

Algemene informatie

Aanbesteding: Cyber Threat Intelligence
Aanbestedende Dienst: Stichting Z-CERT
Referentie: -

Toelichting:
Nota van inlichtingen 2

Vraag en antwoord

Ref.nr. 61
Onderwerp: NVI, Ref.nr. 14

Vraag:

In de NVI, Ref.nr. 14, heeft u geaccepteerd dat het minimum aantal licenties naar 5 wordt bijgesteld, bij gelijkblijvende maximprijs. Dit geeft een concurrentievoordeel aan leveranciers die duur zijn per gebruiker, en een nadeel aan leveranciers die juist bij veel gebruikers relatief goedkoper zijn. Wilt u deze handreiking intrekken?

Antwoord:

No, contracting authority retains the number of users per tier as indicated in note of information. In the contracting authority's view, a relatively cheaper price can be taken advantage of since the best value for money is being considered.

Percelen: P1 Lot 1: CTI Feed
P2 Lot 2: CTI Monitoring Dashboard
Beantwoord op: 31 okt. 2024

Ref.nr. 62
Onderwerp: Prijzenblad/NVI 14

Vraag:

Prijzenblad/NVI 14: Leverancier hanteert een minimum van 10 gebruikers (zoals ook in de oorspronkelijke aanbesteding het geval was). Mag deze voorwaarde in de opmerkingen van het prijzenblad worden opgenomen?

Antwoord:

Please refer to the answer to question 61, contracting authority uses the number of users as indicated in the note of information. For the record: it is not permitted to tender under the conditions that both lots are awarded to tenderer.

Percelen: P1 Lot 1: CTI Feed
P2 Lot 2: CTI Monitoring Dashboard
Beantwoord op: 31 okt. 2024

Ref.nr.
63

Onderwerp:
NVI 14

Vraag:

NVI 14: De 2 lots hebben bij onze oplossing veel overlap, waardoor de kosten van 2 lots samen lager zijn dan de som van de delen. Als wij op beide lots met één prijs mogen aanbieden, zou dit veel gunstiger uitpakken voor de Opdrachtgever. Door dit niet toe te staan benadeelt u geïntegreerde aanbieders en ook uzelf. In de beoordeling kunt u toch de gunstige combinatie van aanbieders bepalen door voor elke mogelijke combinatie de fictieve prijs te berekenen. Gecombineerd aanbieden zal de concurrentie derhalve niet beperken. Wilt u dit nogmaals in overweging nemen?

Antwoord:

This is not agreed, contracting authority retains the division into two separate lots. The reason for this is because there is no need for cross-functionality between the lots so that they are assessed in isolation. We encourage bidders to submit separate bids on both lots.

Percelen: P1 Lot 1: CTI Feed
P2 Lot 2: CTI Monitoring Dashboard
Beantwoord op: 31 okt. 2024

Ref.nr.
64

Onderwerp:
EIS 2.9/NVI 55

Vraag:

EIS 2.9/NVI 55: Hoeveel leden wenst Z-Cert te volgen?

Antwoord:

Between 1500-2000 healthcare institutions are projected to become NIS2 entities.

Percelen: P1 Lot 1: CTI Feed
P2 Lot 2: CTI Monitoring Dashboard
Beantwoord op: 31 okt. 2024

Ref.nr.
65

Onderwerp:
EIS 2.10/NVI 29

Vraag:

EIS 2.10/NVI 29: Hoeveel niet-leden in de supply chain wenst u te volgen?

Antwoord:

This number cannot be specified as it is unknown, we are however looking for the solution to identify, for example, if a leaksite posts about a ransomware attack on a supplier which has healthcare in their description of customers. i.e. a supplier of building management software listing healthcare as one of their areas of expertise

Percelen: P1 Lot 1: CTI Feed
P2 Lot 2: CTI Monitoring Dashboard
Beantwoord op: 31 okt. 2024

Ref.nr.
66

Onderwerp:
EIS 2.14/NVI 39

Vraag:

EIS 2.14/NVI 39: Hoeveel zoekopdrachten verwacht u jaarlijks te maken?

Antwoord:

We expect the solution to provide a threat intel feed that can be searched and filtered. This activity will most likely be used daily. We do not mean a search functionality that starts searching the (dark)web or other sources when searching.

Percelen: P1 Lot 1: CTI Feed
P2 Lot 2: CTI Monitoring Dashboard
Beantwoord op: 31 okt. 2024

Ref.nr.
67

Onderwerp:
question

Vraag:

Regarding the CTI feed, what output format would be acceptable? What TIP /SIEM would you like to integrate it to? What would you describe as “substantive” - what type of metadata do you expect in addition to the IOCs? Are there specific relevance/recency/time-to-live requirements? Do you expect cross-functionality between lots 1 and 2, that is, being able to integrate the feed into the dashboards, or adding from the dashboards to the feed? For the dashboards, do you expect that they would also contain a feed element, separate to the dedicated CTI feed lot? Or is it not required that the dashboard content be machine readable / have downstream ability?

Antwoord:

For the output we would expect commonly used standards like STIX and the

MISP which are supported by most TIP/SIEM platforms.

With substantive we mean information that has a basis in facts and is meaningful. Sources that can be linked or described can help with this.

It is not expected that there is a cross-functionality between lots 1 and 2.

Percelen:	P1 Lot 1: CTI Feed P2 Lot 2: CTI Monitoring Dashboard
Beantwoord op:	31 okt. 2024