Aanbestedingschecklist SOC-diensten

Monitoring & Detectie – HAVIK
Reference Card – Aanbestedingschecklist SOC-Diensten 1.0

Complexiteit document
Eenvoudig ● ○ ○

Samenwerken maakt DIGITAAL VEILIGER

VSSR

Leeswijzer
Deze checklist is opgesteld ter ondersteuning van het gestructureerd doorlopen van drie fasen bij een aanbesteding: voorbereiding, aanbesteding zelf en de implementatie. Elke fase bevat specifieke aandachtspunten die ondersteunen bij het doorlopen van deze fase. De checklist biedt praktische handvatten en kan als leidraad dienen om te waarborgen dat geen globale onderwerpen/aandachtspunten over het hoofd worden gezien. Gebruik deze checklist als ondersteuning bij een Aanbesteding, zodat over de meest basale zaken in ieder geval is nagedacht en er een bewuste keuze over gemaakt kan worden. Raadpleeg de checklist per fase en werk deze systematisch af voor optimale resultaten.

Voorwoord

De Rijksoverheid verwerkt grote hoeveelheden gevoelige informatie en is daarmee een interessant en gewild doelwit. Cybercriminelen en statelijke actoren zoeken naar kwetsbaarheden om zich zo toegang te verschaffen tot bevoorradingsketens, netwerken, systemen en (gevoelige) informatie.

Monitoring- en detectiediensten zijn erop gericht een veelheid aan loggegevens en andere (meta-) datastromen afkomstig van de IT-infrastructuur, randapparatuur, bedrijfsapplicaties en andere dataverwerkingen in een organisatie te analyseren, aggregeren en correleren. Monitoring en detectiesystemen kunnen op basis hiervan verdachte gedragingen detecteren en alarm slaan.

Monitoring- en detectiediensten kunnen binnen een organisatie worden ingericht in de vorm van een Security Operations Center (SOC). Het zelf inrichten van een SOC is, echter, niet voor elke organisatie opportuun. In dergelijke gevallen is het goed mogelijk om SOC-diensten bij externe, gespecialiseerde partijen, in te kopen. Om u op weg te helpen in het proces van het aanbesteden van SOC-diensten vindt u in dit document een checklist met aandachtspunten die tijdens de verschillende fasen van een aanbesteding houvast bieden.

- **Voorbereiding**
- **Aanbesteding**
- **Implementatie**

Achtergrond
VSSR levert verschillende kennisproducten. Dit document maakt onderdeel uit van een set documenten om Rijksoverheidsorganisaties te ondersteunen bij het aanbesteden van SOC-diensten. Het document bevat een overzicht van aandachtspunten die van belang zijn tijdens de verschillende fasen van een aanbesteding.

Doelgroep
Versterken SOC Stelsel Rijk (VSSR) biedt met dit document handvatten voor Senior Management op strategisch niveau, functionarissen die zijn belast met inrichting van de SOC-functie, projectleiders, architecten en security officers die betrokken zijn bij SOC-dienst aanbestedingen of de aanloop hier naartoe.

Voorbereiding

Context

- [ ] **Doel:** Wat probeert uw organisatie te bereiken met een SOC?
- [ ] **Risico:** Welke risico's mitigeert het SOC voor uw organisatie?
- [ ] **Kroonjuwelen:** Wat gaat het SOC bewaken?
- [ ] **Servicetijden:** Is uw organisatie beschikbaar overeenkomstig de dienst-verlening die u gaat vragen?
- [ ] **Locatie:** Wilt u cloud en/of lokale ICT-componenten bewaken?

Processen

- [ ] **Reageren:** Is incident response ingericht in uw organisatie?
- [ ] **Bevoegdheden:** Heeft het stekkermandaat een eigenaar?
- [ ] **Aansturing:** Wie stuurt relevante ICT en 3e-partijen aan?
- [ ] **Eigenaarschap:** Proceseigenaren kennen hun verantwoordelijkheden bij incidentopvolging?
- [ ] **Patching:** Kwetsbaarheden worden binnen uw organisatie volgens policy en proces effectief en snel opgelost?

Data

- [ ] **Data Privacy:** Beschikt u over een DPIA?
- [ ] **Dataretentie en logmanagement:** De scope voor logdata, volumes en retentietijd is bepaald en bijbehorende logmanagement is op orde?
- [ ] **Juridisch:** Zijn er juridische eisen betreft uw logdata?
- [ ] **Locatie:** Zijn er eisen voor de dataopslaglocatie (NL/EER)?
- [ ] **Toegang:** Heeft OG datatoegang nodig bij de ON?

Techniek

- [ ] **Netwerk**: Is een netwerk- en nummerplan beschikbaar?
- [ ] **Assets:** Is een relevante asset-lijst beschikbaar?
- [ ] **Systeemintegratie:** Dient de leverancier te koppelen op een bestaand systeem zoals ITSM, ISMS, etc?
- [ ] **Licentie:** Mag de leverancier bestaande licenties gebruiken?
- [ ] **Data:** Moet Log- en alarmdata worden doorgestuurd vanuit de leverancier naar uw systemen?

Aanbesteding

Leveranciersorganisatie & Proces

- [ ] **Aanbesteding:** Gaat u een openbare procedure volgen?
- [ ] **Locatie:** Zijn er locatie afhankelijke aspecten (aanrijtijden)?
- [ ] **Screening:** Dient personeel in bezit te zijn van VOG/VGB of additionele screening door een erkende POB?
- [ ] **Certificering:** Moet een dienstverlener over bepaalde certificeringen beschikken (bijv. ISO27oox, SOC2/3)?
- [ ] **Bezetting:** Moeten bij de aanbesteding ook tijdens de contractfase actief blijven?

Dienstverlening

- [ ] **SOC:** Waar mag het SOC (niet) zijn gelokaliseerd?
- [ ] **Techniek:** Waar mogen technische middelen (niet) zijn gelokaliseerd?
- [ ] **Cloud:** Is cloud-based dienstverlening toegestaan?
- [ ] **Taal:** In welke taal mag de dienst worden geleverd?
- [ ] **Security:** Zijn er specifieke security-eisen voor de dienstverlening (BIO/ABRO/ABDO)?

Diensten

- [ ] **MDR:** Basis monitoring, detectie en bevindingenonderzoek?
- [ ] **KS:** Wilt u regelmatig scannen op bekende kwetsbaarheden?
- [ ] **IR:** Heeft u hulp nodig heeft bij incident opvolging?
- [ ] **Consultancy:** Heeft u adviserende dienstverlening nodig?
- [ ] **Applicaties:** Is monitoring van speciale applicaties vereist?

Contract Management

- [ ] **Kosten:** Welke prijsmodel gaat u hanteren?
- [ ] **Contract compliance:** Wilt u de dienst kunnen auditeren op contract-afspraken, procesinrichting en security (BIO)?
- [ ] **Kwaliteit:** Wilt u de dienstkwaliteit via red-teaming (aangekondigd of niet) kunnen controleren?
- [ ] **RACI:** Wat zijn rollen en verantwoordelijkheden voor OG/ON?
- [ ] **Exit-strategie:** Wat moet ON overdragen bij einde contract?

Implementatie

Proces

- [ ] **Detectie:** Wie is eigenaar van de detectie use cases?
- [ ] **Demarcatie:** Heeft u de procesdemarcatiepunten en verantwoordelijkheden tussen OG/ON vastgesteld?
- [ ] **Escalatie:** Is er een escalatiematrix opgesteld voor incidenten?
- [ ] **Beschikbaarheid:** Kunt u 24x7 incidenten opvolgen?
- [ ] **Ondersteuning:** Heeft u ondersteuning op locatie nodig bij (grote) incidenten?

Scope

- [ ] **Assets:** Welke assets zijn in scope voor monitoring?
- [ ] **Applicaties:** Zijn er specifiek applicaties in scope?
- [ ] **Logbronnen:** Heeft u een lijst met logbronnen vastgesteld?
- [ ] **Datavolumes:** Wat zijn de geschatte datavolumes?
- [ ] **Detectie:** Bepaal de detectie use cases in scope?

Techniek

- [ ] **Detectie agent:** Het is wel/niet toegestaan om lokale detectie en/of log-agents te installeren?
- [ ] **Dataformaat:** Is het logdata formaat vastgesteld?
- [ ] **Privacy:** Moeten specifieke datavelden worden afgeschermd?
- [ ] **Tools:** Moet ON gebruik maken van tools van OG (bijv. SIEM)?
- [ ] **Audit policy:** Heeft u bepaald welke log audit policies geconfigureerd moeten worden of moet ON hierbij helpen?

Rapportage & Sturing

- [ ] **Prestatie (KPI):** Wat worden de prestatie eisen in de SLA?
- [ ] **Risico (KRI):** Heeft u risico indicatoren voor rapportage opgesteld?
- [ ] **Rapportage:** Zijn rapportage eisen vastgesteld voor de SLA?
- [ ] **Overleg:** Heeft u een OG/ON-overlegstructuur voor de DAP?
- [ ] **Fequenties:** Zijn rapportage en overleg frequentie vastgesteld?

Afkortingen

Afkorting	Betekenis
ABDO	Algemene Beveiligingseisen Defensieopdrachten
ABRO	Algemene Beveiligingseisen Rijksoverheid Opdrachten
BIO	Baseline Informatiebeveiliging Overheid
CTI	Cyber Threat Intelligence
DAP	Dossier (operationele) Afspraken en Procedures
(D)PIA	(Data) Privacy Impact Assessment
EASM	External Attack Service Management
EDR	Endpoint Detection and Response
EER	Europese Economische Ruimte
IR	Incident Response
ISMS	Information Security Management System
ISO	International Organisation for Standardization
ITSM	IT Service Management systeem
KPI	Key Performance Indicator
KRI	Key Risk Indicator
KS	Kwetsbaarheden Scanning
MDR	Managed Detection and Response
NDR	Network Detection and Response
OG/ON	Opdrachtgever / Opdrachtnemer
POB	Particulier Onderzoeksbureau
RACI	Responsible, Accountable, Consulted en Informed
SIEM	Security Information and Event Management
SLA	Service Level Agreement
SOC	Security Operations Center
VGB	Verklaring Geen Bezwaar
VOG	Verklaring Omtrent Gedrag

Uitgave
Versterken SOC Stelsel Rijk (VSSR)
Postbus 117, 2501 CC Den Haag
Turfmarkt 147, 2511 DP Den Haag
070 751 5555

Meer informatie
https://vssr.rijksapplicaties.nl/
vssr.info@minjenv.nl

januari 2025