Eis no.	Functionele eisen	Extra toelichting
	SIEM	
1	De Opdrachtnemer dient voor de uitvoering van de SOC dienst gebruik te maken van het SIEM (gebasseerd op Rapid7 InsightIDR) van de opdrachtgever.	
2	De Opdrachtnemer dient te waarborgen dat (log)gegevens binnen de omgeving van Opdrachtgever blijven en alleen worden geanalyseerd met de SIEM die beschikbaar is gesteld door de Opdrachtgever. SIEM alerting of triggers van use-cases uit het SIEM van de Opdrachtgever, mogen wel naar een systeem van de Opdrachtnemer worden verstuurd.	
3	De Opdrachtnemer beschikt over een (partner) certificering inzake de gebruikte SIEM-software (Rapid7 InsightIDR). Hierbij dient minimaal geborgd te zijn dat de leverancier direct toegang heeft tot expertise bij de producent van de software-onderdelen. Wanneer men op het moment van inschrijving nog niet over een (partner) certificering beschikt, dan zal deze binnen een termijn van 3 maand alsnog worden verkregen en worden overlegd aan aanbesteder.	
	SOC	
4	De Opdrachtnemer heeft een SOC-team binnen de Europese Economische Ruimte (EER+VK) en is 24/7 telefonisch bereikbaar.	
5	De omgeving van de opdrachtgever wordt 24/7 real-time gemonitord op security incidenten en dreigingen, hier wordt volgens SLA afspraak op geacteerd.	
6	Bij afname van een SOC-dienst biedt Opdrachtnemer de Opdrachtgever een 24/7 telefonisch bereikbare Servicedesk met rechtstreeks contact of met directe doorgeleiding naar ter zake kundig bij voorkeur Nederlands sprekend personeel en/of Engels (Cambridge Engels C1 advanced of vergelijkbaar niveau) voor vragen over meldingen en/of opvolgingsadviezen.	
7	De Opdrachtnemer zorgt ervoor dat het (ingezette)-SOC personeel de kennis en vaardigheden heeft voor het uitvoeren hun werkzaamheden en toont dit aan door jaarlijks een opleidingsplan en behaalde/aanwezige certificeringen te overleggen.	
8	De oplossing is flexibel in het op- en afschalen van resources, waaronder in ieder geval de benodigde FTE’s en expertisegebieden, en het op- en afschalen kan binnen een periode van maximaal 2 weken gerealiseerd worden op basis van veranderende omstandigheden en behoeften	
9	Het SOC heeft een real-time en actueel beeld van het bedreigingslandschap door continu bedreigingsinformatie van ten minste twee verschillende bronnen te ontvangen en analyseren	
10	Het SOC monitort 24/7 het internet en dark & deep web ten minste op gecomprimenteerde accounts & datalekken. Indien er account(s) en data lekken worden gevonden, dan wordt de Opdrachtgever hierover geïnformeerd volgens het security incident proces.	

11	Het SOC moet 24/7 het dreigingslandschap analyseren en updates implementeren om nieuwe aanvalstechnieken en -tactieken te kunnen detecteren.	
12	Er wordt door de Opdrachtnemer door middel van threat hunting dagelijks proactief gezocht naar bekende en onbekende dreigingen in de omgeving van de Opdrachtgever. Als er iets wordt gevonden wordt dit met het security incident proces opgepakt.	
13	De Opdrachtnemer voert op basis van beschikbare gegevens (o.a. logbronnen, Threat Intel) bedreigingstrend analyse uit en geeft hierop een waarschuwing en/of advies over mogelijke maatregelen.	
	Use-Case (van logging naar incident)	
14	De Opdrachtnemer beschikt over een bibliotheek met use-cases. Deze dient door de Opdrachtnemer actueel te worden gehouden, zodat ook nieuwe aanvalsmethodes worden gedetecteerd.	
15	De Opdrachtnemer biedt de mogelijkheid om op aanvraag van de Opdrachtgever een custom use-case te maken, toegespitst op de klantspecifieke situatie. De eerste 5 nieuwe custom use-cases per maand zijn onderdeel van de dienstverlening en totaalkosten.	
16	De implementatie van nieuwe custom-made use-cases verloopt via een afgesproken implementatie proces, waar de Opdrachtgever bij betrokken is en om validatie wordt gevraagd	
17	De Opdrachtnemer geeft continue inzage in de use-cases die worden gebruikt, bijvoorbeeld via wekelijkse rapportages of via een portaal met actueel gebruikte use-cases	
18	De Opdrachtnemer heeft een proces ingericht voor het beperken en terugdringen van het aantal van False Positive meldingen.	
19	Per (categorie/ soort) use-case uitkomst is er een handelingssperspectief uitgewerkt aan de hand waarvan de communicatie tussen de Opdrachtnemer en Opdrachtgever plaatsvind. Bij nieuwe use-case (categorie/ soort) wordt deze tevens opgesteld.	
	Incident Response	
20	De Opdrachtnemer beschikt over playbooks om de meest voorkomende incidenten af te handelen	
21	De Opdrachtgever heeft inzicht in het overzicht van playbooks die worden gebruikt, bijvoorbeeld via wekelijkse rapportages of via een portaal met actueel gebruikte playbooks	
22	De effectiviteit van playbooks moet regelmatig (minstens eens per kwartaal) worden geevalueerd aan de hand van postmortem-analyses van incidenten.	
23	De Opdrachtnemer heeft op afroep binnen 2 uur capaciteit beschikbaar ter ondersteuning aan een derde partij voor het uitvoeren van de artefact/ forensisch onderzoek.	
24	De Opdrachtnemer voorziet elke security incident melding van een mitigatie advies of reducerende maatregel advies.	

25	De Opdrachtnemer biedt de mogelijkheid voor First Incident Response (ter plaatse) ter ondersteuning aan een derde partij bij het feitelijk oplossen van een security incident (denk aan Ransom). Dit na triage van de Opdrachtnemer en goedkeuring van de Opdrachtgever.	
26	De oplossing biedt ter ondersteuning voor onder andere forensisch onderzoek een overzichtelijke, chronologische tijdlijn van events binnen een gestelde periode (min 3 maanden) en binnen afzienbare tijd (max 1 uur)	
27	Bij Zero-day Security incidenten/ threats wordt de Opdrachtgever na bekend worden geïnformeerd over de dreiging inclusief het mitigatie advies. Dit incident wordt behandeld als een P2 security incident.	
28	Na een security incident wordt de Opdrachtnemer conform SLA geïnformeerd. Alle security incidenten worden door de Opdrachtnemer via mail of direct in het Servicemanagment systeem (TOPDesk) van de Opdrachtgever gemeld. Voor P1 & P2 security incidenten geldt daarnaast dat er telefonisch of via SMS contact wordt opgenomen op een vooraf afgesproken telefoonnummer.	
	Proces	
29	De afhandeling van incidenten volgt een met de Opdrachtgever vastgesteld security incident proces. Het proces is helder en duidelijk beschreven, inclusief de vastlegging van de verschillende rollen en verantwoordelijkheden (RASCI.)	
30	De Opdrachtnemer evalueert en verbetert het toegepaste security incident proces periodiek (ten minste eens per kwartaal) en stemt dit proces af met SSC Ons, zodat er zo min mogelijk complexiteit in het proces zit en daarmee de kans op fouten en onnodig lange doorlooptijd beperkt wordt.	
31	De Opdrachtnemer verbeterd continue de dienstverlening en de aanpalende processen en procedures en rapporteert eens per kwartaal over de verbeteringen tijdens een meeting.	
32	De Opdrachtnemer borgt via procedures in de dienst dat security incident meldingen aan het operationeel beveiligingsteam van de opdrachtgever worden gemeld via het daarbij opgegeven e-mail adres/Servicemanagement systeem (TOPdesk) en telefoonnummer.	
33	De Opdrachtnemer dient een proces te hebben die de kwaliteit van de use-cases en playbooks controleert en voert verbeteringen door waar mogelijk. De Opdrachtgever wordt eens per kwartaal tijdens een meeting geïnformeerd over bevindingen en doorgevoerde verbeteringen.	
	Rapportage	
34	De Opdrachtnemer biedt een online dashboard waarop het aantal security incidenten en/ of threats per severity en per omgeving (van SSC Ons en Partners) te zien zijn.	
35	Rapportage is beschikbaar in de Nederlandse taal	

36	De Opdrachtnemer faciliteert de Opdrachtgever in het aanbieden van een Heat Map dasboard die te allen tijde online inzichtelijk is voor de Opdrachtgever. Dit betreffen in ieder geval gevonden threats, zoals geografisch locaties, frequentie van aanvallen, doelwitten binnen de omgeving; heatmaps met gebruikersactiviteit (ongebruikelijke inlogpogingen en accountmisbruik), heatmaps met netwerkverkeer (ongebruikelijke pieken, communicatiepatronen)	
37	De Opdrachtnemer levert eens per kwartaal een security verbeteringsadvies rapport op basis van geanalyseerde security incidenten/ data aangeleverd aan de Opdrachtgever	
38	De Opdrachtnemer biedt via het portaal near-realtime filterbare rapportage over/inzicht in : - identificatie en classificatie van incidenten - identificatie en classificatie van threats - identificatie en classificatie van gebeurtenissen (anomalieen) - Waargenomen trends in de omgeving	
39	Voor verbeteren van de beveiligingpositie van SSC Ons en Partners komt de Opdrachtnemer ieder kwartaal met aanbevelingen t.a.v. mogelijk te nemen maatregelen.	
	Crisis oefening	
40	De Opdachtnemer biedt ondersteuning aan crisis oefeningen van de Opdrachtgever. Opdrachten hiervoor doet Opdrachtgever minimaal 15 werkdagen vooraf.	
Eis no.	**Security eisen**	**Extra toelichting**
	Generiek	
41	De Opdrachtnemer zal voor de prestaties voldoende personen inzetten met voldoende opleiding, vaardigheden en kennis van de bedrijfsvoering en organisatie van de Opdrachtgever, om de prestaties te verrichten. Wanneer de hierboven genoemde personen zich bij de Opdrachtgever bevinden, of in direct contact met de Opdrachtgever staan, zal het personeel van de Opdrachtnemer de gedragsvoorschriften van de Opdrachtgever naleven. Hiermee zal gevolg gegeven worden aan redelijke verzoeken van de Opdrachtgever.	
42	Risico's voor informatiebeveiliging en privacy zijn expliciet benoemd en passende beheersmaatregelen zijn expliciet belegd	

43	De ICT-Prestatie stelt de Opdrachtgever in staat te voldoen aan: • De (U)AVG; • De Baseline Informatiebeveiliging Overheid; • ISO 27001:2017; • ISO 27002:2017; • De beveiligingsrichtlijnen voor webapplicaties van het NCSC; • Archiefwet 1995, Archiefbesluit 1995; • Wet Digitale Overheid (WDO)	
44	De Opdrachtnemer accepteert de Gemeentelijke Inkoopvoorwaarden bij IT (GIBIT2023) als leidende inkoopvoorwaarden. De GIBIT2023 is beschikbaar via de website van VNG-Realisatie: https://vng.nl/sites/default/files/2023-12/vng_gibit_2023_artikelen.pdf	
45	De Opdrachtnemer is NEN/ISO 27001 gecertificeerd. De Opdrachtnemer overlegt het certificaat.	
46	De Opdrachtnemer licht toe hoe wordt voldaan aan de GIBIT-artikelen: 6, 25 en 26	
47	Opdrachtnemer committeert zich aan het bijhouden en implementeren van bestaaande en nieuwe standaarden die vanuit het Forum van Standaardisatie van toepassing zijn, ook wanneer deze in de toekomst worden gewijzigd, vernieuwd of aangescherpt.	
48	De ICT-prestatie dient aan te sluiten bij de principes van ‘privacy bij design’ en ‘privacy by default’ zoals beschreven in de AVG.	
49	De Opdrachtnemer geeft transparant en kostenloos inzicht in certificeringsdocumenten en rapportages opgesteld door EDP-auditors.	
50	De Opdrachtnemer (in haar rol als verwerker) zal aan de Opdrachtgever (in haar rol als verwerkingsverantwoordelijke) zo snel mogelijk, maar uiterlijk binnen 24 uur, informeren na vaststelling van een (vermoedelijke) inbreuk in verband met persoonsgegevens (datalek). Opdrachtnemer vermeldt hierbij voor zover bekend de vermeende oorzaak van de (vermoedelijke) Inbreuk, de categorie persoonsgegevens, de categorie betrokkenen en het aantal betrokkenen. Daarbij wordt ook vermeld welke verbetermaatregel zijn/worden getroffen door de Opdrachtnemer.	
51	De Opdrachtnemer heeft beheersmaatregelen tegen malware getroffen.	
52	De Opdrachtnemer treft beheersmaatregelen om onbevoegde toegang tot, schade aan en interferentie (storing/uitval) met informatie en informatievewerkende faciliteiten van Opdrachtgever te voorkomen, zodat de bedrijfsvoering niet wordt onderbroken of aangetast.	
53	De Opdrachtnemer rapporteert jaarlijks over auditresultaten t.a.v. de BIO of ISO 27001 en eens per kwartaal over de voortgang van verbeterinitiatieven die daaruit voortkomen.	

54	De Opdrachtgever is gerechtigd zelf of door een onafhankelijke auditor onderzoek te (laten) doen naar de naleving van plichten uit de overeenkomst	
	Beschikbaarheid	
55	De Opdrachtnemer heeft een wijzigings- en acceptatieproces. Hierin borgt de Opdrachtnemer ten minste dat: • De Opdrachtgever wordt geïnformeerd over wijzigingen die betrekking hebben op de dienst of organisatie van de dienst of organisatie zelf die invloed heeft op de geleverde dienst • De acceptatie wordt hierbij uitgevoerd door de Opdrachtgever.	
56	De Opdrachtnemer zorgt voor Backup en Recovery van gegevens in het portaal: • De Opdrachtnemer maakt dagelijks een online back-up van de data. • De Opdrachtnemer bewaart backups minimaal 60 dagen • De Opdrachtnemer test disaster recovery minimaal eenmaal per jaar. • De Opdrachtnemer doet de Opdrachtgever verslag van disaster recoverytest.	Dit is van toepassing op het portaal (zie eis 38)
57	Gegevens in het portaal kunnen worden geëxporteerd met als doel portering naar andere dienstverleners mogelijk te maken in geval van een exit.	Dit is van toepassing op het portaal (zie eis 38)
	Integriteit	
58	Onderliggende software componenten, zoals operating systemen, database software, browser versie, programmeer framework enz., waarop de software is gebouwd en draait, dienen altijd een door de oorsprokelijke leverancier van de betreffende software of framework ondersteunde versie te zijn. Bijvoorbeeld: als Microsoft Windows gebruikt wordt is dit op basis van een nog door Microsoft ondersteunde versie. Windows 11 zou acceptabel zijn, maar Windows7 niet meer omdat het end-of-life is.	Dit is van toepassing op het portaal (zie eis 38) en systeem van de opdrachtnemer (zie eis 2)
59	De logging is alleen beschikbaar voor daartoe geautoriseerde medewerkers.	
	Vertrouwelijkheid	
60	De Opdrachtgever blijft eigenaar van de gegevens binnen applicatie en deze gegevens mogen niet voor andere doeleinden gebruikt worden door de Opdrachtnemer van de applicatie. Dit geldt zowel voor gegevens in de Test-, Acceptatie- als Productieomgevingen.	
61	Het is de Opdrachtnemer verboden, zonder voorafgaande uitdrukkelijke schriftelijke toestemming van de Opdrachtgever, de uitvoering van een overeenkomst geheel of gedeeltelijk aan derden over te dragen of uit te besteden.	
62	De Opdrachtnemer heeft een geheimhoudingsplicht aangaande alle vertrouwelijke gegevens dan wel anderszins gevoelige informatie van de Opdrachtgever die de Opdrachtnemer in het kader van de opdracht ter kennis is gekomen.	
63	De Opdrachtnemer heeft een geheimhoudingsplicht aangaande de informatie opgenomen in de systemen.	

64	De Opdrachtnemer is verantwoordelijk voor authenticatie en autorisatie van haar eigen medewerkers. De Opdrachtnemer waarborgt hierbij tevens ook met scheiding van taken onbedoelde of ongeautoriseerde toegang. De Opdrachtgever heeft het recht hierop te controleren.	
65	De Opdrachtnemer is verantwoordelijk voor de kwalificaties en screening van het eigen personeel. Op verzoek van Opdrachtgever dient een VOG te worden overlegd, van personen die worden ingezet op de opdracht.	
66	Alle voorwaarden en eisen die gelden voor personeel van de Opdrachtnemer zijn ook van toepassing op derden, die in opdracht van de Opdrachtnemer diensten verrichten voor de Opdrachtgever	
67	Autorisaties kunnen worden ingericht op basis van functies (rol-gebaseerd) waarbij functie-scheiding is toegepast.	
68	Er zijn geen "algemene" accounts / gebruikers binnen de software. Als deze noodzakelijk zijn, betreft het een beperkt aantal en met specifieke doelen. De Opdrachtnemer dient hierin inzicht te geven.	
69	Er is sprake van toepassing van een vorm van multi-factor authenticatie.	
70	De aangeboden websites worden altijd versleuteld dan wel voorzien van PKIoverheid Extended Validation SSL certificaat (EV SSL) (of vergelijkbaar).	Dit is van toepassing op het portaal (zie eis 38) en systeem van de opdrachtnemer (zie eis 2)
71	Bij gebruik van PKI(o) certificaten beschikt de Opdrachtnemer over vastgestelde procedures voor sleutelbeheer. De Opdrachtnemer geeft bij de aanbesteding inzicht in de manier waarop sleutelbeheer is geregeld.	Dit is van toepassing op het portaal (zie eis 38) en systeem van de opdrachtnemer (zie eis 2)
72	De hosting en opslag van data vindt plaats vanaf een locatie binnen de Europees Economische Ruimte (EER).	Dit is van toepassing op het portaal (zie eis 38) en systeem van de opdrachtnemer (zie eis 2)
73	Gegevens van de Opdrachtgever worden versleuteld opgeslagen volgens de laatste stand der techniek	Dit is van toepassing op het portaal (zie eis 38) en systeem van de opdrachtnemer (zie eis 2)
74	Opdrachtnemer beschikt over een gegevens sanitatie proces dat borgt dat gegevens na maximale leeftijd worden opgeruimt en ook niet eerder dan dat. Security incident informatie dient 3 jaar te worden bewaard, waarna het wordt opgeruimd.	Dit is van toepassing op het portaal (zie eis 38) en systeem van de opdrachtnemer (zie eis 2)