BIJLAGE 3 Geschiktheidseisen SOC-diensten - TB

Deze bijlage 3 geeft een overzicht van de geschiktheidseisen voor de **Technische- en beroepsbekwaamheid (TB)**. Voor het opgeven van referenties wordt gegadigde verzocht gebruik te maken van het format dat als bijlage 1B bij de leidraad is gevoegd.

U kunt uw antwoord (ja/nee) op de geschiktheidseisen in **deel IV van het Uniform Europees Aanbestedingsdocument** vermelden bij de betreffende onderdelen van de geschiktheidseisen.

De aanbestedende dienst zal bij voorgenomen selectie (top 5) van de gegadigde - ter verificatie - bewijsstukken opvragen voor de hieronder vermelde eisen voor de Technische en beroepsbekwaamheid (o.a. referentie check).

Eis TB1 – Referenties per kerncompetentie

De beoogde dienstverlening omvat in ieder geval de volgende vijf kerncompetenties:

- **Kerncompetentie 1: Monitoring & detectie**
  - Real-time bewaking van relevante logbronnen (zoals netwerk, endpoints, cloud, applicaties en overige relevante bronnen).
  - Gebruik van geavanceerde detectiemechanismen (bijvoorbeeld SIEM, XDR, SOAR of gelijkwaardige oplossingen).

- **Kerncompetentie 2: Incidentrespons**
  - Analyse, triage en opvolging van beveiligingsmeldingen.
  - Ondersteuning bij het treffen van mitigerende maatregelen en herstel na incidenten.

- **Kerncompetentie 3: Threat intelligence & analyse**
  - Integratie van actuele dreigingsinformatie in de monitoring.
  - Correlatie van dreigingen met gebeurtenissen in onze omgeving.
  - Periodieke dreigings- en trendanalyses.

- **Kerncompetentie 4: Rapportage & compliance**
  - Periodieke operationele en tactische rapportages over incidenten, trends en verbeterpunten.
  - Ondersteuning bij het kunnen aantonen van naleving van relevante wet- en regelgeving en normen (zoals AVG en ISO 27001).

- **Kerncompetentie 5: Samenwerking & dienstverlening**
  - Heldere dienstafspraken (zoals SLA/DAP) en periodieke overleggen op operationeel, tactisch en strategisch niveau.

- Inzicht in monitoring- en alarmeringsinformatie (bijvoorbeeld via een portal of SIEM-omgeving) en de mogelijkheid om gezamenlijk monitoring- en alertingscenario's op te stellen en te verfijnen.

De gegadigde toont zijn technische en beroepsbekwaamheid aan met minimaal één referentie per kerncompetentie.

Per kerncompetentie geldt:

- De referentie betreft een opdracht die in de afgelopen drie (3) jaar is uitgevoerd (lopend of afgerond); indien sprake is van een opdracht met een doorlooptijd langer dan drie jaar, volstaat dat de gegadigde in de afgelopen drie jaar aantoonbaar en substantieel werkzaamheden heeft verricht binnen die opdracht;
- De referentie heeft betrekking op een organisatie met een vergelijkbare of grotere complexiteit (bijvoorbeeld qua aantal medewerkers, omvang van de IT-omgeving of kritieke aard van de processen);
- De referentie maakt duidelijk dat de gegadigde de betreffende kerncompetentie daadwerkelijk en substantieel heeft uitgevoerd binnen het kader van 24/7 SOC-/MDR-dienstverlening of daarmee gelijkwaardige managed security-dienstverlening.
- Er mogen alleen geheel afgeronde opdrachten als referentie worden opgegeven of, indien gebruik gemaakt wordt van een nog niet (geheel) afgeronde opdracht mogen alleen de werkelijk behaalde resultaten van de lopende opdracht worden opgegeven en kan niet volstaan worden met een prognose van de resultaten.
- De referentieopdracht dient naar tevredenheid van de opdrachtgever te zijn uitgevoerd. De aanbestedende dienst kan dit nagaan bij de referenten.
- Een referentie kan betrekking hebben op meer competenties. Indien verschillende uitgevraagde competenties blijken uit één uitgevoerd project, kan dezelfde referentieopdracht worden gebruikt om deze meerdere competenties aan te tonen.

Type IT-omgeving
De referenties moeten betrekking hebben op IT-omgevingen waarin zowel open source als commerciële componenten worden gebruikt (een open source gedomineerd on premise serverlandschap gecombineerd met commerciële SaaS- en cloudoplossingen). Dit sluit aan bij de IT-omgeving van de aanbestedende dienst.

Referenties
Per referentie worden minimaal verstrekt:

- naam en typering van de opdrachtgever;
- korte omschrijving van de geleverde dienstverlening (met expliciete koppeling aan de betreffende kerncompetentie(s) en de rol/bijdrage van de gegadigde);

- looptijd en globale omvang van de omgeving (bijv. aantal systemen/gebruikerstypen/logbronnen)
- contactpersoon bij de opdrachtgever

Eis TB2 – Informatiebeveiligingsmanagementsysteem

De gegadigde beschikt over een aantoonbaar ingericht informatiebeveiligings-managementsysteem voor de dienstverlening die onder deze opdracht valt, blijkend uit:

- een geldig ISO/IEC 27001-certificaat of een gelijkwaardige certificering op het gebied van informatiebeveiliging;
- het certificaat is van toepassing op de locaties en diensten waarvandaan de SOC-/MDR-dienstverlening of gelijkwaardige managed security-dienstverlening wordt geleverd;
- het certificaat is afgegeven door een onafhankelijke, geaccrediteerde certificerende instelling of een hiermee gelijkwaardige onafhankelijke partij.

Bij een gelijkwaardige certificering toont gegadigde bij eventuele verificatie door de aanbestedende dienst aan dat hiermee ten minste een vergelijkbaar niveau van informatiebeveiliging wordt geborgd als met ISO/IEC 27001. Op verzoek kan een uittreksel uit de Verklaring van Toepasselijkheid worden verstrekt voor zover relevant voor de opdracht.

Eis TB3 – Infrastructuur en dataopslag binnen EU/EER

De gegadigde beschikt over een leveringsmodel voor SOC-/MDR-dienstverlening of gelijkwaardige managed security-dienstverlening waarbij:

- alle ten behoeve van deze opdracht verwerkte loggegevens, beveiligingsgebeurtenissen en daarop gebaseerde analyses en rapportages worden opgeslagen en verwerkt binnen de Europese Unie of de Europese Economische Ruimte (EU/EER);
- eventuele (sub)dienstverleners of onderaannemers die bij de uitvoering van de SOC-/MDR-dienstverlening betrokken zijn, eveneens uitsluitend gebruikmaken van infrastructuur (datacenters, cloudregio's) binnen de EU/EER voor de verwerking van deze gegevens;
- geen doorgifte van deze gegevens plaatsvindt naar landen buiten de EU/EER, tenzij en voor zover dit strikt noodzakelijk is, dit plaats vindt met passende waarborgen conform de AVG en uitsluitend na voorafgaande schriftelijke toestemming van de aanbestedende dienst.
- voldaan wordt aan tenminste niveau 2 van de *Sovereignty Effectiveness Assurance Levels (SEAL)* uit het EU Cloud Sovereignty Framework van de Europese Commissie of een vergelijkbaar niveau van borging.

Eis TB4 – Gekwalificeerd en gescreend personeel

De gegadigde beschikt over personeel dat de SOC-/MDR-dienstverlening uitvoert en dat:

- beschikt over passende opleiding en ervaring op het gebied van informatiebeveiliging en SOC-/MDR-werkzaamheden met daarbij verificatie van behaalde diploma's, certificaten en ervaringen.
- door de gegadigde – voor het moment van feitelijke inzet op een opdracht - is onderworpen aan identiteitscontrole en betrouwbaarheids-/integriteits-screening zoals een Verklaring Omtrent het Gedrag (VOG) of een hiermee gelijkwaardige achtergrondscreening, in lijn met de functie en toepasselijke wet- en regelgeving.

Screeningsbeleid en -procedure
De gegadigde beschikt over een gedocumenteerd screeningsbeleid en -procedure voor personeel in (informatie)beveiligingsfuncties, waarin ten minste is vastgelegd:

- welke functies onder welke screeningsniveaus vallen;
- welke checks per functieniveau worden uitgevoerd;
- op welk moment in het HR-proces de screening plaatsvindt;
- hoe wordt omgegaan met periodieke her-screening (indien van toepassing);
- hoe wordt geborgd dat screening plaatsvindt in overeenstemming met toepasselijke privacywetgeving (AVG).