Nota van Inlichtingen Selectiefase - EA Managed SOC Provider

Nr.	Document	Pagina	§ / art.	Vraag
1	Bijlage C Programma van Eisen (Concept)	4	PvE 2.8	Kan EDSN bevestigen dat een actuele SOC 2 Type 2-verklaring kan worden geaccepteerd als bewijs van naleving en een deel van de auditverplichtingen kan vervangen?
2	Bijlage C Programma van Eisen (Concept)	4	PvE 2.8	In PvE 2.8 wordt beschreven dat EDSN gerechtigd is om zelf of via een derde partij audits uit te voeren, waarbij de opdrachtnemer verplicht is hieraan mee te werken. Vraag: Gaat EDSN ermee akkoord met de volgende voorwaarden met betrekking tot audits? •De opdrachtnemer heeft geen bezwaar tegen het uitvoeren van penetratietests of audits, mits deze worden uitgevoerd door een onafhankelijke derde partij. •De opdrachtnemer behoudt het recht om een auditor te weigeren wanneer dit een directe concurrent van de opdrachtnemer is. In dat geval zal opdrachtnemer dit schriftelijk onderbouwen, waarna EDSN de mogelijkheid heeft een andere partij te selecteren. •De auditor krijgt uitsluitend toegang tot data en systemen van EDSN die relevant zijn voor de audit. •De kosten voor het uitvoeren van de audit zijn voor rekening van EDSN, tenzij aantoonbare tekortkomingen aan het licht komen. •De kosten voor het verhelpen van valide bevindingen uit de audit zijn voor rekening van de opdrachtnemer. Vraag: EDSN vraagt in PvE 2.8 medewerking aan audits door of namens EDSN. Kan EDSN bevestigen dat een actuele SOC 2 Type 2-verklaring kan worden geaccepteerd als bewijs van naleving en daarmee een deel van de auditverplichtingen kan vervangen?
3	Bijlage C Programma van Eisen (Concept)	6,13	PvE 3.3, 9.3, 9.5	In de aanbestedingsdocumenten wordt geëist dat alle medewerkers Nederlands beheersen op niveau 3F/B2 en dat trainingen in het Nederlands worden verzorgd. Is het toegestaan om de dienstverlening grotendeels in het Engels uit te voeren, mits er tijdens kantooruren Nederlandstalige ondersteuning beschikbaar is voor afstemming met EDSN? Zo nee, kunt u de reden aangeven?

4	Bijlage C Programma van Eisen (Concept)	6,13	PvE 3.3, 9.3, 9.5	In de aanbestedingsdocumenten wordt geëist dat alle medewerkers Nederlands beheersen op niveau 3F/B2 en dat trainingen in het Nederlands worden verzorgd. Kan worden bevestigd dat de projectmanagementactiviteiten (inclusief implementatieplan) eveneens in het Engels mogen plaatsvinden, waarbij contractdocumenten in het Nederlands worden aangeleverd? Zo nee, kunt u een toelichting geven?
5	Bijlage C Programma van Eisen (Concept)	6,13	PvE 9.5	In de aanbestedingsdocumenten wordt geëist dat alle medewerkers Nederlands beheersen op niveau 3F/B2 en dat trainingen in het Nederlands worden verzorgd. Onze specialisten beschikken over uitstekende Engelse taalvaardigheden en ruime ervaring met het geven van trainingen. Kan EDSN bevestigen dat trainingen ook in het Engels mogen worden verzorgd, mits deze worden gegeven door hooggekwalificeerde specialisten, eventueel aangevuld met Nederlandstalige ondersteuning waar nodig?
6	Bijlage C Programma van Eisen (Concept)	8	PvE 6.23, 6.18	Onsite aanwezigheid binnen 2 uur en rol bij Incident Response(PvE 6.23, PvE 6.18) In PvE 6.23 wordt geëist dat de opdrachtnemer binnen 2 uur fysiek aanwezig is bij kritieke beveiligingsincidenten. Tegelijkertijd stelt PvE 6.18 dat de opdrachtnemer slechts ondersteuning biedt aan de door EDSN gecontracteerde incident response partij tijdens forensisch onderzoek. In de aanbestedingsdocumenten wordt bovendien vermeld dat incident response en forensisch onderzoek buiten de scope vallen.Kunt u toelichten wat precies het verschil is tussen de gevraagde response-activiteiten (zoals bedoeld in PvE 6.23) en de uitgesloten incident response (PvE 6.18)?
7	Bijlage C Programma van Eisen (Concept)	8	PvE 6.18	Is het de intentie van EDSN dat incident response en forensisch onderzoek altijd worden uitgevoerd door een andere partij, of kan dit op termijn alsnog binnen de scope komen (bijvoorbeeld na afloop van een ander contract)?

8	Bijlage C Programma van Eisen (Concept)	8	PvE 6.23	Kunt u verduidelijken waarom de eis van fysieke aanwezigheid binnen 2 uur (PvE 6.23) is opgenomen en in welke specifieke situaties deze eis geldt?
9	Bijlage C Programma van Eisen (Concept)	8	PvE 6.23	Is EDSN bereid deze eis te versoepelen, bijvoorbeeld door in eerste instantie remote ondersteuning toe te staan en fysieke aanwezigheid alleen in uitzonderlijke gevallen te verlangen?
10	Bijlage C Programma van Eisen (Concept)	8	PvE 6.20	Vraag: In PvE 6.20 wordt geëist dat de opdrachtnemer gedurende de gehele looptijd van de ROVK adequaat opgeleid en gecertificeerd personeel beschikbaar heeft om de Managed SOC-dienstverlening 24/7 uit te voeren. Kan EDSN bevestigen dat met deze eis wordt bedoeld dat er gedurende de volledige 24/7-periode daadwerkelijk bemand toezicht (“eyes on glass”) aanwezig moet zijn, en niet alleen geautomatiseerde monitoring of stand-by beschikbaarheid?
11	Bijlage C Programma van Eisen (Concept)	8	PvE 6.25	PvE 6.25 schrijft voor dat de opdrachtnemer bij aanvang van de overeenkomst een exitplan aanlevert. Onze ervaring is dat een exitplan pas zinvol kan worden uitgewerkt wanneer de dienstverlening operationeel is en de daadwerkelijke omgeving en processen duidelijk zijn. Kan EDSN bevestigen dat bij aanvang van de overeenkomst een globaal exitplan met uitgangspunten en werkwijze volstaat, en dat de concrete planning en activiteiten pas worden uitgewerkt in een afzonderlijk decommissioning project indien een beëindigingsscenario zich voordoet?
12	Bijlage C Programma van Eisen (Concept)	9	PvE 6.29	In PvE 6.29 wordt geëist dat data-at-rest en data-in-transit versleuteld is, waarbij minimaal TLS 1.3 wordt toegepast. Er worden echter geen eisen beschreven voor data die ‘in gebruik’ (Data in Use) is, bijvoorbeeld gegevens die actief worden geraadpleegd door security-analisten en threat hunters in het SIEM. Onze ervaring is dat encryptie van data in gebruik in de praktijk een aanzienlijke performance-impact kan hebben op realtime detectie en snelle respons op beveiligingsincidenten. Wij hanteren hiervoor andere adequate beveiligingsmaatregelen, waaronder strikte toegangscontrole, monitoring en compliance met ISO27001 en ISAE-3000/SOC 2 Type 2. Gaat EDSN ermee akkoord dat met deze aanpak wordt voldaan aan de intentie van de eis in PvE 6.29?
13	Bijlage C Programma van Eisen (Concept)	3	Eis 2.4 Artikel 21 ARVODI	Op basis van PvE en artikel 21 ARVODI 2018 geldt voor deze opdracht (waarde maximaal € 1,728 miljoen) het aansprakelijkheidsplafond van € 3 miljoen per gebeurtenis en € 5 miljoen per jaar. Dit betekent dat de potentiële aansprakelijkheid meerdere malen hoger ligt dan de totale contractwaarde, wat niet proportioneel is in verhouding tot de baten. Daarnaast wordt geen onderscheid gemaakt tussen directe en indirecte schade. Wij constateren dat deze limieten en reikwijdte aanzienlijk afwijken van wat gebruikelijk is in de cybersecuritybranche, waar aansprakelijkheid doorgaans is gelimiteerd tot de jaarlijkse waarde of een percentage van de opdrachtsom en indirecte schade wordt uitgesloten. Dit leidt tot een risico dat niet in verhouding staat tot de opdrachtwaarde en kan het aantal inschrijvers beperken. Staat EDSN open om in de gunningsfase te bespreken of bij de conceptovereenkomst zelf aan te geven of de aansprakelijkheid kan worden aangepast naar een proportioneel niveau dat in verhouding staat tot de opdrachtsom? Zo nee, kunt u toelichten.

14	Bijlage C Programma van Eisen (Concept)	3	Eis 2.4 Artikel 21 ARVODI	Is ESDN bereid te aanvaarden dat een partij uitsluitend aansprakelijk is voor de directe schade welke door de wederpartij als gevolg van een toerekenbare tekortkoming wordt geleden en dat een partij niet aansprakelijk is voor gevolgschade of andere indirecte schade (hieronder wordt verstaan schade welke redelijkerwijze niet objectief voorzienbaar was als een gevolg van het handelen of nalaten van de partij aan wie de schade kan worden toegerekend)? Aansprakelijkheid voor gevolgschade of andere indirecte schade brengt namelijk grote bedrijfseconomische risico's met zich mee omdat dat de potentiële schadepost(en) niet te overzien zijn. Hierdoor kan het geclaimde schadebedrag onredelijk hoog oplopen en in geen verhouding staan tot de omvang van de Prestatie. Hoe kijkt u hier tegenaan, in het licht van redelijkheid en billijkheid?
15	Bijlage C Programma van Eisen (Concept)	3	Eis 2.4 Artikel 21 ARVODI	Is EDSN bereid om het aansprakelijkheidsplafond te koppelen aan de jaarlijkse contractwaarde (ongeacht het aantal gebeurtenissen) in plaats van de vaste bedragen uit ARVODI 2018?
16	Selectieleidraad Managed SOC provider	13	Paragraaf 3.8	In de Selectieleidraad komen meerdere keren foutmeldingen voor zoals "Fout! Verwijzingsbron niet gevonden." (o.a. in paragraaf 3.8). Hierdoor is niet duidelijk naar welke passage of welk document wordt verwezen. Kan EDSN een versie van de Selectieleidraad beschikbaar stellen waarin deze interne verwijzingen zijn gecorrigeerd, of aangeven naar welke paragrafen/bijlagen deze verwijzingen behoren?
17	Selectieleidraad Managed SOC provider	17	Paragraaf 3.12	In de Selectieleidraad wordt niet gespecificeerd op welke wijze documenten in de selectiefase moeten worden ondertekend. Mag de aanmelding in de selectiefase digitaal worden ondertekend?
18	Selectieleidraad Managed SOC provider	22	4.2 Planning	De periode tussen notificatie van het aanleveren van de selectiecriteria (9 september) en de uiterste inleverdatum (12 september) bedraagt slechts drie werkdagen.Is EDSN bereid de termijn tussen notificatie en inlevering selectiecriteria te verruimen, zodat inschrijvers voldoende tijd hebben voor een zorgvuldige uitwerking?
19	Selectieleidraad Managed SOC provider	22	4.2 Planning	Kunt u aangeven wat de verwachte startdatum van de overeenkomst is, zodat inschrijvers hiermee rekening kunnen houden in hun planning en resource-allocatie?
20	Selectieleidraad Managed SOC provider	22	4.2 Planning	In de Selectieleidraad staat uiterste datum deelnemingsaanvragen op 8 september 12:00, in TenderNed staat 10:00. Kunt u aangeven welke tijd juist is?
21	Selectieleidraad Managed SOC provider	26	Paragraaf 5.1	In de Selectieleidraad is het UEA als bijlage opgenomen, terwijl op het portaal een digitale UEA-vragenlijst beschikbaar is. Welke versie verwacht u van Gegadigde?
22	Standaardformulier 05 Referentieverklaring	1	Referentie	Is het toegestaan om de contactgegevens van de referenties bij verificatie door te geven? Wij willen zorgvuldig met deze gegevens omgaan. Aanbestedende dienst heeft deze gegevens pas nodig wanneer zij de referentie willen verifiëren.
23	Bijlage C Programma van Eisen (Concept)	7	Eis PvE 6.2	Kan EDSN bepalende kenmerken/specificaties zoals aantallen, hoeveelheid ingested data, etc. van de te monitoren multi cloud omgevingen aanvullen.

24	Selectieleidraad Managed SOC provider	5	2.3	In de Selectieleidraad wordt Microsoft Sentinel benoemd als centrale SIEM-oplossing, met daarbij de kanttekening dat de precieze invulling van de Managed SOC-dienstverlening onderwerp is van overleg in de gunningsfase. Wij beschikken over een gestandaardiseerde SOC-architectuur waarin incidentanalyse, triage, use case-ontwikkeling, rapportage én proactieve threat hunting plaatsvinden binnen een omgeving die samenwerkt met zowel Sentinel als AWS. Deze architectuur is volledig operationeel in hybride cloudomgevingen, wordt uitsluitend gehost binnen de EER, en maakt het mogelijk om beveiligingsinformatie uit meerdere omgevingen centraal te correleren. Een bijkomend voordeel van deze opzet is dat de bestaande AWS-monitoring niet hoeft te worden geïntegreerd in uw bestaande Sentinel: de SOC-architectuur voorziet zelf in de koppeling en correlatie tussen de huidige KA- en CMF-monitoringomgevingen. Is EDSN bereid om een oplossing te overwegen waarbij Sentinel primair fungeert als dataleverende SIEM, terwijl de centrale correlatie, threat detection & hunting, en incidentafhandeling plaatsvinden binnen een complementair platform dat deze integratielast wegneemt en end-to-end zicht biedt over beide omgevingen?
25	Selectieleidraad Managed SOC provider		6.26	In 6.26 beschrijft u dat de Opdrachtnemer dient te beschikken over een roadmap van de dienstverlening voor de aankomende twee jaar. Binnen cybersecuritydienstverlening is het ongebruikelijk om een roadmap op te stellen met (gecommitteerde) specifieke features voor een dergelijke termijn. De markt is immers veranderlijk en innovaties volgen elkaar in rap tempo op. Is de Opdrachtgever bereid de minimale periode van twee jaar los te laten en invulling van de roadmap over te laten aan de marktpartijen?
26	Selectieleidraad Managed SOC provider		3.3	In 3.3 geeft u aan dat alle communicatie tussen Opdrachtnemer en ESDN dient te geschieden in de Nederlandse taal. Binnen operationele SOC-teams is het echter gebruikelijk dat de Engelse taal wordt gehanteerd in systemen en geschrift tijdens triage en analyse van alerts en (potentiële) cyber security incidenten. Is de Opdrachtgever bereid deze eis aan te passen en een uitzondering aan te brengen voor operationele communicatie tussen IT-personeel van Opdrachtgever en Security Analisten van Opdrachtnemer?
27	Selectieleidraad Managed SOC provider		Hoofdstuk 5	In de scopeafbakening (hoofdstuk 5) plaatst u Incident response en forensisch onderzoek expliciet buiten scope. Uit ervaring blijkt echter dat er significante voordelen kunnen worden behaald wanneer Digital Forensics & Incident Response (DFIR) en SOC-dienstverlening bij eenzelfde partij zijn belegd. Zo kan er vanuit Incident Response team sneller worden gereageerd op incidenten door interne escalatie paden tussen het DFIR en SOC-team. Is de Opdrachtgever bereid om de buiten scope plaatsing van DFIR te heroverwegen?
28	Selectieleidraad Managed SOC provider		Uitsluitingsgronden en Geschiktheidseisen	In de Uitsluitingsgronden en Geschiktheidseisen beschrijft u een tweetal kerncompetenties die doormiddel van een of meer (maximaal twee) referenties en/of tevredenheidsveklaring moeten worden onderbouwd. Staat de Opdrachtgever het de Gegadigde toe kerncompetentie nummer twee doormiddel van twee individuele referenten aan te tonen? Bijvoorbeeld: Referent X toont de deskundigheid en ervaring aan met Azure-elementen en referent Y toont dat aan met AWS-elementen.
29	Selectieleidraad Managed SOC provider		Data Microsoft Sentinel	Selectieleidraad H2.3.1: In de huidige situatie wordt reeds gebruik gemaakt van Microsoft Sentinel. Kun u aangeven hoeveel GB aan data er momenteel wordt geïnjecteerd/verwerkt?

30	Selectieleidraad Managed SOC provider		Data CMF-omgeving	Selectieleidraad H2.3.1: Over de CMF-omgeving wordt nog weinig verteld, maar is er wel al een inschatting te maken over de hoeveelheid data (in GB) die verwerkt zal gaan worden?
31	Selectieleidraad Managed SOC provider		Issue tracker tool	6.5 - Om welke “issue tracker tool” gaat het, of is dat nog onbekend? (Ons advies is om een tool te gebruiken waarbij er een API koppeling mogelijk is.)
32	Selectieleidraad Managed SOC provider		5.4.2 Technische bekwaamheid en beroepsbekwaamheid - Referenties	Staat u ervoor open dat wij een referent aanleveren met geïntrigeerde monitoring in multi vendor omgeving met andere omgevingen als AWS?
33	Selectieleidraad Managed SOC provider		4.2 Planning	Het aantal dagen voor het inleveren van de beantwoording is erg kort op de aanmelding/selectie, kunnen wij hiervoor meer tijd krijgen?
34	Programma van eisen		Programma van Eisen 2.13	Verzoek tot aanpassing van vrijwaring van aansprakelijkheid van Derden (Programma van Eisen 2.13) tot de waarde van de mogelijk te leveren dienst te kaderen.
35	Programma van eisen	12		Op pagina 12 noemt u een verklaring omtrent gedrag. Onze medewerkers bevinden zich allemaal in de EER, maar wel ook buiten NL. Accepteert u een europees equivalent (per land kan dit vreschillen) van de Nederlandse Verklaring omtrent gedrag?
36	Programma van eisen & Selectie leidraad	7 Programma van eisen & 9 selectieleidraad		Op pag 7 noemt u 3% jaarlijkse verhoging: Als we de tabel op pagina 9 selectieleidraad (bv 2027-> 2028) bekijken met betrekking tot de waarde van de opdracht verdeeld over de kalenderjaren, zien we een verhoging die hoger is dan het maximum van 3%. Kunt u verduidelijken wat het standpunt van EDSN hierover is?
37	Divers	Divers		Sommige documenten bevatten de foutmelding "Fout! Referentiebron niet gevonden". Kunnen wij de gecorrigeerde versie ontvangen?
38	Overig	Overig		Zijn er diensten nodig met betrekking tot:
39	Overig	Overig		-Integratie van dreigingsinformatie
40	Overig	Overig		-Beoordeling van kwetsbaarheden
41	Overig	Overig		-Pentests op interne en externe netwerken

42	Overig	Overig		-Kunnen we statistieken krijgen over de huidige dienstverlening (aantal incidenten per ernst, volume van EPS, aantal ondersteunde gebruikers, werkstations per type, aantal servers, huidige geïntegreerde bronnen, enz.
43	Selectieleidraad	11,12		EDSN noemt Microsoft Sentinel als centrale SIEM-oplossing. In hoeverre is het toegestaan om aanvullende technologieën (bijvoorbeeld eigen SIEM/SOAR-oplossingen of proprietary tools) te integreren, mits dit aantoonbaar de detectie- en responscapaciteit vergroot?
44	Selectieleidraad	11,12		In hoeverre speelt data autonomie een rol in het toekomst beeld van EDSN en hoe past Sentinel in dat toekomst beeld(voor de looptijd van het contract incl verlengingen)?
45	Programma van eisen	6,7	Scope & Integratie	Er wordt verwezen naar logbronnen zoals Jira, Confluence en AFI. Kan EDSN een geprioriteerde lijst van systemen en applicaties verstrekken die minimaal binnen de looptijd gekoppeld moeten worden?
46	Programma van eisen	6,7	Scope & Integratie	KA-omgeving: Bij een integratie wordt het meeste integratiewerk meestal uitgevoerd op de andere genoemde systemen, zoals Exact, JIRA, Confluence, AFI (Office 365 Backup). Is dit het geval bij EDSN? Vaak bevatten deze omgevingen veel maatwerk. Kunt u een stanraard API aanleveren of verwacht u van de leverancier om aanpassingen te kunnen maken. zodat hoe zou dat er uit moeten zien? heeft EDSN een omschrijving van dit maatwerk/ deze maatwerk API?
47	Selectieleidraad	13	Scope & Integratie	Naast Azure en AWS, verwacht EDSN dat er ook integraties met andere cloudplatformen of SaaS-applicaties nodig zullen zijn? Zo ja, welke staan reeds op de roadmap?
48	Selectieleidraad	13	Scope & Integratie	In hoeverre speelt data autonomie een rol in het toekomst beeld van EDSN en hoe past Azure en AWS in dat toekomst beeld (voor de looptijd van het contract incl verlengingen)?
49	Programma van eisen	8,9	Incident Response & Rollen	EDSN benoemt een separate incident response partij. Hoe worden de verantwoordelijkheden en escalatieroutes tussen SOC-provider en IR-partij in de praktijk belegd, met name in crisissituaties?
50	Programma van eisen	10	Incident Response & Rollen	De eis stelt dat de leverancier binnen 2 uur fysiek in Amersfoort aanwezig moet kunnen zijn. Staat EDSN alternatieve oplossingen toe (zoals een bewezen remote rapid response capability), mits dit sneller en efficiënter is?
51	Selectieleidraad	12	Incident Response & Rollen	In de KA-omgeving mag de SOC direct ingrijpen, in de CMF-omgeving niet. Hoe waarborgt EDSN in de praktijk dat incidentrespons in de CMF-omgeving niet vertraagd wordt door verplichte escalatie?
52	selectieleidraad	9,10	Contract & Governance	De contractduur is 2 jaar met 6 verlengopties. Welke criteria of KPI's hanteert EDSN om te besluiten wel of niet te verlengen?
53	Programma van eisen	12	Contract & Governance	Audits kunnen door EDSN worden uitgevoerd. Worden deze audits altijd vooraf aangekondigd of kan dit ook onaangekondigd plaatsvinden?
54	Programma van eisen	14	Contract & Governance	Er wordt gevraagd om een exit-plan. Hanteert EDSN hiervoor een standaardformat of mag de leverancier een eigen model aanleveren?
55	Programma van eisen	15	Data & Privacy	Alle data dient binnen de EER te worden opgeslagen. Staat EDSN encryptie en verwerking in non-EER datacenters toe als aantoonbaar soevereiniteit en compliance wordt geborgd?
56	Selectieleidraad	14	Data & Privacy	Voert EDSN zelf de verplichte DPIA uit of verwacht men dat de leverancier deze voorbereidt en aanlevert?

57	Selectieleidraad	8	Financieel & Commercieel	De totale opdrachtwaarde wordt geraamd op €1,15M over 8 jaar. Kan EDSN toelichten (gedetailleerd en per kosten element als data hoeveelheid, # log sources, eps, etc)hoe dit bedrag is opgebouwd en of en hoe het rekening houdt met groei in logbronnen en incidentvolumes?
58	Selectieleidraad	16	Financieel & Commercieel	Indexering is gelimiteerd tot CBS-index of max. 3%. Is EDSN bereid een alternatieve indexatie te overwegen indien dreigingslandschap of logvolumes substantieel toenemen?
59	Programma van eisen	18	Financieel & Commercieel	Reis- en verblijfskosten dienen te zijn inbegrepen. Hoe ziet EDSN dit in relatie tot internationale inzet van specialisten (bijvoorbeeld voor forensisch onderzoek of red teaming)?
60	Programma van eisen	20	Samenwerking & Strategie	Er wordt gevraagd om een roadmap van 2 jaar. Op welke manier worden leveranciers betrokken in het bredere security maturity plan van EDSN?
61	Selectieleidraad	7	Samenwerking & Strategie	Wordt van de SOC-provider verwacht dat deze ook threat intelligence deelt of actief samenwerkt met andere sectorpartijen zoals netbeheerders of het NCSC?