

Opsteller
Michel Zegerman

Aantal pagina's
4

Behandelend gremium
[Click or tap here to enter text.](#)

Datum
07 maart 2024

Agendapunt, Onderwerp
Resultaten marktconsultatie SOC

Agendering
Ter info

Kopie aan
N/A

Kenmerk

1 Inleiding

Op 15 februari jl. heeft de leveranciersbijeenkomst in het kader van de marktconsultatie Security Monitoring & Alarmering Waterschappen plaatsgevonden in hotel Van der Valk A1 te Amersfoort. De aanwezige deelnemers zijn hierbij aan de hand van de reeds gedeelde presentatie geïnformeerd over de voorgenomen aanbesteding van Het Waterschapshuis op het gebied van SOC-dienstverlening. Het doel van de marktconsultatie is om een zo goed mogelijk inzicht te verkrijgen in de mogelijkheden die de markt kan bieden en in hoeverre de ambities van de Waterschappen, op het gebied van gezamenlijke SOC-dienstverlening, haalbaar zijn voor de markt.

Aan de leveranciersbijeenkomst hebben 40 bedrijven deelgenomen. Hiervan hebben 19 bedrijven schriftelijk gereageerd op vragen die aanvullend op de sessie zijn gepubliceerd via Tendered. In dit document zijn de belangrijkste bevindingen vanuit de reacties weergegeven.

2 Technisch ontwerp

De meerderheid (geschat 90%) van de marktpartijen geeft aan dat de gewenste oplossing (scenario 3) zonder problemen geleverd kan worden. Ook is het mogelijk om aanvullend (als plusdienst) de optionele oplossing (scenario 1) aan te bieden. De meerderheid van partijen is ook bereid dit dusdanig aan te bieden. Een aantal partijen geeft aan dat zij al bestaande oplossingen hebben draaien die ook voor de Waterschappen bruikbaar zal zijn.

Een aantal partijen geven daarbij wel aan dat een gecombineerde/ hybride oplossing kostenverhogend zal zijn, i.v.m. het optuigen en in standhouden van twee verschillende oplossingen en vanwege de noodzakelijke koppelingen en interfaces.

Er worden geen echte randvoorwaarden aan het leveren van de technische oplossingen gesteld anders dan, dat Project- en Service Level Management centraal (bijvoorbeeld binnen hWh) ingericht moet zijn. Dit zien zij als een vereiste om de verschillen in cybervolwassenheid, de verschillende geïmplementeerde oplossingen en de afstemming rondom keuzes in scenario's centraal gecoördineerd en beheerst te houden. Deze randvoorwaardewordt ook aangehaald onder de paragraaf Samenwerking.

Memo

3 Gebruik Sentinel

Een flink aantal marktpartijen gebruikt de Microsoft SIEM tooling en zal deze dan ook aanbieden voor de gevraagde oplossing. Daarnaast zijn er partijen die geen Microsoft partner zijn, maar die wel kunnen aansluiten op Sentinel. Interfacing tussen de lokale SIEM-oplossingen en de centrale dienstverlening wordt dan ook niet als een probleem ervaren. Ook niet voor wat betreft reeds geïmplementeerde SIEM-oplossingen van andere leveranciers. Ook wordt de integratie met de overige E5-applicaties als voordeel gezien.

Door veel partijen werd het OT-onderwerp vermeden in de antwoorden op de marktconsultatie. Dit was ook logisch daar de meeste aanwezige partijen wel kennis en ervaring m.b.t. KA hebben en weining tot geen ervaring met PA.

De partijen die al bekend zijn met OT en Sentinel waarschuwen dat Sentinel wel gebruikt kan worden voor het verwerken van OT-logdata, maar dat de oplossing hier niet voor gemaakt is. Het vergt daardoor veel inspanning om Sentinel te configureren voor PA. Daarnaast waarschuwen deze partijen voor de grote hoeveelheid logdata die OT-systemen over het algemeen opleveren. Dit kan kosten opdrijvend zijn, mede vanwege vereiste retentietijden van 180 dagen. De kosten van opslag bij Sentinel boven de 90 dagen stijgen exponentieel.

4 Wijze van instappen

Geen van de marktpartijen heeft moeite met het gefaseerd aansluiten van de Deelnemers op de gezamenlijke dienstverlening. Een aantal partijen geeft aan dat het gewenst is om de meest cybervolwassen Deelnemers in eerste instantie aan te sluiten. Dit zal relatief gemakkelijk mogelijk zijn én de lessen die hierbij geleerd worden, kunnen geïmplementeerd worden zodra minder volwassen Deelnemers aangesloten worden. De betreffende partijen geven aan dat hierdoor de implementatiekosten beperkt kunnen worden.

Een aantal partijen geeft aan dat het gewenst is om in een sneller (dan voorgesteld) tempo de Deelnemers aan te sluiten. Hiermee kunnen (implementatie)staffelkortingen ingezet worden, doordat implementatieteams vanuit de betreffende partijen efficiënter ingezet kunnen worden.

Unaniem wordt commitment gevraagd dat de Deelnemers gebruik zullen maken van de SOC-dienstverlening én dat zij zich houden aan een implementatieplanning (4 Deelnemers in het eerste jaar, 6 Deelnemers per jaar in de opvolgende 3 jaar). Als er een (hoge) mate van onzekerheid is, zal dit kostenverhogend werken. Enerzijds omdat staffelkortingen op variabele kosten niet toegepast zullen worden, maar ook omdat vaste/ overheadkosten betaald moeten worden door een beperkt aantal Deelnemers. Er is voorgesteld om een Nota van Deelname met de aanbestedingsdocumentatie te publiceren of in de aanbestedingsleidraad hard te stellen dat Deelnemers zullen participeren.

Memo

Een groot aantal partijen geeft aan dat de Deelnemers zowel technisch, procedureel en organisatorisch hun zaken op orde moeten hebben (cf. aansluiteseisen). Dit is noodzakelijk omdat anders de dienstverlening niet goed/ optimaal zal functioneren ("garbage in = garbage out").

Tenslotte wordt aangegeven dat uniforme SLA en DAP documenten wenselijk zijn zodat een hoge mate van standaardisatie binnen de dienstverlening mogelijk is [noot: deze wordt door hWh gefaciliteerd].

5 Toekomstbestendigheid

Alle marktpartijen geven aan dat het binnen cyber security niet mogelijk is om een statische oplossing aan te bieden. Doorontwikkeling is evident. In de beantwoording van de vragen zien we echter dat nagenoeg alle partijen zich beperkingen tot technische ontwikkeling. Zeker de Microsoft georiënteerde partijen stellen dat zij zullen mee ontwikkelen met de ontwikkelingen van hun leverancier. Daarnaast geeft een handje vol partijen aan dat Use Case Management ook van belang is bij een toekomstbestendige oplossing. Zij richten zich daarbij vooralsnog op de use cases die zij in hun standaard dienstverlening zullen opbouwen. Slechts één partij geeft aan te beseffen dat de Waterschappen een onderdeel zijn de vitale infrastructuur in Nederland. Daarbij dient oog te zijn voor de context en dreigingsbeelden.

Een groot aantal partijen verzoekt om te worden geïnformeerd over de cyber-routekaart van de Waterschappen. Dit wordt ook vermeld onder de paragraaf Samenwerking.

6 Mogelijke verdienmodellen

Er bestaat een grote variatie in verdienmodellen. Deze zijn hieronder weergegeven:

- Abonnement
- Prijs per gB
- Prijs per identity (KA) en object (PA)
- Prijs per medewerker

Verschillende partijen werken ook met een combinatie van de hierboven genoemde prijsmodellen/ componenten.

Daarnaast kan Implementatie-ondersteuning als consultancydienst worden aangeboden. Hierbij worden zowel time-material als fixed price aangeboden.

Memo

7 Samenwerken

De vragen gerelateerd aan dit onderwerp zijn voornamelijk met standaard teksten beantwoord. Hierin is nog geen onderscheidend vermogen gepresenteerd. Basisaspecten als open communicatie, vertrouwen, transparantie en overlegstructuren worden door nagenoeg alle partijen aangehaald. Zoals hierboven al is aangegeven verzoekt een aantal partijen om centrale regie (project- en service level management) en een escalatiestructuur. Deze partijen onderkennen het grote aantal deelnemers dat met eigen Nadere Overeenkomsten, binnen een overkoepelende Raamovereenkomst, verplichtingen aangaat met de leverancier. Marktpartijen streven naar standaardisatie in de dienstverlening. Men verzoekt daarom een mogelijkheid om belangentegenstrijdigheden te kunnen oplossen. Eén partij stelt voor een Stuurgroep in te richten voor dit contract. Voor zowel centraal projectmanagement, SLM en escalatie noemt men hWh, in de rol van Opdrachtgever, als aangewezen partij.

8 Concluderend

Inhoudelijk heeft de marktconsultatie geen nieuwe inzichten opgeleverd. We hebben bevestigd gekregen dat de eisen en wensen van de Waterschappen haalbaar zijn. Als gevolg hiervan hoeven het Integraal Ontwerp en het bijbehorende Programma van Eisen dan ook niet te worden aangepast.

De marktconsultatie heeft wel inzicht gegeven in de brede variatie van kostenstructuren/verdienmodellen. Deze kennis zal verwerkt worden in het opstellen van het zogenaamde prijzenblad dat bij de aanbestedingsdocumentatie wordt gevoegd.