring van onze moedermaatschappij in combinatie met de 403 verklaring welke gedeponeerd is bij de Kamer van Koophandel zonder dat er een eigen UEA voor onze moedermaatschappij wordt ingediend?	Ja.
9	Selectieleidraad	4.3.1	27	Financiële en economische draagkracht	Aanbestedende dienst vraagt na de selectiebeslissing een afschrift van de meest recente premiebetaling (niet ouder dan één jaar). Het door onze verzekeraar afgegeven verzekeringscertificaat is geldig voor het lopende verzekeringsjaar en bevat de vermelding dat de premie volledig is betaald over het lopende jaar. Accepteert u dit geldige verzekeringscertificaat als bewijs van premiebetaling?	Ja. Zie het antwoord op vraag 5.

Nota van Inlichtingen Selectiefase niet-openbare aanbesteding SIEM-SOC

NvI # 2
Datum 10 juni 2024

Provincie Noord-Holland

10	Selectieleidraad	2.6	14	Omvang	Hoeveel assets moeten er (globaal) bewaakt worden?	Globaal zijn de volgende assets van toepassing: - MS365 kantoorapplicaties; - 20 bedrijfsapplicaties onpremise/IaaS gehost; - 2.000 werkplekken; - 1.600 smartphones; - 200 tablets; - 50 netwerklocaties (WAN dienst). **Operationele Technologie:** - 3 Tunnelobjecten met 1 bediencentrale en eigen WAN netwerk met daarin ongeveer 50 endpoints (server, werkstation, PLC); - 20 Bruggen of sluizen (groeiend naar 40) met 1 bediencentrale eigen WAN netwerk met daarin nu 50, groeiend naar 100 endpoints (server, werkstation, PLC).
11	Selectieleidraad	4.3.2	28	Kern-competentie 1	Mogen we in plaats van werkplekken ook assets opvoeren? Rationale: onder OT van Opdrachtgever vallen immers ook bedienplekken, onderhoudsplekken, coördinatorplekken, CCTV-installaties, omroepinstallaties, intercom, praatpalen en (i)VRI's.	Nee. Een werkplek (waar een gebruiker, bedienaar of beheerder) zijn werk achter uitvoert, ongeacht in een IT of OT opstelling. Andere door Inschrijver genoemde voorbeelden van assets vragen andere bewaking waardoor deze niet opgevoerd kunnen worden als werkplek.
12	Selectieleidraad	4.4.2	30	Selectie-criterium S1	Mogen in plaats van Microsoft Sentinel en Darktrace ook andere SIEM-oplossingen beschreven worden die aantoonbaar zijn ingezet voor het bewaken van OT?	Ja, maar wanneer dit andere ervaring is dan beschreven in Selectiecriterium S1 krijgt Gegadigde hier geen punten voor.
13	Selectieleidraad	2.5	13	Taal	Wij begrijpen dat het contact voor de dienst in het Nederlands dient te verlopen, echter willen wij bevestiging over de taalvoorkeur voor de diverse alerts. Kunt u bevestigen dat, hoewel het directe contact met de dienst in het Nederlands dient te verlopen, de inhoudelijke security alerts, inclusief integratie met TopDesk, in het Engels verstuurd mogen worden?	Nee, zie ook het antwoord bij vraag 1.
14	Selectieleidraad	2.5	13	Taal	Wat is voor u het verschil tussen een alert, security incident, of calamiteit?	De Aanbestedende dienst vindt het niet belangrijk om nu toelichting te geven op het verschil tussen een alert, security incident, of calamiteit. In de volgende fase verwacht de Aanbestedende dienst hierop in te gaan.
15	Selectieleidraad	2.5	13	Taal	Kunt u duiden of (en welke vormen van) communicatie u in de Engelse taal toestaat?	Nee, zie ook het antwoord op vraag 1.
16	Selectieleidraad	4.3.2.	28	Referentie	Veel van onze opdrachtgevers willen graag anoniem blijven gezien de gevoeligheid van werkzaamheden die we uitvoeren. Kunnen referenties ook geanonimiseerd worden aangeleverd?	Nee, de Aanbestedende dienst wil de mogelijkheid hebben om een referentie te kunnen contacteren.

Nota van Inlichtingen Selectiefase niet-openbare aanbesteding SIEM-SOC

NvI # 2
Datum 10 juni 2024

Provincie Noord-Holland

17	Selectieleidraad	2.5	13	Meekijk mogelijk-heden	Wat zijn de verwachtingen van de Aanbestedende dienst op het gebied van meekijkmogelijkheden en training on the job? Welke specifieke activiteiten hebben jullie in gedachten op dit vlak?	Aanbestedende dienst wil zelf ook kunnen kijken in de SIEM oplossing. We willen zelf nog data kunnen teruglezen na een melding. Aanbestedende dienst gaat niet 'op de stoel van opdrachtnemer' zitten. Aanbestedende dienst heeft niet de wens om officiële SIEM product trainingen te gaan volgen. Dit kan ondervangen worden door een beperkte training of meekijk/uitleg sessie door een SOC-engineer. De Aanbestedende dienst denkt hierbij aan een sessie van een halve dag tot maximaal een dag.
18	Selectieleidraad	2.5	13	Taal	De Aanbestedende dienst eist dat er altijd gecommuniceerd wordt in de Nederlandse taal. Inschrijver kan dit realiseren voor directe communicatie met personen. Echter incidenten (met actionable advice), rapportages, handleidingen e.d. zijn in het engels. Is dit een knock-out criterium?	Ja, zie ook het antwoord op vraag 1.
19	Bijlagen	2 en 3	34 t/m 39	Referenties	Voor de volgende kerncompetenties wordt per competentie een referentie gevraagd: Kerncompetentie 1: Opzetten en beheren SIEM-oplossing Kerncompetentie 2: SOC ervaring Kerncompetentie 3: OT-ervaring Voor de onderstaande selectiecriteria worden ook referenties gevraagd: S1 Ervaring met SIEM-SOC dienstverlening S2 Bewaken van OT Verwacht de Aanbestede dienst verschillende referenties voor de kerncompetenties en selectiecriteria of mogen dit dezelfde referenties zijn.	Ja, dit mogen dezelfde referenties zijn. Dit zoals beschreven in het hoofdstuk 4 Selectieprocedure.
20	Selectieleidraad	4.4.2.	30	Selectie-criteria	In de selectieleidraad van de SIEM/SOC aanbestesteding spreekt de Provincie Noord-Holland van de mogelijkheid om met Microsoft Sentinel te werken. In de verdere stukken is niet beschreven dat het een eis is om deze oplossing in te zetten. Echter in de selectiecriteria is een van de eisen om een ervaring te delen betreffende het opzetten en beheren van een Microsoft Sentinel oplossing. Ondanks dat Provincie Noord-Holland over bepaalde E5 licenties beschikt, zal de SIEM-oplossing alsnog ingekocht moeten worden op basis van GB/dag, zoals gebruikelijk in de markt. Dit heeft dan geen voordeel op prijsgebied voor Provincie Noord-Holland. Is het toegestaan dat aanbieder deze eis invult met de SIEM-oplossing die aanbieder gebruikt, die ook hoog in de lijst van Gartner te vinden is om zo onze ervaring en geschiktheid te delen met Provincie Noord-Holland? Zo nee, kunt u toelichten hoe u met deze eis zorgt voor een gelijk speelveld voor alle aanbieders?	Het is mogelijk andere SIEM-oplossingen aan te bieden dan nu staan opgesteld (Darktrace) of binnen de licenties beschikbaar zijn (Microsoft Sentinel). Voor dit selectiecriterium krijgt u echter geen punten voor ervaring met een andere SIEM-oplossing dan Microsoft Sentinel en/of Darktrace. Toelichting: De selectiecriteria zijn geen eisen die de Aanbestedende dienst aan Gegadigden stelt. Het zijn criteria waarmee Gegadigden zich kunnen onderscheiden.

Nota van Inlichtingen Selectiefase niet-openbare aanbesteding SIEM-SOC

Nvl # 2
Datum 10 juni 2024

Provincie Noord-Holland

21	Selectieleidraad	4.4.2.	30	Selectie-criteria	Binnen de SIEM-oplossing van de aanbieder zijn veel integraties mogelijk als het gaat om de verschillende logbronnen die aangesloten dienen te worden, zo ook Darktrace. Aanbieder heeft niet specifiek ervaring met de tool darktrace in de SIEM/oplossing, echter wel met andere producten die dezelfde functionaliteit leveren. Mag aanbieder ook een andere oplossing als ervaring delen in plaats van Darktrace? Zo nee, kunt u toelichten waarom specifiek ervaring met deze tool nodig is?	Ja, zie ook het antwoord op vraag 20.
22	Nvl 1	1		Taal	Gegeven uw antwoord in de gedeelde nota van inlichtingen waarin u stelt dat er altijd gecommuniceerd wordt in de Nederlandse taal (B1) gegeven u interpretatieverschillen wilt voorkomen in crisissituaties en calamiteiten. Accepteert u dat standaard meldingen (zijnde geen calamiteit of crisissituatie) Engelstalig kunnen zijn, maar in geval van crisis of calamiteit een Nederlandstalige medewerker met u communiceert cq met u gecommuniceerd wordt?	Nee, zie ook het antwoord op vraag 1.
23	Selectieleidraad	1.4	7	Beschikbare oplossingen	U beschrijft in de 2e paragraaf tooling die nu geimplementeerd is, of waarvoor een licentie aanwezig is. Kunt u duiden of er tooling op de nominatie staat om uitgefaseerd te worden?	Op dit moment is er geen tooling in beeld om uit te faseren.
24	Selectieleidraad	4.3.2	28	Kern-competentie 1	Als een Gegadigde beschikt over (zeer veel) ervaring met publieke sectorpartijen vanuit allerlei securitydienstverlening (niet SOC-SIEM) EN bovendien wel private klanten - met ook OT - conform het gestelde SOC--SIEM profiel bedient, staat de Provincie Noord Holland dan alsnog open voor deelname door Gegadigde?	Het is aan de Gegadigde om te bepalen of u voldoet aan kerncompetentie 1.
25	Selectieleidraad	4.3.2.	28	Kern-competentie 1	Welk verschil ziet de Provincie Noord-Holland technisch tussen (semi)overheidsorganisaties en een niet-publieke opdrachtgever voor wat betreft het implementeren van een SOC-SIEM oplossing? Veel van onze particuliere opdrachtgevers, hebben min of meer vergelijkbare eisen en wensen (en behoren tevens tot de kritieke infrastructuur / essentiele bedrijven in het kader van de NIS2/Cyberbeveiligingswet). Bent u bereid om daar competatentie #1 op aan te passen?	Nee, Aanbestedende dienst past de kerncompetentie niet aan.
26	Selectieleidraad	4.3.2	28	Kern-competentie 3	Als een Gegadigde beschikt over ruime en unieke ervaring met OT security, en met monitoring op het snijvlak van IT en OT, maar nog niet met alleen OT, echter dit de komende maanden wel gaat doen, wenst de Provincie dan alsnog dat deelgenomen door Gegadigde wordt?	Het is aan de Gegadigde om te bepalen of u voldoet aan kerncompetentie 3.
27	Selectieleidraad	4.3.2.	28	Referenties	Indachtig de bovenstaande vragen over de interpretatie van de kerncompetenties / geschiktheid: mits de Provincie ook akkoord kan met afwijkingen op de kerncompetenties, mogen referenties dan conform de beschreven afwijkingen worden aangeleverd?	Zie het antwoord op vraag 24 en 26.