

Nota van Inlichtingen, ronde 1, versie 0.3

In het kader van de aanbesteding met kenmerk IUC 23-003 SOAR zijn tot en met 29 september 2023, (sluitingsdatum van ronde 1 voor het stellen van schriftelijke vragen) door partijen onderstaande vragen gesteld. Bij elke vraag is door de Aanbestedende dienst het bijbehorende antwoord vermeld. De vragen en antwoorden vormen met deze Nota van Inlichtingen een integraal onderdeel van het beschrijvend document. Bij sommige antwoorden wordt verwezen naar aanpassingen in nieuwe versies van het betreffende document. Deze zijn met **blauw gearceerde tekst** aangegeven om het verschil ten opzichte van de vorige versie in 1 oogopslag te zien.

Nr	Locatie (document, hoofdstuk, pagina)	Vraag	Antwoord
1	BD, par 2.4.1.	In de leidraad staat het volgende: De geraamde omvang van de totale opdracht is afgerond € 8.800.00,00 exclusief BTW. Graag zouden wij willen weten wat de correcte waarde is.	De exacte waarde is op voorhand niet te bepalen. Vandaar dat conform artikel 2.15 AW in paragraaf 2.4.1. van het Beschrijvend Document een raming is opgenomen.
2	Beschrijvend-Document-Openbare-Aanbesteding, 4.1, pagina 14	Kunt u bevestigen dat de Gunningseisen (GUE) met JA/NEE/NVT beantwoord dienen te worden (in de bijlage VII Conformiteitenlijst). Bij de Gunningseisen wordt er dus geen uitgebreide onderbouwing/uitleg verwacht? Behalve in het geval dat dit specifiek opgegeven is (zoals GUE 35).	Ja, dat is correct. Bij GUE 35 vult u in dat geval in Bijlage VII Conformiteitenlijst versie 1.0 alleen een 'JA' in én u levert bij de inschrijving de beschrijving hiervan als Bijlage XIII in.
3	Bijlage A, 2.2, pagina 8	Kunt u meer informatie verstrekken rondom de te integreren oplossingen. Zo is uw omschrijving: "Netwerkcomponenten (F5, Juniper)" vrij algemeen.	Vanwege de openbaarheid van de aanbestedingsprocedure is ervoor gekozen om niet alle componenten die worden gebruikt met naam en type-nummer te noemen. We gaan er vanuit dat de aangeboden oplossing veel verschillende producten ondersteunt. De Inschrijver mag ervan uit gaan dat de Opdrachtgever marktconforme enterprise-grade producten gebruikt.
4	Bijlage A, 1.2, pagina 5	Volgens de gebruikte definitie van de SOAR oplossing zou Threat Intel Management (TIM) ook van belang zijn. Echter, de meeste eisen en wensen zijn gericht op alert/incident automation en orchestration. Zijn er specifieke eisen en wensen voor wat betreft TIM? Bijvoorbeeld, aggregatie, de-duplicatie, parsing en scoring.	Threat Intel Management zien we als een belangrijke functionaliteit van een SOAR-oplossing. Op dit moment hebben we een dedicated TIM-oplossing in gebruik (vandaar de eis naar integratiemogelijkheden op basis van STIX/TAXII). Voor de toekomst willen we mogelijkheid openhouden om gebruik te maken van de TIM-functionaliteit in de Oplossing. Die afweging zal dan plaatsvinden op basis van de TIM-mogelijkheden van de Oplossing op dat moment.
5	Beschrijvend-Document-Openbare-Aanbesteding, 3.1, pagina 9	Volgens de planning wordt er tijdens het beoordelen van de SOAR oplossingen geen Proof Of Concept verwacht. Is hier een specifieke reden voor?	De verwachting is dat wanneer voldaan wordt aan alle eisen en wensen de Oplossing toepasbaar is in onze omgeving.
6	In Bijlage VII conformiteitenlijst, Eis GE4,pagina 4	Volstaat het wanneer in geval van een samenwerkingsverband alleen de Inschrijver van het samenwerkingsverband de gedragsverklaring overlegt of moet ook een GVA worden overlegd door een onderaannemer?	Zie paragraaf 5.4.3 van het Beschrijvend Document. De Aanbestedende dienst verlangt van de winnende Inschrijver, winnende leden van een samenwerkingsverband van ondernemers en/of hun onderaannemer(-s) een gedragsverklaring aanbesteden in de zin van hoofdstuk 4.1 AW2012.
7	In Bijlage VII conformiteitenlijst. Eis GE4, pagina 4	Kunt u bevestigen dat u akkoord bent dat wanneer ook een onderaannemer de gedragsverklaring moet overleggen en deze de onderaannemer deze heeft aangevraagd het volstaat wanneer deze later dan 22 november wordt overlegd?	De betreffende gedragsverklaring moet, conform de planning in tabel 1 van het Beschrijvend-Document-Openbare-Aanbesteding IUC 23-003, uiterlijk op maandag 4 december 2023 ingeleverd zijn.
8	In Bijlage VII conformiteitenlijst. Eis UE16, pagina 6	Het gevraagde implementatiewerk heeft een hoge complexiteit en hoog educatie niveau, en kan zeer waarschijnlijk niet uitgevoerd worden door de genoemde social return groepen. Hoe ziet de Belastingdienst de inzet van deze 5% van de uren? Mogen deze uren ook buiten het project ingezet worden?	De Opdrachtgever staat open voor suggesties; in UE15 is aangegeven dat Partijen na het tekenen van de Overeenkomst hier invulling over gaan afstemmen.
9	In Bijlage 02 conceptovereenkomst. In artikel 11.2 op pagina 7	Hieruit concluderen wij dat het mogelijk is om de licentievoorwaarden van de leverancier in te brengen. Is deze conclusie correct?	Dit is correct.
10	In Bijlage 02 conceptovereenkomst. Artikel 2.5 op pagina 4	Kunnen wij hieruit concluderen dat de licentievoorwaarden van de leverancier prevaleren boven de overige documenten mits het de prestatie niet benadeelt?	Niet helemaal. Artikel 11 is bij de interpretatie van dit artikel van doorslaggevende betekenis. Daar waar de licentievoorwaarden zien op het gebruik van de Prestatie, mogen de licentievoorwaarden inderdaad als leidend worden gezien, mits (!) wordt voldaan aan de eisen uit artikel 11. Het is aan de Inschrijvers om deze check te doen en eventueel maatregelen te treffen. Het eenvoudig doorsturen van de licentievoorwaarden is daarmee onvoldoende. Inschrijver zal moeten onderzoeken of de eventueel door te leggen licentievoorwaarden het beoogde en beschreven gebruik niet in de weg staan.

Nr	Locatie (document, hoofdstuk, pagina)	Vraag	Antwoord
11	Bijlage A – H5.1 (pag. 16) Wens 7.	U geeft hier aan punten toe te kennen aan klimaatinspanningen aan de hand van CO2 compensatie en wel heel specifiek gebaseerd op alleen de volgende situatie: “Alle vrijgekomen CO2 vanwege dienstreizen wordt 100% gecompenseerd.” – aan te tonen aan de hand van specifiek hierop toegespitste bewijslast. Wij zijn niet specifiek in het bezit van gevraagde bewijslast. Echter is Gegadigde als onderdeel van een internationale organisatie betrokken bij duurzaamheidsinitiatieven die veel verder gaan dan de genoemde CO2 compensatieregels en gekoppeld zijn aan de Sustainable Development Goals (SDG's) van de Verenigde Naties, alsmede hoge scores in het leiderschapskwadrant van het CDP (A en A-). Meer informatie hierover is terug te vinden op www.cdp.net . Wij willen u dan ook verzoeken om het aantoonbaar maken van MVI en klimaat- en duurzaamheidsinspanningen breder uit te vragen dan het voldoen aan de gevraagde CO2 compensatie en zo recht te doen aan de inspanningen van Gegadigde en eventuele andere Gegadigden die zich in een vergelijkbare situatie bevinden.	De Wens wordt niet aangepast.
12	Beschrijvend document, 2.1, p. 6 Specificatie van de opdracht, 1.2, p. 5	Opdracht geeft aan gebruik te maken van Splunk SOAR wat momenteel voornamelijk wordt gebruikt voor het automatiseren van de afhandeling van smishing en phishing. Gebaseerd op deze ervaring, sluit Splunk SOAR aan bij de toekomstige visie van opdrachtgever op SOAR of loopt opdrachtgever bij deze oplossing tegen problemen aan? In het geval van het laatste, vernemen we graag verdere toelichting. Is de automatisering van de afhandeling van voornamelijk smishing / phishing gebaseerd op prioriteit of loopt opdrachtgever tegen problemen aan voor verdere automatisering?	Wij lopen bij het gebruik van Splunk SOAR niet tegen problemen of beperkingen aan. Betreft prioritering grootste issue als eerste opgepakt en geïmplementeerd
13	Specificatie van de opdracht, 10.1.1.3, p. 30	“... worden tevens de meldingen die middels het automatisch uitbellen/signaleren van de Oplossing bij de Opdrachtnemer beschouwd als daadwerkelijke Incidenten.” Staat opdrachtgever het toe dat de oplossing health monitoring metrics stuurt naar opdrachtnemers (denk aan resource utilisatie, running processes, etc.)? Staat opdrachtgever het toe dat naast monitoring vanuit de SOAR oplossing aanvullende agents worden geïnstalleerd voor aanvullende beschikbaarheidsmonitoring?	Paragraaf 10.1.1.3 betreft aanmelden Incidenten over de Oplossing zelf. Dat wordt hier niet bedoeld; in BIJLAGE-A-Specificatie-van-de-opdracht SOAR 2023 versie 1.1 is de inleidende tekst aangepast. De laatste zin is verwijderd.
14	Specificatie van de opdracht, 10.1.1.2, p. 30	De door opdrachtgever gestelde beschikbaarheid kan op veel verschillende manieren worden ingeregeld. Kan de opdrachtgever specifiekere zijn in de gewenste inrichting m.b.t. beschikbaarheid en redundantie? Denk bijvoorbeeld aan verschillende disaster recovery sites (warm / cold standby) en clustering van SOAR instances.	Wij verwachten hier een door Inschrijver voorgestelde best practice.
15	Bijlage VIII Prijzenformulier versie 1.0, Tabblad Dimensionering	Het licentiemodel van de aanbieder maakt geen gebruik van de metrics “SOC Gebruikers” en “Playbook Ontwikkelaars”. Het licentiemodel van de aanbieder maakt gebruik van “Unrestricted Users”. Unrestricted Users zijn bij de Belastingdienst alle medewerkers van de Belastingdienst en dat zijn er volgens de Belastingdienst website ongeveer 25.000 in 2022. Als de Belastingdienst een aanbieding van ons wil ontvangen dan dient de licentie metric “Unrestricted Users” in het Excel document verwerkt te worden op alle tabbladen.	Het Prijzenformulier wordt niet aangepast; het is aan de Inschrijver om op basis van de beschikbare gegevens een prijs te bepalen.
16	Bijlage VIII Prijzenformulier versie 1.0, Tabblad Dimensionering	Zijn alleen de medewerkers van de Belastingdienst in scope, of doen Toeslagen en Douane ook mee in deze RFP?	Daar waar gesproken wordt over Belastingdienst hoort Toeslagen en Douane daar ook bij. Zie ook Bijlage 01 ICT Begrippenlijst → Aanbestedende dienst: de Belastingdienst, inclusief Douane en Toeslagen.
17	GUE 11	Er wordt gesproken over Hashicorp Hashivault, bedoeld de Belastingdienst echt dit product of bedoeld zei Hashicorp Vault?	Hashicorp Vault
18	GUE 11	De aanbieder heeft een in-platform oplossing met secrets management functionaliteit. Is dit voor de Belastingdienst ook een mogelijkheid om GUE 11 mee in te vullen?	Mits uw Oplossing ook kan koppelen met een andere secrets managements oplossing, is dit akkoord. De reden dat gevraagd wordt om integratie met de bestaande secrets management oplossingen is dat de Oplossing niet de enige tool zal zijn die geautomatiseerd acties uitvoert op de aangesloten componenten. De aangesloten componenten zullen ook door andere automation-platformen aangestuurd worden (denk aan CI/CD pipelines) en daarbij secrets gebruiken die gemanaged worden door de bestaande secrets management oplossingen.

Nr	Locatie (document, hoofdstuk, pagina)	Vraag	Antwoord
19	Beschrijvend-Document-Openbare-Aanbesteding IUC 23-003 §2.4.1	Hier wordt een geraamd bedrag genoemd van € 8.800.00,00 exclusief BTW. Hier lijkt een nul te missen, want verder op in het document §4.2.1 wordt er referentiewaarde ‘prijs’ (Pref) genoemd van € 6.000.000.	Dit is correct; de geraamde waarde is € 8.800.000, 00 (acht miljoen acht honderd duizend) ex BTW. Dit is in Beschrijvend-Document-Openbare-Aanbesteding IUC 23-003, versie 1.1 aangepast.
20	Beschrijvend document, pagina 6, hoofdstuk 2.2 Doelstellingen	Onder 2.2 geeft u aan dat de overeenkomst wordt aangegaan voor de duur van 3 (drie) jaar met de mogelijkheid voor de aanbestedende dienst om de overeenkomst onder gelijkblijvende voorwaarden 7 (zeven) maal voor de duur van 1 (één) jaar te verlengen. Kunt u aangegeven hoe de door opdrachtgever gewenste Purchase Order (PO) structuur eruit komt te zien?	Zie hiervoor Artikel 8 van Bijlage 02 concept Overeenkomst, versie 0.9
21	Beschrijvend document, pagina 7, hoofdstuk 2.4.1, In reikwijdte/Scope	Onder 2.4.1 wordt aangegeven dat De geraamde omvang van de totale opdracht is afgerond € 8.800.00,00 exclusief BTW. Kunnen wij ervan uitgaan dat hier een typefout is gemaakt en dat er eigenlijk € 8.800.000,00 exclusief BTW moet staan?	Dit is correct; de geraamde waarde is € 8.800.000, 00 (acht miljoen acht honderd duizend) ex BTW. Dit is in Beschrijvend-Document-Openbare-Aanbesteding IUC 23-003, versie 1.1 aangepast.
22	Beschrijvend document, pagina 22, hoofdstuk 4.5.1, Gunningseis 1	Onder 5.4.1 GE1 vraagt u om in Bijlage VI de jaarcijfers van de aanbieder in te vullen. Aanbieder zal daar de jaarcijfers opnemen van de aanbiederende werkmaatschappij. U vraagt tevens om bewijsstukken aan te leveren, zijnde de jaarrekeningen van de betreffende boekjaren met een accountantsverklaring of een samenstellingsverklaring. De cijfers van aanbieder worden op concernniveau gecontroleerd door de accountant, te weten op het niveau van de holding, de 100% moeder van aanbieder. Voor de onderliggende werkmaatschappijen wordt er wel een jaarrekening opgesteld en gedeponereerd, maar deze jaarrekeningen zijn niet individueel gecontroleerd. Aanbieder vraagt akkoord om samen met de jaarrekeningen van aanbieder de gecontroleerde geconsolideerde jaarrekening van de holding, de 100% moeder van aanbieder, bij te sluiten. Graag vernemen wij of dit voor u voldoende is.	Akkoord
23	Bijlage-A- specificatie van de opdracht-pagina 22, hoofdstuk 7.4 Indexering prijs.	Kunt u aangeven hoe om te gaan met een door de vendor doorgevoerde wijziging van de licentiestructuur en/of prijsstijging na de initiële periode van drie jaar wanneer deze boven de aangegeven maximale indexatie ligt.	Alleen de in BIJLAGE-A-Specificatie-van-de-opdracht SOAR 2023 genoemde indexatie is toegestaan.
24	Bijlage-A- specificatie van de opdracht-pagina 24, hoofdstuk 8.2 opleidingen uitvoeringseis 31	Bij uitvoeringseis 31 geeft u aan; De opleidingen vinden plaats op locatie van de Opdrachtgever tenzij nadrukkelijk anders overeengekomen. Is het daarbij toegestaan aan deel van deze opleidingen online, onder begeleiding van de Opdrachtnemer, vanaf de locatie van de Opdrachtgever te laten plaatsvinden.	Akkoord
25	Beschrijvend Document, Pagina 9, Hoofdstuk 3.1, Planning aanbesteding.	Wij zien in de planning een overlap op de data voor de eerste en de tweede ronde voor de nadere inlichtingen/ stellen van vragen. Kunt u aangeven of deze planning klopt.	De planning wordt als volgt aangepast: Nadere inlichtingen/stellen van vragen (2) Vr 29-09-2023 t/m Wo 11-10-2023 Dit is in Beschrijvend-Document-Openbare-Aanbesteding IUC 23-003, versie 1.1 aangepast.
26	Bijlage VIII Prijzenformulier versie 1.0, tabblad Additionele diensten	Op tabblad “additionele diensten” wordt gesproken over opleidingen voor 40 personen. Wat voor verdeling wordt er verwacht qua certificeringsniveau in het op te leiden aantal personen	Certificering is geen directe eis m.b.t. de opleidingen. Zie ook vraag 45 voor meer informatie
27	Beschrijvend-Document-Openbare-Aanbesteding IUC 23-003 - 2.4.1	Het lijkt erop dat er nul mist bij het geraamde bedrag van € 8.800.00,00 exclusief BTW. Klopt dit?	Dit is correct; de geraamde waarde is € 8.800.000, 00 (acht miljoen acht honderd duizend) ex BTW. Dit is in Beschrijvend-Document-Openbare-Aanbesteding IUC 23-003, versie 1.1 aangepast.
28	Beschrijvend-Document-Openbare-Aanbesteding IUC 23-003 - 2.4.1	Aangezien onze oplossing Cloud-native is, zal er voor het (tijdelijk) on-premise beschikbaar maken extra kosten gemaakt moeten worden. We gaan ervan uit dat we deze kosten buiten het geraamde bedrag mogen houden. Klopt dit?	Nee, alle kosten moet verdisconteerd zijn conform de aanbestedingsstukken. Inschrijver wordt er op gewezen dat de Aanbestedende dienst geen Oplossing wenst die specifiek en alleen voor de Opdrachtgever wordt aangeboden. Zie ook GUE 30 van BIJLAGE-A-Specificatie-van-de-opdracht SOAR 2023, versie 1.1.
29	BIJLAGE-A-Specificatie-van-de-opdracht SOAR	O.b.v. de beschreven architectuur, nemen wij aan dat de ‘Cloud SOAR’ oplossingen, niet vervangen zullen worden door de nieuwe SOAR technologie, maar dat er vanuit deze Cloud SOAR componenten slechts alerts worden gestuurd naar de nieuwe SOAR oplossing	De aanname klopt.

Nr	Locatie (document, hoofdstuk, pagina)	Vraag	Antwoord
	2023 – 1.1	on-premise. Daarnaast nemen wij aan dat er geen ‘Orchestration’ plaats vindt vanuit de Nieuwe on-premise SOAR solution richting de Cloud omgevingen (conform richtingen van de pijlen). Zijn deze aannames correct? Kunt u dit toelichten.	Er vindt wel orchestratie plaats vanuit de on-premises Oplossing van de cloud-omgevingen, via de cloud-native SOAR-oplossingen (o.a. door optimaal gebruik te maken van de cloud-native Playbooks). Zie ook de aangepaste figuur 1 in BIJLAGE-A-Specificatie-van-de-opdracht SOAR 2023 versie 1.1
30	BIJLAGE-A-Specificatie-van-de-opdracht SOAR 2023	Binnen het Operating / Governance Model (SOC) dat rondom de On-premise SOAR oplossing ingericht is, kunt u aangeven welke rollen/verantwoordelijkheden en evt third parties hier deel van uit maken? Voor de verschillende potentiële ‘Use Cases’ is het voor de inrichting van belang, dat wij een volledig beeld hebben bij de verschillende actoren die met elkaar interacteren binnen de key workflows/ playbooks.	Wij begrijpen deze vraag niet. Kunt u deze in NVI 2 verduidelijken?
31	BIJLAGE-A-Specificatie-van-de-opdracht SOAR 2023	Kunt u een vollediger beeld geven bij de verschillende in te richten Use Cases/ Workflows en playbook varianten. Onze aanname is dat er in ieder geval voor elk van de 3 Cloud omgevingen een specifieke Use Case analyse en inrichting gedaan zal moeten worden, wegens wellicht andere samenwerkingsmodellen met de betreffende cloud vendors. Klopt deze aanname? Hiernaast dezelfde vraag voor On Premise. Onze aanname is dat hier ook diversiteit zal bestaan voor het de Security Incident processen en afhandelingen per IT-deelgebied (e.g.: Applicaties, Infra, Netwerk componenten etc.). Klopt dit? En kunt u derhalve een duidelijk overzicht geven van de verschillende Use Cases of aangeven waar jullie de scope van de uitvraag zien?	Ja, maar de focus ligt in eerste instantie on-premises en dan specifiek phishing/smishing. Zie ook de aangepaste figuur 1 in BIJLAGE-A-Specificatie-van-de-opdracht SOAR 2023 versie 1.1
32	BIJLAGE-A-Specificatie-van-de-opdracht SOAR 2023	Hoe kunt u zelf waarborgen dat er voldoende capaciteit (personeel) beschikbaar gemaakt kan worden vanuit de belastingdienst en eventuele gelieerde relevante 3e partijen voor de verschillende technologieën en betrokkenen in het SOC operating model.	Door het aanstellen van een interne projectmanager en/of juiste tijdige planning met betrokken teams.
33	Bijlage 02 concept Overeenkomst, versie 0.9, pagina 1/hele document	De rechthebbende van de IP gunt licenties uitsluitend op basis van haar eigen voorwaarden en levert onderhoud conform haar eigen voorwaarden en gebied business partners en gelieerde onderneming eveneens onder de voornoemde voorwaarden aan klanten aan te bieden. Aanbieden van licenties onder ARBIT, een gewijzigde versie daarvan, of met enige verwijzing naar of vermenging met ARBIT is daarmee helaas niet mogelijk. Daarbij opgemerkt dat ARBIT de IP-rechten van de rechthebbende onvoldoende beschermt, onduidelijk is mbt gebruik, en eenzijdig opgesteld. Noemenswaardig is ook dat afwijking van ARBIT is toegestaan binnen de overheid. Leverancier verzoekt om voor de software licenties de standaard licentievoorwaarden uitsluitend van toepassing te verklaren op de software en het onderhoud daarop, zoals die al van toepassing zijn bij de Belastingdienst en zoals die ook op veel andere plaatsen binnen de rijksoverheid worden toegepast.	Zie het antwoord bij vraag 10: Artikel 11 is bij de interpretatie van dit artikel van doorslaggevende betekenis. Daar waar de licentievoorwaarden zien op het gebruik van de Prestatie, mogen de licentievoorwaarden inderdaad als leidend worden gezien, mits (!) wordt voldaan aan de eisen uit artikel 11. Het is aan de Inschrijvers om deze check te doen en eventueel maatregelen te treffen. Het eenvoudig doorsturen van de licentievoorwaarden is daarmee onvoldoende. Inschrijver zal moeten onderzoeken of de eventueel door te leggen licentievoorwaarden het beoogde en beschreven gebruik niet in de weg staan.
34	BIJLAGE-A-Specificatie-van-de-opdracht SOAR 2023 – HFDT2.1 - GUE-1 - p6	Een SOAR-oplossing zal normaal gesproken niet een incident detecteren maar acteren op een incident dat bijvoorbeeld uit een SIEM geëscaleerd is naar de SOAR-oplossing. Kunt u deze GUE aanpassen en de detectie eis verwijderen? Indien u hiertoe niet bereid bent/kunt zijn, kunt u dan verder ingaan hoe u de detectie door de SOAR-oplossing ziet?	Het betreft een typefout; de GUE wordt aangepast Dit is in BIJLAGE-A-Specificatie-van-de-opdracht SOAR 2023 versie 1.1 en Bijlage VII Conformiteitenlijst versie 1.1 aangepast.
35	BIJLAGE-A-Specificatie-van-de-opdracht SOAR 2023 – HFDT2.1 - GUE-11 - p6	Onze SOAR-oplossing heeft een eigen Secrets manager. Mag deze als alternatief voor de door U genoemde managers ingezet worden en als volwaardig alternatief gezien worden?	Mits uw Oplossing ook kan koppelen met een andere secrets managements oplossing, is dit akkoord. (Zie ook vraag 18.) De reden dat gevraagd wordt om integratie met de bestaande secrets management oplossingen is dat de Oplossing niet de enige tool zal zijn die geautomatiseerd acties uitvoert op de aangesloten componenten. De aangesloten componenten zullen ook door andere automation-platformen aangestuurd worden (denk aan CI/CD pipelines) en daarbij secrets gebruiken die gemanaged worden door de bestaande secrets management oplossingen.
36	BIJLAGE-A-Specificatie-van-de-opdracht SOAR 2023 – HFDT2.2 - GUE-20	Kunt u beschrijven (in een use case bijvoorbeeld) hoe u de verwerking en analyse van logbestanden en netwerkverkeersgegevens ziet binnen de SOAR-oplossing?	De GUE betreft integraties. De oplossing moet overweg kunnen met bv allerlei logformaten , maar ook met pcap bestanden. In het geval van bv een Suricata (IDS) notable event zou een pcap file opgehaald kunnen worden en zou metadata uit de pcap getoond kunnen worden. Het gaat dus o.a. om het automatiseren van handelingen die anders met de hand gedaan zouden moeten worden, zonder daarvoor zelf allerlei code te hoeven schrijven.
37	BIJLAGE-A-Specificatie-	Wij hebben vele standaard integraties beschikbaar op onze marketplace om achteraf te installeren, echter zijn deze nog niet	Ja

Nr	Locatie (document, hoofdstuk, pagina)	Vraag	Antwoord
	van-de-opdracht SOAR 2023 – HFDT2.2 – W-1 -p8	standaard geïnstalleerd op het platform. Dit kan achteraf gedaan worden en deze integraties zijn beschikbaar als onderdeel van de licentie. Mogen wij ervan uitgaan deze integraties als “out-of-the-box” kwalificeren?	
38	BIJLAGE-A-Specificatie-van-de-opdracht SOAR 2023 – HFDT2.2 – W-2 -p8	Onze integratie voor de SOAR-oplossing werkt in combinatie met een door Splunk zelf ontwikkelde integratie. Mogen wij ervan uitgaan deze integratie als “out-of-the-box” kwalificeert?	Dit kunnen we op basis van deze informatie niet beoordelen; dit is onderdeel van de beoordeling van uw inschrijving.
39	BIJLAGE-A-Specificatie-van-de-opdracht SOAR 2023 – HFDT2.2 – UE16 - p18	Security kennis rondom Threat Management is schaars in de markt, waardoor deze eis moeilijk op elk moment gegarandeerd ingevuld kan worden. Leverancier stelt voor om met Social Return bouwblokken te werken, zoals vaker gehanteerd, waarbij niet alleen kandidaten met een afstand tot de arbeidsmarkt op de uitvoering van de opdracht zijn in te zetten, maar bijvoorbeeld ook binnen de bedrijfsvoering van de opdrachtnemer.	De Opdrachtgever staat open voor suggesties; in UE15 is aangegeven dat Partijen na het tekenen van de Overeenkomst hier invulling over gaan afstemmen.
40	BIJLAGE-A-Specificatie-van-de-opdracht SOAR 2023 – HFDT2.2 – UE59 - p31	Leverancier heeft een volwassen supportafdeling die grotendeels voldoet aan de genoemde SLA's, echter wordt support geleverd op basis van eigen standaardvoorwaarden. Kunnen op basis daarvan afwijkende afspraken gemaakt worden?	Deze vraag is te algemeen; afwijkende afspraken zijn, tenzij deze beter zijn dan wat in UE 59 is gesteld, niet akkoord. Kunt u in NVI 2 aangeven op welke punten u wilt afwijken?
41	Beschrijvend document	1“De Overeenkomst wordt aangegaan voor de duur van 3 (drie) jaar, ingaande op 15 december 2023, met de mogelijkheid voor de Aanbestedende dienst om de Overeenkomst onder gelijkblijvende voorwaarden 7 (zeven) maal voor de duur van 1 (één) jaar te verlengen.” Zal bij start van de overeenkomst een PO worden afgegeven voor 3 jaar waarbij in 1 keer voor 3 jaar kan worden gefactureerd wat betreft de licenties?	Nee, facturatie vindt, conform artikel 8.5 van de concept Overeenkomst, jaarlijks vooraf plaats.
42	Beschrijvend document	Klopt het dat op basis van deze alinea, dat de Belastingdienst niet op zoek is naar een cloud-gebaseerde oplossing? Self hosted of SAAS? On-prem lijkt geen harde eis in de conformiteitenlijst	Dit is correct; dit is in paragraaf 2.4.1. van het Beschrijvend document (scope) benoemd.
43	Beschrijvend document	We denken dat er een foutje is geslopen in de planning. De “Nadere inlichtingen/stellen van vragen (2)” fase begint nu direct na de vorige ronde van inlichtingen. Er is geen mogelijkheid om vragen te stellen naar aanleiding van de eerste ronde van inlichtingen.	Zie ook vraag 25. De planning wordt als volgt aangepast: Nadere inlichtingen/stellen van vragen (2) Vr 29-09-2023 t/m Wo 11-10-2023 Dit is in Beschrijvend-Document-Openbare-Aanbesteding IUC 23-003, versie 1.1 aangepast.
44	Prijzenformulier	In dit document worden twee begrippen door elkaar gebruikt: Op tabblad Huurlicentie 2: “SOC gebruikers t.b.v. Productie omgeving met alleen betrekking op Playbooks” en op tabblad “dimensionering” wordt gesproken over “Ontwikkelen Playbooks” Kan de opdrachtgever aangeven wat ze van de verschillende rollen verwachten. Is dit een admin role die playbooks ontwikkelt of een gebruiker die playbooks gebruikt?	Zie paragraaf 7.2 Toelichting op Bijlage VIII “Prijzenformulier”, hier in staat o.a.: “ Er is onderscheid gemaakt in de verschillende gebruikers; er zijn SOC gebruikers die de Oplossing volledig gebruiken (zie Tabblad Huurlicenties 1) en gebruikers die de Oplossing alleen gebruiken om Playbooks te ontwikkelen en/of te implementeren (zie Tabblad Huurlicenties “
45	Prijzenformulier	Op tabblad “additionele diensten” wordt gesproken over opleidingen voor 40 personen. Tot welk niveau wil de opdrachtgever deze personen opgeleid hebben. Moeten deze personen gebruik kunnen maken van het product of in staat zijn het volledig te beheren incl de genoemde playbooks.	Er zijn opleidingen diverse niveaus nodig. Het uiteindelijke doel is zelf beheer van omgeving en Playbooks uit te voeren. Denk hierbij aan Opleidingen voor 5 beheerders, 5 Playbook makers en 30 SOC gebruikers (volledig gebruik van de Oplossing).
46	Prijzenformulier	Op tabblad “additionele diensten” wordt gesproken over opleidingen. Op welke termijn dienen deze opleidingen plaats te vinden?	Het is op voorhand niet bekend of en wanneer er Opleidingen nodig zijn. (Voor Opleidingen geldt dat er geen afnameverplichting is.)
47		In deze eis wordt gesproken over een aantal controls in de BIO. Kan de opdrachtgever aangeven welke versie van de BIO van kracht is. En indien mogelijk die versie verstrekken?	Het betreft BIO 1.04 en is bij deze Nota van Inlichtingen meegestuurd.
48	Bijlage A, UE 6	De belastingdienst vraagt een on-prem oplossing aan, onze aanname is dat het niet wenselijk is als wij als leverancier een vulnerability test uitvoeren op een oplossing bij de Belastingdienst. Kan deze eis komen te vervallen?	UE 6 wordt niet verwijderd. Conform UE 6 voert Opdrachtgever de Vulnerability scan zelf uit; de UE betreft het meewerken van de Opdrachtnemer bij het oplossen van geconstateerde kwetsbaarheden.
49	Bijlage A, UE 31	Leverancier biedt de meeste opleidingen virtueel aan. Zowel als e-learning of klassikaal. De kosten hiervan zijn lager, en er kan geleerd worden in een eigen tempo. Is dit een optie voor de Belastingdienst?	Akkoord

Nr	Locatie (document, hoofdstuk, pagina)	Vraag	Antwoord
50	Bijlage A, GUE 12	Threat intelligence is geen gebruikelijke functionaliteit voor een SOAR oplossing. Kan de opdrachtgever toelichten wat hier wordt bedoeld? Moet er gekoppeld kunnen worden met bepaalde Tip platformen? (MISP, Eclectiq) of gekoppeld kunnen worden met Thera tintel platformen als Recorderfuture, crowdstrike etc? Kan deze eis vervallen. Een SOAR oplossing verwerkt over het algemeen geen gegevens zoals gevraagd in deze eis. Wel wordt er bijv. via API's connecties gelegd naar oplossingen (SIEM, mail gateways, etc) die deze gegevens verwerken. In deze eis wordt gesproken over Policy en rule beheer. Kan de opdrachtgever aangeven wat zij beschouwen als policies en rules in de context van een SOAR oplossing?	Bij het opstellen van de uitvraag hebben we gebruik gemaakt van de definitie van Gartner voor SOAR: <i>"Gartner defines security orchestration, automation and response (SOAR) as solutions that combine incident response, orchestration and automation, and threat intelligence (TI) management capabilities in a single solution. SOAR tools can be leveraged for many security operations tasks, such as documenting and implementing processes, supporting security incident management, applying machine-based assistance to human security analysts and operators, and better operationalizing the use of TI."</i> Volgens deze definitie en in onze ervaring is Threat Intelligence wel degelijk gebruikelijke functionaliteit voor een SOAR-oplossing. Open Standaarden zijn belangrijk voor de opdrachtgever. Ondersteuning van STIX/TAXII is daarom als eis opgenomen voor integratie met bestaande TI-oplossing.
51	Prijzenformulier	Er wordt uitsluitend gesproken over SOC gebruikers. a. Klopt het dat SOAR alleen ingezet wordt door SOC gebruikers of zijn er ook andere gebruikers binnen Belastingdienst? b. De playbooks cq. inzet van SOAR is uitsluitend Security gerelateerd of ook daarbuiten?	Primair door SOC gebruikers, maar engineers van andere afdelingen worden/ zijn wel betrokken bij het opstellen/aanmaken van Playbooks voor hun omgeving. SOAR: bedoeld voor Security Playbook voor het SOC
52	Prijzenformulier	"een SOC gebruiker" is een unieke user ofwel heeft de user een persoonlijke naam of wordt de SOC gebruiker gedeeld door meerdere personen (bijv. SOC1@belastingdienst.nl)?	Een SOC gebruiker is een uniek persoon; zie ook paragraaf 7.2 Toelichting op Bijlage VIII "Prijzenformulier".
53	Bijlage A,	Prijzen worden gevraagd in euro. Kan de Belastingdienst de licenties ook in USD afnemen (om prijsverhoging te voorkomen ivm verzekeren het koersverschil) bij het uiteindelijke contract?	Nee
54	Bijlage A, wens 1	Koppeling met Cloud SIEM/SOAR (Microsoft, AWS, Google). Kan aanvrager aangeven met welke producten er een koppeling gemaakt moet worden. AWS heeft geen eigen SIEM/SOAR oplossing. Daarnaast is het de vraag of het zinnig is om meerdere SOAR's te koppelen, of vanuit één SOAR direct acties te laten uitvoeren in de desbetreffende omgeving.	Het gaat hier om een Wens; het is aan de Inschrijver aan te geven welke mogelijkheden zijn/haar Oplossing biedt om hier aan tegemoet te komen. Het is expliciet niet de bedoeling dat de Aanbestedende dienst dit voorschrijft.
55		Wil de Belastingdienst de voorwaarden van de softwareleverancier als onderdeel van de aanbesteding ontvangen en zo ja op welk moment?	Ja, conform GUE 43 moeten deze bij de Inschrijving worden ingediend
56		Kan de Belastingdienst aangeven wat ze bedoelen met het "consumer provider principe" zoals genoemd in kerncompetentie 1 voor de referentie?	Zie de uitleg bij GE 3 in het Beschrijvend-Document-Openbare-Aanbesteding IUC 23-003: "...de consumer is eigenaar van de data en de regels en de provider stelt het SOAR- platform ter beschikking..". Inrichting volgens het "consumer provider principe" houdt in dat de consumers van een dienst de werking van de dienst niet mogen kunnen verstoren (non-interferentie tussen Provider en Consumer) en dat de ene consumer het gebruik door de andere consumer niet mag kunnen verstoren (non-interferentie van consumers onderling). In het geval van de SOAR dienst is er sprake van een team (de provider) dat verantwoordelijk voor het beheer en onderhoud van de SOAR-dienst en een beperkt aantal teams (de consumers) die verantwoordelijk zijn voor het gebruik van de SOAR dienst (de consumers). De belangrijkste consumer van de SOAR dienst is het SOC van de opdrachtgever.