

Bijlage 10

Samenvatting marktconsultatie

SIEM-Dienstverlening

Datum: 30 juli 2020
Versie: 1.0
Auteur: Sander Hompus

Inhoudsopgave

1	Inleiding en toelichting	3
2	Reactie op de marktconsultatie	4
2.1	Scoping dienstverlening	4
2.2	Implementatie	5
2.3	Borgen kwaliteit	6
2.4	Verdeling rollen	6
2.5	Toetsing op prijscriteria	6
2.6	Ervaring sector	6
2.7	Duurzaamheid	6

1 Inleiding en toelichting

Met dit document geven wij u uitleg ten aanzien van de Marktconsultatie die SURFnet heeft gehouden met betrekking tot een voorgenomen aanbesteding voor SIEM-Dienstverlening.

De gevolgde marktconsultatie was een informatie-uitwisseling tussen een aanbestedende dienst en (verschillende) relevante marktpartijen. Met de ideeën, kennis en kunde die hiermee is verkregen heeft de SURF de haalbaarheid en de randvoorwaarden van de voorgenomen opdracht van een eventuele aanbesteding vastgesteld en haar bestaande ideeën en wensen getoetst, voordat de daadwerkelijke aanbesteding gestart werd.

De marktconsultatie maakt *geen* onderdeel uit van de aanbestedingsprocedure zelf, maar heeft tot doel gehad de reeds bestaande eisen en/of wensen ten aanzien van de opdracht te toetsen en te verbeteren.

Met de reacties en antwoorden van diverse marktpartijen in de hand, is verder gewerkt aan de aanbestedingsstukken, waar dit document als Bijlage 10 onderdeel van uitmaakt. In dit document wordt samenvattend toegelicht welke antwoorden marktpartijen hebben gegeven op de door SURF gestelde vragen, en hoe verbetervoorstellen of wijzigingssuggesties in eisen, scope, en andere aspecten van de aanbesteding zijn meegenomen in de aanbestedingsstukken die nu voor u liggen. Per vraag of set van vragen, zal worden ingegaan op hoe een en ander verwerkt is in de aanbestedingsstukken.

2 Reactie op de marktconsultatie

In dit hoofdstuk treft u een samenvatting van de gegeven antwoorden op (sets van) vragen die gesteld zijn binnen de marktconsultatie. Ook vindt u hier een korte toelichting hoe een en ander is verwerkt binnen de aanbestedingsstukken. **NB:** De hier benoemde informatie is niet te herleiden tot een marktpartij.

2.1 Scoping dienstverlening

Vraag 1: In welke mate is de beschreven scoping relevant met het oog op de technologische ontwikkelingen en welke relevante onderdelen ontbreken hierin mogelijk die wel meerwaarde bieden?

Door partijen is aangegeven dat de scope in hoofdlijnen goed is. Wel is aangegeven dat goed beschreven dient te worden wat wel en niet binnen scope is. Dit heeft ertoe geleid dat in het Beschrijvend document paragraaf 1.3.1 een bredere uiteenzetting is gegeven van in/out scope. Hierbij geldt dat een aantal onderdelen niet binnen de scope zijn opgenomen, zoals het inzetten van Threat Hunting. Gezien de gewenste scope van de SIEM-dienstverlening, is het inzetten van een actief middel als Threat Hunting als niet passend geacht.

Ook het inzetten van SOAR werd door diverse partijen als optie genoemd om op te nemen in de scope, als doorontwikkeling. Gezien dat SOAR op dit moment nog niet door alle leveranciers aangeboden kan worden, is het te beperkend om dit op te nemen binnen scope dan wel te vereisen. Echter, nergens is een verbod opgenomen om technieken als SOAR toe te passen als dit past binnen de gegeven scope van de dienstverlening en als dit tot leidt tot een verbetering van de dienstverlening (hogere kwaliteit en/of lagere kosten).

Vraag 2: Welke onderdelen van de scoping kunt u aan de instellingen leveren inclusief onderhoudsdiensten en support?

Vanuit de marktpartijen is aangegeven dat zij in staat zijn de gevraagde dienst te leveren, zoals voorgestaan. Hierbij is wel aangegeven dat er gekeken moet worden naar de leveringsvorm, waarbij een SaaS-oplossing en een plaatsing van de oplossing binnen de infrastructuur van de Instelling de uiterste varianten zijn. In Bijlage 1: Opdrachtoomschrijving is specifiek onderbouwd waarom gekozen is voor het uitvragen van de huidige leveringsvormen, waarbij geëist wordt dat Inschrijvers beide vormen kan leveren. Kort gezegd heeft dit te maken met de uitdrukkelijke eis van diverse instellingen zelf regie te hebben op de oplossing, door deze in de infrastructuur geplaatst te hebben en aan de andere kant de wens om ook kleinere Instellingen die niet de capaciteit hebben de oplossing in de eigen infrastructuur geplaatst te hebben aan te kunnen sluiten op de dienstverlening.

Vraag 3: Kunt u een SIEM leveren waarbij deze wordt geplaatst bij een instelling, maar ook waarbij een SIEM wordt geplaatst bij SURF? Bij deze laatste variant dienen de instellingen hierop aan te kunnen sluiten. Beschrijf welke voordelen de verschillende varianten hebben en hoe een Instelling een goede afweging kan maken tussen de leveringsvormen.

Zie het vorige antwoord.

Vraag 4: Kunt u met uw dienstverlening aansluiten op een bestaande SIEM als een instelling deze al heeft?

Partijen geven aan dat dit technisch wel mogelijk is, maar raden het af dit als eis te formuleren. Dit is dan ook niet als eis opgenomen.

Vraag 5: Kunt u aangeven of u op basis van de gedefinieerde scope, doelstellingen en gewenste invulling van de dienstverlening, deelneemt aan deze aanbesteding? Zo niet, onder welke voorwaarden zou u wel deelnemen aan deze Aanbesteding?

In algemeenheid geeft de markt aan in te gaan schrijven. Een aantal afhankelijkheden is wel benoemd.

Vraag 6: In bijlage 2 vindt u een overzicht van voorlopige eisen. Op een aantal eisen is nog geen inhoud geformuleerd. Dit betreft de eisen: A2 (zie vragen 13, 14 en 15 verderop) A6, A9, S7, E1 (zie tevens vragen 7, 8, 9 en 10). Kunt u meedenken ten aanzien van de invulling van deze eisen. En: Vraag 7: Heeft u andere vragen en/of opmerkingen ten aanzien van het Programma van Eisen, zoals weergegeven in Bijlage 2: Programma van eisen.

Voor de verwerking van de gemaakte opmerkingen, wordt u verwezen naar Bijlage 2 Programma van Eisen.

2.2 Implementatie

Vraag 8: Wat is de geschatte doorlooptijd om de gevraagde dienstverlening op orde te krijgen? Dit betreft de tijd na gunning om de dienst te kunnen gaan leveren aan Instellingen.

De gegeven antwoorden liepen uiteen. In Bijlage 1: Opdrachtbeschrijving vindt u een overzicht van hetgeen van de implementatie verwacht wordt waarbij aangesloten is op de gegeven reacties. Tevens vindt u in Bijlage 2 Programma van Eisen (H6) de eisen die hieraan gesteld worden.

Vraag 9: Wat is de geschatte doorlooptijd om een Instelling van de dienst gebruik te laten maken? Dit betreft de tijd vanaf het moment dat een Instelling aangeeft de dienst af te nemen tot en met het moment dat deze Instelling in productie is, use-cases zijn ingericht, er meldingen gegenereerd worden en adviezen worden gegeven. Wat zijn succesfactoren voor snelle tijdslijnen?

De antwoorden op deze vraag liepen niet ver uiteen. In Bijlage 2 Programma van Eisen (H6) vindt u de eisen ten aanzien van de doorlooptijd en/of aantal aan te sluiten Instellingen per kwartaal welke zijn gebaseerd op de in de marktconsultatie gegeven antwoorden.

Vraag 10: Op welke manier acht u het mogelijk om meerdere Instellingen tegelijkertijd aan te sluiten?

Marktpartijen geven aan dat het mogelijk is Instellingen tegelijkertijd en/of parallel aan elkaar aan te sluiten. Van inschrijvers wordt verwacht dat zij aangeven hoe zij hier specifiek vorm aan willen geven, zoals gevraagd in subgunningscriterium K3: Implementatie. Tevens zijn op basis van de uitkomsten van de marktconsultatie de betreffende eisen in Bijlage 2: Programma van Eisen opgesteld.

Vraag 11: Acht u het zinvol voor Aanbestedende dienst om een PoC verplicht te stellen en zo ja, hoe zou die dan ingericht moeten worden?

Marktpartijen geven aan dat een PoC niet zinvol is. Wel geeft de meerderheid aan dat een 'testperiode' wel zinvol kan zijn. Om die reden heeft aanbestedende dienst er voor gekozen a) de implementatietermijn van 6 maanden te hanteren (zie Bijlage 2: Programma van Eisen, H6) en b) toepassing te geven aan een wachtkamerconstructie (zie Beschrijvend Document, H4.2).

2.3 Borgen kwaliteit

Vraag 12: Op welke wijze borgt u de kwaliteit van uw dienstverlening en meer specifiek de borging van een juiste omgang met privacy en security?

Partijen geven diverse maatregelen aan te hebben geïmplementeerd, onder meer op basis van diverse certificeringen. Omdat de diverse normeringen (ISO27001 of vergelijkbare) door marktpartijen veelal worden gehanteerd, is gekozen in subgunningscriterium K1 nader uit te vragen hoe partijen specifiek omgaan met security en privacy by design.

2.4 Verdeling rollen

Vraag 13: Hoe ziet u de rolverdeling Instelling, SURF en uzelf bij uitvoering van deze opdracht? Welke verantwoordelijkheden draagt eenieder voor een optimale realisatie van de doelstellingen.

Vanuit de markt wordt aangegeven dat het handig kan zijn een RACI op te stellen en dit op te nemen als onderdeel van hetgeen een Inschrijver dient aan te leveren bij Inschrijving. Om de rolverdeling te concretiseren, is gepoogd een uitwerking te geven van de rolverdeling in Bijlage 1 Opdrachtoomschrijving. Tevens is bij de diverse subgunningscriteria (met name K1 en K3) gevraagd naar de rolverdeling tussen inschrijver, Instelling en SURF, met de in de aanbestedingsstukken benoemde uitgangspunten als basis.

2.5 Toetsing op prijscriteria

Ten aanzien van de prijscriteria zijn diverse vragen gesteld. De antwoorden hierop liepen uiteen ten aanzien van de onderdelen die uitgevraagd dienen te worden en ten aanzien van berekening aan de hand van eps versus GB/dag. Hiermee is er niet een eenduidige lijn naar voren gekomen voor een prijsmodel dat door alle leveranciers gebruikt wordt. Gevolg is dat Aanbestedende dienst op basis van de gegeven input een zo goed mogelijk prijsmodel heeft ontwikkeld, wetend dat dit niet 100% aansluit bij een der modellen die in de marktconsultatie aangedragen zijn. In het Beschrijvend Document, en op het Prijzenblad, vindt u de toelichting van de wijze waarop omgegaan wordt met de prijs.

2.6 Ervaring sector.

Vraag 17: In welke mate heeft u ervaring met de onderwijs- en onderzoeksector?

De meerderheid van de marktpartijen is bekend met en levert aan de onderwijs- en onderzoeksector. Dit beperkt zich vaak echter tot diensten buiten de SIEM/SOC dienstverlening. Om die reden is in de aanbestedingsstukken niet gevraagd naar specifieke ervaring met het leveren van een SIEM-oplossing binnen de onderwijs- en onderzoeksectoren

Vraag 18: Heeft u ervaring met het leveren van een bijdrage aan onderzoek en onderwijs vanuit de geleverde dienstverlening? Geef aan op welke wijze hier mogelijk ruimte voor kan zijn bij deze Aanbesteding.

Marktpartijen geven aan hier bijdragen aan te kunnen leveren, in diverse vormen.

2.7 Duurzaamheid

Vraag 19: Welke mogelijkheden ziet u om duurzaamheid te bevorderen binnen deze opdracht?



Over het algemeen wordt opgemerkt dat bepaalde leveringsvormen energiezuiniger zijn. Duurzaamheid maakt deel uit van de beoordeling via subgunningscriterium K4.